

การแบ่งปันข้อมูลในบริบทการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สาขาวิชานิติศาสตร์ ไม่สังกัดภาควิชา/เทียบเท่า

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2563

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

Information sharing in the context of counter terrorism by the United Nations
Security Council



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws in Laws
Common Course
FACULTY OF LAW
Chulalongkorn University
Academic Year 2020
Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	การแบ่งปันข้อมูลในบริบทการต่อต้านการก่อการร้ายของ
	คณะมนตรีความมั่นคงแห่งสหประชาชาติ
โดย	นายธีรพันธุ์ แก้วคง
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.ศรทูล สันติवासะ

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของ
การศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

.....	คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.ปาริณา ศรีวินิชย์)	
คณะกรรมการสอบวิทยานิพนธ์	
.....	ประธานกรรมการ
(อาจารย์ ดร.สุพรรณวษา โชติกาญจน์ ถัง)	
.....	อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ศรทูล สันติवासะ)	
.....	กรรมการ
(อาจารย์ ดร.ภาวัฒน์ สัตยานุรักษ์)	

CHULALONGKORN UNIVERSITY

ธีรพันธุ์ แก้วคง : การแบ่งปันข้อมูลในบริบทการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ. (Information sharing in the context of counter terrorism by the United Nations Security Council) อ.ที่ปรึกษาหลัก : ผศ. ดร. ศรทูล สันติवासะ

การแบ่งปันข้อมูลเป็นวิธีการหนึ่งเพื่อการป้องกันและปราบปรามการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติที่มีความมุ่งหมายให้บรรดารัฐอาศัยบทบาทของความร่วมมือและการสานงานระหว่างกันทั้งระดับระหว่างประเทศและระดับภายในรัฐ แม้ว่าการแบ่งปันข้อมูลเป็นมาตรการที่ปรากฏอยู่ก่อนแล้วในตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้ายก็ตาม แต่ยังคงขาดความชัดเจนในเนื้อหาและการกำหนดกระบวนการแบ่งปันข้อมูล ในบริบทของการปราบปรามการก่อการร้ายภายใต้สหประชาชาติ คณะมนตรีความมั่นคงได้รับรองบรรดาข้อมติกำหนดขอบเขตของพันธกรณีในเนื้อหาของข้อมูลที่จะต้องแบ่งปันให้ชัดเจน กำหนดกระบวนการของการแบ่งปันข้อมูลที่เป็นขั้นตอน และกลไกของการบังคับที่มีประสิทธิภาพ ตลอดจนมีการบูรณาการทำงานร่วมกับองค์การระหว่างประเทศอื่น

จากการศึกษาค้นคว้าพบว่าการแบ่งปันข้อมูลนั้นเป็นกลไกหนึ่งซึ่งช่วยเสริมให้เกิดการบังคับใช้มาตรการต่อต้านการก่อการร้ายต่างๆของคณะมนตรีความมั่นคง อาทิ ข้อมูลที่เป็นประโยชน์ต่อการดำเนินคดีในกระบวนการยุติธรรม ข้อมูลของกิจกรรมการเงินที่เกี่ยวข้องกับการก่อการร้ายเพื่อดำเนินมาตรการปราบปรามและอายัดทรัพย์สิน ข้อมูลการเดินทางของผู้โดยสารเพื่อดำเนินมาตรการตรวจจับและยับยั้งการเดินทางของผู้ก่อการร้าย ข้อมูลที่เป็นประโยชน์ต่อการดำเนินมาตรการบังคับทางกฎหมาย และข้อมูลที่เกี่ยวข้องต่อการปราบปรามการแพร่ขยายของอาวุธที่มีอำนาจทำลายล้างสูงของการก่อการร้าย อย่างไรก็ตามการแบ่งปันข้อมูลอันนำไปสู่การบังคับใช้มาตรการต่อต้านการก่อการร้ายต่างๆนั้นขึ้นอยู่กับ การดำเนินการภายในของรัฐในการกำหนดกระบวนการทางกฎหมายและกลไกความร่วมมือ รวมไปถึงการมีความสามารถและองค์ความรู้ของรัฐในการปฏิบัติตามพันธกรณีในการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย

สาขาวิชา นิติศาสตร์

ลายมือชื่อนิสิต

ปีการศึกษา 2563

ลายมือชื่อ อ.ที่ปรึกษาหลัก

6186006834 : MAJOR LAWS

KEYWORD: International law, International organization law, United Nations, Counter terrorism, Domestic implementation, Information sharing, Security council
 Teerapan Kaewkong : Information sharing in the context of counter terrorism by the United Nations Security Council. Advisor: SARATOON SANTIVASA

Information sharing is one of means for prevention and suppression of terrorism adopted by the United Nations Security Council, by means of which states use in the context of cooperation in international and national level to combat terrorism. Even though the information sharing has already been a measure provided in universal legal instruments countering terrorism. However, its content and process has been unclear. In the context of countering against terrorism by the United Nations, the Security Council adopts resolutions clearly define scope of states' obligations regarding the information to be shared, its process and the integration of working process with other international organizations.

The research has shown that information sharing is one of the mechanisms to enhance other Security Council's enforcement of counter-terrorism measures, which are measures regarding the judicial process, financial control, detection of and ban on terrorist travel, law enforcement actions and suppression to the proliferation of weapons of mass destruction by terrorism. However, the efficiency of its enforcement depends on the domestic implementation in establishing the legal process and cooperative mechanism as well as state's capacity and knowledges to perform its obligation to share information in the context of countering terrorism.

Field of Study: Laws

Student's Signature

Academic Year: 2020

Advisor's Signature

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จได้เพราะผู้เขียนได้รับความเมตตาจาก ท่าน ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ ที่ได้กรุณารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ตลอดทั้งให้ความรู้และคำแนะนำตั้งแต่ขั้นเริ่มการพัฒนาหัวข้อ สอนวิธีการวิจัย แนะนำเอกสารที่เป็นประโยชน์ ค่อยรับฟังคำปรึกษาจากผู้เขียนมาโดยตลอด รวมทั้งให้การตรวจทาน ปรับปรุงแก้ไขเนื้อหาวิทยานิพนธ์เล่มนี้ให้สมบูรณ์ ผู้เขียนสำนึกในพระคุณและกราบขอบพระคุณท่านอาจารย์ด้วยความเคารพ

ผู้เขียนกราบขอบพระคุณท่าน อาจารย์ ดร.สุพรรณวษา โชติภิญญาณ ถัง ที่ท่านได้สละเวลาอันมีค่ามาเพื่อเป็นประธานกรรมการสอบวิทยานิพนธ์ และได้ชี้แนะประเด็นต่างๆ รวมทั้งให้ความรู้และข้อมูลของการปฏิบัติงานจริงอันเป็นประโยชน์ให้วิทยานิพนธ์เล่มนี้มีความสมบูรณ์ ผู้เขียนกราบขอบพระคุณท่าน อาจารย์ ดร.ภาวิวัฒน์ สัตยานุรักษ์ ที่ท่านได้กรุณาเป็นกรรมการสอบวิทยานิพนธ์ ทั้งได้ให้ความรู้ แนวทางการทำวิจัยที่สำคัญ ตลอดทั้งให้คำปรึกษาและคำแนะนำกับผู้เขียน และผู้เขียนกราบขอบพระคุณท่าน ศาสตราจารย์ ดร.ชุมพร ปัจจุสานนท์ ที่ได้รับผู้เขียนเป็นนิสิตผู้ช่วย มอบคำแนะนำของการทำงาน และให้คำปรึกษาในเรื่องการเรียนในระดับมหาบัณฑิตมาโดยตลอด

ผู้เขียนกราบขอบพระคุณนาย สรศักดิ์ แก้วคง ผู้เป็นบิดา และนางบุญแทน แก้วคง ผู้เป็นมารดาของผู้เขียนที่ได้อบรมสั่งสอน บ่มเพาะปลูกฝังสิ่งที่ดี ตลอดทั้งกราบขอบพระคุณบุคคลในครอบครัว กราบขอบพระคุณท่านอาจารย์ ดร.วินิตา พรหมหล้า ที่ให้แนวทางในการเรียนภาษาอังกฤษและการเรียนในระดับมหาบัณฑิต กราบขอบพระคุณท่านอาจารย์ ดร.ดวงเด่น นาคสีหราช ที่ให้ความรู้และแนวทางในการเรียนกฎหมายระหว่างประเทศ ผู้เขียนซาบซึ้งในความเมตตาของบุคคลเหล่านี้

ขอบคุณพี่วิลาสินี พี่ณัฐตา พี่กัญญ์กัศ ที่คอยช่วยเหลือให้คำแนะนำในการเรียนและการทำวิทยานิพนธ์ ตลอดทั้งคอยให้กำลังใจกับผู้เขียน ขอบคุณเจ้าหน้าที่หลักสูตร บรรดาเพื่อนในหมวดกฎหมายระหว่างประเทศ พี่ณัททัย คุณพัชรมณต์ คุณธนบรม คุณอิสริยา และอีกหลายท่านที่เป็นกำลังใจและให้คำปรึกษาผู้เขียนมาโดยตลอด สุดท้ายนี้หากวิทยานิพนธ์เล่มนี้มีคุณค่าและประโยชน์อันใดผู้เขียนขอเป็นคุณกตเวทิตาแด่คณาจารย์และผู้มีพระคุณทุกท่าน หากมีส่วนบกพร่องประการใดผู้เขียนขอน้อมรับไว้เพียงแต่ผู้เดียว

ธีรพันธุ์ แก้วคง

สารบัญ

	หน้า
.....	ค
บทคัดย่อภาษาไทย.....	ค
.....	ง
บทคัดย่อภาษาอังกฤษ.....	ง
กิตติกรรมประกาศ.....	จ
สารบัญ.....	ฉ
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา.....	1
1.2 วัตถุประสงค์ของการวิจัย	1
1.3 ข้อยสมมุติฐาน.....	2
1.4 ขอบเขตของการศึกษาวิจัย.....	2
1.5 วิธีการศึกษาวิจัย	2
1.6 ประโยชน์ที่คาดว่าจะได้รับ.....	2
บทที่ 2 บทบาทการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ	4
2.1 บทบาททั่วไปของมาตรการการแบ่งปันข้อมูล.....	4
2.1.1 บทบาทในกฎหมายระหว่างประเทศทั่วไป	5
2.1.1.1 ความร่วมมือด้านสังคมและความมั่นคง	5
2.1.1.2 ความร่วมมือด้านเศรษฐกิจและสิ่งแวดล้อม	8
2.1.2 บทบาทในตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้าย	11
2.1.2.1 ประโยชน์ของการแบ่งปันข้อมูล	20

2.1.2.2	ขอบเขตและข้อจำกัด	21
1.	สารบัญญัติ	21
2.	กระบวนการ	22
2.2	การใช้มาตรการบังคับตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงแห่งสหประชาชาติเพื่อการต่อต้านก่อการร้าย	23
2.2.1	ความมุ่งหมายและหลักการตามกฎหมายบัตรสหประชาชาติ.....	24
2.2.2	ฐานอำนาจทางกฎหมายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ	26
2.2.2.1	อำนาจและหน้าที่	26
2.2.2.2	การดำเนินการเกี่ยวกับการคุ้มครองต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกราน	28
2.2.3	ผลของมาตรการบังคับภายใต้หมวดที่เจ็ดตามกฎหมายบัตรสหประชาชาติ	31
2.2.3.1	หน้าที่ของรัฐในการปฏิบัติตามเงื่อนไขบังคับ (Mandatory term) ตามข้อมติว่าด้วยการลงโทษ	33
2.2.3.2	ความสัมพันธ์ระหว่างระบบกฎหมายระหว่างประเทศ (International legal orders) กับระบบกฎหมายภายในประเทศ (Domestic legal orders).....	35
2.3.1	ลักษณะของประเภทข้อมูลในการแบ่งปัน	36
2.3	บริบทการแบ่งปันข้อมูลภายใต้กรอบการต่อต้านก่อการร้ายของคณะมนตรีความมั่นคง	41
2.3.2	ประโยชน์และความจำเป็นของการแบ่งปันข้อมูลภายใต้กลไกบังคับ	42
2.3.3	พัฒนาการของมาตรการการแบ่งปันข้อมูล.....	43
2.3.3.1	บริบทการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายหลังสงครามเย็น	44
1.	การสร้างกระบวนการ.....	45
2.	การสร้างกลไก.....	46
2.3.3.2	บริบทการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายหลังเหตุการณ์วินาศกรรม 9/11.....	46
1.	กระบวนการที่เพิ่มเติม	49

2. กลไกที่เพิ่มเติม	51
2.3.3.3 บริบทของเหตุการณ์อื่นที่เกี่ยวกับการก่อการร้าย	53
บทที่ 3 มาตรการการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายตามมติคณะมนตรีความมั่นคงแห่งสหประชาชาติ	63
3.1 การแบ่งปันข้อมูลต่อมาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรม	63
3.1.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	63
3.1.2 สารบัญญัติ	64
1. คำนิยามของข้อมูล.....	64
2. การทำงานของมาตรการแบ่งปันข้อมูล.....	65
3.1.3 กระบวนการของความร่วมมือและการประสานงานในการแบ่งปันข้อมูล.....	65
3.1.3.1 การกำหนดกลไกในทางกฎหมาย.....	66
1. กลไกเพื่อรับรองความร่วมมือและการประสานงานระหว่างประเทศ	66
2. กลไกเพื่อรับรองความร่วมมือและการประสานงานภายในประเทศ	67
3.1.3.2 ความร่วมมือด้านกระบวนการยุติธรรม (Judicial cooperation).....	68
1. การจัดตั้งหน่วยงานผู้ประสานงานกลาง (Central authority)	68
2. ความร่วมมือทางข้อมูลกับบริษัทเอกชนภายใต้เขตอำนาจ	70
3. ความร่วมมือทางข้อมูลกับบริษัทเอกชนที่ประกอบกิจการระดับสากล	70
3.1.3.3 การประสานงานด้านกระบวนการยุติธรรม (Judicial coordination).....	76
3.1.4 เครื่องมือและข้อเสนอแนะ.....	77
3.1.4.1 ข้อเสนอของคณะกรรมการต่อต้านการก่อการร้าย (Counter terrorism committee).....	77
1. ข้อท้าทายของความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน.....	78
2. ข้อเสนอแนะในการปรับปรุงความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน	79

3.1.4.2 เครื่องมือแพลตฟอร์มของสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime).....	79
3.2 การแบ่งปันข้อมูลเพื่อปราบปรามการเข้าถึงแหล่งการเงินของการก่อการร้าย	82
3.2.1 ข้อมูลเพื่อการอายัดทรัพย์สินของกลุ่มก่อการร้าย	83
3.2.1.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	83
3.2.1.2 การจัดตั้งหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย.....	83
3.2.1.3 กระบวนการการแบ่งปันข้อมูล	85
1. การกำหนดรายชื่อบุคคลหรือกลุ่มบุคคล (Listing).....	85
2. การทบทวนรายชื่อบุคคลหรือกลุ่มบุคคล (Reviewing)	86
3. การเพิกถอนรายชื่อบุคคลหรือกลุ่มบุคคล (Delisting).....	87
3.2.1.4 การประสานงานของคณะกรรมการ Sanctions.....	88
3.2.2 ข้อมูลเพื่อการปราบปรามกิจกรรมการมีส่วนร่วมทางการเงินกับการก่อการร้าย.....	89
3.2.2.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	89
1. โครงสร้างของกระบวนการ	90
1.1 การจัดตั้งหน่วยข่าวกรองทางการเงิน	90
1.2 ความร่วมมือระหว่างประเทศ.....	91
1.3 ความร่วมมือกับสถาบันทางการเงิน	91
1.4 การประสานงาน	92
1.5 ข้อท้าทาย	92
2. ข้อมูลการบริการกระเป๋าสตางค์ดิจิทัล	93
2.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง.....	94
2.2 กระบวนการ	94
2.3 เครื่องมือในการดำเนินการ	96

3. ข้อมูลการบริการสินทรัพย์เสมือน	98
3.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง.....	99
3.2 กระบวนการ	100
3.3 ข้อท้าทายใหม่ของสินทรัพย์เสมือน	103
4. ข้อมูลการระดมทุนผ่านระบบอินเทอร์เน็ต	105
4.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง.....	106
4.2 กระบวนการ	106
4.3 ตัวอย่างข้อปฏิบัติของบริษัทเอกชน	107
4.4 ข้อท้าทายใหม่ของการระดมทุนผ่านระบบอินเทอร์เน็ต	109
5. ข้อมูลติดตามรูปแบบการเงินของการก่อการร้าย	110
5.1 ข้อเสนอแนะของคณะกรรมการการต่อต้านการก่อการร้าย	112
5.2 กระบวนการตามข้อเสนอแนะ	112
5.3 กลไกความร่วมมือ.....	113
6. ข้อมูลการสำแดงเงินสดที่มีประสิทธิภาพ (Effective cash declaration systems).....	116
6.1 ข้อเสนอแนะของคณะกรรมการการต่อต้านการก่อการร้าย	116
6.2 กระบวนการและกลไกตามข้อเสนอแนะ	116
3.2.2.2 ข้อเสนอแนะของหน่วยงานระหว่างประเทศ	120
1. ข้อเสนอแนะของสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ	120
2. ข้อเสนอแนะของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน.....	121
3.3 การแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย.....	122
3.3.1 การควบคุมชายแดนให้ได้มีประสิทธิภาพ	122
3.3.1.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	122

3.3.1.2	สารบัญญัติ.....	123
3.3.1.3	กระบวนการในการแบ่งปันข้อมูล	124
	1. การจัดตั้งหน่วยงานในความร่วมมือระหว่างประเทศ.....	125
	2. การกำหนดกลไกในความร่วมมือ	125
	3. ข้อท้าทายกับประเด็นนักรบต่างชาติ.....	127
3.3.2	การตรวจบุคคลที่เดินทางเข้าประเทศด้วยข้อมูลผู้โดยสารล่วงหน้า ข้อมูลการบันทึกของ ผู้โดยสาร และข้อมูลลักษณะเฉพาะตัวบุคคล	128
3.3.2.1	พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	129
	1. การแบ่งปันข้อมูลผู้โดยสารล่วงหน้า.....	129
	2. การแบ่งปันข้อมูลการบันทึกของผู้โดยสาร	130
	3. การแบ่งปันข้อมูลลักษณะเฉพาะตัวของผู้โดยสาร.....	131
3.3.2.2	สารบัญญัติของข้อมูล	132
3.3.2.3	กระบวนการในการแบ่งปันข้อมูล	136
	1. โครงสร้างของกระบวนการ	136
	2. ข้อปฏิบัติในการดำเนินการ.....	142
3.3.2.4	มาตรฐานการดำเนินการขององค์การการบินพลเรือนระหว่างประเทศ	149
3.3.3	ข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้าระวังและฐานข้อมูล.....	158
3.3.3.1	พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	158
3.3.3.2	สารบัญญัติ	158
3.3.3.3	กระบวนการในการแบ่งปันข้อมูล	159
3.3.3.4	กลไกควบคุมการใช้ในทางที่ผิด.....	162
3.4	การแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้าย.....	163
3.4.1	พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	163
3.4.2	สารบัญญัติของข้อมูล.....	164

3.4.3	กระบวนการในการแบ่งปันข้อมูล.....	165
3.4.3.1	การจัดตั้งหน่วยงาน.....	165
1.	หน่วยงานปราบปรามการก่อการร้าย.....	165
2.	การทำงานของหน่วยงานปราบปรามการก่อการร้าย	166
3.	สำนักงานกลางแห่งชาติ.....	167
4.	การทำงานของสำนักงานกลางแห่งชาติ	167
3.4.2.2	ความร่วมมือและการประสานงาน.....	169
1.	ความร่วมมือระหว่างประเทศ	169
2.	การประสานงานกับองค์การตำรวจอาชญากรรมระหว่างประเทศ	169
3.4.4	เครื่องมือและกลไกเสริมในการแบ่งปันข้อมูล.....	170
3.5	การแบ่งปันข้อมูลต่อการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงเพื่อใช้ในการก่อการร้าย	174
3.5.1	พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง	174
3.5.2	สารบัญญัติของข้อมูล.....	175
3.5.2.1	อาวุธอานุภาพทำลายล้างสูงและวัสดุเกี่ยวข้อง	176
3.5.2.2	วิธีการขนส่งและการเงิน.....	178
3.5.3	มาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายที่เกี่ยวข้องกับอาวุธ	178
3.5.3.1	สารบัญญัติ.....	179
3.5.3.2	กระบวนการ.....	180
3.5.4	กระบวนการในการแบ่งปันข้อมูลต่อคณะกรรมการลงโทษ	183
3.5.4.1	กระบวนการในการรายงานข้อมูล.....	183
3.5.4.2	รายการในการรายงานข้อมูล	184
3.5.5	ความช่วยเหลือระหว่างประเทศและคำแนะนำ	207
3.5.5.1	องค์การระหว่างประเทศ	207

3.5.5.2 องค์การส่วนภูมิภาค	210
3.6 ตารางสรุปมาตรการการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ.....	211
บทที่ 4 ปัญหาและลู่ทางของการดำเนินมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ	3
4.1 ปัญหาและแนวปฏิบัติจากการดำเนินมาตรการแบ่งปันข้อมูลของรัฐ	3
4.1.1 ปัญหากระบวนการทางกฎหมาย	3
4.1.2 ปัญหาการบังคับใช้กฎหมาย	10
4.1.3 แนวปฏิบัติทางกฎหมายของประเทศไทย.....	15
4.2 ผลกระทบของภาคธุรกิจในการดำเนินมาตรการแบ่งปันข้อมูล	23
4.2.1 ต้นทุนของมาตรการรักษาความปลอดภัย	24
4.2.2 ต้นทุนค่าเสียโอกาส	25
4.3 ผลกระทบต่อผู้มีส่วนเกี่ยวข้องที่เป็นเจ้าของข้อมูล	26
4.3.1 ภาคธุรกิจผู้ให้บริการเทคโนโลยีการสื่อสาร	26
4.3.1.1 การปกป้องข้อมูลของผู้รับบริการ	27
4.3.1.2 การกำหนดมาตรการเยียวยา.....	28
4.3.2 สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงิน.....	29
4.3.2.1 หน้าที่ในการคุ้มครองผลประโยชน์ของลูกค้า	29
4.3.2.2 การปฏิบัติตามข้อกำหนดการป้องกันการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย	30
4.3.2.3 การเยียวยาความเสียหายต่อลูกค้า	31
4.3.3 ปัจเจกชน	32
4.3.3.1 ปัญหาด้านสิทธิความเป็นส่วนตัว	32
4.3.3.2 แนวทางการป้องกันทางกฎหมายและข้อแนะนำ	38
4.3.3.3 แนวปฏิบัติทางกฎหมายประเทศไทยในการปกป้องสิทธิความเป็นส่วนตัว	51

4.3.4 ผลกระทบในมิติอื่นที่เกี่ยวข้องกับการแบ่งปันข้อมูล.....	59
4.3.4.1 ปัญหาของผู้ถูกกล่าวหาว่าเกี่ยวข้องกับก่อการร้ายโดยมิชอบ.....	59
4.3.4.2 ข้อเสนอสำหรับการเยียวยา	60
บทที่ 5 บทสรุปและเสนอแนะ.....	63
บทสรุป.....	63
ข้อเสนอแนะ	66
บรรณานุกรม.....	68
ประวัติผู้เขียน.....	76



จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

มาตรการการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย มีจุดประสงค์ขึ้นก็เพื่อต้องการให้รัฐในสังคมนระหว่างประเทศมีการประสานงานและร่วมมือกันในการแบ่งปันข้อมูล เพื่อการเตรียมการป้องกันและปราบปรามการก่อการร้าย โดยข้อมูลที่ถูกแบ่งปันมานั้นมีความจำเป็นในการใช้เป็นส่วนหนึ่งในการดำเนินมาตรการปราบปรามในด้านต่างๆ อาทิ มาตรการบังคับทางการเงิน มาตรการควบคุมและตรวจจับการเดินทางของการก่อการร้าย รวมถึงการบังคับนำตัวผู้ก่อการร้ายเข้าสู่กระบวนการยุติธรรม

ทั้งนี้บรรดารัฐในสังคมนระหว่างประเทศมีพันธกรณีในการดำเนินมาตรการแบ่งปันข้อมูลภายใต้กรอบการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงตามหมวดที่เจ็ดแห่งกฎบัตรสหประชาชาติ อันยึดถือแนวทางของหลักความมั่นคงร่วมที่สะท้อนออกมาว่าปัญหาการก่อการร้ายนั้นไม่ใช่ปัญหาของประเทศใดประเทศหนึ่งอีกต่อไป รัฐใดรัฐหนึ่งจะดำเนินการต่อต้านการก่อการร้ายอย่างลำพังต่อไปมิได้แล้ว บรรดารัฐในสังคมนระหว่างประเทศควรจะต้องร่วมมือกันในการแบ่งปันข้อมูลเพื่อดำเนินการปราบปรามการก่อการร้ายโดยอาศัยการกำหนดบทบาททั้งด้านความร่วมมือและการประสานงานระหว่างกัน รวมไปถึงการได้กำหนดกระบวนการของการแบ่งปันข้อมูลทั้งในระดับระหว่างประเทศ ระดับภายในประเทศ และพิจารณาอาศัยกลไกเสริมที่จะทำให้กระบวนการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้ายดำเนินการอย่างลุล่วงไปด้วยดี

ดังนั้นการทำวิจัยและการศึกษาในหัวข้อนี้ จำเป็นที่จะต้องศึกษาทั้งบทบาทของการแบ่งปันข้อมูลตลอดจนบริบทของการดำเนินมาตรการ ทั้งพันธกรณีของคณะมนตรีความมั่นคงในด้านสารบัญญัติ และกระบวนการของการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย จนถึงผลกระทบที่อาจเกิดขึ้นจากการดำเนินมาตรการซึ่งผู้เขียนจะได้ทำการศึกษาในแต่ละบทต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1. ศึกษาและวิเคราะห์การแบ่งปันข้อมูลในแง่ของการป้องกันและปราบปรามการก่อการร้าย
2. ศึกษาและวิเคราะห์การแบ่งปันข้อมูลในการหาข้อมูลเบาะแสอันเป็นประโยชน์ในการดำเนินการสืบสวนสอบสวนที่เกี่ยวข้องกับการก่อการร้าย
3. ศึกษาและวิเคราะห์การแบ่งปันข้อมูลและพยานหลักฐานอันเป็นประโยชน์ต่อการดำเนินคดีในกระบวนการยุติธรรม

4. ศึกษาและวิเคราะห์การแบ่งปันข้อมูลที่เป็นประโยชน์ต่อการยับยั้งปัจจัยเสี่ยงที่จะนำไปสู่การก่อการร้ายในรูปแบบใหม่

1.3 ข้อสมมุติฐาน

พันธกรณีการแบ่งปันข้อมูลเพื่อการป้องกันและปราบปรามการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ เป็นกลไกหนึ่งที่จะช่วยขับเคลื่อนการบังคับใช้มาตรการต่อต้านการก่อการร้ายอื่น อย่างไรก็ตามประสิทธิภาพของการบังคับใช้มาตรการการแบ่งปันข้อมูลเพื่อการป้องกันและปราบปรามการก่อการร้ายขึ้นอยู่กับความสามารถของบรรดารัฐต่างๆ ในการดำเนินการภายในรัฐ

1.4 ขอบเขตของการศึกษาวิจัย

มุ่งเน้นศึกษาข้อสมมุติของคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ว่าด้วยมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้าย รวมถึงมาตรการอื่นๆ ที่เกี่ยวข้อง ข้อเสนอแนะ กฎหมายระหว่างประเทศที่เกี่ยวข้องกับการต่อต้านการก่อการร้าย ความตกลงในการร่วมมือเพื่อต่อต้านการก่อการร้าย หลักกฎหมายที่เกี่ยวข้องกับองค์การระหว่างประเทศ

1.5 วิธีการศึกษาวิจัย

การวิจัยนี้จะเป็นการวิจัยทางเอกสาร (Documentary Research) โดยศึกษาค้นคว้าข้อมูลและวิเคราะห์จากกฎหมายระหว่างประเทศ หนังสือกฎหมาย ตำราในทางวิชาการ บทความในฐานข้อมูลในประเทศและต่างประเทศ วารสาร รายงานทางวิชาการ ข่าวจากสำนักข่าวในประเทศและต่างประเทศ ข้อมูลทางระบบคอมพิวเตอร์และระบบอินเทอร์เน็ตที่เกี่ยวข้องกับการต่อต้านการก่อการร้าย เอกสารเผยแพร่หรือรายงานของหน่วยงานในทางราชการในประเทศและต่างประเทศ รวมทั้งบริษัทเอกชนทั้งที่เป็นภาษาไทยและภาษาอังกฤษ สัมภาษณ์เชิงสนทนากับผู้ทรงคุณวุฒิ และผู้ที่มีประสบการณ์หรือบุคคลที่ได้ทำการศึกษาในแวดวงของเรื่องดังกล่าวนี้ ตลอดจนนำข้อมูลจากเอกสารในแขนงอื่นและหาข้อสรุป

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. วิเคราะห์ให้เห็นถึงประเด็นที่สามารถนำไปสู่การพัฒนาแนวทางของการแบ่งปันข้อมูลเพื่อการป้องกันและปราบปรามการก่อการร้ายรูปแบบใหม่
2. วิเคราะห์ให้เห็นถึงประเด็นที่เป็นปัญหาการดำเนินการแบ่งปันข้อมูลและเสนอแนวทางของการแก้ไขเพื่อให้เกิดความยั่งยืนในการปราบปรามการก่อการร้าย

3. ผลจากการศึกษาวิเคราะห์สามารถนำไปเป็นแนวทางเพื่อการปรับใช้ต่อการดำเนินการ
แบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของประเทศไทย



บทที่ 2

บทบาทการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ

ปัญหาการก่อการร้ายในปัจจุบันนี้ได้ส่งผลกระทบต่อความมั่นคงในหลายๆประเทศ การโจมตีประชาชนหรือสาธารณะสมบัติของพลเรือนทั่วไปจนนำมาสู่ความเสียหายแก่ชีวิต ทรัพย์สิน เศรษฐกิจของประเทศ และสภาพทางสังคมวัฒนธรรม การก่อการร้ายได้อาศัยช่องว่างของมาตรการปราบปรามหลักความรับผิดชอบในทางกฎหมาย ดังเช่นมีการสร้างเครือข่ายการดำเนินงานที่มีได้จำกัดอยู่ภายใต้เขตอำนาจของรัฐใดรัฐหนึ่ง สรรค์หาวิธีการใหม่ๆในการเข้าถึงแหล่งการเงินและการสนับสนุนเงิน การเข้าถึงอาวุธที่มีคุณภาพทำลายร้ายสูง รวมทั้งอาศัยการคมนาคมที่สะดวกสบายในปัจจุบันกระจายตัวเพื่อดำเนินการก่อเหตุในหลายประเทศ และเป็นอุปสรรคของผู้บังคับใช้กฎหมายด้วยเหตุนี้ถึงนำไปสู่บทบาทการปราบปรามการก่อการร้ายที่สำคัญโดยจะต้องอาศัยความร่วมมือของสมาชิกสังคมระหว่างประเทศที่จะต้องให้ร่วมมือกันซึ่งกันและกันเพื่อให้เกิดประสิทธิภาพในการปราบปราม โดยบทบาทของการปราบปรามหนึ่งนั้นคือการแบ่งปันข้อมูล (Information-sharing)

ดังนั้นในบทนี้ผู้เขียนจะขออธิบายถึงบทบาทของมาตรการการแบ่งปันข้อมูลในความร่วมมือระหว่างประเทศทั่วไป และโดยเฉพาะอย่างยิ่งในกรอบบริบทของการปราบปรามการก่อการร้ายตามตราสารระหว่างประเทศเพื่อชี้ให้เห็นถึงแนวคิดในทางกฎหมาย เจื่อนไข ขอบเขตและข้อจำกัด ก่อนนำเข้าสู่บริบทการรักษาสันติภาพและความมั่นคงของคณะมนตรีความมั่นคงแห่งสหประชาชาติในการปราบปรามการก่อการร้ายซึ่งเป็นภัยคุกคามต่อสันติภาพในปัจจุบันที่ต้องอาศัยความร่วมมือของบรรดาระัฐในสังคมระหว่างประเทศ

2.1 บทบาททั่วไปของมาตรการการแบ่งปันข้อมูล

ในกรอบความร่วมมือระหว่างประเทศในทั้งด้านเศรษฐกิจ สังคม หรือความมั่นคงของชาติ การดำเนินการแบ่งปันข้อมูลถือเป็นกลไกหนึ่งเพื่อบรรลุวัตถุประสงค์ตามกรอบความร่วมมือต่างๆ โดยบทบาทสำคัญของการแบ่งปันข้อมูลคือการที่รัฐภายใต้ความร่วมมือได้รับรู้ถึงข้อมูลระหว่างกันเพื่อนำข้อมูลดังกล่าวไปดำเนินการให้เกิดประสิทธิภาพตามเป้าหมาย ซึ่งการมีส่วนร่วมของรัฐในการแบ่งปันข้อมูลนี้เอง จึงก่อให้เกิดการสร้างเครือข่ายของการทำงานร่วมกัน ในการแก้ปัญหาใหญ่บางอย่าง อาทิ ปัญหาในเรื่องเศรษฐกิจ สังคม วัฒนธรรม รวมไปถึงเพื่อบรรลุเป้าหมายของการรักษาความปลอดภัย สันติภาพ และความมั่นคงของประเทศ

ดังนั้นในหัวข้อเริ่มต้นนี้ผู้เขียนจะยกตัวอย่างพันธกรณีระหว่างประเทศว่าด้วยการแบ่งปันข้อมูล ซึ่งได้ปรากฏอยู่ในอนุสัญญาระหว่างประเทศต่างๆ ตลอดทั้งการแบ่งปันข้อมูลตามแผนงาน

หรือโครงการระหว่างประเทศเพื่อการพัฒนาทางด้านเศรษฐกิจและสังคม เพื่อให้ได้เข้าถึงบริบทและประโยชน์ของมาตรการแบ่งปันข้อมูลโดยทั่วไป

2.1.1 บทบาทในกฎหมายระหว่างประเทศทั่วไป

หัวข้อนี้ผู้เขียนต้องการที่จะแสดงถึงบทบาทของการแบ่งปันข้อมูลเพื่อให้ทราบในขั้นแรกถึงแนวคิดโดยทั่วไปและแนวคิดในทางกฎหมายของการแบ่งปันข้อมูล โดยจะทำการศึกษากฎหมายระหว่างประเทศ อาทิ อนุสัญญาระหว่างประเทศและความร่วมมือระหว่างประเทศในด้านต่างๆ

2.1.1.1 ความร่วมมือด้านสังคมและความมั่นคง

1.) สนธิสัญญาว่าด้วยการค้าอาวุธ (Arms Trade Treaty 2013)

สนธิสัญญาว่าด้วยการค้าอาวุธ ค.ศ. 2013 มีวัตถุประสงค์หลักคือการป้องกันและจัดการค้าอาวุธแบบเดิมที่ผิดกฎหมาย และสร้างหลักเกณฑ์ระหว่างรัฐผู้ซื้อกับรัฐผู้ขายว่าจะพิจารณาการซื้อขายอาวุธที่เป็นไปตามการเคารพซึ่งกฎหมายสิทธิมนุษยชนระหว่างประเทศ กฎหมายมนุษยธรรมระหว่างประเทศ กฎหมายว่าด้วยการต่อต้านการก่อการร้ายระหว่างประเทศ และมาตรการคว่ำบาตรด้านอาวุธ (Arms Embargo)¹ มาตรการแบ่งปันข้อมูลได้มีบทบาทเข้าไปส่งเสริมรัฐภาคีให้กำหนดความร่วมมือเพื่อช่วยเหลือการปฏิบัติตามข้อบัพัญญัติของสนธิสัญญานี้ รวมถึงการแบ่งปันข้อมูลเกี่ยวกับกิจกรรมและข้อมูลของผู้ดำเนินการที่ผิดกฎหมาย เพื่อป้องกันและจัดการถ่ายโอนซึ่งอาวุธตามแบบแผนซึ่งครอบคลุมอยู่ภายใต้สนธิสัญญานี้ โดยในกระบวนการแบ่งปันข้อมูลรัฐภาคีต้องจัดตั้งและกำหนดหน่วยงานซึ่งทำหน้าที่เป็นจุดติดต่อระดับชาติ (National points of contact)² เพื่อเป็นช่องทางในการแลกเปลี่ยนข้อมูลในเรื่องที่เกี่ยวข้องกับการปฏิบัติตามสนธิสัญญา รัฐภาคีแต่ละรัฐต้องแจ้งให้สำนักเลขาธิการทราบถึงหน่วยงานซึ่งทำหน้าที่เป็นจุดติดต่อระดับชาติของตน และทำการแบ่งปันข้อมูลเพื่ออัปเดตให้เป็นปัจจุบันอยู่เสมอ

2.) อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการลักลอบค้ายาเสพติดและวัตถุที่ออกฤทธิ์ต่อจิตประสาท ค.ศ. 1988 (United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988)

สหประชาชาติได้มีการจัดทำอนุสัญญานี้ขึ้นมาจากปัญหายาเสพติดที่สร้างผลกระทบมากมายทั้งในประเทศที่กำลังพัฒนา และประเทศที่พัฒนาแล้ว การเพิ่มมากขึ้นของการค้ายาเสพติดที่

¹ วิลาลินี หมายเจริญศรี, "การเข้าเป็นภาคีสนธิสัญญาว่าด้วยการค้าอาวุธ ค.ศ. 2013 ของประเทศไทย : ปัญหาและลู่ทาง" (จุฬาลงกรณ์มหาวิทยาลัย, พ.ศ. 2559). วิลาลินี หมายเจริญศรี, "การเข้าเป็นภาคีสนธิสัญญาว่าด้วยการค้าอาวุธ ค.ศ. 2013 ของประเทศไทย : ปัญหาและ ลู่ทาง" (จุฬาลงกรณ์มหาวิทยาลัย, พ.ศ. 2559).

² Arms Trade Treaty 2013, Article 5, 15

ผิดกฎหมาย การค้ายาเสพติดระหว่างประเทศจึงกลายเป็นธุรกิจมูลค่าหลายพันล้านดอลลาร์ที่ถูกครอบงำโดยกลุ่มอาชญากร กลุ่มการก่อการร้าย กลุ่มผู้มีอิทธิพล ซึ่งเป็นเหตุให้เกิดการก่อตั้งอนุสัญญาฉบับนี้³

มาตรการแบ่งปันข้อมูลได้มีบทบาทเข้าไปส่งเสริมในส่วนข้อบทที่ว่าด้วยความช่วยเหลือซึ่งกันและกัน (Mutual legal assistance) ในอนุสัญญากำหนดให้รัฐภาคีจะต้องให้ความช่วยเหลือทางกฎหมายซึ่งกันและกันอย่างกว้างขวางที่สุดต่อการสอบสวน การดำเนินคดี และกระบวนการยุติธรรมที่เกี่ยวข้องกับความผิดทางอาญาที่จัดตั้งขึ้นตามอนุสัญญาฉบับนี้ โดยให้มีการแบ่งปันข้อมูล และรายการของพยานหลักฐาน ระหว่างรัฐภาคีด้วยกัน อำนวยความสะดวกในการแลกเปลี่ยนข้อมูลที่ปลอดภัยและรวดเร็วเกี่ยวกับความผิดทุกด้านที่กำหนดไว้ในอนุสัญญา⁴ ดังนั้นบทบาทของมาตรการแบ่งปันข้อมูลเป็นช่องทางที่ก่อให้เกิดการแลกเปลี่ยนพยานหลักฐานอันเป็นประโยชน์ต่อการดำเนินคดีในกระบวนการยุติธรรมระหว่างรัฐภาคี ทั้งยังเป็นช่องทางในการสื่อสารระหว่างเพื่อการอำนวยความสะดวกในการแลกเปลี่ยนข้อมูลที่ปลอดภัยและรวดเร็วเกี่ยวกับความผิดทุกด้านที่กำหนดไว้ในอนุสัญญา

3.) อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการทุจริต ค.ศ. 2003 (United Nations Convention against Corruption 2003)

ประชุมสมัชชาใหญ่แห่งสหประชาชาติได้รับรองอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการทุจริต⁵ มีวัตถุประสงค์สำคัญคือเพื่อป้องกัน ตรวจสอบ และยับยั้งการโอนทรัพย์สินระหว่างประเทศที่ได้มาโดยผิดกฎหมาย และเพื่อเสริมสร้างความร่วมมือระหว่างประเทศในการส่งทรัพย์สินเหล่านั้นกลับคืนประเทศต้นทาง

โดยมาตรการแบ่งปันข้อมูลได้มีบทบาทในการส่งเสริมความร่วมมือและแลกเปลี่ยนข้อมูล ในระดับชาติ และระดับนานาชาติ เพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ต่อการวิเคราะห์ การโอนทรัพย์สิน หรือการฟอกเงิน รวมถึงความผิดอื่นตามอนุสัญญาได้กำหนด อันจะนำไปสู่การดำเนินมาตรการบังคับกฎหมายหรือการบังคับทรัพย์สินเหล่านั้นกลับคืนสู่ประเทศต้นทาง⁶ ดังนั้นแล้วบทบาทของการแบ่งปันข้อมูลเป็นวิธีการที่เข้าไปเสริมการดำเนินมาตรการต่อต้านการฟอกเงินโดยมี

³ Amira Armenta, Martin Jelsma, "What are the UN drug control conventions and what is their purpose?" (08 October 2015), Retrieved from <https://www.tni.org/en/publication/the-un-drug-control-conventions>

⁴ United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988, Article 7, 9, 20, Final act

⁵ United Nations Office on Drugs and Crime, "Background of The United Nations Convention against Corruption", Retrieved from <https://www.unodc.org/unodc/en/corruption/uncac.html>

⁶ United Nations Convention against Corruption 2003, Article 14, 46, 48

กระบวนการแบ่งปันข้อมูลให้หน่วยงานบังคับใช้กฎหมายหน่วยงานอื่นๆ ที่เกี่ยวข้องต่อการต่อต้านการฟอกเงินแลกเปลี่ยนข้อมูลระหว่างกันตามที่ถูกกำหนดไว้ในอนุสัญญา

4.) อนุสัญญาสหประชาชาติต่อต้านองค์กรอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ.2000 (United Nation Convention Against Transnational Organized Crime 2000)

อาชญากรรมข้ามชาติได้กลายเป็นประเด็นด้านความปลอดภัยที่สำคัญในวาระระดับระหว่างประเทศ⁷ อันนำมาสู่วันที่ 15 พฤศจิกายน พ.ศ. 2543 อนุสัญญาสหประชาชาติเพื่อต่อต้านองค์กรอาชญากรรมข้ามชาติ (UNTOC) ได้รับการรับรองโดยสมัชชาใหญ่แห่งสหประชาชาติโดยมีวัตถุประสงค์สำคัญคือ ปฏิเสธที่หลบภัยสำหรับผู้ที่มีส่วนเกี่ยวข้องในองค์กรอาชญากรรมข้ามชาติ กำหนดให้มีการดำเนินคดีกับอาชญากรรมไม่ว่าการกระทำนั้นจะเกิดขึ้นที่ไหนโดยอาศัยความร่วมมือในระดับระหว่างประเทศ⁸

มาตรการแบ่งปันข้อมูลได้มีบทบาทสำคัญในการส่งเสริมข้อบทที่ว่าด้วยความช่วยเหลือซึ่งกันและกัน ในอนุสัญญาที่กำหนดให้รัฐภาคีจะต้องมีช่องทางของการแบ่งปันข้อมูลและพยานหลักฐานที่มีประสิทธิภาพเพียงพอ มากไปกว่านั้นในส่วนของความร่วมมือด้านการบังคับใช้กฎหมาย อนุสัญญาฉบับนี้ได้ระบุให้รัฐภาคีจะต้องร่วมมืออย่างใกล้ชิดกับอีกฝ่ายหนึ่ง โดยสอดคล้องกับระบบกฎหมายและการบริหารภายในประเทศของตน เพื่อเพิ่มประสิทธิภาพของการบังคับใช้กฎหมาย อำนวยความสะดวกในการแลกเปลี่ยนข้อมูล อันเกี่ยวกับความผิดทุกด้านที่ครอบคลุมในอนุสัญญานี้

ดังนั้นจากตัวอย่างมาตรการแบ่งปันข้อมูลในอนุสัญญาระหว่างประเทศที่ได้ยกมานั้น ได้สะท้อนถึงประโยชน์ของมาตรการแบ่งปันข้อมูลซึ่งเป็นกลไกหนึ่งในการขับเคลื่อนมาตรการต่างๆ อาทิ การป้องกันปัญหาการลักลอบค้ายาเสพติดและวัตถุที่ออกฤทธิ์ต่อจิตประสาท การต่อต้านการทุจริต และการต่อต้านองค์กรอาชญากรรมข้ามชาติ ตลอดจนยังเป็นกลไกในการให้ความช่วยเหลือทางด้านการกระบวนการยุติธรรมและการบังคับใช้กฎหมายของบรรดารัฐภาคีภายใต้อนุสัญญานี้

⁷ US Federal Bureau of Investigation, "Transnational Organized Crime", Retrieved from <https://www.fbi.gov/investigate/organized-crime>

⁸ Council on Foreign Relations, "The Global Regime for Transnational Crime" (September 8, 2015)

2.1.1.2 ความร่วมมือด้านเศรษฐกิจและสิ่งแวดล้อม

1.) อนุสัญญาสหประชาชาติว่าด้วยกฎหมายทะเล ค.ศ. 1982 (United Nations Convention on the Law of the Sea 1982)

อนุสัญญาสหประชาชาติว่าด้วยกฎหมายทะเล ค.ศ. 1982 (United Nations Convention on the Law of the Sea 1982) มีวัตถุประสงค์หลักในการกำหนดกฎเกณฑ์ครอบคลุมเรื่องต่างๆ อาทิ สิทธิและหน้าที่ของรัฐต่าง ๆ ในเขตทางทะเล ทั้งน่านน้ำภายใน ทะเลอาณาเขต เขตต่อเนื่อง เขตเศรษฐกิจจำเพาะ เขตไหล่ทวีป ทะเลหลวง การใช้ประโยชน์จากทรัพยากรธรรมชาติทางทะเล การคุ้มครองและรักษาสิ่งแวดล้อมทางทะเล การวิจัยวิทยาศาสตร์ทางทะเล เป็นต้น⁹

มาตรการแบ่งปันข้อมูลมีบทบาทสำคัญในการช่วยปกป้องและการบำรุงรักษาสิ่งแวดล้อมทางทะเล (Protection and Preservation of the Marine Environment) โดยอนุสัญญาได้กำหนดให้รัฐภาคีแลกเปลี่ยนข้อมูล เพื่อเป็นประโยชน์ในการส่งเสริมการศึกษาหรือดำเนินโครงการวิจัยทางวิทยาศาสตร์ และส่งเสริมให้เกิดการแลกเปลี่ยนข้อมูล ที่เกี่ยวข้องกับข้อมูลของมลพิษ สิ่งแวดล้อมทางทะเล ทั้งนี้รัฐภาคีของอนุสัญญาจะต้องให้ความร่วมมือระดับภูมิภาค และระดับระหว่างประเทศ เพื่อการได้รับข้อมูลความรู้สำหรับข้อมูลการประเมินมลพิษทางทะเล ข้อมูลเส้นทางความเสี่ยงของสิ่งแวดล้อมทางทะเล มากไปกว่านั้นข้อบทที่ว่า การส่งเสริมความร่วมมือระหว่างประเทศ¹⁰ ในอนุสัญญาได้ระบุไว้ให้รัฐและองค์กรระหว่างประเทศที่มีอำนาจต้องส่งเสริมความร่วมมือระหว่างประเทศ ในการวิจัยทางวิทยาศาสตร์ทางทะเลโดยมีจุดประสงค์ที่สันติตามหลักการเคารพในอธิปไตยและเขตอำนาจของรัฐ และบนพื้นฐานของผลประโยชน์ร่วมกัน ตลอดทั้งมีการแบ่งปันข้อมูลที่เป็นในการป้องกันและควบคุมความเสียหายต่อสุขภาพและความปลอดภัยของบุคคลและสิ่งแวดล้อมทางทะเล

2.) ความร่วมมือทางเศรษฐกิจในเอเชียแปซิฟิก (Asia-Pacific Economic Cooperation)

การแบ่งปันข้อมูลระหว่างประเทศภายใต้เขตการค้าเสรี มีบทบาทช่วยแบ่งปันภูมิปัญญาและแนวปฏิบัติที่มีประสิทธิภาพของนโยบายทางการค้า จะสร้างช่วยเพิ่มศักยภาพในการแข่งขันและการต่อรองให้กับภูมิภาค และเขตการค้าเสรี ในกรณีความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (APEC) ได้มีการรับรองแผนกลไกการแบ่งปันข้อมูลในความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิกเกี่ยวกับ

⁹ กรมสนธิสัญญาและกฎหมาย, "กฎหมายระหว่างประเทศด้านทะเล สิ่งแวดล้อม และสังคม", Retrieved from <https://treaties.mfa.go.th/กฎหมายระหว่างประเทศ/กฎหมายทะเล>

¹⁰ United Nations Convention on the Law of the Sea 1982, Article 200, 242

ข้อตกลงการค้าระดับภูมิภาคและข้อตกลงการค้าเสรี¹¹ (APEC Information Sharing Mechanism on Regional Trade Agreements RTAs and FTAs) ทุกประเทศภายใต้ความร่วมมือจะต้องจัดสรรข้อมูลต่อการส่งเสริมเขตการค้าเสรีและความสะดวกให้การเข้าถึงข้อมูล เช่น จะต้องตีพิมพ์รายงานเกี่ยวกับนโยบายการค้าในรูปแบบภาษาอังกฤษในเว็บไซต์ของกระทรวงพาณิชย์ของประเทศตน และแบ่งปันลิงก์เว็บไซต์แต่ละหน่วยงานที่เกี่ยวข้องกับการดำเนินการค้าเสรี¹² อาทิ กระทรวงพาณิชย์ กรมการค้าต่างประเทศ เพื่อถ่ายทอดประเทศสมาชิกในการเข้าถึงข้อมูลแบบ one-stop compilation และเป็นประโยชน์เพื่อการอ้างอิงในรายงาน

3.) เป้าหมายการพัฒนาที่ยั่งยืน (Sustainable Development Goals)

การแบ่งปันข้อมูลสามารถช่วยให้ประเทศสมาชิกประสบความสำเร็จตามเป้าหมายของ SDG ได้อย่างมีประสิทธิภาพ เป้าหมายการพัฒนาที่ยั่งยืนในด้านเศรษฐกิจและสังคมนับเป็นกรอบทิศทางพัฒนาในหลายประเทศทั่วโลกภายหลังจากปี 2015 องค์การสหประชาชาติได้รับรองวาระเป้าหมายพัฒนาอย่างยั่งยืน โดยองค์ประกอบของปัจจัยความสำเร็จของการพัฒนาที่ยั่งยืนอยู่ 5 ประการ เช่น 1. การขจัดความยากจนความหิวโหยท่ามกลางประชาชนและลดความเหลื่อมล้ำในสังคม 2. เสริมสร้างความมั่นคงของประชาชนให้มีวิถีชีวิตการกินดีอยู่ดีและสอดคล้องต่อธรรมชาติ 3. ปกป้องดูแลซึ่งทรัพยากรธรรมชาติ และสภาพภูมิอากาศเพื่อคนรุ่นหลัง 4. การอยู่ร่วมกันอย่างมีสันติ และ 5. ให้ความร่วมมือในการพัฒนาที่ยั่งยืนในระดับโลก¹³ ซึ่งการร่วมมือกันเพื่อพัฒนาเศรษฐกิจและสังคมที่ยั่งยืนนี้เองนำมาซึ่งการให้ความช่วยเหลือต่อการแบ่งปันข้อมูลองค์ความรู้ระหว่างประเทศต่าง ๆ ร่วมกันโดยการแบ่งปันข้อมูล เข้าสู่ฐานข้อมูลแบบเปิด โดยรัฐสมาชิกต่างๆ ของสหประชาชาติ นั้น เป็นประโยชน์ต่อการเข้าถึงข้อมูลของหน่วยงานที่มีหน้าที่รับผิดชอบโดยตรงต่อประเด็นต่างๆ ของประเทศนั้นๆ ตลอดจนสามารถนำข้อมูลที่ได้มาวิเคราะห์ วิจัย และใช้เพื่อวัตถุประสงค์ในด้านการพัฒนาเศรษฐกิจและสังคม¹⁴ ให้ประสบความสำเร็จต่อเป้าหมายของการพัฒนาอย่างยั่งยืน

โดยการแบ่งปันข้อมูลการดำเนินงานของรัฐบาลและหน่วยงานของรัฐบาล ข้อมูลบริการสาธารณะ และข้อมูลจำนวนประชากร เพราะข้อมูลเชิงลึกเหล่านี้สามารถนำไปใช้ในวิเคราะห์เพื่อแจ้งลำดับความสำคัญของนโยบายระดับชาติ และช่วยกำหนดเส้นยุทธศาสตร์ทางนโยบายของรัฐบาล ใน

¹¹ The Asia-Pacific Economic Cooperation, "FTA/RTA Information Sharing" (2015), Retrieved from <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/CTI/Info>

¹² Annex 3 APEC Information Sharing Mechanism for FTAs/RTAs, p. 2, Retrieved from http://mddb.apec.org/Documents/2014/SOM/SOM2/14_som2_049anx03.pdf

¹³ สยาม อรุณศรีมี, ยงยุทธ วัชรคุลย์, "เป้าหมายการพัฒนาที่ยั่งยืน 17 ประการของสหประชาชาติเพื่อโลกอนาคต", วารสารวิจัยสหวิทยาการไทย Vol. 11, Number 3 (June 2016), p. 2

¹⁴ Joel Gurin, Laura Manley and Oleg Petrov, "New discussion paper: How Open Data can drive sustainable development" (2015) Retrieved from www.blogs.worldbank.org/digital-development

การดำเนินการแก้ไขต่อประเด็นปัญหาระดับชาติต่างๆ รวมทั้งประเทศสมาชิกอื่นสามารถนำข้อมูลแบบเปิดเหล่านี้ไปวิเคราะห์และเปรียบเทียบข้อมูลกับประเทศของตนเพื่อการวางนโยบายที่ถูกต้องตลอดจนประเทศที่ประสบความสำเร็จในการพัฒนาเศรษฐกิจและสังคม ก็สามารถจะแบ่งปันบทเรียนหรือองค์ความรู้ต่อประเทศที่กำลังต้องการพัฒนานโยบายเศรษฐกิจและสังคมของตนอยู่ ความสำคัญในการแบ่งปันข้อมูล ทำให้หน่วยงานภายในประเทศดำเนินการอย่างสะดวก¹⁵ ซึ่งโดยปกติแล้วหน่วยงานภายในบางประเทศยังคงต้องขอข้อมูลต่อกันระหว่างหน่วยแบบเป็นทางการ หรือแบบเอกสาร ซึ่งถือเป็นความล่าช้าต่อการเข้าถึงข้อมูล รวมไปถึงหน่วยงานระหว่างประเทศเองก็สามารถเข้าถึงข้อมูลต่าง ๆ ของประเทศนั้นได้อย่างเสรี และเหมาะสมต่อการนำข้อมูลที่ได้มาพัฒนานโยบายทางเศรษฐกิจและสังคม

ความสำคัญของการแบ่งปันข้อมูล ยังช่วยส่งเสริมการเติบโตทางเศรษฐกิจและการสร้างงาน ข้อมูลของหน่วยงานภาครัฐด้านพาณิชย์ สามารถช่วยสร้างธุรกิจใหม่ เพิ่มประสิทธิภาพการดำเนินงานของบริษัทเอกชนที่จะรับรู้ถึงข้อมูลความพร้อมของประเทศที่เหมาะสมสำหรับการลงทุน จากวิเคราะห์ข้อมูลที่หน่วยงานภายในประเทศนั้นทำการแบ่งปันข้อมูลออกมา นอกจากนี้ยังสามารถทำให้ตลาดงานมีประสิทธิภาพมากขึ้นเพราะนักลงทุนสามารถวิเคราะห์และเข้าใจตลาดก่อนการตัดสินใจลงทุนในประเทศนั้นๆ

ความสามารถในการปรับปรุงประสิทธิภาพและประสิทธิผลของการบริการสาธารณะ¹⁶ การแบ่งปันข้อมูลเข้าสู่ฐานข้อมูลแบบเปิดสามารถช่วยเสริมสร้างระบบการดูแลสุขภาพด้วยการเชื่อมโยงข้อมูลระหว่างผู้ป่วยกับผู้ให้บริการทางการแพทย์ ตลอดจนมีความโปร่งใสในการตรวจสอบของประชาชน เพราะประชาชนสามารถเข้าถึงข้อมูลภาครัฐอย่างเสรี ข้อมูลแบบเปิดมีบทบาทสำคัญในการตรวจสอบ กำกับดูแล และป้องกันการจัดสรรงบประมาณที่ไม่ถูกต้อง และการทุจริตของภาครัฐ ข้อมูลแบบเปิดยังอำนวยความสะดวกในการแบ่งปันข้อมูลทั้งภายในประเทศ และระหว่างประเทศ สามารถแบ่งปันข้อมูลเกี่ยวกับการรับมือต่อภัยพิบัติของประเทศอื่น และวิเคราะห์การจัดเตรียมทรัพยากรที่จำเป็นที่จะถูกนำไปใช้อย่างมีประสิทธิภาพในสถานการณ์ฉุกเฉิน

4.) การประเมินสถานการณ์ภัยพิบัติและประสานงานขององค์การสหประชาชาติ (United Nations Disaster Assessment and Coordination)

ภายใต้ความร่วมมือในการทำงานขององค์กรพัฒนาเอกชน หน่วยงานรัฐบาลของหลายประเทศ สหประชาชาติและหน่วยงานภายใต้สหประชาชาติจะต้องทำการแบ่งปันข้อมูลต่อกัน

¹⁵ Joel Gurin, Laura Manley, and Oleg Petrov, "New discussion paper: How Open Data can drive sustainable development," 34, no. 1 (2015), www.blogs.worldbank.org/digital-development.

¹⁶ Ibid.

เกี่ยวกับโปรแกรมที่ถูกวางแผนในพื้นที่ที่ดำเนินการพัฒนาด้านมนุษยธรรม เพื่อทราบถึงความต่อเนื่องของข้อมูลในด้านเศรษฐกิจสังคม, ภูมิศาสตร์, สุขภาพ และสิ่งแวดล้อม รวมไปถึงการนำข้อมูลเหล่านั้นมาใช้เพื่อประเมินโครงการ¹⁷ อาทิ เหตุการณ์ภัยพิบัติแผ่นดินไหวที่ประเทศเฮติปี ค.ศ. 2010 ทีมประเมินสถานการณ์ภัยพิบัติและประสานงานขององค์การสหประชาชาติ (UNDAC) มีข้อร้องเรียนให้องค์กรของฝ่ายรัฐบาล ภาคเอกชน และทีมอาสาสมัครและพันธมิตร ดำเนินการภายใต้ยุทธศาสตร์การจัดการข้อมูล ให้จัดเก็บและทำการแบ่งปันข้อมูลที่แม่นยำ เกี่ยวกับความเสียหายจากภัยพิบัติ องค์ความรู้ด้านเทคนิคและการแพทย์¹⁸ ตลอดจนข้อมูลของการขาดแคลนทรัพยากรที่จำเป็น เพื่อขอความช่วยเหลือจากต่างประเทศและหน่วยงานต่างๆ และข้อมูลอื่นต่อการแก้ไขปัญหาภัยพิบัติ

5.) การปกป้องสิ่งแวดล้อมและการบำบัดกลับคืนซึ่งความสมบูรณ์ของธรรมชาติที่ถูกทำลายไป

การแบ่งปันข้อมูลมีบทบาทช่วยในการแบ่งปันองค์ความรู้ทางวิทยาศาสตร์และเทคโนโลยีระหว่างประเทศ เพื่อปกป้องสิ่งแวดล้อมนั้นจึงเป็นเรื่องสำคัญและเป็นหน้าที่ของหน่วยงานของรัฐที่มีอำนาจบริหารจัดการ ในสหภาพยุโรป คณะกรรมาธิการยุโรปได้กำหนด แผนการแบ่งปันข้อมูลสภาพแวดล้อมทางทะเลร่วมกันในมุมมองของ ปี2020 (EUCISE2020) โดยมีจุดมุ่งหมายที่จะทำการแบ่งปันข้อมูล การปฏิบัติงานระหว่างหน่วยงานทางทะเลของรัฐสมาชิกในยุโรป อาทิ กรมการขนส่ง กรมการคุ้มครองสิ่งแวดล้อม กรมประมง กรมการควบคุมชายแดน ศุลกากรและการป้องกันประเทศ และหน่วยงานการบังคับใช้กฎหมาย เพื่อสร้างความสะดวกในการเข้าถึงข้อมูลการบริหารจัดการกิจกรรมทางทะเลของภาครัฐ องค์กร รวมถึงกฎหมายที่เกี่ยวข้องเพื่อออกแบบ ระบบการตรวจสอบ (Surveillance Systems) และการปฏิบัติการต่อกิจกรรมทางทะเลที่สร้างผลกระทบต่อสภาพสิ่งแวดล้อม ความปลอดภัยและเศรษฐกิจ ของสหภาพยุโรป

2.1.2 บทบาทในตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้าย

ตั้งแต่ปีพ.ศ. 2506 มาจนถึงปัจจุบันมีตราสารทางกฎหมายระหว่างประเทศทั้งหมด 19 ฉบับ เพื่อป้องกันการกระทำของผู้ก่อการร้าย ตราสารเหล่านี้ได้รับการพัฒนาภายใต้การทำงานขององค์กรระหว่างประเทศที่เป็นหลักคือ องค์การสหประชาชาติ องค์การทบวงการพลังงานปรมาณูระหว่างประเทศ (IAEA) และองค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation

¹⁷ Ben Watkins, "Information exchange for humanitarian coordination in the Horn of Africa" (June 2003), The Humanitarian Practice Network

¹⁸ UN Office for the Coordination of Humanitarian Affairs, "Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies" (2011), p. 10-12

Organization) ทั้งนี้ในแต่ละครั้งของการประชุมเพื่อพิจารณาร่างนั้น ได้เปิดโอกาสให้บรรดารัฐในสังคมนระหว่างประเทศเข้าร่วมเจรจาตกลงในการร่างตราสารเหล่านี้

แม้ว่าตราสารทั้ง 19 ฉบับนี้จะไม่ใช่เรื่องข้อเดียวกัน และมีความแตกต่างกันไปตามหัวข้อที่เกี่ยวข้องกับประเภทของอาชญากรรมที่อ้างถึงนั้นๆ แต่คุณลักษณะทั่วไปที่สำคัญที่ทุกตราสารเหล่านี้มีร่วมกัน คือ ได้กำหนดมาตรการทางกฎหมายระหว่างประเทศ¹⁹ อาทิ การกำหนดการพิจารณาโดยหลักการไม่ส่งตัวก็ต้องพิจารณาคดี (Principle of aut dedere aut judicare) และกฎเกณฑ์เกี่ยวกับความร่วมมือในรูปแบบต่างๆ เช่น มาตรการป้องกัน การแลกเปลี่ยนข้อมูล ในส่วนนี้จะได้อธิบายเพื่อป้องกันภัยของมาตรการการแบ่งปันข้อมูล และวิเคราะห์ถึงขอบเขตและข้อจำกัดในกรอบของการต่อต้านการก่อการร้ายตามตราสารระหว่างประเทศทั้ง 19 ฉบับ

1.) อนุสัญญาว่าด้วยความผิดและการกระทำอื่น ๆ บางประการที่กระทำบนเครื่องบิน พ.ศ. 2506 (1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft)

อนุสัญญานี้ใช้บังคับกับความผิดอาญาหรือการกระทำใด ๆ ที่เป็นอันตรายต่อความปลอดภัยของบุคคลหรือทรัพย์สินบนเครื่องบินพลเรือนขณะอยู่บนเครื่องบิน หรือมีส่วนร่วมในการเดินอากาศระหว่างประเทศ ครอบคลุมรวมถึงการกระทำ หรือความตั้งใจที่จะกระทำ ซึ่งความผิดบางอย่างบนเครื่องบินที่ลงทะเบียนในรัฐภาคีตามอนุสัญญานี้ ในเที่ยวบินเหนือทะเลหลวง และพื้นที่อื่นใดที่อยู่นอกเหนืออาณาเขตของรัฐใด ๆ หรือนอกเหนือจากน่านฟ้าที่เป็นของรัฐภาคีการประชุมเพื่อเจรจา และกำหนดข้อตกลงตามอนุสัญญานี้เป็นครั้งแรกในประวัติศาสตร์ของกฎหมายการบินระหว่างประเทศที่รับรองถึงอำนาจและความคุ้มครองบางประการของผู้ควบคุมอากาศยานซึ่งในเที่ยวบินระหว่างประเทศ หรืออำนาจหน้าที่ที่อาจยับยั้งบุคคลใด ๆ ที่มีเหตุอันควรเชื่อว่าจะกำลังกระทำหรือกำลังจะกระทำการ ซึ่งความผิดต่อความปลอดภัยของบุคคลหรือทรัพย์สินบนอากาศยาน หรือผู้ที่เป็นอันตรายต่อระเบียบและข้อบังคับสำหรับการบิน

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทเพื่อการป้องกันหรือขจัดตัดตอนการกระทำหรือกำลังจะกระทำการอันเป็นความผิดต่อความปลอดภัยของบุคคลหรือทรัพย์สินบนอากาศยาน จากกรณีสังเกตในข้อที่ 9 วรรค 3 บัญญัติว่า ผู้ควบคุมอากาศยาน (Aircraft commander) จะต้องแบ่งปันข้อมูลซึ่งอาจจะเป็นพยานหลักฐานหรือข้อมูลอันมีมูลเหตุว่ามีบุคคลผู้ต้องสงสัยว่าจะกระทำความผิดตามบทบัญญัติของข้อนี้ ให้แก่เจ้าหน้าที่ที่มีอำนาจ ตามบทบัญญัติของอนุสัญญาฉบับนี้²⁰

¹⁹ Marcin Marcinko, "The Evolution of UN Anti-Terrorist Conventions towards the Universal Treaty-Based Model of Combating Terrorism," *Groningen Journal of International Law* vol 6(1) of Terrorism and International Law (2014).

²⁰ 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft, Article 9

2.) อนุสัญญาว่าด้วยการปราบปรามการยึดเครื่องบินโดยไม่ชอบด้วยกฎหมาย พ.ศ. 2513 (1970 Convention for the Suppression of Unlawful Seizure of Aircraft)

อนุสัญญามีวัตถุประสงค์ในการเอาผิดกับการกระทำที่ผิดกฎหมายในการเข้ายึดหรือควบคุมอากาศยานระหว่างบิน อันเป็นอันตรายต่อความปลอดภัยของบุคคลและทรัพย์สิน ส่งผลกระทบอย่างร้ายแรงต่อการดำเนินงานของบริการทางอากาศ และบ่อนทำลายความเชื่อมั่นของประชาชนทั่วโลกในความปลอดภัยของการบินพลเรือน

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทเพื่อวิเคราะห์เหตุการณ์การทำความผิดที่เกิดขึ้น และกำหนดเป็นแนวทางของการป้องกันเหตุการณ์ไม่ให้เกิดขึ้นอีกในอนาคต โดยข้อที่ 11 ในอนุสัญญาได้ระบุว่า รัฐภาคีแต่ละรัฐจะต้องแบ่งปันข้อมูลเพื่อรายงานต่อสภาองค์การการบินพลเรือนระหว่างประเทศ (the Council of the International Civil Aviation Organization) โดยเร็วที่สุดเท่าที่จะเป็นไปได้ ถึงข้อมูลที่เกี่ยวข้องกับพฤติกรรมแห่งการทำความผิด ข้อมูลของมาตรการที่ดำเนินการกับผู้กระทำความผิด หรือผู้ต้องหา และโดยเฉพาะอย่างยิ่งผลของข้อมูลการดำเนินการส่งผู้ร้ายข้ามแดนหรือกระบวนการทางกฎหมายของตน²¹

3.) อนุสัญญาเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยของการบินพลเรือน พ.ศ. 2514 (1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation)

อนุสัญญานี้ใช้บังคับกับการกระทำที่ผิดกฎหมายต่อความปลอดภัยของการบินพลเรือนเป็นอันตรายต่อความปลอดภัยของบุคคลและทรัพย์สิน ส่งผลกระทบต่อการดำเนินงานของบริการทางอากาศ และบ่อนทำลายความเชื่อมั่นของประชาคมโลกในความปลอดภัยของการบินพลเรือน

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทเพื่อวิเคราะห์เหตุการณ์การทำความผิดที่เกิดขึ้น และกำหนดเป็นแนวทางของการป้องกันเหตุการณ์ไม่ให้เกิดขึ้นอีกในอนาคต โดยข้อที่ 13 ในอนุสัญญาได้ระบุว่า รัฐภาคีแต่ละรัฐจะต้องรายงานตามกฎหมายของประเทศต่อสภาองค์การการบินพลเรือนระหว่างประเทศ โดยเร็วที่สุดเท่าที่จะเป็นไปได้ ถึงข้อมูลที่เกี่ยวข้องใดที่อยู่ในความครอบครองของตนเกี่ยวกับพฤติกรรมแห่งการทำความผิด มาตรการที่ดำเนินการกับผู้กระทำความผิด หรือผู้ต้องหา และโดยเฉพาะอย่างยิ่งผลของการดำเนินการส่งผู้ร้ายข้ามแดนหรือกระบวนการทางกฎหมายของตน²²

²¹ 1970 Convention for the Suppression of Unlawful Seizure of Aircraft, Article 11

²² 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Article 13

4.) อนุสัญญาว่าด้วยการป้องกันและลงโทษการก่ออาชญากรรมต่อบุคคลที่ได้รับการคุ้มครองในระดับสากลรวมถึงตัวแทนทางการทูต พ.ศ. 2516 (1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents)

อาชญากรรมต่อตัวแทนทางการทูตและบุคคลที่ได้รับการคุ้มครองระหว่างประเทศอื่น ๆ และการกระทำที่เป็นอันตรายต่อความปลอดภัยของบุคคลเหล่านี้ก่อให้เกิดภัยคุกคามร้ายแรงต่อการรักษาความสัมพันธ์ระหว่างประเทศและการสร้างความร่วมมือระหว่างรัฐ

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทเพื่อการป้องกันหรือขจัดตัดตอนการกระทำหรือกำลังจะกระทำการ โดยในข้อที่ 13 ในอนุสัญญาได้ระบุว่ารัฐภาคีจะร่วมมือ ในการป้องกันอาชญากรรมโดยการแลกเปลี่ยนข้อมูล และประสานงาน ในการดำเนินมาตรการทางปกครอง และอื่น ๆ ตามความเหมาะสมเพื่อป้องกันการก่ออาชญากรรมเหล่านั้น ข้อสังเกตในอนุสัญญามีได้ระบุให้ชัดเจนถึงรายละเอียดและกระบวนการของการแบ่งปันข้อมูลรวมถึงมิได้กำหนดบทบาทว่าหน่วยงานใดภายในรัฐภาคีถึงจะมีอำนาจและหน้าที่²³

5.) อนุสัญญาระหว่างประเทศต่อต้านการจับตัวประกัน พ.ศ. 2522 (1979 International Convention against the Taking of Hostages)

อนุสัญญาตัวประกัน (The Hostages Convention) หรืออนุสัญญาระหว่างประเทศต่อต้านการจับตัวประกันมีวัตถุประสงค์มุ่งกำหนดความผิดต่อการจับตัวประกันอันเป็นความผิดร้ายแรงต่อประชาคมระหว่างประเทศ และตามบทบัญญัติของอนุสัญญานี้ บุคคลใดก็ตามที่กระทำการจับตัวประกัน จะถูกดำเนินคดีหรือทำการส่งผู้ร้ายข้ามแดน

การแบ่งปันข้อมูลในอนุสัญญานี้ได้ส่งเสริมการป้องกันหรือขจัดตัดตอนการกระทำหรือกำลังจะกระทำการ โดยข้อที่ 4 ในอนุสัญญาได้ระบุว่ารัฐภาคีจะร่วมมือ ในการป้องกันอาชญากรรมโดยการแลกเปลี่ยนข้อมูล และประสานงาน ในการดำเนินมาตรการทางปกครอง และอื่น ๆ ตามความเหมาะสมเพื่อป้องกันการก่ออาชญากรรมเหล่านั้น ข้อสังเกตในอนุสัญญามีได้ระบุให้ชัดเจนถึงรายละเอียดและกระบวนการของการแบ่งปันข้อมูลรวมถึงมิได้กำหนดบทบาทว่าหน่วยงานใดภายในรัฐภาคีถึงจะมีอำนาจและหน้าที่²⁴

²³ 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, Article 13

²⁴ 1979 International Convention against the Taking of Hostages, Article 4

6.) อนุสัญญาว่าด้วยการคุ้มครองทางกายภาพของวัสดุนิวเคลียร์ พ.ศ. 2523 (1980 Convention on the Physical Protection of Nuclear Material)

อนุสัญญาว่าด้วยว่าด้วยการคุ้มครองทางกายภาพของวัสดุนิวเคลียร์ มีวัตถุประสงค์สำคัญในการกำหนดมาตรการการป้องกันทางกายภาพในทุกๆระดับ เช่น ระหว่างการขนส่งวัสดุนิวเคลียร์ระหว่างประเทศ นอกจากนี้ยังกำหนดกรอบการทำงานทั่วไปสำหรับความร่วมมือระหว่างรัฐในการป้องกัน การกักกัน และการส่งคืนวัสดุนิวเคลียร์ที่ถูกขโมย

การแบ่งปันข้อมูลในอนุสัญญานี้ได้ส่งเสริมในเรื่องของการสืบสวนสอบสวน หรือหาข้อมูลเบาะแสในเหตุการณ์ที่ผิดปกติที่อาจอันจะนำไปสู่การใช้นิวเคลียร์ โดยในข้อที่ 5 และข้อที่ 6 ในอนุสัญญาได้ระบุ รัฐภาคีต้องดำเนินมาตรการที่เหมาะสมสอดคล้องกับกฎหมายภายในประเทศตน เพื่อปกป้องความลับของข้อมูลใด ๆ ที่ได้รับมาโดยอาศัยอำนาจตามบทบัญญัติของอนุสัญญานี้ ไม่ว่าจะได้รับจากรัฐภาคีอื่น หรือโดยการมีส่วนร่วมในกิจกรรมที่ดำเนินการเพื่อการปฏิบัติตามอนุสัญญานี้ ให้รัฐภาคีดำเนินการให้ข้อมูลแก่องค์กรระหว่างประเทศ อาทิ สหประชาชาติ หรือทบวงการพลังงานปรมาณูระหว่างประเทศ (International Atomic Energy Agency) ซึ่งข้อมูลของเหตุการณ์กรณีที่มีการกำจัด การใช้ หรือการเปลี่ยนแปลงวัสดุนิวเคลียร์ โดยไม่ได้รับอนุญาต หรือในกรณีเหตุการณ์ที่เป็นภัยคุกคามที่น่าเชื่อถืออื่น ๆ²⁵

7.) พิธีสารเพื่อการปราบปรามการกระทำความรุนแรงที่ไม่ชอบด้วยกฎหมายที่สนามบินที่ให้บริการการบินพลเรือนระหว่างประเทศ พ.ศ. 2531 (1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation)

พิธีสารเป็นส่วนเสริมของอนุสัญญาเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยของการบินพลเรือน พ.ศ. 2514 (Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation) และไม่มีส่วนเสริมของบทบาทรการแบ่งปันข้อมูล

8.) อนุสัญญาเพื่อปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยในการเดินเรือทางทะเล พ.ศ. 2531 (1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation)

อนุสัญญาฉบับนี้มีวัตถุประสงค์หลักคือการเอาผิดกับการกระทำที่ผิดกฎหมายต่อความปลอดภัยของการเดินเรือทางทะเล หรือการกระทำอันเป็นอันตรายต่อความปลอดภัยของบุคคลและทรัพย์สิน ส่งผลกระทบต่อการทำงานของการบริการทางทะเล และบ่อนทำลายความเชื่อมั่นของประชาคมโลกในความปลอดภัยในการเดินเรือทางทะเล

²⁵ 1980 Convention on the Physical Protection of Nuclear Material, Article 5,6

การแบ่งปันข้อมูลในอนุสัญญานี้ได้ส่งเสริมในเรื่องของการสืบสวนสอบสวน หรือหาข้อมูล เบาะแสในเหตุการณ์ที่ผิดปกติที่อาจจะนำไปสู่การกระทำที่ผิดกฎหมายต่อความปลอดภัยของการเดินเรือทางทะเล โดยในข้อที่ 15 ในอนุสัญญานี้ได้ระบุว่า รัฐภาคีแต่ละรัฐจะต้องรายงานต่อสำนักงานเลขาธิการสหประชาชาติ หรือองค์การทางทะเลระหว่างประเทศ โดยเร็วที่สุดเท่าที่จะเป็นไปได้ ถึงข้อมูลที่เกี่ยวข้องใดที่อยู่ในความครอบครองของตนเกี่ยวกับพฤติกรรมแห่งการกระทำความผิด มาตรการที่ดำเนินการกับผู้กระทำความผิด หรือผู้ต้องหา และโดยเฉพาะอย่างยิ่งผลของการดำเนินการส่งผู้ร้ายข้ามแดนหรือกระบวนการทางกฎหมายของตน²⁶

9.) พิธีสารเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยของแพลตฟอร์มคงที่ซึ่งตั้งอยู่บนไหล่ทวีป พ.ศ. 2531 (1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf)

พิธีสารเป็นส่วนเสริมของอนุสัญญานี้เพื่อปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยในการเดินเรือทางทะเล พ.ศ. 2531 (1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation) และไม่มีส่วนเสริมของบทบาทรการแบ่งปันข้อมูล

10.) อนุสัญญานี้ว่าด้วยการทำเครื่องหมายวัตถุระเบิดพลาสติกเพื่อวัตถุประสงค์ในการตรวจจับ พ.ศ. 2534 (1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection)

อนุสัญญานี้ตกลงที่จะห้ามการผลิต การจัดเก็บ การขนส่ง หรือการนำเข้าวัตถุระเบิดพลาสติกที่ไม่มีเครื่องหมายในอาณาเขตของรัฐภาคี อนุสัญญานี้ไม่ได้ห้ามวัตถุระเบิดที่เป็นพลาสติก (Plastic explosives) แต่มีข้อบังคับว่าเมื่อผลิตขึ้นแล้วจะมีการทำเครื่องหมายสารเคมี (Chemical taggant marke) ซึ่งสามารถอำนวยความสะดวกในการระบุตัววัตถุ และอนุสัญญานี้ยังจัดตั้งคณะกรรมการเทคนิคด้านวัตถุระเบิดระหว่างประเทศ (International Explosives Technical Commission) ซึ่งประกอบด้วยผู้เชี่ยวชาญในการผลิตและตรวจจับวัตถุระเบิดภาคสนาม

การแบ่งปันข้อมูลในอนุสัญญานี้ได้ส่งเสริมในเรื่องความช่วยเหลือทางเทคนิคต่อการดำเนินการตามอนุสัญญา โดยที่ข้อที่ 8 ในอนุสัญญานี้ได้ระบุว่า รัฐภาคีจะต้องร่วมมือกับคณะกรรมการเทคนิคด้านวัตถุระเบิดระหว่างประเทศ (International Explosives Technical Commission) ในการดำเนินการมาตรการที่เหมาะสมเพื่ออำนวยความสะดวกในการปฏิบัติตาม

²⁶ 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Article 15

อนุสัญญานี้ รวมถึงการให้ความช่วยเหลือทางเทคนิค และมาตรการสำหรับการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการพัฒนาทางเทคนิคในการทำเครื่องหมายและการตรวจจับวัตถุระเบิด²⁷

11.) อนุสัญญาระหว่างประเทศ เพื่อการปราบปรามการลอบวางระเบิดของผู้ก่อการร้าย พ.ศ. 2540 (1997 International Convention for the Suppression of Terrorist Bombings)

อนุสัญญาว่าด้วยการลอบวางระเบิดของผู้ก่อการร้ายกำหนดโทษต่ออาชญากรผู้ลอบวางระเบิด มีวัตถุประสงค์หลักคือการกำหนดความผิดฐานการวางระเบิดโดยการก่อการร้าย การใช้วัตถุระเบิดในที่สาธารณะโดยไม่ชอบด้วยกฎหมาย และโดยเจตนา เพื่อฆ่า ทำร้าย หรือทำลายล้างอย่างกว้างขวาง เพื่อบังคับให้รัฐบาลหรือองค์กรระหว่างประเทศกระทำการ หรือละเว้นจากการกระทำบางอย่าง

การแบ่งปันข้อมูลในอนุสัญญานี้ได้ส่งเสริมในเรื่องการป้องกันและช่วยเหลือทางเทคนิคต่อการดำเนินการตามอนุสัญญา โดยที่ข้อที่ 15 ในอนุสัญญาได้ระบุว่า รัฐภาคีจะต้องสร้างกลไกความร่วมมือระหว่างหน่วยงานที่มีอำนาจภายในรัฐตน ในการป้องกันการกระทำความผิดโดยการแลกเปลี่ยนข้อมูล และเพื่ออำนวยความสะดวกต่อการวิจัยและพัฒนาเกี่ยวกับวิธีการตรวจหาวัตถุระเบิดและสารอันตรายอื่น ๆ ที่อาจทำให้เสียชีวิตหรือบาดเจ็บต่อร่างกาย²⁸

12.) อนุสัญญาระหว่างประเทศเพื่อการปราบปรามการจัดหาเงินทุนของการก่อการร้าย พ.ศ. 2542 (1999 International Convention for the Suppression of the Financing of Terrorism)

อนุสัญญาว่าด้วยการจัดหาเงินทุนของผู้ก่อการร้ายมีวัตถุประสงค์หลักเพื่อกำหนดโทษอาชญากรที่กระทำการให้เงินสนับสนุนการก่อการร้ายทุกรูปแบบ

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทเพื่อการป้องกันหรือขจัดตัดตอนการกระทำทำให้เงินสนับสนุนการก่อการร้ายทุกรูปแบบ โดยข้อที่ 18 วรรค 3 และวรรค 4 ในอนุสัญญาได้ระบุว่า รัฐภาคีจะต้องสร้างกลไกความร่วมมือระหว่างหน่วยงานที่มีอำนาจภายในรัฐตน ในการป้องกันการกระทำความผิดโดยการแลกเปลี่ยนข้อมูลที่ถูกต้อง เพื่ออำนวยความสะดวกต่อการสืบสวนความผิดระบุตัวตน เบาะแส หรือกิจกรรมของบุคคลที่มีเหตุอันควรสงสัยว่ามีส่วนเกี่ยวข้องกับการกระทำความผิดดังกล่าวทั้งนี้รัฐภาคีอาจใช้กลไกการแลกเปลี่ยนข้อมูลผ่านฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL)²⁹

²⁷ 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection, Article 8

²⁸ 1997 International Convention for the Suppression of Terrorist Bombings, Article 15

²⁹ 1999 International Convention for the Suppression of the Financing of Terrorism, Article 18

13.) อนุสัญญาระหว่างประเทศเพื่อการปราบปรามการกระทำของการก่อการร้ายทางนิวเคลียร์ พ.ศ. 2548 (2005 International Convention for the Suppression of Acts of Nuclear Terrorism)

อนุสัญญานี้มีวัตถุประสงค์หลักในการคุ้มครองต่อความปลอดภัยของการใช้พลังงานนิวเคลียร์ เช่น คิวคุมครองโรงไฟฟ้านิวเคลียร์ (Nuclear power plants) หรือเครื่องปฏิกรณ์นิวเคลียร์ (Nuclear reactors) จากการก่อการร้าย ครอบคลุมถึงการคุกคาม และความพยายามที่จะก่ออาชญากรรม หรือมีส่วนร่วมในการกระทำความผิดดังกล่าวในฐานะผู้สมรู้ร่วมคิด

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทในการส่งเสริมความช่วยเหลือทางพยานหลักฐานอันเป็นประโยชน์ต่อการดำเนินคดีในกระบวนการยุติธรรม จากข้อที่ 7 ในอนุสัญญาได้ระบุว่ารัฐภาคีต้องการแลกเปลี่ยนข้อมูล เพื่อตรวจจับ ป้องกัน ปราบปราม และสอบสวนความผิดที่ระบุไว้ในอนุสัญญา และเพื่อดำเนินคดีทางอาญากับบุคคลที่ถูกกล่าวหาว่าก่ออาชญากรรมเหล่านั้น โดยเฉพาะอย่างยิ่งรัฐภาคีจะดำเนินมาตรการที่เหมาะสมเพื่อแจ้งข้อมูลให้ทราบโดยไม่ชักช้าต่อรัฐภาคีอื่นในส่วนข้อมูลที่เกี่ยวข้องกับการกระทำความผิดที่ระบุ และแจ้งให้องค์การระหว่างประเทศทราบตามความเหมาะสม อาทิ สำนักงานเลขาธิการสหประชาชาติ (Secretary-General of the United Nations) หรือทบวงการพลังงานปรมาณูระหว่างประเทศ (International Atomic Energy Agency)³⁰

14.) การแก้ไขอนุสัญญาว่าด้วยการปกป้องทางกายภาพของวัสดุนิวเคลียร์ พ.ศ. 2548 (2005 Amendment to the Convention on the Physical Protection of Nuclear Material)

เป็นการแก้ไขของอนุสัญญาว่าด้วยการคุ้มครองทางกายภาพของวัสดุนิวเคลียร์ พ.ศ. 2523 (1980 Convention on the Physical Protection of Nuclear Material) และไม่มีส่วนเสริมของบทบาทการแบ่งปันข้อมูล

15.) พิธีสารของอนุสัญญาเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยในการเดินเรือทางทะเล พ.ศ. 2548 (2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation)

พิธีสารเป็นส่วนเสริมของอนุสัญญาเพื่อปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยในการเดินเรือทางทะเล พ.ศ. 2531 (1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation) และไม่มีส่วนเสริมของบทบาทการแบ่งปันข้อมูล

³⁰ 2005 International Convention for the Suppression of Acts of Nuclear Terrorism, Article 7

16.) พิธีสารเพื่อพิธีสารการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยของแพลตฟอร์มคงที่ที่ตั้งอยู่บนไหล่ทวีป พ.ศ. 2548 (Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf)

พิธีสารเป็นส่วนเสริมของพิธีสารเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยของแพลตฟอร์มคงที่ซึ่งตั้งอยู่บนไหล่ทวีป พ.ศ. 2531 (1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf) และไม่มีส่วนเสริมของบทบาบทการแบ่งปันข้อมูล

17.) อนุสัญญาว่าด้วยการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายที่เกี่ยวข้องกับการบินพลเรือนระหว่างประเทศ พ.ศ. 2553 (2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation)

อนุสัญญานี้มีวัตถุประสงค์สร้างฐานความผิดสำหรับการกระทำที่ผิดกฎหมายต่อการบินพลเรือน หรือการกระทำอันเป็นอันตรายต่อความปลอดภัยและความมั่นคงของบุคคลและทรัพย์สินส่งผลกระทบต่อการทำงานของบริการทางอากาศ ท่าอากาศยาน การเดินอากาศ และบ่อนทำลายความเชื่อมั่นของประชาคมระหว่างประเทศในการดำเนินการบินพลเรือนที่ปลอดภัยและเป็นระเบียบเพื่อทุกคน

การแบ่งปันข้อมูลในอนุสัญญานี้มีบทบาทเพื่อวิเคราะห์เหตุการณ์การทำความผิดที่เกิดขึ้นและกำหนดเป็นแนวทางของการป้องกันเหตุการณ์ไม่ให้เกิดขึ้นอีกในอนาคต โดยข้อที่ 19 ในอนุสัญญาได้ระบุว่า รัฐภาคีแต่ละรัฐจะต้องรายงานตามกฎหมายของประเทศต่อสภาองค์การการบินพลเรือนระหว่างประเทศ (the Council of the International Civil Aviation Organization) โดยเร็วที่สุดเท่าที่จะเป็นไปได้ ถึงข้อมูลที่เกี่ยวข้องใดที่อยู่ในความครอบครองของตนเกี่ยวกับพฤติการณ์แห่งการกระทำความผิด มาตรการที่ดำเนินการกับผู้กระทำความผิด หรือผู้ต้องหา และโดยเฉพาะอย่างยิ่งผลของการดำเนินการส่งผู้ร้ายข้ามแดนหรือกระบวนการทางกฎหมายของตน³¹

18.) พิธีสารส่วนเสริมของอนุสัญญาว่าด้วยการปราบปรามการยึดโดยมิชอบด้วยกฎหมายของ พ.ศ. 2553 (2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft)

³¹ 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, Article 19

พิธีสารเป็นส่วนเสริมของอนุสัญญาว่าด้วยการปราบปรามการยึดเครื่องบินโดยไม่ชอบด้วยกฎหมาย พ.ศ. 2513 (1970 Convention for the Suppression of Unlawful Seizure of Aircraft) และไม่มีส่วนเสริมของบทบาบทการแบ่งปันข้อมูล

19.) พิธีสารของอนุสัญญาว่าด้วยการกระทำความผิดและการกระทำอื่น ๆ บางประการที่กระทำบนเครื่องบินบนเครื่องบิน พ.ศ. 2557 (2014 Protocol to the Convention on Offences and Certain other Acts Committed on Board Aircraft)

พิธีสารเป็นส่วนเสริมของอนุสัญญาว่าด้วยความผิดและการกระทำอื่น ๆ บางประการที่กระทำบนเครื่องบิน พ.ศ. 2506 (1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft) และไม่มีส่วนเสริมของบทบาบทการแบ่งปันข้อมูล

2.1.2.1 ประโยชน์ของการแบ่งปันข้อมูล

ประโยชน์ของการดำเนินมาตรการแบ่งปันข้อมูลตามตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้ายจะพบว่ามาตรการการแบ่งปันข้อมูลมีส่วนช่วยส่งเสริมการดำเนินการปราบปรามการก่อการร้ายให้มีประสิทธิภาพมากยิ่งขึ้นในแง่มุมต่างๆดังต่อไปนี้

- 1.) การแบ่งปันข้อมูลช่วยส่งเสริมการป้องกันและขจัดตัดตอนการกระทำการ หรือการเตรียมการลงมือก่อเหตุก่อการร้าย อาทิ การก่อการร้ายในอากาศยาน การก่อการร้ายในเรือ
- 2.) การแบ่งปันข้อมูลสามารถอำนวยความสะดวกต่อการวิเคราะห์เหตุการณ์ก่อการร้ายที่เกิดขึ้นแล้วออกมาเป็นแนวทางป้องกันเหตุการณ์ก่อการร้ายที่จะเกิดขึ้นในอนาคต
- 3.) การแบ่งปันข้อมูลช่วยให้เกิดช่องทางในการสืบสวนสอบสวน หาข้อมูลเบาะแสเกี่ยวกับเหตุการณ์ที่ผิดปกติซึ่งอาจจะนำไปสู่การก่อเหตุก่อการร้าย
- 4.) การแบ่งปันข้อมูลก่อให้เกิดความช่วยเหลือในทางเทคนิคระหว่างรัฐภาคี หรือองค์ความรู้ในการดำเนินมาตรการป้องกันและปราบปรามการก่อการร้าย หรือการดำเนินการตามพันธกรณีตามอนุสัญญา

5.) การแบ่งปันข้อมูลเพื่อการช่วยเหลือพยานหลักฐานอันเป็นประโยชน์ต่อการใช้ในการดำเนินคดีในกระบวนการยุติธรรม

ดังนั้นประโยชน์ที่ได้กล่าวมาข้างต้นของการแบ่งปันข้อมูลเพื่อการต่อต้านกับการก่อการร้ายจะมีประสิทธิภาพได้หรือไม่ ขึ้นอยู่กับการอาศัยความร่วมมืออย่างใกล้ชิดของบรรดารัฐภาคีตาม

ตราสารต่างๆในการดำเนินการแบ่งปันข้อมูล ตลอดจนการปฏิบัติตามพันธกรณีตามอนุสัญญานั้นๆ ได้กำหนดไว้³²

2.1.2.2 ขอบเขตและข้อจำกัด

เมื่อได้ศึกษาบทบาทและประโยชน์ของมาตรการแบ่งปันข้อมูลตามตราสารระหว่างประเทศ ว่าด้วยการต่อต้านการก่อการร้ายทั้ง 19 ฉบับแล้ว ในช่วงระยะเวลาตั้งแต่ของการริเริ่มบังคับใช้ อนุสัญญาเหล่านี้ได้มีการสร้างกระบวนการของการแบ่งปันข้อมูลตามวัตถุประสงค์ของอนุสัญญานั้นๆ ซึ่งสะท้อนให้เห็นถึงความจำเป็นของการดำเนินการเพื่อเสริมประสิทธิภาพของการปราบปรามการก่อการร้าย

อย่างไรก็ตามเมื่อพิจารณามาตรการแบ่งปันข้อมูลตามตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้ายทั้งหมดแล้ว ยังคงพบว่ามีขอบเขตและข้อจำกัดด้านสารบัญญัติและกระบวนการที่อาจจะไม่สอดคล้องต่อการรับมือของการก่อการร้ายในปัจจุบันที่เปลี่ยนแปลงไป ซึ่งจะอธิบายได้ดังต่อไปนี้

1. สารบัญญัติ

1.) เนื้อหาการแบ่งปันข้อมูลต่างๆ จะถูกกำหนดไว้ตามรูปแบบเฉพาะของตราสารนั้น ซึ่งแต่ละตราสารก็กำหนดรูปแบบข้อมูลเฉพาะตามวัตถุประสงค์ของตราสารนั้นๆ จึงอาจจะก่อให้เกิดการได้รับข้อมูลที่ไม่มีความหลากหลาย³³ เกิดข้อจำกัดขึ้นในถ้อยคำ ว่าเนื้อหาข้อมูลที่มีได้ปรากฏอยู่นอกเหนือบทบัญญัติของตราสารนั้นมีฐานทางกฎหมายระหว่างประเทศ หรือเป็นพันธกรณีให้บรรดารัฐภาคีดำเนินการแบ่งปันให้กันได้หรือไม่ จนเกิดความไม่ชัดเจนและส่งผลให้รัฐที่ห่วงหาซึ่งข้อมูลที่เกี่ยวข้องต่อการก่อการร้ายอ้างช่องว่างดังกล่าวในการไม่ให้ความร่วมมือ อาทิ ในเหตุการณ์การก่อการร้าย “Lockerbie bombing” ที่รัฐบาลลิเบียปฏิเสธที่จะให้ความร่วมมือทางข้อมูลกับชาติตะวันตกในการสืบสวนสอบสวนเหตุการณ์การก่อการร้ายดังกล่าว

2.) ในหลายๆตราสารที่ได้ชี้แจงมาข้างต้น มีการระบุสารบัญญัติของอนุสัญญาว่าในการแบ่งปันข้อมูล การให้ข้อมูล หรือการแลกเปลี่ยนข้อมูล ถูกจำกัดไว้เฉพาะระหว่างรัฐภาคีของ

³² Marcinko, "The Evolution of UN Anti-Terrorist Conventions towards the Universal Treaty-Based Model of Combating Terrorism."

³³ M. Cherif Bassiouni, "The weakness of existing international law in addressing terrorism", *Legal Control of International Terrorism: A Policy-Oriented Assessment*, *Harvard International Law Journal* Vol. 49 No. 1 (2002).

อนุสัญญาเท่านั้น จึงอาจจะเป็นเหตุผลให้รัฐที่มีได้เป็นภาคีของอนุสัญญาใช้เป็นข้ออ้างในการมิให้ความร่วมมือในการแบ่งปันข้อมูลที่อาจเป็นข้อมูลที่สำคัญในดำเนินการปราบปรามหรือดำเนินการพิจารณาคดีของการก่อการร้ายให้มีประสิทธิภาพได้

3.) เนื้อหาสารบัญญัติของบรรดาตราสารระหว่างประเทศทั้ง 19 ฉบับได้ครอบคลุมเพียงแค่ 8 ประเด็นหลักๆเท่านั้น คือ ความปลอดภัยของการบินพลเรือน (Civil aviation) การจับตัวประกัน (The taking of hostages) วัสดุนิวเคลียร์ (The nuclear material) การเดินเรือ (The maritime navigation) วัสดุระเบิด (Explosive materials) การวางระเบิดของผู้ก่อการร้าย (Terrorist bombings) การจัดหาเงินทุนของการก่อการร้าย (The financing of terrorism) การก่อการร้ายด้วยนิวเคลียร์ (Nuclear terrorism)³⁴ ทั้งนี้ตราสารยังมีได้บังคับครอบคลุมถึงการก่อการร้ายในลักษณะใหม่ๆ ที่เกิดขึ้นตามการพัฒนาของเทคโนโลยีในปัจจุบัน เช่น การใช้วิธีทางเทคโนโลยีในปัจจุบันของการก่อการร้าย (Modern technological means) อาทิ เข้าถึงแหล่งเงิน หรือรับสมัครบุคคลให้เข้าร่วมขบวนการ การวางแผน การปลุกระดมบุคคล หรือการดำเนินการโจมตีเป้าหมายอ่อน (Execute attack against soft target) ทั้งการร่วมมือทางข้อมูลเพื่อควบคุมการตรวจคนเข้าเมือง การปราบปรามการเดินทางของนักรบต่างชาติที่เดินทางเข้าไปร่วมฝึกรบเพื่อเป็นผู้ก่อการร้ายในพื้นที่ความขัดแย้ง และการเข้าถึงอาวุธที่มีอำนาจทำลายล้างสูงด้วยการใช้วิธีการใหม่

2. กระบวนการ

1.) ในการกำหนดกระบวนการของมาตรการแบ่งปันข้อมูลตามตราสารระหว่างประเทศเหล่านี้ ส่วนใหญ่อยู่ในรูปแบบของข้อผูกพันทั่วไป กล่าวคือมิได้มีการระบุหน่วยงานที่ควรมีหน้าที่และความรับผิดชอบในการดำเนินการการแบ่งปันข้อมูลหรือไม่แต่อย่างใด

2.) ตราสารระหว่างประเทศไม่ได้กำหนดอย่างชัดเจนถึงผู้เกี่ยวข้อง (Stakeholders) ว่ามีใครบ้างที่จะต้องอยู่ในกระบวนการแบ่งปันข้อมูล และมีได้กำหนดภาระหรือหน้าที่ของผู้เกี่ยวข้องในกระบวนการแบ่งปันข้อมูลแต่อย่างใด รวมถึงกลไกที่จะเข้ามาบังคับให้เกิดการแบ่งปันข้อมูลหรือการเข้าถึงข้อมูลจากผู้เกี่ยวข้องในกระบวนการ

³⁴ Marcinko, "The Evolution of UN Anti-Terrorist Conventions towards the Universal Treaty-Based Model of Combating Terrorism."

3.) เมื่อมิได้กำหนดกระบวนการแบ่งปันข้อมูลที่ชัดเจนภายในกรอบการต่อต้านการก่อการร้ายของบรรดาตราสารระหว่างประเทศเหล่านี้ อาจมีแนวโน้มให้เกิดช่องว่างทางกฎหมายให้บรรดารัฐภาคีใช้ดุลยพินิจของตนเองเกินสัดส่วนไปในการดำเนินกระบวนการแบ่งปันข้อมูลที่มีได้มีกฎเกณฑ์ทางกฎหมายระหว่างประเทศกำกับที่ชัดเจน ซึ่งอาจจะกระทบต่อพันธกรณีระหว่างประเทศบางอย่าง โดยเฉพาะอย่างยิ่งในด้าน สิทธิมนุษยชน การปกป้องสิทธิของบุคคลในยามเกิดการขัดกันทางอาวุธ หรือกฎหมายที่ว่าด้วยสิทธิของผู้ลี้ภัย

2.2 การใช้มาตรการบังคับตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงแห่งสหประชาชาติเพื่อการต่อต้านการก่อการร้าย

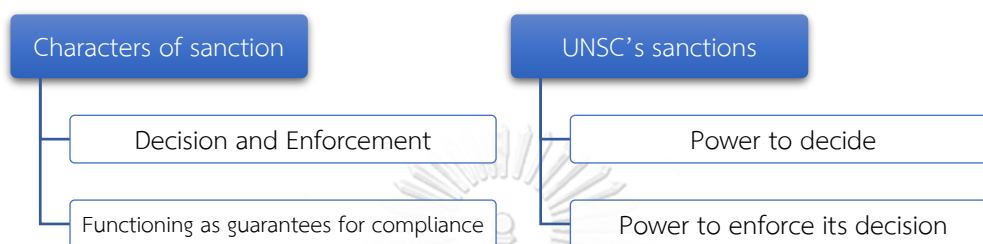
โดยทั่วไปแล้วในสังคมระหว่างประเทศในปัจจุบันนี้มีได้มีองค์กรที่มีลักษณะเป็นศูนย์กลาง (Centralized institution) อย่างแท้จริงในการทำหน้าที่สร้างกฎเกณฑ์ทางกฎหมาย และมีอำนาจในการบังคับใช้กฎหมายต่อรัฐที่ได้กระทำการละเมิดกฎนั้น เมื่อเป็นเช่นนั้นมาตรการที่ก่อให้เกิดการบังคับ เพื่อตอบโต้การกระทำที่มีขอบด้วยกฎหมายในสังคมระหว่างประเทศนั้นจึงถูกเรียกว่า “มาตรการลงโทษ (Sanction)” “มาตรการตอบโต้ (Counter measure)” หรือ การกระทำที่เป็นทุกข์ (Afflictive acts) โดยออกมาอยู่ในรูปแบบของการกระทำฝ่ายเดียวของหน่วยงาน³⁵ องค์กรที่ปฏิบัติหน้าที่ในนามของการรักษผลประโยชน์ของประชาคมระหว่างประเทศโดยรวม (The interest of international community as a whole) ดังนั้นจุดประสงค์ที่สำคัญของการออกมาตรการลงโทษ ก็เพื่อจะก่อให้เกิดการสถาปนาครั้งใหม่ซึ่งความถูกต้องตามกฎหมายระหว่างประเทศ (Re-establish international legality)

การสถาปนาครั้งใหม่ซึ่งความถูกต้องตามกฎหมายระหว่างประเทศ (Re-establish International legality) นั้นได้ถูกสะท้อนออกมาจากกฎบัตรสหประชาชาติที่กำหนดหน้าที่ให้คณะมนตรีความมั่นคงมีอำนาจรับรองมาตรการลงโทษเพื่อการดำรงรักษาและสถาปนาครั้งใหม่ซึ่งสันติภาพและความมั่นคงระหว่างประเทศ โดยลักษณะสำคัญของมาตรการลงโทษของใช้อำนาจตามกฎบัตรของคณะมนตรีความมั่นคงจะประกอบด้วย การมีอำนาจในการตัดสินใจต่อการลงโทษการกระทำใดในสถานการณ์ใดที่ถือว่าการคุกคามต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกราน และอำนาจให้การบังคับต่อการตัดสินใจของคณะมนตรีความมั่นคงเอง ตามองค์ประกอบทั้งสองข้อนี้จะสอดคล้องต่อลักษณะทั่วไปของการลงโทษ ว่าจะต้องมีทั้งรูปแบบของการบังคับ (Form of

³⁵ Denis Alland, "Countermeasures of General Interest", *European Journal of International Law* (Vol. 13, 5, 1221-1239, December 2002), p. 1224

enforcement) และรูปแบบของการทำงานที่สามารถรับรองได้ว่าจะมีการปฏิบัติตาม (Form of guarantees for compliance)

แผนผังแสดงการเปรียบเทียบลักษณะทั่วไปของการลงโทษกับมาตรการลงโทษของคณะมนตรีความมั่นคง



อ้างอิงข้อมูลในแผนผัง : Alain Pellet, Alina Miron, "Sanctions", In The Max Planck Encyclopedia of Public International Law

2.2.1 ความมุ่งหมายและหลักการตามกฎบัตรสหประชาชาติ

ในกฎบัตรสหประชาชาติข้อที่ 1 ได้กล่าวถึงเจตจำนงและความมุ่งหมายของสหประชาชาติว่า ต้องการที่ดำรงไว้ซึ่งสันติภาพและความมั่นคงระหว่างประเทศ³⁶ และการจะทำหน้าที่เพื่อบ่มงูสู่จุดปลายนี้ สหประชาชาติจะดำเนินมาตรการร่วมกัน ในการป้องกัน และขจัดซึ่งภัยคุกคามต่อสันติภาพต่อต้านและปราบปราม การรุกราน รวมถึงการละเมิดซึ่งกฎบัตรนี้ โดยจะนำวิธีทางสันติวิธีและสอดคล้องต่อหลักความยุติธรรม และพันธกรณีตามกฎหมายระหว่างประเทศ เพื่อการแก้ไขและระงับซึ่งข้อพิพาทที่เกิดขึ้นในสังคมระหว่างประเทศ รวมไปถึงสถานการณ์ระหว่างประเทศอันมีความเสี่ยงที่จะนำไปสู่การการคุกคาม การรุกราน การละเมิดต่อสันติภาพและความมั่นคง ทั้งนี้สนับสนุนการพัฒนาสัมพันธ์ไมตรีระหว่างประเทศโดยยึดมั่นต่อหลักการความเท่าเทียมของรัฐ³⁷ สนับสนุนการร่วมมือระหว่างประเทศ เรื่องของการแก้ไขปัญหาระหว่างประเทศในทาง สังคม เศรษฐกิจ และวัฒนธรรมรวมทั้งการส่งเสริมและสนับสนุนและเคารพต่อหลักการว่าด้วยสิทธิมนุษยชนโดยปราศจากอคติในความแตกต่างระหว่าง เชื้อชาติ ศาสนา เพศ รวมถึงจุดยืนทางการเมือง และองค์การ

³⁶ Charter of the United Nations Article 1

³⁷ ร้อยตำรวจเอกเมื่อง พรหมเกษา, "สถานะเหนือกว่าของพันธกรณีตามกฎหมายบัตรสหประชาชาติต่อพันธกรณีตามข้อตกลง ตามกฎหมายระหว่างประเทศอื่น : กรณีศึกษาข้อมติคณะมนตรีความมั่นคงว่าด้วยการต่อต้านการก่อการร้ายและคำวินิจฉัยของศาลยุติธรรมแห่งสหภาพยุโรป" (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2555).

สหประชาชาติยึดมั่นที่จะเป็นศูนย์กลางสำหรับการประสานงานระหว่างประเทศของประชาชาติทั้งหลาย เพื่อให้บรรลุสู่จุดหมายตามกฎบัตรร่วมกัน

ในการดำเนินการตามความมุ่งหมายของกฎบัตรสหประชาชาติ ข้อที่ 2 ได้กล่าวว่า องค์การสหประชาชาตินั้นยึดมั่นต่อหลักการแห่งความเสมอภาคในอธิปไตยของรัฐสมาชิกทั้งปวง รัฐสมาชิกเองจะต้องยึดถือทางปฏิบัติตามข้อผูกพันตามกฎบัตรนี้โดยสุจริตโปร่งใส³⁸ รัฐสมาชิกจะต้องระงับซึ่งข้อพิพาทระหว่างประเทศที่เกิดขึ้นของตนโดยการอาศัยสันติวิธี และละเว้นจากการคุกคาม หรือการใช้กำลังต่อบูรณภาพแห่งอาณาเขต หรือเอกราชทางการเมืองของรัฐอื่นใด ตลอดจนให้การสนับสนุนช่วยเหลือทุกประการ แก่สหประชาชาติในการกระทำใดๆ ที่เป็นการดำเนินการภายใต้กฎบัตร ในกรณีของรัฐที่มีได้เป็นสมาชิกของสหประชาชาติ พึงต้องปฏิบัติตามหลักการตามกฎบัตรนี้ เท่าที่จำเป็นแก่การดำรงไว้ซึ่งสันติภาพและความมั่นคงระหว่างประเทศ และสุดท้ายสหประชาชาติจะต้องมีเข้าทำการแทรกแซงในเรื่องสาระสำคัญภายใต้อำนาจอธิปไตยของรัฐแต่หลักการนี้จะไม่กระทบกระเทือนถึงสิทธิของสหประชาชาติในการบังคับใช้มาตรการภายใต้หมวดที่เจ็ด

การเข้ามามีบทบาทเสริมจากบทบาทตามตราสารระหว่างประเทศในการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงนั้น สอดคล้องกับในช่วง ค.ศ. 1990 มีการศึกษาที่พบว่าแนวโน้มของการก่อการร้ายไม่มีท่าทีว่าจะลดจำนวนลงอย่างมีนัยยะสำคัญ แม้จะมีการบังคับใช้ตราสารระหว่างประเทศแล้วก็ตาม³⁹ จึงจำเป็นที่คณะมนตรีความมั่นคงแห่งสหประชาชาติจะเข้ามาเป็นผู้กำหนดบทบาทเสริมภายใต้กรอบความมั่นคงร่วม ในการต่อต้านภัยการก่อการร้าย ดังนั้นในหัวข้อนี้ผู้เขียนจะอธิบายเพื่อชี้ให้เห็นถึงความสัมพันธ์ของบทบาทคณะมนตรีความมั่นคงกับภัยคุกคามของการก่อการร้าย รวมทั้งประโยชน์และความจำเป็นของมาตรการแบ่งปันข้อมูลภายใต้กลไกการบังคับตามหมวดที่เจ็ดของกฎบัตรสหประชาชาติ

แนวทางในการร่วมมือของรัฐสมาชิกสหประชาชาติให้สอดคล้องต่อหลักความมั่นคงร่วมตามกฎบัตรสหประชาชาติที่ว่า การจะดำรงรักษาไว้ซึ่งสันติภาพและความมั่นคงระหว่างประเทศนั้น รัฐสมาชิกจะต้องให้ความร่วมมือร่วมกันในการปราบปรามภัยคุกคามต่อสันติภาพโดยเฉพาะอย่างยิ่งภัย

³⁸ Charter of the United Nations Article 2

³⁹ Sebastian von Einsiedel, "International Conventions In Assessing the UN's Efforts to Counter Terrorism," (October 2016). อ้างอิงนัยยะทางสถิติการก่อการร้าย W. Enders, T. Sandler and J. Cauley, "UN Conventions, Technology and Retaliation in the Fight Against Terrorism: An Econometric Evaluation," *Terrorism and Political Violence* 2, No. 1 (1990), pp. 83-105, Available from https://i.unu.edu/media/cpr.unu.edu/attachment/2295/OC_08-Assessing-the-UNs-Efforts-to-Counter-terrorism-003.pdf

ของการก่อการร้าย ซึ่งการดำเนินความร่วมมือตามหลักความมั่นคงร่วม⁴⁰ นั้นประกอบด้วย 3 เสาหลักคือ

1.) หลักประสิทธิผล (Effectiveness) กล่าวคือ ประสิทธิภาพของหลักความมั่นคงร่วม (Collective security) จะเกิดขึ้นได้หากปราศจากการร่วมมือของบรรดารัฐสมาชิกสหประชาชาตินั้นหมายความว่ารัฐใดรัฐหนึ่งจะดำเนินการต่อต้านการก่อการร้ายเพียงลำพังมิได้

2.) หลักประสิทธิภาพ (Efficiency) กล่าวคือ บรรดารัฐสมาชิกจะต้องมีความเต็มใจที่จะจริงจัง (Willingness to get serious) กับการป้องกันปัญหาการก่อการร้ายนี้ โดยที่ไม่คิดว่าเป็นปัญหาหรือผลประโยชน์ของรัฐใดรัฐหนึ่ง

3.) หลักคุณธรรม (Equity) กล่าวคือ รัฐสมาชิกสหประชาชาติจะต้องไม่เลือกปฏิบัติในการตอบสนองต่อภัยคุกคามต่อความมั่นคงระหว่างประเทศ เช่น การเพิกเฉยต่อปัญหาการก่อการร้ายซึ่งอาจจะมิได้เป็นปัญหาในภูมิภาคหรืออนุภูมิภาคของตนเอง

2.2.2 ฐานอำนาจทางกฎหมายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ

คณะมนตรีความมั่นคงแห่งสหประชาชาติเป็นองค์กรหลักของสหประชาชาติที่มีอำนาจแตกต่างจากองค์กรอื่น กฎบัตรสหประชาชาติได้ให้ฐานทางอำนาจแก่คณะมนตรีในการรักษาสันติภาพและความมั่นคงระหว่างประเทศ โดยเฉพาะอย่างยิ่งอำนาจภายใต้หมวดที่เจ็ดของกฎบัตร และคำตัดสินของคณะมนตรีมีผลผูกพันทางกฎหมาย อันหมายความว่าประเทศสมาชิกสหประชาชาติทั้งหมดมีพันธกรณีที่ต้องปฏิบัติตามคำตัดสินของคณะมนตรี โดยในส่วนนี้จะได้วิเคราะห์ถึงอำนาจและหน้าที่ของคณะมนตรีความมั่นคง ตลอดจนการดำเนินการเกี่ยวกับการคุ้มครองสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกราน

2.2.2.1 อำนาจและหน้าที่

การศึกษาถึงฐานอำนาจทางกฎหมายที่ว่าด้วยอำนาจและหน้าที่ของคณะมนตรีความมั่นคงแห่งสหประชาชาตินั้น จำเป็นที่จะต้องอธิบายถึงบทบาทของคณะมนตรีความมั่นคงตามที่ได้กำหนดไว้ในกฎบัตรสหประชาชาติเสียก่อน เมื่อพิจารณาแล้วจะพบว่าองค์กรนี้มีหน้าที่หลักคือ การดำรงและรักษาไว้ซึ่งสันติภาพและความมั่นคงระหว่างประเทศ⁴¹ และดำเนินการออกมาตรการระหว่างประเทศ

⁴⁰ General Assembly, "Report of the High-level Panel on Threats, Challenges and Change - A more secure world: our shared responsibility", the Chair of the High-level Panel on Threats, Challenges and Change addressed to the Secretary-General (Fifty-ninth session, 2 December 2004), pp. 31-43

⁴¹ นาดยา ทิพวันต์, ข้อมติขององค์การระหว่างประเทศในฐานะที่เป็นบ่อเกิดของกฎหมายระหว่างประเทศ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, พ.ศ. 2534). นาดยา ทิพวันต์, "ข้อมติขององค์การ

เพื่อบรรลุวัตถุประสงค์โดยอาศัยฐานทางอำนาจในทางกฎหมายที่ได้ปรากฏในกฎบัตรสหประชาชาติ หมวดที่ 6 ว่าด้วยการระงับข้อพิพาทโดยสันติ และหมวดที่ 7 ว่าด้วยการดำเนินงานเกี่ยวกับการคุกคามต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกราน และหมวดที่ 8 ว่าด้วยข้อตกลงส่วนภูมิภาค

เมื่อพิจารณาถึงฐานทางกฎหมายที่ว่าด้วยอำนาจและหน้าที่ของคณะมนตรีความมั่นคงแล้ว กฎบัตรสหประชาชาติ ข้อ 25 กล่าวได้ว่ารัฐภาคีของสหประชาชาติจำเป็นต้องผูกพันต่อข้อมติที่ออกโดยคณะมนตรีความมั่นคงแห่งสหประชาชาติ ซึ่งข้อมติของคณะมนตรีความมั่นคงนั้นถือเป็นการกระทำขององค์การระหว่างประเทศ แต่ยังมีได้ยอมรับหรือพัฒนาถึงระดับที่เป็นสนธิสัญญา แต่ก็มีสภาพของความเป็นกฎเกณฑ์ที่จะกำหนดถึงพฤติกรรม หน้าที่และสิทธิของรัฐสมาชิก ซึ่งในบางครั้ง การกระทำขององค์การระหว่างประเทศในลักษณะนี้ อาจมีความคล้ายคลึงในทำนองเดียวกับสนธิสัญญาที่มุ่งสร้างหลักกฎหมาย (Law-making treaty)⁴² และในข้อที่ 39 ของกฎบัตรสหประชาชาตินั้นได้กำหนดให้คณะมนตรีความมั่นคงมีอำนาจที่จะพิจารณาถึงสถานการณ์ใด ที่ละเมิดต่อสันติภาพและความมั่นคงระหว่างประเทศ

ในช่วงทศวรรษที่ผ่านมาการทำงานของคณะมนตรีความมั่นคง ภายใต้แนวคิดระเบียบโลกใหม่⁴³ (New world order) ที่เป็นการร่วมมือกันของชาติมหาอำนาจที่เป็นสมาชิกถาวรในคณะมนตรีความมั่นคง และมีบทบาทสำคัญในการประกาศเหตุการณ์ใดบ้างที่เป็นภัยต่อสันติภาพและความมั่นคงระหว่างประเทศ ซึ่งไม่ได้มีเพียงแต่ภัยคุกคามต่อสันติภาพของการขัดกันทางอาวุธ เท่านั้น แต่ยังรวมถึงสถานการณ์อื่น ๆ ที่ถูกกำหนดจากคณะมนตรีความมั่นคงว่าเป็นภัยคุกคามต่อสันติภาพอีกด้วย การจะดำเนินการตามหมวดที่ 7 ได้นั้น คณะมนตรีจะต้องพิจารณาถึงว่าเหตุการณ์ใด บ้างที่ถือเป็นการคุกคามต่อสันติภาพ การละเมิดต่อสันติภาพ และการรุกราน นั้นได้เกิดขึ้นและยังคงมีการดำเนินอยู่หรือไม่ ดังเช่น ภัยคุกคามจากการก่อการร้ายนั้นถือเป็นภัยที่คุกคามสันติภาพและความมั่นคง จำเป็นที่จะต้องมีการมาตรการเพื่ออ้างหรือสถาปนากลับคืนมาซึ่งสันติภาพ โดยอาศัยข้อ 40 ซึ่งเป็นเรื่องของการอนุญาตให้คณะมนตรีความมั่นคงใช้มาตรการชั่วคราว ข้อ 41 กำหนดมาตรการบังคับ

ระหว่างประเทศในฐานะที่เป็นบ่อเกิดของกฎหมายระหว่างประเทศ" (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, พ.ศ. 2534).

⁴² ดวงเด่น นาคสีหราช, หลักกฎหมายระหว่างประเทศแผนกคดีเมือง (พิมพ์ครั้งที่ 2: กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, ปี พ.ศ. 2562). ดวงเด่น นาคสีหราช, หลักกฎหมายระหว่างประเทศแผนกคดีเมือง, ed. พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, ปี พ.ศ. 2562).

⁴³ Rosa Giles Carnero, "Terrorist acts in the configuration of the threat to international peace and security," (2012).

http://rabida.uhu.es/dspace/bitstream/handle/10272/15562/TERRORIST_ACTS%20AS_THREATS.pdf?sequence=2

โดยไม่ใช้กำลัง แต่จะอาศัยการบังคับทางเศรษฐกิจ การคมนาคม และทางการทูต⁴⁴ ส่วนข้อ 42 ให้อำนาจคณะมนตรีความมั่นคงในการใช้มาตรการบังคับโดยการใช้กำลังทางทหารได้ เท่าที่เห็นว่ามาตรการตามข้อที่ผ่านมานั้นไม่เพียงพอหรือไม่ได้ประสิทธิภาพในการแก้ไขสถานการณ์ให้กลับคืนสู่สันติภาพ

2.2.2.2 การดำเนินการเกี่ยวกับการคุกคามต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกราน

กลไกทางกฎหมายที่ให้อำนาจคณะมนตรีความมั่นคงในการออกมาตรการลงโทษถูกรับรองไว้ในหมวดที่เจ็ดของกฎบัตรสหประชาชาติ ซึ่งถูกดัดแปลงปรับเปลี่ยนมาจากกติกาสนธิสัญญา (The Covenant of the League of Nations) ข้อที่ 16 ซึ่งมีใจความสำคัญว่า⁴⁵ “รัฐสมาชิกทั้งหลายได้ให้สัญญาว่าจะเข้าร่วมในการดำเนินการร่วมกันกับรัฐที่ได้ทำสงครามโดยละเมิดพันธสัญญา การดำเนินการนี้จะต้องดำเนินการในทุกกรณีในรูปแบบของการคว่ำบาตรทางเศรษฐกิจเป็นกลไกบีบบังคับหลัก และหากยังไม่เพียงพอให้ใช้การแทรกแซงทางทหาร” แต่กติกาสนธิสัญญาได้เปิดโอกาสให้รัฐสมาชิกมีอิสระที่จะกำหนดว่าอะไรคือการละเมิดพันธสัญญา ซึ่งมีความแตกต่างอย่างชัดเจนกับกฎบัตรสหประชาชาติตามหมวดที่เจ็ด ที่ได้ยกให้องค์กรหลัก อย่างคณะมนตรีความมั่นคงแห่งสหประชาชาติเพียงองค์กรเดียวในการทำหน้าที่กำหนดถึงการกระทำที่เป็นการละเมิดต่อสันติภาพและความมั่นคงระหว่างประเทศ⁴⁶ อาทิ การคุกคามต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกรานตามข้อที่ 39 ของกฎบัตรสหประชาชาติ โดยทั้งนี้คณะมนตรีความมั่นคงมีอำนาจในการตัดสินใจดำเนินการเพื่อสถาปนากลับคืนตามข้อที่ 41 และข้อที่ 42

เมื่อพิจารณาจากกฎบัตรสหประชาชาติหมวดที่เจ็ด จะทราบถึงกลไกการใช้อำนาจของคณะมนตรีความมั่นคงว่าสามารถกำหนดการกระทำที่เป็นการคุกคามต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกราน และสามารถที่จะรับรองข้อมติในรูปแบบของคำแนะนำ (Recommendations) หรือข้อมติในรูปแบบมาตรการลงโทษเพื่อสถาปนากลับคืนมาซึ่งสันติภาพและความมั่นคงระหว่างประเทศ ตามข้อที่ 41 และข้อที่ 42 ของกฎบัตรสหประชาชาติ ดังนั้นกฎบัตรสหประชาชาติหมวดที่เจ็ดจึงถูกสะท้อนว่าเป็นกลไกในการลงโทษรัฐที่เป็นเจ้าของการกระทำการคุกคามต่อสันติภาพ การละเมิดสันติภาพ และการกระทำการรุกรานเท่านั้น กล่าวอีกนัยคือกฎบัตรสหประชาชาติหมวดที่เจ็ดเป็นแต่เพียงกลไกในการลงโทษรัฐผู้ที่ละเมิดสันติภาพเท่านั้น หากได้เป็นกลไกในการลงโทษรัฐผู้เป็นเจ้าของการละเมิดต่อกฎหมายระหว่างประเทศไม่แต่อย่างใด

⁴⁴ United Nations Charter Article 40, 41, 42

⁴⁵ The Covenant of the League of Nations, Article 16

⁴⁶ Charter of the United Nations Article 39, 41, 42

(International wrongful act) หากมองในแนวคิดที่ว่า การสถาปนา กลับคืนมาซึ่งสันติภาพ (Re-establishment of peace) ก็กับการสถาปนา กลับคืนมาซึ่งการกระทำที่ถูกต้องตามกฎหมาย (Re-establishment of legality) เป็นคนละเรื่องกัน⁴⁷ เพราะตามตราสารก่อตั้งอย่างกฎบัตรสหประชาชาติมิได้ให้อำนาจคณะมนตรีความมั่นคงเป็นองค์กรที่มีอำนาจในการชี้ขาด (Adjudicate) ในเรื่องของการกระทำที่เป็นมูลละเมิด (Wrongful conduct) ต่อกฎหมายระหว่างประเทศ แต่หากอำนาจนั้นถูกจำกัดไว้เฉพาะเรื่องสันติภาพและความมั่นคงเท่านั้น

อย่างไรก็ตามเมื่อพิจารณาจากแนวปฏิบัติของคณะมนตรีความมั่นคงแห่งสหประชาชาติในการใช้อำนาจตามหมวดที่เจ็ดเพื่อออกมาตรการลงโทษในเรื่องการคุกคามต่อสันติภาพ และการละเมิดสันติภาพ จะพบว่า การใช้อำนาจตามหมวดเจ็ดนั้นมีพื้นฐานมาจากการที่เห็นว่าเหตุการณ์ทั้งสองเรื่องนั้นเป็นผลมาจากการละเมิดกฎหมายระหว่างประเทศ และจำเป็นที่จะต้องออกพันธกรณีเฉพาะกิจต่อรัฐผู้ละเมิดโดยกลไกของมาตรการลงโทษตามข้อที่ 41 และข้อที่ 42 เพื่อเป็นผลให้เกิดการรักษาหรือสถาปนา กลับคืนซึ่งสันติภาพและความมั่นคงระหว่างประเทศตามข้อที่ 39 ของกฎบัตรสหประชาชาติ แม้ว่าในหมวดที่เจ็ดของกฎบัตรอาจจะมีได้มีบทบาทต่อการสร้างกฎหมาย โดยตรง แต่กลับมีบทบาทในการสร้างบรรทัดฐานระดับรอง (Secondary normative function)⁴⁸ ต่อสังคมระหว่างประเทศในเรื่องการรักษาสันติภาพและความมั่นคง

ในแนวปฏิบัติของคณะมนตรีความมั่นคงในหลายๆกรณีของการปรับข้อเท็จจริงให้เข้ากับข้อกฎหมาย (Characterization) นั่นก็คือหมวดที่เจ็ดของกฎบัตร จะพบว่า การเกิดขึ้นของการคุกคามต่อสันติภาพ และการละเมิดสันติภาพเป็นผลมาจากจากการละเมิดกฎหมายระหว่างประเทศ เพราะในท้ายที่สุดแล้วการรักษาไว้ซึ่งสันติภาพ และการเคารพกฎหมายระหว่างประเทศนั้นถูกสะท้อนถึงการเกิดความสงบเรียบร้อยของสังคม (Public order) ซึ่งถือเป็นกฎเกณฑ์พื้นฐาน (Fundamental rules) ของสังคมที่หากปราศจากการเคารพปฏิบัติแล้วจะนำไปสู่การเกิดขึ้นของสังคมที่ไร้ซึ่งกฎเกณฑ์ ดังนั้นการใช้อำนาจตามหมวดที่เจ็ดของกฎบัตรตามแนวปฏิบัติของคณะมนตรีความมั่นคงที่ผ่านมาจะครอบคลุมไปยังเรื่องต่อไปนี้

1. ความขัดแย้งระหว่างรัฐ (Inter-State conflicts) เช่น กรณีของเกาหลีตามข้อมติที่ 82/1950 กรณีของหมู่เกาะฟอล์กแลนด์ตามข้อมติที่ 502/1982 กรณีของสงครามอิรักอิหร่านตามข้อมติที่ 598/1987 กรณีของอิรักคูเวต (สงครามอ่าว) ตามข้อมติที่ 660/1990

⁴⁷ Vera Gowlland-debbas, "Collective security revisited in light of the flurry over UN reform an international law perspective," *International Law and the Quest for its Implementation* (2007).

⁴⁸ Alina Miron Alain Pellet, "Sanctions," in *In The Max Planck Encyclopedia of Public International Law (MPEPIL)* ed. Edited under the Direction of Rüdiger Wolfrum (Published under the Auspices of the Max Planck Institute for Comparative Public Law and International Law, 2011).

2. ความขัดแย้งภายใน (Internal conflicts) เช่น กรณีของโซมาเลียตามข้อมติที่ 794/1992 กรณีของซูดานตามข้อมติที่ 1556/2004
3. ฝ่าฝืนหลักการปกครองระบอบประชาธิปไตยและรัฐธรรมนูญ (Breach of the principle of democracy and of the constitutional order) เช่น กรณีของเฮติตามข้อมติที่ 940/1994 กรณีของเซียร์ราลีโอนตามข้อมติที่ 1132/1997
4. การละเมิดกฎหมายสิทธิมนุษยชนและกฎหมายมนุษยธรรม (Human rights and humanitarian law violation) เช่น กรณีของบรูไนตามข้อมติที่ 1577/2004 กรณีของลิเบียตามข้อมติที่ 1970/2011
5. การก่อการร้าย เช่น ข้อมติที่ 1267/1999 ข้อมติที่ 1373/2001 ข้อมติที่ 1540/2004
6. โจรสลัด เช่น ข้อมติที่ 1816/2008 ข้อมติที่ 1976/2011⁴⁹

จากแนวปฏิบัติของคณะมนตรีความมั่นคงที่ได้กล่าวมาข้างต้นนั้น ก็พอจะทราบได้ว่าการใช้อำนาจตามหมวดที่เจ็ดนั้นมิได้จำกัดอยู่แค่เรื่องของรัฐอีกต่อไป แต่ขยายขอบเขตไปจนถึงเรื่องของการปกป้องบุคคล (Protection of individuals) คือการรักษาความมั่นคงทางมนุษย์ (Human security) ไปพร้อมกับการรักษาความมั่นคงของรัฐ ซึ่งสอดคล้องกับข้อที่ 1 ของกฎบัตรสหประชาชาติที่มุ่งให้ความสำคัญของสิทธิปัจเจกบุคคล (Individual rights) และศักดิ์ศรีของความเป็นมนุษย์ (Human dignity)⁵⁰ ดังแผนผัง

⁴⁹ United Nations Security Council Resolution 82/1950

United Nations Security Council Resolution 502/1982

United Nations Security Council Resolution 598/1987

United Nations Security Council Resolution 660/1990

United Nations Security Council Resolution 794/1992

United Nations Security Council Resolution 1556/2004

United Nations Security Council Resolution 940/1994

United Nations Security Council Resolution 1132/1997

United Nations Security Council Resolution 1577/2004

United Nations Security Council Resolution 1970/2011

United Nations Security Council Resolution 1267/1999

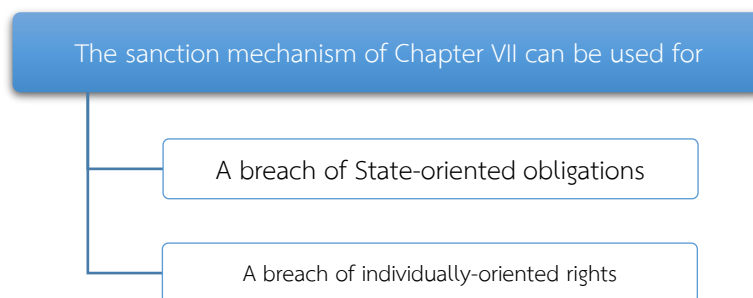
United Nations Security Council Resolution 1373/2001

United Nations Security Council Resolution 1540/2004

United Nations Security Council Resolution 1816/2008

United Nations Security Council Resolution 1976/2011

⁵⁰ Vera Gowlland-debbas, "Collective security revisited in light of the flurry over UN reform an international law perspective", *International Law and the Quest for its Implementation* (2007), p.



ถึงกระนั้นก็ตามการใช้อำนาจตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงมิได้เกิดขึ้นอย่างเป็นปกติเมื่อมีการกระทำที่เป็นการละเมิดกฎหมายระหว่างประเทศ เพราะการใช้อำนาจตามหมวดเจ็ดดังกล่าวอาจจะถูกขัดขวางในกรณีที่รัฐสมาชิกถาวรได้ใช้สิทธิในการยับยั้ง (Veto) มาตรการตามหมวดที่เจ็ดดังกล่าว หรือขาดซึ่งคะแนนเสียงถึง 9 ใน 15 คะแนนเสียงการใช้อำนาจตามหมวดที่เจ็ดในการออกมาตรการต่างๆ ก็มีโอกาสเกิดขึ้นได้ ซึ่งกลไกเหล่านี้ถูกสะท้อนออกมาว่าการใช้อำนาจของคณะมนตรีความมั่นคงตามหมวดที่เจ็ดมีวาระซ่อนเร้นทางการเมือง (Political hidden agenda)⁵¹ และเป็นที่ยืนยันว่ามาตรการของคณะมนตรีความมั่นคงนั้นไม่ใช่วิธีที่มีประสิทธิภาพระหว่างประเทศ

2.2.3 ผลของมาตรการบังคับภายใต้หมวดที่เจ็ดตามกฎหมายบัตรสหประชาชาติ

ในกฎบัตรสหประชาชาติข้อที่ 25 ระบุไว้อย่างชัดเจนว่าบรรดารัฐสมาชิกสหประชาชาติตกลงยอมรับและปฏิบัติตามคำวินิจฉัยของคณะมนตรีความมั่นคงแห่งสหประชาชาติ⁵² กล่าวคือเมื่อคณะมนตรีความมั่นคงได้วินิจฉัยว่าจะใช้มาตรการใดตามข้อ 41 และข้อ 42 ตามหมวดที่เจ็ดของกฎบัตรเพื่อชำระไว้หรือสถาปนากลับคืนมาซึ่งสันติภาพและความมั่นคงระหว่างประเทศแล้วนั้น พันธกรณีดังกล่าวจักก่อให้เกิดความผูกพันของรัฐสมาชิกแห่งสหประชาชาติในการปฏิบัติตามคำวินิจฉัยนั้น ส่วนบทบาทของการประเมินการปฏิบัติตามคำวินิจฉัย จากบรรดารัฐสมาชิกนั้น ในทางปฏิบัติส่วนใหญ่ของคณะมนตรีความมั่นคงจะรับรององค์กรย่อย หรือที่เรียกว่า คณะกรรมการลงโทษ ขึ้นมาเพื่อมีส่วนร่วม หรือสำรวจการดำเนินการตามคำวินิจฉัยของบรรดารัฐสมาชิก และรายงานต่อคณะมนตรีความมั่นคง⁵³ ซึ่งในกรณีของมาตรการต่อต้านการก่อการร้ายจะมีคณะกรรมการลงโทษที่ถูกรับรองภายใต้ข้อมติของคณะมนตรีความมั่นคงถึง 3 คณะคือ

⁵¹ Sally Morphet, "Resolutions and Vetoes in the UN Security Council: Their Relevance and Significance," in *Review of International Studies* (Published by Cambridge University Press October, 1999).

⁵² Charter of the United Nations Article 25

⁵³ Laurie Blank, "Creating a More Effective Tool for the Enforcement of International Law," *Article from Emory University* (1995).

(1.) คณะกรรมการความมั่นคง (Committee of the Security Council) หรือชื่อปัจจุบันคือ คณะกรรมการลงโทษกลุ่มอัลไคดะ (The Al-Qaida Sanctions Committee) ที่ถูกจัดตั้งโดยข้อมติที่ 1267/1999

(2.) คณะกรรมการต่อต้านการก่อการร้าย (the Counter-Terrorism Committee) ที่ถูกจัดตั้งขึ้นตามข้อมติที่ 1373/2001 ซึ่งจะเน้นดูแลเรื่องการ Implementation counter-terrorism resolutions ของบรรดารัฐต่างๆ

(3.) คณะกรรมการความมั่นคง (the Security Council Committee) ที่ถูกจัดตั้งโดยข้อมติที่ 1540/2004 จะดูแลเรื่องการไม่แพร่อาวุธอาวุธทำลายล้างสูง⁵⁴

ดังนั้นพันธกรณีของบรรดารัฐต่างๆในการดำเนินการตามคำวินิจฉัยของคณะมนตรี ก็คือการดำเนินการออกกฎหมายภายในของรัฐตน (National legal orders) เพื่อที่จะก่อให้เกิดผลลัพธ์ต่อวัตถุประสงค์ของคำวินิจฉัยคณะมนตรีในเรื่องนั้น โดยทั่วไปแล้วคำวินิจฉัยจะอยู่ในรูปของข้อมติ (Resolutions) ที่จะระบุไว้เป็นในทำนองทั่วไป (Generic formula) คล้ายๆกันว่า “Decides that all States shall take the measures...” ซึ่งประโยคดังกล่าวนี้ถูกสะท้อนออกมาว่า คณะมนตรีความมั่นคงมีคำวินิจฉัยที่กำหนดให้รัฐจำเป็นที่จะต้องออกมาตรการทางกฎหมายภายใน (Domestic legal measures) ของรัฐตนเพื่อที่จะสร้างให้เกิดผลต่อคำวินิจฉัยในข้อมติของคณะมนตรีความมั่นคงนั่นเอง ทั้งนี้ได้หมายรวมถึงประเทศที่อยู่บนฐานคิดแบบทฤษฎีเอกนิยม (Monism) กว่า 20 ประเทศ อาทิ สหราชอาณาจักร สหรัฐอเมริกา ซึ่งเป็นรัฐที่นำเอากฎหมายระหว่างประเทศดำเนินการใช้เป็นมาตรการภายในระดับชาติโดยอัตโนมัติ⁵⁵

จุฬาลงกรณ์มหาวิทยาลัย



⁵⁴ Security Council Counter-Terrorism Committee, About Counter-Terrorism Committee and our mandate (2020), Available from <https://www.un.org/sc/ctc/about-us>

⁵⁵ Alain Pellet, Alina Miron, "Sanctions", In *The Max Planck Encyclopedia of Public International Law (MPEPIL) Vol. 9*, Edited under the Direction of Rüdiger Wolfrum. (Published under the Auspices of the Max Planck Institute for Comparative Public Law and International Law, 2011), pp.44

2.2.3.1 หน้าที่ของรัฐในการปฏิบัติตามเงื่อนไขบังคับ (Mandatory term) ตามข้อมติว่าด้วยการลงโทษ

ในแต่เดิมเงื่อนไขบังคับที่ปรากฏในข้อมติที่ตัดสินตามหมวดที่เจ็ดของคณะมนตรีผู้กพันรัฐสมาชิกและรัฐที่ไม่มีเป็นสมาชิกตามนัยยะของกฎบัตรข้อที่ 2(6) มีหน้าที่ที่จะต้องปฏิบัติตาม ได้มีแนวคำพิพากษาภายในรัฐว่าข้อมติไม่มีอำนาจในการสร้างผลใช้บังคับได้เอง (non-self-executing obligations) จึงจำเป็นต้องรอการตรากฎหมายภายในของรัฐเสียก่อน⁵⁶ ดังเช่นที่ปรากฏในคดี *Diggs v. Dent* ของประเทศสหรัฐอเมริกา หรือคดี *Biadley v. Commonwealth of Australia and the Postmaster-General* ซึ่งจะแตกต่างจากกรณีของสหภาพยุโรป (European Union) ที่มีอำนาจในการออก “Regulations” ที่มีผลบังคับทางกฎหมายใช้โดยตรงในรัฐสมาชิก โดยที่รัฐสมาชิกไม่จำเป็นต้องตรากฎหมายภายในออกมารองรับ (Self-executing obligations)⁵⁷

อย่างไรก็ตามมีแนวโน้มจากการปฏิบัติของคณะมนตรีในการใช้อำนาจในการสร้างผลใช้บังคับได้เอง เมื่อพิจารณาจากข้อมติคณะมนตรีความมั่นคงเพื่อต่อต้านการก่อการร้ายที่ 1267/1999⁵⁸ กับข้อมติที่ 1989/2011⁵⁹ ที่ได้สร้างกลไกของมาตรการลงโทษในการกำหนดรายชื่อของบุคคล (United Nations Sanction Listing measure) จากตัวคณะมนตรีความมั่นคงเอง และแม้ว่าข้อมตินี้ คณะมนตรีความมั่นคงจะมีได้บังคับรัฐให้ปฏิบัติตามวิธีการที่เฉพาะต่อการดำเนินการตามข้อมติ แต่ไม่ได้หมายความว่ารัฐสามารถกำหนดทั้งเนื้อหาหรือที่เป็นการเฉพาะของตน ต่อมาตรการการลงโทษตามข้อมติที่ 1267/1999 ดังนั้นมาตรการลงโทษต่อรายชื่อบุคคลที่ถูกกำหนดได้สะท้อนถึง “Pure obligations of result” ที่รัฐถูกกำหนดให้ปฏิบัติตามและการันตีผลว่าได้บรรลุซึ่งเป้าหมายของพันธกรณีตามข้อมติคณะมนตรีความมั่นคง

ซึ่งจะแตกต่างจาก “Obligations of means or conduct” ที่เป็นพันธกรณีที่ให้รัฐดำเนินการปฏิบัติตามและทำให้ดีที่สุดเท่าที่จะทำได้ แต่มีจำเป็นที่รัฐจะต้องการันตีผลว่าได้บรรลุซึ่งเป้าหมายของพันธกรณีตามข้อมติคณะมนตรีความมั่นคง⁶⁰ ดังที่คณะกรรมการกฎหมายระหว่างประเทศได้เคยมีแนวคิดที่จะวางกฎเกณฑ์ของการแยกระหว่าง “Obligations of result” และ “Obligations of means or conduct” ไว้ในร่างสนธิสัญญาว่าด้วยความรับผิดชอบของรัฐแต่มีประสพ

⁵⁶ Ibid, p. 40

⁵⁷ Ibid, p. 37

⁵⁸ United Nations Security Council Resolution 1267/1999 (All of the four pages)

⁵⁹ United Nations Security Council Resolution 1989/2011 (All of the eighteen pages)

⁶⁰ Constantin P. Economides, "The Sources of International Responsibility - Obligations of Means and Obligations Of Result - The traditional meaning of obligations of means or conduct and obligations of result," in *The Law of International Responsibility*, ed. Alain Pellet Edited By James Crawford, Simon Olleson, Kate Parlett (Published Oxford Commentaries on International Law, 20 May 2010).

ผลสำเร็จ จึงได้แต่เพียงวางหลักการไว้ในส่วนอรรถกถา ข้อ 12 ในร่างสนธิสัญญาว่าด้วยความรับผิดชอบของรัฐฉบับสมบูรณ์ปี 2001⁶¹

ในการลงโทษรัฐที่มีได้ปฏิบัติตามมาตรการลงโทษในข้อมติของคณะมนตรีนั้น ในกรณีที่มีรัฐบางรัฐทำการละเมิดมาตรการลงโทษตามข้อมติ ซึ่งตัวอย่างเองเคยปรากฏว่าคณะมนตรีความมั่นคงได้มีมาตรการลงโทษรัฐที่มีได้ปฏิบัติตามพันธกรณีของมาตรการลงโทษตามข้อมติที่ได้ลงโทษรัฐอื่นไปก่อนหน้านั้น กล่าวคือในข้อมติที่ 1343/2001 คณะมนตรีความมั่นคงได้ตัดสินลงโทษประเทศไลบีเรียสำหรับการละเมิดข้อมติว่าด้วยการปิดล้อมทางธุรกิจเพชร⁶² ต่อประเทศเซียร์ราลีโอน ซึ่งประเทศไลบีเรียได้มีการดำเนินธุรกิจนำเข้าและส่งออกซึ่งเพชรกับประเทศเซียร์ราลีโอนอยู่ภายหลังจากที่มีการออกมาตรการปิดล้อมจากคณะมนตรี จึงถือเป็นการละเมิดมาตรการลงโทษต่อข้อมติที่ 1306/2000 ของคณะมนตรีความมั่นคง แม้ว่าในข้อมติคณะมนตรีที่ 1306/2000 จะไม่ได้กำหนดให้รัฐทำการปิดล้อมทางธุรกิจเพชรต่อประเทศเซียร์ราลีโอนในรูปแบบเชิงบังคับอย่างชัดเจน ดังเช่นการระบุว่า “Decides that all States shall ...” แต่ในข้อมติดังกล่าวนั้นได้ใช้คำว่า “Calls upon all states to ...” อันมีลักษณะไม่เป็นรูปแบบบังคับ (Non-Mandatory term) มีข้อสังเกตต่อไปว่าในตัวเนื้อหาของข้อมตินั้น การจะพิจารณาจากตัวถ้อยคำขึ้นต้นอย่างเดียวแล้วสรุปว่าเป็นรูปแบบบังคับ (Mandatory term) หรือไม่เป็นรูปแบบบังคับหรือไม่นั้น อาจต้องอาศัยการพิจารณาจากประโยคตามหลังจากนั้นประกอบด้วยว่าสุดท้ายแล้วข้อมติดังกล่าวต้องการให้รัฐดำเนินการอะไร⁶³

ในความเห็นของผู้เขียนเมื่อได้พิจารณาพันธกรณีการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายตามข้อมติที่ 1373/2001 ได้ระบุไว้ทำนองที่ว่า “Calls upon all States to exchange information”⁶⁴ และข้อมติอื่นๆตามมาที่กำหนดให้รัฐมีพันธกรณีในการแบ่งปันข้อมูล ซึ่งก็มี

จุฬาลงกรณ์มหาวิทยาลัย

⁶¹ International Law Commission, "Draft articles on Responsibility of States for Internationally wrongful Acts with Commentaries" (2001), Article 12, pp. 11-12

⁶² “Calls upon all States, in particular those through which rough diamonds from Sierra Leone are known to transit, and all relevant international and regional organizations to act strictly in accordance with the provisions of this resolution notwithstanding the existence of any rights or obligations conferred or imposed by any international agreement or any contract entered into or any licence or permit granted prior to the date of adoption of this resolution” *from UNSC Resolution 1306/2000*

⁶³ Alain Pellet, Alina Miron, "Sanctions", In *The Max Planck Encyclopedia of Public International Law (MPEPIL) Vol. 9*, Edited under the Direction of Rüdiger Wolfrum. (Published under the Auspices of the Max Planck Institute for Comparative Public Law and International Law, 2011), pp. 47

⁶⁴ “Calls upon all States to exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts and Cooperate, particularly through bilateral and multilateral arrangements and agreements,

ความหมายว่าคณะมนตรีความมั่นคงต้องการให้รัฐออกกฎหมายเพื่อดำเนินการแบ่งปันข้อมูลในฐานะที่เป็น “A system of second degree of sanctions” เพราะคณะมนตรีความมั่นคงมิได้มีอำนาจในการเข้าไปกำหนดมาตรการลงโทษภายในรัฐ และที่เป็นเช่นนั้นก็เพราะอำนาจในการออกกฎหมายภายในเป็นของรัฐแต่เพียงผู้เดียว ทั้งนี้ได้หมายรวมถึงประเทศที่อยู่บนฐานคิดแบบทฤษฎีเอกนิยมกว่า 20 ประเทศ อาทิ สหราชอาณาจักร สหรัฐอเมริกา ซึ่งเป็นรัฐที่นำเอากฎหมายระหว่างประเทศดำเนินการใช้เป็นมาตรการภายในระดับชาติโดยอัตโนมัติ⁶⁵

แม้ว่าในข้อมติจะใช้คำว่า “Call upon” แต่ก็มีได้หมายความว่ารัฐจะไม่จำเป็นต้องปฏิบัติตามก็ได้ เพราะอย่างไรก็ตามการแบ่งปันข้อมูลถือเป็นส่วนหนึ่งของการดำเนินการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงตามหมวดที่เจ็ดบรรดาระฐมีพันธกรณีที่จะต้องดำเนินการอยู่แล้ว หากพิจารณาจากกฎบัตรสหประชาชาติ

2.2.3.2 ความสัมพันธ์ระหว่างระบบกฎหมายระหว่างประเทศ (International legal orders) กับระบบกฎหมายภายในประเทศ (Domestic legal orders)

การที่รัฐสมาชิกสหประชาชาติจะต้องออกมาตรการทางกฎหมายภายใน (Domestic legal measures) ของรัฐตนเพื่อที่จะสร้างเกิดผลต่อคำวินิจฉัยในข้อมติของคณะมนตรีความมั่นคงนั้น เนื่องจากข้อมติส่วนใหญ่ของคณะมนตรีความมั่นคงไม่มีอำนาจในการสร้างผลใช้บังคับได้เอง (Non-self-executing obligations) จึงจำเป็นต้องรอการตรากฎหมายภายในของรัฐเสียก่อน จากกรณีนี้สามารถวิเคราะห์ได้เบื้องต้นว่าท้ายที่สุดแล้ว กฎหมายระหว่างประเทศจะได้รับการปฏิบัติอย่างสอดคล้องหรือไม่นั้น ก็ขึ้นอยู่กับดำเนินการของกฎหมายภายใน⁶⁶

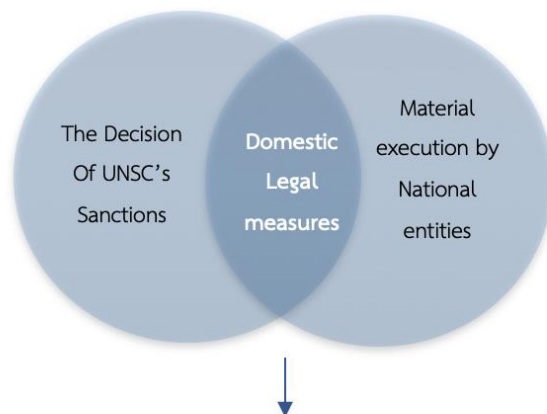
ในทั้งนี้ความสัมพันธ์ระหว่างระบบกฎหมายระหว่างประเทศ กับระบบกฎหมายภายในประเทศ จึงปรากฏให้ได้ทราบว่าจะระบบกฎหมายภายในประเทศจักทำหน้าที่เสมือนเป็น “ระบบกฎหมายในการรับรอง (Legal orders of reception)” กล่าวคือมีหน้าที่ในการรับรองพันธกรณีที่เกิดผลผูกพันจากข้อมติคณะมนตรีความมั่นคงซึ่งถือเป็นกฎหมายระหว่างประเทศ ดังนั้นสามารถสรุปกระบวนการได้ว่าการออกกฎหมายภายในประเทศขึ้นมาเพื่อรับรองพันธกรณีข้อมติคณะมนตรีความมั่นคงนั้น เกิดจากการหลอมรวมระหว่างคำวินิจฉัยของมาตรการลงโทษจากคณะมนตรีความมั่นคงกับ

to prevent and suppress terrorist attacks and take action against perpetrators of such acts” *from UNSC Resolution 1373/2001*

⁶⁵ Thomas J. Biersteker, "Counter-terrorism measures undertaken under UN Security Council auspices," *Business and Security: Public-Private Sector* (2003), <https://www.sipri.org/sites/default/files/files/books/SIPRI04BaiFro/SIPRI04BaiFro05.pdf>

⁶⁶ Benedetto Conforti, "International Law and the Role of Domestic Legal Systems," *American journal of international law* 88 (Martinus Nijhoff Publishers 1993).

กระบวนการออกกฎหมายภายในโดยหน่วยงานแห่งชาติของรัฐ (Material execution by national entities)



Legal orders of reception for implementation

2.3.1 ลักษณะของประเภทข้อมูลในการแบ่งปัน

Barbara Jankowski ได้ให้ลักษณะทั่วไปของข้อมูลที่ถูกทำการแบ่งปันภายใต้ภารกิจของสหประชาชาติในบทความที่ชื่อว่า “Information Sharing Among Military Operational Staff: The French Officers’ Experience” โดยอธิบายว่าลักษณะข้อมูลจะขึ้นอยู่กับผู้ผลิตข้อมูลและผู้รับข้อมูลเป็นหลัก ว่าต้องการที่จะให้ข้อมูลนั้นอยู่ในลักษณะรูปแบบใด ซึ่งการจะปรับใช้ข้อมูลแต่ละลักษณะนั้น จะต้องคำนึงถึงรูปแบบของภารกิจเป็นหลัก⁶⁷ หากภารกิจนั้นมีความอ่อนไหวที่จะสร้างผลกระทบต่อการปฏิบัติการทางทหารหรือความลับต่อการดำเนินงานของหน่วยงานราชการ ข้อมูลที่จะถูกใช้ในการแบ่งปันนั้นควรจะต้องถูกจำแนกประเภท เพื่อเกิดความชัดเจนและเพื่อเป็นประโยชน์ต่อเจ้าหน้าที่ผู้ปฏิบัติงานภายใต้ภารกิจนั้น และลักษณะของข้อมูลดังต่อไปนี้ได้ปรากฏอยู่ในข้อมติของคณะมนตรีความมั่นคงแห่งสหประชาชาติรวมถึงรายงาน และเอกสารต่างๆ ที่เกี่ยวข้องกับการต่อต้านการก่อการร้ายและภารกิจอื่นๆ

1. ข้อมูลที่เป็นความลับ (Confidential Information)

ในกรณีนี้สามารถแบ่งได้ออกเป็น สองประเภทย่อยอีกคือ ข้อมูลที่เป็นความลับที่สุด (Strictly Confidential Information) คือข้อมูลที่ถูกแบ่งปันภายใต้ภารกิจที่มีลักษณะเฉพาะขององค์การและเป็นความลับอย่างมาก หากข้อมูลประเภทนี้ได้ถูกแพร่เผยโดยมิได้รับอนุญาตจากสหประชาชาติสามารถก่อให้เกิดความเสียหายร้ายแรงโดยเฉพาะ หรือขัดขวางการทำงานของสหประชาชาติ ความ

⁶⁷ Barbara Jankowski, "Information Sharing Among Military Operational Staff: The French Officers’ Experience," in *Information Sharing in Military Operations*, ed. ed. Anthony J. (Cham: Springer Nature, 2017).

ปลอดภัยของเจ้าหน้าที่ การทำงานของประเทศสมาชิกภายใต้ภารกิจ และรวมถึงผลกระทบทั้งทางตรงและทางอ้อมต่อการดำเนินงานตามแผนในระยะยาวภายใต้ ภารกิจ การปฏิบัติการ และแผนกำหนดการ ที่ถูกตั้งขึ้นโดยสหประชาชาติ ถ้าหากข้อมูลชนิดนี้มีการรั่วไหลหรือเผยแพร่เกิดขึ้น ผลกระทบที่สามารถคาดคะเนไว้คือ อาจจะทำให้เกิดความเสียหายต่อร่างกายและชีวิตของผู้ปฏิบัติงานของสหประชาชาติ⁶⁸ และประเทศที่สามที่อยู่ภายใต้ภารกิจ อาจก่อให้เกิดการละเมิดสิทธิความเป็นส่วนตัวในทางการแพทย์ของบุคคล กลุ่มกองทหารที่ปฏิบัติงานในพื้นที่ภายใต้ภารกิจจะตกอยู่ในอันตราย รวมถึงอาจก่อให้เกิดวินาศกรรมที่สร้างความเสียหายอย่างมีนัยสำคัญต่อช่องทางการสื่อสารของภารกิจรักษาสันติภาพ (Peacekeeping mission's communication channels) และนำมาซึ่งการสูญเสียความเชื่อมั่นของประชาชนในการปฏิบัติการรักษาสันติภาพของสหประชาชาติ อย่างไรก็ตามลักษณะข้อมูลประเภทนี้จะพบได้ในภารกิจที่เกี่ยวข้องกับการรักษาสันติภาพ หรือการใช้กำลังเพื่อการปราบปรามกลุ่มติดอาวุธ แต่ในส่วนของมาตรการปราบปรามการก่อการร้ายนั้นกลับไม่พบอย่างเป็นทางการว่าจะต้องแบ่งปันข้อมูลในลักษณะนี้

ในส่วนของข้อมูลที่เป็นความลับ (Confidential Information) นั้นข้อมูลจะมีลักษณะที่มีได้เคร่งครัดในการแบ่งปันและการเข้าถึงมากเท่ากับกรณีแรก แต่ก็ยังมีลักษณะของความเป็นข้อมูลในชั้นความลับอยู่ โดยทั่วไปจะเป็นข้อมูลในทางเศรษฐกิจและการบริหารที่สำคัญ⁶⁹ ต่อการบริหารจัดการภายในองค์กร หรือระหว่างองค์กร อาทิ สัญญาและการติดต่อที่สำคัญ แผนกลยุทธ์และการเงินรายชื่อบุคคลที่เกี่ยวข้องต่อภารกิจ ซึ่งข้อมูลเหล่านี้จะต้องมีลักษณะที่เป็นความลับและอาจจะถูกฝ่ายตรงข้ามนำไปเพื่อหาประโยชน์ได้ หากข้อมูลประเภทนี้ได้แพร่เผยออกไปโดยปราศจากการอนุญาต อาจสร้างผลกระทบต่อการทำงานขององค์กร อาจส่งผลให้เกิดอันตราย แก่สหประชาชาติหรือประเทศสมาชิก และเลวร้ายที่สุดอาจกระทบต่อความสัมพันธ์ระหว่างสหประชาชาติและองค์กรอื่น⁷⁰ หรือขาดความมั่นใจระหว่างสหประชาชาติกับองค์กรอื่น อย่างไรก็ตามข้อมูลในชั้นนี้อาจสามารถฟื้นฟูความเสียหายที่เกิดจากการแพร่ข้อมูลได้ โดยการเจรจาระหว่างผู้ที่มีส่วนเกี่ยวข้องต่อภารกิจ มีภารกิจชี้แจงและมาตรการแก้ไขปัญหาที่ทัน่วงที

⁶⁸ United Nations Archives and Records Management Section, "UN ARMS Records and Information Management Guidance", (2007) Retrieved from https://archives.un.org/sites/archives.un.org/files/6-guidance_sensitive_information.pdf

⁶⁹ Dragan Z. Damjanović, Types of information warfare and examples of malicious programs of information warfare, (Republic of Serbia 2017).

⁷⁰ Ibid p.6, (See United Nations Archives and Records Management Section)

2. ข้อมูลข่าวกรอง (Intelligence Information)

เป็นลักษณะของข้อมูลที่มีความสำคัญต่อการใช้เพื่อการตัดสินใจดำเนินการทางทหาร หรือนโยบายของรัฐบาล ซึ่งข้อมูลในลักษณะนี้จะมีระดับความน่าเชื่อถือโดยจากการพิจารณาแหล่งที่มาของข้อมูล อาทิ ข้อมูลข่าวกรองที่ได้มาจากมนุษย์ (Human Intelligence) โดยอาจมีการเก็บข้อมูลมาจากเจ้าหน้าที่ผู้มีอำนาจในท้องถิ่นที่หน่วยปฏิบัติการได้ตั้งอยู่ ตลอดจนกลุ่มคนในท้องถิ่นที่มีความน่าเชื่อถือ รวมถึงหน่วยทหารและพลเรือนโดยทั่วไปที่มีความสัมพันธ์ทั้งทางตรงและทางอ้อมกับแหล่งข้อมูลที่สามารถนำมาเพื่อประกอบเป็นข่าวกรอง⁷¹ กรณีที่สองคือ ข่าวกรองในทางเทคนิค (Technical intelligence) คือข้อมูลข่าวกรองที่ได้มาจากวิธีการใช้เครื่องมือทางเทคโนโลยี เช่น ข้อมูลภาพถ่ายทางอากาศ ข้อมูลภาพถ่ายทางดาวเทียม ข้อมูลที่อยู่ในระบบอินเทอร์เน็ตของเซฟเวอร์ เป้าหมาย และ Signals intelligence (SIGINT) ซึ่งถูกพัฒนาให้มีประสิทธิภาพอย่างมากในปัจจุบัน ในการค้นหาสัญญาณที่อาจจะเชื่อได้ว่าเป็นข้อมูลข่าวกรองที่สำคัญ เช่น ในบริบทของการรักษาสันติภาพของสหประชาชาตินั้นอาจนำเทคโนโลยีนี้มาใช้ในการข่าวกรองเพื่อทราบถึงสถานการณ์ของความโหดร้ายในพื้นที่ขัดแย้ง อาทิ เพื่อทราบว่า การฆ่าล้างเผ่าพันธุ์ได้ดำเนินการภายใต้คำสั่งของผู้บังคับบัญชาระดับสูงคนใดบ้าง การสื่อสารและการติดต่อแบบใดที่ใช้ในระดับปฏิบัติการระหว่างฝ่ายคู่ขัดแย้ง การค้นหาหลักฐานเพื่อสนับสนุนว่าฝ่ายใดมีความตั้งใจในการปล่อยอาวุธ การค้นหาแหล่งที่ตั้งของหน่วยรบหรือกองกำลังติดอาวุธ รวมถึงกลุ่มก่อการร้ายต่างๆ และกรณีสุดท้าย⁷² ข้อมูลข่าวสารแบบเปิดเพื่อลดการพึ่งพาการเข้าถึงแหล่งข้อมูลข่าวกรองจากรัฐสมาชิก สหประชาชาติสามารถนำข้อมูลข่าวกรองในลักษณะแบบเปิด มาเพื่อเป็นประโยชน์ต่อการปฏิบัติการได้ ซึ่งแหล่งข้อมูลสาธารณะนั้นก็ถือได้ว่าเป็นข่าวกรองในรูปแบบหนึ่ง ข้อมูลที่ได้ อาจมาจาก นกหนังสือพิมพ์ นักวิชาการ เจ้าพนักงานสืบสวนสอบสวน วารสาร หนังสือนิตยสาร อุตสาหกรรมสิ่งพิมพ์ และสิ่งพิมพ์ของรัฐบาล โดยเฉพาะอย่างยิ่งในปัจจุบันข่าวสารจากโทรทัศน์ วิทยุ และเว็บไซต์ในระบบอินเทอร์เน็ตถือได้ว่าเป็นข้อมูลที่สามารถเข้าถึงได้อย่างรวดเร็ว

ดังนั้นแหล่งที่มาของข้อมูลข่าวกรองในลักษณะทั้งหมดที่ได้กล่าวมานี้ ในปัจจุบันนี้มีข้อมูลที่ถูกรผลิตขึ้นมาจำนวนมาก และเป็นที่เพียงพอต่อความต้องการในการนำข้อมูลไปวิเคราะห์ เพื่อเป็นข่าวกรองตามเป้าประสงค์ที่ตรงตามความต้องการของสหประชาชาติในการปฏิบัติการรักษาสันติภาพและความมั่นคงระหว่างประเทศ

⁷¹ Victor Catano and Jeffery Gauger, "Information Fusion: Intelligence Centers and Intelligence Analysis," in *Information Sharing in Military Operations*, ed. ed. Anthony J (Cham: Springer Nature, 2017).

⁷² Gustavo Díaz, "Intelligence at the United Nations for peace operations", (Complutense University of Madrid, January 2007), p. 35.

3. ข้อมูลเพื่อการปฏิบัติงาน (Operational Information)

การแบ่งปันข้อมูลในลักษณะนี้ของสหประชาชาติในภารกิจต่อต้านการก่อการร้าย ถูกกล่าวถึงเป็นครั้งแรกใน Madrid Guiding Principle ข้อที่ 10⁷³ และสหประชาชาติมิได้ให้นิยามที่ชัดเจนของลักษณะข้อมูลดังกล่าว หากพิจารณาจากรายงานของการใช้ข้อมูลในการปฏิบัติการของหน่วยงานที่มีอำนาจแห่งชาติ หน่วยงานด้านความมั่นคง กองกำลังทหาร และองค์กรพัฒนาเอกชน (Non-governmental organizations)⁷⁴ จะพบว่าลักษณะของข้อมูลนี้เป็นข้อมูลที่จะเสริมประสิทธิภาพและประโยชน์ต่อการปฏิบัติการโดยทั่วไปขององค์กร ข้อมูลสามารถนำไปวิเคราะห์สถานการณ์และสถานะแวดล้อมในปัจจุบันเพื่อประโยชน์ต่อการวางแผนของการปฏิบัติการนั้นๆ และเป็นข้อมูลที่เกี่ยวข้องกับข้อกำหนดด้านความปลอดภัย ของเจ้าหน้าที่ผู้ปฏิบัติการ ตลอดจนเป็นข้อมูลเกี่ยวกับการแก้ปัญหาและการดำเนินงานในพื้นที่ห่างไกล การแบ่งปันข้อมูลในลักษณะนี้จะกำจัดวงแคบอยู่เฉพาะผู้มีส่วนเกี่ยวข้อง และ Partners Beneficial ต่อการปฏิบัติการกิจเท่านั้น⁷⁵ แต่อย่างไรก็ตามในสงครามอัฟกานิสถาน มีกองกำลังร่วมรักษาสันติภาพ “The UN sanctioned International Security Assistance Force (ISAF)”⁷⁶ ที่ถูกจัดตั้งจากข้อมติคณะมนตรีความมั่นคงที่ 1386 ปี 2001 อดีตทหารของหน่วยสืบราชการลับและการข่าวกรองของประเทศสหรัฐอเมริกาได้รวบรวมข้อมูลที่สำคัญต่อการปฏิบัติการทางทหาร แต่นายทหารผู้นี้มีได้ถูกอนุญาตให้แบ่งปันข้อมูลดังกล่าวให้กับกลุ่มประเทศชาติพันธมิตร ในเครื่องกองกำลังร่วมของรัฐสมาชิก NATO แม้ว่ากลุ่มชาติพันธมิตรเหล่านั้นได้รับมอบหมายภารกิจที่มีความเสี่ยง⁷⁷ เช่นกัน ภายหลังจากหนึ่งในทหารของกลุ่มชาติพันธมิตรได้โต้แย้งว่าการกระทำของสหรัฐไร้ซึ่งศีลธรรมและละเมิดต่อสิทธิในการได้รับทราบข้อมูลที่มีความจำเป็นต่อการปฏิบัติการ

ดังนั้นข้อมูลลักษณะนี้จึงจะเป็นข้อมูลที่สำคัญและเป็นประโยชน์โดยเฉพาะ ต่อการปฏิบัติการนั้นๆ และต่อสถานการณ์นั้นๆ ข้อมูลจะเกี่ยวข้องต่อการดำเนินมาตรการความปลอดภัยของผู้ปฏิบัติงาน และการรับรู้และประเมินภารกิจในกรณีของผู้ปฏิบัติงานอยู่ที่พื้นที่ห่างไกลจากกัน และ

⁷³ “In undertaking efforts to intensify and accelerate the timely exchange of relevant operational information and financial intelligence regarding actions or movements, and patterns of movements, of terrorists or terrorist networks, including FTFs, in accordance with domestic and international law”

⁷⁴ Joseph Soeters, "Information Sharing in Military and Security Operations," in *Information Sharing in Military Operations*, ed. ed. Anthony J. (Cham: Springer Nature, 2017).

⁷⁵ Ibid p.6, (See Joseph Soeters)

⁷⁶ Sharon Otterman, NATO: Keeping the Peace in Afghanistan, (2005) Retrieved from <https://www.cfr.org/backgrounder/nato-keeping-peace-afghanistan>

⁷⁷ Ibid p.7, (See Joseph Soeters)

การแบ่งปันข้อมูลในลักษณะนี้โดยทั่วไปจะทำการแบ่งปันเฉพาะผู้มีส่วนเกี่ยวข้องในภารกิจโดยแท้จึงถูกจำกัดอยู่ในวงที่แคบ

4. ข้อมูลที่มีส่วนเกี่ยวข้องอื่น (Relevant Information)

โดยทั่วไปแล้วข้อมูลประเภทนี้ถูกกล่าวถึงและมักปรากฏในข้อมติของคณะมนตรีความมั่นคงอยู่เป็นเสมอ เพราะเป็นลักษณะของข้อมูลที่กว้างและไม่ได้เฉพาะเจาะจงต่อการใช้งานในภารกิจใดภารกิจเดียว ซึ่งข้อมติในการต่อต้านการก่อการร้ายของคณะมนตรีที่ถูกรับรองให้มีการแบ่งปันข้อมูลในลักษณะนี้ สามารถพบเห็นได้โดยทั่วไป⁷⁸ ในกรณีของ “การกำหนดรายชื่อบุคคล” (Listing) ที่มีส่วนเกี่ยวข้องกับกลุ่มก่อการร้าย Al-Qaida ในข้อมติที่ 1267 ปี 1999⁷⁹ มีการกำหนดว่ารัฐสหประชาชาติจะต้องให้ข้อมูล (Supply relevant information) ซึ่งเป็นข้อมูลทั่วไปของบุคคล ที่อาจเป็นประโยชน์ต่อการ⁸⁰ “การกำหนดรายชื่อบุคคล” (Listing) ให้แก่คณะกรรมการลงโทษ (The Al-Qaeda sanctions committee) แต่เมื่อพิจารณาเพื่อให้เห็นความชัดเจนมากขึ้นแล้วใน ข้อมติที่ 2396 ปี 2017⁸¹ ได้กำหนดว่าข้อมูลที่มีส่วนเกี่ยวข้องอื่น (Relevant Information) เป็นข้อมูลที่จะต้องถูกแบ่งปันระหว่างหน่วยงานที่มีอำนาจแห่งชาติ เช่น หน่วยงานบังคับใช้กฎหมาย ฝ่ายตุลาการ เจ้าหน้าที่รักษาความปลอดภัยชายแดน ซึ่งสามารถใช้ประโยชน์จากการแบ่งปันข้อมูลในลักษณะดังกล่าวนี้อย่างเป็นระบบ และข้อมูลในลักษณะเหล่านี้ถือเป็นทรัพยากรที่มีความจำเป็นต่อการสืบสวนสอบสวน การดำเนินการฟ้องร้องคดี รวมไปถึงการคัดกรองบุคคลที่จุดตรวจคนเข้าเมือง⁸² ข้อมูลในลักษณะนี้จึงเป็นข้อมูลใดก็ได้ที่สามารถนำไปใช้ต่อการดำเนินการสอบสวน หรือการดำเนินการในทางข่าวกรอง เพื่อติดตาม ป้องกัน สอบสวน อาชญากรรมหรือกิจกรรมทางอาชญากรรม (Criminal activity)⁸³

⁷⁸ “The relevant UNSC resolutions, in particular 1267 (1999), 1373 (2001), 1624 (2005), 2322 (2016) and 2396 (2017)”

⁷⁹ United Nations Security Council Resolution 1267/1999, pp. 9

⁸⁰ Niamh Kinchin, "According to Law in the context of the UNSC's Targeted sanctions, in Administrative Justice in the UN: Procedural Protections, Gaps and Proposals for Reform," (Elgar Publishing: 2018).

⁸¹ United Nations Security Council Resolution 2396/2017, pp. preamble

⁸² “Information should be shared among national agencies, such that law enforcement, judicial and border security officers can proactively and systematically use that information as a resource, where appropriate and necessary, for investigations, prosecutions and screening at points of entry”

⁸³ John A. E. Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?," (2005), <https://www.utrechtlawreview.org/articles/10.18352/ulr.1>

ดังนั้นลักษณะของข้อมูลนี้เป็นข้อมูลโดยทั่วไปอย่างกว้าง แต่สามารถนำมาเพื่อเป็นประโยชน์ในทางใดทางหนึ่งของวัตถุประสงค์ของภารกิจ ผู้มีส่วนเกี่ยวข้อง ในการใช้ข้อมูลมีอยู่เป็นจำนวนมาก ขึ้นอยู่กับว่าจะนำข้อมูลไปใช้ในวัตถุประสงค์ของตนอย่างไร ข้อสังเกตจากผู้เขียนเห็นว่าข้อมูลลักษณะนี้เป็นข้อมูลดิบที่เกิดขึ้นโดยทั่วไป แต่อยู่ที่ผู้ใช้ประโยชน์เองได้เล็งเห็นผลว่าจะนำข้อมูลชุดนั้นมาทำให้เกิดประโยชน์ต่อการดำเนินงานของตนอย่างไรในลักษณะและรูปแบบใดต่างหาก ซึ่งการต่อต้านการก่อการร้ายมีความจำเป็นอย่างมากที่จะต้องอาศัยชุดข้อมูลในลักษณะนี้ เพื่อทำการแบ่งปันระหว่างผู้มีส่วนเกี่ยวข้อง เพราะพัฒนาการของเทคโนโลยีและกลุ่มก่อการร้ายเอง ก่อให้เกิดความยากในการปฏิบัติการทางข้อมูล โดยเฉพาะปัจจัยที่สำคัญในการเก็บข้อมูลจึงต้องอาศัยข้อมูลที่มีอยู่โดยทั่วไป แต่สามารถนำมาใช้ให้เกิดประโยชน์ซึ่งจะต้องอาศัยการวิเคราะห์ที่แม่นยำ และฐานข้อมูลขนาดใหญ่ในการช่วยเหลือซึ่งจะได้เขียนอธิบายในบทถัดไป

2.3 บริบทการแบ่งปันข้อมูลภายใต้กรอบการต่อต้านก่อการร้ายของคณะมนตรีความ

มั่นคง

เมื่อคณะมนตรีความมั่นคงได้รับรองข้อมติตามหมวดที่ 7 ในการกำหนดว่าการก่อการร้ายถือเป็นภัยคุกคามต่อสันติภาพและความมั่นคง สหประชาชาติจึงจำเป็นต้องมีมาตรการเพื่อต่อต้านการก่อการร้ายที่มีแนวโน้มจะเกิดเพิ่มมากขึ้น หากแต่ว่าวิธีการต่อต้านการก่อการร้ายจะสำเร็จได้อย่างรวดเร็วและมีประสิทธิภาพมิได้ ถ้ารัฐมิให้ความร่วมมือระหว่างกัน และยังคงเห็นปัญหาการก่อการร้ายเป็นของประเทศใดเป็นหนึ่ง ดังเช่นความร่วมมือในการแบ่งปันข้อมูลระหว่างกันเพื่อต่อต้านการก่อการร้ายนั้นมีความสำคัญมากต่อรัฐบางรัฐที่ได้มีข้อมูลเกี่ยวกับกลุ่มก่อการร้ายเลย ดังนั้นประโยชน์ของการได้รับรู้และทราบความถึงความเสี่ยง หรือการเตรียมการของกลุ่มก่อการร้าย จะทำให้รัฐนั้นจะสามารถดำเนินการปราบปรามได้อย่างทันท่วงที⁸⁴ ซึ่งหนึ่งในหนทางการแก้ไขปัญหาการก่อการร้ายของคณะมนตรีคือการให้รัฐร่วมมือกันในการแบ่งปันข้อมูลเกี่ยวกับการก่อการร้าย ยิ่งรัฐร่วมมือแบ่งปันข้อมูลกันมากเพียงใด ประสิทธิภาพที่ยุติการระบาดของกลุ่มก่อการร้ายก็ยิ่งเร็วเท่านั้น

บริบทของการแบ่งปันข้อมูลภายใต้มาตรการของการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคง นั้นไม่ได้มีความแตกต่างกันมากนัก รวมถึงระดับของการแบ่งปันข้อมูลไม่ได้ถูกแบ่งแยกไว้อย่างชัดเจน ส่วนใหญ่จะให้น้ำหนักไปที่การนำข้อมูลที่ได้ไปเสริมหรือช่วยมาตรการบังคับให้เกิดประสิทธิภาพในการดำเนินการ หัวนี้จะอธิบายถึงลักษณะของประเภทข้อมูลในการแบ่งปันและพัฒนาการของมาตรการการแบ่งปันข้อมูลตั้งแต่อดีตจนถึงปัจจุบัน

⁸⁴ General Assembly, "Calling for Strong Coordinated Action by Member States to Tackle Terrorism, Violent Extremism Worldwide" (2018) Retrieved from <https://www.un.org/press/en/2018/ga12035.doc.htm>

2.3.2 ประโยชน์และความจำเป็นของการแบ่งปันข้อมูลภายใต้กลไกบังคับ

คณะมนตรีความมั่นคงมีบทบาทสำคัญในดำเนินมาตรการบังคับเพื่อการต่อต้านการก่อการร้ายโดยอาศัยความร่วมมือระหว่างบรรดารัฐต่างๆ ภายใต้กรอบของหลักความมั่นคงร่วม (Collective security) ในการเอาชนะการก่อการร้าย โดยความจำเป็นนั้นคือการที่รัฐจะต้องอาศัยบทบาททั้งของกระแสนงาน และการร่วมมือกันในการต่อต้านการก่อการร้ายโดยที่รัฐใดรัฐหนึ่งจะกระทำเพียงลำพังมิได้

นำมาสู่ความสำคัญและประโยชน์ของของมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ ที่โดยอาศัยทั้งบทบาทของการประสานงานและบทบาทความร่วมมือระหว่างรัฐเพื่อส่งเสริมมาตรการต่อต้านการก่อการร้ายต่างๆ ที่ถูกกำหนดโดยคณะมนตรีความมั่นคงสามารถดำเนินเพื่อให้เกิดผลลุล่วงได้เป็นอย่างดี อาทิ การแบ่งปันข้อมูลที่สำคัญและพยานหลักฐานของการก่อการร้ายเพื่อดำเนินมาตรการทางกระบวนการยุติธรรม การแบ่งปันข้อมูลเพื่ออายัดทรัพย์สินของการก่อการร้าย หรือการแบ่งปันข้อมูลการเดินทางของบุคคลเพื่อตรวจจับการเดินทางของผู้ก่อการร้ายซึ่งผู้เขียนจะได้อธิบายให้เห็นภาพอย่างละเอียดในบทต่อ ทั้งนี้ ความจำเป็นของการดำเนินมาตรการการแบ่งปันข้อมูลภายใต้กลไกบังคับของคณะมนตรีความมั่นคงสหประชาชาติเมื่อพิจารณาทั้งในแง่ของฐานทางกฎหมายและการบังคับใช้แล้วจะพบว่ามีความจำเป็นใน 3 แง่มุมคือ

1. ความจำเป็นในด้านเนื้อหา

มาตรการแบ่งปันข้อมูลภายใต้กลไกบังคับตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงมีเนื้อหาที่ครอบคลุมชัดเจนกว่าที่ถูกกำหนดในตราสารระหว่างประเทศ เพราะมาตรการแบ่งปันข้อมูลนั้นถูกกำหนดออกมาจากเหล่าบรรดาข้อมติของคณะมนตรีความมั่นคงว่าด้วยการต่อต้านการก่อการร้ายทั้งหลาย ที่เปรียบเสมือนกับเป็นอนุสัญญาว่าด้วยการต่อต้านการก่อการร้ายที่ครอบคลุม (Comprehensive convention on terrorism)⁸⁵ และเป็นระบบกลไกที่กำหนดกฎหมายต่อต้านการก่อการร้ายในระดับโลก (Legalized global anti terrorism system) ดังนั้นสารบัญญัติเนื้อหาของข้อมูลในการต่อต้านการก่อการร้ายมีความกว้างพอและเป็นส่วนในการปิดช่องว่างของบทบัญญัติตามตราสารระหว่างประเทศ

⁸⁵ Hans Koechler, "The United Nations and International Terrorism: Challenges to Collective Security", (Shanghai, 15 November 2002), p. 1

2. ความจำเป็นในด้านกระบวนการ

มาตรการแบ่งปันข้อมูลภายใต้กลไกบังคับตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงมีการกำหนดกระบวนการที่ชัดเจนว่ารัฐมีหน้าที่และความรับผิดชอบในการแบ่งปันข้อมูลอะไรบ้าง ในบางข้อมติได้กำหนดว่าหน่วยงานใดระดับภายในรัฐจะมีหน้าที่และความรับผิดชอบในการเป็นจุดติดต่อ ในการให้การกระแสนงาน หรือความร่วมมือต่อการแบ่งปันข้อมูลเพื่อดำเนินการต่อต้านการก่อการร้าย ทั้งในรูปแบบความช่วยเหลือซึ่งกันและกันหรือความร่วมมือด้านการตรวจคนเข้าเมือง หน่วยงานใดเป็นหน้าที่ในการรวบรวมข้อมูล กล่าวคือข้อมติคณะมนตรีมีการกำหนดกระบวนการที่ชัดเจนกว่า ในบางกรณีข้อมติเองจะแนะนำคู่มือปฏิบัติ (Practical guide) หรือมาตรฐานสากล (International standard) แก่รัฐให้ดำเนินการตามกระบวนการ ซึ่งคู่มือปฏิบัติหรือมาตรฐานเหล่านั้นถูกพัฒนาจากหน่วยงานที่ทำงานภายใต้สหประชาชาติเอง รวมทั้งแหล่งองค์การระหว่างประเทศอื่นที่เกี่ยวข้องต่อการปราบปรามการก่อการร้าย

3. ความจำเป็นในด้านการบังคับ

มาตรการแบ่งปันข้อมูลภายใต้กลไกบังคับตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงมีลักษณะเป็นพันธกรณีที่กำหนดให้รัฐจะต้องดำเนินการตาม และเป็นพันธกรณีที่มีความเหนือกว่า (Prevail) ตามข้อที่ 103 ของกฎบัตรสหประชาชาติ และอยู่เหนือกว่าพันธกรณีตามบรรดาตราสารระหว่างประเทศอื่นๆ ซึ่งลักษณะดังกล่าวนี้สะท้อนให้ว่ากลไกการบังคับในการแบ่งปันข้อมูลต่อการต่อต้านการก่อการร้ายนั้นมีประสิทธิภาพในการปราบปรามได้เร็วกว่ากลไกตามตราสารระหว่างประเทศ ตัวอย่าง ในกรณีที่คณะมนตรีความมั่นคงมีมาตรการบังคับให้ประเทศอิรักชี้แจงข้อมูลของการพัฒนาอาวุธที่มีอำนาจทำลายล้างสูง แม้ว่าประเทศอิรักจะมีพันธกรณีอยู่แล้วตามพิธีสารเพื่อกำกับการใช้ ผลิต และครอบครองอาวุธที่มีพลังทำลายล้างสูงอย่างอาวุธชีวภาพในสงคราม ค.ศ. 1925⁸⁶

2.3.3 พัฒนาการของมาตรการการแบ่งปันข้อมูล

ในระยะเวลาของการดำเนินการกำหนดบทลงโทษต่อต่อต้านการก่อการร้ายภายใต้กลไกการบังคับของคณะมนตรีความมั่นคง พัฒนาการของมาตรการการแบ่งปันข้อมูลตั้งแต่อดีตถึงปัจจุบัน (3 ทศวรรษที่ผ่านมา 1990-2020) นั้นสามารถพิจารณาและแจกแจงรูปแบบของการแบ่งปันข้อมูลออกมาอยู่ใน 3 รูปแบบ คือ

⁸⁶ Matthew Happold, "Security Council Resolution 1373 and the Constitution of the United Nations," in *Current legal developments - Leiden Journal of International Law* (under the Foundation of the Leiden Journal of International Law, 2003).

1.) การแบ่งปันข้อมูลในรูปแบบการให้ข้อมูลระหว่างหน่วยงานของรัฐกับคณะกรรมการ
ลงโทษตามข้อมติคณะมนตรีความมั่นคง

2.) การแบ่งปันข้อมูลในรูปแบบการมีกลไกการประสานงานระหว่างองค์กรของรัฐ หรือ
ระหว่างคณะกรรมการกำหนดบทลงโทษ (Coordination mechanism for counter terrorism
activities)

3.) การแบ่งปันข้อมูลในรูปแบบความตกลงระหว่างประเทศ (Cooperating on
international agreements) ทั้งนี้การพิจารณาของผู้เขียนเองเห็นว่าควรจะต้องทำความเข้าใจในขั้น
แรกเสียก่อนว่าในข้อมตินั้นๆ รัฐมีหน้าที่ที่จะต้องแบ่งปันข้อมูลในรูปแบบลักษณะใด เพื่อส่งผลต่อ
ประสิทธิภาพของดำเนินมาตรการว่าด้วยการต่อต้านการก่อการร้าย

ซึ่งในส่วนนี้ผู้เขียนจะอธิบายถึงพัฒนาการของมาตรการตามบริบทเหตุการณ์ก่อการร้าย
ระหว่างประเทศที่สำคัญ เพื่อชี้ให้เห็นถึงพัฒนาการของการสร้างกระบวนการและกลไกการแบ่งปัน
ข้อมูลคณะมนตรีความมั่นคงก่อนจะนำเข้าสู่บทที่ 3 ในส่วนของมาตรการการแบ่งปันข้อมูล

2.3.3.1 บริบทการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายหลังสงครามเย็น

หลังสงครามเย็นจบลงปีคริสต์ศักราช 1991 บริบทการทำหน้าที่รักษาสันติภาพและความ
มั่นคงระหว่างประเทศที่เกี่ยวข้องกับภัยการก่อการร้ายของคณะมนตรีความมั่นคงได้มีบทบาทในการ
ตอบโต้การกระทำที่เกี่ยวข้องต่อการก่อการร้ายในหลายๆเหตุการณ์ในอดีตที่ผ่านมาอย่างแตกต่างกัน
ซึ่งเหตุการณ์เหล่านั้นจำเป็นที่จะต้องถูกวินิจฉัยตามหมวดที่เจ็ดของกฎบัตรสหประชาชาติว่าคือนี่คือ
เหตุการณ์ของการคุกคามต่อสันติภาพ ซึ่งจะกระตุ้นต่อกลไกของการใช้อำนาจตามหมวดที่เจ็ดของ
คณะมนตรีความมั่นคงในการดำเนินมาตรการกำหนดบทลงโทษ

ตัวอย่างเช่น 1. เหตุการณ์ก่อการร้ายตามข้อมติที่ 748/1992 ที่ตอบโต้ว่าการกระทำของ
ประเทศลิเบียที่ได้ล้มเหลวในการต่อต้านการก่อการร้าย และปฏิบัติเสฐที่จะปฏิบัติตามข้อมติที่
731/1992 ที่เรียกร้องให้รัฐบาลประเทศลิเบียจำนนต่อความรับผิดชอบของเหตุการณ์ Pan Am
Flight 103 (Lockerbie Bombing) จากการกระทำของผู้ก่อการร้ายชาวลิเบีย⁸⁷

⁸⁷ ศูนย์ข้อมูลและข่าวสืบสวนเพื่อสิทธิพลเมือง Thai Civil Rights and Investigative Journalism (TCIJ), "10
อุบัติเหตุทางการบินที่ทั่วโลกจดจำ - Pan Am Flight 103 (Lockerbie Bombing)" (มีนาคม, 2557), Retrieved
from <https://www.tcijthai.com/news/2014/03/watch/3986>

2. เหตุการณ์ก่อการร้ายตามข้อมติที่ 1044/1996 เรียกร้องให้รัฐบาลชูดานปฏิบัติตามคำขอขององค์การเอกภาพแห่งแอฟริกา (Organization of African Unity - OAU) ต่อกรณีการพยายามลอบสังหารประธานาธิบดี Hosni Mubarak แห่งอียิปต์⁸⁸

3. เหตุการณ์การวางระเบิดที่สถานทูตอเมริกาในประเทศเคนยาและประเทศแทนซาเนียตามข้อมติที่ 1214/1998 ข้อมติที่ 1267/1999 (Sanctions listing regime) ข้อมติที่ 1333/2000 และข้อมติที่ 1363/2001 ในการตอบโต้และลงโทษกลุ่ม Al-Qaeda ที่นำโดยนาย Osama bin Laden⁸⁹

ในแต่ละกรณีดังที่ได้กล่าวมาข้างต้นเป็นเหตุการณ์ที่ถูกสะท้อนถึงบริบทการใช้อำนาจของคณะมนตรีความมั่นคงที่เจ็ดในการรักษาหรือสถาปนากลับคืนซึ่งสันติภาพ และเป็นสิ่งที่สังเกตว่าการโต้ตอบการกระทำการก่อการร้ายเหล่านั้น เป็นไปเพียงเพื่อตอบโต้เหตุการณ์เฉพาะ (Respond to a particular situation) เท่านั้นหาได้ครอบคลุมไปทุกๆ เหตุการณ์ที่เกี่ยวข้องต่อการก่อการร้ายไม่

1. การสร้างกระบวนการ

การสร้างกระบวนการภายใต้การทำงานของคณะกรรมการกำหนดบทลงโทษกลุ่มจัดตั้งรัฐอิสลามและกลุ่มแอลไคดา (ISIL (Da'esh) & Al-Qaida Sanctions Committee) คณะมนตรีความมั่นคงแห่งสหประชาชาติได้มีข้อมติที่กล่าวถึงการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายในนัยยะเริ่มต้นคือ ข้อมติที่ 1267/1999 หรือเพียงแค่ 2 ปีก่อนเหตุการณ์วินาศกรรม 9/11 ข้อมติได้มุ่งเน้นมาตรการลงโทษ ไปที่สถานการณ์ของประเทศอัฟกานิสถาน กำหนดให้นายอุซามะห์บินลาดีน และผู้ร่วมกระบวนการของเขาให้มีสถานะเป็นผู้ก่อการร้าย⁹⁰ และจัดตั้งระบอบการลงโทษ (Sanction regime) ต่อประเทศ องค์กร หน่วยงาน และบุคคลที่มีส่วนเกี่ยวข้องกับการสนับสนุนการก่อการร้าย ซึ่งในข้อ 9 ของข้อมติคณะมนตรีความมั่นคงได้มีการเรียกร้องให้ทุกรัฐ (Calls upon all States) ให้การร่วมมือในการมอบข้อมูล กับคณะกรรมการกำหนดบทลงโทษกลุ่มจัดตั้งรัฐอิสลามและกลุ่มแอลไคดา (ISIL (Da'esh) & Al-Qaida Sanctions Committee) ที่ถูกจัดตั้งตามข้อมตินี้ด้วย

⁸⁸ Los Angeles Times, "Egypt's Leader Survives Assassination Attempt : Africa: Muslim extremists suspected in attack on Mubarak's motorcade in Ethiopia" (JUNE 27, 1995), Retrieved from <https://www.latimes.com/archives/la-xpm-1995-06-27-mn-17703-story.html>

⁸⁹ CNN Editorial Research, "1998 US Embassies in Africa Bombings Fast Facts" (2020), Retrieved from <https://edition.cnn.com/2013/10/06/world/africa/africa-embassy-bombings-fast-facts/index.html>

⁹⁰ United Nations Security Council, "Demands that Taliban turn over Osama Bin Laden to appropriate authorities" (1999) Retrieved from <https://www.un.org/press/en/1999/19991015.sc6739.doc.html>

การจัดหาข้อมูลที่เกี่ยวข้องต่อกลุ่มก่อการร้ายและผู้ก่อการร้ายแก่คณะกรรมการ⁹¹ เมื่อพิจารณาจะพบว่าการแบ่งปันข้อมูลในนัยยะช่วงแรกของมาตรการต่อต้านการก่อการร้ายนั้น เป็นเพียงการแบ่งปันข้อมูลระหว่างรัฐกับคณะกรรมการความมั่นคงเพียงเท่านั้นเท่านั้น

2. การสร้างกลไก

การสร้างกลไกภายใต้การทำงานของคณะกรรมการกำหนดบทลงโทษกลุ่มจัดตั้งรัฐอิสลามและกลุ่มแอลเคดา คณะกรรมการกำหนดบทลงโทษกลุ่มจัดตั้งรัฐอิสลามและกลุ่มแอลเคดามีหน้าที่หลักคือการพัฒนารายชื่อบุคคลหรือกลุ่มบุคคลที่จะต้องถูกลงโทษ กล่าวคือคณะกรรมการจะกำหนดกระบวนการให้รัฐมอบข้อมูลที่สำคัญเพื่อการนำไปวิเคราะห์ หรือช่วยในการเสริมความมีเหตุผลในการดำเนินมาตรการลงโทษบุคคลหรือกลุ่มบุคคล ซึ่งการมีข้อมูลที่สำคัญจากรัฐ โดยเฉพาะรัฐซึ่งเป็นเจ้าของสัญชาติ หรือถิ่นที่อยู่ รวมทั้งรัฐที่มีอำนาจในการบังคับเอาซึ่งทรัพย์สิน ข้อมูลจากบรรดารัฐเหล่านี้ที่มอบให้แก่คณะกรรมการจะมีน้ำหนักและเหตุผลที่เพียงพอต่อการดำเนินมาตรการกำหนดรายชื่อบุคคลหรือกลุ่มบุคคลที่ถูกลงโทษได้อย่างมีประสิทธิภาพ และอยู่บนพื้นฐานของหลักการมีเหตุผล

2.3.3.2 บริบทการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายหลังเหตุการณ์วินาศกรรม

9/11

หลังจากเหตุการณ์ก่อวินาศกรรมวันที่ 11 กันยายน 2544 ได้มีการยืนยันอีกครั้งว่าภัยก่อการร้ายเป็นภัยคุกคามสันติภาพและความมั่นคงระหว่างประเทศ⁹² ดังซึ่งได้ปรากฏตามข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติ ข้อมติที่ 1368/2001 มีมติเป็นเอกฉันท์เมื่อวันที่ 12 กันยายน 2544 หลังจากที่สหประชาชาติแสดงความมุ่งมั่นที่จะต่อสู้กับภัยคุกคามต่อสันติภาพและความมั่นคงระหว่างประเทศซึ่งเกิดจากการก่อการร้าย และตระหนักถึงสิทธิของการป้องกันตัวเอง และการป้องกันตนเองส่วนรวมซึ่งจะออกอธิบายเป็น 5 ประเด็นดังต่อไปนี้

ประเด็นแรก จากเหตุการณ์ข้างต้นคณะมนตรีเรียกร้องให้ทุกประเทศร่วมมือกันนำผู้กระทำความผิด ผู้เตรียมการจัดการ และผู้สนับสนุนการโจมตี เข้าสู่กระบวนการยุติธรรม และผู้ที่รับผิดชอบในการสนับสนุนหรือปิดบังผู้กระทำความผิด รวมถึงผู้ให้ความช่วยเหลือและผู้สนับสนุนจะต้องรับผิดชอบประชาคมระหว่างประเทศถูกเรียกร้องให้เพิ่มความพยายามในการปราบปรามและป้องกันกิจกรรมของผู้ก่อการร้ายผ่านความร่วมมือและการดำเนินการเป็นภาคีอนุสัญญาที่เกี่ยวข้องกับต่อต้านการก่อ

⁹¹ United Nations Security Council Resolution 1267/1999, pp. 9

⁹² United Nations Security Council Resolution 1368/2001, preamble

การร้าย (ในปัจจุบันมี 19 ตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้าย)⁹³ และให้ความร่วมมือกับกลไกเดิมตามข้อมติคณะมนตรีความมั่นคงที่ 1269/1999 ที่ว่าด้วยการยึดและอายัดทรัพย์สินของผู้ก่อการร้าย และคณะมนตรีความมั่นคงแห่งสหประชาชาติแสดงความพร้อมที่จะดำเนินการเพื่อตอบสนองต่อการโจมตีและต่อสู้กับการก่อการร้ายทุกรูปแบบตามกฎหมายบัตรสหประชาชาติ

ประเด็นที่สอง ข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ 1373/2001 ซึ่งมีมติเป็นเอกฉันท์และถูกรับรองในวันที่ 28 กันยายน 2544 เป็นการออกมาตรการต่อต้านการก่อการร้ายของคณะมนตรีเป็นที่มีพันธกรณีต่อทุกรัฐในสังคมระหว่างประเทศหลังเหตุการณ์ที่เกิดขึ้นจากการโจมตีของผู้ก่อการร้าย 11 กันยายนในสหรัฐอเมริกา มติดังกล่าวได้รับการรับรองภายใต้หมวดที่ 7 ของกฎบัตรสหประชาชาติและมีผลผูกพันกับรัฐ จากการอธิบายที่กล่าวมาทั้งหมดนั้น สะท้อนให้เห็นว่าคณะมนตรีความมั่นคงแห่งสหประชาชาติ ได้ออกข้อมติที่มีวัตถุประสงค์เพื่อขัดขวางกลุ่มผู้ก่อการร้ายใน

⁹³ 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft
 1970 Convention for the Suppression of Unlawful Seizure of Aircraft
 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation
 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents
 1979 International Convention against the Taking of Hostages
 1980 Convention on the Physical Protection of Nuclear Material
 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation
 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf
 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection
 1997 International Convention for the Suppression of Terrorist Bombings
 1999 International Convention for the Suppression of the Financing of Terrorism
 2005 International Convention for the Suppression of Acts of Nuclear Terrorism
 2005 Amendment to the Convention on the Physical Protection of Nuclear Material
 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
 2005 Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf
 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation
 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft
 2014 Protocol to the Convention on Offences and Certain other Acts Committed on Board Aircraft

รูปแบบต่าง ๆ เกี่ยวกับการก่อการร้าย บรรดารัฐต่างๆได้รับการสนับสนุนให้แบ่งปันข้อมูลของพวกเขาที่เกี่ยวข้องกับกลุ่มผู้ก่อการร้าย เพื่อช่วยในการต่อสู้กับการก่อการร้ายระหว่างประเทศ ในรายละเอียดยังเรียกร้องให้ทุกรัฐทำการการปรับแก้กฎหมายภายในชาติของตนจากการระบุว่าทุกรัฐควรตรวจสอบให้แน่ใจว่าการกระทำของผู้ก่อการร้ายเป็นอาชญากรรมร้ายแรงในกฎหมาย⁹⁴ และระเบียบข้อบังคับของประเทศของตน

ประเด็นที่สาม ข้อมติที่ 1373/2001 ที่มีมาตรการลงโทษต่อการก่อการร้ายอย่างครอบคลุม⁹⁵ โดยสร้างพันธกรณีผูกพันบรรดารัฐต่างๆ ทั้งหมดให้ดำเนินการปฏิบัติตาม และได้ถือเป็นว่าแนวปฏิบัติใหม่ของคณะมนตรีในการต่อต้านการก่อการร้าย ซึ่งหากสังเกตในตัวข้อมตินี้มิได้ระบุถึงการเกิดขึ้นของเหตุการณ์ก่อการร้ายอย่างเฉพาะที่เป็นการคุกคามต่อสันติภาพดังที่คณะมนตรีความมั่นคงเคยระบุเหตุการณ์ก่อการร้ายอย่างเฉพาะเหล่านั้นในอดีตที่ผ่านมา เช่น การก่อการร้ายในการพยายามลักลอบสังหารบุคคลสำคัญของประเทศ การก่อการร้ายในการวางระเบิดสถานที่สำคัญ แต่ในข้อมตินี้ได้เป็นวิธีการเขียนอย่างครอบคลุมและทั่วไปว่าเป็นเหตุการณ์ของ “การกระทำการก่อการร้าย” ที่กลายเป็นการคุกคามต่อสันติภาพ มากไปกว่านั้นข้อมตินี้มีการบังคับใช้อย่างมีได้ระบุระยะเวลาอย่างแน่นอน⁹⁶ ซึ่งหมายความว่าพันธกรณีในการต่อต้านการก่อการร้ายของบรรดารัฐต่างๆตามข้อมตินี้เป็นพันธกรณีที่ผูกพันรัฐให้จะต้องดำเนินการต่อต้านไปเรื่อยๆ จนกว่า “การกระทำการก่อการร้าย” จะหมดไป หรือมีการรับข้อมติของคณะมนตรีในอนาคตถึงการระงับการบังคับใช้ข้อมตินี้

ประเด็นที่สี่ ในความล้มเหลวต่อการกำหนดค่านิยมของการก่อการร้ายของที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติ ข้อมติที่ 1373/2001 หลีกเลียงที่จะให้ค่านิยมของการก่อการร้ายอย่างชัดเจน แต่ข้อมติได้เน้นไปที่พันธกรณีของรัฐต่อการเพิ่มศักยภาพของรัฐบาลของรัฐในการดำเนินการมาตรการต่อต้านการก่อการร้ายที่เกิดขึ้นในสังคมนระหว่างประเทศ โดยพันธกรณีตามข้อมตินี้จะมุ่งเน้นไปที่การดำเนินการในสองแง่มุมคือ การอัปเดตกฎหมายภายในเพื่อรับรองฐานความผิดที่เกี่ยวข้องต่อการก่อการร้าย และเพิ่มประสิทธิภาพของกลไกการบังคับกฎหมาย⁹⁷ ในการต่อต้านการก่อการร้าย ซึ่งสะท้อนให้เห็นถึงแนวปฏิบัติใหม่ของคณะมนตรีความมั่นคงในการรับรองข้อมติที่มีผลผูกพันรัฐ เกิน

⁹⁴ Security Council, "Wide-ranging anti-terrorism resolution; calls for suppressing financing, improving international cooperation" (2001), Retrieved from <https://www.un.org/press/en/2001>

⁹⁵ Matthew Happold, "Security Council Resolution 1373 and the Constitution of the United Nations", In *Current legal developments - Leiden Journal of International Law Vol. 16*, (Published under the Foundation of the Leiden Journal of International Law, 2003), pp. 594

⁹⁶ Ibid, p. 607

⁹⁷ Eric Rosand, "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism," In *The American Journal of International Law* 97 No. 2 (Published by: Cambridge University Press, Apr ,2003).

กว่าพันธกรณีในการต่อต้านการก่อการร้ายตามอนุสัญญาต่อต้านการก่อการร้ายระหว่างประเทศต่างๆ ที่มีผลผูกพันเฉพาะรัฐที่เป็นภาคี

ประเด็นสุดท้าย ทั้งนี้ในข้อมติที่ 1373/2001 มิได้จำกัดมาตรการต่อต้านการก่อการร้ายในเรื่องหนึ่งๆ แบบที่อนุสัญญาว่าด้วยการต่อต้านการก่อการร้ายต่างๆ พยายามจัดเป็นประเภท เช่น เรื่องมาตรการทางการเงิน เรื่องมาตรการทางด้านความปลอดภัยในการดำเนินการทางอากาศ หรือเรื่องอาวุธอานุภาพร้ายแรง แต่ข้อมตินี้ได้มุ่งเน้นไปที่มาตรการสำคัญๆ ในหลายๆ เรื่อง⁹⁸ เช่น การดำเนินมาตรการทางการเงิน การแก้ไขกฎหมายเพื่อเอาผิดการก่อการร้าย การควบคุมและจัดการชายแดน การควบคุมการค้าอาวุธและการแพร่ขยายซึ่งอาวุธร้ายแรง การให้ความช่วยเหลือในการกฎหมาย การร่วมมือในการแบ่งปันข้อมูลระหว่างรัฐกับรัฐ และรัฐกับองค์ภาวะของคณะมนตรีความมั่นคง เช่น คณะกรรมการลงโทษ

1. กระบวนการที่เพิ่มเติม

กระบวนการที่ถูกเพิ่มเติมภายใต้การทำงานของคณะกรรมการต่อต้านการก่อการร้าย (The United Nations Security Council Counter-Terrorism Committee - CTC) ข้อมติที่ 1373/2001 ได้รับรองคณะกรรมการต่อต้านการก่อการร้าย เพื่อเฝ้าดูแลรัฐในริเริ่มการดำเนินการตามข้อมติ ซึ่งในคณะกรรมการจะประกอบไปด้วยสามคณะอนุกรรมการ ที่มีหน้าที่ในการทบทวนรายงานของการดำเนินการของรัฐ ประกอบทั้งกลุ่มผู้เชี่ยวชาญจากเลขาธิการสหประชาชาติที่จะคอยให้การช่วยเหลือและแนะนำการทบทวนรายงานจากรัฐ อย่างไรก็ตามนั้นข้อมติที่ 1373/2001 ไม่ได้ให้คำสั่งหรือบทบาทต่อคณะกรรมการในการมีส่วนร่วมต่อการต่อต้านการก่อการร้ายแต่อย่างใด⁹⁹ หนทางของการดำเนินการของคณะกรรมการจะเน้นไปที่การเป็นตัวกลางประสานการทำงานร่วมระหว่างคณะมนตรีความมั่นคงและรัฐต่างๆ ในการดำเนินมาตรการต่อต้านการก่อการร้าย และช่วยเหลือคำแนะนำต่อองค์การระหว่างประเทศอื่นๆ อาทิ องค์การระหว่างภูมิภาค องค์การระหว่างในระดับอนุภูมิภาค

ภาระหน้าที่ของคณะกรรมการต่อต้านการก่อการร้ายจะแตกต่างจากคณะกรรมการลงโทษ อื่นๆ ที่โดยส่วนใหญ่แล้วจะมีหน้าที่ร้องเรียนและกล่าวโทษ รัฐที่มีได้ปฏิบัติตามข้อมติ แต่จะมี

⁹⁸ The Counter-Terrorism Committee, "Global survey of the implementation of Security Council resolution 1373 (2001) by Member States" (January, 2016), p. 7, Available from https://www.un.org/sc/ctc/wp-content/uploads/2016/10/Global-Implementation-Survey-1373_EN.pdf

⁹⁹ Eric Rosand, "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism", In *The American Journal of International Law* 97, No. 2, (Published by: Cambridge University Press, Apr ,2003), p. 335

หน้าที่คอยช่วยเหลือและประสานการทำงานร่วมกับรัฐในการดำเนินการให้บรรลุเป้าหมายตามข้อมติที่ 1373/2001 อย่างรวดเร็วที่สุด และหลีกเลี่ยงการกระทำที่จะทำให้รัฐเกิดความรู้สึกถึงการคุกคามโดยข้อมติ¹⁰⁰ อาทิ ไม่ได้เจาะจงไปที่รัฐใดรัฐหนึ่งให้ปฏิบัติเป็นพิเศษ ไม่มีการกล่าวโทษรัฐ และเน้นไปที่การช่วยเหลือทางเทคนิคต่อการดำเนินการตามข้อมติ โดยในขั้นตอนแรกรัฐจะต้องจัดทำรายงานในการดำเนินการตามข้อมติของตนให้แก่คณะกรรมการการต่อต้านการก่อการร้าย จากนั้นเมื่อคณะกรรมการการต่อต้านการก่อการร้ายได้รับรายงานจากรัฐแล้วจะเข้าสู่กระบวนการของการทบทวนรายงาน เพื่อประเมินว่ารัฐที่ได้รายงานมานั้นมีความสามารถอยู่ในขั้นใด ของการดำเนินการตามข้อมติ และการจัดกลุ่มรัฐตามความสามารถของการดำเนินการตามข้อมติที่ได้รายงานมา



ดังนั้นในกระบวนการของทบทวนรายงานของคณะกรรมการการต่อต้านการก่อการร้ายได้มีการแบ่งแผนการประเมินความสามารถในการดำเนินการตามข้อมติ 1373/2001 ของรัฐออกด้วยกันอยู่ 3 ขั้นตอน คือ

- **Stage A:** คณะกรรมการการต่อต้านการก่อการร้ายจะประเมินถึงการออกกฎหมายของรัฐว่าได้ครอบคลุมทุกแง่มุม ของข้อมติหรือไม่ อาทิ การเข้าเป็นภาคีอนุสัญญาว่าด้วยการต่อต้านการก่อการร้ายต่างๆ และมีกฎหมายภายในที่ออกมาเพื่ออนุวัติการ
- **Stage B:** คณะกรรมการการต่อต้านการก่อการร้ายจะประเมินถึงการมีกลไกการบังคับกฎหมาย ของรัฐว่าได้ครอบคลุมทุกแง่มุม ของข้อมติหรือไม่ และมีกลไกการประสานงานที่มีประสิทธิภาพของรัฐบาล ในการต่อต้านการก่อการร้าย หรือการร่วมมือระหว่างประเทศของรัฐในระดับทวิภาคี ระดับพหุภาคี หรือภูมิภาคและอนุภูมิภาค อาทิ การร่วมมือเพื่อแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย

¹⁰⁰ The CTC provided guidance to member states regarding the content of such reports in a note from its chairman, "Guidance for the Submission of Reports Pursuant to Paragraph of Security Council Resolution 1373 (2001) of 28 September 2001, Available from <http://www.un.org/Docs/sc/committees/1373>

- **Stage C:** คณะกรรมาธิการการต่อต้านการก่อการร้ายจะประเมินถึงการออกกฎหมายหรือการมีกลไกการบังคับกฎหมาย ของรัฐในการนำผู้ก่อการร้ายหรือบุคคลผู้สนับสนุนการก่อการร้ายเข้าสู่กระบวนการยุติธรรม¹⁰¹

อย่างไรก็ตาม คณะกรรมาธิการการต่อต้านการก่อการร้ายมิได้มีหน้าที่ช่วยเหลือทางทรัพยากรต่อรัฐใดในการดำเนินการตามข้อมติ แต่จะให้ความใส่ใจในรัฐที่มีอุปสรรคในการดำเนินการ โดยเฉพาะ **Stage A** ถือว่าถูกจัดให้สำคัญที่สุด และหากรัฐต้องการความช่วยเหลือ คณะกรรมาธิการการต่อต้านการก่อการร้ายก็พร้อมที่จะให้ผู้เชี่ยวชาญให้คำแนะนำต่อการดำเนินการ ตรงข้ามกับรัฐที่ได้ออกกฎหมายอย่างเพียงพอ ครอบคลุมทุกแง่มุมของข้อมติแล้ว ดังนั้นสามารถสรุปได้ว่า คณะกรรมาธิการการต่อต้านการก่อการร้ายได้ใช้ “แนวทางที่ไม่เน้นการเผชิญหน้า (Non-confrontational approach)” ต่อรัฐในเฝ้ามองการดำเนินการตามข้อมติ¹⁰² แต่จะคอยช่วยเหลือและคำแนะนำแก่รัฐที่มีความบริสุทธิ์ใจที่จะดำเนินการตามข้อมติ แม้ว่าอาจจะไม่มีความสามารถในการดำเนินการตามข้อมติในครบทุกแง่มุม

2. กลไกที่เพิ่มเติม

กลไกที่ถูกเพิ่มเติมภายใต้การทำงานของคณะกรรมการการต่อต้านการก่อการร้าย (The United Nations Security Council Counter-Terrorism Committee - CTC)

2.1 กลไกการประเมินการดำเนินการออกกฎหมาย (Assessing the implementation of legislation)

คณะกรรมาธิการการต่อต้านการก่อการร้ายจะประเมินถึงการออกกฎหมายของรัฐโดยการทบทวนจากรายงานที่รัฐได้ส่งมา ว่ารัฐมีการดำเนินนโยบายภายในรัฐตนในการต่อต้านการก่อการร้ายไปในทิศทางใด และสอดคล้องกับข้อมติของคณะมนตรีความมั่นคงหรือไม่ ตาม **Stage A** ถือว่าถูกจัดให้สำคัญที่สุด รัฐจะต้องมีกฎหมายมาเพื่ออนุญาตให้การเข้าร่วมเป็นภาคีของอนุสัญญาว่าด้วยการต่อต้านการก่อการร้ายทั้งหลาย ซึ่งเป็นพันธกรณีตามข้อมติที่ 1373/2001 ผู้กพันให้รัฐต้องดำเนินการ

¹⁰¹ Eric Rosand, "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism", In *The American Journal of International Law* 97, No. 2, (Published by: Cambridge University Press, Apr, 2003), p. 336

¹⁰² "The Security Council did not explicitly grant the CTC the authority to make and report such determinations to the Council. This is in contrast with the 1267 Committee, which is authorized by Resolution 1267 to make periodic reports to the Council on information submitted to it regarding alleged violations of the resolution.", In Eric Rosand (2003).

เป็นภาคีต่ออนุสัญญาทั้งหลายอย่างไม่ร้อช้า มากไปกว่านั้นในระยะเวลาของการรับรองข้อมตินี้ขึ้นมา เกิดปัญหาเรื่องการใช้ประโยชน์จากพันธกรณีต่อต้านการก่อการร้ายจากข้อมติ คณะมนตรีความมั่นคงในการละเมิดซึ่งสิทธิมนุษยชนและหลักสิทธิขั้นพื้นฐาน¹⁰³ จากข้อเรียกร้องจากหน่วยงานระหว่างประเทศ อาทิ องค์การนิรโทษกรรมสากล (Amnesty international) คณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ (United Nations Human Rights Council) หรือสภายุโรป (The council of Europe) เรียกร้องและผลักดันเรื่องนี้ จนกระทั่งคณะกรรมการการต่อต้านการก่อการร้ายเองได้พัฒนาความก้าวหน้าของการดำเนินงาน ให้ครอบคลุมถึงการปกป้องกฎหมายของรัฐว่าด้วยการก่อการร้ายจนนำไปสู่การละเมิดซึ่งสิทธิมนุษยชนและหลักสิทธิขั้นพื้นฐาน¹⁰⁴ ทั้งยังคงหลักการที่จะไม่สูญเสียเป้าหมายของหน้าที่ในการช่วยเหลือรัฐในการดำเนินการออกกฎหมายเพื่อต่อต้านการก่อการร้าย

2.2 กลไกการประเมินการดำเนินการตามกลไกการบังคับใช้กฎหมาย (Assessing the implementation of executing machinery)

คณะกรรมการการต่อต้านการก่อการร้ายจะประเมินถึงการมีกลไกการบังคับใช้กฎหมาย ของรัฐจากการทบทวนรายงานที่รัฐได้มีประสิทธิภาพต่อการดำเนินการบังคับใช้กฎหมายว่าด้วยการต่อต้านการก่อการร้ายในรัฐของตนหรือไม่ ตาม **Stage B** และ **Stage C** ถึงแม้ว่าข้อมติที่ 1373/2001 จะมีได้ให้อำนาจหน้าที่ของคณะกรรมการการต่อต้านการก่อการร้ายสามารถเข้าไปเยี่ยมเยือน รัฐในการดำเนินการบังคับใช้กฎหมายอย่างชัดเจน ตรงข้ามกับความสามารถในการเยี่ยมเยือน รัฐของคณะกรรมการลงโทษตามข้อมติที่ 1540/2004 แต่คณะกรรมการการต่อต้านการก่อการร้ายอาจใช้ช่องว่างของข้อมติในการดำเนินการดังกล่าว¹⁰⁵ ประกอบทั้งคณะกรรมการการต่อต้านการก่อการร้ายต้องการประเมินสิ่งที่มีได้ในการรายงานของรัฐ เช่น ข้อมูลตามความเป็นจริงมากกว่าการประเมินจากข้อมูลตามการรายงาน ซึ่งเป็นที่น่ากังวลของบรรดารัฐถึงการเข้ามาแทรกแซงกิจการภายใน (Interference in the internal affairs of states) คณะกรรมการการในส่วนของการดำเนินการบังคับใช้กฎหมายของรัฐ

¹⁰³ Eric Rosand, "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism", In *The American Journal of International Law* 97, No. 2, (Published by: Cambridge University Press, Apr, 2003), p. 340

¹⁰⁴ Ibid, p. 341

¹⁰⁵ Ibid, p. 339

2.3.3.3 บริบทของเหตุการณ์อื่นที่เกี่ยวข้องกับการก่อการร้าย

1. การต่อต้านการแพร่อาวุธที่มีอานุภาพทำลายล้างสูง

หลังจากสงครามโลกครั้งที่สองจบลง อัตราจำนวนที่เพิ่มขึ้นของอาวุธอานุภาพทำลายล้างสูงนั้นส่งผลกระทบต่อความมั่นคงสันติภาพและหน้าที่ในการป้องกันไม่ให้เกิดสงครามของสหประชาชาติ แม้สมัชชาใหญ่แห่งสหประชาชาติได้รับรองข้อมติเกี่ยวกับการลดอาวุธอานุภาพทำลายล้างสูง¹⁰⁶ แต่ก็ยังคงมีบางประเทศที่ทำการพัฒนาอาวุธเพื่อคลานอำนาจของประเทศตนในเวทีโลก ประเทศที่มีรายงานว่ามี การแพร่ขยายของอาวุธอานุภาพทำลายล้างสูงจะอยู่ในภูมิภาคตะวันออกกลาง แอฟริกาเหนือ และเอเชียตะวันออกเฉียงใต้ โดยประเทศในภูมิภาคเหล่านี้ส่วนมากแล้วมิได้เป็นภาคีสมาชิกต่ออนุสัญญาไม่แพร่ขยายอาวุธอานุภาพทำลายล้างสูง ปัญหาในปัจจุบันคือกลุ่มการก่อการร้ายพยายามจะสรรหาอาวุธอานุภาพทำลายล้างสูงเพื่อการครอบครอง และกระทำการใช้อาวุธเคมี ชีวภาพ ซึ่งก่อให้เกิดความรุนแรงต่อชีวิตและทรัพย์สินของประชาชน¹⁰⁷ สร้างความเสียหายร้ายแรงต่อระบบเศรษฐกิจและสังคม โดยมีจุดประสงค์เพื่อบีบบังคับให้รัฐบาลเปลี่ยนแปลงนโยบายตามความประสงค์ของกลุ่มตน

การแบ่งปันข้อมูลภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติเพื่อการสกัดการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงจะมุ่งเน้นไปที่การจำกัดการแพร่ขยายของอาวุธ ในพื้นที่ความขัดแย้งเป็นหลัก ข้อมติที่ 1540/2004 ได้จัดตั้งคณะกรรมการที่ 1540¹⁰⁸ ซึ่งจะคอยช่วยเหลือรัฐในการดำเนินการตามมาตรการลงโทษ ต่อกลุ่มเครือข่ายก่อการร้ายการอัลดุลกาเดอร์ข่าน (Abdul Qadeer Khan) และในการป้องกันการเข้าซื้อ การครอบครอง และการพัฒนาอาวุธเคมี อาวุธชีวภาพ และอาวุธนิวเคลียร์ ต่อมาข้อมติที่ 2325/2016 ระบุให้ต้องทำการแบ่งปันข้อมูลภายใต้ความร่วมมือในระดับระหว่างประเทศ ระดับภูมิภาค และอนุภูมิภาค เกี่ยวกับการได้มาซึ่งอาวุธ การครอบครอง การพัฒนา การถ่ายโอน การขนส่งภายในพื้นที่ความขัดแย้ง และการข้ามชายแดนซึ่งต้องแบ่งปันข้อมูลโดยอาศัยความร่วมมือระหว่างประเทศโดยใช้ข้อมูลของหน่วยงานที่เกี่ยวข้องกับกิจการชายแดนระหว่างกัน¹⁰⁹ รวมถึงการแบ่งปันประสบการณ์ในทางปฏิบัติของรัฐต่อการควบคุม และจำกัดการ

¹⁰⁶ กรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ, "การลดอาวุธที่มีอานุภาพทำลายล้างสูง (2016)" Retrieved from http://www.mfa.go.th/thai_inter_org/th

¹⁰⁷ General Intelligence and Security Service (AIVD)(2003), "Proliferation of weapons of mass destruction Risks for companies and scientific institutions", Retrieved from <https://fas.org/irp/world/netherlands>

¹⁰⁸ United Nations Security Council Resolution 1540/2004, pp. 4

¹⁰⁹ United Nations Security Council Resolution 2325/2016, pp. 23

เข้าถึงระบบเทคโนโลยีและฐานข้อมูลอันเป็นองค์ความรู้ที่สามารถใช้ในการพัฒนาอาวุธอนุภาพทำลายร้ายสูง ที่กลุ่มก่อการร้ายพยายามที่จะเข้าถึงข้อมูลเหล่านี้โดนการแฮกระบบ

ในข้อมติที่ 2253/2015 เป็นข้อมติที่มุ่งเน้นใช้กับมาตรการลงโทษต่อกลุ่มอัลกออิดะห์ (Al Qaeda) และกลุ่มรัฐอิสลามในประเทศอิรัก โดยรัฐต้องแบ่งปันข้อมูลเกี่ยวกับการค้าอาวุธข้ามชาติชนิดอนุภาพทำลายร้ายสูง รวมไปถึงชนิดอื่น ๆ จำพวกอาวุธเล็ก อาวุธเบา ที่ใช้และถือครองอย่างผิดกฎหมายมิให้มีการถ่ายโอนถ่ายไปยังกลุ่มก่อการร้าย¹¹⁰ โดยอาศัยการแบ่งปันข้อมูลความเคลื่อนไหวของการเตรียมการของกลุ่มก่อการร้ายย่อย ๆ ที่อยู่ในบัญชีการเฝ้าระวังของรัฐบาลในพื้นที่ความขัดแย้ง รวมถึงนำข้อมูลที่เก็บได้แบ่งปันระหว่างองค์กรผู้บังคับใช้กฎหมาย ในออกดำเนินมาตรการป้องปราม หน่วยงานศุลกากรของรัฐควรเข้มงวดต่อการบริหารจัดการชายแดนของรัฐตน เมื่อมีข้อมูลซึ่งถูกรับรองและแบ่งปันมาจากรัฐอื่นให้มีการเฝ้าระวังการเดินทางข้ามชายแดนของบุคคลที่ทำหน้าที่จัดหาอาวุธสำหรับผู้ก่อการร้ายและดำเนินการนั้นภายใต้เขตอำนาจของตน¹¹¹ ทั้งรวบรวมข้อมูลของเอกชนที่ก่อตั้งกิจการในเขตอำนาจของตนในการจัดจำหน่ายวัตถุดิบและส่วนประกอบสำคัญที่สามารถใช้ในการผลิตระเบิดชั่วคราวหรืออาวุธที่ไม่ธรรมดา (Unconventional weapons) ที่อาจมีเกี่ยวข้องโยงโยกับกลุ่มก่อการร้ายที่ติดอาวุธ

คณะกรรมการลงโทษตามข้อมติที่ 1540/2004 (Security Council Committee established pursuant to resolution 1540/2004) มีหน้าที่ที่จะต้องทบทวนรายงานของบรรดารัฐในการดำเนินการป้องกันการแพร่ขยายของอาวุธที่มีอาวุธภาพทำลายร้ายสูง¹¹² อาทิ รัฐมีพันธกรณีที่จะต้องให้ข้อมูลต่อคณะกรรมการในเรื่องการดำเนินการออกกฎหมายควบคุมสินค้าหรือวัสดุที่สามารถใช้เพื่อพัฒนาอาวุธที่มีอนุภาพทำลายร้ายสูง รวมถึงข้อมูลของการกำหนดขั้นตอนการใช้ใบอนุญาตอุตสาหกรรมหรือธุรกิจที่เกี่ยวข้องต่อการใช้วัสดุจำพวก เคมี ชีวภาพ และสารกัมมันตรังสี ทั้งนี้ผู้เขียนจะแจกแจงพันธกรณีการแบ่งปันข้อมูลที่เกี่ยวข้องกับการป้องกันการแพร่ขยายของอาวุธที่มีอาวุธภาพทำลายร้ายสูงในบทที่สามต่อไป

2. องค์กรการก่อการร้าย

กิจกรรมของผู้ก่อการร้ายมิได้หลายวัตถุประสงค์ ซึ่งกลุ่มก่อการร้ายจะต้องดำเนินยุทธศาสตร์เพื่อให้บรรลุจุดหมายเพียงวัตถุประสงค์เดียวหรือหลายวัตถุประสงค์ก็ได้ และการแบ่งปันข้อมูลภายใต้ความร่วมมือระหว่างประเทศ จะเป็นวิธีการที่สำคัญเพื่อทราบถึงข้อมูลความเคลื่อนไหวของกลุ่มผู้ก่อการร้ายได้ก่อนล่วงหน้า และสามารถเพิ่มขีดการป้องกันการกระทำของผู้ก่อการร้าย หรือกลุ่ม

¹¹⁰ United Nations Security Council Resolution 2253/2015, preamble

¹¹¹ Ibid, pp. 26

¹¹² 1540 Committee Security Council Committee, "General Information", (2020), Retrieved from <https://www.un.org/en/sc/1540/about-1540-committee/general-information.shtml>

เหล่านั้นได้โดยตรงเช่น ข้อมูลในการเคลื่อนไหวของตัวแทนขององค์กรการก่อการร้าย ผ่านการพิจารณาจากเอกสารการเดินทาง ตัวเครื่องบิน หรือข้อมูลของหน่วยตรวจคนเข้าเมืองของประเทศนั้น เส้นทางการเงินและวัสดุอุปกรณ์ที่ถูกซื้อ รวมถึงความเคลื่อนไหวในเครือข่ายสังคมออนไลน์เพื่อประชาสัมพันธ์กิจกรรมขององค์กรเพื่อหาสมาชิกใหม่เข้าร่วมองค์กร หาแหล่งเงินทุนสนับสนุน หรือ สร้างคะแนนนิยมในหมู่กลุ่มชน¹¹³ และอีกวิธีหนึ่งที่กลุ่มผู้ก่อการร้ายใช้ ก็คือการดำเนินการทางการเมืองผ่านสื่อสิ่งพิมพ์ วิทยุ หรือโทรทัศน์

3. การเพิ่มจำนวนของนักรบต่างชาติ

ในช่วงปีที่ 2014 นักรบต่างชาติ (Foreign terrorist fighters) ได้ถูกกำหนดไว้ในข้อมติของคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ 2178/2014 ซึ่งกำหนดว่าพวกเขาเป็น “บุคคลที่เดินทางไปยังรัฐอื่นห่างจากที่อยู่อาศัย หรือประเทศตามสัญชาติของตน เพื่อความมุ่งประสงค์การวางแผนหรือการเตรียมการ หรือการมีส่วนร่วมในการกระทำของผู้ก่อการร้าย หรือการจัดหา หรือรับการฝึกอบรม ผู้ก่อการร้ายรวมถึงการเชื่อมต่อกับกลุ่มติดอาวุธ”¹¹⁴ ทำให้คณะมนตรีความมั่นคงเองได้ตระหนักถึงปัญหาดังกล่าว ซึ่งกลุ่มก่อการร้ายได้โน้มน้าวบุคคล ผ่านการประชาสัมพันธ์ ผ่านระบบอินเทอร์เน็ต เครือข่ายสังคมออนไลน์ต่าง ๆ เพื่อให้บุคคลตามกลุ่มที่อ่อนไหว (Sensitive group) ซึ่งมีทั้งเด็ก วัยรุ่น รวมถึงผู้หญิงที่อยู่อาศัยในต่างประเทศ¹¹⁵ ได้เดินทางเพื่อมาเข้าร่วมฝึกรบที่จะเป็นนักรบต่างชาติในอนาคต กับกลุ่มการก่อการร้าย ซึ่งคณะมนตรีความมั่นคงต้องการที่จะขอให้กลุ่มประเทศสมาชิกได้ทำการติดตาม

พวกเขาเหล่านั้นผ่านการแลกเปลี่ยนข้อมูลที่สำคัญบางอย่างแก่กัน เช่น ข้อมูลการเดินทางของบุคคลที่มีแนวโน้มเป็นเป้าหมายของการไปฝึกรบ เช่น กลุ่มวัยรุ่นในครอบครัวผู้อพยพที่ไม่สามารถกลืนตัวเองให้เข้ากับสภาพสังคมในประเทศที่เจริญแล้ว จะถูกชักชวนจากกลุ่มผู้ก่อการร้าย ข้อมูลการใช้เครือข่ายสังคมออนไลน์ต่าง ๆ ผ่านระบบอินเทอร์เน็ต เช่น สื่อสังคมออนไลน์เฟสบุ๊ก ทวิตเตอร์ ซึ่งมีรายงานถึงการหลั่งไหลของนักรบต่างชาติ มีแนวโน้มเพิ่มขึ้นจนสูงกว่าช่วงเวลาใดๆ ใน

¹¹³ สำนักข่าวห้องสมุดบ้านจอมยุทธ์, "ลักษณะขององค์กรการก่อการร้าย" (2013) Retrieved from

https://www.baanjomjyut.com/library/global_community/04_3.html

¹¹⁴ “Foreign terrorist fighters, namely individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict, and resolving to address this threat”

¹¹⁵ CTED, “Foreign terrorist fighters” (2014) Retrieved from https://www.un.org/sc/ctc/wp-content/uploads/2019/06/ctc_cted_fact_sheet_designed_ftfs_updated_15_november_2018.pdf

ประวัติศาสตร์ โดยนักรบต่างชาติที่เดินทางไปประเทศอิรักและประเทศซีเรีย ใช้ชีวิตและทำงานในโรงเรียนนานาชาติสำหรับพวกกลุ่มสุดโต่งทางศาสนา (Religion fundamentalists)¹¹⁶

เหตุการณ์นี้เคยเกิดขึ้นในสมัยสงครามอัฟกานิสถานช่วงปี 1990 มีการประเมินว่ามีนักรบต่างชาติราว 2.2 หมื่นคน¹¹⁷ และอีกหลายพันคนอยู่ในประเทศอัฟกานิสถาน ประเทศเยเมน ประเทศลิเบีย ประเทศปากีสถานและประเทศโซมาเลียโดยนักรบต่างชาติจำนวนมากมาจากประเทศตูนิเซีย ประเทศโมร็อกโก ประเทศฝรั่งเศสและประเทศรัสเซีย หรือแม้แต่ในประเทศอังกฤษเองก็ตาม ซึ่งคณะกรรมการความมั่นคงพยายามเรียกร้องให้ประเทศต่างๆ มีการร่วมมือกันระหว่างประเทศ เพื่อแบ่งปันข้อมูล และแลกเปลี่ยนข่าวกรองเพื่อช่วยระบุตัวนักรบเหล่านั้น

4. การปราบปรามการค้ามนุษย์ และการลักพาตัวเพื่อเรียกค่าไถ่

การค้ามนุษย์ในพื้นที่ที่ได้รับผลกระทบจากการขัดกันทางอาวุธมีอัตราเพิ่มจำนวนมากขึ้นในปัจจุบัน โดยกลุ่มก่อการร้ายใช้การค้ามนุษย์เพื่อหารายได้ และนำเหยื่อไปเป็นแรงงานทางเพศ (Sexual slavery) ความกังวลต่อกลุ่มก่อการร้ายรัฐอิสลาม (Islamic State) ใช้การบังคับเหยื่อผู้หญิงและเด็กชนกลุ่มน้อยทางศาสนาและชาติพันธุ์เช่น Yezidis แห่งอิรักเพื่อการค้ามนุษย์¹¹⁸ คณะมนตรีความมั่นคงแห่งสหประชาชาติได้ออกข้อมติที่ได้ประนามว่าการค้ามนุษย์ทำลายซึ่งหลักกฎหมาย และรัฐควรมีมาตรการในการต่อต้านขบวนการดังกล่าว

การแบ่งปันข้อมูลระหว่างองค์กรที่มีอำนาจของรัฐกับเอกชนผู้ให้บริการเครือข่ายระบบอินเทอร์เน็ตเกี่ยวกับกลุ่มเครือข่ายการค้ามนุษย์ที่ใช้ระบบการสื่อสารในทางที่ผิดวัตถุประสงค์เพื่ออำนวยความสะดวกต่อการค้ามนุษย์โดยเฉพาะอย่างยิ่งการขายและการค้า¹¹⁹ ข้อมติที่ 2331/2016 เรียกร้องให้รัฐสมาชิก (Calls on Member States to) ออกมาตรการทางกฎหมายเพื่ออำนวยความสะดวกแก่การเก็บข้อมูลและแบ่งปันข้อมูลระหว่างองค์กรภายในประเทศ โดยเน้นการแบ่งปันข้อมูลจากองค์กรสตรีในท้องถิ่นในการให้ข้อมูลเพื่อช่วยระบุ ถึงบุคคลและเครือข่ายที่เกี่ยวข้องกับขบวนการค้ามนุษย์ในพื้นที่ความขัดแย้ง สร้างความร่วมมือระหว่างประเทศในการแบ่งปันข้อมูลที่จำเป็นเพื่อใช้

¹¹⁶ “Religious fundamentalism refers to the belief of an individual or a group of individuals in the absolute authority of a sacred religious text or teachings of a particular religious leader prophet and God”

¹¹⁷ กรุงเทพธุรกิจ, "นักรบต่างชาติ 2.5 หมื่นร่วมรบกลุ่มสุดโต่ง" (2015) Retrieved from <https://www.bangkokbiznews.com/news/detail/642098>

¹¹⁸ Security Council, "Condemns Human Trafficking in Strongest Terms (2016)" Retrieved from <https://www.un.org/press/en/2016/sc12647.doc.htm>

¹¹⁹ United Nations Security Council Resolution 2331/2016, preamble

ในการบังคับทางกฎหมาย¹²⁰ ตรวจสอบข้อมูลเส้นทางการเงินของขบวนการค้ำมนุษย์ รวมถึงมีมาตรการร่วมกันในการปกป้องข้อมูลส่วนบุคคลของผู้ที่ตกเป็นเหยื่อไว้เป็นความลับ

ประเทศสมาชิกที่รับผู้ลี้ภัยเนื่องจากผลกระทบจากการขัดกันทางอาวุธควรจัดทำข้อมูลของเหยื่อการค้ามนุษย์ เหยื่อที่รอดชีวิตจากความรุนแรงทางเพศ เพื่อแบ่งปันกับรัฐสมาชิกหรือองค์การระหว่างประเทศ เช่น หน่วยงานของสหประชาชาติ Special Representative on Sexual Violence in Conflict and the Special Representative on Children in Armed Conflict¹²¹ มีวัตถุประสงค์ในด้านของการให้ความช่วยเหลือ ดูแลทางสังคมจิตใจ (Psychosocial support) และควรจัดทำเอกสารเกี่ยวกับกรณีความรุนแรงที่เกิดขึ้นเพื่อเป็นข้อมูลที่ใช้ดำเนินการออกมาตรการทางกฎหมายในอนาคต และตามข้อมติที่ 2388/2017 ได้สนับสนุนให้รัฐสมาชิกสร้างศักยภาพในการแลกเปลี่ยนข้อมูล เสริมสร้างเครือข่ายความร่วมมือในระดับภูมิภาค และระหว่างประเทศเกี่ยวกับการปราบปรามการค้ามนุษย์ และความรุนแรงทางเพศในพื้นที่ความขัดแย้งทางอาวุธ การติดตามและระบุตัวตนของบุคคลหรือกลุ่มการค้ามนุษย์ จัดทำข้อมูลบุคคลเพื่อขอออกเอกสารขอส่งตัวผู้ร้ายข้ามแดนภายใต้ความช่วยเหลือระหว่างประเทศในทางกฎหมาย อีกทั้งสนับสนุนให้รัฐสมาชิกร่วมมือในการการแบ่งปันข้อมูลกับ¹²² สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime) และหน่วยงานของสหประชาชาติ อาทิ สำนักงานข้าหลวงใหญ่ผู้ลี้ภัยแห่งสหประชาชาติ (Office of the United Nations High Commissioner for Refugees) องค์กรทุนเพื่อเด็กแห่งสหประชาชาติ (United Nations Children's Fund) และองค์การระหว่างประเทศอื่น ๆ ในระดับระหว่างประเทศหรือภูมิภาค อาทิ องค์กรตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL) และองค์การระหว่างประเทศเพื่อการโยกย้ายถิ่นฐาน (the International Organization for Migration)

ปัญหาที่ติดตามกันมาจากการค้ามนุษย์คือ ปัญหาการลักพาตัวเพื่อเรียกค่าไถ่ (Kidnapping for ransom) โดยกลุ่มก่อการร้ายเพื่อหวังเงินประกันตัวของรัฐที่เป็นเจ้าของสัญชาติของตัวประกันหรือแม้แต่ผู้นำในรัฐบาล หรือกลุ่มประชาชนผู้ต่อต้าน มีรายงานว่ากลุ่มก่อการร้าย Al Qaeda-affiliated และ Islamist extremist groups สามารถเก็บเงินค่าประกันตัวได้ถึง 105 ล้านดอลลาร์สหรัฐ¹²³ ซึ่งทำให้เกิดความกังวลต่อสถานการณ์นี้ว่าเป็นภัยคุกคามอีกชนิดหนึ่งต่อสันติภาพ โดยเฉพาะในบริเวณพื้นที่ความขัดแย้งอย่าง ประเทศแถบภูมิภาคแอฟริกาตะวันตก ประเทศเยเมน

¹²⁰ Ibid, pp. 6

¹²¹ Ibid, pp. 13

¹²² United Nations Security Council Resolution 2388/2017, pp. 58

¹²³ Security Council, “Urges cooperation to tackle kidnapping for ransom by terrorists” (2014) Retrieved from <https://news.un.org/en/story/2014/01/460552>

และประเทศซีเรีย¹²⁴ กลุ่มก่อการร้ายในพื้นที่เหล่านี้จะใช้เงินที่หาได้จากการลักพาตัวเพื่อเรียกค่าไถ่ในการเสริมความสามารถของกลุ่ม เพื่อซื้ออาวุธ เพื่อจัดเตรียมกำลังคนในการก่อการร้าย รวมไปถึงใช้เพื่อวางแผนและสร้างการโจมตีระลอกใหม่ หลังจากที่ถูกปราบปราม

คณะมนตรีความมั่นคงแห่งสหประชาชาติได้รับรองข้อมติที่ 2133/2014 ให้รัฐสมาชิกแบ่งปันข้อมูลเพื่อป้องกันกลุ่มก่อการร้ายไม่ให้ได้รับผลประโยชน์ทั้งโดยตรงหรือทางอ้อมจากการจ่ายค่าไถ่ โดยมีการอ้างอิงถึงรูปแบบวิธีการในการป้องกันตามข้อมติที่เกี่ยวข้องกับการต่อต้านการก่อการร้ายฉบับก่อน อาทิ ข้อมติของคณะมนตรีที่ 1373 (2001), 1904 (2009), 1989 (2011), 2083 (2012) โดยมีการสื่อสารและแบ่งปันข้อมูลผ่านความร่วมมือระหว่างประเทศ หรือกับพันธมิตรภาคเอกชน ตลอดจนสร้างเครือข่ายระหว่างผู้มีส่วนเกี่ยวข้องทั้งหมด¹²⁵ ให้แบ่งปันข้อมูลเส้นทางการเงินของกลุ่มก่อการร้ายที่ได้จากการจ่ายค่าไถ่ เพื่อทำการยึดและอายัดทรัพย์สิน ตลอดจนการปราบปรามการฟอกเงินและเครือข่ายทางการเงินของผู้ก่อการร้าย โดยใช้การแบ่งปันข้อมูลระหว่างกันเพื่อติดตามแหล่งที่มาของรายได้ ของกลุ่มก่อการร้าย ดังนั้นมาตรการแบ่งปันข้อมูลเพื่อปราบปรามการลักพาตัวเพื่อเรียกค่าไถ่ สามารถใช้วิธีการเดียวกันกับการต่อต้านการก่อการร้ายโดยข้อมติที่ 2133/2014 มีการรับรองวิธีการดำเนินการ¹²⁶ เช่นเดียวกันกับข้อมติที่เกี่ยวข้องกับการต่อต้านการก่อการร้าย

5. การปราบปรามการลักลอบขายของโบราณที่มีมูลค่า

การทำลายมรดกทางวัฒนธรรมอย่างผิดกฎหมาย และการขโมยทรัพย์สินและลักลอบขนของทรัพย์สินโบราณทางวัฒนธรรมในกรณีที่เกิดความขัดแย้งทางอาวุธ ถือเป็นภัยคุกคามต่อสันติภาพและความมั่นคงระหว่างประเทศ¹²⁷ รัฐมีหน้าที่ในการปกป้องทรัพย์สินโบราณวัตถุที่มีคุณค่าทางวัฒนธรรม เช่นเดียวกับ สหประชาชาติเองต่อภารกิจการรักษาสันติภาพและความมั่นคงระหว่างประเทศ คณะมนตรีความมั่นคงได้พิจารณาว่าความเสี่ยงของมรดกทางวัฒนธรรมที่เกี่ยวข้องกับสถานการณ์ความขัดแย้งทางอาวุธในแต่ละประเทศ จนในปี 1999 คณะมนตรีความมั่นคงเรียกร้องให้ กลุ่มตอลิบานที่

¹²⁴ Council of the European Union, "Council conclusions on Kidnap for Ransom" (2014), Retrieved from <https://www.consilium.europa.eu/media/28038/143318.pdf>

¹²⁵ Organization for Security and Co-operation in Europe, "Declaration on the OSCE role in countering kidnapping and hostage groups in the context of the implementation of UN Security Council resolution 2133 (2014)" Retrieved from <https://www.osce.org>

¹²⁶ "Reaffirms its decision in resolution [1373 \(2001\)](#), [1904 \(2009\)](#), [1989 \(2011\)](#) and [2083 \(2012\)](#) that all States shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts"

¹²⁷ United Nations Security Council Resolution 2347/2017, preamble

ทำการควบคุมพื้นที่บางส่วนของดินแดนของประเทศอัฟกานิสถานให้เคารพต่อมรดกทางวัฒนธรรมและประวัติศาสตร์¹²⁸

ปี 2003 ในสงครามอิรักคณะมนตรีความมั่นคงได้เน้นย้ำต่อความจำเป็นในการเคารพมรดกทางโบราณคดีในทางประวัติศาสตร์ วัฒนธรรม และศาสนาของประเทศอิรัก และเพื่อการคุ้มครองสถานที่ทางโบราณคดี อาทิ พิพิธภัณฑ์ห้องสมุดศาสนา และอนุสาวรีย์ที่สำคัญ และยังเรียกร้องให้สหรัฐอเมริกาและประเทศสมาชิก อำนวยความสะดวกในการนำมรดกทางโบราณคดีกลับคืนอย่างปลอดภัยสู่สถาบันทรัพย์สินทางวัฒนธรรมแห่งชาติอิรัก รวมทั้งรายการอื่น ๆ ของโบราณวัตถุ และห้ามมิให้มีการแลกเปลี่ยนหรือถ่ายโอนรายการทรัพย์สินทางวัฒนธรรม ซึ่งนำไปสู่การออกมาตรการห้ามการส่งออกซึ่งสินค้าทางวัฒนธรรมของประเทศอิรักระหว่างการรักษาสันติภาพและความมั่นคง จนกระทั่งได้มีการรับรองข้อมติหลังจากสงครามเพื่อรับรองรัฐบาลชั่วคราวในอิรักในปี 2547 จึงถือว่าความดูแลดังกล่าวตกอยู่ในอำนาจของรัฐบาลอิรักอย่างเป็นทางการ

ในการแบ่งปันข้อมูลภายใต้ความร่วมมือเพื่อปราบปรามการลักลอบขายของโบราณที่มีคุณค่าทางวัฒนธรรม คณะมนตรีความมั่นคงได้รับรองข้อมติที่ 2199/2015, 2322/2016 และ 2347/2017 ให้รัฐสมาชิก (Calls upon Member States) ดำเนินการแบ่งปันข้อมูลระหว่างองค์กรภายในประเทศ ฝึกอบรมแก่เจ้าหน้าที่ตำรวจและศุลกากร และพัฒนาฐานข้อมูลเพื่อทำการรวบรวมเกี่ยวกับกลุ่มก่อการร้ายที่ลักลอบขายของโบราณที่มีคุณค่าทางวัฒนธรรม และทำการแบ่งปันข้อมูลในระดับความร่วมมือระหว่างประเทศ ติดตามเส้นทางการเงินของกลุ่มก่อการร้ายโดยการแบ่งปันข้อมูลของบุคคลได้เงินมาแบบผิดกฎหมายจากการค้าขายโบราณวัตถุ โดยเพิ่มความร่วมมือของภาคเอกชนในเขตอำนาจของตน หรือผู้ที่เกี่ยวข้องทั้งหมด

พัฒนาฐานข้อมูลเพื่อทำการเก็บข้อมูลเกี่ยวกับการกระทำความผิดทางอาญาที่เกี่ยวข้องกับทรัพย์สินทางวัฒนธรรม และการลักลอบขุดทรัพย์สินทางวัฒนธรรม เพื่อทำการแลกเปลี่ยนข้อมูลผ่านความร่วมมือในการบริหารจัดการชายแดน¹²⁹ เพื่อสกัดซึ่งการนำเข้าวัตถุโบราณทางประวัติศาสตร์ ภายใต้ความดูแลของประเทศปลายทาง หรือการส่งออกภายใต้ความดูแลของประเทศต้นทาง ออกกฎหมายเพื่ออำนวยความสะดวกแก่การแบ่งปันข้อมูลต่อหน่วยงานที่ดำเนินการทางกฎหมายเพื่อหยุดการค้าขายทรัพย์สินทางวัฒนธรรมที่ผิดกฎหมาย รัฐสมาชิกในพื้นที่ความขัดแย้งควรจัดทำข้อมูลประวัติมรดกทางวัฒนธรรมและรายการทรัพย์สินในระดับท้องถิ่นและระดับชาติของตน¹³⁰ เพื่อ

¹²⁸ Kristin Hausler, "The evolution role of the United Nations Security Council and the protection of culture heritage in the event of armed conflict," (2018). <http://www.qil-qdi.org/cultural-heritage-security-council-resolution-2347-matters>.

¹²⁹ Security Council, "Condemns Destruction, Smuggling of Cultural Heritage by Terrorist Groups" (2017) Retrieved from <https://www.un.org/press/en/2017/sc12764.doc>

¹³⁰ United Nations Security Council Resolution 2347/2017, pp. 17(a)

รวบรวมข้อมูลแบบดิจิทัล และทำการแบ่งปันหรือเปิดให้รัฐสมาชิกภายใต้ความร่วมมือสามารถเข้าถึงข้อมูล ตลอดจนข้อมูลอื่น ๆ จากหน่วยงานที่มีอำนาจหน้าที่รับผิดชอบโดยเฉพาะ¹³¹ สนับสนุนให้รัฐสมาชิกมีการใช้ข้อมูลผ่านฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL Database of Stolen Works of Art) ฐานข้อมูลขององค์การศึกษาศาสตร์และวัฒนธรรมแห่งสหประชาชาติ (UNESCO Database of National Cultural Heritage Laws) และฐานข้อมูลขององค์การศุลกากรโลก (WCO ARCHEO Platform) เพื่อเป็นองค์การกลางในการแบ่งปันข้อมูลที่จำเป็นต่อทีมการวิเคราะห์และการติดตามเพื่อการลงโทษ¹³² เพื่อการดำเนินการสืบสวน เพื่อดำเนินคดีกับอาชญากรรม และเพื่อการยึดทรัพย์สินทางวัฒนธรรมกลับคืนถิ่นที่ตั้งเดิม



¹³¹ Ibid, pp. 17 (e)

¹³² Ibid, pp. 17 (f)

สรุปท้ายบท

เมื่อทำการวิเคราะห์ในบทนี้จะได้ผลการวิเคราะห์ว่าบทบาทของการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้ายนั้นได้ปรากฏแรกเริ่มเดิมทีช่วงปี ค.ศ. 1963 ที่ประชาคมระหว่างประเทศเริ่มตกลงกันเพื่อจัดทำตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้าย จนปัจจุบันมีทั้งหมด 19 ฉบับ ซึ่งสะท้อนให้เห็นว่านอกจากการปราบปรามการก่อการร้ายแล้วก็คือ การให้รัฐภาคนั้นหันมาร่วมมือกัน ไม่หวงแหนซึ่งข้อมูลหรือกีดกันการเข้าถึงข้อมูลแก่กัน เพื่อประโยชน์ในการต่อต้านการก่อการร้ายโดยการรับรู้ข้อมูลของผู้กระทำความผิด ข้อมูลพยานหลักฐานที่มีส่วนสำคัญต่อการใช้เพื่อดำเนินคดีตามกฎหมาย อย่างไรก็ตามการแบ่งปันข้อมูลตามตราสารก็มีข้อจำกัดทางกฎหมายมากมาย ทั้งให้ด้านของสารบัญญัติและกระบวนการที่เป็นอุปสรรคต่อการแบ่งปันข้อมูลให้มีประสิทธิภาพต่อการปราบปรามการก่อการร้ายในปัจจุบันที่อุบัติขึ้นใหม่อย่างรวดเร็ว

จากปัญหาดังกล่าวนำมาสู่บทบาทการแบ่งปันข้อมูลภายใต้การดำเนินงานของคณะมนตรีความมั่นคงแห่งสหประชาชาติในการต่อต้านการก่อการร้ายที่เป็นอีกหนึ่งกลไกที่เข้ามาช่วยเสริมบทบาทเดิมตามตราสารระหว่างประเทศ การแบ่งปันข้อมูลภายใต้กรอบของคณะมนตรีความมั่นคงจะเน้นไปที่การสร้างความร่วมมือระหว่างรัฐตามแนวทางของหลักความมั่นคงร่วม กล่าวคือรัฐใดรัฐหนึ่งจะทำการปราบปรามการก่อการร้ายเพียงลำพังต่อไปไม่ได้แล้ว ต้องร่วมมือกันและบรรลุซึ่งผลไปพร้อมกัน ประโยชน์ของการแบ่งปันข้อมูลที่ได้จะเข้าไปช่วยเสริมประสิทธิภาพของการดำเนินมาตรการปราบปรามการก่อการร้ายอื่นๆ เช่น มาตรการอายัดทรัพย์สิน มาตรการห้ามการเดินทาง เป็นต้น ซึ่งในทั้งนี้ความจำและประโยชน์ที่จะได้รับจากการดำเนินมาตรการแบ่งปันข้อมูลภายใต้กรอบของคณะมนตรีความมั่นคง จะช่วยอุดช่องว่างการดำเนินการภายใต้กรอบของตราสารระหว่างประเทศ ซึ่งสามารถพิจารณาเบื้องต้นได้จากองค์ประกอบทั้ง 3 ด้าน คือ ด้านเนื้อหาสาระ ด้านกระบวนการ และด้านการบังคับใช้ ที่ค่อนข้างชัดเจนว่าการดำเนินการภายใต้กรอบของคณะมนตรีความมั่นคงมีการกำหนดขอบเขตการแบ่งปันข้อมูลที่กว้างกว่า ครอบคลุมกว่า และมีการกำหนดกลไกที่ชัดเจนกว่า บรรดาตราสาร มีพัฒนาการของการกำหนดกระบวนการและกลไกแบ่งปันข้อมูลสำคัญอยู่ สองช่วงหลักๆคือ บริบทหลังสงครามเย็น และบริบทหลังเหตุการณ์วินาศกรรม

จากการศึกษาค้นพบในบทนี้ยังไม่สามารถตอบสมมุติฐานที่ตั้งไว้ เพียงเพราะจุดประสงค์ของผู้เขียนในการศึกษาบทนี้เพื่อที่จะแสดงให้เห็นถึงบทบาทของการแบ่งปันข้อมูลก่อน และวิเคราะห์ให้ทราบถึงแนวคิดทางกฎหมายของการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย อย่างไรก็ตามสิ่งที่ค้นพบในบทนี้นั้นแสดงให้เห็นว่าคณะมนตรีความมั่นคงได้สร้าง Value added ให้กับการแบ่งปันข้อมูลอันจะนำไปสู่การดำเนินมาตรการต่อต้านการก่อการร้ายในมิติต่างๆ ซึ่งบทถัดไปผู้เขียนจะได้แจกแจงมาตรการการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงเพื่อให้

ทราบถึงพันธกรณีของรัฐ เนื้อหาสารบัญญัติของข้อมูล ตลอดจนแสดงให้เห็นถึงโครงสร้างของ
กระบวนการและกลไกของการแบ่งปันข้อมูลโดยละเอียด



บทที่ 3

มาตรการการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายตามมติคณะมนตรีความมั่นคงแห่งสหประชาชาติ

มาตรการการแบ่งปันข้อมูลเพื่อดำเนินการต่อต้านการก่อการร้าย มีจุดประสงค์ก็เพื่อที่จะต้องการให้บรรดารัฐต่างๆอาศัยบทบาทของการร่วมมือ หรือ การประสานงานระหว่างกันทั้งในระดับระหว่างประเทศ และระดับภายในประเทศ เพื่อให้เกิดการลื่นไหลของข้อมูลที่เป็นต่อการนำไปใช้ในดำเนินมาตรการต่อต้านการก่อการร้ายในแง่ต่างๆ ได้อย่างมีประสิทธิภาพ ทั้งนี้ผู้เขียนจะแบ่งประเภทของมาตรการในการต่อต้านการก่อการร้ายออกเป็น 5 ประเภท คือ

1.) มาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรม, 2.) มาตรการยับยั้งการเข้าถึงแหล่งการเงินของการก่อการร้าย, 3.) มาตรการตรวจจับการเดินทางของผู้ก่อการร้าย, 4.) มาตรการการบังคับในทางกฎหมายต่อการก่อการร้าย, 5.) มาตรการต่อต้านการแพร่ขยายอาวุธที่มีอำนาจทำลายล้างสูงเพื่อใช้ในการก่อการร้าย ทั้งนี้ในแต่ละประเภทมาตรการนั้นผู้เขียนจะทำการวิเคราะห์ว่าการแบ่งปันข้อมูลได้เข้าไปมีส่วนเกี่ยวข้องอย่างไร ตลอดทั้งแจกแจงถึงพันธกรณีของคณะมนตรีความมั่นคง สารบัญญัติ เนื้อหา กระบวนการ รวมถึงกลไกอื่นๆในกระบวนการของการแบ่งปันข้อมูลในการต่อต้านการก่อการร้าย

3.1 การแบ่งปันข้อมูลต่อมาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรม

ความร่วมมือระหว่างประเทศด้านกระบวนการยุติธรรมเป็นกุญแจสำคัญในการจัดการกับความท้าทายของการก่อการร้ายข้ามชาติจำนวนมาก ในส่วนนี้ผู้เขียนจะอธิบายถึงอำนาจหน้าที่ของหน่วยงานด้านกระบวนการยุติธรรมในคดีก่อการร้าย กระบวนการความร่วมมือและการมีส่วนร่วมในแพลตฟอร์ม หรือเครือข่ายความร่วมมือด้านการพิจารณาคดี และการบังคับใช้กฎหมายระหว่างหน่วยงาน เพื่ออำนวยความสะดวกในการรวบรวมซึ่งพยานหลักฐาน หรือการแบ่งปันข้อมูลที่เป็น การเข้าถึงหลักฐานดิจิทัล และพยานหลักฐานที่เกี่ยวข้องกับผู้ต้องสงสัยว่าเป็นผู้ก่อการร้ายตามกฎหมายระหว่างประเทศ เพื่อจุดประสงค์ที่จะนำผู้ก่อการร้ายเข้าสู่กระบวนการยุติธรรม

3.1.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ข้อมติ 1373/2001 ได้ตัดสินใจให้บรรดารัฐต่างๆ (Decides also that all States shall) จะต้องหามาตรการการให้ความช่วยเหลือระหว่างรัฐด้วยกันโดยอาศัยการมีส่วนร่วมในกระบวนการยุติธรรม ในกระบวนการทางอาญาหรือการสืบสวนสอบสวนต่อการกระทำที่เกี่ยวข้องกับการก่อการร้าย ทั้งนี้ได้กำหนดอีกว่าให้รัฐมีการร่วมมือระหว่างกันในการแบ่งปันข้อมูลและ

พยานหลักฐานที่เกี่ยวข้องกับคดีการก่อการร้ายผ่านความร่วมมือระหว่างประเทศแบบพหุภาคี แบบภายในภูมิภาค แบบอนุภูมิภาค หรือแบบทวิภาคี และในแต่ละระดับของความตกลงร่วมมือเหล่านี้¹³³

ข้อมติที่ 2178/2014 ได้เรียกร้องให้รัฐสมาชิก (Calls upon Member States) พัฒนาความร่วมมือระหว่างประเทศในระดับ เช่น ในระดับภูมิภาค และในระดับอนุภูมิภาค เพื่อเพิ่มขีดความสามารถของการแบ่งปันข้อมูลและพยานหลักฐานที่เป็นประโยชน์ต่อกระบวนการยุติธรรมในการวินิจฉัยบุคคลที่เป็นนักรบต่างชาติ¹³⁴

ข้อมติที่ 2322/2016 ผลักดันให้รัฐสมาชิก (Encourages Member States) มีการดำเนินการภายในประเทศ ในการเก็บซึ่งข้อมูลที่มีความจำเป็นและพยานหลักฐานทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการแสวงหาผลประโยชน์ของผู้ก่อการร้ายของผ่านระบบอินเทอร์เน็ต (Terrorist exploitation of the Internet)¹³⁵ โดยสอดคล้องต่อกฎหมายภายในของรัฐสมาชิก

3.1.2 สารบัญญัติ

1. คำนิยามของข้อมูล

มาตรการของการต่อต้านการก่อการร้ายแต่ละประเภะนั้นได้กำหนดรูปแบบของการแบ่งปันข้อมูลไว้แตกต่างกัน เพื่อประโยชน์ที่จะให้เกิดการได้รับข้อมูลและใช้ให้เกิดผลลัพธ์ตามจุดประสงค์ มาตรการนั้นอย่างมีประสิทธิภาพที่สุด หากเมื่อพิจารณาถึงข้อมติที่เกี่ยวข้องกับการปราบปรามการก่อการร้ายในช่วงแรก (ค.ศ. 1990-2001) มิได้ให้คำจำกัดความของคำว่า “ข้อมูล” ว่าเป็นข้อมูลประเภทใด เพียงแต่ให้ลักษณะว่าจะต้องใช้เพื่อการต่อต้านการก่อการร้าย แต่เมื่อมีข้อมติในการต่อต้านการก่อการร้ายที่ถูกรับรองตามมาในภายหลังจะพอที่จะสามารถกำหนดความหมายกว้างๆ ว่าเป็น ข้อมูลที่ปรากฏอยู่ทุกประเภท¹³⁶ ที่สามารถใช้ในการสืบสวนสอบสวนของหน่วยงานบังคับใช้กฎหมาย การปฏิบัติงานของหน่วยข่าวกรอง เพื่อติดตาม ป้องกัน รวมถึงการสอบสวนอาชญากรรมและการก่อการร้าย และกระบวนการเหล่านี้สะท้อนออกมาได้ว่าข้อมูลที่ได้ทำการแบ่งปันผ่านความร่วมมือต่างๆนั้น ด้วยตัวของมันเองไม่สามารถที่จะนำไปสู่การต่อต้านการก่อการร้ายได้ แต่จะทำได้ก็ต่อเมื่อการที่

¹³³ United Nations Security Council Resolution 1373/2001, pp. 2(f) ,3(b)

¹³⁴ United Nations Security Council Resolution 2178/2014, pp. 11

¹³⁵ “The Relevant Resolutions, in particular 1267 (1999), 1373 (2001), 1624 (2005), 2322 (2016) and 2396 (2017)”

¹³⁶ Larry D. Thompson, "Intelligence Collection and Information Sharing within the United States" (2003) Retrieved from <https://www.brookings.edu/testimonies/intelligence-collection-and-information-sharing-within-the-united-states>

หน่วยงานที่มีอำนาจหน้าที่ของรัฐ ได้นำข้อมูลเหล่านั้นมาดำเนินการเพื่อออกมาตรการต่างๆ
“Information must lead to take the action”

2. การทำงานของมาตรการแบ่งปันข้อมูล

เมื่อเป็นเช่นนั้นการทำงานของมาตรการแบ่งปันข้อมูลจึงเป็นกลไกที่มีความสำคัญและจำเป็น เพื่อที่จะส่งเสริมให้มาตรการต่อต้านการก่อการร้ายต่างๆ ของคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ได้กำหนดขึ้นมาสามารถดำเนินการให้ลุล่วงได้เป็นอย่างดี มาตรการที่ถูกกำหนดจากกลไกการใช้อำนาจตามหมวดที่เจ็ดของคณะมนตรีความมั่นคงได้มุ่งเน้นที่จะต่อต้านการก่อการร้ายอย่างเป็นวงกว้าง และได้รับรองข้อมติออกมาอย่างมากมายเพื่อกำหนดพันธกรณีที่รัฐจะต้องแบ่งปันข้อมูลในด้านต่างๆ จำเป็นต้องศึกษาถึงความสัมพันธ์ของการแบ่งปันข้อมูลกับมาตรการต่างๆ ในการต่อต้านการก่อการร้ายด้วย เช่น มาตรการต่างๆ ที่เกี่ยวข้องกับการดำเนินงานในกระบวนการยุติธรรม มาตรการอายัดทรัพย์สินเครือข่ายก่อการร้าย มาตรการควบคุมและตรวจคนเข้าเมือง การสืบสวนสอบสวนหรือจับกุมบุคคลที่เกี่ยวข้องกับการก่อการร้าย รวมถึงยับยั้งกระแสรายของอาวุธ อาวุธทำลายร้ายสูง ซึ่งเป้าหมายสุดท้ายของการแบ่งปันข้อมูลเพื่อใช้ในการดำเนินมาตรการเหล่านี้ คือ การได้นำตัวผู้ก่อการร้ายเข้าสู่กระบวนการยุติธรรม

ดังนั้นในบทนี้ผู้เขียนจะอธิบายให้ทราบถึง มาตรการของการแบ่งปันข้อมูลว่าถูกกำหนดไว้เป็นอย่างไร กระบวนการและผู้มีส่วนเกี่ยวข้องทั้งหมด ฟังก์ชันที่ถูกสะท้อนจากการแบ่งปันข้อมูลออกมาในแต่ละประเด็น และวิเคราะห์ถึงกลไกอื่นๆ ในการแบ่งปันข้อมูลที่น่าไปสู่ดำเนินมาตรการในทางปฏิบัติ

3.1.3 กระบวนการของความร่วมมือและการประสานงานในการแบ่งปันข้อมูล

คณะมนตรีความมั่นคงให้รัฐต่างๆ ดำเนินกระบวนการของความร่วมมือและการประสานงานในการแบ่งปันซึ่งข้อมูลและพยานหลักฐาน รวมทั้งข้อมูลที่ได้รับจากอินเทอร์เน็ต หรือในพื้นที่ที่มีความขัดแย้ง อันเกี่ยวข้องกับการก่อการร้ายโดยต้องสอดคล้องกับการมีกฎหมายรับรองภายในประเทศ รวมทั้งกฎหมายระหว่างประเทศ

ทั้งนี้รัฐควรเพิ่มขีดความสามารถในทางกฎหมายของตนในสร้างช่องทางเพื่อร่วมมือกับภาคเอกชนโดยเฉพาะอย่างยิ่งกับผู้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร (Information and communications technology service providers)¹³⁷ โดยจะต้องดำเนินการออกกฎหมายที่

¹³⁷ United Nations Security Council Counter Terrorism Committee, "The 2015 Madrid Guiding Principles and 2018 Addendum", *Security Council Guiding Principles on Foreign Terrorist Fighters* (2018), Available from <https://www.un.org/sc/ctc/wp-content/uploads/2019/09/Security-Council-Guiding-Principles-on-Foreign-Terrorist-Fighters.pdf>

บังคับใช้ภายในรัฐ ที่ให้อำนาจและหน้าที่ของหน่วยงานเฉพาะในการรวบรวมข้อมูลดิจิทัล และพยานหลักฐานที่เกี่ยวข้องกับการก่อการร้าย และผู้ก่อการร้ายนักรบต่างชาติ และเรียกร้องให้รัฐปรับปรุงความร่วมมือระหว่างประเทศระดับภูมิภาค และอนุภูมิภาคตามความเหมาะสมผ่านข้อตกลงพหุภาคีและทวิภาคีให้สอดคล้องกับพฤติการณ์ของการก่อการร้ายในปัจจุบัน

3.1.3.1 การกำหนดกลไกในทางกฎหมาย

1. กลไกเพื่อรับรองความร่วมมือและการประสานงานระหว่างประเทศ

เพื่อเสริมสร้างความร่วมมือระหว่างประเทศในการป้องกัน ตรวจสอบ และดำเนินคดีกับการกระทำของผู้ก่อการร้าย รัฐจะต้องการดำเนินการสร้างกลไกในความร่วมมือระหว่างประเทศ เพื่อรวบรวมข้อมูลดิจิทัล และพยานหลักฐานในคดีที่เกี่ยวข้องกับการก่อการร้ายและนักรบก่อการร้ายจากต่างประเทศ (FTFs) ซึ่งใน The 2015 Madrid Guiding Principles and 2018 Addendum : Guiding Principle ข้อที่ 49 ได้แนะนำการกำหนดกลไกความร่วมมือระหว่างประเทศได้นั้น¹³⁸

1.) รัฐควรดำเนินการออกกฎหมาย หรือทบทวนและปรับปรุงกฎหมายว่าด้วยความช่วยเหลือซึ่งกันและกัน (Mutual legal assistance laws) อาทิ การแบ่งปันข้อมูล หรือข้อมูลดิจิทัล และพยานหลักฐาน ซึ่งเกี่ยวข้องกับความผิดที่เกี่ยวกับการก่อการร้ายโดยสอดคล้องกับพันธกรณีระหว่างประเทศ ตลอดจนพิจารณาทบทวนกฎหมายว่าด้วยความช่วยเหลือซึ่งกันและกัน และ เพื่อปรับปรุงกลไกเพื่อรองรับปริมาณของคำขอสำหรับการแบ่งปันข้อมูล หรือข้อมูลดิจิทัล และพยานหลักฐานที่เกี่ยวข้องการก่อการร้ายที่เพิ่มขึ้นค่อนข้างมากในปัจจุบัน

2.) กำหนดอำนาจและหน้าที่ให้หน่วยงานรัฐสำหรับปฏิบัติงานในการให้ความช่วยเหลือซึ่งกันและกัน ตลอดทั้งกำหนดกระบวนการการให้ความช่วยเหลือและความรับผิดชอบในหน้าที่อย่างชัดเจน

3.) รัฐควรพิจารณาการให้สัตยาบันและดำเนินการตามตราสารระหว่างประเทศที่ว่าด้วยการต่อต้านการก่อการร้าย หรือตราสารในระดับภูมิภาคเพื่อสร้างกำหนดกระบวนการพื้นฐานสำหรับการขอและให้ความช่วยเหลือทางกฎหมายซึ่งกันและกัน

4.) ในกรณีที่คำขอความช่วยเหลือระหว่างประเทศจากรัฐที่มีได้อยู่ภายในความร่วมมือ ให้รัฐดำเนินการให้ความร่วมมือบนพื้นฐานของหลักประติบัติต่างตอบแทน (Reciprocal basis) หรือเป็นกรณี ๆ ไป (Case-by-case basis)

5.) พิจารณาให้มีการพัฒนาและการมีส่วนร่วมในเวทีความช่วยเหลือซึ่งกันและกันในด้านกฎหมายระหว่างประเทศและระดับภูมิภาค (Mutual legal assistance cooperation platforms)

¹³⁸ United Nations Security Council Counter Terrorism Committee, "The 2015 Madrid Guiding Principles and 2018 Addendum", Security Council Guiding Principles on Foreign Terrorist Fighters (2018), Guiding Principle 49

รวมทั้งสร้างเครือข่ายที่ไม่เป็นทางการของหน่วยงานที่เกี่ยวข้อง เพื่อพัฒนาและเสริมสร้างการเตรียมการให้ความช่วยเหลือทางกฎหมาย สำหรับความร่วมมือข้ามภูมิภาคอย่างรวดเร็วต่อการกระทำผิดที่เกี่ยวข้องกับการก่อการร้าย

2. กลไกเพื่อรับรองความร่วมมือและการประสานงานภายในประเทศ

รัฐจะต้องดำเนินการสร้างกลไกทางกฎหมายภายในรัฐ เพื่อรวบรวมและเข้าถึงข้อมูลดิจิทัลและพยานหลักฐาน ในคดีที่เกี่ยวข้องกับการก่อการร้ายและนักรบต่างชาติ (FTFs) ซึ่งใน The 2015 Madrid Guiding Principles and 2018 Addendum : Guiding Principle ข้อที่ 44 ได้แนะนำการกำหนดกลไกทางกฎหมายได้ว่า

1.) ออกแบบบทบัญญัติที่เกี่ยวข้องกับการเก็บรักษาข้อมูลดิจิทัลโดยเฉพาะเจาะจง ซึ่งควรจะแยกจากบทบัญญัตินี้ออกจากบทบัญญัติที่ว่าด้วยการเก็บพยานหลักโดยทั่วไปออกจากกัน โดยเฉพาะในส่วนที่เป็นกระบวนการ และบทบัญญัตินี้ควรมีกลไกทางกฎหมายโดยเฉพาะในการค้นหาและยึดซึ่งข้อมูลดิจิทัล

2.) ออกแบบกลไกพิเศษ "Round-the-clock mechanism" เพื่อสร้างช่องทางให้บริษัทเอกชนร่วมมือกับหน่วยงานบังคับใช้กฎหมาย และกำหนดระเบียบกฎเกณฑ์ หรือมีการออกกฎหมายที่ให้อำนาจชัดเจนในการขอเก็บหลักฐานดิจิทัล และการร้องขอให้เปิดเผยข้อมูลในกรณีฉุกเฉิน¹³⁹

3.) พัฒนาเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) และความสามารถทางนิติวิทยาศาสตร์ภายในหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรมทางอาญา และหน่วยงานบังคับใช้กฎหมาย

4.) สร้างกลไกอำนวยให้เกิดความร่วมมือระหว่างหน่วยงานสืบสวนที่เกี่ยวข้อง รวมถึง "Police-to-police" และกับภาคเอกชนโดยเฉพาะอย่างยิ่งกับผู้ให้บริการ ICT ในการรวบรวมข้อมูลดิจิทัลและหลักฐานในคดีที่เกี่ยวข้องกับการก่อการร้ายและนักรบก่อการร้ายจากต่างประเทศ

5.) ประสานงานเพื่อรวบรวมหลักฐานอิเล็กทรอนิกส์จากผู้ดำเนินการที่เกี่ยวข้อง (Relevant actors) โดยยึดถือข้อเสนอแนะจากหน่วยงานระหว่างประเทศ เช่น ข้อเสนอแนะของสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ "[The Practical Guide for Requesting Electronic Evidence across Borders developed by the Executive](#)

¹³⁹ Security council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001)", [the President of the Security Council](#), pp 24-29

Directorate, UNODC¹⁴⁰ หรือชื่อแนะนำของสมาคมอัยการระหว่างประเทศ (The International Association of Prosecutors)

3.1.3.2 ความร่วมมือด้านกระบวนการยุติธรรม (Judicial cooperation)

ในปัจจุบันรัฐสมาชิกของสหประชาชาติ ได้มีความร่วมมือในกระบวนการยุติธรรมระหว่างประเทศที่อยู่ภายในภูมิภาคของรัฐเป็นจำนวนมากไม่น้อย แต่นั่นก็ยังมีเพียงพหุต่อการปราบปรามการก่อการร้ายในปัจจุบันที่มีได้จำกัดการกระทำแค่เพียงในภูมิภาคใดภูมิภาคหนึ่ง ในหลายๆความตกลงในภูมิภาคนั้นควรถูกแก้ไขให้มีลักษณะของการร่วมมือที่กว้างขึ้นเป็น ความร่วมมือข้ามภูมิภาค (Cross-regional cooperation) และเปิดโอกาสในรัฐที่อยู่นอกภูมิภาค ได้เข้ามาให้สัตยาบันต่อความร่วมมือในภูมิภาคนั้นด้วย เพื่อสร้างเครือข่ายที่ออกมาอยู่ในรูปแบบเครือข่ายระหว่างภูมิภาค (Interregional networking)¹⁴¹ จึงจะส่งผลให้เกิดความไหลลื่นของการแบ่งปันข้อมูล และพยานหลักฐานที่จำเป็นต่อกระบวนการพิจารณาคดีจะกว้างขึ้น

1. การจัดตั้งหน่วยงานผู้ประสานงานกลาง (Central authority)

สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ (Counter Terrorism Executive Directorate – CTED) ได้เสนอให้รัฐออกแบบหน่วยงานผู้ประสานงานกลาง (Central authority) หรือหน่วยงานที่มีลักษณะใกล้เคียง ซึ่งจะต้องมีอำนาจหน้าที่ในการให้ความช่วยเหลือซึ่งกันและกัน กับหน่วยงานของรัฐต่างประเทศ หรือองค์การระหว่างประเทศในการรับมือกับการก่อการร้าย แต่ละประเทศที่อยู่ภายใต้ความร่วมมือจะต้องมีการตั้งแต่หน่วยงานในระดับชาติ เป็นหน่วยงานกลางของประเทศภายใต้ความร่วมมือเพื่อมีหน้าที่เก็บข้อมูลและแบ่งปันข้อมูลภายในประเทศกับหน่วยงานของภาครัฐต่างๆ รวมถึงภาคเอกชนที่อยู่ภายใต้เขตอำนาจของรัฐตน¹⁴² ดังเช่นบริษัทที่เกี่ยวข้องกับเทคโนโลยีการสื่อสาร บริษัทขนส่งสินค้าทางเรือ และบริษัทสายการบินที่เป็นเจ้าของข้อมูลที่สามารถเป็นประโยชน์ต่อการพิจารณาคดีในกระบวนการยุติธรรม

¹⁴⁰ United Nations Office on Drugs and Crime, *The Practical Guide for Requesting Electronic Evidence Across Borders* (2019),

<https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html>

¹⁴¹ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 432

¹⁴² Security Council, "Letter dated 13 May 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), p.12 (D)

ข้อสังเกตในเรื่องความร่วมมือระหว่างประเทศในกระบวนการยุติธรรม ความร่วมมือทำงานในระดับภูมิภาคอาจพบอุปสรรคน้อยกว่า เพราะประเทศที่อยู่ในภูมิภาคเดียวกัน มักธรรมเนียมปฏิบัติในทางกฎหมายคล้ายคลึงกัน ดังนั้นรัฐมักที่จะใช้ความร่วมมือในกระบวนการยุติธรรมภายในภูมิภาคที่ระบุประเภทของความร่วมมือที่เคารพต่อสิทธิของรัฐผู้ร้องขอ และรัฐผู้ถูกร้องขอ สิทธิของผู้ต้องสงสัยที่เป็นคนสัญชาติของตน รวมทั้งขั้นตอนที่จะต้องปฏิบัติ มาเป็นเงื่อนไขในการพิจารณา¹⁴³ ดังนั้นความร่วมมือในระดับภูมิภาคสามารถแก้ปัญหาบางอย่างที่เกิดขึ้นระหว่างรัฐที่มีธรรมเนียมปฏิบัติทางกฎหมายที่แตกต่างกัน ซึ่งบางประเทศก็ให้ความช่วยเหลือในการแบ่งปันข้อมูลที่เป็นสิ่งกันและกัน เฉพาะกับเจ้าหน้าที่ผู้มีอำนาจของศาล เท่านั้นไม่ใช้กับพนักงานอัยการ

เมื่อพิจารณาจากข้อมติที่ 1373/2001 ที่เรียกร้องให้รัฐมีการเชื่อมต่อกันในกระบวนการสืบสวนสอบสวนหรือกระบวนการดำเนินคดีที่เกี่ยวข้องกับการก่อการร้าย รวมถึงบุคคลที่มีส่วนเกี่ยวข้องต่อการเป็นส่วนหนึ่งของนักรบต่างชาติ ตามข้อมติที่ 2178/2014 ความสำคัญของความตกลงที่ว่าด้วยความช่วยเหลือซึ่งกันและกันคือการแบ่งปันข้อมูลซึ่งเป็นข้อมูลดิจิทัล และหลักฐาน ในระบบอินเทอร์เน็ต โดยรัฐควรสร้างเสริมประสิทธิภาพและปรับปรุงความตกลงในความช่วยเหลือซึ่งกันและกัน ในกรณีที่เกี่ยวข้องกับการก่อการร้ายให้สอดคล้องกับเทคนิคการสืบสวน และการได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์¹⁴⁴



จึงจะส่งผลให้ไม่เกิดพรมแดนของการแบ่งปันข้อมูลระหว่างรัฐภายใต้ความร่วมมือ อย่างไรก็ตามรัฐมีความจำเป็นอย่างมากที่จะต้องมียุทธศาสตร์กลางที่ทำหน้าที่เป็นคนกลางรับประสานการร้องขอหรือการขอร้องต่อรัฐภาคีต่างๆภายใต้ความร่วมมือ

¹⁴³ United Nations Office on Drugs and Crime, *Basic principles of international cooperation against terrorism* (2009),

https://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/English.pdf

¹⁴⁴ Special Procedures of the Human Rights Council, "Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism" (2017), p.3

2. ความร่วมมือทางข้อมูลกับบริษัทเอกชนภายใต้เขตอำนาจ

การเก็บข้อมูลหรือพยานหลักฐานทางอิเล็กทรอนิกส์ในระบบอินเทอร์เน็ตนั้น รัฐต้องอาศัยความร่วมมือกับภาคเอกชนที่ประกอบกิจการภายใต้เขตอำนาจรัฐของรัฐ การที่บริษัทเอกชนนั้นเป็นเจ้าของข้อมูลที่อาจใช้เป็นพยานหลักฐานทางอิเล็กทรอนิกส์ในการใช้ดำเนินในกระบวนการยุติธรรม¹⁴⁵ เช่น บริษัทผู้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Service Providers), บริษัทผู้ให้บริการด้านโทรคมนาคม (Telecommunication Service Providers) จะต้องมีการออกกฎหมายที่ให้อำนาจเจ้าหน้าที่และรับรองข้อมูลจากการเก็บได้จากภาคเอกชน รวมถึงข้อมูลของเอกชนนั้นที่ได้บริการอยู่นอกเขตแดน (External-territory service) เพื่อการใช้ข้อมูลเหล่านั้นเป็นพยานหลักฐานเมื่อเข้าสู่กระบวนการยุติธรรมเพื่อพิจารณาคดีที่เกี่ยวข้องกับการก่อการร้ายและนักรบต่างชาติ

3. ความร่วมมือทางข้อมูลกับบริษัทเอกชนที่ประกอบกิจการระดับสากล

การขอความร่วมมือในการเก็บข้อมูลของภาคเอกชนที่ประกอบกิจการในระดับโลก (Global private company) ซึ่งมีได้ก่อตั้งอยู่ภายใต้เขตอำนาจของรัฐ ดังนั้นรัฐอาจจะต้องร้องขอไปที่บริษัทเจ้าของข้อมูลนั้นโดยเป็นการเฉพาะ แต่ต้องพิจารณาถึงประเด็นในทางกฎหมายด้วยว่า บริษัทที่ทำกิจการระดับโลกนั้นได้ถูกก่อตั้งขึ้นภายใต้เขตอำนาจของรัฐใด (State where the corporation is incorporated) หรือข้อมูลของบริษัทเอกชนที่รัฐต้องการนั้นถูกเก็บไว้ภายใต้เขตอำนาจของรัฐใด (State where the data are stored) ดังนั้นเมื่อพิจารณาแล้วจะพบว่าข้อมูลที่สามารถเป็นโยชน์ต่อกระบวนการยุติธรรมที่อยู่ในระบบอินเทอร์เน็ตส่วนใหญ่แล้วจะมีบริษัทใหญ่ๆเป็นเจ้าของในการบริการทางเทคโนโลยีสารสนเทศ¹⁴⁶ เช่น ข้อมูลของบริษัทสื่อสังคมออนไลน์ (Social media firms), บริษัทโทรคมนาคม (Telecommunications companies), ผู้ให้บริการอีเมลและอินเทอร์เน็ต (E-mail and Internet service providers), ผู้ให้บริการเว็บไซต์และบริการโฮสต์ข้อมูลที่สำคัญในโครงสร้างพื้นฐานด้าน ICT ทั่วโลก (Providers of website and data hosting services are all integral partners in the global ICT infrastructure) บริษัทเหล่านี้ล้วนทำกิจการในระดับโลกซึ่งมีผู้ใช้

¹⁴⁵ Security Council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), pp. 26

¹⁴⁶ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp. 21-23

มากมายทั่วโลกเป็นผู้รับบริการ และฐานข้อมูลกลาง (Data Centre) ของบริษัทเหล่านี้ก็อยู่ภายใต้เขตอำนาจอธิปไตยในหลายๆรัฐ

หากพิจารณาไปอีกจะพบว่า บริษัทเอกชนนั้นต่างต้องอยู่ภายใต้กฎหมายในประเทศที่บริษัทนั้นได้ดำเนินธุรกิจ และจะต้องให้ความร่วมมือกับหน่วยงานบังคับใช้กฎหมายในประเทศนั้นตามกฎหมายภายใน แต่เมื่อมีข้อพิจารณาอีกว่าการให้บริการของบริษัทเหล่านั้นได้มีบางส่วนให้บริการอยู่นอกเขตแดน (External-territory service) ในหลายๆประเทศ ซึ่งก่อให้เกิดความขัดแย้งกันต่อประเด็นที่เกี่ยวกับเขตอำนาจ ในการบังคับใช้กฎหมายภายใน ของรัฐซึ่งเป็นผู้ที่ได้รับบริการจากบริษัทเอกชนนั้นอยู่ ดังนั้นบริษัทเอกชนที่ทำกิจการในลักษณะนี้มักจะมีการออกมาแก้ปัญหของการบังคับใช้กฎหมายภายในต่อการให้บริการระหว่างประเทศของผู้เขา ในรูปแบบของระเบียบและเงื่อนไขของการให้ความร่วมมือกับหน่วยงานภายในประเทศผู้รับบริการ

ตัวอย่างเช่น บริษัท Facebook ได้ออก “Guidelines for Cooperation with Law Enforcement Worldwide, Preservation of Data, and Emergency Requests” เปิดช่องทางให้หน่วยงานบังคับใช้กฎหมายหรือหน่วยงานที่เกี่ยวข้องจากรัฐที่ได้รับบริการของบริษัท สามารถส่งคำร้องให้มีการแบ่งปันหรือช่วยเหลือทางข้อมูล ซึ่งจะต้องไปตามเงื่อนไขของทางบริษัท Facebook ดังตารางต่อไปนี้

ตารางเงื่อนไขของ Facebook Guidelines for Cooperation with Law Enforcement Worldwide, Preservation of Data, and Emergency Requests

กรณี	ช่องทางให้การให้ความร่วมมือ	เงื่อนไข	ข้อมูลที่สามารถแบ่งปันได้
1	ผ่านกระบวนการขอบังคับทางกฎหมายระหว่างประเทศ (International Legal Process Requirements)	ทางบริษัทจะเปิดเผยข้อมูลบัญชีผู้ใช้ตามที่ผู้ใช้ตามข้อกำหนดในการบริการ และกฎหมายที่บังคับใช้เท่านั้น ซึ่งอาจต้องมีคำขอ Mutual Legal Assistance Treaty (สนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันด้านกฎหมาย) หรือหนังสือส่งประเด็นไปสืบพยานในการขอให้เปิดเผยข้อมูลเนื้อหาของบัญชีผู้ใช้	1. ข้อมูลเนื้อหา การสื่อสาร และข้อมูลอื่นๆ ที่ผู้ใช้บริการให้เมื่อใช้ผลิตภัณฑ์ของบริษัท 1.1 ข้อมูลของผู้ใช้งานที่มีการคุ้มครองพิเศษ 1.2 เครือข่ายและการเชื่อมต่อของผู้ใช้งาน 1.3 ประวัติความถี่และการใช้งานของผู้ใช้งาน 1.4 ข้อมูลเกี่ยวกับการทำธุรกรรมในการใช้งานของ Facebook 1.5 สิ่งที่คุณคิดที่สามทำและข้อมูลที่คุณคิด

<p>2</p>	<p>คำขอเร่งด่วน (Emergency Requests)</p>	<p>เพื่อตอบสนองต่อสถานการณ์ที่เกี่ยวข้องกับภัยอันตรายชัดเจนที่จะเกิดขึ้นกับเด็ก หรือความเสียหายต่อการเสียชีวิต หรือการบาดเจ็บทางกายภาพอย่างรุนแรงที่จะเกิดขึ้นกับบุคคลใดๆ และต้องการการเปิดเผยข้อมูลโดยเร็วที่สุดนั้น เจ้าหน้าที่บังคับใช้กฎหมายอาจยื่นคำขอผ่านระบบคำขอแบบออนไลน์สำหรับบริการบังคับใช้กฎหมาย</p> <p>หมายเหตุ: เราจะไม่ตรวจสอบหรือตอบรับคำขอที่ส่งโดยผู้ที่ไม่ใช่เจ้าหน้าที่บังคับใช้กฎหมาย ผู้ใช้ที่ทราบว่าไม่มีสถานการณ์ฉุกเฉินเกิดขึ้นควรติดต่อเจ้าหน้าที่ที่มีอำนาจบังคับใช้กฎหมายในท้องถิ่นโดยตรงทันที</p>	<p>เหล่านี้ให้เกี่ยวกับตัวผู้ใช้งาน</p> <p>2. ข้อมูลของอุปกรณ์ของผู้ใช้บริการ</p> <p>2.1 ระบบปฏิบัติการของผู้ใช้บริการ เวอร์ชันของฮาร์ดแวร์และซอฟต์แวร์ ระดับแบตเตอรี่ ความแรงของสัญญาณ พื้นที่จัดเก็บที่มีประเภทเบราว์เซอร์ ชื่อและประเภทไฟล์และแอป</p> <p>2.2 การทำงานของอุปกรณ์</p> <p>2.3 สัญญาณของอุปกรณ์</p> <p>2.4 ข้อมูลจากการตั้งค่าอุปกรณ์การเข้าถึงตำแหน่งที่ตั้ง GPS</p> <p>2.5 เครือข่ายและการเชื่อมต่อ</p>
----------	--	--	--

3	<p>การยื่นคำขอออนไลน์ (Online Submission of Requests)</p>	<p>เจ้าหน้าที่บังคับใช้กฎหมายอาจใช้ระบบคำขอแบบออนไลน์สำหรับการบังคับใช้กฎหมายเพื่ออื่น ติดตาม และดำเนินการตามคำขอ ผู้บังคับใช้กฎหมายที่ต้องการข้อมูลบันทึกของบัญชีผู้ใช้จาก Facebook หรือ Instagram ต้องส่งคำขอไปที่ Facebook Inc ซึ่งมีที่อยู่เมสซึ่งออกให้โดยรัฐบาลเพื่อเข้าสู่ระบบคำขอแบบออนไลน์สำหรับการบังคับใช้กฎหมาย "ไปรษณีย์ที่อยู่ในสหรัฐอเมริกา 1601 Willow Road, Menlo Park CA 94025"</p>
---	---	---

ที่มาของข้อมูลในตาราง¹⁴⁷



¹⁴⁷ Facebook, "Guidelines for Cooperation with Law Enforcement Worldwide, Preservation of Data, and Emergency Requests", Available from <https://www.facebook.com/safety/groups/law/guidelines/>

บริษัทเอกชนที่ให้บริการในระดับระหว่างประเทศ ส่วนใหญ่แล้วจะมีข้อกำหนดและเงื่อนไขของการบริการของบริษัท ในข้อกำหนดและเงื่อนไขสามารถที่จะทำการลบเนื้อหาหรือระงับการใช้งานของผู้ใช้บริการ กรณีที่ได้ละเมิดต่อข้อกำหนดและเงื่อนไขของการให้บริการ ซึ่งหากเกิดความจำเป็นที่จะต้องระงับข้อมูลการใช้งานของผู้รับบริการ ที่มีส่วนเกี่ยวข้องต่อการสนับสนุนการก่อการร้าย¹⁴⁸ อาทิ ประชาสัมพันธ์กิจกรรมของกลุ่มก่อการร้าย การรับสมัครบุคคล นักรบต่างชาติ หรือการปลุกปั่นที่จะนำไปสู่การก่อเหตุการณ์ของการก่อการร้าย บริษัทเอกชนผู้เป็นเจ้าของข้อมูลและให้บริการนั้นก็ย่อมสามารถเข้ามาตราการลบและระงับการใช้งานได้จากการพิจารณาด้วยตนเอง

โดยส่วนมากแล้วบริษัทเอกชนที่ให้บริการระหว่างประเทศ ส่วนใหญ่จะทำการกลั่นกรองข้อมูลเนื้อหาที่อัปโหลดโดยผู้ใช้ในเชิงรุก และเต็มใจที่ปฏิบัติตามคำขอของหน่วยงานผู้บังคับใช้กฎหมายต่อการลบเนื้อหาที่ขัดต่อข้อกำหนดในการให้บริการและคำสั่งทางกฎหมายที่เกี่ยวข้องต่อการต่อต้านการก่อการร้าย ตัวอย่างเช่น บริษัท YouTube¹⁴⁹ ได้ลบข้อมูลเนื้อหาที่เกี่ยวข้องต่อการก่อการร้ายมากกว่า 14 ล้านคลิปวิดีโอในช่วงปี 2012-2015, Facebook¹⁵⁰ ได้รับการแจ้งเตือนและทบทวนข้อมูลของผู้ใช้บริการมากกว่า 1 ล้านบัญชีที่ละเมิดข้อกำหนดและเงื่อนไขของการให้บริการในแต่ละสัปดาห์, และ Twitter¹⁵¹ ได้ระงับบัญชีของผู้ใช้บริการที่เกี่ยวข้องกับการประชาสัมพันธ์ของกลุ่มจัดตั้งรัฐอิสลามแห่งอิรักและลิแวนต์ (Islamic State of Iraq and the Levant – ISIL) มากกว่า 2,000 บัญชีในแต่ละเดือน

อย่างไรก็ตาม การลงโทษทางอาญาหรือมาตรการบังคับใช้กฎหมายอาจจะเหมาะสมสำหรับการระงับข้อมูลและการเก็บข้อมูลเพื่อเป็นพยานหลักฐานในการดำเนินคดีที่เกี่ยวข้องต่อการก่อการร้าย แต่สิ่งที่ต้องให้ความสำคัญคือข้อมูลที่ไม่ได้มีลักษณะของการสนับสนุนการก่อการร้ายโดยตรง (Objectionable content information) โดยถูกแพร่เผยในระบบอินเทอร์เน็ตอย่างมากมาจากผู้ก่อการร้ายเองหรือผู้ที่สนับสนุนการก่อการร้าย ซึ่งมาตรการระงับข้อมูลและเก็บเป็นหลักฐานเพื่อเอาผิดอย่างเดียวไม่ได้ จะต้องหาวิธีการเพื่อตอบโต้กับความคิดสุดโต่ง (Counter-Narratives) หรือตอบโต้กับเนื้อหาในการโน้มน้าม (Counter-Messaging) ของผู้ก่อการร้าย ในปัจจุบันได้มีความ

¹⁴⁸ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp. 24-26

¹⁴⁹ Daisuke Wakabayashi, "YouTube Sets New Policies to Curb Extremist Videos," *The New York Times* 2017, <https://www.nytimes.com/2017/06/18/business/youtube-terrorism.html>

¹⁵⁰ Gordon Corera, "Facebook reveals measures to remove terrorist content," *BBC News* 2017, <https://www.bbc.com/news/technology-40290258>

¹⁵¹ Foo Yun Chee, "Twitter suspended 166,153 accounts for terrorism content in second half 2018," *REUTERS* 2019, <https://www.reuters.com/article/us-twitter-security/twitter-suspended-166153-accounts-for-terrorism-content-in-second-half-2018-idUSKCN1SF1LN>

ร่วมมือในการดำเนินมาตรการตอบโต้ข้อมูลที่ไม่ได้มีลักษณะของการสนับสนุนการก่อการร้ายโดยตรง (Objectionable content information) ประเภทนี้แล้ว เช่น ศูนย์สื่อสารดิจิทัลระดับภูมิภาคจัดตั้งขึ้นตามความร่วมมือระหว่างมาเลเซียกับสหรัฐฯ¹⁵² ในการต่อสู้กับการประชาสัมพันธ์ข้อมูลชวนเชื่อของผู้ก่อการร้าย และสื่อสารข้อมูลข่าวสารที่ถูกต้องจากหน่วยงานของรัฐให้กับประชาชน ซึ่งประเทศมาเลเซียได้รับเลือกให้เป็นที่ตั้งของศูนย์ฯ ในภูมิภาคเอเชียตะวันออกเฉียงใต้

3.1.3.3 การประสานงานด้านกระบวนการยุติธรรม (Judicial coordination)

การมอบหมายหน่วยงานให้มีหน้าที่ประสานงาน รัฐควรจะมีการตั้งแต่งหน่วยงานเพื่อที่ประสานการทำงานระหว่างหน่วยงานของรัฐภาคีอื่น (Inter-agency) หรือหน่วยงานบังคับใช้กฎหมายที่ทำงานภายใต้ลักษณะความร่วมมือที่เป็นเครือข่ายของหน่วยงานของรัฐต่างประเทศ เพื่ออำนวยความสะดวกแก่กันต่อการแบ่งปันข้อมูลรวมถึงพยานหลักฐานที่จำเป็นต่อการพิจารณาคดีบุคคลต้องสงสัยที่เกี่ยวข้องกับการก่อการร้าย¹⁵³ จากการใช้รูปแบบเดิมที่รัฐของสหประชาชาติจะมักใช้ช่องทางทางการทูต (Diplomatic channels) ในการส่งข้อมูลและแลกเปลี่ยนซึ่งพยานหลักฐานในคดี เป็นเหตุให้ระยะเวลาในกระบวนการพิจารณาคดีนั้นยาวนานขึ้น และไม่เป็นที่พอใจต่อการดำเนินมาตรการการป้องกันการกระทำที่เกี่ยวข้องต่อการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ¹⁵⁴

ในหนึ่งรัฐนั้นสามารถที่จะให้สัตยาบันในหลายๆความร่วมมือได้ ในกรณีที่เป็นภาคีของความร่วมมือแบบทั้งพหุภาคีและแบบทวิภาคีในเวลาเดียวกัน ถ้ามีการเรียกร้องให้ทำการแบ่งปันข้อมูล เมื่อมีการพิจารณาแล้วว่าการดำเนินการนั้นอยู่ภายใต้ความร่วมมือฉบับใดฉบับหนึ่ง หรือภายใต้ทั้งสองฉบับเท่าที่ไม่เกิดข้อขัดแย้งในการบังคับใช้ ก็สามารถที่จะดำเนินการให้สอดคล้องต่อความร่วมมือที่รัฐตนได้เป็นภาคีอยู่ แต่ในกรณีที่พิจารณาแล้วว่าการดำเนินการบังคับใช้ ก็ให้ทำการเลือกดำเนินการแบ่งปันข้อมูลตามความเหมาะสมของความร่วมมือหนึ่งในที่ขัดแย้งกัน โดยรัฐจะต้อง

¹⁵² Leanne Goh, "Malaysia will set up centre to counter IS propaganda," *Thestar.com.my* 2015, <https://www.thestar.com.my/news/nation/2015/10/10/malaysia-will-set-up-centre-to-counter-is-propaganda>.

¹⁵³ Security Council, *Ninth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range* ((2019).

¹⁵⁴ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", *the President of the Security Council* (2016), pp. 431

พิจารณาการเลือกจาก หมวดที่ว่าด้วยกับข้อขัดกัน (Provide for the interrelation)¹⁵⁵ ที่อยู่ในความร่วมมือฉบับนั้น หากมิได้กำหนดหมวดที่ว่าด้วยข้อขัดกันไว้ในความร่วมมือ ก็ให้ใช้ข้อกำหนดที่เอื้ออำนวยมากที่สุดของความร่วมมือฉบับนั้นในการดำเนินการแบ่งปันข้อมูล

3.1.4 เครื่องมือและข้อเสนอแนะ

หน่วยงานระหว่างประเทศที่บทบาทในการปราบปรามการก่อการร้ายได้พัฒนาเครื่องมือที่จะช่วยเหลือให้รัฐดำเนินการปราบปรามการก่อการร้ายได้อย่างราบรื่นมากขึ้น อาทิ โปรแกรมแบ่งปันทรัพยากรอิเล็กทรอนิกส์ แพลตฟอร์มกลางในเก็บรวบรวมข้อมูลและความรู้ต่างๆ หรือแม้กระทั่งฐานข้อมูลกลางเพื่ออำนวยความสะดวกในการเผยแพร่และแบ่งปันข้อมูลที่เกี่ยวข้องกับการก่อการร้าย ทั้งนี้เป็นประโยชน์ให้บรรดารัฐต่างๆ ได้ใช้งานเครื่องมือเหล่านี้ต่อการดำเนินมาตรการปราบปรามการก่อการร้ายของตน ตลอดทั้งหน่วยงานระหว่างประเทศเหล่านั้นได้เสนอเอกสารข้อเสนอแนะนำขึ้นตอนและกระบวนการต่างๆ ในการปราบปรามการก่อการร้าย ให้บรรดารัฐต่างๆ พิจารณาเพื่อนำไปปรับใช้

3.1.4.1 ข้อเสนอของคณะกรรมการต่อต้านการก่อการร้าย (Counter terrorism committee)

คณะกรรมการต่อต้านการก่อการร้าย ได้รับรอง Addendum to the 2015 Madrid Guiding Principles ซึ่งใน Guiding Principle 14 ได้สนับสนุนให้รัฐมีความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน ระหว่างกันเพื่ออำนวยความสะดวกในกระบวนการทางอาญาเพื่อต่อต้านการก่อการร้าย¹⁵⁶ เอกสารชิ้นนี้แม้จะไม่มีค่าบังคับทางกฎหมายอย่างเคร่งครัดแต่ก็ได้รับการยอมรับว่ามีค่าบังคับทางกฎหมายในลักษณะที่เป็น Soft Law ซึ่งหากรัฐมิได้มีความร่วมมือระหว่างประเทศ หรือกฎหมายที่ขอข้อมูลหรือแบ่งปันข้อมูลระหว่างรัฐ ก็เรียกร้องให้ใช้หลักปฏิบัติต่างตอบแทน (Reciprocity)¹⁵⁷ หรือหลักการพิจารณาเป็นกรณีไป (Case by case basis)¹⁵⁸ ซึ่งจำเป็นที่จะต้องใช้

¹⁵⁵ The United Nations Office on Drugs and Crime (UNODC), "Links between conventions (multilateral/regional/bilateral)", Manual on International Cooperation in Criminal Matters related to Terrorism (2009), p. 20, Retrieved from https://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/English.pdf

¹⁵⁶ Addendum to the 2015 Madrid Guiding Principles (2018), Guiding Principle 14, Retrieved from https://www.un.org/sc/ctc/wp-content/uploads/2018/12/2018-Addendum-to-the-2015-Madrid-Guiding-Principles_as_adopted.pdf

¹⁵⁷ “หลักปฏิบัติต่างตอบแทน (Reciprocity) คือหลักการนี้จะใช้ในกรณีที่ไม่มีสนธิสัญญาหรือข้อตกลงในเรื่องความช่วยเหลือซึ่งกันและกัน แต่ประเทศผู้ร้องขอและประเทศผู้รับคำร้องได้พิจารณาแล้วว่า จะดำเนินการให้ความช่วยเหลือการดำเนินคดีทางอาญาแก่กัน และเป็นการตอบแทนในลักษณะเดียวกัน”

ระยะที่นานมากกว่าการมีความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน (Mutual legal assistance agreement) โดยเฉพาะ

1. ข้อท้าทายของความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน

ความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน ได้ถูกนำเสนอและเป็นที่ยอมรับของรัฐบาลในการให้ความช่วยเหลือแก่กัน แต่เมื่อก่อนความช่วยเหลือซึ่งกันและกันส่วนใหญ่จะถูกออกแบบมาเพื่อช่วยเหลือทางข้อมูลและหลักฐานแบบวัตถุที่มีรูปร่าง (Physical objects) เป็นส่วนใหญ่ อาทิ ข้อมูลที่เป็นแผ่นเอกสาร หรือพยานเอกสารและพยานเอกสารวัตถุอันต้องมีการรับรองอย่างเป็นทางการ ซึ่งอาจจะเพิ่มระยะเวลาต่อการดำเนินการและมีความไม่สะดวกอย่างมากในการเคลื่อนย้ายระหว่างพรมแดนกอปรในปัจจุบันมีข้อมูลอิเล็กทรอนิกส์ ที่สามารถเคลื่อนผ่านพรมแดนอย่างอิสระผ่านระบบอินเทอร์เน็ตในไม่กี่วินาที ในรายงานของรัฐบาลสหรัฐอเมริกาเผยว่าในช่วงทศวรรษที่ผ่านมา¹⁵⁹ มีอัตราการเพิ่มขึ้นของการขอพยานหลักฐานจากต่างชาติ มากกว่า 60% และอัตราการเพิ่มขึ้นของการขอเอกสารทางอิเล็กทรอนิกส์ ที่ร้องขอมายังสำนักงานกิจการระหว่างประเทศของกระทรวงยุติธรรมสหรัฐอเมริกามากถึง 1000% ในหลายๆรัฐทั่วโลกกำลังเผชิญกับวิกฤตคำร้องขอที่ตกค้าง ที่ผ่านความตกลงในความช่วยเหลือซึ่งกันและกันซึ่งบางกรณีอาจใช้เวลานานนับเดือนในการตอบรับและดำเนินการ

ปัญหาที่เกิดจากความร่วมมือในรูปแบบเดิมทำให้หลายๆรัฐตระหนักถึงความสามารถที่จำกัดของระบบการร่วมมือในความช่วยเหลือซึ่งกันและกันในปัจจุบัน ที่มีสามารถจะรับรองความต้องการข้อมูลและพยานหลักฐานในปัจจุบันได้ ดังนั้นคณะกรรมการต่อต้านการก่อการร้าย จึงเรียกร้องไปยังรัฐสมาชิกให้มีการทบทวนเนื้อหาของความช่วยเหลือซึ่งกันและกัน และกฎหมายภายในของรัฐสมาชิกที่เกี่ยวข้อง ทั้งยังสนับสนุนให้ลงทุนในการเสริมสร้างความสามารถในการให้ความช่วยเหลือ และมีการแก้ไขความตกลงหรือเพิ่มเติมเนื้อหา ในความช่วยเหลือซึ่งกันและกันให้สอดคล้องกับทางปฏิบัติต่อเทคโนโลยีการแบ่งปันข้อมูลและการร้องขอซึ่งพยานหลักฐานแบบดิจิทัล¹⁶⁰ที่มีเพิ่มมากขึ้นในปัจจุบัน

¹⁵⁸ “หลักการพิจารณาเป็นกรณีไป (Case by case basis) คือการดำเนินการเป็นแต่ละกรณีไปซึ่งพิจารณาจากลักษณะเฉพาะของกรณีและผู้ร้องขอมานั้น จากสถานะทางกฎหมายของผู้รับคำร้องขอ”

¹⁵⁹ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 433

¹⁶⁰ “พยานหลักฐานแบบดิจิทัล (Digital evidence) คือข้อมูลอะไรก็ตามที่อยู่ในช่องทางเทคโนโลยีการสื่อสารที่ถูกใช้โดยวัตถุประสงค์ในการก่อการร้าย”

2. ข้อเสนอแนะในการปรับปรุงความตกลงว่าด้วยความช่วยเหลือซึ่งกันและกัน

คณะกรรมการต่อต้านการก่อการร้าย ได้เสนอแนวทางของการให้ความช่วยเหลือซึ่งกันและกันระหว่างรัฐ โดยช่องทางสื่อสารอย่างไม่เป็นทางการที่ทำงาน 24/7 เพื่อให้รัฐได้พัฒนาเครือข่ายช่องทางการร่วมมือผ่านระบบอินเทอร์เน็ตที่สามารถทำงานได้ 24 ชั่วโมงตลอดทั้งสัปดาห์ ขึ้นมาเป็นตัวเลือกของการช่วยเหลือการแบ่งปันข้อมูลและส่งผ่านพยานหลักฐานในระบบอินเทอร์เน็ตได้อย่างรวดเร็วเหมาะสม เพื่อที่จะนำข้อมูลและพยานหลักฐานที่ได้ไปใช้ในกระบวนการยุติธรรมในคดีที่เกี่ยวข้องต่อการก่อการร้ายและนักรบต่างชาติ

3.1.4.2 เครื่องมือแพลตฟอร์มของสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่ง

สหประชาชาติ (United Nations Office on Drugs and Crime)

สมาคมอัยการระหว่างประเทศ (International Association of Prosecutors – IAP) และสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime) ได้ทำงานอย่างใกล้ชิดต่อมาตรการต่อต้านการก่อการร้ายกับ สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ ในการพัฒนาตัวช่วยเหลือทางเทคนิค ให้แก่หน่วยงานของรัฐเพื่อประโยชน์ต่อการป้องกันและเก็บพยานหลักฐานของกลุ่มก่อการร้ายที่ใช้ประโยชน์จากระบบเทคโนโลยีการสื่อสารเป็นส่วนหนึ่งของการปฏิบัติการ¹⁶¹ และได้รับรองร่าง “*Practical Guide for Requesting Electronic Evidence Across Borders*”¹⁶² ซึ่งการได้ตัวผู้กระทำความผิดฐานการก่อการร้ายเข้าสู่กระบวนการยุติธรรม

โดยทั้งนี้จำเป็นต้องมีความร่วมมือจากหลายหน่วยงานของรัฐเป็นตัวกลาง อาทิ หน่วยงานกลาง อัยการ และพนักงานสืบสวนสอบสวน ในการรวบรวมและแบ่งปันซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ ในการต่อต้านการก่อการร้าย รวมทั้งข้อมูลที่เป็นประโยชน์ต่อการสืบสวนสอบสวนข้ามพรมแดน ในปัจจุบันได้มีหลายภูมิภาค เช่น ประเทศในแถบแอฟริกาใต้สะฮารา เอเชีย เอเชียตะวันออกเฉียงใต้ หมู่เกาะแปซิฟิก ละตินอเมริกา ได้ริเริ่มฝึกอบรมหน่วยงานที่เกี่ยวข้องในประเทศ และร่างแผนการปฏิบัติในรูปของข้อกำหนดตามกฎหมายตามแนวทางของ “*Practical Guide for Requesting Electronic Evidence Across Borders*” ในการใช้ข้อมูลอิเล็กทรอนิกส์ และการร่วมมือการส่งผ่านข้อมูลกับภาคเอกชน ที่ตั้งอยู่ภายใต้เขตอำนาจของรัฐ

¹⁶¹ Security Council, “Ninth report of the Secretary-General on the threat posed by ISIL (Da’esh) to international peace and security and the range”, *United Nations efforts in support of Member States in countering the threat* (2019), pp. 63

¹⁶² UNODC and partners, “Practical Guide for Requesting Electronic Evidence Across Borders”, Available from <https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html>

- UNODC's SHERLOC Portal แพลตฟอร์ม

จุดประสงค์ของ “*Practical Guide for Requesting Electronic Evidence Across Borders*” เพื่อสร้างแนวปฏิบัติของความร่วมมือทางข้อมูลของหน่วยงานรัฐต่างๆที่เกี่ยวข้อง ผ่าน UNODC's SHERLOC Portal แพลตฟอร์ม ซึ่งเป็นแพลตฟอร์มกลางในเก็บรวบรวมข้อมูลและความรู้ต่างๆ รวมถึงเป็นแพลตฟอร์มกลางในการแบ่งปันข้อมูลทรัพยากรอิเล็กทรอนิกส์ (Electronic resources) และกฎหมายระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมและการก่อการร้าย

ตาราง : UNODC's SHERLOC Portal แพลตฟอร์ม ประกอบด้วย 8 ฐานข้อมูล

ลำดับ	ฐานข้อมูล (Data bases)	คำอธิบาย
1	Electronic Evidence	ข้อมูลภาพรวมของทรัพยากรประเภทต่างๆ ที่สามารถนำมาเป็นหลักฐานทางอิเล็กทรอนิกส์ที่รวบรวมได้จากกฎหมาย (Law) หลักกฎหมาย (Jurisprudence) บทคัดย่อ บรรณานุกรม (Bibliographic abstracts) และนโยบาย (Policies) ซึ่งได้ถูกการยอมรับและรับรองในกฎหมายระดับชาติ และระดับภูมิภาคของรัฐ เพื่อใช้เป็นหลักฐานทางอิเล็กทรอนิกส์ในการดำเนินคดี ข้อมูลของประเภททรัพยากรทั้งหมดสามารถเข้าถึงได้โดยตรงจากฐานข้อมูลที่อยู่หน้าแรกของ SHERLOC แพลตฟอร์มจะปรากฏประเภทของทรัพยากรไว้คือ 1. Electronic Evidence in the Case Law Database 2. Electronic Evidence in the Database of Legislations และ 3. Electronic Evidence in the Bibliographic Database
2	Case Law Database	ฐานข้อมูลคดีทางกฎหมายที่ครอบคลุม เป็นข้อมูลทางคดีให้เห็นแนวคำตัดสินของศาลในประเทศสมาชิกต่อการพิจารณาปัญหาในคดีที่เกี่ยวข้องกับอาชญากรรมและการก่อการร้ายในศาลของพวกเขาอย่างไร
3	Online Directory of Competent National Authorities	สารบบ (Directory) ของหน่วยงานระดับชาติ (National Authorities) ที่ได้รับมอบหมายให้มีหน้าที่และดำเนินการตามคำร้องขอเกี่ยวกับความช่วยเหลือซึ่งกันและกัน ใน

		การส่งผู้ร้ายข้ามแดน และการโอนผู้ต้องหาการลักลอบนำเข้าแรงงานทางทะเล การค้าอาวุธปืน การป้องกันอาชญากรรมองค์กรข้ามชาติ การค้าทรัพย์สินทางวัฒนธรรม การป้องกันการทุจริต ความร่วมมือระหว่างประเทศในกระบวนการทางแพ่งและทางปกครองเกี่ยวกับการทุจริต (Corruption) และการก่อการร้าย
4	Strategies	ฐานข้อมูลที่มีเครื่องมือในเชิงยุทธศาสตร์ (Strategic instruments) ตามการดำเนินการในระดับภูมิภาคและภายในประเทศของอนุสัญญาว่าด้วยองค์กรอาชญากรรมและพิธีสาร ตลอดจนกฎหมายระหว่างประเทศที่ว่าด้วยการต่อต้านการก่อการร้ายอื่นๆ
5	Legislative guide	ข้อมูลของคู่มือกฎหมายในปัจจุบัน ที่ตีพิมพ์เพื่อเป็นประโยชน์ต่อรัฐต้องการให้สัตยาบันหรือดำเนินการตามอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ
6	Database of Legislation	ฐานข้อมูลกฎหมายที่เป็นพื้นที่จัดเก็บข้อมูลอิเล็กทรอนิกส์ของกฎหมายที่เกี่ยวข้องกับข้อกำหนดต่างๆภายในรัฐ ตามการดำเนินการของอนุสัญญา พิธีสาร หรือกฎหมายระหว่างประเทศที่ว่าด้วยการต่อต้านการก่อการร้าย กฎหมายส่วนใหญ่ที่รวมอยู่ในฐานข้อมูลนี้ได้ถูกประกาศใช้เป็นพิเศษเพื่อต่อต้านอาชญากรรมและการก่อการร้ายในรูปแบบต่างๆ
7	Bibliographic Database	ฐานข้อมูลบรรณานุกรม ประกอบคำอธิบาย บทสรุป บทความที่เกี่ยวข้องกับอาชญากรรมและการก่อการร้ายที่เผยแพร่โดยประเทศสมาชิกที่ได้ทำการวิจัยและค้นคว้า
8	Treaties	ฐานข้อมูลของสนธิสัญญา กฎหมายระหว่างประเทศเพื่อต่อต้านการก่อการร้าย 19 ฉบับและกฎหมายระหว่างประเทศอื่นๆ ที่เกี่ยวข้อง

3.2 การแบ่งปันข้อมูลเพื่อปราบปรามการเข้าถึงแหล่งการเงินของการก่อการร้าย

มาตรการปราบปรามการเข้าถึงแหล่งการเงินของการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาตินั้น ในช่วงเริ่มแรกของการดำเนินการ (ค.ศ. 1990- 2000) จะมุ่งเน้นไปที่การจำกัดการจัดการทรัพย์สินของบุคคลหรือกลุ่มคนที่มีส่วนเกี่ยวข้องต่อการก่อการร้าย เช่น การอายัดโดยไม่มีชั่งข้า ซึ่งเงินทุน หรือทรัพย์สินทางการเงินอื่น ๆ หรือทรัพยากรทางเศรษฐกิจของบุคคลและกลุ่มบุคคลที่ได้ถูกกำหนดในรายชื่อการลงโทษของคณะมนตรีความมั่นคง

ในภายหลังปี ค.ศ. 2001 การปราบปรามการเข้าถึงแหล่งการเงินของการก่อการร้ายของบุคคลที่เกี่ยวข้องกับการก่อการร้ายนั้นได้เปลี่ยนแปลงวิธีการของการเข้าถึงแหล่งเงิน ในปัจจุบัน ขบวนการก่อการร้ายได้ใช้วิธีการในรูปแบบต่างๆในการหลบซ่อนแหล่งที่มาของการเงิน รวมทั้งเส้นทางการเงินที่ใช้เป็นปัจจัยสำคัญในการก่อเหตุโดยอาศัยเทคโนโลยีที่ถูกพัฒนาขึ้นตามยุคสมัย เช่น การระดมเงินทุนผ่านเว็บไซต์ (Crowdfunding sites) หรือโซเชียลมีเดีย แพลตฟอร์มการส่งข้อความในรูปแบบของการเข้ารหัส (Encrypted messaging platforms) บัตรเติมเงิน (Prepaid cards) กระเป๋าเงินดิจิทัล (Mobile Payment) และการโอนเงินทางอิเล็กทรอนิกส์ในรูปแบบอื่นๆ¹⁶³ เพราะฉะนั้นคณะมนตรีความมั่นคงแห่งสหประชาชาติได้มีข้อเรียกร้องให้บรรดารัฐมีการประเมินความเสี่ยงทางการเงินของการก่อการร้าย (Dedicated terrorism-financing risk assessment) โดยอาศัยการร่วมมือทางข้อมูลในหลายๆภาคส่วนในการปราบปรามการเข้าถึงแหล่งเงิน

ในหัวข้อส่วนนี้ผู้เขียนจะวิเคราะห์ว่าการแบ่งปันข้อมูลนั้น สามารถมีส่วนช่วยเสริมมาตรการของการดำเนินการปราบปรามทางการเงินอย่างไรโดยจะแบ่งออกเป็น 2 หัวข้อใหญ่ๆในการอธิบาย คือ 1. ข้อมูลเพื่อการอายัดทรัพย์สินของกลุ่มก่อการร้าย และ 2. ข้อมูลเพื่อการปราบปรามกิจกรรมการมีส่วนร่วมทางการเงินกับการก่อการร้ายและแจ้งให้เห็นถึงกระบวนการ พันธกรณีของคณะมนตรีที่จะให้มีดำเนินการแบ่งปันข้อมูล ตลอดจนข้อปฏิบัติต่างๆที่อยู่ในลักษณะของกฎหมายแบบอ่อน (Soft law)

¹⁶³ Security Council, "Letter dated 3 June 2020 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 43

3.2.1 ข้อมูลเพื่อการอายัดทรัพย์สินของกลุ่มก่อการร้าย

3.2.1.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ย้อนกลับไปเริ่มต้นของมาตรการยับยั้งการเงินของการก่อการร้ายตั้งแต่มีการรับรองข้อมติที่ 1267/1999 ข้อมติดังกล่าวนี้ถูกรับรองขึ้นในช่วงการปราบปรามกลุ่ม Al-Qaida และ Taliban¹⁶⁴ โดยมีกลไกในการกำหนดรายชื่อบุคคลจากสหประชาชาติ (UN sanction list) เพื่อหน่วยงานบังคับใช้กฎหมายของรัฐจะต้องดำเนินการอายัดเงินทุนและทรัพย์สิน และป้องกันไม่ให้บุคคลได้จัดหาเงินทุน รวมทั้งการดำเนินการปิดล้อมทางอาวุธแก่บุคคลและคณะบุคคลเหล่านี้ที่ถูกกำหนดไว้ในรายชื่อ¹⁶⁵

ข้อมติเรียกร้องบรรดารัฐต่างๆ (Calls upon all States to) มีพันธกรณีที่จะต้องจัดหา (Supply) ซึ่งข้อมูลที่เป็นต่อการปราบปรามกลุ่มก่อการร้ายให้แก่คณะกรรมการลงโทษกลุ่มก่อการร้ายอัลไคดะ (Al-Qaida Sanctions Committee)

3.2.1.2 การจัดตั้งหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย

เพื่อให้บรรลุซึ่งวัตถุประสงค์ตามข้อมติของการปราบปรามการเงินของการก่อการร้าย รัฐจะต้องมีการดำเนินการทางกฎหมายภายในรัฐตนเพื่อกำหนดหน่วยงานภายในที่มีอำนาจที่จำเป็นเพื่ออายัดเงินทุน หรือทรัพย์สินอื่น ๆ ของผู้ก่อการร้าย รวมทั้งผู้ที่ให้เงินสนับสนุนการก่อการร้าย และองค์กรก่อการร้าย

ทั้งนี้ข้อมติที่ 1989/2011 ในหัวข้อ "Measures implementation" เรียกร้องให้บรรดารัฐดำเนินการตาม¹⁶⁶ "มาตรฐานสากลที่ครอบคลุมซึ่งรวมอยู่ในคำแนะนำสี่สิบข้อของ Financial Action Task Force เกี่ยวกับการฟอกเงินและ FATF Nine ข้อเสนอแนะพิเศษเกี่ยวกับการจัดหาเงินทุนของผู้ก่อการร้าย" (The comprehensive international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing) เพื่อการดำเนินการต่อต้านการก่อการร้ายที่เป็นเป้าหมายอย่างมีประสิทธิภาพ

คำแนะนำในหัวข้อที่ 8 ในเรื่องการจัดตั้งหน่วยงานภายใน อาทิ หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย (Anti-money laundering and combating the financing of terrorism regulator) เพื่อดำเนินการอายัด

¹⁶⁴ United Nations Security Council Resolution 1267/1999, pp. 4

¹⁶⁵ กรมองค์การระหว่างประเทศ, "การต่อต้านการก่อการร้ายในกรอบสหประชาชาติ (Counter-Terrorism)" (2010), Retrieved from <http://www.mfa.go.th/main/th/issues/9899>

¹⁶⁶ United Nations Security Council Resolution 1989/2011, pp. 41

ทรัพย์สิน หรือเพิกถอนการอายัดทรัพย์สิน ห้ามจำหน่าย ห้ามจ่ายโอนไปซึ่งเงินทุนหรือทรัพย์สินอื่นๆ ที่เป็นของบุคคลหรือกลุ่มบุคคลที่ถูกกำหนดในรายชื่อของคณะกรรมการ¹⁶⁷

1. หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย จะต้องใช้อำนาจหน้าที่ในการออกระเบียบการ และบังคับใช้กฎหมายเพื่อการดำเนินการอายัดทรัพย์สิน และการเพิกถอน ซึ่งการอายัดทรัพย์สินได้กลไกของคณะกรรมการลงโทษตามข้อมติที่ 1267/1999¹⁶⁸
2. รัฐจะต้องออกกฎหมายเพื่อกำหนดความรับผิดชอบเพื่อการอายัดทรัพย์สินของบุคคลหรือกลุ่มบุคคลอย่างเปิดเผย ซึ่งบุคคลดังกล่าวนั้นจะต้องได้รับการตัดสินจากหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย หรือศาลที่มีเขตอำนาจในคดีถึงการอายัด และดำเนินการลงโทษบุคคลหรือกลุ่มบุคคลหากพวกเขาไม่ได้ปฏิบัติตามคำสั่ง
3. อำนาจหน้าที่ของหน่วยงาน ในการอายัดและเพิกถอนการอายัดเงินหรือทรัพย์สินอื่น ๆ ควรครอบคลุมไปถึงกองทุนหรือทรัพย์สินอื่น ๆ ที่ได้มาหรือสร้างขึ้นจากกองทุนหรือทรัพย์สินอื่น ๆ เช่น ทรัพย์สินหรือเงินอันเกิดจากดอกเบี้ยในทางนิตินัย ที่ผู้ก่อการร้ายเป็นเจ้าของหรือควบคุมโดยตรง หรือโดยอ้อม รวมทั้งผู้ที่ให้เงินทุนแก่การก่อการร้าย หรือองค์กรก่อการร้าย

¹⁶⁷ The Financial Action Task Force, "FATF Special Recommendations on Terrorist Financing", FATF Standards (2008), p. 10, available from <https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf>

¹⁶⁸ *ประเทศไทยได้จัดตั้งสำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ สำนักงาน ป.ง. เป็นหน่วยงานของรัฐซึ่งมีอำนาจหน้าที่ในการวางหลักเกณฑ์ และดูแลให้มีการปฏิบัติตามกฎหมาย ว่าด้วยการป้องกันและปราบปรามการฟอกเงิน รวมทั้งเป็นหน่วยงานตรวจสอบวิเคราะห์ข้อมูลทางการเงินที่เกี่ยวข้องกับการฟอกเงิน ในหน้าที่ของหน่วยงานวางหลักเกณฑ์ (Regulator)

สำนักงาน ป.ง.มีบทบาทในการศึกษาหามาตรการในการป้องกัน และปราบปรามการฟอกเงิน โดยมีฐานะเป็นฝ่ายเลขานุการของคณะกรรมการป้องกันและปราบปรามการฟอกเงิน (คณะกรรมการ ป.ง.) ส่วนในสถานะของหน่วยงานผู้บังคับใช้กฎหมาย (Law Enforcement) สำนักงาน ป.ง. มีอำนาจหน้าที่ในการตรวจสอบและดำเนินการเกี่ยวกับธุรกรรมหรือทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดฟอกเงิน ตามมติของคณะกรรมการธุรกรรม ตลอดจนดูแลให้ผู้มีส่วนเกี่ยวข้องปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ดังกล่าว

สำนักงาน ป.ง. เป็นหน่วยงาน จัดตั้งขึ้นตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และพระราชกำหนดแก้ไขเพิ่มเติมพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พ.ศ. 2546 เพื่อเพิ่มความผิดมูลฐานว่าด้วย "การก่อการร้าย" ซึ่งมีเลขาธิการ ป.ง. เป็นข้าราชการพลเรือนสามัญ ซึ่งพระบาทสมเด็จพระเจ้าอยู่หัวทรงพระกรุณาโปรดเกล้าฯ แต่งตั้งขึ้นตามคำแนะนำของคณะรัฐมนตรีและได้รับความเห็นชอบจากสภาผู้แทนราษฎรและวุฒิสภา ทำหน้าที่ควบคุมดูแลโดยทั่วไปซึ่งราชการของสำนักงาน และเป็นผู้บังคับบัญชาข้าราชการในสำนักงาน และรองเลขาธิการเป็นผู้ช่วยสั่งและปฏิบัติราชการ

4. บุคคลหรือกลุ่มบุคคลภายใต้เขตอำนาจของรัฐจะต้อง ถูกห้ามโดยกฎหมายไม่ให้รับเงินหรือทรัพย์สิน ทรัพยากรทางเศรษฐกิจ หรือบริการทางการเงิน หรือบริการอื่น ๆ ที่เกี่ยวข้องไม่ว่าโดยตรง หรือโดยอ้อม ทั้งหมด หรือร่วมกัน เพื่อประโยชน์ ซึ่งเกี่ยวข้องกับบุคคลหรือกลุ่มบุคคลที่ถูกกำหนดในรายชื่อการลงโทษ ผู้ก่อการร้าย ผู้ที่สนับสนุนการก่อการร้าย องค์กรก่อการร้าย นิติบุคคลที่เป็นเจ้าของหรือควบคุมไม่ว่าทางตรงหรือทางอ้อมโดยบุคคลหรือนิติบุคคลดังกล่าว และบุคคลและหน่วยงานที่ดำเนินการในนามของ หรือสามารถโยนโยนไปถึงบุคคลหรือกลุ่มบุคคลที่ถูกกำหนดในรายชื่อลงโทษ

3.2.1.3 กระบวนการการแบ่งปันข้อมูล

1. การกำหนดรายชื่อบุคคลหรือกลุ่มบุคคล (Listing)

ประการแรก กระบวนการของการแบ่งปันข้อมูลเพื่อการอายัดทรัพย์สินของกลุ่มก่อการร้าย เมื่อได้พิจารณาข้อมติที่ 1989/2011 สามารถอธิบายกระบวนการได้ว่า¹⁶⁹ รัฐสมาชิกจะต้องมอบหมายอำนาจให้หน่วยงานในการป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ทั้งนี้หน่วยงานดังกล่าวจะทำหน้าที่เป็นตัวกลางประสานข้อมูลกับคณะกรรมการลงโทษกลุ่มก่อการร้าย เพื่อที่ทางคณะกรรมการลงโทษจะใช้ข้อมูลในการวิเคราะห์และกำหนดรายชื่อของบุคคลหรือกลุ่มบุคคลในการอายัดทรัพย์สิน

ประการที่สอง หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ของแต่ละรัฐสมาชิกสหประชาชาติจะทำงานร่วมกันและประสานข้อมูลกับทีมติดตาม (The Monitoring Team)¹⁷⁰ ของคณะกรรมการลงโทษกลุ่มก่อการร้าย ในกรณี que ทีมติดตามได้ทำการร้องขอซึ่งข้อมูลบุคคล ข้อมูลทรัพย์สินบุคคล หรือกลุ่มบุคคลที่เกี่ยวข้องต่อการก่อการร้ายจากรัฐสมาชิก ทั้งนี้ก็เพื่อให้คณะกรรมการลงโทษได้ดำเนินการกำหนด (Designation) รายชื่อบุคคลหรือกลุ่มบุคคล โดยวิเคราะห์จากเนื้อหาข้อมูลจากบรรดารัฐสมาชิกที่สำคัญเพิ่มเติมเพื่อการตัดสินใจ (Additional material for the narrative summary) และเป็นเหตุผลให้การดำเนินการกำหนดรายชื่อ (Reasons for listing)

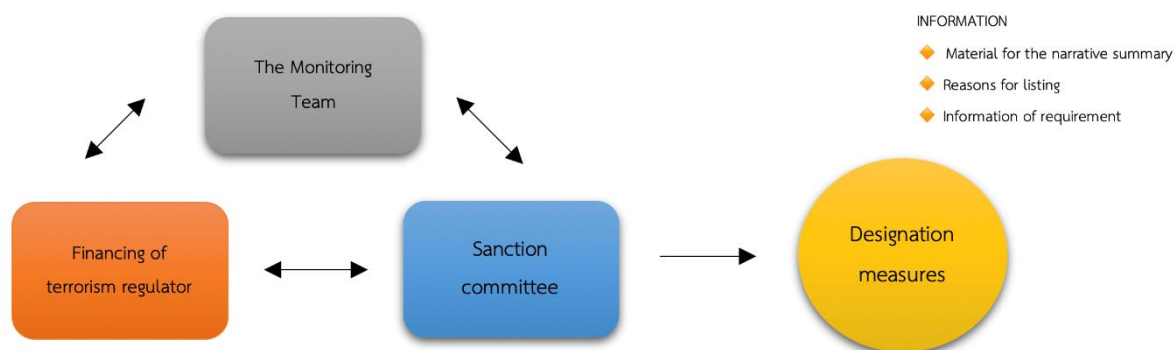
ประการที่สาม รัฐสมาชิกจะต้องมอบหมายให้หน่วยงานปราบปรามให้ข้อมูลคำแถลง (Statement) เมื่อถูกร้องขอจากคณะกรรมการลงโทษโดยตรง เพื่อที่จะนำข้อมูลจากคำแถลงไปใช้ใน

¹⁶⁹ United Nations Security Council Resolution 2253/2015, pp. 43-53

¹⁷⁰ United Nations Security Council Resolution 1989/2011, pp. 12-20

การพัฒนาเนื้อหาข้อมูลสำคัญเพิ่มเติมในการตัดสินใจ (Additional material for the narrative summary) และเป็นเหตุผลให้การดำเนินการกำหนดรายชื่อ (Reasons for listing)¹⁷¹

แผนผังแสดงโครงสร้างของการกำหนดรายชื่อบุคคลหรือกลุ่มบุคคล (Listing)



2. การทบทวนรายชื่อบุคคลหรือกลุ่มบุคคล (Reviewing)

ประการแรก ในกรณีที่หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ของรัฐสมาชิกสหประชาชาติใดได้กำหนดรายชื่อบุคคลด้วยตนเอง หรือส่งข้อมูลของบุคคลและกลุ่มบุคคลให้กับคณะกรรมการลงโทษเพื่อดำเนินการกำหนดรายชื่อ หน่วยปราบปรามของรัฐสมาชิกจะต้องประสานข้อมูลกับทีมติดตาม ของคณะกรรมการลงโทษกลุ่มก่อการร้าย โดยให้แจ้งถึงข้อมูลคำสั่งศาลแห่งรัฐตน หรือหน่วยงานทางกฎหมาย ถึงข้อมูลของการที่ได้ ทบทวน รายชื่อบุคคล หรือกลุ่มบุคคลตามกระบวนการทางกฎหมายภายใน ตลอดจนข้อมูลของการ พิจารณาคดีที่ได้เริ่มขึ้นบางส่วน¹⁷² รวมถึงข้อมูลที่เกี่ยวข้องอื่นๆ

ประการที่สอง หน่วยงานปราบปรามการเงินของรัฐสมาชิกสหประชาชาติโดยเฉพาะอย่างยิ่ง

1.) รัฐซึ่งเป็นเจ้าของข้อมูลของการกำหนดรายชื่อบุคคล 2.) รัฐซึ่งเป็นที่อยู่อาศัยหรือเจ้าของสัญชาติ ของบุคคลหรือกลุ่มบุคคลที่อยู่ในรายชื่อของคณะกรรมการลงโทษ จะต้องส่งข้อมูลการระบุตัวตน เพิ่มเติม และข้อมูลอื่น ๆ เพิ่มเติม ให้แก่คณะกรรมการลงโทษ พร้อมกับข้อมูลเอกสารที่เกี่ยวข้องกับ บุคคลหรือกลุ่มบุคคลที่ระบุไว้ในรายชื่อลงโทษ รวมถึงข้อมูลอัปเดตเกี่ยวกับสถานะการดำเนินการของ บุคคลที่ถูกกำหนดในรายชื่อลงโทษ¹⁷³ เช่น ข้อมูลการเคลื่อนย้าย การจำคุก หรือข้อมูลการเสียชีวิต

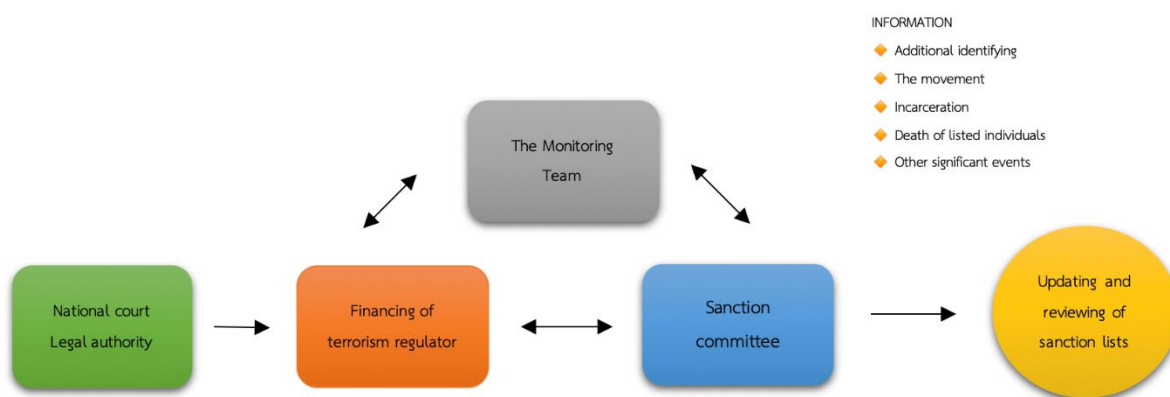
¹⁷¹ ISIL (Da'esh) & Al-Qaida Sanctions Committee, "The guidelines Document of the Committee for the conduct of its work", Revised and adopted by the Committee on 5 September (2018), p. 6

¹⁷² United Nations Security Council Resolution 2368/2017, pp. 85-88

¹⁷³ United Nations Security Council Resolution 1989/2011, pp. 36-40

ของบุคคล (Death of listed individuals) หรือเหตุการณ์สำคัญอื่น ๆ เพื่อที่จะให้คณะกรรมการ
 ลงโทษมีข้อมูลเกี่ยวกับบุคคลหรือกลุ่มบุคคลที่ถูกกำหนดในรายชื่อเพื่อการอัปเดตและการทบทวน
 รายชื่ออยู่ตลอดเวลา¹⁷⁴

แผนผังแสดงโครงสร้างของการทบทวนรายชื่อบุคคลหรือกลุ่มบุคคล (Reviewing)



3. การเพิกถอนรายชื่อบุคคลหรือกลุ่มบุคคล (Delisting)

ประการแรก หน่วยงานปราบปรามการเงินของรัฐสมาชิกสหประชาชาติโดยเฉพาะอย่างยิ่ง

1.) รัฐซึ่งเป็นเจ้าของข้อมูลของการกำหนดรายชื่อบุคคล 2.) รัฐซึ่งเป็นที่อยู่อาศัยหรือเจ้าของสัญชาติ
 ของบุคคลหรือกลุ่มบุคคลที่อยู่ในรายชื่อของคณะกรรมการลงโทษ สามารถให้ข้อมูลที่เกี่ยวข้อง
 ทั้งหมดแก่คณะกรรมการลงโทษ ในกรณีที่รัฐสมาชิกรับรองคำร้องที่จะยื่นคำร้องต่อคณะกรรมการ เพื่อ
 แสดงเจตจำนงของตนต่อคำร้องให้เพิกถอน (Delisting requests) ซึ่งรายชื่อของบุคคลหรือกลุ่ม
 บุคคลได้ โดยทั้งนี้¹⁷⁵

ประการที่สอง เมื่อคณะกรรมการลงโทษเห็นควรตามคำร้องของรัฐสมาชิก ให้สำนัก
 เลขาธิการ (The Secretariat) ดำเนินการภายใน 3 วันเพื่อลบรายชื่อบุคคลหรือกลุ่มบุคคลออกจาก
 รายการการลงโทษ และให้แจ้งต่อบรรดารัฐสมาชิกสหประชาชาติที่อยู่ในการปฏิบัติการปราบปราม
 ตามข้อมติ¹⁷⁶

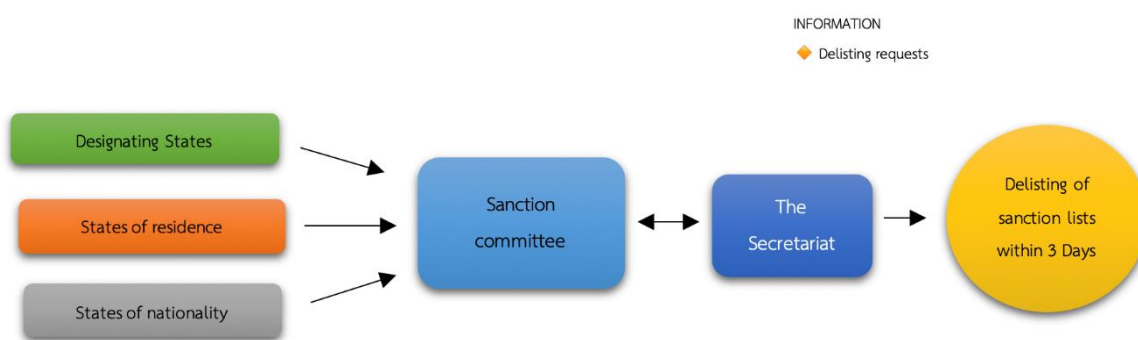
¹⁷⁴ ISIL (Da'esh) & Al-Qaida Sanctions Committee, "The guidelines Document of the Committee for the conduct of its work", Revised and adopted by the Committee on 5 September (2018), p. 10

¹⁷⁵ United Nations Security Council Resolution 1989/2011, pp. 21-35

¹⁷⁶ ISIL (Da'esh) & Al-Qaida Sanctions Committee, "The guidelines Document of the Committee for the conduct of its work", Revised and adopted by the Committee on 5 September (2018), p. 7

ประการที่สาม บรรดารัฐสมาชิกสหประชาชาติเมื่อได้รับการรับแจ้งข้อมูลถึงการเพิกถอนรายชื่อบุคคลหรือกลุ่มบุคคลจากเลขอาชญากรรม ให้ดำเนินการตามกระบวนการทางกฎหมายภายในของตนถึงการเพิกถอนซึ่งรายชื่อแก่หน่วยงานที่มีหน้าที่บังคับตามกฎหมายของตนภายในเวลาที่เหมาะสม

แผนผังแสดงโครงสร้างของการเพิกถอนรายชื่อบุคคลหรือกลุ่มบุคคล (Delisting)



3.2.1.4 การประสานงานของคณะกรรมการ Sanctions

คณะกรรมการลงโทษนำแนะให้รัฐสมาชิกให้ความร่วมมือกับกลไกความร่วมมืออย่างต่อเนื่องกับหน่วยงานต่อต้านการก่อการร้ายของสหประชาชาติ (United Nations counter-terrorism bodies) รวมถึงคณะกรรมการต่อต้านการก่อการร้าย (the Counter- Terrorism Committee) และคณะกรรมการที่จัดตั้งขึ้นตามมติ 1540 (1540 Sanction Committee) ตลอดจนกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้อง ในการแบ่งปันข้อมูลผ่านช่องทางที่เหมาะสม หรือให้ความร่วมมือขอประสานงานกับรัฐสมาชิก¹⁷⁷ อาทิ

1. การขอประสานงานกับหน่วยงานของรัฐสมาชิกที่มีอำนาจหน้าที่ในการดำเนินการตามข้อมติ เช่น การขอเข้าถึงข้อมูลของการดำเนินงานของหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย
2. การขอประสานเชื่อมโยงรัฐสมาชิกในการดำเนินการตามข้อมติ ภายใต้อำนาจหน้าที่ของหน่วยงานต่อต้านการก่อการร้ายของสหประชาชาติ รวมถึงคณะกรรมการต่อต้านการก่อการร้าย (the Counter- Terrorism Committee) และคณะกรรมการที่จัดตั้งขึ้นตามมติ 1540 (1540 Sanction Committee) ตลอดจนกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้อง ในการอำนวยความสะดวกและติดตามความช่วยเหลือทางเทคนิค

¹⁷⁷ United Nations Security Council Resolution 2368/2017, pp. 89-99

3. ทั้งนี้รัฐสมาชิกควรให้ความร่วมมือในการประสานงาน หากมีกลไกความร่วมมืออื่นๆ นอกเหนือจากกลไกของสหประชาชาติ อาทิ กลไกระดับภูมิภาค หรือกลไกอนุภูมิภาค ในการอำนวยความสะดวก และติดตามความช่วยเหลือทางเทคนิคของรัฐสมาชิกในการดำเนินการตามข้อมติเพื่อปราบปรามการเข้าถึงแหล่งการเงินของการก่อการร้าย¹⁷⁸

3.2.2 ข้อมูลเพื่อการปราบปรามกิจกรรมการมีส่วนร่วมทางการเงินกับการก่อการร้าย

3.2.2.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ในปัจจุบันพันธกรณีการแบ่งปันข้อมูลเพื่อดำเนินมาตรการต่อต้านทางการเงินของการก่อการร้ายได้ถูกเพิ่มขึ้นตามบริบทของเทคโนโลยีในสมัยใหม่ ที่ถูกนำมาเป็นเครื่องมือในการเข้าถึงแหล่งเงินของการก่อการร้าย ในข้อมติที่ 1373/2001, 2170/2014 และ 2199/2015 ทั้งสามข้อมติได้มีเป้าประสงค์ให้เกิดการแบ่งปันข้อมูลระหว่างรัฐสรุปได้ 2 ประการคือ

พันธกรณีประการแรกคือ “Respond” เพื่อการยับยั้งการเคลื่อนไหวของเงินที่ผิดกฎหมาย อาทิ เงินที่ได้มาจากการค้าอาวุธเถื่อน ค่าน้ำมัน การค้ามรดกทางวัฒนธรรม การลักพาตัวเพื่อเรียกค่าไถ่ รวมทั้งเงินที่ถูกเอาไปสนับสนุนการก่อการร้าย (Financial engagement to terrorism) ไม่ที่จะเป็นการสนับสนุนทางตรงหรือทางอ้อม ไม่ให้ตกอยู่ในการครอบครองของกลุ่มจัดตั้งรัฐอิสลามแห่งอิรักและลิแวนต์ (Islamic State of Iraq and the Levant – ISIL)¹⁷⁹

พันธกรณีประการที่สองคือ “Protect” ในทางตรงกันข้ามรัฐจะต้องมีมาตรการแบ่งปันข้อมูลเพื่อป้องกันไม่ให้กลุ่มก่อการร้ายดังกล่าวเข้าถึงเงินทุนเพื่อใช้ในกิจกรรมก่อการร้าย และประสิทธิภาพของการแบ่งปันข้อมูลของหน่วยข่าวกรองทางการเงิน (Financial intelligence unit) ของรัฐจะเกิดขึ้นได้ ก็ต่อเมื่อหน่วยงานทำหน้าที่เป็นตัวกลางประสานระหว่างหน่วยงานบังคับใช้กฎหมายของรัฐบาล อาทิ หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย กับสถาบันทางการเงินหรือภาคเอกชน ข้อมติที่ 2199/2015 ต้องการก่อให้เกิดการแบ่งปันข้อมูลการเงินแบบสื่อสารสองทาง¹⁸⁰ โดยที่หน่วยข่าวกรองทางการเงินอาจจัดทำคำแนะนำและข้อเสนอแนะ แก่สถาบันทางการเงินหรือภาคเอกชนที่เกี่ยวข้อง ให้ดำเนินการบันทึก

¹⁷⁸ United Nations Security Council Resolution 2253/2015, pp. 88-86

¹⁷⁹ United Nations Security Council Resolution 2170/2014, pp. 10

¹⁸⁰ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), p.3

ข้อมูลและแบ่งปันข้อมูลเท่าที่จำเป็นต่อการดำเนินมาตรการปราบปรามการเงินก่อการร้ายของ
ภาครัฐ¹⁸¹

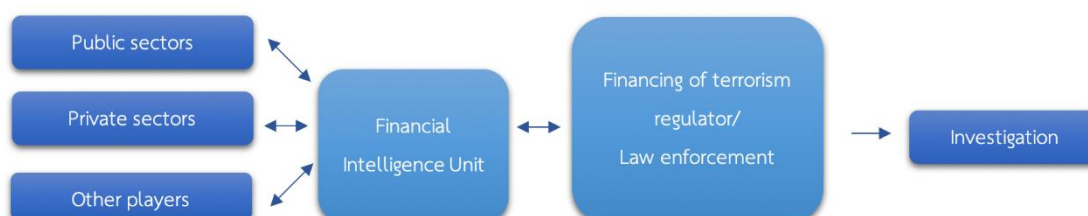
การแก้ปัญหาข้ามชาติ ในข้อมติที่ 2178/2014 ให้ขยายมาตรการในการแบ่งปันข้อมูล
เส้นทางการเงินไปยังนักรบต่างชาติ และการระดมเงินทุนขนาดใหญ่ผ่านช่องทางเทคโนโลยีการสื่อสารใน
หลายรูปแบบในปัจจุบันของกลุ่มก่อการร้ายต่างๆ

1. โครงสร้างของกระบวนการ

1.1 การจัดตั้งหน่วยข่าวกรองทางการเงิน

หน่วยข่าวกรองทางการเงินจะมีหน้าที่เป็นหน่วยงานกลางในการประสานข้อมูลทั้งระหว่าง
ประเทศ และภายในประเทศกล่าวคือระหว่างหน่วยงานของรัฐเอง และภาคเอกชนสาขาต่างๆ ที่ก่อตั้ง
ขึ้นภายใต้เขตอำนาจ¹⁸² และอยู่ภายใต้ตามกฎหมายภายใน อาทิ ธนาคารเอกชน ผู้ให้บริการ
อินเทอร์เน็ตเบคกิ้ง ผู้ให้บริการเครือข่ายการสื่อสารที่ก่อตั้งอยู่ในดินแดนที่รัฐนั้นมีอำนาจอธิปไตย
หรือเป็นบริษัทที่จดทะเบียนภายใต้กฎหมายของรัฐ แม้ว่าจะได้มีการให้บริการเครือข่ายนอกเขต
อำนาจของรัฐนั้นก็ตาม ให้ถือว่ารัฐได้มีอำนาจเหนือกิจการดังกล่าวตามหลักสัญชาติ โดยการจด
ทะเบียน รวมถึงสถาบันการเงินต่างๆ เพื่อให้ได้มาซึ่งข้อมูลเส้นทางการเงินของการก่อการร้ายที่อาศัย
เทคโนโลยีในปัจจุบัน ที่อาจจะกระทำผ่านระบบกระเป๋าเงินดิจิทัล (Mobile Payment) การ
แลกเปลี่ยนและการค้าสกุลเงินดิจิทัล การระดมทุนผ่านช่องทางสื่อสารในระบบอินเทอร์เน็ต ทั้งนี้จะ
เป็นข้อมูลให้หน่วยงานบังคับใช้กฎหมายดำเนินมาตรการที่ยั่งยืนกิจกรรมทางการเงินของการก่อการร้าย
หรือกลุ่มก่อการร้าย และป้องกันเงินเหล่านั้นมิให้เข้าสู่ระบบการเงินระหว่างประเทศ ซึ่งโครงสร้างการ
แบ่งปันข้อมูลระหว่างหน่วยงานต่างๆจะออกมาตามแผนผังด้านล่าง

แผนผังโครงสร้าง : การแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องภายในของรัฐ



¹⁸¹ United Nations Security Council Resolution 2199/2015, pp. 14

¹⁸² United Nations Security Council Resolution 1373/2001, pp. 3

เมื่อพิจารณาตามความจำเป็นในการได้มาซึ่งข้อมูลเส้นทางการเงินนั้น รัฐเองจะต้องมีความร่วมมือทั้งภายในประเทศและระหว่างประเทศ ในความร่วมมือภายในประเทศนั้นจะเกิดขึ้นระหว่างหน่วยข่าวกรองทางการเงิน ที่เป็นหน่วยงานกลาง และสถาบันทางการเงินต่างๆ (Financial institutions) อาทิ ธนาคาร ธุรกิจมูลค่าเงินทุกประเภท (Money-value business of all types) ธุรกิจการเงิน และอาชีพทางการเงิน (Financial professions) หรือแม้กระทั่งหน่วยงานของรัฐเอง จะต้องมีการแบ่งปันข้อมูลส่วนตัวของบุคคล อาทิ ข้อมูลประกันสังคม และข้อมูลการบันทึกภาษี จะนำมาสู่การได้ข้อมูลที่จำเป็นมากเพียงพอต่อการดำเนินมาตรการสอบสวนสืบสวนของหน่วยงาน ป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย

1.2 ความร่วมมือระหว่างประเทศ

ในความร่วมมือระหว่างประเทศต่อการสืบสวนทางการเงินของการก่อการร้าย (Terrorism-financing investigation) ที่อาจเกี่ยวพันในทางระหว่างประเทศ การแบ่งปันข้อมูลควรมีบทบาทที่สำคัญในการส่งเสริมมาตรการปราบปรามทางการเงินให้มีประสิทธิภาพยิ่งขึ้น รัฐควรจะต้องออกแบบกลไกการแบ่งปันข้อมูล เพื่อนำไปดำเนินมาตรการต่อต้านทางการเงินของหน่วยงานต่างๆภายในรัฐ ตน ที่มีอำนาจและหน้าที่ที่เกี่ยวข้อง ในขณะที่เดียวกันก็ควรจะมีช่องทางการให้ความช่วยเหลือทางคดีข้ามพรมแดนที่เกี่ยวกับเงินทุนเพื่อการก่อการร้าย (Cross-border terrorism-financing cases)¹⁸³

1.3 ความร่วมมือกับสถาบันทางการเงิน

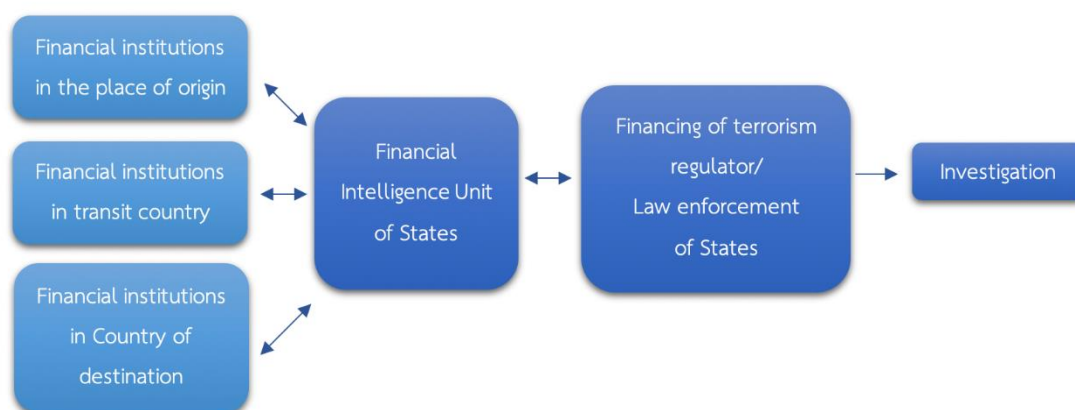
หน่วยงานบังคับใช้กฎหมาย จะต้องมีมาตรการที่เข้มงวด และสร้างกลไกในการเข้าถึงข้อมูลของสถาบันทางการเงินต่างๆ ในตรวจสอบการเงินและเส้นทางการเงิน ซึ่งก็ถือเป็นส่วนหนึ่งของแหล่งรายได้ของกลุ่มก่อการร้ายที่สำคัญ¹⁸⁴ โดยส่วนมากแล้วกลุ่มนี้กรบต่างชาติจะอาศัยการเงินของตัวเองในการเดินทางไปรวมรบ ซึ่งจะต้องมีการใช้เงินเพื่อเป็นค่าใช้จ่ายในการเดินทาง โดยมักจะดำเนินการถอนเงินผ่านสถาบันทางการเงินไม่ว่าจะตั้งอยู่ในประเทศต้นทาง (Place of origin) หรือประเทศทางผ่าน (Transit country) หรือประเทศที่เป็นจุดหมาย (Country of destination or conflict)

¹⁸³ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 413

¹⁸⁴ United Nations Security Council Resolution 2178/2014, pp. 11

zone)¹⁸⁵ ตามตลอดเส้นทางของการเดินทางของกลุ่มนักรบต่างชาติ ดังนั้นสถาบันทางการเงินที่เกี่ยวข้องจะต้องสามารถตรวจจับและดำเนินการส่งข้อมูลถึงหน่วยข่าวกรองทางการเงินของรัฐเพื่อดำเนินมาตรการปราบปรามได้ทันท่วงที ฉะนั้นแล้วหน่วยข่าวกรองทางการเงินจะมีบทบาทที่สำคัญในการวิเคราะห์ถึงการเข้าร่วมเดินทางของกลุ่มนักรบต่างชาติจากการแบ่งปันข้อมูลกับสถาบันทางการเงินต่างๆ

แผนผังโครงสร้าง : การแบ่งปันข้อมูลระหว่างหน่วยงานของรัฐและสถาบันการเงินต่างประเทศ



1.4 การประสานงาน

กระบวนการในการแบ่งปันข้อมูลเมื่อมีข้อมติที่ 1373/2001 ออกมาในภายหลังกำหนดว่าหน่วยงานบังคับใช้กฎหมายที่มีหน้าที่ในป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้ายของรัฐจะต้องมีหน้าที่แบ่งปันข้อมูลเพื่อทำการสืบสวนสอบสวนเส้นทางการเงินด้วย ซึ่งจำเป็นจะต้องสร้างหน่วยงานขึ้นมารับหน้าที่โดยเฉพาะเพื่อให้เกิดประสิทธิภาพในกระบวนการดำเนินการบังคับมาตรการ โดยส่วนตัวผู้เขียนเห็นควรว่าให้อำนาจหน้าที่เรื่องการประสานงาน ควรมอบหมายให้หน่วยข่าวกรองทางการเงินทั้งระดับภายในประเทศและระดับระหว่างประเทศ

1.5 ข้อท้าทาย

ตามการรายงานของสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ มีข้อสังเกตระบุว่ารัฐส่วนมากแล้วจะดำเนินการแบ่งปันข้อมูลทางการเงินผ่านช่องทางความช่วยเหลือซึ่ง

¹⁸⁵ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp.35-36

กันและกัน ต่อเมื่อมีคดีที่เกี่ยวข้องต่อการก่อการร้ายเกิดขึ้น เพื่อที่จะได้ทำการอายัดทรัพย์สิน ตามข้อมูลที่รัฐตนได้รับจากความช่วยเหลือของรัฐต่างชาติ แต่อย่างไรนั้นข้อมูลที่ได้ถูกแบ่งปันมาดังกล่าว ควรจะต้องมีกลไกพิจารณาจากหน่วยงานที่มีหน้าที่โดยเฉพาะ เช่น หน่วยงานข่าวกรองทางการเงิน หรือ หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ก่อนที่จะมีการดำเนินมาตรการในลักษณะเฉพาะ หรือควรที่จะแยกการดำเนินการแบ่งปันข้อมูลทางการเงินออกจากความช่วยเหลือซึ่งกันและกัน โดยรัฐต้องสร้างกลไกขึ้นมารับรองการดำเนินการแบ่งปันข้อมูลทางการเงินโดยเฉพาะ หรือมอบหมายให้เป็นหน้าที่ของหน่วยงานข่าวกรองทางการเงิน ทั้งนี้ก็เพื่อให้เกิดความคล่องตัวในการปฏิบัติงานของแต่ละหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะ และไม่เป็นการเพิ่มภาระที่มากเกินไปของหน่วยงานที่มีหน้าที่ให้ความช่วยเหลือซึ่งกันและกัน

2. ข้อมูลการบริการกระเป๋าเงินดิจิทัล

การบริการกระเป๋าเงินดิจิทัล (Mobile Payment)¹⁸⁶ คือการทำธุรกรรมการชำระเงินผ่านเครือข่ายของระบบโทรศัพท์มือถือ การเติบโตอย่างรวดเร็วของการใช้บริการเช่นนี้ในปัจจุบันนั้นได้ถูกระบุว่าเป็นช่องทางในการระดมทุนของการก่อการร้ายที่มีศักยภาพมากที่สุด ตามรายงานของรัฐมีการตรวจพบได้ในหลายๆเหตุการณ์โจมตีของการก่อการร้าย จำนวนเงินที่ใช้เพื่อก่อเหตุการณ์เหล่านั้นถูกระบุว่ามีการโอนผ่านช่องทางบริการกระเป๋าเงินดิจิทัล (Mobile money transfers)¹⁸⁷ แม้รัฐจำนวนไม่น้อยได้มีการออกกฎระเบียบว่าด้วยการโอนเงินหรือข้อบังคับของธนาคารว่าด้วยมาตรการต่อต้านการก่อการร้าย (Regulation on Anti-Terrorism money transfers)¹⁸⁸ แต่ก็มีความสามารถที่จะหยุดยั้งการโอนเงินระหว่างผู้โอน กับผู้รับโอนได้อย่างมีประสิทธิภาพ

ฉะนั้นหน่วยงานของรัฐมีความจำเป็นที่จะต้องร่วมมือกับสถาบันทางการเงินรวมถึงภาคเอกชนผู้ให้บริการโทรคมนาคม ในการติดตาม การโอนเงินผ่านมือถือที่มีความเสี่ยงว่าจะเกี่ยวข้องกับการก่อการร้าย โดยอาศัยการแบ่งปันข้อมูลต่อกันในการวิเคราะห์ เพื่อให้หน่วยงานบังคับใช้กฎหมายดำเนินมาตรการปราบปราม

¹⁸⁶ "การทำงานของกระเป๋าเงินดิจิทัลมีหลักการง่ายๆคือ การนำเงินสดไปเติม เพื่อเก็บไว้แบบดิจิทัลในกระเป๋าเงินอิเล็กทรอนิกส์ แล้วสามารถนำเงินดังกล่าวออกไปใช้จ่ายตามที่ต้องการ ความสะดวกของบริการกระเป๋าเงินดิจิทัล ผู้ใช้บริการสามารถหักเงินจากบัญชีธนาคารของตน เพื่อนำไปเติมในกระเป๋าเงินดิจิทัล แล้วใช้เงินที่มีในกระเป๋า" ที่มา: ไทยรัฐฉบับพิมพ์ 23 ส.ค. 2562

¹⁸⁷ Tom KEATINGE, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses," in *Director of the Centre for Financial Crime and Security Studies* (Royal United Services Institute, 2018).

¹⁸⁸ Security Council, *Eighth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range* (2019).

2.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ข้อมติที่ 2462/2019 ได้ถูกรับรองมาเพื่อแก้ปัญหาจากการที่ผู้ก่อการร้าย รวมถึงนักรบต่างชาติ และกลุ่มผู้ก่อการร้าย อาจดำเนินการเคลื่อนย้ายและโอนเงิน ผ่านสถาบันทางการเงิน หรือการใช้เทคโนโลยีของวิธีการชำระเงินที่ เช่น บัตรเติมเงิน การชำระเงินผ่านมือถือ หรือที่เรียกว่าบริการกระเป๋าเงินดิจิทัล หรือสินทรัพย์เสมือน คณะมนตรีความมั่นคงแห่งสหประชาชาติจึงได้เรียกร้องให้รัฐสมาชิก (Calls upon Member States) ส่งเสริมการเข้าถึงข้อมูลและความสามารถในการวิเคราะห์ทางการเงินของผู้ก่อการร้ายของหน่วยข่าวกรองทางการเงิน ต่อการพัฒนาบุคคลากรเจ้าหน้าที่ให้มีความสามารถในการสร้างตัวชี้วัดความเสี่ยง¹⁸⁹

2.2 กระบวนการ

ก. กระบวนการแบ่งปันข้อมูลเพื่อใช้วิเคราะห์ถึงเส้นทางการเงิน

ประการแรก บรรดารัฐสมาชิกจะต้องออกกฎหมายและระเบียบข้อบังคับ ให้อำนาจหน่วยข่าวกรองทางการเงิน ในการอาศัยการแบ่งปันข้อมูลหรือความสามารถในการเข้าถึงข้อมูลของภาคเอกชนภายใต้เขตอำนาจของตน เช่น ผู้ให้บริการโทรคมนาคม ผู้ให้บริการกระเป๋าเงินดิจิทัล (Digital wallet providers) หรือผู้ให้บริการสินทรัพย์เสมือน (Virtual asset service providers)

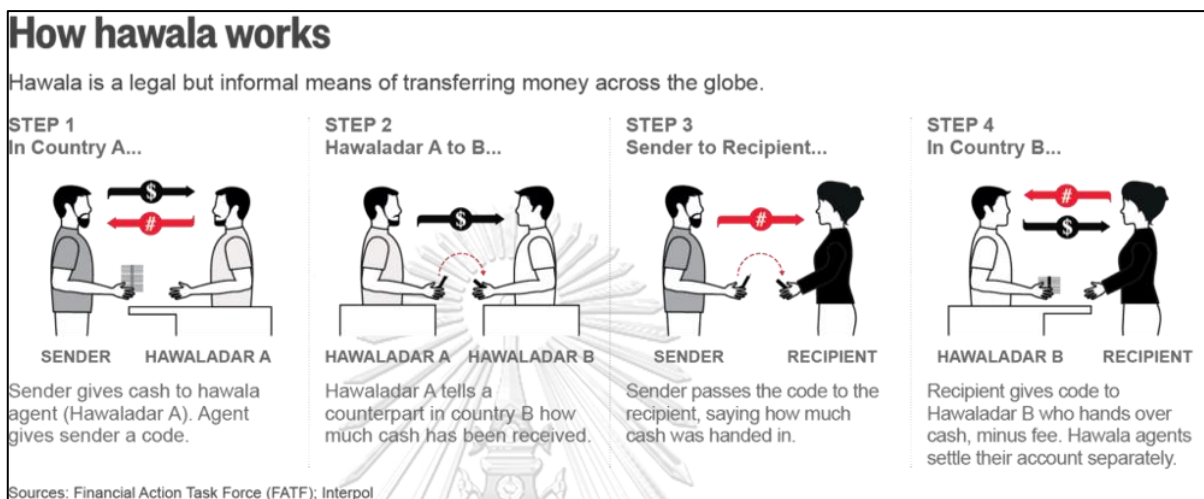
ทั้งนี้ข้อมูลที่รับมาเพื่อเสริมความสามารถต่อการวิเคราะห์ถึงวิธีการทางการเงิน (Financial means) ของการก่อการร้าย รวมถึงเรียกร้องให้มีการแบ่งปันข้อมูลระหว่างหน่วยงานภายในของรัฐเองด้วย อาทิ หน่วยข่าวกรอง หน่วยงานบังคับใช้กฎหมาย เจ้าหน้าที่อัยการหรือเจ้าหน้าที่ฝ่ายตุลาการ ในการรวบรวมและแบ่งปันข้อมูลทางการเงินของการก่อการร้าย

ประการที่สอง หน่วยข่าวกรองทางการเงิน เมื่อได้ข้อมูลจากภาคเอกชนที่เกี่ยวข้อง (Private stakeholders) แล้วจะต้องแบ่งปันข้อมูลต่อหน่วยงานบังคับใช้กฎหมาย เช่น หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการ เพื่อทำการสืบสวนสอบสวนต่อเส้นทางการเงิน เพราะจากประเด็นข้อท้าทายที่พบนั้นผู้ก่อการร้าย รวมถึงนักรบต่างชาติ และกลุ่มผู้ก่อการร้าย มิได้เป็นคนที่ใช้งานบริการกระเป๋าเงินดิจิทัลในการโอนเงินโดยตรง แต่จะกระทำผ่านนายหน้า หรือ “Hawala-type”¹⁹⁰ ซึ่งเป็นคนกลางในการใช้บริการกระเป๋าเงินดิจิทัลเพื่อการโอนเงิน

¹⁸⁹ United Nations Security Council Resolution 2462/2019, pp. 17,18,19

¹⁹⁰ "Hawala" เป็นวิธีการในการโอนเงินแบบไม่เป็นทางการโดยไม่มีกายการเงินจริง (Physical money) คำนิยามของ Interpol กล่าวว่าคือ "การโอนเงินโดยไม่มีกายการเงิน" คำจำกัดความอื่นก็คือ "Trust" Hawala ถูกนำมาใช้ในวันนี้เป็นช่องทางในการโอนเงินทางเลือกที่มีอยู่นอกกระบวนธนาคารแบบดั้งเดิม การทำธุรกรรมระหว่างโบรกเกอร์นั้นไม่มีการทำสัญญาใช้เงินเพราะระบบนี้มีพื้นฐานมาจากความไว้วางใจ *ที่มา: Investopedia* (<https://www.investopedia.com/terms/h/hawala.asp>)

ไปยังนายหน้าอีกคนแทน แม้ว่าหน่วยงานข่าวกรองทางการเงินและบริษัทเอกชนจะทราบถึงข้อมูลบัญชีของผู้ใช้งานบริการ แต่ผู้ใช้บริการเหล่านั้นอาจจะไม่ใช่ผู้ก่อการร้ายตัวจริง จึงจะต้องอาศัยการสืบสวนสอบสวนเพิ่มเติมและข้อมูลด้านข่าวกรองจากหน่วยงานรัฐอื่นๆด้วย¹⁹¹ การใช้บริการกระเป่าเงินดิจิทัลในการโอนเงินของ Hawala จะมีลักษณะดังรูปต่อไปนี้



อ้างอิงรูปภาพ URL: https://miro.medium.com/max/552/0*5wcOlB-ldtCO6ufs.png

ประการที่สาม จากข้อกังวลที่เกิดขึ้นมีการระบุว่ารัฐสมาชิกจำเป็นต้องเพิ่มความร่วมมือระมัดระวังต่อ เอกชนรายใหม่ หรือธนาคารขนาดเล็ก ที่ส่งเสริม Digital interfaces ให้แก่การบริการของตน เช่น บริการกระเป่าเงินดิจิทัลที่สามารถเข้าถึงบริการอย่างง่ายและรวดเร็ว รัฐสมาชิกควรจะต้องเข้มงวดเรื่องเงื่อนไขและข้อกำหนดต่อบริษัทเอกชนหรือธนาคารเอกชนก่อนที่จะอนุญาตการให้บริการกระเป่าเงินดิจิทัล เพราะผู้ก่อการร้ายอาจใช้ประโยชน์จากบริการของเอกชนและธนาคารเหล่านั้น เนื่องจากความสะดวกและรวดเร็วต่อการเปิดบัญชีกระเป่าเงินดิจิทัล และขั้นตอนการระบุตัวตนที่ไม่เข้มงวด¹⁹² ดังนั้นควรจะมีขั้นตอนของการตรวจสอบที่ชัดเจนในการอนุมัติ ซึ่งอาจอาศัยการออกข้อกำหนดที่รัดกุมออกมาโดยหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย

¹⁹¹ Security Council, "Letter dated 13 May 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp.21

¹⁹² Security Council, "Letter dated 3 June 2020 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 44

ในหลายประเทศในภูมิภาคยุโรปได้นำแนวทางปฏิบัตินี้ไปริเริ่ม จนพัฒนาออกมาเป็นโครงการที่ชื่อว่า “Black Wallet” มีการออกคู่มือ สำหรับหน่วยข่าวกรองทางการเงินภายในประเทศ ในการตรวจสอบเทคโนโลยีที่เกี่ยวข้องกับการบริการโอนเงิน และมุ่งเป้าไปที่การระบุ กับประเมิน ความเสี่ยงทางการเงินจากการก่อการร้ายและการฟอกเงินในภูมิภาค¹⁹³ และต่อมาโครงการก็ได้รับทุน สนับสนุนจากสหภาพยุโรป ยิ่งไปกว่านั้นโครงการได้จัดตั้งคณะทำงานที่ทำร่วมกันกับภาคเอกชน ใน การศึกษาเทคโนโลยีสินทรัพย์เสมือนจริง และเทคโนโลยีที่เกิดขึ้นใหม่ในปัจจุบันมีแนวโน้มที่จะเป็น ช่องทางการเงินใหม่ของการก่อการร้าย

2.3 เครื่องมือในการดำเนินการ

ก. แพลตฟอร์มสำหรับการทำงานร่วมกันระหว่างภาครัฐและภาคเอกชน

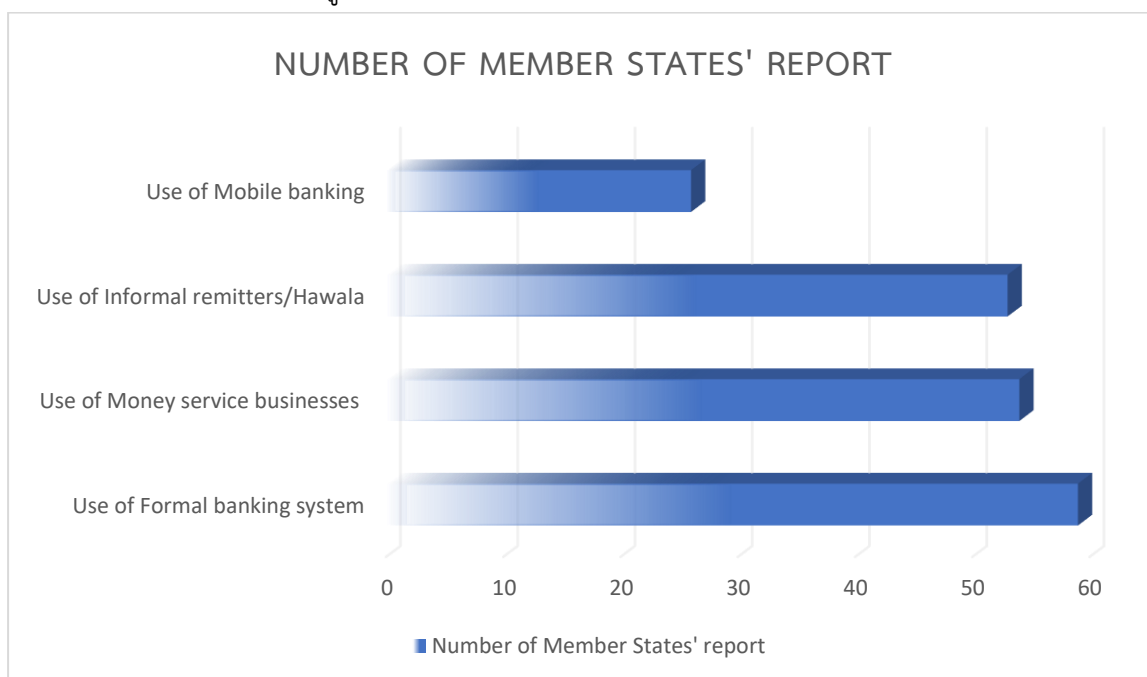
“Black Wallet Project” เป็นตัวอย่างที่เห็นได้ชัดของการพัฒนาแพลตฟอร์มที่จะส่งเสริม การมีส่วนร่วมของภาคเอกชน มีวัตถุประสงค์เพื่อสร้างแพลตฟอร์มสำหรับการทำงานทางข้อมูล ร่วมกันระหว่างภาครัฐและภาคเอกชน โดยเฉพาะกลุ่ม Financial Technology Firms¹⁹⁴ ในการระบุ ความเสี่ยงทางการเงินเพื่อการก่อการร้าย วิเคราะห์และประเมินความเสี่ยงให้ได้มาซึ่งข้อมูลเชิง คุณภาพ (Qualitative information) วัตถุประสงค์ของโครงการประกอบด้วย:

- 1.) ระบุตัวบ่งชี้ความเสี่ยงที่จะช่วยให้ภาคเอกชนตรวจจับและระบุธุรกรรมการเงินและ กิจกรรมทางการเงินที่น่าสงสัย
- 2.) ระบุมาตรการที่ประเมินความเสี่ยงและสามารถวัดได้ (Risk-mitigating measures) เพื่อ ปรับใช้กับบริการของเอกชนประเภทต่างๆที่เกี่ยวข้องกับการทำธุรกรรมการเงินผ่าน เทคโนโลยี
- 3.) เพื่อให้การฝึกอบรมแก่เจ้าหน้าที่ในหน่วยงานป้องกันและปราบปรามการฟอกเงินและ การต่อต้านการสนับสนุนเงินแก่การก่อการร้าย และพนักงานของกลุ่มบริษัทที่เกี่ยวข้อง กับการทำธุรกรรมการเงินผ่านเทคโนโลยี
- 4.) เพื่อให้การฝึกอบรมแก่เจ้าหน้าที่ในหน่วยงานป้องกันและปราบปรามการฟอกเงินและ การต่อต้านการสนับสนุนเงินแก่การก่อการร้ายเกี่ยวกับรูปแบบของการบริการของการ ทำธุรกรรมการเงินผ่านเทคโนโลยี
- 5.) เพื่อพัฒนาคู่มือสำหรับหน่วยข่าวกรองทางการเงิน เพื่อช่วยในการแบ่งปันข้อมูลเพื่อการ สืบสวนสอบสวน

¹⁹³ Ibid, pp. 43

¹⁹⁴ The Finnish and Swedish Police, "Black Wallet Project", (2019) Available from https://www.poliisi.fi/en/national_bureau_of_investigation/black_wallet

ข. การประสานข้อมูลกับเอกชนที่เกี่ยวข้องและความร่วมมือระหว่างประเทศ



อ้างอิงข้อมูลในแผนผัง : UN Document S/2020/493

เมื่อพิจารณาตามแผนผังจะสังเกตได้ว่าการก่อการร้ายส่วนใหญ่ยังคงใช้เทคโนโลยีในการเข้าถึงแหล่งเงินแบบระบบธนาคารอย่างเป็นทางการ (Formal banking system) เช่น การโอนเงินหรือการเข้าถึงแหล่งเงินในรูปแบบของระบบธนาคารปกติ ซึ่งจะแตกต่างกันอย่างชัดเจนเมื่อเปรียบเทียบกับตัวเลขรายงานของการใช้เทคโนโลยีแบบกระเป๋าสตางค์เงินดิจิทัล ทั้งนี้อาจจะเป็นเฉพาะผู้ก่อการร้ายเหล่านั้นเองที่อาศัยอยู่ในประเทศที่ยังไม่เข้าถึงเทคโนโลยีสมัยใหม่ อย่างไรก็ตามรัฐสมาชิกก็มีความกังวลเกี่ยวกับปัญหาดังกล่าว จะเห็นได้อย่างชัดเจนว่าแนวโน้มของการใช้บริการกระเป๋าสตางค์เงินดิจิทัลของกลุ่มก่อการร้ายมีปริมาณที่เพิ่มขึ้นอย่างเป็นนัยยะสำคัญ ประกอบกับมีเทคโนโลยีใหม่ๆ ที่ถูกพัฒนาขึ้นในปัจจุบันมีความเสี่ยงที่อาจจะตกเป็นเครื่องมือของการก่อการร้าย รัฐสมาชิกควรจะต้องมีมาตรการที่ชัดเจนในการควบคุมและร่วมมือทางข้อมูลกับภาคเอกชนหรือธนาคารผู้ให้บริการ

ในรายงานของคณะกรรมการการต่อต้านการก่อการร้าย ได้เผยว่ามีหลายรัฐสมาชิกได้ริเริ่มพัฒนามาตรการต่อต้านการเงินของการก่อการร้าย ที่อาศัยเทคโนโลยีในปัจจุบัน อาทิ กระเป๋าสตางค์ดิจิทัล และสร้างกลไกการประสานข้อมูลกับสถาบันและภาคเอกชนที่เกี่ยวข้องทั้งภายในประเทศและระหว่างประเทศ ในการประสานข้อมูลในระดับระหว่างประเทศนั้นบรรดารัฐสมาชิกได้อาศัยช่องทางในการดำเนินการผ่านองค์กรประสานงานต่อต้านการก่อการร้ายแห่งชาติ กระทรวงการ

ต่างประเทศ หรือผ่านเวทีการประสานงานและการแบ่งปันข้อมูลของกลุ่ม Egmont (the Egmont Group)¹⁹⁵ ซึ่งปัจจุบันมีหน่วยงานข่าวกรองทางการเงินของประเทศเป็นสมาชิกทั้ง 164 ประเทศ¹⁹⁶

ทั้งนี้เป็นที่น่าสังเกตว่ารัฐสมาชิกที่มีการดำเนินมาตรการแบ่งปันข้อมูลที่เป็นไปอย่างมีประสิทธิภาพนั้น โดยส่วนมากแล้วจะอาศัยกลไกของกฎหมายระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้าย¹⁹⁷ เช่น การเข้าเป็นภาคีอนุสัญญาว่าด้วยการต่อต้านการก่อการร้ายและพิธีสารที่เกี่ยวข้องของสหประชาชาติ 19 ฉบับ ซึ่งเพียงพอต่อการอำนวยความสะดวกต่อการแบ่งปันข้อมูลและเสริมสร้างความร่วมมือระหว่างประเทศในการต่อต้านการก่อการร้าย

3. ข้อมูลการบริการสินทรัพย์เสมือน

สินทรัพย์เสมือน คือ สินทรัพย์ที่เปรียบเทียบเป็นการแสดงถึงค่าสกุลเงินในบางสถานการณ์ ซึ่งสกุลเงินเหล่านี้สามารถกำหนดเป็นสื่อกลางในการแลกเปลี่ยนทรัพย์สินที่มีมูลค่า ในกิจกรรมที่เฉพาะเจาะจง เช่น เงินในระบบเกม หรือแบบจำลองการซื้อขายทางการเงิน (Financial trading simulation) สินทรัพย์เสมือนมักเรียกในอีกชื่อว่า "เงินเสมือน" (Virtual currency)¹⁹⁸ อาจแบ่งได้ตามคุณสมบัติการใช้งานได้ใน 3 รูปแบบคือ

1. รูปแบบเงินเสมือนที่ไม่สามารถใช้ซื้อสินค้าจริงได้และแลกเปลี่ยนเป็นเงินจริงไม่ได้ โดยรับมาจากโลกออนไลน์ด้วยกิจกรรมต่างๆ เช่น การเล่นเกมออนไลน์แล้วได้รับแต้มหรือเงินเสมือน แต่จะใช้ได้ก็ต่อเมื่อใช้ในโลกออนไลน์ได้เท่านั้น
2. รูปแบบใช้เงินจริงแลกเปลี่ยนเป็นเงินเสมือน แต่ไม่สามารถแลกเปลี่ยนกลับมาเป็นเงินจริงได้ เช่น Facebook Credit ซึ่งจะสามารถใช้ซื้อสินค้าและบริการออนไลน์หรือแอปพลิเคชันต่างๆได้

¹⁹⁵ “The Egmont Group คือ กลุ่มหน่วยข่าวกรองทางการเงิน เป็นองค์การระหว่างประเทศที่อำนวยความสะดวกในการร่วมมือและการแบ่งปันข่าวกรองระหว่างหน่วยข่าวกรองทางการเงินแห่งชาติ (Financial intelligence units FIUs) เพื่อตรวจสอบและป้องกันการฟอกเงินและการจัดหาเงินทุนของผู้ก่อการร้าย – มีหน่วยงานประเทศไทยเป็นภาคีสมาชิกคือ สำนักงานป้องกันและปราบปรามการฟอกเงิน”

¹⁹⁶ The Egmont Group, "About Egmont Group of Financial Intelligence Units" (2020) Available from <https://egmontgroup.org/en/content/about>

¹⁹⁷ Security Council, "Letter dated 3 June 2020 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 47

¹⁹⁸ Techtargt, "Definition of virtual asset" (2020), Retrieved from <https://whatis.techtargt.com/definition/virtual-asset>

3. รูปแบบที่สามารถใช้เงินจริงแลกเปลี่ยนกับเงินเสมือนได้ทั้งสองทาง สามารถใช้ซื้อของได้ทั้งในโลกออนไลน์และโลกจริง ดังในกรณีของ Cryptocurrency เช่น Bitcoin ที่เคยได้รับความสนใจอยู่ในขณะหนึ่ง ซึ่งจะได้กล่าวต่อในหัวข้อถัดไป¹⁹⁹

สินทรัพย์เสมือน เป็นที่นิยมในยุคสมัยปัจจุบันที่เป็นสังคมไร้เงินสด) โดยคุณสมบัติและลักษณะการใช้งานของสินทรัพย์เสมือนที่อยู่บนระบบออนไลน์ ไร้พรมแดนของการเคลื่อนย้าย และมีเครือข่ายแบบ Peer-to-Peer จึงนับว่ามีแนวโน้มที่จะตกอยู่ในความเสี่ยงต่อการใช้งานของการก่อการร้ายในการทำธุรกรรมทางการเงินที่อยู่นอกเหนือจากควบคุมของรัฐ²⁰⁰ และข้อที่น่ากังวลคือแบบแพลตฟอร์มที่ไม่เปิดเผยชื่อ (Anonymity) แต่ใช้ชื่อในลักษณะของนามแฝง (Pseudonymity) ซึ่งสามารถทำการปกปิดธุรกรรมทางการเงินที่ผิดกฎหมายได้

3.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ข้อมติที่ 2462/2019 ได้เรียกร้องให้บรรดารัฐต่างๆ (Calls upon all States) มีการแบ่งปันข้อมูลกับภาคเอกชนผู้ให้บริการสินทรัพย์เสมือน เพื่อเพิ่มความสามารถในการติดตามและตรวจสอบความโปร่งใสของบริการธุรกรรมทางการเงิน²⁰¹ อาทิ การตรวจสอบย้อนกลับ (Traceability)²⁰² พร้อมสนับสนุนให้หน่วยงานของรัฐที่เกี่ยวข้องกับการแบ่งปันข้อมูลและต่อต้านการก่อการร้าย พัฒนาศักยภาพทางเทคโนโลยีของตน เช่น เทคโนโลยีทางการเงิน (Financial technologies) และ "เร็กเทค" หรือ "RegTech" (Regulatory technologies) คือเทคโนโลยีที่มาเพิ่มประสิทธิภาพให้กับงานกำกับดูแล ไม่ว่าจะเป็นการดูแลเรื่องความปลอดภัย การรักษาความมั่นคงของระบบการเงิน การจัดส่งข้อมูล การประมวลผล วิเคราะห์ติดตามผล และการสร้างรีพอร์ตเพื่อให้ผู้ใช้งานเข้าถึงข้อมูลได้อย่างถูกต้องและรวดเร็ว²⁰³

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

¹⁹⁹ กันตภณ ศรีชาติ, "เงินเสมือน (Virtual Currency) ต่างจากเงินจริงอย่างไร", สำนักนโยบายการออมและการลงทุน, ธนาคารแห่งประเทศไทย (2017), Available from

https://www.bot.or.th/Thai/ResearchAndPublications/DocLib/_article20_08_13.pdf

²⁰⁰ Tom KEATINGE, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses", Director of the Centre for Financial Crime and Security Studies, Royal United Services Institute (2018), p.9

²⁰¹ United Nations Security Council Resolution 2462/2019, pp. 20 (a), (b), (c), (d)

²⁰² "การตรวจสอบย้อนกลับ" คือความสามารถในการติดตามธุรกรรมทางธุรกิจกลับไปยังเอกสารต้นทาง เป็นแนวคิดหลักสำหรับผู้ตรวจสอบบัญชี กล่าวคือเป็นระบบที่มีการตรวจสอบย้อนกลับระดับสูงเพื่อช่วยในการตรวจสอบธุรกรรมและการเงินของลูกค้า ที่มา: Accountingtools (<https://www.accountingtools.com/articles/2017/5/15/traceability>)

²⁰³ Digital Ventures, "ทำความรู้จักกับ RegTech" (2017), Retrieved from <http://dv.co.th/blog-th/get-to-know-regtech>

3.2 กระบวนการ

1. กระบวนการแบ่งปันข้อมูลเพื่อติดตามความโปร่งใสของธุรกรรมออนไลน์

ประการแรก รัฐจะต้องมีการดำเนินการให้หน่วยข่าวกรองทางการเงิน และหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย มีมาตรการดังต่อไปนี้

1. การแบ่งปันข้อมูลความเสี่ยงของเงินที่อาจเกี่ยวข้องกับกรก่อการร้าย กับสถาบันทางการเงิน รวมทั้งหน่วยธุรกิจและผู้ประกอบอาชีพที่มีใช้สถาบันการเงิน (Designed Non-Financial Businesses and Professions – DNFBPs)²⁰⁴ ซึ่งก็รวมถึง ผู้ให้บริการสินทรัพย์เสมือน (Virtual assets service providers) ด้วย
2. ลักษณะของข้อมูลที่ใช้ต่อการแบ่งปันข้อมูล จะต้องเป็นข้อมูลที่ครอบคลุมเพียงพอต่อการเอาผิดทางอาญา (Comprehensive information on criminal schemes)
3. เมื่อได้รับข้อมูลจากผู้ให้บริการแล้ว ต้องทำการประเมินและจัดการกับความเสี่ยงที่อาจเกิดขึ้นเกี่ยวกับการให้บริการสินทรัพย์เสมือน ซึ่งหน่วยข่าวกรองทางการเงินและหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย จะต้องมีกระบวนการและข้อบังคับมารองรับให้มีอำนาจในการตรวจสอบ

ประการที่สอง ข้อเสนอนี้ยังได้เสนอให้รัฐดำเนินการตาม “Guidance for a risk-based approach virtual assets and virtual asset service providers”²⁰⁵ ที่ ถูก รับ รอง ขึ้น จาก คณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Financial Action Task Force – FATF) ในมาตรการของเรื่องแบ่งปันข้อมูลระหว่างหน่วยงานของรัฐกับสถาบันการเงิน ภาคเอกชน หรือ รวมทั้งหน่วยธุรกิจและผู้ประกอบอาชีพที่มีใช้สถาบันการเงิน ซึ่งจะอธิบายได้ตามตารางต่อไปนี้

ตาราง : การแบ่งปันข้อมูลระหว่างหน่วยงานของรัฐกับเอกชนในเรื่อง Virtual assets

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐและภาคเอกชนมีความสำคัญในการต่อต้านการฟอกเงินและการสนับสนุนเงินแก่การก่อการร้ายที่เกี่ยวข้องกับสินทรัพย์เสมือน (Virtual

²⁰⁴ "Types of "non-financial" businesses have been identified as being susceptible to money laundering and terrorist financing due to the nature of their business and the transactions with activity that they may conduct" ที่มา: *Department of Commerce and Investment* (<https://www.dci.gov.ky/what-is-dnfbp>)

²⁰⁵ Financial Action Task Force, "Guidance for a risk-based approach virtual assets and virtual asset service providers" (2019), Available from <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>

Asset) และผู้ให้บริการสินทรัพย์เสมือน (Virtual Asset Service Provider) ประเภทของข้อมูลที่เกี่ยวข้องกับความเสี่ยงในใช้บริการสินทรัพย์เสมือนที่ภาครัฐและเอกชนควรแบ่งปันข้อมูลต่อกันคือ

ประเภท	ลักษณะของข้อมูลที่ต้องทำการแบ่งปัน
A	ข้อมูลการประเมินความเสี่ยง (Risk assessment) ของการฟอกเงินและการสนับสนุนการเงินของการก่อการร้าย
B	ข้อมูลหลักเกณฑ์การจำแนกประเภทระหว่างฟอกเงินกับการระดมทุนการก่อการร้าย และข้อมูลวิธีการของนักฟอกเงิน (Launderers) หรือนักระดมทุนของการก่อการร้าย (Terrorist financier) ที่ได้ใช้ประโยชน์จากบริการของผู้ให้บริการสินทรัพย์เสมือน (Virtual Asset Service Provider) ในทางที่ผิด เช่น ข้อมูลการโอนสินทรัพย์เสมือน (Virtual assets transfer), ข้อมูลของการแลกเปลี่ยนสินทรัพย์ (Exchange activities), ข้อมูลของการกระทำอันเป็นที่สงสัย (Issuance activities) ในบริบทว่าจะเกี่ยวข้องต่อการฟอกเงินและการสนับสนุนการเงินของการก่อการร้าย, หรือข้อมูลทั่วไปของสินทรัพย์เสมือน
C	ข้อมูลข้อเสนอแนะทั่วไป (General feedback), รายงานการทำธุรกรรมที่น่าสงสัยที่มีข้อมูลเชิงคุณภาพและเป็นประโยชน์ The quality and usefulness of suspicious transaction report (STRs) และรายงานอื่นๆที่เกี่ยวข้อง
D	ข้อมูลเกี่ยวกับตัวชี้วัดที่น่าสงสัย (Information on suspicious indicators) ต่อการใช้บริการสินทรัพย์เสมือน (Virtual Asset) และข้อมูลการทำธุรกรรมของผู้ให้บริการสินทรัพย์เสมือน (Virtual Asset Service Provider Transactions)
E	ข้อมูลในกลุ่มเป้าหมายจากหน่วยข่าวกรอง (Targeted intelligence) ซึ่งข้อมูลนั้นต้องมีความจำเป็นต่อการดำเนินมาตรการป้องกัน (Safeguards) ของหน่วยงานรัฐ เช่น ข้อมูลที่อยู่ภายใต้ข้อตกลงว่าด้วยการรักษาความลับ (Confidentiality agreement)
F	ข้อมูลของประเทศ บุคคล หรือองค์กร ผู้เป็นเจ้าของสินทรัพย์เสมือนหรือการทำธุรกรรมที่เกี่ยวข้องกับสินทรัพย์เสมือนที่ถูกดำเนินมาตรการลงโทษทางการเงิน (Financial sanction) แต่ต้องถูกร้องขอให้แบ่งปันข้อมูลตาม “Recommendation 6 of FATF”

ผู้เขียนขออธิบายเพิ่มเติมในส่วนของข้อมูลประเภท F กล่าวคือ “*Recommendation 6 of FATF*”²⁰⁶ นั้นถูกรับรองอยู่ใน The FATF Recommendations ของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน มีการอธิบายว่า ข้อมติโดยคณะมนตรีความมั่นคงแห่งสหประชาชาติกำหนดให้บรรดาระัฐต่างๆ ต้องอายัดทรัพย์สินโดยไม่ชักช้า รวมถึงเงินหรือทรัพย์สินอื่นๆ เพื่อให้แน่ใจว่าจะไม่มีเงินทุน หรือสินทรัพย์อื่นใดที่มีอยู่ไม่ว่าทางตรงหรือทางอ้อม เพื่อประโยชน์ของบุคคลหรือนิติบุคคลใด ๆ

- บุคคลหรือนิติบุคคลที่กำหนดโดยคณะมนตรีความมั่นคงแห่งสหประชาชาติซึ่งได้ใช้อำนาจภายใต้หมวดที่ 7 ของกฎบัตรสหประชาชาติ²⁰⁷
- บุคคลหรือนิติบุคคลที่กำหนดโดยข้อมติที่ 1267/1999 และข้อมติที่มีการอ้างถึง
- บุคคลหรือนิติบุคคลที่ถูกกำหนดโดยรัฐโดยอาศัยตามข้อมติ 1373/2001 และข้อมติที่มีการอ้างถึง

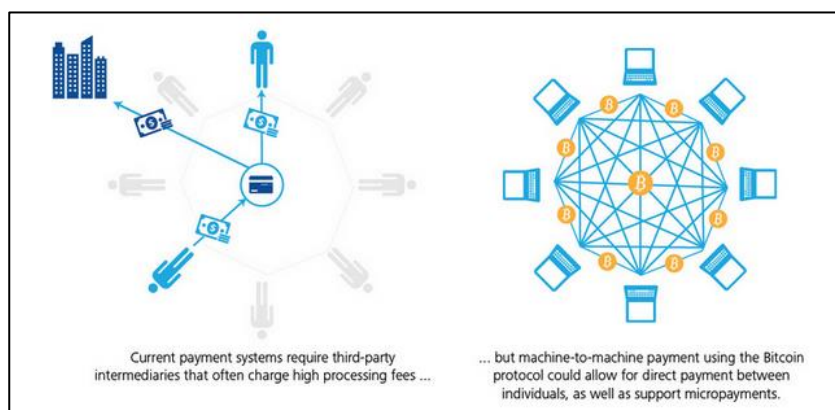
ดังนั้นจึงถือได้ว่าสินทรัพย์เสมือนก็อยู่ในขอบข่ายของทรัพย์สินอื่นๆ ตามข้อมติของคณะมนตรีความมั่นคงในการดำเนินการมาตรการลงโทษทางการเงิน กับผู้เป็นเจ้าของสินทรัพย์เสมือนหรือการทำธุรกรรมที่เกี่ยวข้องกับสินทรัพย์เสมือนนั่นเอง อย่างไรก็ตามสินทรัพย์เสมือน ในปัจจุบันได้ถูกพัฒนาให้อยู่ในหลากหลายรูปแบบตามประเภทของการใช้งานและบริการของผู้ให้บริการ

²⁰⁶ Financial Action Task Force, "The FATF Recommendations" (2012), p.11, Available from <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendation%202012.pdf>

²⁰⁷ สุทธิพร สายเชื้อ, "ปัญหาและอุปสรรคในการดำเนินการตามมาตรการในพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้าย พ.ศ. 2556 : ศึกษากรณีธุรกิจประกันชีวิต" (จุฬาลงกรณ์มหาวิทยาลัย, ปีพ.ศ. 2558). สุทธิพร สายเชื้อ, "ปัญหาและอุปสรรคในการดำเนินการตามมาตรการในพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้าย พ.ศ. 2556 : ศึกษากรณีธุรกิจประกันชีวิต" (หน้า 144 จุฬาลงกรณ์มหาวิทยาลัย, ปีพ.ศ. 2558).

3.3 ข้อท้าทายใหม่ของสินทรัพย์เสมือน

ก. บล็อกเชน (Blockchain) หรือระบบโครงข่ายในการเก็บบัญชีธุรกรรมออนไลน์



อ้างอิงรูปภาพ

URL: <https://storage.googleapis.com/techsauce-prod/uploads/2016/04/blockchain.png>

“Blockchain” เปรียบเสมือนห่วงโซ่ที่สร้างขึ้นเพื่อกระจายข้อมูลเก็บไว้ในชิ้นส่วนโซ่ที่ต่อกัน แต่ข้อมูลเหล่านั้นจะไม่สามารถถูกเปลี่ยนแปลงได้ หรือจะอธิบายได้ว่า “Blockchain” นั้นเป็น อินเทอร์เน็ตในรูปแบบใหม่โดยเริ่มแรกถูกสร้างขึ้นมาเพื่อสร้างสกุลเงินดิจิทัล (Cryptocurrency)²⁰⁸ เมื่อธุรกรรมต่างๆ ถูกบันทึกในบล็อกเหล่านี้แล้ว จะไม่มีใครสามารถเข้าไปเปลี่ยนแปลงข้อมูลใดๆ ได้ เพราะทุกผู้ใช้งานต่างก็มีสำเนาหรือประวัติการทำธุรกรรมทั้งหมดอยู่กับตัว จึงเป็นเรื่องที่เป็นไปไม่ได้เลย ที่ใครจะมาปลอมแปลงข้อมูล โดยปราศจากการรับรู้ ดังนั้นผู้ก่อการร้ายจึงใช้เทคโนโลยีนี้ในการ ระดมเงินทุน แต่อย่างไรก็ตามแม้จะไม่ทราบว่าใครใดเป็นผู้ทำธุรกรรม แต่สามารถหาร่องรอยของ บุคคลผู้ทำธุรกรรมได้ที่ทิ้งไว้ในบัญชี ซึ่งอาจจะสามารถสืบตามภายหลังได้โดยการร่วมมือกับผู้ ให้บริการ Blockchain²⁰⁹ ซึ่งเป็นก็เป็นเรื่องยากที่ผู้ก่อการร้ายจะปกปิดร่องรอยได้ทั้งหมด

หน่วยข่าวกรองทางการเงิน และหน่วยงานป้องกันและปราบปรามการฟอกเงินและการ ต่อต้านการสนับสนุนเงินแก่การก่อการร้าย จะสามารถติดตามข้อมูลของการทำธุรกรรมที่น่าสงสัยว่า

²⁰⁸ Jeerichuda Juntrabut, "เทคโนโลยี Blockchain คืออะไร และมันจะมาเปลี่ยนโลกได้อย่างไร" (2017)

Retrieved from <https://siamblockchain.com/2017/06/04/blockchain-คืออะไร/>

²⁰⁹ C. Edward Kelso, "Terrorists Prefer Cash to Crypto, According to Congressional Testimony" (2018) Retrieved from <https://news.bitcoin.com/terrorists-prefer-cash-to-crypto-according-to-congressional-testimony/>

จะเกี่ยวข้องกับการระดมเงินทุนเพื่อการก่อการร้ายผ่านบล็อกเชนได้จากการร่วมมือข้อมูลกับบริษัทผู้ให้บริการ Blockchain ต่างๆ (Blockchain Service Providers) โดยการดำเนินการตาม “Guidance for a risk-based approach virtual assets and virtual asset service providers” ที่ได้อธิบายในหัวข้อที่ข้างต้น

ข. สกุลเงินดิจิทัล (Cryptocurrency)

สกุลเงินดิจิทัล คือ สินทรัพย์เสมือนประเภทหนึ่ง หรือที่เรียกกันว่า 'สกุลเงินดิจิทัล' เนื่องจากมันไม่ได้มีรูปที่จับต้องได้ ไม่ได้มีลักษณะทางกายภาพ เช่นเดียวกับกับ สกุลเงินทั่วไป อย่าง ดอลลาร์สหรัฐฯ หรือเงินยูโร โดยทั่วไปสกุลเงินดิจิทัลจะไม่ได้อยู่ภายใต้การควบคุมหรือจัดการโดยหน่วยงานทางการเงินหรือธนาคารใดๆ เหมือนสกุลเงินแบบดั้งเดิม แต่จะเป็นการ 'ควบคุมด้วยตัวผู้ใช้งานเอง' ผ่านการใช้เทคนิคการเข้ารหัสที่มีความซับซ้อนและหลากหลายรูปแบบ²¹⁰ นอกจากนี้ ผู้ใช้ภายในเครือข่ายเดียวกัน จะมีส่วนร่วมกันทั้งระบบในกระบวนการทำธุรกรรมของสกุลเงินดิจิทัลผ่านอินเทอร์เน็ต ซึ่งเป็นลักษณะของการ 'ยืนยันการทำธุรกรรม' ของผู้ใช้ในเครือข่ายเดียวกัน สกุลเงินดิจิทัลเดียวกันให้แก่กันและกัน ดังนั้นลักษณะของการทำธุรกรรมของสกุลเงินดิจิทัล จะมีลักษณะแบบกึ่งไม่ระบุชื่อทำให้เหมาะสำหรับเป็นที่พักพิงของกิจกรรมที่เลวร้าย เช่น การฟอกเงิน การหลีกเลียงภาษี และการระดมทุนของการก่อการร้าย ซึ่งผู้ใช้งานสกุลเงินดิจิทัลส่วนมากจะมักให้ความสำคัญกับการไม่เปิดเผยตัวตน

ค. การพนันเสมือนจริง (Virtual gambling) และ คาสิโนออนไลน์ (Casino online platforms)

การแบ่งปันข้อมูลต่อสินทรัพย์เสมือนยังได้ครอบคลุมไปถึงการพนันเสมือนจริง (Virtual gambling) และ คาสิโนออนไลน์ (Casino online platforms) เพราะมีรายงานจากรัฐว่าการก่อการร้ายได้อาศัยช่องในแพลตฟอร์มคาสิโนออนไลน์ทำการระดมเงินทุน ซึ่งทั้งนี้ได้เรียกร้องให้รัฐได้มีมาตรการการควบคุมที่เข้มงวด (Stricter controls) และการตรวจสอบประวัติการให้บริการของผู้ให้บริการ คาสิโน²¹¹ และประวัติการใช้บริการของผู้เล่นเพื่อเป็นข้อมูลในการดำเนินการต่อต้านการเงินของการก่อการร้ายของหน่วยข่าวกรองทางการเงินและหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย

²¹⁰ Admiral Markets, "Cryptocurrency คือ : พื้นฐานการลงทุนสกุลเงินดิจิทัล" (2017), Retrieved from <https://admiralmarkets.com/th/education/articles/cryptocurrencies/trading-cryptocurrency-guide>

²¹¹ Security Council, "Letter dated 3 June 2020 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 44

4. ข้อมูลการระดมทุนผ่านระบบอินเทอร์เน็ต

ข้อมูลการระดมทุนผ่านระบบอินเทอร์เน็ต (Fundraising on the Internet) สื่อสังคมออนไลน์ในปัจจุบันที่อยู่ในระบบอินเทอร์เน็ตกำลังกลายเป็นเครื่องมือส่วนหนึ่งของการก่อการร้ายที่หันมาใช้พื้นที่ของสังคมออนไลน์ในการประชาสัมพันธ์แนวความคิดความเชื่อ (Propaganda) และการระดมทุนทรัพย์ที่จะนำไปใช้ในกิจกรรมการก่อการร้ายต่างๆ ผู้ก่อการร้ายเข้าใจระบบการทำงานพื้นฐานของสังคมออนไลน์ได้ค่อนข้างดี เพราะแพลตฟอร์มเหล่านี้ใช้งานได้โดยมิต้องสร้างบัญชีที่เปิดเผยตัวตน (Anonymity)²¹² ภายหลังเหตุการณ์วินาศกรรม 9/11 การเติบโตของการระดมทุนผ่านระบบอินเทอร์เน็ตของการก่อการร้ายได้มีตัวเลขที่สูงขึ้นซึ่งเหตุผลหลักๆ สามารถอธิบายได้ว่าระบบอินเทอร์เน็ตสามารถเป็นเครือข่ายที่มีผู้คนมาใช้งานจำนวนมากกว่า 800 ล้านคนและจะมีจำนวนเพิ่มขึ้นเรื่อยๆ จึงง่ายต่อกลุ่มก่อการร้ายที่พยายามจะนำเสนอแนวความคิดความเชื่อของตนเองผ่านเครือข่ายอินเทอร์เน็ตในกระจายข้อมูลของตนไปถึงผู้คนให้ได้มากที่สุด เมื่อชุดแนวคิดของการก่อการร้ายได้รับการตอบสนองจากคนที่มีแนวความคิดความเชื่อเหมือนกัน หรือลัทธิสุดโต่งทางความคิด (Fundamentalism) ก็จะเกิดความอยากสนับสนุนกลุ่มก่อการร้ายและวาระซ่อนเร้น (Hidden agenda) ทางความคิดที่จะนำไปสู่การก่อเหตุโจมตี

ผู้ระดมทุนของการก่อการร้ายชื่อนาย Babar Ahmad สัญชาติอังกฤษได้เผยว่าเขาเข้าร่วมกับกลุ่ม Taliban in Afghanistan และ นักรบญิฮาด (Jihadist) โดยหน้าที่หลักของเขาคือการโพสภาพและคลิปวิดีโอกิจกรรมของกลุ่ม พร้อมข้อความประชาสัมพันธ์ผ่าน Webhosting service และสื่อสังคมออนไลน์ต่างๆ เช่น Twitter ซึ่งการประชาสัมพันธ์จะเน้นไปที่การโน้มน้าวบุคคลที่มีความคิดความเชื่อเหมือนกันให้ช่วยเหลือทางด้านทุนทรัพย์²¹³ ในทำนองที่ว่า "การสนับสนุนญิฮาดเป็นภาระหน้าที่ของมุสลิมทุกคน" และ "หากบุคคลหนึ่งไม่สามารถไปรบในญิฮาดได้ เขาคงนั้นมีพันธะทางศาสนาที่จะต้องสนับสนุนทางทุนทรัพย์" ประกอบกับการบอกรายละเอียดของการโอนเงิน และการประชาสัมพันธ์ ในหลายรูปแบบของช่องทางในการทำธุรกรรม เช่น การโอนเงินไปที่ปลายทางหนึ่งไปยังอีกปลายทางหนึ่ง

²¹² Stacey Yuen, "Terror financiers are using social media propaganda" (December, 2017), CNBC news, <https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html>

²¹³ Michael Jacobson, "Terrorist Financing and the Internet," in *Studies in Conflict & Terrorism*, Bruce Hoffman (Washington, D.C., USA: 2010).

4.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ในข้อมติที่ 2462/2019 เรียกร้องให้บรรดารัฐสมาชิก (Calls upon Member States) เสริมสร้างความร่วมมือระหว่างประเทศเพื่อป้องกันและต่อต้านการระดมทุนของการก่อการร้ายซึ่งสามารถอธิบายได้ตามนี้²¹⁴

4.2 กระบวนการ

ประเด็นแรก รัฐสมาชิกจะต้องมีการสร้างกลไกประสานงานในทั้งระดับทวิภาคีและพหุภาคี โดยที่หน่วยข่าวกรองทางการเงิน สามารถที่จะทำการแบ่งปันข้อมูลระหว่างกันกับหน่วยงานของรัฐสมาชิกอื่นๆ ที่อยู่ภายใต้ไคกลไกความร่วมมือเดียวกันนั้น และจะต้องมีการออกกฎระเบียบและข้อบังคับภายในให้อำนาจเจ้าพนักงานที่เกี่ยวข้องต่อการแบ่งปันข้อมูล มีความสามารถตอบรับความคำขอความช่วยเหลือจากหน่วยงานต่างประเทศ

ประเด็นที่สอง หน่วยข่าวกรองทางการเงิน ของรัฐสมาชิกจะทำหน้าที่เป็นหน่วยงานกลาง ในการรับเรื่องการรายงานจาก หน่วยที่เสนอรายงานต่างๆ เกี่ยวกับธุรกรรมที่น่าสงสัยและข้อมูลอื่นที่เกี่ยวข้องกับการฟอกเงินหรือรายงานเกี่ยวกับการทำธุรกรรมที่ยืนยันแล้วว่าผิดกฎหมาย รวมทั้งการจัดหาเงินทุนของการก่อการร้าย ซึ่งรัฐสมาชิกจะต้องตรวจสอบเพื่อให้แน่ใจว่าหน่วยข่าวกรองทางการเงิน ได้แบ่งปันข้อมูลผ่านช่องทางที่มีการป้องกันอย่างปลอดภัยต่อการเผยแพร่ข้อมูลและผลการวิเคราะห์นั้นไปยังหน่วยงานที่สามอีกต่อไป

ประเด็นที่สาม ให้ดำเนินการแบ่งปันข้อมูลระหว่างหน่วยข่าวกรองทางการเงิน โดยเฉพาะ ข้อมูลของผู้ก่อการร้ายในรายบุคคล ที่อาจจะทำหน้าที่เป็นผู้ระดมทุนเพื่อการก่อการร้าย ผู้สะสมทุนเพื่อการก่อการร้าย และผู้อำนวยการความสะดวกเพื่อการก่อการร้าย โดยยึดหลักการของการดำเนินการตามมาตรฐานของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Standards of Financial Action Task Force – FATF)

ในรายงานของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน ได้เปิดเผยว่าปัจจุบันสื่อสังคมออนไลน์ เช่น Twitter ได้กลายเป็นช่องทางหลักที่การก่อการร้ายใช้เพื่อการระดมทรัพย์สินทรัพย์ จากการสำรวจพบว่าม็อดตราของผู้สนับสนุนเงินทุนเพื่อการก่อการร้าย มีมากกว่าหลายหมื่นคน²¹⁵ และในการบริจาคเหล่านั้นม็อดตราจำนวนเงินที่สูงโดยผู้ระดมทุนจะเลือก

²¹⁴ United Nations Security Council Resolution 2462/2019, pp. 28 (a), (b), (d)

²¹⁵ The Financial Action Task Force (FATF), "Fundraising through social media", FATF Report Emerging Terrorist Financing Risks (2015), p.31, Available from <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>

เป้าหมายที่มีความสนใจตรงกัน และเริ่มทำการสนทนากันผ่าน “Direct message” ซึ่งมีรูปลักษณะที่คล้ายกล่องข้อความคู่สนทนาส่วนตัว²¹⁶



อ้างอิงที่มารูปภาพ: Twitter Public Policy

4.3 ตัวอย่างข้อปฏิบัติของบริษัทเอกชน

ทั้งนี้บริษัทเอกชนผู้เป็นเจ้าของแพลตฟอร์มที่ให้บริการสื่อสังคมออนไลน์จะต้องมีความร่วมมือทางข้อมูลกับหน่วยงานของรัฐในการเข้ายับยั้งช่องทางของการระดมทุนเหล่านี้ Twitter Social network company ได้ออก "Guidelines for law enforcement" เพื่อที่หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง อาทิ หน่วยข่าวกรองทางการเงิน หรือหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย สามารถขอทำการแบ่งปันข้อมูลได้ดังต่อไปนี้ และตามเงื่อนไขตามตารางต่อไปนี้

1. ข้อมูลเกี่ยวกับบัญชีผู้ใช้งาน Twitter
2. ข้อมูลเกี่ยวกับนโยบายคำขอระดับเนื้อหาบน Twitter หรือ ข้อมูลทั่วไปนโยบายความเป็นส่วนตัว (Privacy Policy) ข้อกำหนดในการให้บริการ (Terms of Service) และกฎของ Twitter (Twitter Rules)

ตารางที่ 1: ช่องทางและเงื่อนไขการขอข้อมูลบัญชีผู้ใช้งาน Twitter โดยหน่วยงานบังคับใช้กฎหมาย

- **ช่องทางแรก** ผ่านช่องทางการร้องขอข้อมูลบัญชีผู้ใช้งานจากหน่วยงานบังคับใช้กฎหมายนั้นกับบริษัท Twitter โดยตรง แต่จะต้องปรากฏว่ามีคำร้องขอส่งไปยังบริษัท Twitter, Inc. เมืองซานฟรานซิสโกแคลิฟอร์เนีย ประเทศสหรัฐอเมริกา²¹⁷ โดยตรง หรือ บริษัทนานาชาติของ Twitter ในเมืองดับลิน ประเทศไอร์แลนด์
- **ช่องทางที่สอง** ผ่านช่องทางสนธิสัญญาความช่วยเหลือทางกฎหมายร่วมกัน (Mutual legal assistance treaties) หน่วยงานบังคับใช้กฎหมายอาจส่งคำขอ (Requests) ที่ออกอย่าง

²¹⁶ Waqas, "Twitter suspends 125,000 accounts for promoting terrorist acts," in *HackRead Cyber Security Intelligence* (2016).

²¹⁷ อ้างอิงที่อยู่: "Twitter, Inc., c/o Trust & Safety - Legal Policy, 1355 Market Street, Suite 900, San Francisco, CA 94103"

ถูกต้องผ่านสนธิสัญญาความช่วยเหลือทางกฎหมายซึ่งกันและกัน หรือ คำร้องจากศาลในประเทศผู้ร้องไปยังศาลของประเทศผู้รับคำร้องเพื่อขอให้ดำเนินการใช้อำนาจศาลในการช่วยเหลือศาลของประเทศผู้ร้อง (Letters rogatory) เมื่อส่งคำขอผ่านขั้นตอนให้ระบุว่าคำขอนั้นดำเนินการผ่านสนธิสัญญาความช่วยเหลือทางกฎหมายร่วมกัน (Mutual legal assistance treaties) และระบุชื่อประเทศต้นทางของความช่วยเหลือทางกฎหมายร่วมกัน

ประเภทของข้อมูล	เงื่อนไขในการแบ่งปันข้อมูล
ข้อมูลส่วนตัวผู้ใช้งาน (Private information)	ข้อมูลที่ไม่เปิดเผยต่อสาธารณะเกี่ยวกับผู้ใช้บริการของ Twitter จะไม่ถูกเปิดเผยต่อหน่วยงานบังคับใช้กฎหมาย ยกเว้นเพื่อใช้ข้อมูลนั้นต่อกระบวนการทางกฎหมาย และมีขั้นตอนทางกฎหมายในการขอที่เหมาะสม (Appropriate legal process) เช่นหมายศาล (Subpoena) คำสั่งศาล (Court order) หรือกระบวนการทางกฎหมายที่ถูกต้องอื่นๆ (Other valid legal process)
เนื้อหาของการสื่อสารของผู้ใช้งาน (Contents of communications)	ข้อมูลเนื้อหาของการสื่อสาร เช่น ข้อความทวิต กล่องข้อความคู่สนทนาส่วนตัว (Direct Messages) ข้อความตรงรูปภาพ (Photos) จะต้องปรากฏว่ามีหมายจับ หมายค้นหา ที่ถูกต้องหรือคำสั่งที่เทียบเท่าจากหน่วยงานยุติธรรมหรือศาลที่มีเขตอำนาจที่เหมาะสม
คำขอเปิดเผยข้อมูลฉุกเฉิน (An emergency disclosure request)	หากมีเหตุฉุกเฉินเร่งด่วนที่เกี่ยวข้องกับอันตรายของการเสียชีวิตหรือการบาดเจ็บทางร่างกายอย่างรุนแรงต่อบุคคลที่ใช้งาน Twitter ซึ่งอาจมีข้อมูลที่จำเป็นในการป้องกัน เจ้าหน้าที่บังคับใช้กฎหมายสามารถส่งคำร้องขอเปิดเผยข้อมูลฉุกเฉินผ่านทางเว็บไซต์ส่งคำขอทางกฎหมายของบริษัท Legalrequests.twitter.com ²¹⁸

อย่างไรก็ตามนโยบายความโปร่งใสและการมีกระบวนการที่เหมาะสม (Purposes of transparency and due process) ของทางบริษัท Twitter จำเป็นจะต้องแจ้งให้ผู้ใช้งานทราบถึง

²¹⁸ Twitter, "Guidelines for law enforcement" (2020), Available from <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support>

การร้องขอข้อมูลบัญชีของผู้ใช้ เช่น การแจ้งเตือนก่อนการเปิดเผยข้อมูลบัญชี (Prior to disclosure of account information) เว้นแต่เสียว่าจะเป็นไปได้ตามข้อยกเว้นดังนี้

ข้อยกเว้นแรก ทางบริษัทจะต้องถูกห้ามโดยคำสั่งที่ออกตามข้อบังคับของประเทศสหรัฐอเมริกาว่าด้วย “การขอให้มีการการแจ้งเตือนล่าช้า (Delay of Notification)” ตาม *An order under 18 U.S.C. § 2705 (b)*²¹⁹ ซึ่งจะต้องมีระยะเวลาของการห้ามการแจ้งเตือนผู้ใช้งานอย่างชัดเจน เช่น ห้ามแจ้งเตือนเป็นเวลา 90 วัน ทางบริษัท Twitter จึงจะไม่ทำการแจ้งเตือนผู้ใช้งานถึงการเปิดเผยข้อมูลบัญชี

ข้อยกเว้นที่สอง ตามนโยบายข้อยกเว้นการแจ้งเตือนถึงการเปิดเผยข้อมูลบัญชีของผู้ใช้งานให้รวมไปถึง สถานการณ์การต่อต้านที่จำเป็นเร่งด่วน (Counterproductive circumstances) เช่น เหตุฉุกเฉินเกี่ยวกับภัยคุกคามต่อชีวิต (Emergencies regarding imminent threat to life) การแสวงประโยชน์ทางเพศกับเด็ก (Child sexual exploitation) และ การก่อการร้าย (Terrorism)

4.4 ข้อท้าทายใหม่ของการระดมทุนผ่านระบบอินเทอร์เน็ต

ก. แพลตฟอร์มการระดมทุนจากฝูงชน (Crowdfunding platform)

ในรายงานของสำนักผู้บริหรด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ การใช้อินเทอร์เน็ตในการระดมทุนของการก่อการร้ายนั้น มีจำนวนไม่น้อยที่การก่อการร้ายได้อาศัยการระดมทุนผ่านแพลตฟอร์มการระดมทุนจากฝูงชน (Crowdfunding platform)²²⁰ ในหลายประเทศ ภูมิภาคยุโรปผู้ให้บริการแพลตฟอร์มหรือบริการเว็บโฮสติ้ง (Web-hosting services) มิได้มีความผิดในกรณีที่การก่อการร้ายได้ใช้บริการของตนเพื่อเป็นช่องทางในการเปิดระดมทรัพย์ แต่จะมีความผิดหากปรากฏว่าผู้ให้บริการแพลตฟอร์มเหล่านั้นได้เพิกเฉยต่อการเคลื่อนไหว หรือกิจกรรมของการระดมทุนผ่านบริการแพลตฟอร์มของตน ดังนั้นในข้อเท็จจริงที่เกิดขึ้นในหลายๆรัฐได้ออกกฎหมายที่จำเป็นให้หน่วยงานที่มีอำนาจ ได้ร่วมมือกับผู้ให้บริการแพลตฟอร์มการระดมทุนจากฝูงชนทั้งหมายในการเข้าถึงข้อมูลบัญชี หรือมีอำนาจในการออกคำสั่งให้ปิดหรือระงับบัญชีที่มีความสำคัญต่อการ

²¹⁹ U.S. Code § 2705.Delayed notice, Available from <https://www.law.cornell.edu/uscode/text/18/2705>

²²⁰ “Crowdfunding คือ การระดมทุนจากฝูงชนคนละจำนวนไม่มาก เพื่อสนับสนุนกิจกรรม โครงการ หรือธุรกิจผ่านเว็บไซต์กลาง หรือที่เรียกว่า Platform การระดมทุนในรูปแบบดังกล่าวเหมาะสำหรับธุรกิจที่เพิ่งเริ่มกิจการเนื่องจากทำได้ง่ายและสะดวก” ที่มา: คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (https://www.eta.or.th/th/Useful-Resource/knowledge-sharing/articles/index-article-other-p1/Crowdfunding-Investment-Revolution_Ep2.aspx)

เผยแพร่โฆษณาชวนเชื่อของผู้ก่อการร้ายและการระดมทุน²²¹ และการแบ่งปันข้อมูลเฉพาะในประเภท ดังที่ประโยชน์ต่อการดำเนินการสอบสวนสืบสวนของหน่วยงานบังคับใช้กฎหมายของประเทศต่างๆ ภายใต้ความร่วมมือ อาทิ

1. ข้อมูลอัตลักษณ์ส่วนตัวของบัญชีผู้ใช้บริการแพลตฟอร์มการระดมทุนจากฝูงชน (Personal identification information)
2. ข้อมูลรายละเอียดการทำธุรกรรมของการระดมเงิน (Information of Transaction detail)
3. ข้อมูลของหมายเลขที่ใช้สำหรับระบุตัวตนของเครื่องคอมพิวเตอร์ของผู้ใช้บริการแพลตฟอร์มที่เชื่อมต่ออยู่บนเครือข่าย (Internet Protocol address – IP address)²²²

อย่างไรก็ตามการแบ่งปันข้อมูลเพื่อตรวจจับการระดมทุนเพื่อการก่อการร้ายผ่านระบบ อินเทอร์เน็ต สื่อสังคมออนไลน์ หรือแม้กระทั่งแพลตฟอร์มต่างๆ นั้นมีข้อท้าทายที่เกิดขึ้นอย่างมาก เพราะพื้นฐานของการใช้บริการจากสื่ออินเทอร์เน็ต ผู้ใช้บริการสามารถที่จะปกปิดข้อมูลที่แท้จริง (Anonymity) ซึ่งมีผลทำให้หน่วยงานบังคับใช้กฎหมายไม่สามารถประเมินเพื่อแยกแยะได้ว่าผู้ใช้งาน บัญชีใดเป็นผู้เห็นใจ ผู้สนับสนุน หรือผู้ก่อการร้ายตัวจริง

ข้อมูลที่ได้มาจากการร่วมมือของเอกชนผู้ให้บริการนั้นก็ยังถือว่าสำคัญต่อการดำเนินการ สืบสวนสอบสวนต่อไป และสามารถใช้เป็นพยานหลักฐานในกระบวนการยุติธรรม เพียงแต่หน่วยงาน ที่มีอำนาจที่เกี่ยวข้อง ควรต้องเพิ่มระดับของการแบ่งปันข้อมูลกับบริษัทเอกชนผู้ให้บริการเพื่อเข้าถึง ข้อมูลในส่วนอื่นๆเพิ่มเติม เพื่อนำไปใช้ในการวิเคราะห์ในกรณีที่ซับซ้อน รวมทั้งในข้อกำหนดการ รายงาน ของความร่วมมือระหว่างหน่วยงานรัฐกับเอกชนทั้งหลายนั้นควรจะต้องมีการปรับเปลี่ยน แก้ไขเนื้อหาที่เกี่ยวกับประเภทของข้อมูลที่เป็นประโยชน์ต่อการดำเนินการปราบปรามการระดมทุน อยู่เสมอ

5. ข้อมูลติดตามรูปแบบการเงินของการก่อการร้าย

ข้อมูลติดตามรูปแบบการเงินของการก่อการร้าย หรือ “Financial profile” การแบ่งปัน ข้อมูลเพื่อต่อต้านการเงินของการก่อการร้ายของหน่วยงานบังคับใช้กฎหมายนั้น จะเป็นไปได้อย่าง ล้าบากหากว่าไม่ได้มีความร่วมมือทางข้อมูลกับธนาคาร สถาบันทางการเงิน หรือแม้กระทั่ง บริษัทเอกชน เพราะข้อมูลของสถาบันต่างๆนี้สามารถที่นำไปตรวจจับการทำธุรกรรมที่เกี่ยวข้องกับ การก่อการร้าย ในบรรดากลไกการตรวจจับการฟอกเงินของสถาบันทางการเงินนั้น ในทางปฏิบัติ

²²¹ Financial Action Task Force, "FATF report Emerging Terrorist Financing Risks" (2015), p.32, Available from <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>

²²² Ibid, pp. 34

พบว่าไม่สามารถนำกลไกเหล่านั้นมาใช้กับการตรวจจับการธุรกรรมเพื่อการก่อการร้ายได้ ดังตัวอย่างที่ต้องย้อนไปในเหตุการณ์วินาศกรรม 9/11 ผู้ก่อการร้ายหรือสลัดอากาศ (Hijackers) ทั้ง 19 คน²²³ ได้วางแผนการที่จะปิดบัง (Disguise) และไม่ให้ทราบถึงเจตนาของการทำธุรกรรมที่แท้จริง และแม้ว่าหน่วยงานที่มีอำนาจของอเมริกา (US authorities) ได้มีข้อมูลอย่างเพียงพอว่าสลัดอากาศทั้ง 19 คน อาจจะเป็นส่วนหนึ่งของสมาชิกกลุ่ม Al-Qaeda แต่ผลปรากฏว่าพนักงานหรือเจ้าหน้าที่ในสถาบันทางการเงินที่สลัดอากาศทั้ง 19 คนนั้นได้เปิดบัญชีการทำธุรกรรมการเงินกลับไม่ได้ถูกสงสัยหรือตรวจสอบเกี่ยวกับการทำธุรกรรมของพวกเขาว่าอาจจะไปเกี่ยวข้องกับก่อการร้าย

จากเหตุการณ์ข้างต้นนี้พิจารณาได้ว่าหน่วยงานบังคับใช้กฎหมายของประเทศสหรัฐอเมริกา ก่อนปี 2001 นั้นยังมีได้มีมาตรการหรือความร่วมมือทางข้อมูลกับสถาบันทางการเงินอย่างเช่น ธนาคารหรือบริษัทเอกชนที่เกี่ยวข้องกับการเงินซึ่งกลายเป็นช่องทางที่ถูกการก่อการร้ายใช้ประโยชน์ ดังนั้นในปัจจุบันสถาบันทางการเงินหลายแห่งของประเทศสหรัฐอเมริกาได้ร่วมมือกับหน่วยงานของรัฐบาลในการที่จะสร้าง “A profile of the terrorist” ภายหลังจากเหตุการณ์วินาศกรรมสำนักงานสอบสวนกลางของสหรัฐอเมริกา (Federal Bureau of Investigation – FBI)²²⁴ ได้ทำการตรวจสอบการทำธุรกรรมทางการเงินของสลัดอากาศทั้ง 19 คน ซึ่งได้ข้อเท็จจริงว่าบุคคลทั้ง 19 คนนั้นได้ทำการเปิดบัญชีธุรกรรมการเงินพร้อมกัน และได้แสดงตนเองว่าเป็นนักเรียน และได้ใช้จ่ายเงินในสัดส่วนที่มากกว่าครึ่งของบัญชีไปกับการเสียค่าลงทะเบียนเรียนกับสถาบันฝึกหัดนักบิน (Pilot training school) และเงินในบัญชีของพวกเขาถูกโอนมาจากประเทศสหรัฐอาหรับเอมิเรตส์เหตุการณ์ในทำนองเดียวกันที่ประเทศอังกฤษ ผู้ก่อการร้ายได้ใช้เงินจากรายได้ที่ถูกกฎหมายของสมาชิกคนหนึ่งในช่วงการคนหนึ่งที่ฝากเงินไว้ในบัญชีธนาคารต่าง ๆ และใช้เงินนั้นเพื่อการก่อเหตุโจมตี

ในข้อเท็จจริงที่ได้ปรากฏมานั้น การสร้างแบบจำลอง “Financial Profiles” ของผู้ก่อการร้ายอาจจะเป็นข้อมูลสำคัญที่ช่วยให้สถาบันทางการเงินและหน่วยงานบังคับใช้กฎหมายสามารถตรวจจับประเภทของการโจมตี (Identical types of attacks) ได้ไม่มากนักน้อย ดังนั้นสถาบันทางการเงินมิสามารถที่จะใช้ข้อมูลในมือของตนในการวิเคราะห์การธุรกรรมที่เกี่ยวข้องกับการก่อการร้ายได้เพียงลำพัง จึงจำเป็นจะต้องอาศัยความร่วมมือในการแบ่งปันข้อมูลหลายประเภท (Other types of information) กับหน่วยงานของภาครัฐ²²⁵ อาทิ หน่วยข่าวกรองทางการเงิน หรือหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย จึงจะสามารถเพิ่มศักยภาพในการติดตามสัญญาณของการก่อเหตุโจมตีจากการก่อการร้ายได้ ซึ่งการแบ่งปันข้อมูล

²²³ CNN Library, "September 11 Hijackers Fast Facts", *CNN News* (2019), Retrieved from <https://edition.cnn.com/2013/07/27/us/september-11th-hijackers-fast-facts/index.html>

²²⁴ Juan Miguel del Cid Gómez, "A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates," *Perspectives on terrorism* 8, 4 (2010).

²²⁵ *Ibid*, pp. 35

ระหว่างกันจะนำไปสู่ข้อมูลที่เป็นตัวชี้วัด ในการประเมินและคาดหมายได้ถึงวิธีการปฏิบัติการของการก่อการร้าย รัฐสมาชิกควรจะต้องให้ความสำคัญกับการแบ่งปันข้อมูลระหว่างหน่วยงานรัฐและสถาบันการเงินต่อการดำเนินมาตรการติดตามการเงินที่เกี่ยวข้องต่อการก่อการร้าย

5.1 ข้อเสนอแนะของคณะกรรมการการต่อต้านการก่อการร้าย

การดำเนินการตามข้อมติที่ 2178/2014 ที่มุ่งเน้นไปที่การปราบปรามนักรบต่างชาติ ได้มีช่องว่างเกิดขึ้นต่อมาตรการแบ่งปันข้อมูลทางการเงิน ซึ่งคณะกรรมการการต่อต้านการก่อการร้าย (UN Counter Terrorism Committee – CTC) ได้ ออก “*Global recommendation in preventing the financing of foreign terrorist fighters*”²²⁶ แม้เอกสารชิ้นนี้จะไม่ได้พันธผูกพันตามกฎหมาย (Legal binding) แต่สามารถใช้เพื่อเป็นเครื่องมือในการดำเนินการตามกฎหมายระหว่างประเทศ และเป็นส่วนเสริมของการดำเนินการ ต่อแง่มุมของประเด็นที่มีความสำคัญ (Thematic perspectives)

5.2 กระบวนการตามข้อเสนอแนะ

ข้อเสนอส่วนแรก รัฐสมาชิกจะต้องออกกฎระเบียบและข้อบังคับให้หน่วยข่าวกรองทางการเงิน แบ่งปันข้อมูลโดยสรุปรวม จากหน่วยงานบังคับใช้กฎหมาย หรือหน่วยงานที่เกี่ยวข้อง อาทิ ศาลากร หน่วยงานตรวจคนเข้าเมือง หรือหน่วยข่าวกรองแห่งชาติ ข้อมูลที่เกี่ยวข้องสวัสดิการสังคม ข้อมูลภาษีของบุคคล

ข้อเสนอส่วนสอง หน่วยข่าวกรองทางการเงิน จะต้องร่วมมือทางข้อมูลกับสถาบันทางการเงิน แลกเปลี่ยนข้อมูลเพื่ออำนวยความสะดวกการติดตามช่องทางทางการเงินของนักรบต่างชาติ และการก่อการร้าย และอำนวยความสะดวกต่อโปรแกรม “Financial profiles”²²⁷

ทั้งนี้สอดคล้องกับข้อมติที่ 2253/2015 เรียกร้องให้บรรดารัฐสมาชิกให้ความสำคัญต่อการแบ่งปันข้อมูลระหว่างหน่วยงานภายในของรัฐและระหว่างหน่วยงานของรัฐบาลเพื่อปราบปรามการสนับสนุนการเงินของการก่อการร้ายให้เกิดมีประสิทธิภาพ และเรียกร้องให้รัฐสมาชิกมีมาตรการเฝ้า

²²⁶ Security Council, "Letter dated 15 December 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 158 (D), (E)

²²⁷ “The recommendation are as follows: (E) Enhance access for financial intelligence units to aggregated information from law enforcement or other relevant public agencies (for example, customs, border agencies or national intelligence agencies), as well as social welfare and tax information, where permitted, in order to facilitate the tracking of foreign terrorist fighter financing channels and build financial profiles of foreign terrorist fighters, particularly with regard to known foreign terrorist fighters already in conflict zones and returnees.”

ระวังการทำธุรกรรมที่เกี่ยวข้องต่อการก่อการร้าย (Vigilance over relevant financial transactions) โดยการพัฒนาความสามารถของหน่วยงานที่มีความสำคัญต่อการแบ่งปันข้อมูล²²⁸ อาทิ หน่วยงานบังคับใช้กฎหมาย หน่วยข่าวกรอง หน่วยบริการรักษาความปลอดภัย (Security services units) และหน่วยข่าวกรองทางการเงิน ผ่านความร่วมมือทางข้อมูลทั้งระดับภายในรัฐเอง และระดับระหว่างรัฐ

ประการถัดมาข้อเสนอแนะยังต้องการให้รัฐสมาชิกมีการบูรณาการและใช้ประโยชน์จากการแบ่งปันข้อมูลหลายประเภท (Other types of information) ที่ได้มาจากหน่วยงานรัฐหรือสถาบันการเงินและภาคเอกชน เพื่อเสริมคุณภาพของข่าวกรองทางการเงินเพื่อดำเนินมาตรการต่อต้านการเงินของการก่อการร้าย และต่อต้านกลุ่มก่อการร้ายอย่าง กลุ่มจัดตั้งรัฐอิสลามแห่งอิรักและลิแวนต์ (Islamic State of Iraq and the Levant – ISIL) กลุ่มอัลกออิดะฮ์ (Al-Qaida) บุคคลหรือกลุ่มคนที่เกี่ยวข้อง (Associated individuals or groups) กลุ่มองค์กรและหน่วยต่างๆ (Undertakings and entities)

จากการพิจารณาข้อเสนอแนะข้างต้นนั้น การแบ่งปันข้อมูลในหลายๆประเภทเพื่อต่อต้านการเงินของการก่อการร้ายจะเป็นประโยชน์ต่อการสร้างเครื่องมือที่เรียกว่า “Financial Profiles” ที่จะเป็นตัวชี้วัดในการสังเกตการณ์การทำธุรกรรมที่เกี่ยวข้องต่อการก่อการร้ายของหน่วยงานบังคับใช้กฎหมายหรือสถาบันทางการเงิน ในแง่ที่ว่าข้อมูลเหล่านั้นจะสามารถทำการติดตามรูปแบบกิจกรรมทางการเงินที่ผิดปกติได้ (Unusual activities) ซึ่งเครื่องมือดังกล่าวที่ถูกพัฒนาขึ้นและมีประสิทธิภาพได้นั้นจะต้องอาศัยความร่วมมือทางข้อมูลจากหลายส่วนๆที่เรียกว่า “Public-private Terrorism-financing Information-sharing Platform” ให้เกิดขึ้นได้เสียก่อน

5.3 กลไกความร่วมมือ

ในรายงานของคณะกรรมการต่อต้านการก่อการร้าย ได้ยกตัวอย่างการปฏิบัติการดำเนินการตามข้อมติและข้อเสนอแนะดังกล่าวอย่างเห็นได้ชัด ในหลายประเทศในภูมิภาคยุโรป ทางรัฐบาลประเทศเหล่านั้นได้มอบหมายให้หน่วยข่าวกรองทางการเงินของตนให้ข้อมูลรายชื่อบุคคลหรือกลุ่มบุคคล ที่มีข้อมูลทางข่าวกรอง (ที่ได้ข้อมูลมาจาก สถาบันทางการเงิน ภาคเอกชน หรือหน่วยงานภาครัฐอื่นๆ) และถูกพิจารณาว่าบุคคลเหล่านั้นมีส่วนเกี่ยวข้องต่อการทำธุรกรรมที่สุ่มเสี่ยงหรือเป็นประโยชน์ต่อการก่อการร้ายให้แก่หน่วยงานที่เสนอรายงาน เพื่อนำส่งรายงานการทำธุรกรรมและรายชื่อบุคคลที่น่าสงสัยให้แก่ “FIU.NET”²²⁹ ซึ่งเป็นแพลตฟอร์มเครือข่ายคอมพิวเตอร์ที่สนับสนุนการ

²²⁸ United Nations Security Council Resolution 2253/2015, pp. 25

²²⁹ FIU.NET, "Coordinated crimes need a coordinated response" (2020), Available from <https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net>

ทำงานของหน่วยข่าวกรองทางการเงินในสหภาพยุโรป (Financial Intelligence Units in the European Union) ในการต่อต้านการฟอกเงินและการจัดหาเงินทุนของการก่อการร้าย และได้ถูกรับรองขึ้นในปี 2016 ตาม “*Council Decision 2000/642/JHA*”²³⁰

“FIU.NET” จะรวบรวมรายงานการทำธุรกรรมที่น่าสงสัย (The suspicious transaction reports) และข้อมูลข่าวกรองทางการเงินจากประเทศในภูมิภาคยุโรปทั้งหมด 28 ประเทศ ซึ่งเป็นข้อมูลเหล่านี้จะเป็นกุญแจสำคัญในการระบุรูปแบบทางการใช้เงินของผู้ก่อการร้าย รวมทั้งใช้เพื่อสังเกตการณ์บุคคลและเครือข่าย ตลอดจนอำนวยความสะดวกและผู้สนับสนุนเงินเพื่อการก่อการร้าย²³¹

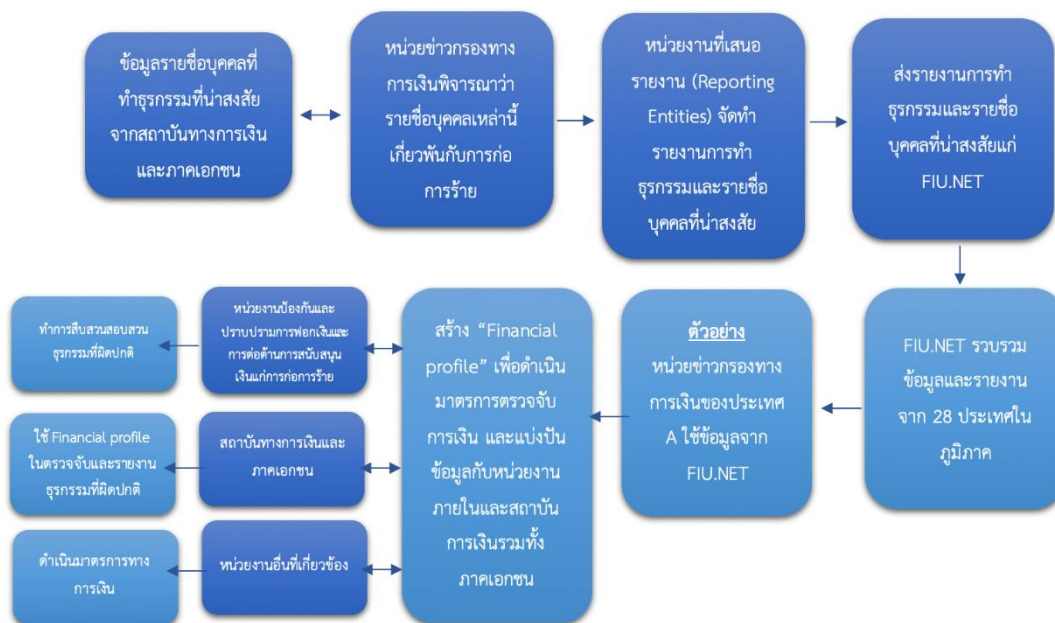
หน่วยข่าวกรองทางการเงินและหน่วยงานบังคับใช้กฎหมายของแต่ละประเทศในภูมิภาคจะสามารถนำข้อมูลใน FIU.NET อาทิ รายชื่อบุคคลที่ได้รับยืนยันว่าเกี่ยวข้องกับการเงินของการก่อการร้ายในรายงาน รวมถึงข้อมูลของลักษณะการทำธุรกรรมที่ผิดปกติ มาทำการวิเคราะห์และสร้างเป็น “Financial profile” เพื่อเป็นตัวชี้วัดให้แก่หน่วยงานภายในรัฐตนได้ดำเนินมาตรการป้องกันการเงินของการก่อการร้าย ดังเช่น

- หน่วยข่าวกรองทางการเงินและหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย จะได้ข้อมูลรายชื่อบุคคลที่จะต้องเฝ้าระวังและทำการสอบสวน
- สถาบันทางการเงินและภาคเอกชนจะได้ข้อมูลของลักษณะการทำธุรกรรมที่ผิดปกติ ไว้เป็นตัวชี้วัดสำหรับการทำธุรกรรมการเงินในบัญชีของลูกค้าที่มีแนวโน้มจะอยู่ในความเสี่ยง
- หน่วยงานศุลกากรและหน่วยงานตรวจคนเข้าเมืองจะได้ข้อมูลประเภทอื่นๆ ที่จะสามารถดำเนินมาตรการป้องกันการเงินของการก่อการร้าย เช่น ข้อมูลของบุคคลที่อยู่ในเกณฑ์ว่า จะต้องสำแดงทรัพย์สิน จำนวนเงิน หรือวัตถุประสงค์ของการใช้เงินในประเทศตน จากทั้งหมดจะสรุปได้ตามแผนผังด้านล่างนี้

²³⁰ Council Decision 2000/642/JHA (2016), Available from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0642&from=EN>

²³¹ Security Council, *Fifth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range* (2017).

แผนผังโครงสร้าง : ตัวอย่างการแบ่งปันข้อมูลข่าวกรองทางการเงินตาม FIU.NET ของกลุ่มประเทศในภูมิภาคยุโรป



ดังนั้นจะสรุปได้ว่าข้อมูลที่นำมาสู่การสร้าง “Financial profile” นั้นขั้นแรกจะต้องมีแพลตฟอร์มในการแบ่งปันข้อมูลที่จะเปิดโอกาสให้มีการแลกเปลี่ยนซึ่ง ข้อมูลที่ได้รับการรับรองข้อมูลที่เป็นลักษณะความลับ หรือข้อมูลประเภทอื่น รวมถึงข้อมูลข่าวกรองระหว่างหน่วยงานของรัฐบาล และหน่วยงานรัฐที่ทำหน้าที่แทนเอกชน (Pre-authorized representatives of the private sectors) เช่น หน่วยข่าวกรองทางการเงิน และจากนั้นหน่วยงานของรัฐที่เกี่ยวข้องเหล่านี้จะต้องมีความร่วมมือเพื่อแบ่งปันข้อมูลกับสถาบันทางการเงินหรือภาคเอกชนในการระบุเครือข่ายการเงินของการก่อการร้าย และใช้ข้อมูลเพื่อพัฒนา “Financial profile” ต่อไป²³²

²³² Security Council, “Second report of the Secretary-General on the threat posed by ISIL (Da’esh) to international peace and security and the range”, United Nations efforts in support of Member States in countering the threat (2016), pp. 55-57

6. ข้อมูลการสำแดงเงินสดที่มีประสิทธิภาพ (Effective cash declaration systems)

6.1 ข้อเสนอแนะของคณะกรรมการการต่อต้านการก่อการร้าย

“Global recommendation in preventing the financing of foreign terrorist fighters” ที่ได้ถูกรับรองโดยคณะกรรมการการต่อต้านการก่อการร้ายเพื่อเสริมประสิทธิภาพของมาตรการแบ่งปันข้อมูลต่อการเงินของการก่อการร้าย โดยชี้แนะให้รัฐสมาชิกมอบหมายให้หน่วยงานที่เกี่ยวข้องต่อการตรวจสอบการเงินที่อาจเกี่ยวข้องต่อการก่อการร้ายร่วมมือกันทางข้อมูลเพื่อพัฒนา “ระบบการสำแดงเงินสดที่มีประสิทธิภาพ” ซึ่งมีวัตถุประสงค์ที่จะยับยั้งมิให้จำนวนเงินเหล่านั้นได้เข้ามาในระบบการเงินของประเทศ หรือป้องกันมิให้เงินเหล่านั้นออกไปสู่ระบบการเงินระหว่างประเทศด้วยเช่นกัน

ข้อเสนอของคณะกรรมการ ข้อ (C) กล่าวคือให้รัฐสมาชิกจัดทำโปรแกรมของการเปิดเผยหรือการสำแดงซึ่งเงินสด ขึ้นที่หน่วยตรวจคนเข้าเมืองหรือหน่วยศุลกากรของประเทศเพื่อการหยุดยั้งการขนส่งเงินสดข้ามพรมแดนที่ผิดกฎหมาย และให้อำนาจแก่หน่วยงานบังคับใช้กฎหมายต่อการสืบสวนสอบสวน ยึดหรืออายัดซึ่งทรัพย์สินที่เป็นเงินสดนั้นที่มีการพิจารณาว่า²³³

1. มีข้อมูลว่าจะใช้จำนวนเงินสดนั้นไปกับการรับสมัครนักรบต่างชาติ
2. มีข้อมูลว่าจะใช้จำนวนเงินสดนั้นไปเพื่อการก่อหรือกระทำการที่เกี่ยวข้องต่อการก่อการร้าย

6.2 กระบวนการและกลไกตามข้อเสนอแนะ

รัฐสมาชิกจะต้องการช่องทางของการแบ่งปันข้อมูลระหว่างหน่วยงานของรัฐ อาทิ หน่วยงานตรวจคนเข้าเมือง หรือ หน่วยงานศุลกากร ให้ความร่วมมือทางข้อมูลกับหน่วยข่าวกรองทางการเงิน และหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย โดยข้อมูลที่สำคัญต่อการนำมาวิเคราะห์ คือ ข้อมูลการรายงานของการสำแดงเงินสด และข้อมูลโดยทั่วไปที่เกี่ยวข้องต่อการสำแดงเงินสด ซึ่งข้อมูลเหล่านี้จะได้มาจากหน่วยงานของรัฐที่เป็นผู้รับผิดชอบด่านแรกโดยตรงก่อนการเข้าสู่ประเทศของจำนวนเงินเหล่านั้น

ข้อมูลที่ได้จากการแบ่งปันจะช่วยเสริมประสิทธิภาพของการดำเนินการของหน่วยข่าวกรองทางการเงิน และหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้ายในการสืบสวนสอบสวนหรือดำเนินการยึดซึ่งเงินสด ที่ถูกพิจารณาและปรากฏว่ามีส่วน

²³³ Security Council, "Letter dated 15 December 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 158 (C)

เกี่ยวข้องกับการเงินที่เป็นเงินสดเพื่อการก่อการร้ายที่หมุนเวียนอยู่ภายในระบบเศรษฐกิจของรัฐสมาชิก (Cash-based economy)²³⁴

เช่นเดียวกันกับใน The FATF Recommendation ที่ 31 และ 32 ของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Financial Action Task Force – FATF) ให้รัฐสมาชิกดำเนินมาตรการของการสำแดงเงินสดที่มีประสิทธิภาพการตรวจสอบการเงินของการก่อการร้าย ซึ่งผู้เขียนขออธิบายได้ตามตารางนี้²³⁵

ตาราง : ข้อเสนอแนะและรายละเอียดต่อการดำเนินต่อระบบการสำแดงเงินสดที่มีประสิทธิภาพตาม The FATF Recommendation ที่ 31 และ 32

ข้อเสนอแนะ	หัวข้อ	รายละเอียด
31	Powers of law enforcement and investigative authorities	<ul style="list-style-type: none"> - รัฐสมาชิกควรจะต้องดำเนินการเพื่อให้มีกลไกที่มีประสิทธิภาพในการตรวจสอบซึ่งบุคคลหรือนิติบุคคลที่เป็นเจ้าของบัญชีเงินที่ได้ทำการสำแดง ณ ที่จุดตรวจของหน่วยงาน Border security - รัฐสมาชิกจะต้องแน่ใจว่ามีกฎระเบียบและข้อบังคับที่ให้หน่วยงานที่เกี่ยวข้องสามารถทำการตรวจสอบซึ่งทรัพย์สินของบุคคลหรือนิติบุคคลโดยปราศจากการแจ้งเตือนบุคคลเหล่านั้นล่วงหน้า (Without prior notification to the owners) - รัฐสมาชิกจะต้องแน่ใจว่ามีช่องทางที่เพียงพอต่อการแบ่งปันข้อมูลระหว่างหน่วยข่าวกรองทางการเงินกับหน่วยงานบังคับใช้กฎหมายในการสืบสวนสอบสวนในความผิดฐานที่เกี่ยวข้องและการจัดหาเงินทุนของ

²³⁴ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 418

²³⁵ Financial Action Task Force, "The FATF Recommendations" (2012), p.23, Available from <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

ข้อแนะนำ	หัวข้อ	รายละเอียด
		การก่อการร้าย
32	Cash couriers	<ul style="list-style-type: none"> - รัฐสมาชิกควรจะออกมาตรการให้หน่วยงานที่เกี่ยวข้องทำการตรวจจับ (Detect) การขนส่งเงินสดข้ามพรมแดน (Physical cross-border transportation of currency) หรือตราสารเงินผ่านระบบการสำแดงการเงิน (Declaration systems) หรือระบบการเปิดเผยรายการของเงิน (Disclosure systems) - รัฐสมาชิกควรตรวจสอบให้แน่ใจว่าหน่วยงานบังคับใช้กฎหมายของตน มีอำนาจตามกฎหมายในการหยุด (Stope) หรือยับยั้ง (Restrain) เงินหรือตราสารทางการเงิน อันซึ่งเป็นที่น่าสงสัยว่าเกี่ยวข้องกับการจัดหาเงินทุนของการก่อการร้าย การฟอกเงิน หรือการกระทำที่ถือเป็นความผิด (Predicate offences) เช่น การสำแดงเงินหรือการเปิดเผยเงินซึ่งไม่ตรงกับความเป็นจริง - รัฐสมาชิกควรจะต้องแน่ใจว่าได้ดำเนินมาตรการการลงโทษที่มีประสิทธิภาพ (Effective sanction) มาตรการการลงโทษตามสัดส่วน (Proportionate sanction) หรือ มาตรการลงโทษโดยการห้ามปราบ (Dissuasive sanction) ต่อบุคคลผู้ซึ่งทำการสำแดงเงินหรือการเปิดเผยเงินซึ่งไม่ตรงกับความเป็นจริง

ในตัวอย่างของการดำเนินการเพื่อตรวจจับการเงินของการก่อการร้ายผ่านระบบสำแดงการเงิน ในภูมิภาคเอเชียตะวันออกเฉียงใต้หลายประเทศ หน่วยงานที่ทำหน้าที่ข่าวกรองทางการเงินมี

ความร่วมมือกันภายใต้กลุ่มที่ชื่อว่า The region's Financial Intelligence Consultative Group (FICG) ซึ่งเป็นหน่วยปฏิบัติการของเวทีการประชุมสุดยอด Counter terrorist financing (CTF Summit) ประกอบด้วย หัวหน้าหน่วยข่าวกรองจากกลุ่มประเทศอาเซียน ประเทศออสเตรเลีย และ ประเทศนิวซีแลนด์ ผลลัพธ์ที่สำคัญของการประชุมจนถึงปัจจุบัน ได้แก่

1. แบ่งปันข้อมูลของการประเมินความเสี่ยงในระดับภูมิภาคเป็นครั้งแรก เกี่ยวกับการจัดหาเงินทุนเพื่อการก่อการร้าย
2. แบ่งปันข้อมูลของการประเมินการเงินขององค์กรไม่แสวงหาผลกำไร และข้อมูลการเคลื่อนย้ายเงินข้ามพรมแดน
3. แบ่งปันข้อมูลตัวชี้วัด (Red flag indicator) ของการประเมินความเสี่ยงของการเงินของการก่อการร้าย

ทั้งหมดนี้จะช่วยอำนวยความสะดวกให้กับคณะทำงานด้านการเงินเพื่อต่อต้านการก่อการร้ายในภูมิภาคเอเชียตะวันออกเฉียงใต้ (SEA-CTFWG) ซึ่งจัดตั้งขึ้นเพื่อมอบคู่มือกลไกของปฏิบัติงานสำหรับหน่วยข่าวกรองทางการเงินในระดับภูมิภาค เพื่อดำเนินการจัดลำดับความสำคัญเชิงกลยุทธ์ ประสานงาน และปฏิบัติการเพื่อต่อสู้กับการจัดหาเงินทุนการก่อการร้ายในภูมิภาคโดยเฉพาะอย่างยิ่งที่เชื่อมโยงกับองค์กรในเครือของกลุ่มจัดตั้งรัฐอิสลามแห่งอิรักและลิแวนต์ (Islamic State of Iraq and the Levant – ISIL)²³⁶

นอกจากนี้ทางกลุ่ม The region's Financial Intelligence Consultative Group (FICG) จะดำเนินการร่วมประเมินข่าวกรองในระดับภูมิภาคกับคณะทำงานด้านการเงินเพื่อต่อต้านการก่อการร้ายในภูมิภาคเอเชียตะวันออกเฉียงใต้ (SEA-CTFWG) เพื่อทำความเข้าใจแนวทางปฏิบัติของการเคลื่อนไหวข้ามพรมแดน และวิธีการใช้เงินเพื่อการก่อการร้าย ตลอดจนการริเริ่มพัฒนาการเตรียมการโดยเฉพาะในประเทศสมาชิก ที่ต้องพึ่งพาการทำธุรกรรมเป็นเงินสดอย่างมาก (Rely heavily on cash transactions) ให้มีระบบตรวจสอบการสำแดงเงินที่มีประสิทธิภาพและสามารถปฏิบัติให้ได้จริง (Practical)²³⁷

²³⁶ AUSTRAC, "Counter Terrorism Financing Summit" (2019), Retrieved from <https://www.austrac.gov.au/about-us/international-engagement/international-partners>

²³⁷ Security Council, "Fifth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range", United Nations efforts in support of Member States in countering the threat (2017), pp. 42-43

3.2.2.2 ข้อเสนอแนะของหน่วยงานระหว่างประเทศ

หน่วยงานภายใต้สหประชาชาติอย่างสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ และคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน มีส่วนสำคัญอย่างมากในการพัฒนาคำแนะนำและข้อเสนอแนะแก่บรรดารัฐสมาชิกในการดำเนินการตามมาตรการแบ่งปันข้อมูลเพื่อการปราบปรามการเข้าถึงแหล่งการเงินของการก่อการร้าย แม้ว่าในทางกฎหมายแล้วคำแนะนำและข้อเสนอจะไม่มีผลผูกพันทางกฎหมายต่อบรรดารัฐสมาชิกสหประชาชาติ แต่รัฐสมาชิกสามารถนำข้อเสนอแนะดังกล่าวมาปรับใช้ในการดำเนินการของตน

1. ข้อเสนอแนะของสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ

สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ (Counter Terrorism Executive Directorate – CTED) ได้ระบุว่าในปัจจุบันในหลายประเทศสมาชิก ได้เริ่มดำเนินการตามข้อมติที่ 2199/2015 โดยหน่วยงานของภาครัฐมีการร่วมมือกับสถาบันการเงินทั้งในประเทศและระหว่างประเทศ ทั้งนี้ได้ออกคำแนะนำและข้อเสนอแนะให้แก่สถาบันทางการเงินรวมถึงภาคเอกชนเพื่อใช้เตรียมสอบกิจกรรมที่น่าสงสัยและคาดว่าจะเกี่ยวข้องกับการก่อการร้าย อาทิในเอกสารชื่อ “*Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions*” และ “*Technical guide to Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters*” ตัวอย่างการดำเนินการของกลุ่มประเทศโอเชียเนีย (Oceania countries) แคนาดา และฝรั่งเศส สถาบันการเงินในประเทศเหล่านี้ได้ให้ความร่วมมือกับหน่วยงานของรัฐเพราะมีการใช้เทคโนโลยีขั้นสูง (Advance technology)²³⁸ มาช่วยในการวิเคราะห์การทำธุรกรรมของบัญชีลูกค้าที่มีอยู่ในระบบของธนาคารหลายล้านบัญชีได้ในเวลาอันรวดเร็ว โดยเฉพาะบัญชีที่มีการธุรกรรมการเงินไปยังกลุ่มประเทศที่มีความเสี่ยง เช่น สาธารณรัฐอาหรับซีเรีย (Syrian Arab Republic) และประเทศที่อยู่ใกล้เคียงภายในภูมิภาคเดียวกัน²³⁹ โดยจะสามารถจัดส่งข้อมูลที่วิเคราะห์ได้ว่าอยู่ในความเสี่ยง ต่อหน่วยงานข่าวกรองทางการเงินภายในประเทศและต่างประเทศเพื่อการดำเนินการตามมาตรการในขั้นถัดไป

²³⁸ Australian Transaction Reports and Analysis Centre, "Fact sheet: How we work with industry and partners" (2020), Available from https://www.austrac.gov.au/sites/default/files/2020-05/How%20we%20work%20with%20industry%20and%20partners_Fact%20sheet%20_New.pdf

²³⁹ Australian Transaction Reports and Analysis Centre, "How we work with industry and partners" (2020), Available from https://www.austrac.gov.au/sites/default/files/2020-05/AUSTRAC%20Infographic_how%20we%20work%20with%20industry%20and%20partners_New.pdf

ของการปราบปราม ดังนั้นสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติได้ส่งเสริมการพัฒนาศักยภาพในเทคโนโลยีการแบ่งปันข้อมูลของสถาบันทางการเงิน ภาคเอกชน และหน่วยงานข่าวกรองทางการเงินให้มีการพัฒนาระบบอัลกอริทึมของการวิเคราะห์ (Sophisticated algorithms of filters) เพื่อแจ้งเตือนถึงความเสี่ยงของธุรกรรมการเงินได้ในเวลาอันเร็วรวดเร็ว และแบ่งปันข้อมูลสู่ขั้นตอนของการดำเนินการสืบสวนสอบสวนของหน่วยงานบังคับใช้กฎหมายต่อไป²⁴⁰

2. ข้อเสนอแนะของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน อย่างไรก็ตามหากรัฐสมาชิกที่ยังไม่มีการออกคำแนะนำและข้อเสนอแนะต่อสถาบันทางการเงิน หรือเอกชนในประเทศของตน สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติได้มีข้อเสนอให้รัฐสมาชิกได้ดำเนินการนำ *Risk-Based Approach Guidance for the Banking Sector* ที่ถูกรับรองขึ้นโดยคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน²⁴¹ มาใช้เพื่อเป็นเครื่องมือให้แก่รัฐสมาชิกในการออกคำแนะนำให้กับสถาบันทางการเงินภายในประเทศ สรุปลงได้ว่าข้อท้าทายสำหรับรัฐสมาชิกคือการต่อต้านและป้องกันการเข้าถึงแหล่งเงินของการก่อการร้ายในปัจจุบันที่อาศัยเทคโนโลยีที่ถูกพัฒนาขึ้นและสะดวกในการเข้าใช้งานต่อการดำเนินกิจกรรมของการก่อการร้าย ซึ่งการสร้างความร่วมมือระหว่างหน่วยงานรัฐกับภาคเอกชนเป็นเครื่องมือที่สำคัญในการได้มาซึ่งข้อมูลในการตรวจจับ ความผิดปกติของเส้นทางการเงินที่อาจมีส่วนเกี่ยวข้องกับการสนับสนุนการก่อการร้าย ในส่วนต่อไปนี้จะเห็นรูปแบบของวิธีการแบ่งปันข้อมูลเพื่อติดตาม เส้นทางการเงินที่ต้องสงสัย ซึ่งผู้เขียนจะอธิบายถึงความสัมพันธ์ของการแบ่งปันข้อมูลระหว่างผู้มีส่วนเกี่ยวข้อง พร้อมกับวิเคราะห์ให้เห็นถึงกระบวนการของวิธีการในการแบ่งปันข้อมูล

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

²⁴⁰ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp.37

²⁴¹ Financial Action Task Force, "Risk-Based Approach Guidance for the Banking Sector" (2014), Available from <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>

3.3 การแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย

ในปัจจุบันแต่ละประเทศได้มีการเชื่อมต่อกันทางเศรษฐกิจ สังคม และการเมืองจนนำมาสู่การเติบโตของการเดินทางข้ามชายแดนซึ่งไม่ได้จำกัดเพียงแค่การเดินทางของผู้คน แต่ยังรวมไปถึงสินค้าและบริการ รวมทั้งทรัพยากรที่ใช้ในการพัฒนาเศรษฐกิจในแง่ต่างๆ เช่นเดียวกันกับกรณีของการก่อการร้าย ผู้ก่อการร้าย ผู้ต้องสงสัยว่าเป็นผู้ก่อการร้าย และนักรบต่างชาติ ได้อาศัยความสะดวกของการเดินทางข้ามชายแดนในปัจจุบัน เพื่อมุ่งประสงค์ต่อเป้าหมายที่เกี่ยวข้องกับการก่อการร้าย รวมไปถึงการเคลื่อนย้ายอย่างผิดกฎหมาย²⁴²

การดำเนินมาตรการต่อการตรวจคนเข้าเมืองของแต่ละประเทศนับว่ามีความสำคัญอย่างยิ่งต่อการปกป้องการกระทำของการก่อการร้ายไม่ว่าจะเป็นการดำเนินการทั้ง พรมแดนทางทะเล (Maritime borders) พรมแดนทางอากาศ (Air borders) และพรมแดนทางบก (Land borders) ซึ่งในส่วนนี้ผู้เชี่ยวชาญจะขอแบ่งประเด็นออกเป็น **3 ประเด็น** คือ 1. การควบคุมชายแดนให้ได้มีประสิทธิภาพ 2. การตรวจบุคคลที่เดินทางเข้าประเทศ และ 3. รายชื่อเฝ้าระวังและฐานข้อมูล (Watch lists and database) เพื่ออธิบายถึงสารบัญญัติของพันธกรณีในการดำเนินมาตรการแบ่งปันข้อมูล ตลอดจนชี้ให้เห็นถึงกระบวนการ อำนาจหน้าที่ของหน่วยงานที่เกี่ยวข้อง

3.3.1 การควบคุมชายแดนให้ได้มีประสิทธิภาพ

3.3.1.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ข้อมติที่ 1373/2001 ของคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ดำเนินการลงโทษ (Sanctions) ต่อการก่อการร้ายโดยอาศัย “นานาชาติวิธีการ”²⁴³ โดยการต่อต้านการก่อการร้ายในทุก รูปแบบ ซึ่งการแบ่งปันข้อมูลก็เป็นหนึ่งในวิธีเหล่านั้น ตามข้อที่ 3 (a) ข้อมติเรียกร้องให้บรรดารัฐต่างๆ (Calls upon all States to) ได้หาวิถีทางในการดำเนินการแบ่งปันข้อมูลต่อการเคลื่อนไหวของผู้ก่อการร้าย หรือกลุ่มเครือข่ายก่อการร้าย ทั้งนี้ให้รวมไปถึงข้อมูลของการปลอมแปลงเอกสารการเดินทาง (Forged or falsified travel documents) ของบุคคลที่เกี่ยวข้องต่อการก่อการร้าย

ยิ่งไปกว่านั้นในข้อที่ 2 (g) ข้อมติได้ตัดสินใจให้รัฐบรรดารัฐต่างๆ (Decides also that all States shall) ดำเนินมาตรการป้องกันการเคลื่อนไหวของผู้ก่อการร้าย หรือกลุ่มก่อการร้ายโดยมีการ

²⁴² The Council's Counter-Terrorism Committee and its Executive Directorate, "The factsheet about border management" (2019), Available from https://www.un.org/sc/ctc/wp-content/uploads/2019/06/ctc_cted_fact_sheet_designed_border_management_december_2018.pdf

²⁴³ United Nations Security Council Resolution 1373/2001, pp. 2(g), 3(a)

ควบคุมชายแดนที่มีประสิทธิภาพ (Effective border controls) การควบคุมการออกเอกสารประจำตัว และเอกสารการเดินทาง ตลอดจนมีมาตรการในการป้องกันการปลอมแปลงหรือการใช้เอกสารระบุตัวตนและเอกสารการเดินทางโดยทุจริต ทั้งหมดของการดำเนินการตามมาตรการเหล่านี้จะต้องอาศัยการแบ่งปันข้อมูลระหว่างประเทศ ภูมิภาค หรืออนุภูมิภาค

3.3.1.2 สารบัญญัตินี้

การควบคุมชายแดนให้ได้มีประสิทธิภาพนั้นเป็นมาตรการสำคัญต่อการต่อต้านการก่อการร้าย เพราะเปรียบเสมือนเป็นมาตรการด่านแรกสุดของรัฐ ในการป้องกันการเดินทางข้ามแดนและการเคลื่อนไหวของการก่อการร้าย รวมทั้งสิ่งของและสินค้าที่ผิดกฎหมาย ในระดับภายในประเทศ เทคโนโลยีการแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับการจัดการชายแดนนั้นเป็นเครื่องมือที่สำคัญในการเป็นช่องทางที่สำคัญต่อการได้รับข้อมูลจากการแบ่งปันข้อมูลมาจากแต่ละหน่วยงาน

ข้อมติ 1373/2001 เรียกร้องให้บรรดารัฐต่างๆมีการควบคุมชายแดนของตนให้มีประสิทธิภาพ เพื่อป้องกันการเคลื่อนไหวของผู้ก่อการร้ายและกลุ่มก่อการร้าย แต่ในข้อมติมิได้อธิบายถึงขั้นตอนกระบวนการและวิธีการอย่างไรที่จะเป็นการควบคุมที่มีประสิทธิภาพ²⁴⁴ จึงจำเป็นที่จะต้องอาศัยการพิจารณาจากเอกสารแนวปฏิบัติที่เกี่ยวข้อง ซึ่งจะได้อธิบายต่อไปในส่วนของกระบวนการ

ในการดำเนินการแบ่งปันข้อมูลนั้นหากพิจารณาประกอบกับข้อมติที่ 2322/2016 จะพอทราบว่าข้อมติดังกล่าวยังคงคำแนะนำถึงพันธกรณีของรัฐสมาชิก (Reiterating the obligation of Member States) ให้ดำเนินการการควบคุมชายแดนให้ได้มีประสิทธิภาพ โดยวิธีการหนึ่งในนั้นคือการแบ่งปันข้อมูลระหว่างหน่วยงานที่มีอำนาจโดยลักษณะของการแบ่งปันข้อมูลตามข้อมตินี้จะต้องเป็นการแบ่งปันข้อมูลในลักษณะที่ “รวดเร็ว”²⁴⁵ ซึ่งเนื้อหาของข้อมูลที่ต้องแบ่งปันนั้นได้อธิบายไว้ในวรรคที่ 5 คือข้อมูลต่อไปนี้

1. ข้อมูลที่เป็นข่าวกรองเกี่ยวกับภัยคุกคามของการก่อการร้าย ซึ่งข้อมูลเหล่านั้นจะต้องถูกลดระดับ (Downgrading) จากข้อมูลที่มีสถานะเป็นความลับ มาเป็นข้อมูลที่ใช้อย่างเป็นทางการ ระหว่างหน่วยงานที่มีความรับผิดชอบในการควบคุมชายแดน เช่น สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย
2. ข้อมูลหนังสือเดินทางของบุคคลเพื่อใช้เป็นหลักฐานในการประเมินความเสี่ยง (Evidence-based traveller risk assessment) ต่อการเดินทางของผู้ก่อการร้าย นักรบต่างชาติ หรือบุคคลที่อยู่ในรายชื่อเฝ้าระวัง

²⁴⁴ United Nations Security Council Resolution 1373/2001, pp. 2(g)

²⁴⁵ United Nations Security Council Resolution 2322/2016, pp. preamble, 5

3.3.1.3 กระบวนการในการแบ่งปันข้อมูล

ในกระบวนการในการแบ่งปันข้อมูลเพื่อควบคุมชายแดนให้ได้มีประสิทธิภาพนั้น ตามข้อมติที่ 1373/2001 มิได้อธิบายถึงขั้นตอนกระบวนการและวิธีการอย่างไรที่จะเป็น “การแบ่งปันข้อมูลเพื่อควบคุมชายแดนให้มีประสิทธิภาพ” จึงจำเป็นที่จะต้องอาศัยการพิจารณาจากเอกสารแนวปฏิบัติที่เกี่ยวข้อง ซึ่งเอกสารสำคัญที่ได้อธิบายวิธีการแบ่งปันข้อมูลเพื่อการควบคุมชายแดนให้ได้มีประสิทธิภาพคือ **"Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of Foreign Terrorist Fighters"**²⁴⁶ ใน ข้อ ป ฎิ บั ตี ที่ 7 : Develop and implement Border Security and Management information exchange programs and mechanism ได้ระบุว่า

1. รัฐสมาชิกจะต้องสร้างช่องทางการสื่อสารเพื่อทำการแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องทั้งหมด อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย ซึ่งอาจจะอยู่ในรูปแบบของฐานข้อมูล ที่หน่วยงานภายในรัฐสามารถใช้งานได้ร่วมกัน
2. ฐานข้อมูลจะต้องแก้ไขจุดบกพร่องของการแบ่งปันข้อมูลระหว่างหน่วยงานภายในอยู่เสมอ หรือตั้งจัดคณะทำงานดูแลและคอยตรวจสอบแก้ไขปัญหา เพราะถือว่าหากอุปสรรคเกิดขึ้นจะส่งผลต่อการดำเนินมาตรการควบคุมชายแดนให้ได้มีประสิทธิภาพได้
3. มีการแบ่งปันข้อมูลที่เกี่ยวข้องเกือบทุกด้านของข้อมูลผู้โดยสาร ข้อมูลสินค้า รวมไปถึงข้อมูลที่ใช้ในการสืบสวนสอบสวน ข้อมูลการวิเคราะห์ความเสี่ยงของเจ้าหน้าที่หน่วยลาดตระเวน และข้อมูลของการมีส่วนร่วมในการปฏิบัติการข้ามพรมแดนพิเศษ (Special cross-border operational engagement information) ข้อมูลจากตำรวจอาชญากรรม (Criminal police) หน่วยอาชญากรรม (Organised crime units) หน่วยข่าวกรอง (Intelligence services) หน่วยงานด้านวีซ่า (Visa regime authorities) และทั้งหมดนี้นั้นจะต้องมีการดำเนินการที่ทันท่วงที และแม่นยำเพื่อประโยชน์ต่อการทำงานของหน่วยงานอื่นที่ต้องการเข้าถึงข้อมูล ณ เวลานั้น
4. การแบ่งปันข้อมูลนั้นไม่ควรจะจำกัดเพียงหัวข้อใดหัวข้อเดียว ควรจะมีการแบ่งปันข้อมูลที่หลากหลายจากหน่วยงานภายในที่เกี่ยวข้อง เพื่อขยายฐานข้อมูลให้ควบคุมเรื่องอื่นในอนาคต

²⁴⁶ UN Counter-Terrorism Centre (UNCCT), "Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters" (2016), [United Nations office for counter-terrorism](#), p.12

1. การจัดตั้งหน่วยงานในความร่วมมือระหว่างประเทศ

การแบ่งปันข้อมูลเพื่อควบคุมชายแดนให้ได้มีประสิทธิภาพหากปราศจากการร่วมมือระหว่างประเทศเสียแล้วนั้น คงจะดำเนินการให้ควบคุมชายแดนให้เกิดประสิทธิภาพไม่ได้ ในกระบวนการแบ่งปันข้อมูลระดับระหว่างประเทศ (International level) เอกสาร "Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of Foreign Terrorist Fighters" ข้อปฏิบัติที่ 8 : Establish Border Cooperation Centres ได้เสนอให้มีการจัดตั้งศูนย์ความร่วมมือชายแดน (Border Cooperation Centres – BCCs)

ข้อ 1 ศูนย์ความร่วมมือชายแดนจะทำหน้าที่เสมือนเป็นตัวกลางประสานงานทางข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องต่างๆ ภายในรัฐ ไม่ว่าจะเป็น สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย

ข้อ 2 ศูนย์ความร่วมมือชายแดนจะอำนวยความสะดวกในการแบ่งปันข้อมูลข้ามพรมแดนและตัวกลางช่วยเหลือระหว่างหน่วยงานภายในที่มีหน้าที่เกี่ยวข้อง (inter-alia the responsible authority) กับหน่วยงานบังคับใช้กฎหมาย หรือหน่วยงานของต่างประเทศ (Counterparts across the border) ของประเทศซึ่งอยู่ภายใต้ความร่วมมือในระดับความตกลงทวิภาคี และพหุภาคีภายใต้ความร่วมมือต่อการแบ่งปันข้อมูลและข้อมูลข่าวกรองเพื่อการต่อต้านการก่อการร้าย²⁴⁷

2. การกำหนดกลไกในความร่วมมือ

คณะมนตรีความมั่นคงแห่งสหประชาชาติได้รับรองข้อมติที่ 2322/2016 ถึงการเรียกร้องให้บรรดารัฐสมาชิกมีกระบวนการการแบ่งปันข้อมูลให้ชัดเจนขึ้น และเพื่ออธิบายการว่าในการที่รัฐสมาชิกจะดำเนินการมาตรการการควบคุมชายแดนให้ได้มีประสิทธิภาพ ตามต้องประสงค์ของข้อมติที่ 1373/2001 นั้น องค์ประกอบที่สำคัญคือจะต้องสร้างช่องทางของการแบ่งปันข้อมูลระหว่างหน่วยงานที่มีอำนาจ ที่เกี่ยวข้องทั้งหมดทั้งภายในประเทศ และระหว่างประเทศ ให้เกิดการเข้าถึงข้อมูลได้อย่างรวดเร็ว

ประการแรก กำหนดกลไกความร่วมมือในการแบ่งปันข้อมูลในระดับความตกลงทวิภาคีและพหุภาคีในข้อมูลที่ทำเป็นต่อการตรวจจับการเดินทางของการก่อการร้าย จากนั้นจะต้องมีช่องทางการสื่อสาร อาทิ ฐานข้อมูลกลางเพื่อให้เกิดการไหลเวียนของข้อมูลอย่างรวดเร็ว ระหว่างหน่วยงานของรัฐภายในความตกลง

ประการที่สอง หน่วยงานของรัฐที่มีหน้าที่คัดกรองการเดินทางของบุคคลก่อนเข้าหรือออกประเทศ อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หรือ

²⁴⁷ Ibid, pp. 14

หน่วยงานบังคับใช้กฎหมาย จะต้องสามารถใช้ข้อมูลเหล่านั้นในการวิเคราะห์และตรวจจับ ผู้ต้องสงสัยที่เกี่ยวข้องกับการก่อการร้ายได้ทันที²⁴⁸

ทั้งนี้ในเมื่อได้มีกลไกความร่วมมือระหว่างประเทศแบบพหุภาคีหรือทวิภาคีในการแบ่งปันข้อมูลอย่างรวดเร็ว ในทางระหว่างประเทศเพื่อการควบคุมชายแดนให้ได้มีประสิทธิภาพนั้นแล้ว ในเอกสาร "Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of Foreign Terrorist Fighters" ได้มีการแนะนำข้อกำหนดกลไกในความร่วมมือของรัฐสมาชิกว่าในการแบ่งปันข้อมูลระหว่างประเทศนั้น

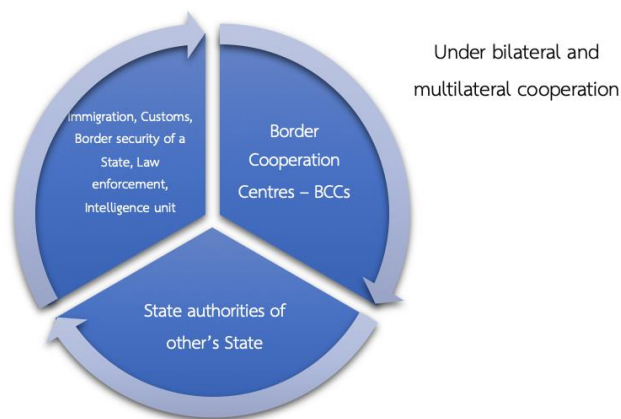
ข้อเสนอแนะแรก ศูนย์ความร่วมมือชายแดน ของแต่ละประเทศภายใต้ความร่วมมือควรจะมีบทบาทเป็นกลไกการแบ่งปันข้อมูลจากหน่วยงานต่างๆ ทั้งภายในประเทศของตนเอง หรือหน่วยงานของต่างประเทศที่อยู่ภายใต้ความร่วมมือ และเสมือนเป็นจุดติดต่อในการรับเรื่อง ติดต่อ ประสานงานช่วยเหลือทางข้อมูลที่เกี่ยวข้องต่อการจัดการชายแดน

ข้อเสนอแนะสอง ศูนย์ความร่วมมือชายแดนควรจะต้องทำการจัดประเภทระหว่าง “On request information” กับ “Ad hoc information” จากข้อมูลที่ทำกรแบ่งปัน โดยไม่ว่าข้อมูลนั้นจะเกี่ยวข้องกับ เหตุการณ์ คดีการสอบสวน หรือ ข้อมูลข่าวกรองที่เฉพาะเจาะจง เช่น การย้ายถิ่นที่ผิดปกติ การก่ออาชญากรรมข้ามพรมแดน

ข้อเสนอแนะที่สาม การดำเนินมาตรการการควบคุมชายแดนให้ได้มีประสิทธิภาพ นั้นศูนย์ความร่วมมือชายแดนจะต้องหาวิธีการของการประสานงานระหว่างพรมแดน เพื่อดำเนินการแบ่งปันข้อมูล เช่น การอำนวยความสะดวกของการติดต่อหรือที่อยู่ทางอิเล็กทรอนิกส์ มีช่องทางการประสานงานแบบเร่งด่วน หรือกำหนดหน่วยงาน “Hotline Unit” ภายในศูนย์เพื่อดำเนินรับเรื่องติดต่อ ประสานอย่างเร่งด่วน

²⁴⁸ United Nations Security Council Resolution 2322/2016, pp. preamble, 5

แผนผังโครงสร้าง : ลักษณะการแบ่งปันข้อมูลของศูนย์ความร่วมมือชายแดน (Border Cooperation Centres – BCCs)



3. ข้อท้าทายกับประเด็นนักรบต่างชาติ

ในข้อมติที่ 2178/2014 ให้มีการดำเนินมาตรการควบคุมชายแดนให้ได้มีประสิทธิภาพ (Effective border controls) ครอบคลุมไปถึงการต่อต้านนักรบต่างชาติ และจะต้องมีการแบ่งปันข้อมูลบุคคลที่กำลังจะมีการเดินทาง เพื่อใช้เป็นหลักฐานในการประเมินความเสี่ยง (Evidence-based traveller risk assessment) ต่อการเดินทางของนักรบต่างชาติ เพื่อให้ได้มาซึ่งข้อมูลในการวิเคราะห์และประเมิน²⁴⁹ ข้อมติที่ 2396/2017 รัฐสมาชิกจะต้องดำเนินการให้หน่วยงานที่เกี่ยวข้อง อาทิ สำนักงานตรวจคนเข้าเมือง สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย ใช้อำนาจตามกฎหมายภายในเพื่อเก็บและแบ่งปันข้อมูลของบุคคลที่มีมูลเหตุอันสมควร (Reasonable ground)ว่าจะเกี่ยวข้องต่อการเดินทางของนักรบต่างชาติ²⁵⁰

ประการแรก หน่วยงานภายในที่เกี่ยวข้องของรัฐ อาทิ สำนักงานตรวจคนเข้าเมือง สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย จะต้องเก็บข้อมูลของบุคคล เช่น ข้อมูลหนังสือเดินทาง ข้อมูลที่เกี่ยวข้องต่อการออกเอกสารประจำตัวอื่นๆ และข้อมูลเอกสารอนุญาตให้เข้าประเทศ (Visa) หรือข้อมูลที่เกี่ยวข้องกับบุคคลดังกล่าวที่ได้มาจากการประสานงานภายใต้ความร่วมมือ หรือข้อมูลของบุคคลจากองค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL)

ประการที่สอง หน่วยงานภายในที่เกี่ยวข้องของรัฐ อาทิ สำนักงานตรวจคนเข้าเมือง สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย จะต้องทำการแบ่งปันข้อมูลหนังสือเดินทางของบุคคลนั้นระหว่างกัน เพื่อใช้ข้อมูลที่ได้ในการประเมินและตรวจสอบบุคคลซึ่งมีมูลเหตุอัน

²⁴⁹ United Nations Security Council Resolution 2178/2014, pp. 2

²⁵⁰ United Nations Security Council Resolution 2396/2017, pp. 2,3,4

สมควร หรือเชื่อได้ว่าเป็นนักรบต่างชาติ มากไปกว่านั้นรัฐสมาชิกจะต้องประสานข้อมูลนั้นทันทีกับรัฐอื่นที่อยู่ภายใต้ความร่วมมือ รวมทั้งแบ่งปันข้อมูลดังกล่าวที่ถูกทำการประเมินออกมาแล้วแก่ องค์การตำรวจอาชญากรรมระหว่างประเทศ

ประการที่สาม หน่วยงานภายในที่เกี่ยวข้องของรัฐ อาทิ สำนักงานตรวจคนเข้าเมือง สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย 1.) จะต้องเก็บและแบ่งปันข้อมูลหนังสือเดินทางของบุคคล ที่ได้เดินทางไปยังพื้นที่แห่งความขัดแย้ง หรือมีมูลเหตุอันสมควรว่าบุคคลดังกล่าวกำลังจะเดินทางไปยังพื้นที่แห่งความขัดแย้ง 2.) จะต้องเก็บและแบ่งปันข้อมูลหนังสือเดินทางของครอบครัวของบุคคลนั้น ในกรณีที่สมาชิกในครอบครัวของเขามีประวัติการเดินทางไปยัง ประเทศบ้านเกิดหรือประเทศที่มีสัญชาติ (Countries of origin or nationality) หรือไปยังประเทศของพื้นที่ที่มีความขัดแย้ง (Countries of conflict zone) 3.) จะต้องเก็บและแบ่งปันข้อมูลหนังสือเดินทางของบุคคลเหล่านั้นระหว่างหน่วยงานภายในรัฐตนที่เกี่ยวข้องต่อการดำเนินการควบคุมชายแดนทั้งหมด หรือ 4.) จะต้องเก็บและแบ่งปันข้อมูลหนังสือเดินทางของบุคคลเหล่านั้นกับประเทศภายใต้ความร่วมมือ หรือ 5.) จะต้องเก็บและแบ่งปันข้อมูลหนังสือเดินทางของบุคคลเหล่านั้นกับประเทศโดยเฉพาะที่เป็นประเทศบ้านเกิดของบุคคลนั้น ประเทศที่บุคคลนั้นมีสัญชาติ ประเทศที่บุคคลนั้นมีถิ่นที่อยู่ถาวร หรือประเทศที่เป็นทางผ่านของการเดินทางของบุคคลนั้น 6.) แบ่งปันข้อมูลหนังสือเดินทางของบุคคลเหล่านั้นกับองค์การตำรวจอาชญากรรมระหว่างประเทศ

3.3.2 การตรวจบุคคลที่เดินทางเข้าประเทศด้วยข้อมูลผู้โดยสารล่วงหน้า ข้อมูลการบันทึกของผู้โดยสาร และข้อมูลลักษณะเฉพาะตัวบุคคล

ภัยคุกคามของการก่อการร้ายระหว่างประเทศ เป็นสิ่งที่ต้องเผชิญไม่เพียงแต่โดยหน่วยงานที่เกี่ยวข้องต่อการควบคุมชายแดนเท่านั้น แต่ยังรวมถึงสายการบิน (Airlines) และผู้ให้บริการสนามบินด้วย (Airport operators) ซึ่งการตรวจสอบความปลอดภัยจะต้องอาศัยข้อมูลเพื่อการประเมินถึงความเสี่ยงของผู้โดยสารก่อนออกเดินทาง (Prior to departure) ในขั้นตอนของการเช็คอินถือได้ว่ามีความสำคัญอย่างมาก โดยทั้งนี้หน่วยงานที่เกี่ยวข้องต่อการควบคุมชายแดนจะต้องมีหน้าที่คอยตรวจสอบข้อมูลของผู้เดินทางอย่างสม่ำเสมอ รวมทั้งการประเมินถึงความเสี่ยงเปลี่ยนแปลงของปัจจัยเสี่ยง (Risk factors) ที่อาจจะเกิดขึ้นจากวิธีการใหม่ๆของการก่อการร้ายในส่วนของการเดินทางขาเข้าด้วยเช่นกัน²⁵¹

²⁵¹ World Customs Organization, International Air Transport Association, and International Civil Organization, "Fact sheet of Guidelines on advance passenger information (API)" (2014), pp.5, Available from https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/api-guidelines-main-text_2014.pdf

ระบบตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า (Advance Passenger Information System – APIS) คือการนำข้อมูลในรายละเอียดของเที่ยวบินโดยสายของบริษัทยุโรปก่อนออกเดินทาง ให้แก่หน่วยงานควบคุมชายแดนในประเทศ เพื่อที่แบ่งปันรายละเอียดข้อมูลนั้นด้วยวิธีการทางอิเล็กทรอนิกส์ไปยังหน่วยงานควบคุมชายแดนในประเทศปลายทางของเที่ยวบินโดยสายนั้น นอกจากนี้การแบ่งปันข้อมูลเพื่อตรวจสอบและคัดกรองผู้โดยสารล่วงหน้ายังสามารถทำหน้าที่เป็นเครื่องมือในการตัดสินใจของหน่วยงานควบคุมชายแดนในการอนุญาตผู้โดยสารให้ขึ้นเครื่องบินหรือเข้าสู่ประเทศ การเก็บข้อมูลรายละเอียดของผู้โดยสารจะถูกทำการตรวจสอบสำหรับการอนุญาตขึ้นเครื่องหรือเข้าสู่ประเทศจากหน่วยงานควบคุมชายแดน

ทั้งนี้ยังเพื่อตรวจสอบและคัดกรองจากข้อมูลเพิ่มเติมว่าผู้โดยสารหรือลูกเรือนั้นได้ถูกระบุไว้ในรายชื่อของบุคคลที่อยู่ภายใต้การห้ามเดินทางหรือการคว่ำบาตรของคณะมนตรีความมั่นคงแห่งสหประชาชาติหรือเปล่า รวมทั้งสายการบินที่เป็นคนให้ข้อมูลหน่วยงานควบคุมชายแดน ก็สามารถใช้บริการตรวจสอบและคัดกรองผู้โดยสารล่วงหน้าเพื่อปฏิบัติตามกฎหมายที่เกี่ยวข้องของประเทศที่เป็นจุดหมายของการเดินทาง (Relevant legislation of the countries they fly to) เช่น กฎหมายที่เกี่ยวข้องกับการห้ามการเดินทาง (Legislation implementing travel bans)²⁵² จึงนำมาสู่มาตรการแบ่งปันข้อมูล

3.3.2.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

1. การแบ่งปันข้อมูลผู้โดยสารล่วงหน้า

มาตรการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติในข้อมติที่ 2178/2016 และ 2309/2016 มีการกำหนดพันธกรณีให้บรรดารัฐสมาชิกของสหประชาชาติดำเนินการดังต่อไปนี้

ประการแรก เรียกร้องให้บรรดารัฐสมาชิก (Calls upon Member States) ออกมาตรการตามกฎหมายภายในเพื่อให้มีสร้างช่องทางการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) จากสายการบินที่ดำเนินกิจการภายใต้เขตอำนาจของรัฐตน ให้กับหน่วยงานที่มีความเหมาะสมในการดำเนินงานเพื่อตรวจจับ การเดินทางขาออกจากประเทศของตน การเดินทางขาเข้าประเทศของตน รวมทั้งการเดินทางที่มีการเปลี่ยนผ่านประเทศของตน (Transit through their territories) ทั้งวิธีการของการเดินทางด้วยอากาศยานพาณิชย์และอากาศยานส่วนตัว²⁵³ รวมไปถึงวิธีการเดินทางอื่นๆ ของบุคคลที่มีรายชื่อตามที่คณะกรรมการเกี่ยวกับมาตรการ

²⁵² Ibid, pp. 8

²⁵³ United Nations Security Council Resolution 2309/2016, pp. 6(g)

ลงโทษ (Sanctions Committees) ได้ระบุไว้โดยอาศัยอำนาจตาม ข้อมติที่ 1267/1999 และข้อมติที่ 1989/2011

ประการที่สอง ข้อมติ 2178/2014 และ 2309/2016 ข้างต้นยังได้เรียกร้องให้บรรดารัฐสมาชิก (Calls upon Member States) ดำเนินการแบ่งปันข้อมูลการ รายงานเกี่ยวกับการเดินทาง ขาออก การเดินทางขาเข้าประเทศของตน และการเดินทางที่มีการเปลี่ยนผ่านประเทศของตน รวมไปถึงถึงวิธีการเดินทางอื่นๆ ของบุคคลที่มีรายชื่อตามที่คณะกรรมการเกี่ยวกับมาตรการลงโทษได้ระบุไว้²⁵⁴ โดยต้องแบ่งปันข้อมูลเหล่านั้นโดยไม่ชักช้ากับประเทศที่บุคคลนั้นมีถิ่นที่อยู่ (The State of residence) หรือบุคคลนั้นมีสัญชาติ (The State of Nationality) โดยผ่านกระบวนการตามกฎหมายภายในและคำนึงถึงพันธกรณีระหว่างประเทศว่าด้วยสิทธิมนุษยชน

2. การแบ่งปันข้อมูลการบันทึกของผู้โดยสาร

ในมาตรการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาตินั้น ตามข้อมติที่ 2396/2017 ได้ระบุหลักการของการแบ่งปันข้อมูลการบันทึกของผู้โดยสาร (Passenger name record – PNR) ไว้ซึ่งผู้เขียนจะขอแบ่งอธิบายในแต่ละประการดังต่อไปนี้

ประการแรก ข้อมติได้ตัดสินใจให้รัฐสมาชิก (Decides that Member States shall) พัฒนาความสามารถในการเก็บข้อมูล ประมวลผลข้อมูล และวิเคราะห์ข้อมูล ซึ่งข้อมูลบันทึกการเดินทางของผู้โดยสาร (Passenger Name Record – PNR) และหาช่องทางที่สะดวกต่อการแบ่งปันข้อมูลระหว่างหน่วยงานระดับชาติที่มีอำนาจหน้าที่ เพื่อดำเนินการต่อความประสงค์ของข้อมติในเป้าหมายต่อการป้องกัน ติดตาม สืบสวนสอบสวน ความผิดที่เกี่ยวข้องต่อการก่อการร้ายและเกี่ยวข้องกับการเดินทาง²⁵⁵

ประการสอง ข้อมติได้ตัดสินใจให้บรรดารัฐสมาชิกจะต้องพัฒนาความสามารถในการเก็บซึ่งข้อมูล ประมวลผล และวิเคราะห์ ซึ่งข้อมูลการบันทึกของผู้โดยสารโดยอาศัยการแบ่งปันข้อมูลดังกล่าวจากบริษัทสายการบินที่ได้ดำเนินการอยู่ภายใต้เขตอำนาจของรัฐตน ในกระบวนการต่างๆของการดำเนินการต่อข้อมูลการบันทึกของผู้โดยสาร นั้นจะต้องเป็นไปตามมาตรฐานสากลที่ถูกกำหนดโดยองค์การการบินพลเรือนระหว่างประเทศ

ประการที่สาม รัฐสมาชิกจะต้องแน่วแน่ในใจว่าข้อมูลการบันทึกของผู้โดยสาร จะถูกนำไปดำเนินการเพื่อการต่อต้านการก่อการร้ายของหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องในการดำเนินการที่มีวัตถุประสงค์เพื่อป้องกัน ติดตาม สืบสวนสอบสวน ซึ่งการกระทำของการก่อการร้าย

²⁵⁴ United Nations Security Council Resolution 2178/2014, pp. 9

²⁵⁵ United Nations Security Council Resolution 2396/2017, pp.12

รวมถึงการเดินทางที่เกี่ยวข้องต่อการก่อการร้าย และจะต้องดำเนินการเหล่านั้นให้สอดคล้องกับหลักการที่ว่าด้วยสิทธิมนุษยชน เสรีภาพขั้นพื้นฐาน

ประการที่สี่ ข้อมติได้สนับสนุนให้รัฐสมาชิกได้แบ่งปันข้อมูลของข้อมูลการบันทึกของผู้โดยสาร ต่อรัฐสมาชิกของสหประชาชาติที่น่าจะเกี่ยวข้อง หรือที่คาดว่าจะสามารถทำการติดตามซึ่งผู้ก่อการร้ายหรือนักรบต่างชาติ ที่ได้เดินทางกลับไปในประเทศ ที่มีฐานะที่เป็นประเทศต้นทาง ประเทศเจ้าของสัญชาติ ประเทศปลายทาง ประเทศต้องการย้ายถิ่นไป หรือประเทศปลายทางที่สาม โดยเฉพาะผู้ก่อการร้าย นักรบต่างชาติ หรือบุคคลซึ่งมีรายชื่อตามที่คณะกรรมการเกี่ยวกับมาตรการลงโทษ ได้ระบุไว้โดยอาศัยอำนาจตาม ข้อมติที่ 1267/1999 ข้อมติที่ 1989/2011 และข้อมติที่ 2253/2015

3. การแบ่งปันข้อมูลลักษณะเฉพาะตัวของผู้โดยสาร

ประการแรก ข้อมติที่ 2322/2016 และ 2396/2017 ได้ตัดสินใจให้บรรดารัฐสมาชิก (Decides that Member States shall) พัฒนาระบบการเก็บข้อมูลไบโอเมตริกซ์ (Biometric data) อาทิ ข้อมูลลายนิ้วมือ (Fingerprints) ข้อมูลการถ่ายภาพ (Photographs) ข้อมูลการจดจำใบหน้าบุคคล (Facial recognition) และข้อมูลชีวประวัติ (Biographical data) หน่วยงานระดับชาติ ที่มีอำนาจหน้าที่ อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หน่วยงานบังคับใช้กฎหมาย หรือศูนย์ความร่วมมือชายแดน

ประการที่สอง หน่วยงานระดับชาติที่มีอำนาจหน้าที่ ประการแรก จะต้องทำการแบ่งปันข้อมูลเหล่านี้ต่อรัฐสมาชิกอื่นภายใต้ความร่วมมือระหว่างประเทศ ตลอดจนต่อหน่วยงานระหว่างประเทศ หรือองค์การตำรวจอาชญากรรมระหว่างประเทศ ที่มีส่วนเกี่ยวข้องหรือรับรู้ถึงบุคคลผู้เป็นเจ้าของข้อมูลอัตลักษณ์เหล่านั้นที่เกี่ยวข้องต่อการก่อการร้าย²⁵⁶

3.1 ในประเด็นข้อท้าทายเกี่ยวกับการเดินทางของนักรบต่างชาติ

ประการแรก มาตรการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ได้รับรอง ข้อมติที่ 2322/2016 ซึ่งได้เรียกร้องให้บรรดารัฐสมาชิกของสหประชาชาติแบ่งปันข้อมูลชีวประวัติบุคคล (Biographical information) และข้อมูลชีวภาพบุคคล (Biometric information) ของนักรบต่างชาติ ผู้ก่อการร้ายหรือกลุ่มผู้ก่อการร้าย รวมไปถึงข้อมูลอื่นๆที่สามารถแสดงให้เห็นถึงลักษณะของความสัมพันธ์ของบุคคลกับการก่อการร้าย

ประการที่สอง ข้อมติที่ 2396/2017 ได้ตัดสินใจให้บรรดารัฐสมาชิกสหประชาชาติจะต้องดำเนินการพัฒนาระบบเก็บข้อมูลชีวภาพบุคคล อาทิ ลายนิ้วมือ (Fingerprints) รูปถ่าย

²⁵⁶ Ibid, pp. 15

(Photographs) การจดจำใบหน้า (Facial recognition) หรือข้อมูลอื่นที่ระบุว่าเป็นข้อมูลไบโอเมตริกซ์ (Biometric data) เพื่อดำเนินการตรวจสอบและระบุบุคคลซึ่งเป็นผู้ก่อการร้าย หรือนักรบต่างชาติ

● สรุปพันธกรณีทั้งสามข้อที่ได้อธิบายมาในข้างต้น

จากการพิจารณาข้อมติทั้งหมดที่กล่าวมาข้างต้น การแบ่งปันข้อมูลต่อการจัดการตรวจคนเข้าเมืองจะสรุปได้ในแต่ละประการดังนี้

1. การแบ่งปันข้อมูลระดับภายในรัฐ คณะมนตรีความมั่นคงแห่งสหประชาชาติต้องการที่จะให้รัฐต่าง ๆ นั้นหาช่องทางต่อการแบ่งปันข้อมูลระหว่างหน่วยงานภายในของรัฐตนที่มีหน้าที่เกี่ยวข้อง ต่อมาตรการการจัดการตรวจคนเข้าเมืองเพื่อการต่อต้านการก่อการร้าย ซึ่งหน่วยงานภายในทั้งหลายที่เกี่ยวข้องจะต้องดำเนินการรวบรวมการเก็บข้อมูล (Processing and collecting data) คือ

1. ข้อมูลผู้โดยสารล่วงหน้า (API)
2. ข้อมูลการเดินทางของผู้โดยสาร (PNR)
3. ข้อมูลไบโอเมตริกซ์

และมีการแบ่งปันข้อมูลทั้ง 3 ลักษณะนี้ระหว่างหน่วยงานของรัฐในระดับภายในชาติ และภาคเอกชนที่เกี่ยวข้อง อาทิ สายการบิน และผู้ให้บริการสนามบิน

2. การแบ่งปันข้อมูลระดับระหว่างรัฐ เมื่อได้ดำเนินการให้มีระบบการแบ่งปันข้อมูลระหว่างหน่วยงานภายในของรัฐแล้ว รัฐต่างๆจะต้องมีช่องทางให้การแบ่งปันข้อมูลตามที่ข้อมติได้กำหนดเหล่านั้นผ่านความร่วมมือระหว่างประเทศในเรื่องประสานงานการจัดการตรวจคนเข้าเมือง (International coordinated border management) เช่น การแบ่งปันข้อมูลภายใต้ความร่วมมือการจัดการตรวจคนเข้าเมืองกับกลุ่มประเทศที่คาดว่าเป็นประเทศที่เป็นถิ่นที่อยู่ของผู้ก่อการร้ายหรือผู้ก่อการร้ายนั้นมีสัญชาติ (The State of residence or nationality) ประเทศที่เป็นต้นทางผ่าน หรือย้ายถิ่นฐานของผู้ก่อการร้าย

3.3.2.2 สารบัญญัตินี้ของข้อมูล

1. ข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API)

ข้อมูลผู้โดยสารล่วงหน้าโดยทั่วไปแล้วผู้ให้บริการสายการบินจะเป็นผู้ทำการเก็บข้อมูลนี้ เมื่อผู้โดยสารคนนั้นทำการเช็คอินผ่านระบบของสายการบิน ข้อมูลจะถูกเก็บและบันทึกไว้ในฐานข้อมูลของบริษัททันที ข้อมูลเหล่านั้นจะประกอบไปด้วย

ข้อมูลผู้โดยสารล่วงหน้า
(Advance Passenger
Information – API)

รูปในหนังสือเดินทาง, ชื่อเต็ม, วันเกิด, เพศ, สัญชาติ, ประเภทเอกสารการเดินทาง (หนังสือเดินทางหรือบัตรประจำตัวประชาชน), หมายเลขหนังสือเดินทางหรือบัตรประจำตัวประชาชน, ประเทศที่ออกหนังสือเดินทางหรือบัตรประจำตัวของบุคคล, วันที่ออกหนังสือเดินทางหรือวันหมดอายุของหนังสือเดินทาง²⁵⁷

2. ข้อมูลการบันทึกของผู้โดยสาร (Passenger name record – PNR)

องค์กรอาชญากรรมและการก่อการร้ายมักมีส่วนเกี่ยวข้องกับการเดินทางระหว่างประเทศ (International traveling) อยู่เป็นเสมอ เพราะเหล่าผู้ก่อการร้ายจะอาศัยการเดินทางเพื่อทำกิจกรรมต่างๆ เช่น การรับสมัครบุคคลให้เข้าร่วมกับแนวคิดของกลุ่ม การเดินทางของนักรบต่างชาติ เพื่อไปฝึกรบและกลับมายังประเทศเป้าหมายของการก่อเหตุ ตลอดจนการเดินทางเพื่อพบปะกับกลุ่มเครือข่ายผู้สนับสนุนทั้งการเงินและอาวุธ เพื่อดำเนินการต่อต้านการเดินทางเหล่านี้ดังกล่าว ในปัจจุบันมีการอาศัยเครื่องมือของการแบ่งปันข้อมูลส่วนบุคคลระหว่างหน่วยงานบังคับใช้กฎหมายแต่ละประเทศภายใต้การร่วมมือเพื่อต่อต้านการก่อการร้าย โดยการใช้ระบบบันทึกข้อมูลของผู้โดยสาร (Passenger name record – PNR)²⁵⁸ ซึ่งมีส่วนสำคัญอย่างมากต่อประสิทธิภาพของการดำเนินการควบคุมชายแดนเพื่อต่อต้านการก่อการร้าย หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องต่อการดำเนินการควบคุมชายแดนจะสามารถอาศัยข้อมูลในระบบนี้ ในการระบุอัตลักษณ์ของผู้ก่อการร้ายและนักรบต่างชาติ รวมไปถึงการนำข้อมูลที่ได้สามารถวิเคราะห์ถึงความเคลื่อนไหวของการก่อการร้าย แผนการในการก่อเหตุในอนาคต ทั้งนี้ระบบดังกล่าวจะช่วยให้องค์กรที่เกี่ยวข้องต่อการควบคุมชายแดนสามารถดำเนินการตามกฎหมายในการต่อต้านผู้ก่อการร้ายเหล่านี้ทันทีที่จุดตรวจคนเข้าเมือง

โดยปกติแล้วการแบ่งปันข้อมูลของผู้โดยสาร (Passenger name record – PNR) จะถูกดำเนินการบันทึกเข้าไปอยู่ในระบบคอมพิวเตอร์ ของบริษัทสายการบินเพื่อวัตถุประสงค์ ในการให้บริการเดินอากาศ เมื่อผู้โดยสารทำการจองตั๋วจะต้องมีการกรอกรายละเอียดข้อมูลส่วนตัวของตน บางอย่างเท่าที่จำเป็นต่อความสะดวกในการให้บริการของสายการบิน หากหน่วยงานบังคับใช้กฎหมายสามารถเข้าถึงข้อมูลในส่วนนี้ของผู้โดยสารจากบริษัทสายการบิน หน่วยงานบังคับใช้

²⁵⁷ United Kingdom government services and information, "Advance Passenger Information before you travel" (2020), Retrieved from <https://www.nidirect.gov.uk/articles/advance-passenger-information-you-travel>

²⁵⁸ European Council, Council of the European Union, "Regulating the use of passenger name record (PNR) data" (2016), Retrieved from <https://www.consilium.europa.eu/en/policies/against-terrorism/passenger-name-record/>

กฎหมายจะมีความสามารถในการดำเนินการป้องกัน (Safeguard)²⁵⁹ บุคคลผู้ทำการเดินทางที่มีความเสี่ยงว่าจะเกี่ยวข้องกับการก่อการร้ายได้ ในหลายประเทศมีการดำเนินการแบ่งปันข้อมูลดังกล่าวระหว่างบริษัทสายการบินกับหน่วยงานบังคับใช้กฎหมายของรัฐไปแล้ว แต่ก็เกิดปัญหาขึ้นว่าหน่วยงานของรัฐได้ใช้ข้อมูลเหล่านั้นไปในทางที่เกิดความเสียหายของบุคคล หรือใช้ข้อมูลไปเกินขอบเขตจุดประสงค์ของการดำเนินมาตรการป้องกัน และการดูแลกำกับ (Oversight) เพราะโดยปกติแล้วข้อมูลบันทึกของผู้โดยสาร เป็นข้อมูลที่มีลักษณะกว้างมากกว่าลักษณะของข้อมูลผู้โดยสารล่วงหน้า หรือเรียกได้ว่าเป็นข้อมูลในรายละเอียดที่เกี่ยวข้องกับบุคคลนั้นๆต่อการเดินทางอย่างรอบด้าน

ข้อมูลบันทึกของผู้โดยสาร (Passenger name record – PNR)

รายละเอียดของตัวเครื่องบิน, รายละเอียดของการเช็คอิน, ประวัติส่วนตัวของผู้โดยสาร, วันเดินทาง, กำหนดการเดินทาง (Itinerary), รายละเอียดของการติดต่อ, ชื่อบริษัทนำเที่ยว (Name of travel agency), วิธีการชำระเงิน (Means of payment), รายละเอียดที่นั่ง, ข้อมูลสัมภาระ (Baggage information), รายละเอียดข้อมูลที่สามารถระบุตัวตนของบุคคล (ชื่อ, นามสกุล, วันเกิด, สัญชาติ, เพศ, อื่นๆ), รายละเอียดสั่งอาหารบนเครื่อง (Meal ordered on board), ข้อมูลทางการแพทย์ของบุคคล (Personal medical information), ข้อมูลบัตรเครดิตและเดบิต²⁶⁰

3. ข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว (Traveler identity)

แนวคิดของการใช้ข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว เพื่อต่อต้านการเดินทางของการก่อการร้าย มีขึ้นอย่างชัดเจนภายหลังเหตุการณ์วินาศกรรม 9/11 ที่ประเทศสหรัฐอเมริกา ซึ่งการแบ่งปันข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว นั้นถือเป็นเครื่องมือทางเทคโนโลยีที่สำคัญ และสามารถช่วยให้หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องต่อการควบคุมชายแดนดำเนินการต่อต้านการก่อการร้าย โดยการบ่งบอก ถึงลักษณะเฉพาะตัวของบุคคลที่สงสัยว่าเกี่ยวข้องต่อการก่อการร้าย จากการวิเคราะห์อาศัยข้อมูลลักษณะทางกายภาพของมนุษย์ (Human physical

²⁵⁹ Security Council, "Letter dated 27 December 2019 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2019), pp. 293

²⁶⁰ European Parliamentary Research Service Blog, "Passenger Name Records (PNR) For The Prevention Of Terrorist Offences And Serious Crime" (2016), Retrieved from <https://epthinktank.eu/2019/08/14/passenger-name-records-pnr-for-the-prevention-of-terrorist-offences-and-serious-crime-european-parliament-impact-2014-2019/>

characteristics)²⁶¹ ข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยวที่สามารถที่จะช่วยในการระบุตัวตนของบุคคลเกิดขึ้นได้ในทันที (Instantaneous identification) โดยหน่วยงานบังคับใช้กฎหมายที่ทำหน้าที่ตรวจคนเข้าเมืองที่สนามบิน พรหมแดนเข้าภายในประเทศ (Borders of the nation) หรือท่าเรือเข้าประเทศ (National ports of entry) สามารถดำเนินมาตรการป้องกันการเข้าสู่ประเทศของบุคคลหรือทำการสืบสวนสอบสวนบุคคลได้ในเวลาที่ทันการ

นอกจากนี้หน่วยงานยังสามารถใช้ประโยชน์เพื่อการตรวจจัดการปลอมแปลงเอกสารเดินทางหรือเอกสารเดินทางที่ถูกโจรกรรมโดยผู้ก่อการร้าย รวมทั้งการใช้เอกสารในการเดินทางที่เป็นของปลอม ของเหล่าบรรดานักรบต่างชาติ ที่มีการรายงานจำนวนในปัจจุบันที่สูงขึ้น ซึ่งโดยทั่วไปแน่นอนว่าข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยวจะต้องตรงกับข้อมูลในเอกสารเดินทางหรือเอกสารอนุญาตเข้าประเทศ (Visa) ของตัวนักท่องเที่ยวเองเท่านั้น²⁶² จากปัญหาที่เกิดขึ้นในปัจจุบันนั้นการก่อการร้ายได้อาศัยวิธีการที่หลากหลาย เพื่อที่จะทำการเดินทางไปในที่ต่างๆทั่วโลกโดยปราศจากการตรวจจับของหน่วยงานที่มีหน้าที่ควบคุมชายแดน การจะแก้ปัญหาที่กล่าวมานั้นรัฐต่างๆจำนวนไม่น้อย ได้ริเริ่มการใช้เครื่องมือที่จะช่วยในการต่อต้านการก่อการร้ายที่ตามทันต่อวิธีการใหม่ๆ ในปัจจุบันคือการแบ่งปันข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว เพื่อการต่อต้านการก่อการร้าย²⁶³ ผู้เขียนจะขอแบ่งประเด็นเพื่ออธิบายข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว ให้ทราบอย่างเข้าใจว่าข้อมูลนี้มีหลักๆอยู่ 2 ลักษณะคือ 1.) ข้อมูลชีวประวัติบุคคล (Biographical information) 2.) ข้อมูลชีวภาพบุคคล (Biometric information)

3.1 ข้อมูลชีวประวัติบุคคล (Biographical information)

ข้อมูลชีวประวัติของบุคคลโดยทั่วไปแล้วจะเป็นข้อมูลที่เป็นที่ประจักษ์ได้ทั่วไป เช่น ข้อมูลที่แสดงอยู่เอกสารเดินทาง ข้อมูลที่อยู่ในหนังสือเดินทางของบุคคล รวมไปถึงข้อมูลในเอกสารขอเข้าประเทศ (Visa) หรือเอกสารในการเข้าประเทศที่หน่วยตรวจคนเข้าเมืองมีให้กรอก

²⁶¹ John Woodward, *A former CIA operations officer, "Biometrics: facing up to terrorism" (2001).*

²⁶² Security Council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", *the President of the Security Council* (2018), p. 13-17

²⁶³ United Nations Counter-Terrorism Office, "United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism" Document Available from https://www.un.org/sc/ctc/wp-content/uploads/2019/03/UNOCT-Biometrics-Summary-Bro_WEB.pdf

ข้อมูลชีวประวัติบุคคล (Biographical information)	ชื่อ, ที่อยู่, เพศ, สถานภาพสมรส, วันเดือนปีเกิด, ประวัติการจ้างงาน, การศึกษา, สถานที่เกิด, เชื้อชาติ, กลุ่มชาติพันธุ์, ประวัติศาสตร์ทางสังคม (Social History) ²⁶⁴
---	--

3.2 ข้อมูลชีวภาพบุคคล (Biometric information)

ข้อมูลไบโอเมตริกเป็นข้อมูลของลักษณะทางกายภาพของบุคคล ซึ่งสามารถใช้ตรวจสอบในการระบุตัวตนของบุคคลนั้นๆ ได้ผ่านเครื่องทางดิจิทัล ประสิทธิภาพของการใช้ระบบข้อมูลไบโอเมตริก อยู่ในขั้นที่สามารถจะพิสูจน์ลักษณะเฉพาะของบุคคลได้อย่างแม่นยำ จึงเหมาะสมที่จะนำระบบดังกล่าวมาใช้ในหน่วยงานที่มีการดำเนินการเกี่ยวกับการรักษาความมั่นคง ซึ่งข้อมูลไบโอเมตริกมีอยู่ในหลากหลายรูปแบบดังต่อไปนี้

ข้อมูลชีวภาพบุคคล (Biometric information)	ลายนิ้วมือ (Fingerprints), ลายฝ่ามือ (Palmprint), ดีเอ็นเอ (DNA), รูปทรงใบหน้า (Facial geometry), เสียง (Voice identification), จอประสาทตาเรตินา (Retina), รูปแบบม่านตา (Iris patterns scans), การจดจำใบหน้า (Face recognition), สแกนร่างกาย (Body scan), รูปทรงของมือ (Hand geometry) ²⁶⁵
--	---

3.3.2.3 กระบวนการในการแบ่งปันข้อมูล

1. โครงสร้างของกระบวนการ

1.1 ข้อมูลข้อมูลผู้โดยสารล่วงหน้า

ในข้อมติที่ 2396/2017 ข้อมติได้ตัดสินให้บรรดารัฐสมาชิกจะต้องดำเนินการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าจากสายการบินที่ดำเนินกิจการภายใต้เขตอำนาจของรัฐตน โดยที่จะต้องสอดคล้องตามมาตรฐานในเก็บข้อมูลและการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าขององค์การการบินพลเรือนระหว่างประเทศ (Standard established by International Civil Aviation Organization - ICAO)²⁶⁶ และดำเนินมาตรการดังกล่าวตามพันธกรณีในการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าต่อการเดินทางของนักรบต่างชาติ สุดท้ายรัฐสมาชิกจะต้องแน่นอนใจว่ากระบวนการวิเคราะห์ข้อมูล (API

²⁶⁴ United Nations Counter-Terrorism Office, "United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism" (2018), p.11, Document Available from https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf

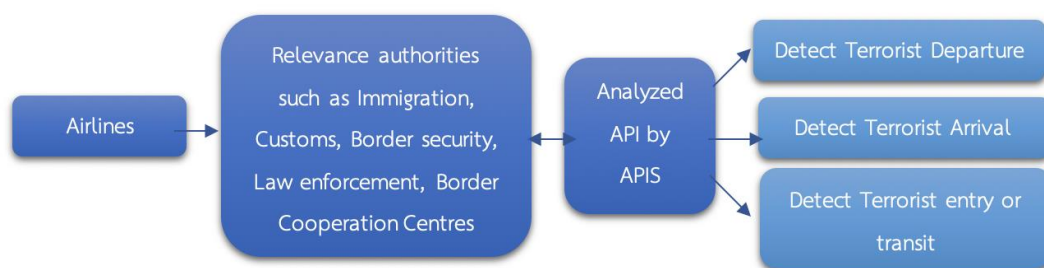
²⁶⁵ Ibid, p. 12

²⁶⁶ United Nations Security Council Resolution 2396/2017, pp. 11

analyzed) รวมถึง การเก็บข้อมูลผู้โดยสารล่วงหน้า การประเมินข้อมูลผู้โดยสารล่วงหน้า ของหน่วยงานเกี่ยวข้องที่มีอำนาจ เช่น สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หน่วยงานบังคับใช้กฎหมาย หรือศูนย์ความร่วมมือชายแดน ได้ปฏิบัติงานเพื่อวัตถุประสงค์ในการป้องกัน ตรวจจับ และสอบสวนการกระทำความผิดของผู้ก่อการร้าย และการเดินทางของผู้ก่อการร้าย ให้สอดคล้องและเคารพหลักการสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน

ข้อมูลที่จะต้องทำการแบ่งปันนั้นได้ระบุไว้ในข้อมติที่ 2396/2017 ว่ารัฐสมาชิกจะต้องดำเนินการให้มีระบบตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า (Advance Passenger Information System – APIS) โดยที่หน่วยงานที่มีหน้าที่รับผิดชอบของรัฐจะต้องมีความสามารถในการขอเข้าถึง (Require to access) ข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) จากบริษัทสายการบินที่มีการก่อตั้งกิจการภายใต้เขตอำนาจของรัฐสมาชิกนั้น²⁶⁷ วัตถุประสงค์เพื่อ 1.) ติดตาม (Detect) การเดินทางขาออก (Departure) ของบุคคลที่ต้องสงสัยจากอาณาเขตของรัฐสมาชิก 2.) ติดตามถึงการเดินทางของบุคคลที่ต้องสงสัยที่เข้ามาท่องเที่ยวภายในอาณาเขตของรัฐสมาชิก 3.) ติดตามถึงการเดินทางของบุคคลที่ต้องสงสัยที่จะเข้ามาในหรือเข้ามาในเพื่อเป็นทางผ่าน (Transit) ซึ่งอาณาเขตของรัฐสมาชิก โดยใช้วิธีการเดินทาง เช่น เครื่องบินพลเรือน หรือวิธีการอพยพของนักรบต่างชาติและผู้ก่อการร้ายที่อาจจะเข้าเมืองแบบผิดกฎหมาย

แผนผังโครงสร้าง : การแบ่งปันข้อมูล API ระหว่างหน่วยงานรัฐกับบริษัทเอกชนสายการบิน



ยิ่งไปกว่านั้นในข้อมติดังเรียกร้องให้บรรดารัฐสมาชิกแบ่งปันข้อมูลการรายงาน ข้อมูลการเดินทางขาออกจากอาณาเขตของตน ข้อมูลการเดินทางท่องเที่ยวภายในอาณาเขตของตน ข้อมูลการเดินทางเข้ามาในหรือเข้ามาในเพื่อเป็นทางผ่านตนซึ่งอาณาเขตของตน ด้วยการแบ่งปันข้อมูลการรายงานเหล่านี้ ต่อ 1.) ประเทศที่เป็นถิ่นที่อยู่ของบุคคลหรือบุคคลนั้นมีสัญชาติ (The State of residence or nationality) 2.) ประเทศที่เป็นต้นทาง ทางผ่าน หรือย้ายถิ่นฐานของบุคคล ซึ่งรัฐสมาชิกจะต้องแนบแนใจว่าข้อมูลผู้โดยสารล่วงหน้า ที่ตนสามารถเข้าถึงได้จากบริษัทสายการบินนั้นได้รับการ

²⁶⁷ United Nations Security Council Resolution 2396/2017, pp 11

วิเคราะห์จากหน่วยงานที่มีหน้าที่ที่เกี่ยวข้องทั้งหมดก่อนจะนำข้อมูลนั้นไปใช้เพื่อการตรวจจับการ
เดินทางของการก่อการร้าย²⁶⁸

แผนผังโครงสร้าง : การแบ่งปันข้อมูลการรายงานระหว่างหน่วยงานภายในรัฐกับต่างประเทศ



1.2 ข้อมูลการบันทึกของผู้โดยสาร

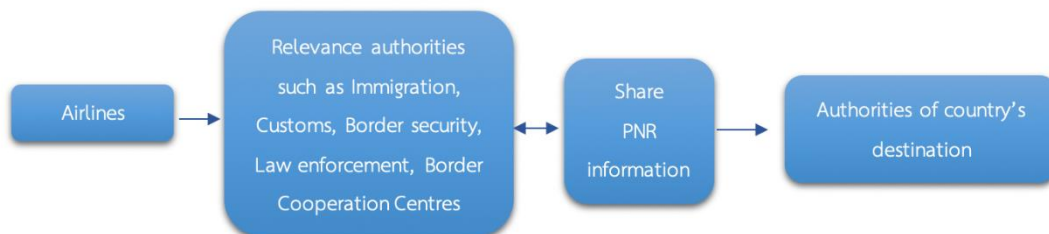
องค์การการบินพลเรือนระหว่างประเทศ ทำงานกับบรรดารัฐสมาชิกของตนให้การปฏิบัติ
ตามมาตรฐานสำหรับการเก็บ การใช้ การแบ่งปัน ป้องกัน ประมวล ซึ่งข้อมูลข้อมูลการบันทึกของ
ผู้โดยสาร²⁶⁹

ข้อสังเกต จากการพิจารณาข้อมติของคณะมนตรีความมั่นคงแห่งสหประชาชาติว่าด้วยการ
แบ่งปันข้อมูลทั้ง ข้อมูลผู้โดยสารล่วงหน้าและ ข้อมูลการบันทึกของผู้โดยสาร ซึ่งทั้งสองลักษณะข้อมูล
นี้จะต้องดำเนินการแบ่งปันกับผู้มีส่วนเกี่ยวข้อง ต่างก็เป็นพันธกรณีที่หน่วยงานของบรรดารัฐสมาชิก
เช่น สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หน่วยงานบังคับใช้
กฎหมาย หรือศูนย์ความร่วมมือชายแดน จะต้องดำเนินการโดยอาศัยการแบ่งปันข้อมูลเหล่านี้จาก
บริษัทสายการบินที่ให้บริการภายใต้เขตอำนาจ และจะต้องแบ่งปันข้อมูลที่ได้ต่อหน่วยงานของ
ประเทศที่เป็นจุดหมายปลายทางของเที่ยวบิน

²⁶⁸ Ibid, pp. 11

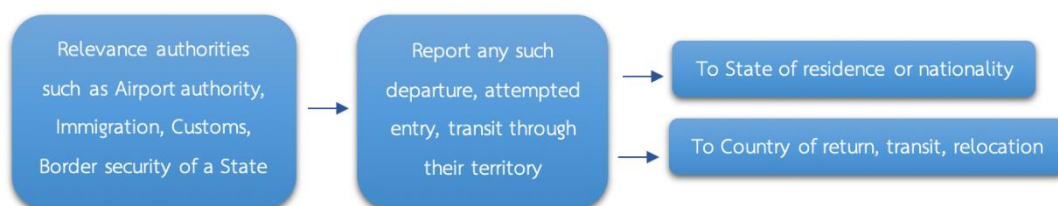
²⁶⁹ United Nations Security Council Resolution 2396/2017, pp. 12

แผนผังโครงสร้าง : การแบ่งปันข้อมูล PNR ระหว่างหน่วยงานรัฐกับบริษัทเอกชนสายการบิน



ยิ่งไปกว่านั้นในข้อมติยังเรียกร้องให้บรรดารัฐสมาชิกแบ่งปันข้อมูลการรายงาน (Report) ข้อมูลการเดินทางขาออกจากอาณาเขตของตน ข้อมูลการเดินทางท่องเที่ยวภายในอาณาเขตของตน ข้อมูลการเดินทางเข้ามาในหรือเข้ามาในเพื่อเป็นทางผ่านตนซึ่งอาณาเขตของตน ด้วยการแบ่งปันข้อมูลการรายงานเหล่านี้ต่อ 1.) ประเทศที่เป็นถิ่นที่อยู่ของบุคคลหรือบุคคลนั้นมีสัญชาติ (The State of residence or nationality) 2.) ประเทศที่เป็นต้นทาง ทางผ่าน หรือย้ายถิ่นฐานของบุคคล ซึ่งรัฐสมาชิกจะต้องแนบแน่ใจว่าข้อมูลการบันทึกของผู้โดยสาร ที่ตนสามารถเข้าถึงได้จากบริษัทสายการบินนั้นได้รับการวิเคราะห์จากหน่วยงานที่มีหน้าที่ที่เกี่ยวข้องทั้งหมดก่อนจะนำข้อมูลนั้นไปใช้เพื่อการตรวจจับการเดินทางของการก่อการร้าย²⁷⁰

แผนผังโครงสร้าง : การแบ่งปันข้อมูลการรายงานระหว่างหน่วยงานภายในรัฐกับต่างประเทศ



ผู้เขียนเห็นว่า การดำเนินการแบ่งปันข้อมูลของรัฐสมาชิกที่จะก่อให้เกิดประสิทธิภาพต่อมาตรการควบคุมชายแดนเพื่อการต่อต้านการก่อการร้าย จะต้องมีการดำเนินการแบ่งปันข้อมูลทั้งสองลักษณะ เพราะอาศัยเพียงแค่ ข้อมูลผู้โดยสารล่วงหน้า ลักษณะเดียวกันนั้นหน่วยงานบังคับใช้กฎหมายหรือหน่วย

²⁷⁰ Ibid, pp. 11

ข่าวกรองที่นำข้อมูลส่วนนี้ไปใช้ อาจมีสารที่ทำการติดตาม ประมวล และวิเคราะห์ถึงแผนการ ในรายละเอียดของบุคคลที่อาจจะมีการดำเนินการก่อการร้ายได้อย่างครอบคลุมเสียทีเดียว

ดังนั้นการอาศัยการแบ่งปันข้อมูลการบันทึกของผู้โดยสาร ร่วมด้วยในกับการดำเนินการ เหล่านั้น จะทำให้หน่วยงานที่เกี่ยวข้องมีข้อมูลที่หนักแน่นขึ้นและชัดเจนกว่าต่อการดำเนินมาตรการ ต่างๆ ซึ่งแน่นอนว่าในความเป็นจริงนั้นมีความเป็นไปได้ยากสำหรับการเข้าถึงข้อมูลการบันทึกของผู้โดยสาร เพราะมีความเสี่ยงในการทำงานของหน่วยงานบังคับใช้กฎหมายที่จะไปละเมิดสิทธิส่วนบุคคลหรือหลักการว่าด้วยสิทธิมนุษยชน

1.3 ข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว

ประการแรก กระบวนการนั้นจะต้องทำการแบ่งปันข้อมูลเหล่านี้ผ่านช่องทางความร่วมมือ ระหว่างหน่วยงานบังคับใช้กฎหมาย อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หน่วยงานบังคับใช้กฎหมาย หรือศูนย์ความร่วมมือชายแดน ในระดับที่เป็นทวิภาคี ภูมิภาค หรือทั่วโลก²⁷¹ ซึ่งการดำเนินกระบวนการแบ่งปันข้อมูลดังกล่าวจะต้องสอดคล้องต่อกฎหมาย ภายในของรัฐ และพันธกรณีระหว่างประเทศรวมถึงหลักการว่าด้วยสิทธิมนุษยชน ทั้งนี้ข้อมติได้ตก ย้ำให้รัฐสมาชิกของสหประชาชาติแบ่งปันข้อมูลเหล่านี้ให้แก่ ฐานข้อมูลรายการชื่อบุคคลเฝ้าระวัง แห่งชาติ (National watch lists) และ ฐานข้อมูลการคัดกรองบุคคลในระดับพหุภาคี (Multilateral screening databases) เช่น ฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL databases)

ประการที่สอง การดำเนินกระบวนการแบ่งปันข้อมูลดังกล่าวจะต้องสอดคล้องต่อกฎหมาย ภายในของรัฐ และพันธกรณีระหว่างประเทศรวมถึงหลักการว่าด้วยสิทธิมนุษยชน ทั้งนี้ข้อมติยัง เรียกร้องให้รัฐสมาชิกสหประชาชาติ หน่วยงานระหว่างประเทศ (International entities) หน่วยงาน ระดับภูมิภาค (Regional entities) หน่วยงานระดับอนุภูมิภาค (Sub regional entities)²⁷² ให้และ แบ่งปันองค์ความรู้ต่อรัฐสมาชิกในการดำเนินการตามข้อเรียกร้องของข้อมตินี้ รวมไปถึงสนับสนุนให้ บรรดารัฐสมาชิกสหประชาชาติแบ่งปันข้อมูลเหล่านี้ต่อ ฐานข้อมูลรายการชื่อบุคคลเฝ้าระวังแห่งชาติ และ ฐานข้อมูลการคัดกรองบุคคลในระดับพหุภาคี เช่น ฐานข้อมูลขององค์การตำรวจอาชญากรรม ระหว่างประเทศ หรือ หน่วยงานระหว่างประเทศ ที่เกี่ยวข้อง

ข้อสังเกต จากที่ได้กล่าวถึงพันธกรณีของรัฐสมาชิกสหประชาชาติตามข้อมติที่เกี่ยวข้องต่อ การแบ่งปันข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว ไปแล้วในข้างต้น เมื่อพิจารณาแล้วจะพบว่ารัฐ สมาชิกจำเป็นต้องออกกฎระเบียบและข้อบังคับ ว่าด้วยการให้อำนาจหน่วยงานบังคับใช้กฎหมาย

²⁷¹ United Nations Security Council Resolution 2322/2016, pp. 3

²⁷² United Nations Security Council Resolution 2396/2017, pp. 15

ภายในรัฐต้น และมอบหมายหน้าที่ในการเก็บและแบ่งปันซึ่งข้อมูลไบโอเมตริกซ์ (Biometric data) หน่วยงานบังคับใช้กฎหมายของรัฐในที่นี้อาจหมายถึงถึง สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หน่วยงานบังคับใช้กฎหมาย หรือศูนย์ความร่วมมือชายแดน ซึ่งจะต้องมีหน้าที่ในการควบคุมชายแดน การตรวจคนเข้าเมือง ตลอดจนการสืบสวนสอบสวน ทั้งยังต้องมีหน้าที่ในการเปรียบเทียบ ข้อมูลไบโอเมตริกซ์ ที่ตนเก็บไว้ได้กับฐานข้อมูลไบโอเมตริกซ์ระหว่างประเทศ หรือภายใต้ประเทศที่มีความร่วมมือทางข้อมูลต่อกัน

ในบริบทของการสืบสวนสอบสวนคดีที่เกี่ยวข้องต่อการก่อการร้ายนั้น หน่วยงานบังคับใช้กฎหมายที่มีหน้าที่ในการเก็บข้อมูลไบโอเมตริกซ์ สามารถที่แบ่งปันข้อมูลกับหน่วยงานทางนิติวิทยาศาสตร์ เพื่อประโยชน์ต่อการดำเนินงานในกระบวนการยุติธรรม²⁷³ รวมถึงให้ความช่วยเหลือต่อหน่วยงานที่มีหน้าที่สืบสวนสอบสวนคดี หรือหน่วยงานอัยการ ต่อการเชื่อมโยงบุคคลผู้ต้องสงสัยเข้ากับ รูปแบบของกิจกรรมการก่อการร้าย เหตุการณ์การก่อการร้าย สถานที่หรือวัตถุ รวมถึงบุคคลที่เกี่ยวข้องต่อการก่อการร้ายจากการใช้ข้อมูลไบโอเมตริกซ์ของบุคคล

อย่างไรก็ตามนั้นข้อดีทั้งสองยังได้กล่าวถึงความสำคัญของการดำเนินการแบ่งปันข้อมูลไบโอเมตริกซ์ ให้สอดคล้องต่อหลักการสิทธิมนุษยชน ด้วยเหตุผลที่ว่าเทคโนโลยีของการเก็บข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว ได้สะท้อนความขัดแย้งของการปฏิบัติตามข้อมติของรัฐสมาชิกระหว่างพันธกรณีที่จะทำการแบ่งปันข้อมูล (Obligation to share information) กับพันธกรณีที่จะต้องดำเนินการให้สอดคล้องต่อหลักการสิทธิมนุษยชน ผู้เขียนมีความเห็นว่าหากรัฐสมาชิกจะต้องดำเนินการตามพันธกรณีของข้อมติที่จะต้องทำการแบ่งปันข้อมูลข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว เพื่อระบุตัวผู้สงสัยที่อาจจะเกี่ยวข้องต่อการก่อการร้ายแล้วนั้น ขณะเดียวกันก็ควรจะต้องชั่งน้ำหนักโดยยึดหลักการที่ว่าด้วยความจำเป็น (Principle of necessity) ต่อการดำเนินการเพราะโดยธรรมชาติ ของ “ระบบไบโอเมตริก” ตั้งแต่กระบวนการของการเก็บ ประมวล และแบ่งปันอาจจะกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล ดังนั้นรัฐสมาชิกจะต้องนำเดินการภายใต้ขอบเขตของการใช้เทคโนโลยีอย่างจำกัด (Limited technical scope) และจะต้องมีการให้ความใส่ใจอย่างยิ่ง (Greater attention) ในเรื่องที่เกี่ยวข้องกับการปกป้องสิทธิมนุษยชน ในประเด็นหลัก อาทิ สิทธิที่จะเป็นอิสระจากการกระทำที่ไร้กฎเกณฑ์ (The right to be free from arbitrary) การรบกวนความเป็นส่วนตัวโดยไม่ชอบด้วยกฎหมาย ตลอดจนทั้งกระบวนการของการดำเนินการของระบบไบโอเมตริก

²⁷³ Security Council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), p. 14

2. ข้อปฏิบัติในการดำเนินการ

2.1 ข้อมูลผู้โดยสารล่วงหน้า

การใช้ระบบตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า (Advance Passenger Information System – APIS) ในการตรวจจับนักรบต่างชาติ หรือบุคคลที่มีส่วนเกี่ยวข้องกับการก่อการร้าย หน่วยงานของรัฐที่หน้าที่เกี่ยวข้องต่อการเก็บข้อมูลดังกล่าวจากบริษัทสายการบินไม่ว่าจะเป็นหน่วยงานบังคับใช้กฎหมายหรือหน่วยงานควบคุมชายแดนที่สนามบินนานาชาติ จะต้องปฏิบัติตามการให้สอดคล้องกับมาตรฐานในเก็บข้อมูลและการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าขององค์การการบินพลเรือนระหว่างประเทศ (Standard established by International Civil Aviation Organization - ICAO)

ยิ่งไปกว่านั้นสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ ได้รับรองหลักการที่ให้รัฐสมาชิกดำเนินการตามข้อมติของการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคง ที่ว่าด้วยเรื่องการแบ่งปันผู้โดยสารล่วงหน้า²⁷⁴ มาเป็น “Madrid Guiding Principles” ที่ได้ระบุว่าการดำเนินการเก็บข้อมูลและประมวลข้อมูลผู้โดยสารล่วงหน้า จะต้องได้รับอนุญาตภายใต้กฎหมายภายในของประเทศและรัฐสมาชิกจะต้องพิจารณาข้อแนะนำดังต่อไปนี้ ตาม “*Guiding principle 19 ของ Madrid Guiding Principles*”

หัวข้อ	รายละเอียด
ข้อ A	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่ากฎหมายภายในให้อำนาจหน่วยงานของรัฐสามารถรวบรวม ใช้ และรักษาซึ่งข้อมูลผู้โดยสารล่วงหน้า และในการดำเนินการ (Implementing) ระบบข้อมูลผู้โดยสารล่วงหน้า นั้น จะต้องสอดคล้องกับภาคผนวก 9 ของอนุสัญญาว่าด้วยการบินพลเรือนระหว่างประเทศ (Annex 9 to the Convention on International Civil Aviation) และแนวปฏิบัติเกี่ยวกับข้อมูลผู้โดยสารล่วงหน้าขององค์การศุลกากรโลก (World Customs Organization) สมาคมขนส่งทางอากาศระหว่างประเทศ (International Air Transport Association - IATAS) และแนวทางปฏิบัติที่แนะนำ (SARPs) ขององค์การการบินพลเรือนระหว่างประเทศ (ICAO) และเคารพอย่างเต็มที่ต่อหลักการสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานรวมถึงการสอดคล้องกับมาตรา 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR)
ข้อ B	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่ามีทรัพยากรเพียงพอ (Adequate resources) และ

²⁷⁴ Security Council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), p. 4

หัวข้อ	รายละเอียด
	การสนับสนุนในการเสริมสร้างขีดความสามารถของหน่วยงานที่รับผิดชอบเพื่อใช้ระบบตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า (Advance Passenger Information System – APIS) และการใช้ระบบข้อมูลผู้โดยสารล่วงหน้า จะต้องมีความสามารถที่จะวิเคราะห์และตอบสนองต่อข้อมูลผู้โดยสารแบบเรียลไทม์ (Passenger data in real time) และมีมาตรการที่สามารถป้องกันไม่ให้ผู้โดยสารที่ไม่ผ่านเกณฑ์ของการวิเคราะห์เข้าถึงเครื่องบินหรือพื้นที่อาคารผู้โดยสารขาออก (Departure terminal) ภายในสนามบิน
ข้อ C	รัฐสมาชิกจะต้องแน่ใจว่ามีมาตรการให้บริษัทสายการบิน (Air carriers) แบ่งปันข้อมูลผู้โดยสารล่วงหน้า (API) โดยผ่านการใช้ "Single windows" ²⁷⁵ ต่อหน่วยงานที่เกี่ยวข้องต่อการควบคุมชายแดน หรือจะแต่งตั้งหน่วยงานตัวแทนในการรับข้อมูลดังกล่าว (Primary receiver of information) เช่น การจัดตั้งหน่วยข้อมูลผู้โดยสาร (Passenger Information Units - PIU)
ข้อ D	รัฐสมาชิกจะต้องกำหนดมาตรฐานของข้อกำหนดว่าด้วยการใช้โปรแกรมข้อมูลผู้โดยสารล่วงหน้า (Advance passenger information programme) และโปรโตคอลเกี่ยวกับการสื่อสารและแนวทางปฏิบัติเกี่ยวกับข้อมูลผู้โดยสารล่วงหน้า ต่อหน่วยงานที่มีหน้าที่เกี่ยวข้องและบริษัทสายการบิน
ข้อ E	รัฐสมาชิกจะต้องดูแลให้หน่วยงานที่เกี่ยวข้องและบริษัทสายการบิน มีการปฏิบัติตามและยึดมั่นต่อการเก็บและแบ่งปันข้อมูลเฉพาะที่ถูกกำหนดและระบุไว้ในแนวทางปฏิบัติอย่างเคร่งครัด กล่าวคือจะทำการเก็บหรือแบ่งปันข้อมูลนอกจากที่กำหนดไว้ในข้อกำหนดมิได้ แต่ทั้งนี้อาจเป็นไปตามข้อยกเว้นในข้อกำหนดที่ได้
ข้อ F	รัฐสมาชิกจะต้องแน่ใจว่าในการดำเนินการ (Implementing) ระบบข้อมูลผู้โดยสารล่วงหน้า นั้น หน่วยงานที่เกี่ยวข้องและบริษัทสายการบินจะต้องเคารพในหลักการสิทธิมนุษยชน ต่อการดำเนินการรวบรวมข้อมูล วิเคราะห์ข้อมูล แบ่งปันข้อมูล จัดเก็บข้อมูล และใช้ข้อมูลนั้นของผู้โดยสารเพื่อดำเนินมาตรการต่อต้านการก่อการร้าย
ข้อ G	รัฐสมาชิกจะต้องแนบมั่นใจว่าเจ้าหน้าที่ในหน่วยงานที่เกี่ยวข้องจะมีความรู้ (Knowhow) และทรัพยากรที่เพียงพอ (Adequate resources) ต่อการดำเนินการ (Implementing) ระบบข้อมูลผู้โดยสารล่วงหน้า นั้นให้เกิดประสิทธิภาพ
ข้อ H	ส่งเสริมให้รัฐสมาชิกแบ่งปันและรวมข้อมูลผู้โดยสารล่วงหน้า เข้ากับฐานข้อมูลทั่วโลก

²⁷⁵ "Single windows" คือ ระบบการบริการเชื่อมโยงข้อมูลหน่วยงานภาครัฐและภาคธุรกิจ สำหรับการเข้า ส่งออก และโลจิสติกส์ รองรับการเชื่อมโยงข้อมูลระหว่างประเทศสมาชิกอาเซียนและประเทศในภูมิภาคอื่นๆ" *ที่มา: กรมศุลกากร*

หัวข้อ	รายละเอียด
	(Global indices) และฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL) เช่น "Stolen and Lost Travel Documents database (SLTD)" และ "Travel Documents Associated with Notices system"

ที่มาของข้อมูลในตาราง²⁷⁶

2.2 ข้อมูลการบันทึกของผู้โดยสาร

สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ (Counter Terrorism Executive Directorate – CTED) ได้ออกคำแนะนำต่อการดำเนินมาตรการแบ่งปันข้อมูลการบันทึกของผู้โดยสาร และรับรองหลักการออกมาเป็น “*Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee*” Guiding Principle ที่ 1 ว่าด้วยเรื่องพันธกรณีของการแบ่งปันข้อมูลการบันทึกของผู้โดยสารซึ่งจะขออธิบายในรายละเอียดตามตารางดังต่อไปนี้

หัวข้อ	รายละเอียด
ข้อ A	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่ากฎหมายภายในให้อำนาจหน่วยงานของรัฐสามารถรวบรวม ใช้ และรักษาซึ่งข้อมูลการบันทึกของผู้โดยสาร (Passenger name record – PNR) และในการดำเนินการ (Implementing) ระบบข้อมูลการบันทึกของผู้โดยสารนั้น จะต้องสอดคล้องกับภาคผนวก 9 ของอนุสัญญาว่าด้วยการบินพลเรือนระหว่างประเทศ (Annex 9 to the Convention on International Civil Aviation) และแนวปฏิบัติเกี่ยวกับข้อมูลผู้โดยสารล่วงหน้าขององค์การศุลกากรโลกการขนส่งทางอากาศระหว่างประเทศ (World Customs Organization) และแนวทางปฏิบัติที่แนะนำ (SARPs) ขององค์การการบินพลเรือนระหว่างประเทศ (ICAO) และเคารพอย่างเต็มที่ต่อหลักการสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานรวมถึงการสอดคล้องกับมาตรา 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR)
ข้อ B	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่ามีทรัพยากรเพียงพอ (Adequate resources)

²⁷⁶ Counter Terrorism Executive Directorate – CTED, "Madrid Guiding Principles", *Counter-Terrorism Committee of United Nations Security* (2015), p.14 (*Guiding principle 19*), Available from https://www.un.org/sc/ctc/wp-content/uploads/2016/10/Madrid-Guiding-Principles_EN.pdf

หัวข้อ	รายละเอียด
	และการสนับสนุนในการเสริมสร้างขีดความสามารถของหน่วยงานที่รับผิดชอบเพื่อใช้ระบบข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR)
ข้อ C	รัฐสมาชิกจะต้องแน่ใจว่ามีมาตรการให้บริษัทสายการบิน (Air carriers) แบ่งปันข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR) โดยผ่านการใช้ "Single windows" ต่อหน่วยงานที่เกี่ยวข้องต่อการควบคุมชายแดน หรือจะแต่งตั้งหน่วยงานตัวแทนในการรับข้อมูลดังกล่าว (Primary receiver of information) เช่น การจัดตั้งหน่วยข้อมูลผู้โดยสาร (Passenger Information Units - PIU)
ข้อ D	รัฐสมาชิกจะต้องจัดตั้งหน่วยงานที่มีหน้าที่รับผิดชอบโดยเฉพาะ (Specific entities) สำหรับการรวบรวมข้อมูล จัดเก็บข้อมูล ประมวลผลข้อมูล และวิเคราะห์ข้อมูล ซึ่งข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR) ที่ได้รับการแบ่งปันข้อมูลมาจากบริษัทผู้ให้บริการเดินอากาศ อาทิ การจัดตั้งหน่วยข้อมูลผู้โดยสาร (Passenger Information Units - PIUs) ซึ่งจะมีหน้าที่รับข้อมูลจากสายการบิน และเปรียบเทียบเพื่อคัดแยกระหว่างข้อมูล ข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR) กับ ข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) เพื่อแบ่งปันข้อมูลเหล่านั้นต่อหน่วยงานบังคับใช้กฎหมายต่างๆ เพื่อประโยชน์แก่การตั้งเกณฑ์การกำหนดไว้ล่วงหน้าเพื่อระบุตัวบุคคล (Pre-determined criteria to identify person) ซึ่งอาจจะเกี่ยวข้องต่อการก่อการร้าย ทั้งนี้กระบวนการดังที่กล่าวมาจะต้องอยู่บนฐานของการไม่เลือกปฏิบัติ (Non-discriminatory grounds) ตามพันธกรณีของกฎหมายระหว่างประเทศว่าด้วยสิทธิมนุษยชน และหน่วยข้อมูลผู้โดยสาร (Passenger Information Units - PIUs) จะต้องมีหน้าที่ในการกำกับหน่วยงานที่มีอำนาจ (Competent authorities) ให้ดำเนินการต่อข้อมูลเหล่านั้นโดยคำขอที่มีเหตุผล (Reasoned requests)
ข้อ E	กำหนดเจ้าหน้าที่ผู้มีหน้าที่ปกป้องข้อมูล (Data-protection officer) ในหน่วยข้อมูลผู้โดยสาร (Passenger Information Units - PIUs) ซึ่งรับผิดชอบในการตรวจสอบการประมวลผลข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR) และสำหรับการดำเนินการป้องกันที่เกี่ยวข้องอื่นๆ (Relevant safeguards)
ข้อ F	รัฐสมาชิกควรพิจารณาการแบ่งปันข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR) กับ ข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) กับรัฐสมาชิกอื่นที่มีสามารถในการตรวจสอบ ซึ่งผู้ก่อการร้ายและนักรบต่างชาติ (FTFs) ในกรณีที่พวกเขาได้เดินทางกลับไปยังประเทศที่เป็นต้นทาง ประเทศที่เป็น

หัวข้อ	รายละเอียด
	จุดหมายปลายทาง ประเทศที่สามที่จะย้ายถิ่นฐานไป ทั้งนี้ให้ตรวจจับบุคคลโดยเฉพาะที่เป็นบุคคลซึ่งมีรายชื่อตามที่คณะกรรมการเกี่ยวกับมาตรการลงโทษ (Sanctions Committees) ได้ระบุไว้โดยอาศัยอำนาจตาม ข้อมติที่ 1267/1999 ข้อมติที่ 1989/2011 และข้อมติที่ 2253/2015 และทั้งหมดของกระบวนการจะต้องสอดคล้องกับพันธกรณีระหว่างประเทศว่าด้วยเรื่องสิทธิมนุษยชน
ข้อ G	รัฐสมาชิกจะต้องอนุญาตให้ข้อมูลการบันทึกของผู้โดยสาร (Passenger name record – PNR) ถูกพิจารณาเทียบกับฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL databases) และรายการชื่อการคว่ำบาตรของสหประชาชาติ (United Nations sanctions lists)
ข้อ H	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่าการประมวลผลและการเก็บรักษา ซึ่งข้อมูลการบันทึกของผู้โดยสาร (Passenger name record – PNR) มีการกำกับดูแล (Oversight) และการปกป้องความเป็นส่วนตัว (Privacy protections) ในขณะเดียวกันก็ต้องแน่ใจว่ามีการใช้มาตรการป้องกัน (Precautions) จากการใช้ข้อมูลการบันทึกของผู้โดยสารในทางที่ผิดโดยหน่วยงานของรัฐ
ข้อ I	รัฐสมาชิกจะต้องให้การเคารพในสิทธิเสรีภาพของเจ้าของข้อมูลจากการแทรกแซงตามอำเภอใจหรือผิดกฎหมาย (Arbitrary or unlawful interference) กับความเป็นส่วนตัวของบุคคล ภายใต้กฎหมายระหว่างประเทศ ตลอดจนการคุ้มครองที่เกี่ยวข้อง ภายใต้กฎหมายภายในประเทศซึ่งอาจรวมถึงการเข้าถึงการแก้ไข (Rectification) การกำหนดข้อจำกัด (Restrictions) ในการใช้งานข้อมูลส่วนบุคคล และการชดใช้เยียวยาทางกระบวนการยุติธรรม (Judicial redress)

ที่มาของข้อมูลในตาราง²⁷⁷

2.3 ข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว

สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติได้ออกคำแนะนำต่อการดำเนินมาตรการแบ่งปันข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว และรับรองหลักการออกมาเป็น “Annex to the letter dated 28 December 2018 from the Chair of the Security Council

²⁷⁷ Security Council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), p. 6

Committee” Guiding Principle ที่ 3 ว่าด้วยเรื่องพันธกรณีของการรวบรวม ใช้ และแบ่งปันข้อมูล ซึ่งข้อมูลไบโอเมตริกซ์ ซึ่งสามารถสรุปได้ดังตารางต่อไปนี้

หัวข้อ	รายละเอียด
ข้อ A	รัฐสมาชิกจะต้องต่อต้านภัยคุกคามจากการเคลื่อนไหวของผู้ต้องสงสัยว่าเกี่ยวข้องกับ การก่อการร้ายและนักรบต่างชาติที่จะพยายามเดินทางข้ามพรมแดนระหว่างประเทศ (International borders) โดยรัฐสมาชิกจะต้องแบ่งปันข้อมูลไบโอเมตริกซ์ (Biometric data) ของบุคคลผู้ที่พยายามจะทำการเข้ามายังประเทศตน (Entering) ออกเดินทางจากประเทศตน (Departing) กำลังจะเข้ามาทำการพักพิงที่ประเทศตน (Seeking residence) ซึ่งต้องแบ่งปันข้อมูลเพื่อการเปรียบเทียบกับฐานข้อมูลไบโอเมตริกซ์ระหว่างประเทศ ภายในประเทศที่มีการร่วมมือทางข้อมูล หรือฐานข้อมูล Known and suspected FTFs
ข้อ B	พัฒนาและเพิ่มประสิทธิภาพของการใช้ระบบไบโอเมตริกซ์ในลักษณะที่เหมาะสมแก่ ความถูกต้องของการพิสูจน์ตัวตนของบุคคล (Authenticate the identity of individuals) และป้องกันบุคคลจากข้อมูลที่เป็นเท็จ (False particulars) และการ แอบอ้างเป็นบุคคลอื่น (Impersonate other people)
ข้อ C	รัฐสมาชิกจะต้องแนบเนียนใจว่ามีการบำรุงรักษาที่มีประสิทธิภาพ (Effective maintenance) ต่อระบบฐานข้อมูลไบโอเมตริกซ์ (Biometric databases) และมีการ ปฏิบัติตามโปรโตคอลของการแบ่งปันข้อมูล (Data-sharing protocols)
ข้อ D	รัฐสมาชิกจะต้องดำเนินการตามกรอบที่ว่าด้วยหลักการด้านสิทธิมนุษยชน (Human rights-based frameworks) ในการใช้เทคโนโลยีไบโอเมตริกซ์ (Biometric technology) ซึ่งจำเป็นจะต้องมีซึ่งจะต้องมีขั้นตอนของการป้องกัน (Procedural safeguards) รวมทั้งการกำกับดูแลอย่างมีประสิทธิภาพ (Effective oversight) อาทิ จัดตั้งหรือขยายหน้าที่ให้กับหน่วยงานกำกับดูแลที่เหมาะสม (Appropriate oversight bodies) ต่อการดำเนินการตามกฎหมายที่เกี่ยวข้องต่อการละเมิดข้อมูล ส่วนบุคคล และมาตรการที่ว่าด้วยการเยียวยาบุคคล (Remedies in case of violations) ทั้งนี้รัฐสมาชิกจะต้องมีกระบวนการตรวจสอบ (Review process) เนื้อหาของนโยบายระดับชาติ และการตัดสินใจ (Decision-making) ทั้งหมดเกี่ยวกับการ ใช้ไบโอเมตริกซ์เพื่อวัตถุประสงค์ในการต่อต้านการก่อการร้ายอยู่เสมอ เพื่อปกป้อง ไม่ให้เกิดการละเมิดต่อหลักการว่าด้วยสิทธิมนุษยชน
ข้อ E	รัฐสมาชิกจะต้องพิจารณาถึงประเด็นปัญหาเฉพาะ (Specific issues) ที่อาจจะเกิดขึ้น

หัวข้อ	รายละเอียด
	ระหว่างการค้าเงินงานที่ไปกระทบต่อการปกป้องและส่งเสริมสิทธิของเด็ก (The rights of the child) ในบริบทที่หน่วยงานของรัฐได้ทำการเก็บข้อมูลไบโอเมตริกซ์ เช่น เมื่อข้อมูลไบโอเมตริกซ์ของเด็กถูกจัดเก็บโดยหน่วยงานของรัฐจะต้องเป็นไปตามวัตถุประสงค์ต่อการคุ้มครองเด็ก (Child-protection purposes) และจะต้องวางกรอบทางกฎหมายที่เหมาะสม (Appropriate legal frameworks) รวมทั้งมาตรการป้องกัน (Safeguards)
ข้อ F	รัฐสมาชิกจะต้องประเมินความเสี่ยงอย่างสม่ำเสมอตั้งแต่ตอนจนปลาย (The end-to-end processes) ของระบบข้อมูลไบโอเมตริกซ์ เพื่อป้องกันภัยคุกคามทางไซเบอร์ทุกชนิด อาทิ การขโมยข้อมูลส่วนตัว (Identity theft) การแฮคเพื่อลบข้อมูล (Deletion) การเปลี่ยนข้อมูล (Replacement of data) และการสร้างความเสียหายโดยเจตนาต่อข้อมูล (Deliberate damage)
ข้อ G	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่าการกระทำของเจ้าหน้าที่รัฐในการประเมินการจับคู่ระหว่างข้อมูลไบโอเมตริกซ์ (Biometric matches) กับบุคคลนั้นจะต้องสอดคล้องต่อบริบทของกฎหมายระหว่างประเทศ พันธกรณีระหว่างประเทศว่าด้วยสิทธิมนุษยชน ความจำเป็นในการรับทราบข้อมูลอย่างครบถ้วน (The need for a fully-informed) และการกระทำที่ชอบด้วยกฎหมาย (Lawful response)
ข้อ H	รัฐสมาชิกจะต้องแนบเนียนใจว่าระบบปฏิบัติการของข้อมูลไบโอเมตริกซ์และกรอบกฎหมาย (The legal frameworks) อนุญาตให้มีการทำงานร่วมกัน (Interoperability) กับฐานข้อมูลไบโอเมตริกซ์ระหว่างประเทศ หรือประเทศภายใต้ความร่วมมือทางข้อมูล หรือฐานข้อมูลไบโอเมตริกซ์ขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL Biometric Databases)
ข้อ I	รัฐสมาชิกสามารถเชื่อมต่อและใช้ประโยชน์สูงสุดจากฐานข้อมูลไบโอเมตริกซ์ขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL Biometric Databases)

ที่มาของข้อมูลในตาราง²⁷⁸

²⁷⁸ Security Council, "Guiding Principle 3 - Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), p. 9

3.3.2.4 มาตรฐานการดำเนินการขององค์การการบินพลเรือนระหว่างประเทศ

1. มาตรฐานในการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า

การแบ่งปันข้อมูลผู้โดยสารล่วงหน้าตามพันธกรณีของคณะมนตรีความมั่นคงแห่งสหประชาชาตินั้น ในข้อมติที่เกี่ยวข้องที่ได้กล่าวมาข้างต้น ต้องการที่ควบคุมคุณภาพ (Quality control) ของบรรดาระัฐสมาชิกให้มีการดำเนินการตามข้อมติ ซึ่งจะต้องเป็นไปตามมาตรการขององค์การการบินพลเรือนระหว่างประเทศ เหตุผลหลักๆก็คือ การแบ่งปันข้อมูลที่เกี่ยวข้องของผู้โดยสารจะเกิดขึ้นระหว่างบริษัทสายการบินและหน่วยงานของรัฐที่เกี่ยวข้องต่อการดำเนินการควบคุมชายแดน อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หน่วยงานบังคับใช้กฎหมาย หรือศูนย์ความร่วมมือชายแดน เพื่อให้เป็นไปตามมาตรฐานเดียวกันในการเก็บและแบ่งปันข้อมูลที่ได้ถือว่า เป็นข้อมูลส่วนตัวของบุคคล²⁷⁹

ตามรายงานของสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติได้ระบุว่า มีมากกว่า 50 รัฐสมาชิกที่มีการดำเนินการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า แต่ก็ยังมีรัฐสมาชิกจำนวนไม่น้อยที่ไม่สามารถทำการแบ่งปันข้อมูลเหล่านี้ได้ และอาจส่งผลให้ขาดประสิทธิภาพของการตรวจสอบการเดินทางโดยอากาศยานของนักบินต่างชาติ หรือผู้ก่อการร้ายในบัญชีต่อผู้มีส่วนเกี่ยวข้องต่างๆ ในการแบ่งปันข้อมูล ไม่ว่าจะป็นรัฐที่ปลายทางของอากาศยาน รัฐที่อากาศยานทำการเปลี่ยนผ่าน หรือรัฐที่เป็นต้นทางของการโดยสารอากาศยาน

ดังนั้นในการแก้ปัญหาการดำเนินการตามข้อมติคณะมนตรีความมั่นคงที่ว่าด้วยเรื่องการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า ควรจะต้องถูกชูประเด็นให้มีความสำคัญอย่างมากต่อการดำเนินการมาตรการควบคุมชายแดนเพื่อต่อต้านการก่อการร้าย สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ ได้สนับสนุนการพัฒนาระบบให้เป็นไปตามมาตรฐานสากล จึงกำหนดให้บรรดาระัฐสมาชิกของสหประชาชาติ ที่ได้เป็นภาคีสมาชิกขององค์การการบินพลเรือนระหว่างประเทศทุกรัฐจะต้องพัฒนาระบบข้อมูลผู้โดยสารล่วงหน้า และการดำเนินการพัฒนานั้นจะต้องครอบคลุม²⁸⁰ ต่อมาตรฐานและคำแนะนำขององค์การการบินพลเรือนระหว่างประเทศสำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ ทำงานอย่างใกล้ชิดกับองค์การการบินพลเรือนระหว่างประเทศ ในการพัฒนามาตรฐานสากล และได้รับรอง ภาคผนวกที่ 9 ของอนุสัญญาว่าด้วยการบินพลเรือน

²⁷⁹ Security Council, "Letter dated 22 December 2017 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2017), pp. 40

²⁸⁰ Security Council, "Letter dated 14 December 2017 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2017), pp. 3

ระหว่างประเทศ (Annex 9 to the Convention on International Civil Aviation)²⁸¹ เพื่อให้
บรรดารัฐสมาชิกได้ดำเนินการตามในการพัฒนาระบบข้อมูลผู้โดยสารล่วงหน้า (Advance
passenger information system) ซึ่งผู้เขียนจะขออธิบายตามตารางดังต่อไปนี้



²⁸¹ International Civil Aviation Organization, "Annex 9 to the Convention on International Civil Aviation Facilitation", Fifteenth Edition, (October 2017), p. 9-1 CHAPTER 9. Passenger data exchange systems, Available from https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

ตารางที่ 1: มาตราฐานสากลในการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าขององค์การการบินพลเรือนระหว่างประเทศ ตาม Annex 9 to the Convention on International Civil Aviation – Chapter 9 : Passenger data exchange systems – B. Advance passenger information (API)

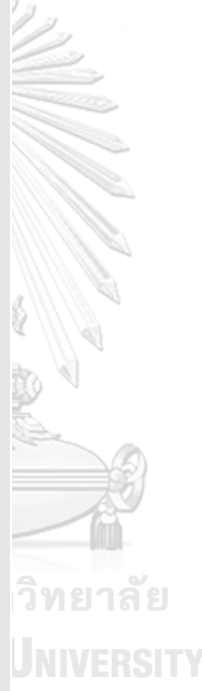
ข้อ	รายละเอียดของปฏิบัติ
9.1	รัฐภาคีถูกกำหนดให้มีการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (API) จากผู้ดำเนินการเดินอากาศ (Aircraft operators) ในการแบ่งปันข้อมูลควรรสร้างช่องทางของการเคลื่อนย้ายข้อมูลแบบ "Passenger Data Single Window" สำหรับแต่ละประเภทข้อมูลที่อนุญาตให้หน่วยงานภายในของรัฐภาคีที่เกี่ยวข้องสามารถเข้าถึงข้อมูล เช่น ข้อมูลของผู้โดยสาร และข้อมูลของลูกเรือ ทั้งหมดที่อยู่ภายใต้เขตอำนาจของรัฐภาคี
9.2	รัฐภาคีและบริษัทสายการบินจะต้องมีช่องทางของการสื่อสารในเรื่องการสนับสนุนการปฏิบัติงาน (Operational support) การสนับสนุนทางเทคนิค (Technical support) โดยอย่างเหมาะสม (Appropriate level) เช่น มีการแบ่งปันข้อมูลกันตลอดเวลา 24 ชั่วโมงตลอด 7 วัน เพราะวิเคราะห์และตอบสนองต่อการหยุดทำงานหรือความล้มเหลวของระบบให้กลับสู่การปฏิบัติงานทำงานปกติอย่างรวดเร็วที่สุด
9.3	รัฐภาคีและบริษัทสายการบินจะต้องสร้างขั้นตอนการแจ้งเตือนที่เหมาะสม (Appropriate notification) รวมถึงขั้นตอนของการกู้ระบบคืน (Recovery procedures) สำหรับการบำรุงรักษาระบบข้อมูลที่จะหมดอายุตามกำหนดเวลา และการหยุดทำงานหรือความล้มเหลวของระบบที่ไม่ได้เป็นไปตามการหมดอายุของเวลาที่กำหนดไว้
9.4	รัฐภาคีและบริษัทสายการบินจะต้องมีช่องทางของการติดต่อกัน (Contact support) อย่างเหมาะสม กล่าวคือในทางปฏิบัติจริงจะต้องตลอดเวลา 24 ชั่วโมงตลอด 7 วัน
9.5	รัฐภาคีแต่ละรัฐจะต้องจัดตั้งระบบการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) - หมายเหตุ พันธกรณีตามข้อมติที่ 2178/2014 และ 2309/2016 ได้เรียกร้องให้บรรดารัฐสมาชิกออกมาตรการตามกฎหมายภายในเพื่อร้องขอให้มีการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) จากสายการบินที่ดำเนินกิจการภายใต้เขตอำนาจของรัฐตน

ชื่อ	รายละเอียดของปฏิบัติ
	<p>กับหน่วยงานที่มีความเหมาะสม (Appropriate authorities) ในการดำเนินงานเพื่อตรวจจับ (Detect) การเดินทางขาออกจากประเทศของตนเอง การเดินทางเข้าประเทศของตน รวมทั้งการเดินทางที่มีการเปลี่ยนผ่านประเทศของตน (Transit through their territories) โดยวิธีการของการเดินทางด้วยอากาศยานพาณิชย์และอากาศยานส่วนตัว รวมไปถึงวิธีการเดินทางอื่นๆ ของบุคคลที่มีรายชื่อตามที่คณะกรรมการเกี่ยวกับมาตรการลงโทษ (Sanctions Committees) ได้รับรู้ไว้โดยอาศัยอำนาจตาม ข้อมติที่ 1267/1999 และข้อมติที่ 1989/2011</p>
9.6	<p>ระบบการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) ของแต่ละรัฐภาคีนั้นจะต้องดำเนินการโดยหน่วยงานที่มีอำนาจตามกฎหมายที่เหมาะสม (Appropriate legal authority) และทั้งนี้จะต้องมีกฎหมายรับรองการให้อำนาจอย่างชัดเจน อาทิ กฎหมาย (Legislation) ระเบียบข้อบังคับ (Regulation) กฎีกา (Decree) และจะต้องสอดคล้องกับมาตรฐานที่ยอมรับในระดับสากลสำหรับการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (API internationally recognized standards)</p> <ul style="list-style-type: none"> - หมายเหตุ การแบ่งปันข้อมูลผู้โดยสารล่วงหน้าจะเกี่ยวข้องกับการบันทึกข้อมูลชีวประวัติของผู้โดยสารหรือถูกระบุ รายละเอียดเที่ยวบินโดยสายการบินก่อนออกเดินทาง ซึ่งข้อมูลเหล่านี้จะถูกส่งทางอิเล็กทรอนิกส์ไปยังหน่วยงานควบคุมชายแดนในประเทศปลายทาง (Destination Country) หรือภายในประเทศต้นทาง (Departure Country) ดังนั้นข้อมูลเหล่านี้มีอำนาจหน้าที่จะต้องได้รับล่วงหน้าก่อนที่จะมีการออกเดินทาง หรือการมาถึงของเที่ยวบินนั้น - หมายเหตุ "United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport" เป็นกฎเกณฑ์รับรองโดยสหประชาชาติในการแบ่งปันข้อมูลในแบบอิเล็กทรอนิกส์สำหรับการพาณิชย์และการขนส่ง - หมายเหตุ ในการแบ่งปันข้อมูลในแบบอิเล็กทรอนิกส์สำหรับการพาณิชย์และการขนส่งนั้นให้ไปตามคำแนะนำของแนวทางที่ได้รับการยอมรับในระดับสากลจากองค์การศุลกากรโลก (World Customs Organization) สมาคมขนส่งทางอากาศระหว่างประเทศ (International Air Transport Association) และองค์การการบินพลเรือนระหว่างประเทศ (ICAO)

รายละเอียดของการปฏิบัติ	
ชื่อ	
9.7	รัฐภาคีจะต้องออกกฎหมายเพื่อรับรองวัตถุประสงค์ของการบันทึกและแบ่งปันข้อมูลผู้โดยสารล่วงหน้า ออกกฎระเบียบข้อบังคับต่อหน่วยงานที่มีหน้าที่เกี่ยวข้อง รวมถึงให้หน่วยงานเหล่านั้นมีหน้าที่กำหนดชุดข้อมูล API ทั่วไป (A common set of API data elements) ที่ถูกร้องขอจากหน่วยงานของรัฐอื่น ให้สอดคล้องกับมาตรฐานการสร้างข้อความ (Message construction standards) และอาจจะแต่งตั้งหน่วยงานหนึ่งทำหน้าที่แทนหน่วยงานที่เกี่ยวข้องอื่นๆ ต่อการรับ API Data
9.8	เมื่อข้อมูลการระบุตัวตนของผู้โดยสารถูกส่งผ่านมายังหน่วยงานของรัฐภาคี รัฐภาคีจะต้องร้องขอเพียงข้อมูลที่มีอยู่เฉพาะเท่าที่ระบบสามารถทำการอ่านได้เท่านั้น (Information is available in machine readable form in travel documents)
9.9	หากรัฐภาคีไม่ได้ปฏิบัติตาม ข้อ 9.8 ข้างต้นได้ ให้เป็นไปตามคำแนะนำของ the WCO's Data Maintenance Request (DMR) process for any deviation from the standard
9.10	รัฐภาคีควรมองข้ามข้อกำหนดจำนวนครั้งต่อการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าในเที่ยวบินนั้นๆ
9.11	หากรัฐภาคีทำการร้องขอข้อมูลผู้โดยสารล่วงหน้า ควรจะต้องดำเนินการเพื่อจำกัดภาระการปฏิบัติงานและการบริหารของผู้ดำเนินการเดินอากาศ (Aircraft operators)
9.12	รัฐภาคีควรละเว้นการเก็บค่าปรับและบทลงโทษกับผู้ดำเนินการเดินอากาศ (Aircraft operators) สำหรับการเกิดผิดพลาดใดๆ ขึ้นจากความล้มเหลวของระบบปฏิบัติงาน ซึ่งอาจส่งผลให้ไม่มีการส่งข้อมูล หรือสร้างเสียหายไปยังหน่วยงานที่ทำการควบคุมระบบแบ่งปันข้อมูล API
9.13	รัฐภาคีจะต้องทำการแบ่งปันข้อมูลผู้โดยสารล่วงหน้าโดยส่งผ่านข้อมูลเหล่านั้นทางรูปแบบอิเล็กทรอนิกส์เท่านั้น มิควรส่งผ่านข้อมูลเหล่านั้นในรูปแบบกระดาษ (Paper form)
9.14	รัฐภาคีแต่ละรัฐควรพิจารณาการใช้ระบบ An interactive Advance Passenger Information (iAPI) system
9.15	รัฐภาคีที่จะดำเนินการใช้ระบบ An interactive Advance Passenger Information (iAPI) ควรจะต้อง

ชื่อ	รายละเอียดของปฏิบัติ
	<ul style="list-style-type: none"> - A: ปรึกษาหารือกับผู้ดำเนินการเดินอากาศ (Aircraft operators) ก่อนการพัฒนาและเปิดการใช้งานของระบบ iAPI - B: พัฒนาระบบร่วมกับผู้ดำเนินการเดินอากาศ (Aircraft operators) - C: ปฏิบัติงานให้เป็นที่ไปตามคำแนะนำของแนวทางที่ได้รับการยอมรับในระดับสากลจาก องค์การศุลกากรขนส่งทางอากาศระหว่างประเทศ (World Customs Organization) สมาคมขนส่งทางอากาศระหว่างประเทศ (International Air Transport Association) และ องค์การการบินพลเรือนระหว่างประเทศ (ICAO)
9.16	<p>รัฐภาคีและผู้ดำเนินการเดินอากาศ (Aircraft operators) ซึ่งได้ใช้ระบบการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า (Advance Passenger Information – API) และ ระบบ An interactive Advance Passenger Information (iAPI) จะต้องมีความสามารถในการติดต่อหากันตลอด 24 ชั่วโมงตลอด 7 วัน ในกรณีที่ระบบปฏิบัติงานดังกล่าวเกิดความขัดข้อง (The event of a system outage or failure)</p>

ที่มาของข้อมูลในตาราง²⁸²



²⁸² International Civil Aviation Organization, "Annex 9 to the Convention on International Civil Aviation Facilitation", Fifteenth Edition, (October 2017), p. 9-1 CHAPTER 9. Passenger data exchange systems, Available from https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

2. มาตรฐานในการแบ่งปันข้อมูลการบันทึกของผู้โดยสาร

สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ ทำงานอย่างใกล้ชิดกับองค์การการบินพลเรือนระหว่างประเทศ ในการพัฒนามาตรฐานสากล และได้รับรองออกมาเป็นภาคผนวกที่ 9 ของอนุสัญญาว่าด้วยการบินพลเรือนระหว่างประเทศ เพื่อให้บรรดารัฐสมาชิกได้ดำเนินการตามในการพัฒนาการดำเนินการต่อข้อมูลการบันทึกของผู้โดยสาร

การกำหนดหลักเกณฑ์ขององค์การการบินพลเรือนระหว่างประเทศต่อการแบ่งปันข้อมูลในประเภทนี้จะค่อนข้างไม่รัดกุมเท่ากับข้อมูลผู้โดยสารล่วงหน้า เพราะลักษณะของข้อมูลการบันทึกของผู้โดยสารจะเป็นข้อมูลที่กว้างและเกี่ยวข้องทั้งหมดกับตัวผู้โดยสารเอง ในการเดินทางครั้งนั้นๆ ซึ่งในลักษณะที่กว้างนี้ก็อาจจะเป็นไปได้ต่อการกำหนดกฎเกณฑ์ให้ชัดเจน

หากจะต้องมีการกำหนดกฎเกณฑ์ของลักษณะที่ชัดเจนจนเกินไป ก็จะส่งผลต่อการดำเนินการของหน่วยงานบังคับใช้กฎหมายของรัฐที่อาจจะไม่สามารถเข้าถึงข้อมูลอย่างครอบคลุม ดังนั้นหลักเกณฑ์ของการแบ่งปันข้อมูลในลักษณะนี้จะเน้นไปที่ไม่ก่อความเสียหายต่อผู้เป็นเจ้าของข้อมูลในที่นี้คือผู้โดยสารเป็นหลัก ไม่กระทบต่อหลักการว่าด้วยสิทธิมนุษยชนและสิทธิหลักพื้นฐานของบุคคล รวมถึงมีมาตรการเยียวยาที่ชัดเจนต่อการละเมิดข้อมูลของบุคคลโดยหน่วยงานบังคับใช้กฎหมายของรัฐ ซึ่งในภาคผนวกที่ 9 ของอนุสัญญาว่าด้วยการบินพลเรือนระหว่างประเทศ ว่าด้วยเรื่องการดำเนินการต่อข้อมูลการบันทึกของผู้โดยสาร ผู้เขียนจะขอสรุปและอธิบายตามตารางดังต่อไปนี้

ตารางที่ 2: มาตราฐานสากลในการแบ่งปันข้อมูลการบินที่ตกลงกันโดยพลเรือนระหว่างประเทศ ตาม Annex 9 to the Convention on International Civil Aviation – Chapter 9 : Passenger data exchange systems – D. Passenger name record (PNR)

ชื่อ	รายละเอียดของการปฏิบัติ
9.22	<p>รัฐภาคีแต่ละรัฐที่ร้องขอแบ่งปันข้อมูลการบินที่ตกลงกันโดยพลเรือน (Passenger name record – PNR) จะต้องดำเนินการให้สอดคล้องกับ ข้อกำหนดของการขอข้อมูล (Data requirements) และการจัดเก็บข้อมูลดังกล่าวให้สอดคล้องกับแนวทางปฏิบัติที่มีอยู่ใน "ICAO Doc 9944", "ICAO - Guidelines on Passenger Name Record (PNR) Data", และ "PNRGOV message" ที่ได้รับการตีพิมพ์จากองค์การศุลกากรโลก (World Customs Organization – WCO) และได้รับการรับรอง (Endorsed) จากองค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization – ICAO) และสมาคมขนส่งทางอากาศระหว่างประเทศ (International Air Transport Association – IATA)</p>
9.22.1	<p>รัฐภาคีที่ทำการขอซึ่งการโอนข้อมูลการบินที่ตกลงกันโดยพลเรือน (Passenger name record – PNR) จะต้องดำเนินการโดยใช้ "the EDIFACT-based PNRGOV message" จากบริษัทสายการบินไปยังหน่วยงานของรัฐภาคี การปฏิบัติตามข้อนี้เป็นสิ่งประกันว่าความสามารถของข้อมูลจะทำงานร่วมกันได้ทั่วโลก (Global interoperability)</p> <ul style="list-style-type: none"> - หมายเหตุ "PNRGOV message" คือ ข้อความอิเล็กทรอนิกส์มาตรฐานที่รับรองร่วมกันโดยองค์การศุลกากรโลก (World Customs Organization – WCO) องค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization – ICAO) และสมาคมขนส่งทางอากาศระหว่างประเทศ (International Air Transport Association – IATA) - หมายเหตุ ข้อกำหนดนี้ไม่ได้มีวัตถุประสงค์เพื่อแทนที่หรือแทนที่ข้อความใด ๆ ที่แลกเปลี่ยนระหว่างผู้ดำเนินการเดินอากาศ (Aircraft operators) และหน่วยงานศุลกากรของรัฐภาคีในการปฏิบัติงานในพื้นที่
9.23	<p>รัฐภาคีแต่ละรัฐที่ร้องขอแบ่งปันข้อมูลการบินที่ตกลงกันโดยพลเรือน (Passenger name record – PNR) จะต้องพิจารณาความเป็นส่วนตัวของข้อมูล (Data</p>

ชื่อ	รายละเอียดของกรปฏิบัติ
	<p>privacy) จากการเก็บและแบ่งปันซึ่งข้อมูลการบินที่ของผู้โดยสาร โดยจะต้องสอดคล้องกับระบบของประเทศตนเองและระบบของประเทศอื่นๆ และรัฐภาคีแต่ละรัฐที่ร้องขอแบ่งปันข้อมูลการบินที่ของผู้โดยสาร (Passenger name record – PNR) จะต้องดำเนินการให้สอดคล้องกับข้อกำหนดทางกฎหมายที่ถูกกำหนดขึ้น (Legal requirements)</p>

ที่มาของข้อมูลในตาราง²⁸³



²⁸³ International Civil Aviation Organization, "Annex 9 to the Convention on International Civil Aviation Facilitation", Fifteenth Edition, (October 2017), p. 9-4
 CHAPTER 9. Passenger data exchange systems, Available from https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

3.3.3 ข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้าระวังและฐานข้อมูล

“ข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้าระวังและฐานข้อมูล (Watch lists and database)” นับว่าเป็นขั้นตอนท้ายสุดในการนำข้อมูลทั้งหมดของบุคคลที่ได้จากการเก็บข้อมูลและการแบ่งปันข้อมูลของหน่วยงานบังคับใช้กฎหมายที่มีหน้าที่เกี่ยวข้อง มาบูรณาการ เพื่อดำเนินมาตรการควบคุมชายแดนให้มีประสิทธิภาพ เพื่อการต่อต้านการก่อการร้าย เพราะหน้าที่หลักของการใช้ “Watch lists and database” ก็เพื่อที่จะประมวลผลและพิสูจน์ผลถึงข้อมูลทุกรูปแบบของตัวของนักท่องเที่ยว เช่น ข้อมูลผู้โดยสารล่วงหน้า, ข้อมูลการบันทึกของผู้โดยสาร, ข้อมูลชีวประวัติบุคคล, ข้อมูลชีวภาพบุคคล ในการติดตามผู้ก่อการร้าย นักรบต่างชาติ นักรบต่างชาติที่จะเดินทางไปร่วมฝึกรบหรือกลับคืนสู่ประเทศต้นทาง ทั้งที่เป็นบุคคลที่ต้องสงสัย หรืออยู่ตัวอย่างแน่ชัดแล้วว่าเกี่ยวข้องกับการก่อการร้าย

3.3.3.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ประการแรก ข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ 2396/2017 ได้ตัดสินใจให้บรรดารัฐสมาชิกสหประชาชาติ (Decides that Member States shall) จะต้องพัฒนา “Watch lists and database” เพื่อตรวจจับผู้ก่อการร้ายที่ทราบและอยู่ในรายชื่อ ผู้ต้องสงสัยว่าเกี่ยวข้องต่อก่อการร้าย รวมทั้งนักรบต่างชาติ นักรบต่างชาติที่จะเดินทางไปร่วมฝึกรบหรือกลับคืนสู่ประเทศต้นทาง²⁸⁴

ประการที่สอง ข้อมติที่ 2396/2017 ยังระบุต่อไปอีกหาส่งเสริมให้รัฐสมาชิกแบ่งปันข้อมูลต่อการพัฒนาระบบ “Watch lists and database” ผ่านกลไกความร่วมมือระดับทวิภาคีและพหุภาคี รวมถึงผ่าน Watch lists and database ขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL)

3.3.3.2 สารบัญญัติ

ลักษณะของข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้าระวังและฐานข้อมูล (Watch lists and database) จะถูกแบ่งออกเป็น 3 ลักษณะ **ประเภทแรกคือ** “Watch lists and database” ที่เป็นระบบที่ใช้ภายในชาติของรัฐตนเอง กล่าวคือมีการแบ่งปันข้อมูลทุกรูปแบบของตัวของนักท่องเที่ยวระหว่างหน่วยงานบังคับใช้กฎหมายกันเองภายในรัฐตน อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย

ประเภทที่สองคือ “Watch lists and database” ที่เป็นระบบที่ใช้ระดับภูมิภาคหรืออนุภูมิภาค กล่าวคือมีการการแบ่งปันข้อมูลทุกรูปแบบของตัวของนักท่องเที่ยว (API, PNR, Biographical info, Biometric info) ระหว่างหน่วยกลาง เช่น ศูนย์ความร่วมมือชายแดน ที่มีหน้าที่

²⁸⁴ United Nations Security Council Resolution 2396/2017, pp. 13

เพื่อให้ความร่วมมือกับหน่วยงานของต่างประเทศ (Counterparts across the border) ภายใต้วความร่วมมือต่อการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย

ประเภทที่สาม “Watch lists and database” ที่เป็นระบบระดับสากล กล่าวคือมีการการแบ่งปันข้อมูลทุกรูปแบบของตัวของนักท่องเที่ยว (API, PNR, Biographical info, Biometric info) ผ่านหน่วยงานระหว่างประเทศ เช่น Watch lists and database ขององค์การตำรวจอาชญากรรมระหว่างประเทศ²⁸⁵

ทั้งสามลักษณะของการแบ่งปันข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้าระวังและฐานข้อมูล (Watch lists and database) ก็เพื่อที่จะให้เกิดระบบของการแจ้งเตือน (Alert systems) เช่น การแจ้งเตือนล่วงหน้า (Advance warning) หรือขั้นตอนการตรวจสอบล่วงหน้า (Advance checking procedure) ในการรับรู้ถึงบุคคล หรือระบุตัวตนของบุคคล ที่เป็นอาชญากรที่ต้องสงสัย (Suspected criminals) ผู้ก่อการร้าย รวมไปถึงจนถึงสิ่งของที่น่าสงสัย วัสดุที่น่าสงสัยที่ติดตัวบุคคลนั้น มาจากการเดินทาง ยิ่งไปกว่าหน่วยงานบังคับใช้กฎหมายสามารถดำเนินการโดยใช้ฐานข้อมูลนี้ในการตรวจจับอาชญากรที่ต้องสงสัยรวมถึงผู้ก่อการร้ายที่เคยผ่านระบบคัดกรองตรวจจับในก่อนหน้านั้น ดังนั้นหน่วยงานบังคับใช้กฎหมายของรัฐที่มีหน้าที่เป็นจุดผ่านแดน (Border-crossing points) มีความจำเป็นที่จะต้องใช้การแบ่งปันข้อมูลใน “Watch lists and database” ในการดำเนินการต่อต้านการเดินทางของการก่อการร้าย²⁸⁶

3.3.3.3 กระบวนการในการแบ่งปันข้อมูล

ในกระบวนการของการแบ่งปันข้อมูลนั้นให้หน่วยงานบังคับใช้กฎหมาย หน่วยความมั่นคง ชายแดน ศุลกากร ทหาร และหน่วยข่าวกรอง มีหน้าที่ในการใช้ระบบ “Watch lists and database” ในการคัดกรองบุคคลที่เดินทาง ประเมินความเสี่ยงของบุคคลที่เกี่ยวข้องต่อการก่อการร้าย รวมทั้งการดำเนินการสืบสวนสอบสวนบุคคล โดยทั้งนี้การดำเนินการดังกล่าวของรัฐสมาชิกจะต้องเป็นไปตามกฎหมายภายในและเคารพต่อพันธกรณีระหว่างประเทศที่ว่าด้วยสิทธิมนุษยชน

ทั้งนี้สำนักผู้บริหารด้านการต่อต้านการก่อการร้ายแห่งสหประชาชาติ ได้ออกคำแนะนำต่อการดำเนินกับข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้าระวังและฐานข้อมูล และได้รับรองหลักการออกมาเป็น “Annex to the letter dated 28 December 2018 from the Chair of the Security Council

²⁸⁵ INTERPOL, "Main Database and our 18 databases" (2020), Available from https://www.interpol.int/en/content/download/15012/file/GI-04_Databases_Factsheets_EN_2020-03.pdf

²⁸⁶ Security Council, "Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), pp.9, 10, 11, 12

Committee” Guiding Principle ที่ 2 ว่าด้วยเรื่องการพัฒนาระบบ Watch lists and database การต่อต้านการก่อการร้ายแบบบูรณาการโดยผู้เขียนจะได้สรุปและอธิบายตามตารางดังต่อไปนี้

หัวข้อ	รายละเอียด
ข้อ A	รัฐสมาชิกจะต้องจัดให้มีการกำกับดูแลอย่างมีประสิทธิภาพ (Effective oversight) ของทุกขั้นตอนของการดำเนินการพัฒนา Watch list or database และให้ความใส่ใจต่อฟังก์ชันของการจัดการข้อมูล (Data-management functions) เพื่อที่จะหลีกเลี่ยงการใช้ข้อมูลในฐานะข้อมูลไปในทางที่ผิดวัตถุประสงค์และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized extension of access)
ข้อ B	รัฐสมาชิกควรตรวจสอบให้แน่ใจว่ามีเกณฑ์ที่ชัดเจนและเหมาะสม (Clear and appropriate criteria) ในการกำหนดความหมายของการกระทำการก่อการร้าย (Terrorist acts) รวมถึงขั้นตอนการใส่รายชื่อและข้อมูลของบุคคลที่ต้องสงสัยใน Watch lists and databases ซึ่งจะต้องสอดคล้องกับข้อมติของคณะมนตรีความมั่นคงแห่งสหประชาชาติ พันธกรณีระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้าย และอนุสัญญาต่อต้านการก่อการร้ายสากล
ข้อ C	รัฐสมาชิกจะต้องกำหนดกรอบการกำกับดูแล (Regulatory framework) อย่างชัดเจนสำหรับ การลงทะเบียนเพื่อเข้าถึงข้อมูล การใช้งานข้อมูล การพิจารณาข้อมูล การเก็บรักษาข้อมูล และการลบซึ่งข้อมูลใน Watch list or database
ข้อ D	รัฐสมาชิกจะต้องแน่ใจว่าเครือข่ายการสื่อสาร (Communications network) ของตนจะต้องมีความปลอดภัยและมีระดับความปลอดภัยที่จะสามารถปกป้องสภาพแวดล้อมของระบบปฏิบัติงาน (Operational environment of Watch list or database) เช่น ข้อมูล (The data) ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) เครือข่ายการสื่อสาร (The communications network)
ข้อ E	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่าระบบ Watch list or database จะมีการรวบรวมข้อมูลจากหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง (Authorized relevant law enforcement agencies)
ข้อ F	รัฐสมาชิกจะต้องแน่ใจว่า Watch list or database เป็นที่เข้าถึงของหน่วยงานบังคับใช้กฎหมาย (Law enforcement agencies) และหน่วยงานควบคุมชายแดน (Border control authorities)
ข้อ G	รัฐสมาชิกจะต้องตรวจสอบให้แน่ใจว่าการดำเนินมาตรการต่อต้านการก่อการร้ายของหน่วยงานบังคับใช้กฎหมายและหน่วยงานควบคุมชายแดน จะต้องสอดคล้องต่อข้อมูล

หัวข้อ	รายละเอียด
	<p>ที่มีอยู่จริงในฐานข้อมูล Watch list or database ตลอดจนเป็นไปตามกฎหมายภายในและพันธกรณีระหว่างประเทศว่าด้วยสิทธิมนุษยชน</p>
ข้อ H	<p>รัฐสมาชิกจะต้องพิจารณาการดำเนินงานที่เฉพาะ (Specific frameworks) ต่อการปกป้องและส่งเสริมสิทธิเด็ก ในกรณีที่มีข้อมูลของเด็กอยู่ในฐานข้อมูล Watch lists or databases หรือฐานข้อมูลที่เกี่ยวข้องต่อการปกป้องเด็ก (Databases for child-protection purposes) รวมไปถึงข้อมูลที่เกี่ยวข้องกับการสาบสูญหายของเด็กที่เป็นเหยื่อของการลักพาตัว (Kidnappings) และการหายตัวไปของเด็กที่ไม่สามารถอธิบายได้ (Unexplained disappearances) ซึ่งข้อมูลเหล่านี้ อาจจะได้มาจากการแบ่งปันข้อมูลภายในประเทศที่ให้ความร่วมมือในระดับทวิภาคี หรือพหุภาคี หรือได้ข้อมูลเหล่านี้มาจากระบบการแจ้งเตือนหมายเหลือง (Yellow alert system) จาก 18 ฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ</p>
ข้อ I	<p>รัฐสมาชิกควรจะมีส่วนร่วมและใช้ประเทศจากฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ และแน่ใจว่าหน่วยงานบังคับใช้กฎหมาย หน่วยควบคุมชายแดน ศุลกากร หน่วยงานส่วนหน้าในการตรวจคนเข้าเมือง (Frontline border posts) เช่น ทางอากาศ ทางพรมแดน ทางทะเลของรัฐตนได้เชื่อมต่อกับฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ โดยผ่าน สำนักงานกลางแห่งชาติ National Central Bureaus (NCBs)</p> <ul style="list-style-type: none"> - หมายเหตุ “สำนักงานกลางแห่งชาติ (National Central Bureaus)” จะถูกจัดตั้งขึ้นในแต่ละประเทศสมาชิกขององค์การตำรวจอาชญากรรมระหว่างประเทศ(International Criminal Police Organization) ซึ่งหน่วยงานกลางแห่งชาตินี้นับเป็นกลไกที่สำคัญที่สุดขององค์การตำรวจสากล เนื่องจากบุคลากรที่ทำงานในส่วนนี้จะป็นเจ้าหน้าที่ฝ่ายปกครองหรือตำรวจของประเทศนั้นๆ และองค์การตำรวจสากลจะประสานการทำงานโดยผ่านเจ้าหน้าที่เหล่านี้ ประเทศไทยเองก็มีสำนักงานกลางแห่งชาติ (NCB) โดยของไทยจะใช้ชื่อว่า INTERPOL National Central Bureau Bangkok หรือสำนักงานกลางแห่งชาติตำรวจสากลกรุงเทพ สังกัดกองการต่างประเทศ สำนักงานตำรวจแห่งชาติ
ข้อ J	<p>รัฐสมาชิกได้ดำเนินการเชื่อมต่อฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ จะต้องมีการออกกฎระเบียบข้อบังคับว่าด้วยการใช้ข้อมูลในฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศเพื่อคัดกรองนักท่องเที่ยวที่เดินทางผ่าน</p>

หัวข้อ	รายละเอียด
	จุดตรวจอากาศยาน จุดตรวจระหว่างพรมแดน และจุดตรวจทางทะเล และเพื่อการดำเนินการประเมินความเสี่ยงของข้อมูลบุคคล ตลอดจนทำการสืบสวนสอบสวนบุคคลที่อาจจะเกี่ยวข้องต่อการก่อการร้าย นักรบต่างชาติ รวมถึงครอบครัวของบุคคลดังกล่าว

ที่มาของข้อมูลในตาราง²⁸⁷

3.3.3.4 กลไกควบคุมการใช้ในทางที่ผิด

ในระดับภายในประเทศ การดำเนินการต่อการพัฒนาระบบ “Watch lists and database” นั้น ในปัจจุบันมิได้มีมาตรฐานสากล (Common international standard) ที่เป็นที่ยอมรับเพื่อจะมากำกับกับการดำเนินการของรัฐต่อการพัฒนา “Watch lists and database” ในระบบภายในประเทศของตน อย่างไรก็ตามรัฐควรที่จะต้องนำมาตราฐานและเกณฑ์สากล (Universal standards and criteria) ในหลักการที่ว่าด้วยสิทธิมนุษยชนมาใช้ต่อการกำหนดรายชื่อของบุคคล ใน “National watch lists and database” ภายในรัฐตน จัดตั้งหน่วยตรวจสอบอิสระเพื่อกำหนดมาตรการของการจัดการและการแบ่งปันข้อมูลใน “National watch lists and database” และการกำหนดขั้นตอนและกระบวนการ หรือเงื่อนไขในกรณีที่มีเหตุผลอันควรเชื่อว่าจะต้องดำเนินการลบรายชื่อบุคคลออกจากฐานข้อมูลไว้เป็นที่ชัดเจน

ในระดับระหว่างประเทศ Watch lists and database ขององค์การตำรวจอาชญากรรมระหว่างประเทศ ได้สร้างกลไกของการควบคุมที่จะมีให้องค์การดำเนินการกระทบต่อหลักการว่าด้วยสิทธิมนุษยชน ดังนั้นจึงมีการจัดตั้งหน่วยตรวจสอบอิสระขึ้นมาชื่อว่า “The Commission for the Control of INTERPOL Files”²⁸⁸ เพื่อมีหน้าที่ในการควบคุมรัฐสมาชิกขององค์การตำรวจอาชญากรรมระหว่างประเทศปฏิบัติให้สอดคล้องกับหลักเกณฑ์ที่เข้มงวดในการแบ่งปันข้อมูลระหว่างองค์การกับรัฐสมาชิก เพื่อแน่อนใจว่าการดำเนินการดังกล่าวจะเป็นไปตามกฎหมาย และคุณภาพของการแบ่งปันข้อมูล (Quality of the information sharing) เพื่อปกป้องข้อมูลส่วนบุคคลรวมทั้งสิทธิความเป็นส่วนตัวของบุคคล

²⁸⁷ Security Council, "Guiding Principle 2 - Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2018), p. 8

²⁸⁸ INTERPOL, "Commission for the Control of INTERPOL's Files (CCF)" (2020), Retrieved from <https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF>

3.4 การแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้าย

ในหลายๆประเทศหน่วยงานบังคับใช้กฎหมาย มีบทบาทหลักในการต่อต้านการก่อการร้าย ความจำเป็นของการได้รับข้อมูลสำคัญต่างๆเพื่อนำมาดำเนินมาตรการปราบปรามจึงมีความจำเป็นอย่างยิ่ง ซึ่งมาตรการปราบปรามเหล่านั้นจะเกิดขึ้นอย่างมีประสิทธิภาพได้ หากได้ปราศจากการอาศัยความร่วมมือและการประสานงานในการแบ่งปันข้อมูล ที่สอดคล้องกับพันธกิจของคณะมนตรีความมั่นคงแห่งสหประชาชาติได้มีความพยายามที่จะสร้างพันธกรณีให้รัฐสมาชิกมีการแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้าย

3.4.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ประเด็นแรก พันธกรณีการแบ่งปันข้อมูลของรัฐสมาชิกแห่งสหประชาชาติที่เกี่ยวกับการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้ายนั้น คณะมนตรีความมั่นคงแห่งสหประชาชาติได้รับรองข้อมติที่สำคัญหลายๆ อยู่จำนวนสองฉบับ นั่นคือ **ข้อมติที่ 2178/2014** ได้กระตุ้นให้บรรดารัฐสมาชิกของสหประชาชาติ (Urges Member States) อาศัยกฎหมายภายในรัฐและกฎหมายระหว่างประเทศดำเนินการให้มีการแบ่งปันข้อมูลการปฏิบัติกา ในการต่อต้านการกระทำ และความเคลื่อนไหว ของผู้ก่อการร้าย นักรบต่างชาติ และเครือข่ายก่อการร้าย²⁸⁹ ผ่านกลไกความร่วมมือทั้งแบบพหุภาคีและทวิภาคีโดยเฉพาะกับประเทศที่เป็นถิ่นที่อยู่ของผู้ก่อการร้าย หรือผู้ก่อการร้ายนั้นมีสัญชาติ

ประเด็นที่สอง ในส่วน **ข้อมติที่ 2309/2016** ได้เรียกร้องให้รัฐดำเนินการพัฒนาความร่วมมือระดับระหว่างประเทศ ความร่วมมือระดับภูมิภาค ในการแบ่งปันข้อมูลต่อการดำเนินการบังคับทางกฎหมายเพื่อต่อต้านการคุกคามจากการก่อการร้าย และการเดินทางของนักรบต่างชาติ รวมไปถึงทั้งการเดินทางกลับสู่ประเทศต้นทางของนักรบต่างชาติ²⁹⁰

ประเด็นที่สาม ในปัจจุบันนี้การก่อการร้ายได้อาศัยวิธีการใหม่ๆ เพื่อหลบเลี่ยงการตรวจจับของหน่วยงานบังคับใช้กฎหมาย และส่วนสำคัญที่ทำให้เกิดช่องว่างดังกล่าวคือการแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายที่ไม่ค่อยได้ประสิทธิภาพ กล่าวคือใช้ระยะเวลาในการแบ่งปันข้อมูลทีนานไป ซึ่งในหลายๆรัฐสมาชิกได้ริเริ่มนำแนวทางของการแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายแบบระบบเรียลไทม์ (Real time exchange information) และเชื่อมต่อฐานข้อมูลของหน่วยงานบังคับใช้กฎหมายของรัฐเหล่านั้นกับฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ ข้อมติของคณะมนตรีความมั่นคงแห่งสหประชาชาติ **ข้อมติที่ 2178/2014** ได้รับรองการ

²⁸⁹ United Nations Security Council Resolution 2178/2014, pp. preamble, 3, 11

²⁹⁰ United Nations Security Council Resolution 2309/2016, pp. 8

ทำงานของฐานข้อมูลองค์การตำรวจอาชญากรรมระหว่างประเทศในการต่อต้านการก่อการร้ายและติดตามความเคลื่อนไหวของผู้ก่อการร้าย²⁹¹ รวมไปถึงการเดินทางของนักรบต่างชาติ โดยการดำเนินการแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายของรัฐสมาชิกผ่านเครือข่ายการสื่อสารที่ปลอดภัยตลอด 24 ชั่วโมงและ 7 วัน หรือที่เรียกว่า "INTERPOL I-24/7 secure communications network" และฐานข้อมูลที่มีการดำเนินการอยู่แล้ว อาทิ ฐานข้อมูลทั่วโลกและการประกาศแจ้งเตือน (Global databases and notices) คณะมนตรีความมั่นคงได้สนับสนุนให้องค์การตำรวจอาชญากรรมระหว่างประเทศให้แนวทางและการสนับสนุนต่อรัฐสมาชิกสหประชาชาติในการร่วมมือต่อการแบ่งปันข้อมูลกับฐานข้อมูลขององค์การ ตลอดจนการให้คำแนะนำต่อการดำเนินการปฏิบัติของรัฐสมาชิก²⁹²

3.4.2 สารบัญญัติของข้อมูล

ในการแบ่งปันข้อมูลของหน่วยงานบังคับใช้กฎหมายเพื่อการต่อต้านการก่อการร้าย ข้อมูลที่เกี่ยวข้องกับการก่อการร้าย (Terrorism-related information) จะได้มาจากการพิจารณาข้อมูลอาชญากรรมประเภทอื่นๆที่เกี่ยวข้องด้วย เช่น ข้อมูลบันทึกประวัติอาชญากรรม, ข้อมูลรายงานเหตุการณ์การบังคับใช้กฎหมาย, ข้อมูลบันทึกการดำเนินการและคำตัดสินของศาล, ข้อมูลของบุคคลที่อยู่ในรายชื่อเฝ้าระวัง และข้อมูลของผู้ต้องสงสัยคดีการก่อการร้าย แหล่งข้อมูลสำคัญเหล่านี้จะได้อาจมาจากหน่วยงานบังคับใช้กฎหมายของรัฐ รวมถึงหน่วยงานบังคับใช้กฎหมายของรัฐต่างประเทศที่อยู่ภายใต้ความร่วมมือทางข้อมูลต่อกัน

การแบ่งปันข้อมูลต่อการบังคับใช้กฎหมาย จะมีความแตกต่างจากการแบ่งปันข้อมูลในเรื่องอื่นๆ เช่น ข้อมูลความมั่นคงของชาติ หรือข้อมูลเพื่อการข่าวกรอง เพราะการแบ่งปันต่อการบังคับใช้กฎหมายจะเน้นไปที่การได้รับข้อมูลมาเพื่อ "ลงมือดำเนินการ" และลักษณะของการดำเนินการจะต้องเป็นไปในแบบ "การแบ่งปันข้อมูลให้ครอบคลุมต่อแผนงานอย่างมีประสิทธิภาพ" จะอธิบายได้ว่าเป็นการใช้งานของข้อมูลที่อยู่ในระบบปิดระหว่างหน่วยงานบังคับใช้กฎหมายของรัฐที่สามารถเก็บข้อมูลที่เกี่ยวข้อง และแบ่งปันข้อมูลเหล่านั้นให้กับหน่วยงานบังคับใช้กฎหมายของรัฐอื่นที่ได้รับอนุญาตให้

²⁹¹ United Nations Security Council Resolution 2178/2014, pp. preamble, 13

²⁹² INTERPOL, "INTERPOL's activities against the foreign terrorist fighter threat", Published on the occasion of the Leaders' Summit on Countering ISIL and Violent Extremism (New York, 2015), Available from https://www.cato.org/sites/cato.org/files/wp-content/uploads/information_sheet_foreign_fighter.pdf

เข้าถึงข้อมูล โดยมีความสามารถที่จะแบ่งปันข้อมูลได้อย่างทันเวลาและปลอดภัย²⁹³ ต่อการนำไปดำเนินมาตรการบังคับในทางกฎหมายต่างๆ

3.4.3 กระบวนการในการแบ่งปันข้อมูล

กระบวนการของการแบ่งปันข้อมูลซึ่งข้อมติได้กำหนดเรียกร้องให้รัฐสมาชิกพัฒนาความร่วมมือระดับระหว่างประเทศ ความร่วมมือระดับภูมิภาค ความร่วมมือระดับอนุภูมิภาค ทั้งรูปแบบทวิภาคีและพหุภาคีในการแบ่งปันข้อมูลเพื่อวัตถุประสงค์ต่อการนำข้อมูลเหล่านั้นในการวินิจฉัย และสืบสวนสอบสวน การก่อการร้าย รวมทั้งแบ่งปันแนวทางในการปฏิบัติที่ดีที่สุด ระหว่างรัฐที่อยู่ภายใต้ความร่วมมือ ซึ่งการดำเนินการของรัฐสมาชิกตามพันธกรณีนี้จะต้องสอดคล้องกับหลักการที่ว่าด้วยสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานรวมไปจนถึงพันธกรณีตามกฎหมายระหว่างประเทศอื่นๆ ที่เกี่ยวข้อง

เมื่อพิจารณาข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติทั้งสองที่ได้กล่าวมาแล้วนั้นข้างต้น จะพบว่าข้อมติต้องการที่จะให้มีการแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายของรัฐสมาชิก ซึ่งจะต้องเป็นข้อมูลที่เป็นประโยชน์ต่อการดำเนินการสอบสวนคดีในเชิงรุก กล่าวคือข้อมูลที่สามารถใช้ในการดำเนินการตรวจจับการรับสมัครการก่อการร้าย การจัดหาเงินทุนของการก่อการร้าย การเดินทางของการก่อการร้าย และการสื่อสารเพื่อการก่อการร้าย ซึ่งทั้งหมดเป็นคือการดำเนินการมาตรการต่อต้านการก่อการร้ายของหน่วยงานบังคับใช้กฎหมายในเชิงรุก²⁹⁴

ส่วนการสอบสวนคดีก่อการร้ายโดยทั่วไปนั้น การแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายเป็นวิธีการที่สำคัญมาก ต่อการดำเนินการจับกุมบุคคลผู้ต้องสงสัยต่อการก่อการร้าย การระงับเหตุความรุนแรงจากกลุ่มผู้ก่อการร้ายรายย่อย รวมไปถึงการป้องกันเหตุการณ์ก่อการร้ายล่วงหน้า (Pre-empting terrorist activity) ซึ่งจะต้องมีหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะ

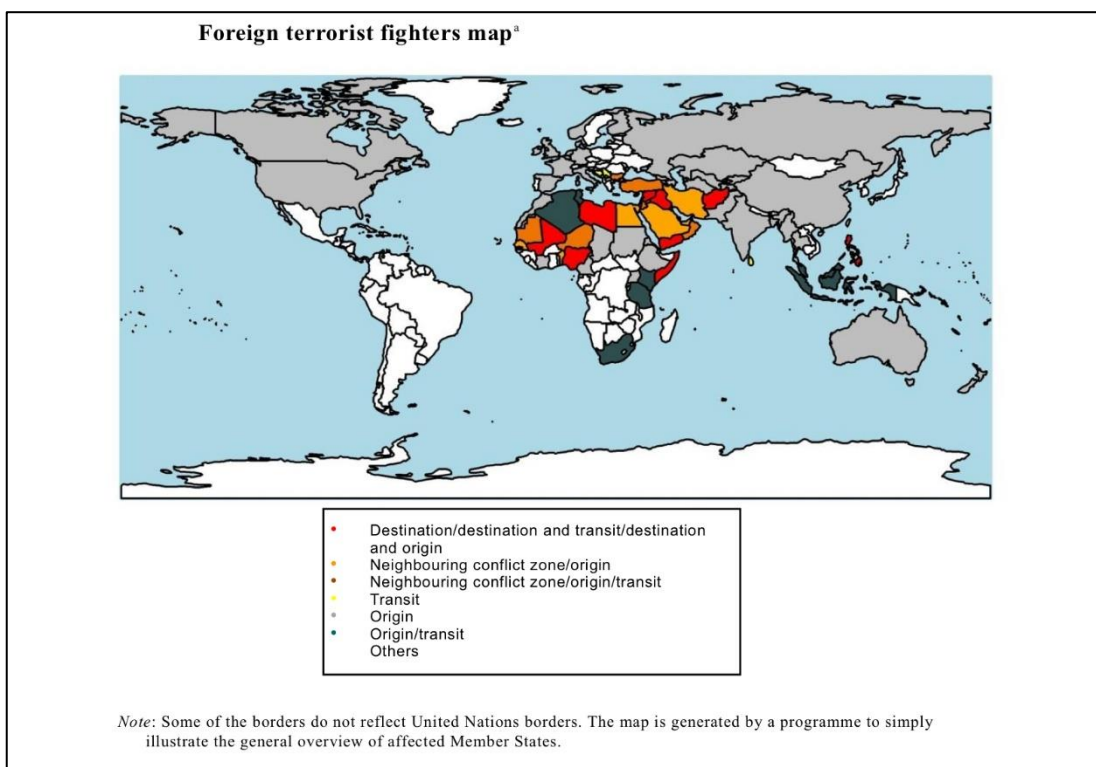
3.4.3.1 การจัดตั้งหน่วยงาน

1. หน่วยงานปราบปรามการก่อการร้าย

ตัวอย่างรายละเอียดในเรื่องของการดำเนินการปฏิบัติตามข้อมติของคณะมนตรีความมั่นคงของรัฐสมาชิก คณะกรรมาธิการการต่อต้านการก่อการร้าย ได้มีรายงานออกมาว่าด้วยการแบ่งปันข้อมูลต่อการปฏิบัติงานของหน่วยงานบังคับใช้กฎหมาย

²⁹³ Office of the Director of National Intelligence, “Law enforcement information sharing” (2020), Retrieved from <https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing>

²⁹⁴ Security Council, *Second report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range* (2016).



อ้างอิงข้อมูลรูปภาพ : UN Document S/2015/683

ในภูมิภาคอเมริกา และภูมิภาคโอเชียเนีย ทุกประเทศในภูมิภาคดังกล่าว ได้จัดตั้งหน่วยต่อต้านการก่อการร้ายโดยเฉพาะ ตามพันธกรณีของข้อมติที่ 2178/2014 ซึ่งในอีกแง่หนึ่งนั้น หน่วยต่อต้านจะทำหน้าที่เสมือนหน่วยปฏิบัติการกลาง ในการเก็บข้อมูลและแบ่งปันข้อมูล อาทิ ข้อมูลบันทึกประวัติอาชญากรรม, ข้อมูลรายงานเหตุการณ์การบังคับใช้กฎหมาย, ข้อมูลบันทึกการดำเนินการและคำตัดสินของศาล, ข้อมูลของบุคคลที่อยู่ในรายชื่อเฝ้าระวัง และข้อมูลของผู้ต้องสงสัยคดีการก่อการร้าย รวมไปถึงข่าวกรองต่อต้านการก่อการร้ายที่สำคัญ

2. การทำงานของหน่วยงานปราบปรามการก่อการร้าย

หน่วยงานปราบปรามการก่อการร้ายจะดำเนินการแบ่งปันข้อมูลระหว่างหน่วยงานบังคับใช้กฎหมายในภูมิภาคที่มีหน้าที่ต่อต้านการก่อการร้ายทั้งหมด โดยเฉพาะ การดำเนินมาตรการการต่อต้านนักรบต่างชาติ ตามที่ข้อมติ 2178/2014 มีวัตถุประสงค์ไว้เป็นสำคัญ²⁹⁵ หน่วยต่อต้านจะทำการอาศัยรวบรวมข้อมูลที่เกี่ยวข้องจากหน่วยต่อต้านของแต่ละประเทศ ยิ่งไปกว่านั้นหน่วยต่อต้านจะ

²⁹⁵ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2020), pp. 99

มีหน้าที่ในการรายงานเพื่อแจ้งเตือนหน่วยงานบังคับใช้กฎหมายของรัฐ และรัฐภายในภูมิภาคในกรณี ที่คาดว่าจะเป็ นเหตุการณ์ที่มีความจำเป็นจะต้องแจ้งเป็นการเฉพาะเจาะจงต่อรัฐดังกล่าวในการ ประสานงานเพื่อสืบสวนสอบสวนต่อการดำเนินการก่อการร้าย

3. สำนักงานกลางแห่งชาติ

ประเทศสมาชิกทุกๆประเทศขององค์การตำรวจอาชญากรรมระหว่างประเทศ จะต้องมีการ จัดตั้ง สำนักงานกลางซึ่งเรียกว่า “National Central Bureau (NCB)” เป็นศูนย์รวบรวมข้อมูลกลาง ทุกอย่างจากหน่วยงานบังคับใช้กฎหมายภายในประเทศนั้น ซึ่ง NCB เป็นกลไกช่องทางที่สำคัญในการ ดำเนินงานขององค์การตำรวจอาชญากรรมระหว่างประเทศ ที่มีวัตถุประสงค์เพื่อทำหน้าที่ ประสานงาน และติดต่อแลกเปลี่ยนข้อสนเทศหรือข้อมูล²⁹⁶ เกี่ยวกับอาชญากรรมต่อองค์การตำรวจ อาชญากรรมระหว่างประเทศ หรือต่อกองบัญชาการกลางแห่งชาติของประเทศสมาชิกอื่น ทั้งนี้ ใน กองบัญชาการกลางแห่งชาติของแต่ละประเทศสมาชิกจะมีเจ้าหน้าที่ติดต่อประสานงานขององค์การ ตำรวจอาชญากรรมระหว่างประเทศ หรือของประเทศสมาชิกอื่นประจำการอยู่ด้วย จึงทำให้การ ติดต่อประสานงาน และการแลกเปลี่ยนข้อมูลหรือข้อสนเทศเป็นไปด้วยความสะดวก รวดเร็ว

4. การทำงานของสำนักงานกลางแห่งชาติ

หน่วยงานบังคับใช้กฎหมายของรัฐสมาชิกอื่นๆจะให้ข้อมูลต่างๆ ผ่าน "สำนักงานกลาง แห่งชาติ" ของตน และข้อมูลเหล่านั้นจะถูกรวบรวมไว้ในฐานข้อมูลกลางขององค์การตำรวจ อาชญากรรมระหว่างประเทศ การใช้ข้อมูลในฐานข้อมูลกลางจะเป็นไปเพื่อการต่อต้านการก่อการร้าย และการดำเนินการแจ้งเตือนต่างๆต่อรัฐสมาชิกขององค์การตำรวจอาชญากรรมระหว่างประเทศ อาทิ

1.) ทำการติดต่อกับประเทศสมาชิก เพื่อขอทราบรายงานและสถิติอาชญากรรมของประเทศ เหล่านั้น โดยประเทศภาคีสมาชิกจะจัดส่งไปยังสำนักงานกลางทุกๆปี ทำรายงานส่งให้ประเทศภาคี ทราบถึงความเคลื่อนไหว ของผู้ร้ายซึ่งประเทศภาคีต้องการทราบ จัดส่งใบแจ้งรูปพรรณของผู้ร้าย บางคนไปให้ประเทศภาคี ทำการแจ้งข่าวคราวการเคลื่อนไหวของผู้ร้ายบางคนเพื่อเป็นการ แลกเปลี่ยนข่าวสารและประสานงานในการที่จะจับกุมต่อไป ตลอดจนรวบรวมประวัติอาชญากร สำคัญๆ ของโลก เพื่อสะดวกในการสืบสวนและจับกุมของประเทศภาคี

2.) ร่วมมือกับสมาชิกตำรวจสากลประเทศอื่น ในการจับกุม ปราบปราม และดำเนินการ สอบสวนคดีอาชญากรรมหรือความผิดตามกฎหมายระหว่างประเทศ อันได้แก่ การกระทำความผิด

²⁹⁶ INTERPOL, "The National Central Bureau is a country's focal point for all INTERPOL activities." (2018), Retrieved from <https://www.interpol.int/Who-we-are/Member-countries/National-Central-Bureau-NCBs>

อาญาต่อบุคคล การค้าทาส การลักทรัพย์ ปล้นทรัพย์ สลัดอากาศ โจรสลัด การกระทำความผิดต่างๆ เกี่ยวกับยานพาหนะสัญจร การฉ้อโกงระหว่างประเทศ การกระทำความผิดเกี่ยวกับการปลอมเงินตรา ยาเสพติดให้โทษ การส่งผู้ร้ายข้ามแดน

3.) การประกาศแจ้งเตือนตำรวจทั่วโลกถึงบุคคลและคณะบุคคลที่อยู่ภายใต้มาตรการคว่ำบาตรที่กำหนดโดยคณะมนตรีความมั่นคงแห่งสหประชาชาติ (Notices of UNSC sanctions)²⁹⁷

4.) หมายแดง (Red Notice) คือ คำร้องขอไปยังหน่วยงานบังคับใช้กฎหมายทั่วโลก (Law enforcement worldwide) ในการค้นหาและจับกุมบุคคลที่อยู่ระหว่างการส่งผู้ร้ายข้ามแดน บุคคลที่ยอมมอบตัว หรือการดำเนินการทางกฎหมายที่มีลักษณะในฐานความผิดเหมือนกัน

5.) หมายเหลือง คือ การแจ้งเตือนของตำรวจทั่วโลกสำหรับผู้สูญหาย มีการเผยแพร่สำหรับเหยื่อของการลักพาตัวโดยผู้ปกครอง (Parental abductions) การลักพาตัวทางอาญา (Criminal abductions or kidnappings) หรือการหายตัวไปโดยไม่ได้อธิบาย

6.) หมายอื่นๆ ตามลักษณะของอาชญากรรมดังรูปภาพดังต่อไปนี้

Types of Notice			
	Red Notice To seek the location and arrest of wanted persons with a view to extradition or similar lawful action.		Yellow Notice To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.
	Blue Notice To collect additional information about a person's identity, location or activities in relation to a crime.		Black Notice To seek information on unidentified bodies.
	Green Notice To provide warnings and intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.		Orange Notice To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety.
	INTERPOL–United Nations Security Council Special Notice Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees.		Purple Notice To seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

อ้างอิง URL รูปภาพ :

https://www.samuitimes.com/wp-content/uploads/2017/08/interpol_notice_red_bull_heir_Thailand.jpg

²⁹⁷ “Notices alert police globally to individuals and entities who are subject to sanctions imposed by the United Nations Security Council”

ดังนั้นลักษณะของการแบ่งปันข้อมูลและการประสานงานระหว่างหน่วยงานบังคับใช้กฎหมายของรัฐสมาชิกผ่านองค์การตำรวจอาชญากรรมระหว่างประเทศจะอยู่ในรูปแบบตามแผนผังดังต่อไปนี้

แผนผังโครงสร้าง : การแบ่งปันข้อมูลผ่านฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ



3.4.2.2 ความร่วมมือและการประสานงาน

1. ความร่วมมือระหว่างประเทศ

ตามข้อมติของคณะมนตรีความมั่นคงทั้งสองมติข้างต้นว่าด้วยการแบ่งปันข้อมูลต่อการปฏิบัติงานของหน่วยงานบังคับใช้กฎหมาย รัฐสมาชิกมีความจำเป็นอย่างยิ่งในการดำเนินการร่วมมือกันผ่านความตกลงช่วยเหลือทางข้อมูลทั้งแบบทวิภาคีและพหุภาคีเพื่อให้รัฐสมาชิกได้มีการเพิ่มประสิทธิภาพของการดำเนินมาตรการต่อต้านการก่อการร้าย อย่างไรก็ตามรัฐสมาชิกของสหประชาชาติอาจจะใช้ประโยชน์จากความร่วมมือของหน่วยงานบังคับใช้กฎหมายที่มีอยู่แล้วโดยทั่วไปในระดับระหว่างประเทศและระดับภูมิภาค เช่น

- องค์การตำรวจอาชญากรรมระหว่างประเทศ
- หน่วยงานสหภาพยุโรปเพื่อความร่วมมือด้านการบังคับใช้กฎหมาย (The European Union Agency for Law Enforcement Cooperation - Europol)
- องค์การตำรวจแห่งชาติสำหรับสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (The National Police organization for the Association of Southeast Asian Nations – ASEANAPOL)

2. การประสานงานกับองค์การตำรวจอาชญากรรมระหว่างประเทศ

รัฐสมาชิกสหประชาชาติที่ได้เข้าร่วมเป็นภาคีขององค์การตำรวจอาชญากรรมระหว่างประเทศ หน่วยงานที่เสมือนเป็นหน่วยงานกลางประสานระหว่างองค์การตำรวจอาชญากรรมระหว่างประเทศกับหน่วยงานบังคับใช้กฎหมายภายในของรัฐที่เรียกกันว่า “สำนักงานกลางแห่งชาติ (National Central Bureaus)” จะถูกจัดตั้งขึ้นในแต่ละประเทศสมาชิกขององค์การตำรวจ

อาชญากรรมระหว่างประเทศ(International Criminal Police Organization) ซึ่งหน่วยงานกลางแห่งชาตินี้ นับเป็นกลไกที่สำคัญที่สุดขององค์การตำรวจสากล เนื่องจากบุคลากรที่ทำงานในส่วนนี้จะ เป็นเจ้าหน้าที่ฝ่ายปกครองหรือตำรวจของประเทศนั้นๆ และองค์การตำรวจสากลจะประสานการทำงานและการแบ่งปันข้อมูลโดยผ่านเจ้าหน้าที่เหล่านี้²⁹⁸ ประเทศไทยเองก็มีสำนักงานกลางแห่งชาติ (NCB) โดยของไทยจะใช้ชื่อว่า INTERPOL National Central Bureau Bangkok หรือสำนักงานกลางแห่งชาติตำรวจสากลกรุงเทพ สังกัดกองการต่างประเทศ สำนักงานตำรวจแห่งชาติ

3.4.4 เครื่องมือและกลไกเสริมในการแบ่งปันข้อมูล

ในปัจจุบันองค์การตำรวจอาชญากรรมระหว่างประเทศได้พัฒนาฐานข้อมูลในหลากหลายประเภท เพื่อเป็นประโยชน์ต่อใช้ข้อมูลดำเนินการสืบสวนสอบสวนอาชญากรรมของหน่วยงานบังคับใช้กฎหมายของรัฐสมาชิก อย่างไรก็ตามข้อมูลที่จำเป็นต่อการดำเนินการนั้นจะมีประสิทธิภาพหรือไม่ จะขึ้นอยู่กับว่ารัฐสมาชิกขององค์การตำรวจอาชญากรรมระหว่างประเทศได้ส่งเสริมและแบ่งปันข้อมูลแบบ Up-to-Date ต่อฐานข้อมูลกลางขององค์การตำรวจอาชญากรรมระหว่างประเทศมากน้อยเพียงใด รัฐสมาชิกของสหประชาชาติและความร่วมมือของหน่วยงานบังคับใช้กฎหมายของภูมิภาคต่างๆ ได้ถูกผลักดันให้เชื่อมต่อกับฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ เพื่อการแบ่งปันข้อมูล และการใช้ข้อมูลเพื่ออำนวยความสะดวกต่อการดำเนินการสืบสวนสอบสวน ตลอดจนเป็นการส่งเสริมการร่วมมือในการประสานงานของหน่วยงานตำรวจระหว่างประเทศ (International police cooperation) ซึ่งฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศผู้เขียนจะขออธิบาย และสรุปตามตารางดังต่อไปนี้

ตาราง : คุณสมบัติของฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ

<p>คุณสมบัติของการแบ่งปันข้อมูลทั่วโลก</p> <p>Global Information Sharing</p>	<p>ฐานข้อมูลของ INTERPOL จะช่วยให้ประเทศสมาชิกสามารถเข้าถึงฐานข้อมูลอาชญากรรมที่หลากหลายได้ทันที เช่น ข้อมูลการบันทึกลายนิ้วมือ ข้อมูลดีเอ็นเอ ข้อมูลรายละเอียดการจดทะเบียนยานยนต์ที่ถูกขโมย ข้อมูลรายละเอียดการพกอาวุธปืน ข้อมูลเอกสารการเดินทางที่ถูกขโมยและสูญหาย และอื่น ๆ อีกมากมาย ฐานข้อมูลแบ่งปันข้อมูลที่สนับสนุนข้อมูลจากประเทศสมาชิกตามเงื่อนไขดังต่อไปนี้</p>
--	---

²⁹⁸ ThaiArmedForce, "องค์การตำรวจสากล (INTERPOL) คือใคร?" (2019), Retrieved from <https://thaiarmedforce.com>

- มีการแบ่งปันข้อมูลผ่านระบบการสื่อสารของหน่วยงาน บังคับใช้กฎหมายที่ปลอดภัยตลอด 24 ชั่วโมงทั้ง 7 วัน (Information is shared through the I-24/7 secure police communications system)
- เป็นไปตามมาตรฐานสากลในการแบ่งปันข้อมูล (In compliance with international standards)
- ดำเนินการแบ่งปันข้อมูลอย่างถูกกฎหมาย (Legally founded)
- มีคุณสมบัติด้านความปลอดภัย (Embedded with security features)
- มีคุณสมบัติในความยืดหยุ่นและสามารถปรับแต่งได้ (Flexible and can be customized)

ทุกฐานข้อมูลของ INTERPOL ยกเว้นฐานข้อมูล "Child sexual exploitation images" จะปฏิบัติงานผ่านระบบแดชบอร์ดแบบ 24 ชั่วโมงตลอด 7 วัน²⁹⁹ (The I-24/7 Dashboard) และฐานข้อมูลทั้งหมดจะปฏิบัติงานในลักษณะที่จำกัดผู้เข้าถึง (Restricted-access Internet portal) ปัจจุบัน INTERPOL ได้ขยายการเข้าถึงฐานข้อมูลมิใช่เฉพาะแต่ สำนักงานกลางแห่งชาติ (National Central Bureaus) เท่านั้นแต่ยังรวมถึง เจ้าหน้าที่บังคับใช้กฎหมายแนวหน้า (Frontline law enforcement officers) อาทิ เจ้าหน้าที่รักษาชายแดนในประเทศสมาชิก (Border guards in member countries) ให้เข้าถึงการแบ่งปันข้อมูลเกี่ยวกับบุคคลที่เป็นที่ต้องการ (Wanted persons) เอกสารการเดินทางที่ถูกขโมย และยานยนต์ที่ถูกขโมย โดยการขยายการเข้าถึงนี้จะช่วยให้หน่วยงานที่เกี่ยวข้องสามารถที่จะแบ่งปันข้อมูลเฉพาะในการดำเนินการกิจที่ได้จากฐานข้อมูล INTERPOL ต่อฐานข้อมูลในระดับชาติ (National databases) อย่างมีประสิทธิภาพและทันเวลา (Timely)

²⁹⁹ “ระบบแดชบอร์ด (Dashboard) หมายถึง หน้ากระดานที่ใช้ในการสรุปข้อมูลแบบ Executive ในมุมมองที่ดูง่าย รวมถึงระบบที่ช่วยสรุปผลการดำเนินงานที่มีการบันทึกข้อมูลทั้งหมด” ที่มา: *Davov.tech*

ตาราง : ประเภทฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ

ฐานข้อมูล	รายละเอียด
Nominal Data	ฐานข้อมูลที่มีข้อมูลมากกว่า 225,346 รายการ เกี่ยวกับข้อมูลอาชญากรรมระหว่างประเทศ (International criminals) ข้อมูลผู้สูญหาย (Missing persons) ข้อมูลศพของบุคคลพร้อมกับประวัติอาชญากรรมของบุคคล (Their criminal histories) ภาพถ่าย (Photographs) และลายนิ้วมือ (Fingerprints)
DNA Profiles	มีข้อมูลโปรไฟล์ DNA ประมาณ 226,000 รายการ จาก 87 ประเทศ โปรไฟล์ดีเอ็นเอเป็นชุดเครื่องหมายทางพันธุกรรมที่มีรหัสตัวเลขเฉพาะสำหรับแต่ละบุคคล และสามารถใช้เพื่อช่วยแก้ปัญหาอาชญากรรมและระบุตัวผู้สูญหายและศพที่ไม่ปรากฏหลักฐาน
Fingerprints	INTERPOL จัดการระบบข้อมูลการระบุลายนิ้วมืออัตโนมัติซึ่งมีลายนิ้วมือมากกว่า 220,000 ชุด และเครื่องหมายที่เกิดเหตุ (Crime scene marks) มากกว่า 17,000 รายการที่ส่งโดยประเทศสมาชิกไม่ว่าจะทางอิเล็กทรอนิกส์หรือทางไปรษณีย์
Child sexual exploitation images	“ไม่เปิดรายละเอียดของข้อมูลสู่สาธารณะ” แต่ฐานข้อมูลนี้สามารถระบุเหยื่อได้ 21,458 ราย และผู้กระทำความผิด 9,698 รายโดยใช้ฐานข้อมูลรูปภาพ INTERPOL International Child Sexual Exploitation (ICSE)
Stolen and Lost Travel Documents	เก็บข้อมูลเอกสารการเดินทางมากกว่า 89 ล้านฉบับที่รายงานว่าสูญหายหรือถูกขโมยใน 179 ประเทศ ฐานข้อมูลนี้ช่วยให้ สำนักงานกลางแห่งชาติ (National Central Bureaus - INTERPOL NCBs) และหน่วยงานที่ได้รับอนุญาตอื่น ๆ เช่นเจ้าหน้าที่ตรวจคนเข้าเมืองและเจ้าหน้าที่ควบคุมชายแดนสามารถตรวจสอบความถูกต้องของเอกสารการเดินทางที่ต้องสงสัยได้ในไม่กี่วินาที
Stolen Administrative Documents	ข้อมูลเกี่ยวกับเอกสารทางการเกือบ 1.6 ล้านฉบับที่ใช้ระบุวัตถุสิ่งของ ตัวอย่างเช่นเอกสารการจดทะเบียนรถและใบอนุญาตการนำเข้า / ส่งออก
Stolen Motor Vehicles	ข้อมูลรายละเอียดเกี่ยวกับยานพาหนะประมาณ 7.4 ล้านคันที่ถูก รายงานว่าถูกขโมยไปทั่วโลก ในปี 2019 มีการระบุยานพาหนะที่ถูก

ฐานข้อมูล	รายละเอียด
	ขโมยได้เกือบ 210,000 ชิ้นโดยใช้ฐานข้อมูลนี้
Stolen Works of Art	อนุญาตให้ประเทศสมาชิกค้นคว้าบันทึกผลงานศิลปะ และมรดกทางวัฒนธรรมราว 52,000 ชิ้นที่รายงานว่าถูกขโมยโดย 134 ประเทศที่เข้าร่วม
Foreign Terrorist Fighters	ฐานข้อมูลเชิงวิเคราะห์ที่สร้างขึ้นในเดือนสิงหาคม 2015 โดยมีผู้ต้องสงสัยว่าเป็นนักรบต่างชาติ (FTFs) มากกว่า 53,000 คน ข้อมูลที่กำหนดได้รับการจัดเตรียมโดย 77 ประเทศ
Firearms	INTERPOL Illicit Arms Records and Tracing Management System (iARMS) ³⁰⁰ เป็นแพลตฟอร์มส่วนกลางสำหรับการรายงานการสืบค้นและการติดตามอาวุธปืนที่สูญหาย ถูกขโมย ถูกค้าหรือลักลอบนำเข้า โดยหน่วยงานบังคับใช้กฎหมายทั่วโลกซึ่งมีบันทึกมากกว่า 1.4 ล้านรายการที่อัปโหลดโดย 87 ประเทศ

ที่มาของข้อมูลในตาราง³⁰¹



³⁰⁰ Cited: [Interpol.int/en/Crimes/Firearms-trafficking](https://www.interpol.int/en/Crimes/Firearms-trafficking)

³⁰¹ INTERPOL, "Fact sheet of INTERPOL's Databases" (2020), Available from https://www.interpol.int/en/content/download/15012/file/GI-04_Databases_Factsheets_EN_2020-03.pdf

3.5 การแบ่งปันข้อมูลต่อการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงเพื่อใช้ในการก่อการร้าย

ในทศวรรษที่ผ่านมาตัวกระทำที่ไม่ใช่รัฐ (Non-state actors) อย่างขบวนการก่อการร้ายต่างๆ ได้เข้ามามีบทบาทต่อความมั่นคงของสังคมระหว่างประเทศมากขึ้น กลุ่มการก่อการร้ายและกลุ่มสนับสนุนการก่อการร้าย ได้พยายามหาช่องทางในการเข้าถึงซึ่งการใช้อาวุธที่มีอานุภาพทำลายล้างสูง (Weapons of Mass Destruction - WMDs) กล่าวคืออาวุธที่มีวัสดุประกอบทางเคมี ชีวภาพ รังสี และนิวเคลียร์ (Chemical, Biological, Radiological and Nuclear materials - CBRN) ซึ่งวัสดุเหล่านี้หากตกไปอยู่ในมือของขบวนการก่อการร้ายแล้วนั้นจะถือเป็นภัยคุกคามอย่างร้ายแรงต่อสันติภาพและความมั่นคงระหว่างประเทศ (Serious threat to international peace and security)³⁰²

ในช่วงหลายปีที่ผ่านมาขบวนการก่อการร้ายได้พัฒนาวิธีการปฏิบัติและวิธีการใหม่ๆ ในการจัดหา และใช้ อาวุธอันตรายเหล่านี้มากขึ้น เพื่อเพิ่มความเสียหายของการก่อเหตุการก่อการร้าย และกระตุ้นให้ความรู้สึกร่วมของเหล่าประชาชนที่เป็นเป้าหมายเกิดความหวาดกลัวมากขึ้นและด้วยความก้าวหน้าทางเทคโนโลยีได้เปิดโอกาสให้มีการขยายช่องทางการค้าของอาวุธอานุภาพทำลายล้างสูง และวัสดุประกอบอาวุธทั้งอย่างที่ถูกกฎหมายและผิดกฎหมาย รวมถึงการใช้ประโยชน์จากอินเทอร์เน็ตอย่างเว็บมืด และสื่อโซเชียลมีเดียทำให้อาวุธเหล่านี้บางส่วนสามารถเข้าถึงได้ง่ายมากขึ้น

3.5.1 พันธกรณีตามข้อมติของคณะมนตรีความมั่นคง

ข้อมติที่ 1540/2004 ตัดสินให้บรรดารัฐต่างๆ (Decides that all States) ดำเนินมาตรการป้องกัน การแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ตลอดจนดำเนินการควบคุมการจัดส่ง วัสดุประกอบอาวุธ โดยเฉพาะการดำเนินการของตัวกระทำที่ไม่ใช่รัฐ (Non-state actors) ทั้งนี้ข้อมติที่ 1540/2004³⁰³ ได้ขยายเป้าหมายของมาตรการป้องกันการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงต่อขบวนการก่อการร้ายที่มีความพยายามจะจัดหา พัฒนา ใช้ และค้า ซึ่งอาวุธที่มีอานุภาพทำลายล้างสูง ตลอดจนการจัดส่ง วัสดุประกอบอาวุธที่มีอานุภาพทำลายล้างสูง มาตรการป้องกันดังกล่าวจะต้องบังคับกับบุคคลที่มีรายชื่อตามที่คณะกรรมการเกี่ยวกับมาตรการลงโทษ ได้ระบุไว้โดยอาศัยอำนาจตามข้อมติที่ 1267/1999 และข้อมติที่ 1989/2011 ทั้งนี้ให้ขยายไปถึงขบวนการก่อการร้าย ผู้ก่อการร้าย นักรบต่างชาติ และบุคคลที่มีเหตุอันควรเชื่อว่าเกี่ยวข้องกับการก่อการร้ายที่อยู่ภายใต้การ

³⁰² Office of Counter-Terrorism UN Counter-Terrorism Centre (UNCCT), "Access to weapons of mass destruction", Chemical biological, radiological and nuclear terrorism (2020), Retrieved from <https://www.un.org/counterterrorism/cct/chemical-biological-radiological-and-nuclear-terrorism>

³⁰³ United Nations Security Council Resolution 1540/2004, preamble

บังคับของการดำเนินมาตรการต่อต้านการก่อการร้ายของข้อมติที่ 1373/2001 และข้อมติอื่นที่เกี่ยวข้อง

ดังที่ได้กล่าวข้างต้นมาจะเห็นได้ว่าคณะมนตรีความมั่นคงได้รับรอง ถึงความเป็นไปได้ที่แน่นอนชัดว่าการก่อการร้ายระหว่างประเทศ นั้นมีความสัมพันธ์กับการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง³⁰⁴ อาทิ การค้าอาวุธผิดกฎหมาย การเคลื่อนย้ายอย่างผิดกฎหมายของ วัสดุประกอบอาวุธนิวเคลียร์ เคมี ชีวภาพ และวัสดุอื่นที่เป็นอันตรายถึงแก่ชีวิต รัฐต่างๆมีความจำเป็นที่จะต้องดำเนินมาตรการป้องกันการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ตามข้อมติที่ 1540/2004 ไปพร้อมกับมาตรการต่อต้านการก่อการร้ายตามข้อมติที่ 1373/2001³⁰⁵ ดังที่ระบุไว้ที่วรรคสี่ตอนท้ายว่า คณะมนตรีความมั่นคงได้เน้นย้ำถึงความจำเป็นต่อบรรดารัฐในการยกระดับการประสานงาน ในระดับชาติ อนุภูมิภาค ระดับภูมิภาค และระดับนานาชาติ เพื่อเสริมสร้างการตอบโต้ระหว่างประเทศ ต่อความท้าทายและภัยคุกคามต่อความมั่นคงทั้งการก่อการร้ายและการแพร่ขยายของอาวุธอานุภาพทำลายล้างสูง

3.5.2 สารบัญญัติของข้อมูล

คณะกรรมการเกี่ยวกับมาตรการลงโทษ ต้องการให้รัฐแบ่งข้อมูลในการตรากฎหมายเพื่อการปราบปรามการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูงทุกแง่มุมตามข้อมติ กับคณะกรรมการซึ่งข้อมูลที่จะต้องแบ่งปันมานั้น เนื้อหาใจความหลักนั้นเกี่ยวข้องกับการออกกฎหมายภายในเพื่อควบคุมอาวุธที่มีอานุภาพทำลายล้างสูงทุกประเภท วัสดุที่สำคัญในการผลิต วิธีการขนส่ง ตลอดทั้งเรื่องการควบคุมการเงินที่ไหลเวียนอยู่ในภาคธุรกิจที่ทำกิจการในส่วนตัวส่วนหนึ่งเกี่ยวข้องกับอาวุธ ซึ่งผู้เขียนจะแจกแจงสาระของข้อมูลเป็นข้อๆดังต่อไปนี้

³⁰⁴ Elizabeth Wilmshurst Gabriel H. Oosthuizen, "Terrorism and Weapons of Mass Destruction: United Nations Security Council Resolution 1540," *Chatham House international law programme* (September, 2014).

³⁰⁵ United Nations Security Council Resolution 1373/2001, pp.4

3.5.2.1 อาวุธอานุภาพทำลายล้างสูงและวัสดุเกี่ยวข้อง

- อาวุธนิวเคลียร์

ข้อมูลการดำเนินการออกกฎหมาย หรือข้อมูลการออกกฎหมายใน ต่อการควบคุมอาวุธนิวเคลียร์³⁰⁶ อาทิ การมีกฎหมายระดับชาติในการลงโทษต่อการกระทำการใช้อาวุธนิวเคลียร์ การผลิตอาวุธนิวเคลียร์ หรือการริเริ่มโครงการการผลิตอาวุธนิวเคลียร์ และการกระทำที่เป็นการเข้าครอบครองซึ่งอาวุธนิวเคลียร์ ทั้งนี้กฎหมายดังกล่าวจะต้องมีการกำหนดบทบัญญัติในการลงโทษอย่างชัดเจนทั้งทางแพ่งและอาญา

- วัสดุเกี่ยวข้องกับอาวุธนิวเคลียร์

ข้อมูลของการดำเนินการออกมาตรการทางกฎหมาย ต่อการดำเนินการสร้างความปลอดภัยแก่วัสดุนิวเคลียร์ ในกระบวนการของการผลิต การใช้ การกักเก็บวัสดุ และการขนส่ง รวมทั้งมีระเบียบข้อปฏิบัติในการจัดทำบัญชีรายการวัสดุนิวเคลียร์ ขั้นตอนการรักษาความปลอดภัยวัสดุ การป้องกันทางกายภาพของวัสดุ การขออนุญาตใช้วัสดุในทางสันติหรือพลังงาน การกำหนดเงื่อนไขของการออกใบอนุญาต³⁰⁷ อาทิ การใช้ การขนส่ง และการจัดเก็บของภาคอุตสาหกรรมที่ดำเนินกิจการโรงงานนิวเคลียร์ ทั้งนี้ระเบียบข้อบังคับดังกล่าวจะต้องกำหนดโทษอย่างชัดแจ้งในกรณีที่เกิดการฝ่าฝืนกฎหมายทั้งทางแพ่งและอาญา

- อาวุธเคมี

ข้อมูลการดำเนินการออกกฎหมาย หรือข้อมูลการออกกฎหมายในระดับชาติ ต่อการควบคุมอาวุธเคมี อาทิ การมีกฎหมายระดับชาติในการลงโทษต่อการกระทำการใช้อาวุธเคมี การผลิตอาวุธเคมี หรือการริเริ่มโครงการการผลิตอาวุธเคมี กักตุนหรือการจัดเก็บ และการกระทำที่เป็นการเข้าครอบครองซึ่งอาวุธเคมี ทั้งนี้กฎหมายดังกล่าวจะต้องมีการกำหนดบทบัญญัติในการลงโทษอย่างชัดเจนทั้งทางแพ่งและอาญา³⁰⁸

³⁰⁶ Security Council, "Letter dated 12 September 2011 from the Chair of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2011), pp. 40-42

³⁰⁷ Security Council, "Letter dated 8 July 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2008), pp. 36-41

³⁰⁸ Security Council, "Letter dated 25 April 2006 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2006), pp. 49-50

ในการอนุวัติการพันธกรณีตามข้อมติของคณะมนตรีความมั่นคง รัฐส่วนใหญ่ใช้วิธีการแก้ไขเพิ่มเติมกฎหมายที่ว่าด้วยการต่อต้านการก่อการร้ายเพื่อให้มีบทลงโทษสำหรับความผิดเหล่านี้ด้วย

- วัสดุเกี่ยวข้องกับอาวุธเคมี

ข้อมูลของการดำเนินการออกมาตรการตามกรอบกฎหมาย ต่อการดำเนินการสร้างความปลอดภัยแก่วัสดุเคมี ในกระบวนการของการผลิต การใช้ การกักเก็บวัสดุ และการขนส่ง รวมทั้งมีระเบียบข้อปฏิบัติในการจัดทำบัญชีรายการวัสดุนิวเคลียร์ ขั้นตอนการรักษาความปลอดภัยวัสดุ การป้องกันทางกายภาพของวัสดุ การขออนุญาตใช้วัสดุในทางสันติหรืออุตสาหกรรม การกำหนดเงื่อนไขของการออกใบอนุญาต³⁰⁹ อาทิ การใช้ การขนส่ง และการจัดเก็บของภาคอุตสาหกรรมที่ดำเนินกิจการอุตสาหกรรมเคมี รวมทั้งข้อมูลการวางข้อกำหนดของการออกใบอนุญาตสำหรับการนำวัสดุเคมีเพื่อการสร้างสิ่งอำนวยความสะดวก หรือการอนุญาตให้บุคลากรใช้วัสดุที่เกี่ยวข้องกับอาวุธเคมี ทั้งนี้ ระเบียบข้อบังคับดังกล่าวจะต้องกำหนดโทษอย่างชัดเจนในกรณีที่เกิดการฝ่าฝืนกฎหมายทั้งทางแพ่งและอาญา

- อาวุธชีวภาพ

ข้อมูลการดำเนินการออกกฎหมาย หรือข้อมูลการออกกฎหมายในระดับชาติ ต่อการควบคุมอาวุธชีวภาพ อาทิ การมีกฎหมายระดับชาติในการลงโทษต่อการกระทำที่ใช้อาวุธชีวภาพ การผลิตอาวุธชีวภาพ หรือการริเริ่มโครงการการผลิตอาวุธชีวภาพ กักตุนหรือการจัดเก็บ และการกระทำที่เป็นการเข้าครอบครองซึ่งอาวุธชีวภาพ ทั้งนี้กฎหมายดังกล่าวจะต้องมีการกำหนดบทบัญญัติในการลงโทษ อย่างชัดเจนทั้งทางแพ่งและอาญา³¹⁰

ทั้งนี้ข้อมติคณะมนตรีความมั่นคงที่ 1540/2004 ได้ครอบคลุมถึงพันธกรณีตามอนุสัญญาห้ามอาวุธชีวภาพ (Biological and toxin weapons convention) ดังนั้นรัฐจะต้องมีกฎหมายที่เกี่ยวข้องต่อการห้ามการพัฒนา การขนส่ง การโยกย้าย ซึ่งอาวุธชีวภาพด้วย

³⁰⁹ Security Council, "Letter dated 12 September 2011 from the Chair of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2011), pp. 62-64

³¹⁰ Security Council, "Letter dated 8 July 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2008), pp. 28-29

- วัสดุเกี่ยวข้องกับอาวุธชีวภาพ

ข้อมูลของการดำเนินการออกกฎหมายและมาตรการที่ครอบคลุม (Comprehensive legislation and measures) ต่อการดำเนินการสร้างความปลอดภัยแก่วัสดุนิวเคลียร์ (Biological materials) ในกระบวนการของการผลิต การใช้ การกักเก็บวัสดุ และการขนส่ง รวมทั้งมีการกำหนดขั้นตอนการรักษาความปลอดภัยของวัสดุ การป้องกันทางกายภาพของวัสดุ (Physical protection) การขออนุญาตใช้วัสดุในทางสันติ การกำหนดเงื่อนไขของการออกใบอนุญาต อาทิ การใช้ การออกใบอนุญาตการใช้การวัสดุชีวภาพ ที่เกี่ยวข้องกับอาวุธชีวภาพตามกิจกรรมที่ได้รับอนุญาตโดยเฉพาะ³¹¹ กิจกรรมที่มีวัตถุประสงค์ทางวิชาการ (Academic) การค้า (Commercial) การแพทย์ (Medical) การอุตสาหกรรม (Industrial) หรือสาธารณสุข (Public health) กิจกรรมการวิจัยพันธุวิศวกรรมที่เกี่ยวข้องกับวัสดุชีวภาพ (Research of genetic engineering activities) ทั้งนี้ระเบียบข้อบังคับดังกล่าวจะต้องกำหนดโทษอย่างชัดเจนในกรณีที่เกิดการฝ่าฝืนกฎหมายทั้งทางแพ่งและอาญา

3.5.2.2 วิธีการขนส่งและการเงิน

รัฐจะต้องให้ข้อมูลแก่คณะกรรมการเกี่ยวกับมาตรการลงโทษ ในข้อมูลที่เกี่ยวข้องกับการออกกฎหมาย หรือมาตรการบังคับใช้กฎหมาย ในการควบคุมวิธีการของการส่งมอบ ของอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้อง ทั้งนี้จุดประสงค์สำคัญคือรัฐต้องมีข้อมูลการบังคับใช้กฎหมายเหล่านี้เพื่อที่จะห้ามตัวกระทำที่ไม่ใช่รัฐในการพัฒนา ผลิต หรือขนย้ายซึ่งอาวุธและวัสดุที่เกี่ยวข้อง

รัฐจะต้องมีข้อมูลของการดำเนินการตามกฎหมายเพื่อห้ามการจัดหาแหล่งเงินทุนสำหรับกิจกรรมการแพร่กระจายของอาวุธที่มีอำนาจทำลายล้างสูง รวมทั้งแหล่งเงินทุนที่เกี่ยวข้องต่อวิธีการของการส่งมอบ คณะกรรมการลงโทษได้เสนอข้อแนะนำว่ารัฐที่ได้อนุญาตอนุญาตที่ว่าด้วยการต่อต้านการเงินของการก่อการร้ายแล้ว ให้ดำเนินการแก้ไขเพิ่มเติมกฎหมายการต่อต้านการเงินของการก่อการร้ายโดยเพิ่มความผิดในการจัดหาแหล่งเงินทุนให้กับกิจกรรมที่ผิดกฎหมายเกี่ยวกับอาวุธนิวเคลียร์ เคมีและชีวภาพ รวมทั้งวิธีการส่งมอบ

3.5.3 มาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายที่เกี่ยวข้องกับอาวุธ

มาตรการแบ่งปันข้อมูลเพื่อการควบคุมอาวุธที่มีอำนาจทำลายล้างสูง เป็นส่วนคาบเกี่ยวจากพันธกรณีการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายจากข้อมติที่ 1373/2001 ซึ่งจะแตกต่าง

³¹¹ Security Council, "Letter dated 25 April 2006 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2006), pp. 63-68

จากข้อมติที่ 1540/2004 ที่มุ่งเน้นให้รัฐแบ่งปันข้อมูลเกี่ยวข้องกับการออกมาตรการควบคุมอาวุธต่อ คณะกรรมการลงโทษ ดังนั้นในส่วนนี้เองผู้เชี่ยวชาญจะอธิบายถึงสารบัญญัติและกระบวนการ รวมทั้ง หน้าที่และความรับผิดชอบของหน่วยงานรัฐในการปราบปรามการก่อการร้ายที่เกี่ยวข้องกับอาวุธที่มี อานุภาพทำลายล้างสูง

3.5.3.1 สารบัญญัติ

การค้าระหว่างประเทศนั้น สินค้า เทคโนโลยี หรือการบริการ ที่ใช้เพื่อการพาณิชย์ระหว่าง ประเทศบางจำพวกนั้นสามารถใช้ประโยชน์ที่เกี่ยวข้องกับอาวุธที่มีอานุภาพทำลายล้างสูง อาทิ สินค้า สองทาง³¹² (Dual-use items) ซึ่งหน่วยงานของรัฐที่หน้าที่เกี่ยวข้องต่อการค้าต่างประเทศจะต้องมี มาตรการควบคุมสินค้าสองทางเพื่อต่อต้านการแพร่ขยายของอาวุธดังกล่าว ทั้งนี้คณะกรรมการตาม ข้อมติที่ 1540/2004 ได้ระบุว่าในการดำเนินมาตรการต่อทั้งการควบคุมชายแดน และการควบคุมการ ส่งออก โดยการออกกฎหมาย ระเบียบ รวมถึงข้อบังคับต่างๆ ของรัฐนั้นอาจไม่พอเพียงและไม่มี ประสิทธิภาพต่อการดำเนินมาตรการต่อต้านการแพร่ขยายของอาวุธตามข้อมติคณะมนตรี

ดังนั้นรัฐจะต้องมีการบังคับใช้กฎหมายภายในรัฐอย่างมีประสิทธิภาพโดยจะต้องมุ่งเน้นไปที่ การบังคับใช้กฎหมายเพื่อดำเนินมาตรการดังต่อไปนี้

1. มีรายการควบคุมที่น่าเชื่อถือของสินค้าสองทาง (Credible control lists of dual-use items)
2. มีมาตรการดำเนินการและบังคับใช้กฎหมายอย่างเหมาะสม (Appropriate implementation and enforcement measure)
3. มีการฝึกอบรมเจ้าหน้าที่บังคับใช้กฎหมายอย่างมีประสิทธิภาพ (Effective training of enforcement officials)
4. มีการแบ่งปันข้อมูลระหว่างหน่วยงานของรัฐและระหว่างหน่วยงานของรัฐและภาคเอกชน (Information sharing between state authorities and between state authorities and private actors)³¹³

³¹² “สินค้าที่ใช้ได้สองทาง” หมายความว่า สินค้าที่สามารถนำไปใช้ได้ทั้งทางการพาณิชย์และการทหาร โดยการ นำไปใช้ ออกแบบ พัฒนา ผลิต ใช้ ดัดแปลง จัดเก็บ ลำเลียง หรือกระทำด้วย ประการใด ๆ เพื่อให้ได้มาซึ่งอาวุธที่มี อานุภาพทำลายล้างสูง และ “อาวุธที่มีอานุภาพทำลายล้างสูง” หมายความว่า อาวุธนิวเคลียร์ อาวุธเคมี อาวุธ ชีวภาพ และอาวุธอื่นใด ซึ่งก่อให้เกิดอันตรายต่อชีวิตมนุษย์จำนวนมากหรือต่อสิ่งแวดล้อม *ที่มา: ประกาศกระทรวง พณิชย์*

³¹³ Security Council, "Reporting and compilation of information in Letter dated 8 July 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2008), pp. 53

และทั้งนี้ในข้อมติที่ 1810/2008 คณะมนตรีความมั่นคงแห่งสหประชาชาติได้รับรองว่าในการดำเนินมาตรการต่อต้านการแพร่ขยายของอาวุธที่มีอำนาจทำลายล้างสูงของบรรดารัฐอื่นๆ จะต้องเป็นไปเพื่อการป้องกันเท่านั้น³¹⁴ และไม่ควรมุ่งดำเนินการเพื่อเป็นการขัดขวางความร่วมมือระหว่างประเทศ ในการใช้ วัสดุ เครื่องมือ และเทคโนโลยี ที่เกี่ยวข้องกับอาวุธในทางสันติ

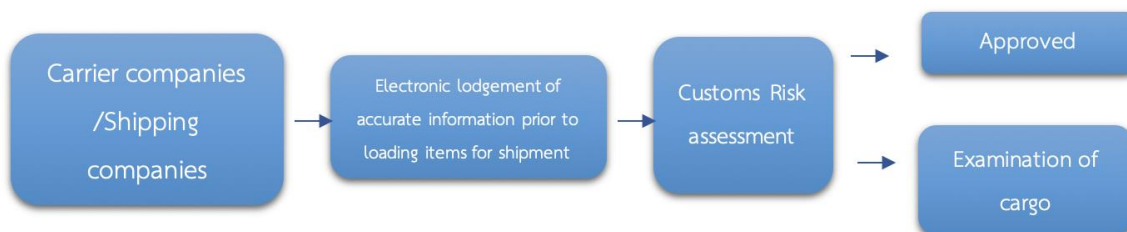
3.5.3.2 กระบวนการ

ประเด็นแรก หน่วยงานควบคุมชายแดน ของรัฐอย่าง หน่วยงานศุลกากร มีบทบาทที่สำคัญ จะต้องบรรลุซึ่งมาตรการต่อต้านการแพร่ขยายของอาวุธที่มีอำนาจทำลายล้างสูง และในขณะเดียวกันจะต้องมีมาตรการที่สกัดกั้นการเข้าถึงอาวุธของตัวกระทำการที่มีใช้ เช่น การก่อการร้าย การแบ่งปันข้อมูลในการนำเข้าสินค้า หน่วยงานศุลกากรจะต้องดำเนินการแบ่งปันข้อมูลกับผู้มีส่วนเกี่ยวข้อง ของภาคเอกชน อาทิ บริษัทผู้ให้บริการด้านการขนส่ง บริษัทผู้ให้บริการขนส่งทางเรือ ดังต่อไปนี้

1. หน่วยงานศุลกากร จะต้องสามารถเข้าถึงข้อมูลการบันทึกทางอิเล็กทรอนิกส์ก่อนการโหลดสินค้าสำหรับการจัดส่ง (Electronic lodgement of accurate information prior to loading items for shipment) จากบริษัทผู้ให้บริการด้านการขนส่ง (Carrier companies) บริษัทผู้ให้บริการขนส่งทางเรือ (Shipping companies) และนำข้อมูลจากภาคเอกชนมา ประเมินความเสี่ยงตามข้อกำหนดหรือตามประสบการณ์ของเจ้าหน้าที่ศุลกากร (Experience of customs officers)
2. หน่วยงานศุลกากร จะต้องสามารถที่จะทำการตรวจสอบสินค้าในบรรจุทุกในกรณีให้เห็นว่าปฏิบัติไปเพื่อประโยชน์ของหน่วยงานศุลกากร และจะต้องปฏิบัติโดยใช้วิธีการทางเทคโนโลยีที่ไม่รุกรานสำหรับการตรวจสอบทางกายภาพ (Non-invasive technology or physical inspection) ของสินค้าในบรรจุทุกของเอกชน
3. หน่วยงานศุลกากร จะดำเนินการตามกฎหมายหรือระเบียบข้อบังคับของการตรวจสอบสินค้าในบรรจุทุกของเอกชนโดยพื้นฐานเพื่อความจำเป็น และมี Voluntary arrangements ต่อภาคเอกชนเพื่อให้ดำเนินการตาม

³¹⁴ United Nations Security Council Resolution 1810/2008, preamble

แผนผังโครงสร้าง : ข้อมูลในกรณีการนำเข้าสินค้าในบรรทุกของเอกชน

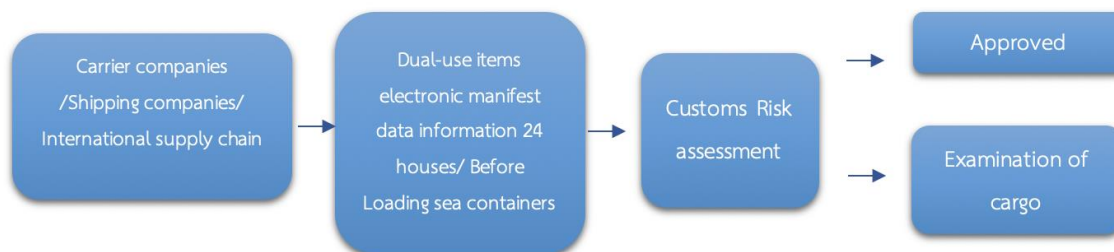


ประเด็นที่สอง ตามมาตรการต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง รัฐจะต้องมีมาตรการป้องกันมิให้ตัวกระทำการที่มีไซรัลล์ อย่าง การก่อการร้าย สามารถเข้าถึงถูกเข้าถึงสินค้าที่ใช้ได้สองทาง ที่อาจจะถูกนำไปใช้เพื่อเป็นวัสดุในการพัฒนาอาวุธที่มีอานุภาพทำลายล้างสูง เช่น อาวุธชีวภาพ อาวุธเคมี หรืออาวุธกัมมันตภาพรังสี คณะกรรมการตามข้อมติบังคับให้หน่วยงานศุลกากร ของรัฐจะต้องมีดำเนินการออกมาตรการให้³¹⁵ บริษัทผู้ให้บริการด้านการขนส่ง บริษัทผู้ให้บริการขนส่งทางเรือ หรือบริษัทที่อยู่ในห่วงโซ่อุปทานระหว่างประเทศ ให้ข้อมูลแก่หน่วยงานดังต่อไปนี้

1. บริษัทผู้ให้บริการด้านการขนส่ง บริษัทผู้ให้บริการขนส่งทางเรือ หรือบริษัทที่อยู่ในห่วงโซ่อุปทานระหว่างประเทศ จะต้องให้ข้อมูลรายการอิเล็กทรอนิกส์ ต่อหน่วยงานศุลกากรเกี่ยวกับการนำเข้าสินค้าที่ใช้ได้สองทางในบรรทุกของตนตลอด 24 ชั่วโมง หรือก่อนได้ทำการโหลดบรรทุกตู้คอนเทนเนอร์ หรือในกรณีของผู้ให้บริการขนส่งสินค้าทางอากาศ จะต้องให้ข้อมูลดังกล่าวก่อนเมื่อออกเดินทางจากประเทศต้นทาง
2. หน่วยงานศุลกากร หรือเจ้าหน้าที่ศุลกากรจะต้องมีอำนาจสามารถพิจารณาการขนส่งที่มีความเสี่ยงสูง ผ่านระบบระบุเป้าหมายอัตโนมัติ ซึ่งจะประเมินจากข้อมูลที่ได้รับมา ทั้งจะช่วยเหลือสนับสนุนการเคลื่อนย้ายสินค้าที่ได้รับการอนุมัติล่วงหน้า (Pre-approved eligible goods) ข้ามพรมแดนอย่างรวดเร็ว และเป็นมาตรการที่ลดภาระงานของการตรวจสอบสินค้าที่ปฏิบัติตามข้อกำหนด ณ จุดตรวจที่ชายแดน

³¹⁵ Security Council, "Reporting and compilation of information in Letter dated 12 September 2011 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", *the President of the Security Council* (2011), pp. 71-72

แผนผังโครงสร้าง : ข้อมูลในกรณีการนำเข้าสินค้าที่ใช้ได้สองทางในบรรทุกของเอกชน



ประเด็นที่สาม คณะกรรมการตามข้อมติได้สนับสนุนให้หน่วยงานของรัฐให้ร่วมมือกับภาคเอกชนที่ทำธุรกรรมการค้าวัสดุที่อาจพัฒนาเป็นอาวุธที่มีอานุภาพทำลายล้างสูง เพื่อสร้างความตระหนักรู้ของภาคอุตสาหกรรม (Industry awareness) ในการดำเนินมาตรการต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง³¹⁶ โดยทั้งนี้ภาคเอกชนที่ทำธุรกรรมการค้าวัสดุที่อาจพัฒนาเป็นอาวุธที่มีอานุภาพทำลายล้างสูงมีความสำคัญต่อการแบ่งปันข้อมูลที่เป็นข่าวกรองต่อหน่วยงานของรัฐเกี่ยวกับข้อมูลของลูกค้าของอุตสาหกรรมหรือที่เรียกกันว่า กระบวนการการรู้จักลูกค้าที่สามารถระบุตัวตน (Know Your Customer - KYC)³¹⁷ หรือข้อมูลที่เป็นที่สงสัยของพฤติกรรมในการทำธุรกรรมจัดซื้อในอุตสาหกรรม (Suspicious procurement behaviour) ทั้งนี้รัฐเองควรรหาช่องทางในการทำความเข้าใจกับภาคเอกชน และหาตัวแทนภาคเอกชน (Industry representatives) ให้การแจ้งเตือนหน่วยงานที่บังคับใช้กฎหมายของรัฐ³¹⁸ ถึงข้อมูลที่พิสูจน์ได้ว่าเป็นข้อมูลที่มีความสำคัญ ต่อมาตรการควบคุมชายแดนและการส่งออกที่มีประสิทธิภาพเพื่อต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

³¹⁶ Security Council, "Reporting and compilation of information in Letter dated 8 July 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2008), pp. 75-76

³¹⁷ กระบวนการการรู้จักลูกค้าที่สามารถระบุตัวตน (Know Your Customer - KYC) หมายถึง กระบวนการการรู้จักลูกค้าที่สามารถระบุตัวตน (Identification) และพิสูจน์ตัวตน (Verification) ได้อย่างถูกต้อง เช่น ในการทำธุรกรรมต่างๆ ลูกค้าจะต้องเปิดเผยข้อมูล และผ่านการตรวจสอบข้อเท็จจริงในข้อมูลของลูกค้า (Customer Due Diligence - CDD) เพื่อเป็นการยืนยันและป้องกันความเสี่ยงที่จะเกิดขึ้นจากการโจรกรรม การก่อการร้าย *ที่มา: กรุงเทพธุรกิจออนไลน์* (<https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2562/ThaiPDF/25620191.pdf>)

³¹⁸ Security Council, "Reporting and compilation of information in Letter dated 12 September 2011 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2011), pp. 89-92

3.5.4 กระบวนการในการแบ่งปันข้อมูลต่อคณะกรรมการลงโทษ

การแบ่งปันข้อมูลต่อการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงตามตามข้อเรียกร้องของคณะมนตรีความมั่นคงตั้งแต่มีการรับรองข้อมติที่ 1540/2004 เป็นต้นมานั้น ทำให้บรรดารัฐมีพันธกรณีจะต้องให้ข้อมูลของการดำเนินการ (Implement) ตามข้อมติดังกล่าวต่อคณะกรรมการตามข้อมติที่ 1540 (1540 Committee - Security Council Committee established pursuant to resolution 1540) โดยทั้งนี้จะแบ่งลักษณะของการให้ข้อมูลของรัฐต่อคณะกรรมการแบ่งออกเป็น 2 ด้านหลัก³¹⁹ คือ

1. ข้อมูลของการปฏิบัติตามในการออกกฎหมาย (Legislative compliance) ของรัฐ
2. ข้อมูลของการปฏิบัติตามในการบังคับใช้กฎหมาย (Enforcement compliance) ของรัฐ

สาเหตุที่จะต้องแยกข้อมูลออกเป็น 2 ชุดดังกล่าวนี้เพื่อความสะดวกของคณะกรรมการตามข้อมติที่ 1540 ในการนำไปเป็นตัวชี้วัดถึงการปฏิบัติตามมาตรการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ของรัฐ หรือที่เรียกว่า “The 1540 Matrix” ซึ่งจะได้อธิบายในประเด็นถัดไป แม้ว่าบางรัฐจะได้มีการดำเนินการตามข้อมติที่ 1540/2004 ในการออกกฎหมาย เพื่อสร้างกลไกภายในรัฐตนในการต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง ก็ได้เป็นสิ่งที่ยังคงเชื่ออย่างแนบแน่นว่ารัฐนั้นจะมีการบังคับใช้กฎหมายที่เพียงพอซึ่งเป็นประสงค์หลักของคณะกรรมการที่จะต้องคอยประเมินถึงความมีประสิทธิภาพของการดำเนินการ ของรัฐจากการให้ข้อมูลที่เกี่ยวข้องอย่างรอบด้านต่อคณะกรรมการตามข้อมติที่ 1540

3.5.4.1 กระบวนการในการรายงานข้อมูล

คณะมนตรีความมั่นคงแห่งสหประชาชาติได้รับรองบรรดาข้อมติต่างๆ ที่เรียกร้องไปยังรัฐสหประชาชาติได้ส่งข้อมูลของการรายงานเกี่ยวกับการดำเนินการตามมาตรการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง อาทิ ข้อมติที่ 1540/2004 ข้อมติที่ 1673/2004 ข้อมติที่ 1810/2008 ข้อมติที่ 1977/2011 ข้อมติที่ 2055/2012 และข้อมติที่ 2325/2016 จากข้อมติทั้งหมดที่ได้กล่าวมานั้นจะพิจารณาเกี่ยวกับพันธกรณีของการแบ่งปันข้อมูลและการรายงานของรัฐต่อคณะกรรมการได้เป็นประการต่อไปนี้

ประการแรก รัฐจะต้องดำเนินการส่งข้อมูลการรายงาน หรือ ให้ข้อมูลที่เป็นปัจจุบัน (Provide up-to-date information) ที่เกี่ยวกับแผนการดำเนินงานของหน่วยงานภายในรัฐในการดำเนินการตามข้อมูลต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง

³¹⁹ Daniel Salisbury, Ian J. Stewart and Andrea Viski, "Preventing the Proliferation of WMDs - Measuring the Success of UN Security Council Resolution 1540" (2018), p. 42

ประการที่สอง ข้อมูลที่รัฐจะต้องดำเนินการส่งรายงานให้คณะกรรมการนั้นได้ถูกระบุไว้ในแบบ “The matrix” ที่จัดทำขึ้นจากคณะกรรมการตามข้อมติที่ 1540 ซึ่งในแบบตาม “The matrix” ข้อมูลจะถูกระบุไว้ตามเพื่อถามกลับมายังรัฐตามรายการต่างๆของข้อมูล และรัฐจะต้องทำการตรวจสอบและแก้ไขข้อมูลในแบบที่ได้รับมา

ประการที่สาม ในการให้ข้อมูลแต่ละประเภทตามแบบ “The matrix” ของรัฐนั้น รัฐจะต้องแน่ใจว่าข้อมูลเหล่านั้นได้มาจากรายงานระดับประเทศเป็นหลัก (Originate primarily from national reports) และจะต้องเป็นข้อมูลที่ถูกรวบรวมโดยหน่วยงานของรัฐบาลอย่างเป็นทางการ (Complemented by official Government information)³²⁰

3.5.4.2 รายการในการรายงานข้อมูล

ในแบบของ “The matrix” ที่คณะกรรมการตามข้อมติที่ 1540 ได้รับรองขึ้นมานั้น ได้ระบุชื่อรายการของการดำเนินมาตรการ (Matrices list measures for compliance) ซึ่งจะเป็นข้อมูลในระดับรัฐบาลอย่างเป็นทางการของรัฐที่จะประกอบไปด้วยสองทัศนะ คือ 1. ทัศนะด้านการปฏิบัติการในเรื่องของการออกกฎหมาย (Legislative compliance viewpoint) และ 2. ทัศนะด้านการปฏิบัติการในเรื่องของการบังคับใช้กฎหมาย (Enforce compliance viewpoint)³²¹ ดังรูปภาพต่อไปนี้

1	National legal framework			2	Enforcement: civil/criminal penalties and others		
	if YES, source document of national implementation law				if YES, source document		
N	C	B		YES			
W	W	W		N	C	B	
				W	W	W	

ตัวย่อ NW: Nuclear weapons / CW: Chemical weapons / BW: Biological weapons

อ้างอิงที่มาของรูปภาพ : The 1540 Matrix Template.PDF

ทั้งนี้ก็เป็นประโยชน์ต่อการปฏิบัติงานของคณะกรรมการตามข้อมติที่ 1540 ในการใช้ข้อมูลจาก “The matrix” เพื่อเป็นเครื่องมือที่จะอำนวยความสะดวกด้านการช่วยเหลือทางเทคนิค และเปิดทางให้คณะกรรมการสามารถทำการเจรจากับรัฐในการดำเนินการตามข้อมติคณะมนตรีความมั่นคงที่ 1540/2004 มากไปกว่านั้นในบริบทของการสังเกตการณ์การดำเนินมาตรการต่อต้านการแพร่

³²⁰ Security Council, "Reporting and compilation of information in Letter dated 8 July 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1540 (2004)", the President of the Security Council (2008), pp. 12-21

³²¹ Andrea Viski, "UNSCR 1540: Implementation trends", in Preventing the Proliferation of WMDs - Measuring the Success of UN Security Council Resolution 1540 (2018), p. 40-41

ขยายอาวุธที่มีอานุภาพทำลายล้างสูงตามข้อมตินั้น คณะกรรมการอาจได้รับคำเชิญจากรัฐให้เข้าไป การเยี่ยมชมการดำเนินการ (Visits to States at their invitation)³²² ซึ่งในปัจจุบันคณะกรรมการได้ ส่งเหล่าผู้เชี่ยวชาญที่เรียกว่า “1540 experts” เข้าทำการเยี่ยมชมรัฐเพื่อหารือเกี่ยวกับการ ดำเนินการตามมติ 1540/2004 มากกว่าแล้ว 30 กว่าประเทศ อาทิ สหรัฐอเมริกาในปี 2011, สาธารณรัฐประชาชนจีนในปี 2014, สาธารณรัฐเปรูในปี 2018 หรือประเทศคูเวตในปี 2019³²³

อย่างไรก็ตามแบบ The matrices ไม่ใช่เครื่องมือในการวัดการปฏิบัติตามพันธกรณีการไม่ แพร่ขยายอาวุธของรัฐ เพียงแต่เป็นเครื่องมือที่ช่วยอำนวยความสะดวกแก่บรรดารัฐต่างๆ ในการ ดำเนินการตามข้อมติที่ 1540/2004 ข้อมติที่ 1673/2004 ข้อมติที่ 1810/2008 ข้อมติที่ 1977/2011 ข้อมติที่ 2055/2012 และข้อมติที่ 2325/2016 ดังนั้น The matrices จะไม่ใช่ข้อมูลที่เป็น ตัวตัดสินว่ารัฐได้ปฏิบัติตามข้อเรียกร้องของข้อมติที่ 1540/2004 และข้อมติที่เกี่ยวข้องมากนักย ึ่งเพียงใด และทั้งนี้ข้อมูลที่ปรากฏอยู่ใน The matrices ก็มาจากการที่รัฐเต็มใจที่จะแบ่งปันข้อมูล ให้กับคณะกรรมการ ตามที่ได้ระบุมาในการรายงานเท่านั้นและมีได้สร้างความผูกพันของพันธกรณี ใดๆตามข้อมติที่ 1540/2004 หรือข้อมติอื่นๆที่เกี่ยวข้อง ซึ่งผู้เขียนเองมองว่าการที่คณะมนตรีความ มั่นคงได้กล่าวข้อมูลที่ปรากฏอยู่ใน The matrices มิได้สร้างพันธะผูกพันก็เพื่อที่จะโน้มน้าวให้ บรรดารัฐแบ่งปันข้อมูลเกี่ยวกับการดำเนินมาตรการต่อต้านการแพร่ขยาย ในเชิงที่เป็นไปตามความ สมัครใจของรัฐ มากกว่าในลักษณะที่เป็นเชิงบังคับที่จะต้องให้ข้อมูล

ข้อมูลในแบบ The matrix จะกล่าวถึงข้อกำหนดตามข้อมติ พร้อมกับข้อมูลของมาตรการทั้ง ในแง่ทางกฎหมาย และการบังคับใช้กฎหมาย ที่รัฐได้ดำเนินการไปแล้วตามข้อมูลที่ได้ส่งรายงานมาที่ คณะกรรมการ ซึ่งจะขออธิบายข้อกำหนดต่างๆ ดังตาราง 4 รูปแบบดังต่อไปนี้

- ตารางที่ 1 : ข้อมูลของรัฐในการเข้าร่วมเป็นภาคีของอนุสัญญาที่เกี่ยวข้องกับการต่อต้านการ แพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง
- ตารางที่ 2 : ข้อมูลของรัฐเกี่ยวกับการออกกฎหมายและการบังคับใช้กฎหมายเพื่อการ ต่อต้านการต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง
- ตารางที่ 3 : ข้อมูลของรัฐเกี่ยวมาตรการเพื่อการควบคุมภายในประเทศเพื่อป้องกันการ แพร่กระจายของอาวุธที่มีอานุภาพทำลายล้างสูง
- ตารางที่ 4 : ข้อมูลของรัฐเกี่ยวมาตรการเพื่อการควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอานุภาพทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ

³²² United Nations Security Council Resolution 2325/2016, pp.16 (Operative Paragraph)

³²³ Security Council Committee established pursuant to resolution 1540 (2004), "Dialogues and Visits to States" (2020), Available from <https://static.un.org/en/sc/1540/national-implementation/dialogues-and-visits-to-states.shtml>

ตารางที่ 1 : ข้อมูลของรัฐในการเข้าร่วมเป็นภาคีของอนุสัญญาที่เกี่ยวข้องกับการต่อต้านการแพร่ขยายของอาวุธที่มีอำนาจทำลายล้างสูง

	ข้อมูลของการยึดปฏิบัติ (Adherence) ตามตราสารที่มีผลผูกพันตามกฎหมาย, ข้อมูลของการเป็นสมาชิกขององค์การที่เกี่ยวข้องต่อต้านการแพร่ขยาย, ข้อมูลของการมีส่วนร่วมและการเตรียมการตลอดจนทั้งแฉ่งการต่างของรัฐ	ข้อมูลของรัฐที่เกี่ยวข้องอื่นๆ (เช่น การลงนาม (Signing) การภาคยานุวัติ (Accession) การให้สัตยาบัน (Ratification) และอื่นๆ)
1	สนธิสัญญาไม่แพร่ขยายอาวุธนิวเคลียร์ (Nuclear Non-Proliferation Treaty)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
2	เขตปลอดอาวุธนิวเคลียร์/พิธีสาร (Nuclear Weapons Free Zone/ Protocol(s))	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
3	อนุสัญญาระหว่างประเทศเพื่อปราบปรามการก่อการร้ายทางนิวเคลียร์ (International Convention for Suppression of Acts of Nuclear Terrorism)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
4	อนุสัญญาว่าด้วยการคุ้มครองวัสดุนิวเคลียร์ (Convention on the Physical Protection of Nuclear Material)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ

	ข้อมูลของการยึดปฏิบัติ (Adherence) ตามตราสารที่มีผลผูกพันตามกฎหมาย, ข้อมูลของการเป็นสมาชิกขององค์การที่เกี่ยวข้องต่อการต่อต้านการแพร่ขยาย, ข้อมูลของการมีส่วนร่วมและการเตรียมการตลอดจน ทั้งแถลงการณ์ต่างๆของรัฐ	ข้อมูลของรัฐที่เกี่ยวข้องอื่นๆ (เช่น การลงนาม (Signing) การภาคยานุวัติ (Accession) การให้สัตยาบัน (Ratification) และอื่นๆ)
5	การแก้ไขอนุสัญญาว่าด้วยการคุ้มครองวัสดุนิวเคลียร์ปี 2005 (Amendments to the Convention on the Physical Protection of Nuclear Materials 2005)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
6	สนธิสัญญาว่าด้วยการห้ามทดลองอาวุธนิวเคลียร์โดยสมบูรณ์ (Comprehensive Nuclear Test Ban Treaty)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
7	อนุสัญญาว่าด้วยอาวุธเคมี (Chemical Weapons Convention)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
8	อนุสัญญาห้ามอาวุธชีวภาพ (Biological Weapons Convention)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
9	พิธีสารเจนีวาปี 1925 ว่าด้วยการห้ามใช้อาวุธเคมีและชีวภาพในสงคราม (The 1925 Geneva Protocol prohibits the use of chemical and biological weapons in war)	เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ

ข้อมูลของการยึดปฏิบัติ (Adherence) ตามตราสารที่มีผลผูกพันตามกฎหมาย, ข้อมูลของการเป็นสมาชิกขององค์การที่เกี่ยวข้องต่อการต่อต้านการแพร่ขยาย, ข้อมูลของการมีส่วนร่วมและการเตรียมการตลอดจนทั้งแถลงการณ์ต่างๆของรัฐ	ข้อมูลของรัฐที่เกี่ยวข้องอื่นๆ (เช่น การลงนาม (Signing) การภาคยานุวัติ (Accession) การให้สัตยาบัน (Ratification) และอื่นๆ)
10	อนุสัญญาเพื่อการปราบปรามการใช้ระเบิดในการก่อการร้ายปี 1977 (Convention for the Suppression of Terrorist Bombing of 1977)
11	อนุสัญญาระหว่างประเทศเพื่อการปราบปรามการจัดหาเงินทุนของการก่อการร้าย (International Convention for the Suppression of the Financing of Terrorism 1999)
12	พิธีสารของอนุสัญญาเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยในการเดินเรือทางทะเล (The 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation)
13	พิธีสารเพื่อการปราบปรามการกระทำที่ไม่ชอบด้วยกฎหมายต่อความปลอดภัยของแพลตฟอร์มดิจิทัลที่ตั้งอยู่บนไหล่ทวีป (The 2005 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf)

ข้อมูลของการยึดปฏิบัติ (Adherence) ตามตราสารที่มีผลผูกพันตามกฎหมาย, ข้อมูลของการเป็นสมาชิกขององค์การที่เกี่ยวข้องต่อการต่อต้านการแพร่ขยาย, ข้อมูลของการมีส่วนร่วมและการเตรียมการตลอดจน ทั้งแถลงการณ์ต่างๆของรัฐ	ข้อมูลของรัฐที่เกี่ยวข้องอื่นๆ (เช่น การลงนาม (Signing) การภาคยานุวัติ (Accession) การให้สัตยาบัน (Ratification) และอื่นๆ)
14	อนุสัญญาว่าด้วยการปราบปรามการกระทำโดยมิชอบด้วยกฎหมายเกี่ยวกับการบินพลเรือนระหว่างประเทศ (Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation) เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
15	ตราสารที่มีผลผูกพันตามกฎหมายในภูมิภาคที่เกี่ยวข้อง (Other relevant regional legally binding instruments) เช่น ข้อมูลของการลงนาม (Signing) ข้อมูลของการภาคยานุวัติ (Accession) ข้อมูลของการให้สัตยาบัน (Ratification) หรือข้อมูลอื่นๆ
16	ทบวงการพลังงานปรมาณูระหว่างประเทศ (International Atomic Energy Agency (IAEA)) เช่น ข้อมูลของการเข้าร่วมเป็นภาคี
17	การเตรียมการของรัฐที่เกี่ยวข้องโดยตรง (Directly relevant Arrangements) เช่น ข้อมูลของการดำเนินงานภายในของรัฐ

ข้อมูลของการยึดปฏิบัติ (Adherence) ตามตราสารที่มีผลผูกพันตามกฎหมาย, ข้อมูลของการเป็นสมาชิกขององค์การที่เกี่ยวข้องต่อการต่อต้านการแพร่ขยาย, ข้อมูลของการมีส่วนร่วมและการเตรียมการตลอดจน ทั้งแถลงการณ์ต่างๆของรัฐ	ข้อมูลของรัฐที่เกี่ยวข้องอื่นๆ (เช่น การลงนาม (Signing) การภาคยานุวัติ (Accession) การให้สัตยาบัน (Ratification) และอื่นๆ)
18 คำแถลงของรัฐเกี่ยวกับการไม่จัดหาอาวุธ WMDs และวัสดุที่เกี่ยวข้องต่อผู้กระทำการที่ไม่ใช่รัฐ (Statement on non- provision of WMD and related materials to non-State actors)	เช่น ข้อมูลของการดำเนินงานภายในของรัฐ
19 การเป็นสมาชิกในองค์กรระหว่างประเทศระดับภูมิภาคหรือภูมิภาคที่เกี่ยวข้อง (Membership in relevant international, regional or sub-regional organizations)	เช่น ข้อมูลของการเข้าร่วมเป็นภาคี

ที่มาของข้อมูลในตาราง³²⁴

³²⁴ Security Council Committee established pursuant to resolution 1540 (2004), "Section I - Operative paragraph 1 and related matters from Operative paragraph 5, Operative paragraph 8 (a),(b),(c) and Operative paragraph 10 in Resolution 1540/2004 in the Approved 1540 Matrix Template" (2020), Available from <https://www.un.org/en/sc/1540/national-implementation/1540-matrices.shtml>

ตารางที่ 2 : ข้อมูลของรัฐที่เกี่ยวข้องกับการออกกฎหมายและการบังคับใช้กฎหมายเพื่อการต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง

รายชื่อกิจกรรมที่กฎหมายระดับภายในรัฐจะต้องห้ามบุคคลหรือหน่วยงานเป็นส่วนใดส่วนหนึ่งของกิจกรรมใดกิจกรรมหนึ่งต่อไปนี้จะต้องมีการบังคับใช้กฎหมาย	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในประเทศ	ข้อมูลหรือเอกสารของการบังคับใช้ในประเทศ กฎหมายที่ใช้ในประเทศ
1 การผลิตซึ่งอาวุธที่มีอานุภาพทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับใช้ทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
2 การได้มาซึ่งอาวุธที่มีอานุภาพทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับใช้ทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
3 การครอบครองซึ่งอาวุธที่มีอานุภาพทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับใช้ทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน

รายชื่อกิจกรรมที่กฎหมายระดับภายในรัฐจะต้องห้ามบุคคลหรือหน่วยงานเป็นส่วนใดส่วนหนึ่งของกิจกรรมใดกิจกรรมหนึ่งต่อไปนี้จะจะต้องมีการบังคับใช้กฎหมาย	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับใช้รัฐกฎหมาย
4 การพัฒนาซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
5 การขนส่งซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
6 การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
7 การใช้ซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้ง

รายชื่อกิจกรรมที่กฎหมายระดับภายในรัฐจะต้องห้ามบุคคลหรือหน่วยงานเป็นส่วนใดส่วนหนึ่งของกิจกรรมใดกิจกรรมหนึ่งต่อไปนี้จะต้องมีการบังคับใช้กฎหมาย	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
	ห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	ทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
8 พยายามมีส่วนร่วมในกิจกรรมหนึ่งทั้งหมดข้างต้น	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล คณะบุคคล หรือหน่วยงานในการเข้าถึงการนำเข้า การผลิต หรือการครอบครองอาวุธโดยปราศจากการได้รับใบอนุญาตจากหน่วยงานของรัฐ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
9 เข้าร่วมในฐานะผู้สมัครร่วมคิดในกิจกรรมใดกิจกรรมหนึ่งทั้งหมดข้างต้น	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล หรือหน่วยงานในการช่วยเหลือ (Aid) สนับสนุน (Abet) จัดหา (Procure) หรือให้คำปรึกษา (Counsel) เกี่ยวกับกิจกรรมต้องห้ามที่เกี่ยวข้องทั้งหมดข้างต้น	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
10 ช่วยเหลือในกิจกรรมใดกิจกรรมหนึ่งทั้งหมดข้างต้น	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล หรือหน่วยงานในการช่วยเหลือ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือ

รายชื่อกิจกรรมที่กฎหมายระดับภายในรัฐจะต้องห้ามบุคคลหรือหน่วยงานเป็นส่วนใดส่วนหนึ่งของกิจกรรมใดกิจกรรมหนึ่งต่อไปนี้จะจะต้องมีการบังคับใช้กฎหมาย	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
	(Aid) สนับสนุน (Abet) จัดหา (Procure) หรือให้คำปรึกษา (Counsel) เกี่ยวกับกิจกรรมต้องห้ามเกี่ยวข้องทั้งหมดข้างต้น	หน่วยงานได้ทำการฝ่าฝืน
11 สนับสนุนทางการเงินแก่กิจกรรมใดกิจกรรมหนึ่งทั้งหมดข้างต้น	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล หรือหน่วยงานในการช่วยเหลือ (Aid) สนับสนุน (Abet) จัดหา (Procure) หรือให้คำปรึกษา (Counsel) เกี่ยวกับกิจกรรมต้องห้ามเกี่ยวข้องทั้งหมดข้างต้น	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
12 มีส่วนต่อวิธีการจัดส่งแก่กิจกรรมใดกิจกรรมหนึ่งทั้งหมดข้างต้น	เช่น ข้อมูลของการออกกฎหมายที่เกี่ยวข้องกับการห้ามบุคคล หรือหน่วยงานในการช่วยเหลือ (Aid) สนับสนุน (Abet) จัดหา (Procure) หรือให้คำปรึกษา (Counsel) เกี่ยวกับกิจกรรมต้องห้ามเกี่ยวข้องทั้งหมดข้างต้น	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน

ที่มาของข้อมูลในตาราง³²⁵

ตารางที่ 3 : ข้อมูลของรัฐที่เกี่ยวข้องกับการควบคุมภายในประเทศเพื่อป้องกันการแพร่กระจายของอาวุธที่มีอำนาจทำลายล้างสูง

	รายชื่อมาตรการที่จะต้องมีเพื่อสร้างการควบคุมภายในประเทศเพื่อป้องกันการแพร่กระจายของอาวุธที่มีอำนาจทำลายล้างสูง รวมทั้งควบคุมวัสดุที่เกี่ยวข้องกับอาวุธ (Related materials)	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับปฏิบัติตามกฎหมายที่ใช้ในรัฐ
1	มาตรการในการพิจารณาสำหรับการผลิตซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับกฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการออกใบอนุญาตดำเนินการกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
2	มาตรการในการพิจารณาสำหรับการใช้งานซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับกฎกระทรวง (Ministerial Regulation) ที่เกี่ยวข้องกับเงื่อนไขของการออกใบอนุญาตดำเนินการกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน

³²⁵ Security Council Committee established pursuant to resolution 1540 (2004), "Section II - Operative paragraph 2 Nuclear Weapons (NW), Chemical Weapons (CW) and Biological Weapons (BW) in the Approved 1540 Matrix Template" (2020), Available from <https://www.un.org/en/sc/1540/national-implementation/1540-matrices.shtml>

รายชื่อมาตรการที่จะต้องมีเพื่อสร้างการควบคุมภายในประเทศ เพื่อป้องกันผลกระทบกระจายของอาวุธที่มีอำนาจทำลายล้างสูง รวมทั้งควบคุมวัสดุที่เกี่ยวข้องกับอาวุธ (Related materials)	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับใช้รัฐ
	ทำลายล้างสูง	
3 มาตรการในการพิจารณาการจัดเก็บซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับ กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
4 มาตรการในการพิจารณาสำหรับการขนส่งซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับ กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
5 มาตรการเพื่อการรักษาความปลอดภัยในการผลิตซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับ กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน

รายชื่อมาตรการที่จะต้องมีเพื่อสร้างการควบคุมภายในประเทศ เพื่อป้องกันผลกระทบของอาวุธที่มีอำนาจทำลายล้างสูง รวมทั้งควบคุมวัสดุที่เกี่ยวข้องกับอาวุธ (Related materials)	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมาย กฎหมายที่ใช้ในรัฐ
6 มาตรการเพื่อความปลอดภัยในการใช้งานซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับ กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการขอออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้ง ทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
7 มาตรการเพื่อการรักษาความปลอดภัยในการจัดเก็บซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับ กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการขอออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้ง ทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
8 มาตรการเพื่อความปลอดภัยในการขนส่งซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับ กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการขอออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้ง ทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
9 มาตรการเพื่อการป้องกันทางกายภาพซึ่งอาวุธที่มีอำนาจ	เช่น ข้อมูลของการออกกฎหมายในระดับ	เช่น ข้อมูลของการบังคับทางกฎหมายทั้ง

รายชื่อมาตรการที่จะต้องมีเพื่อสร้างการควบคุมภายในประเทศ เพื่อป้องกันการแพร่กระจายของอาวุธที่มีอำนาจทำลายล้างสูง รวมทั้งควบคุมวัสดุที่เกี่ยวข้องกับอาวุธ (Related materials)	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
ทำลายล้างสูง	กฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการขอออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	ทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน
10 มาตรการในการพิจารณาความน่าเชื่อถือของบุคลากรซึ่งอาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการออกกฎหมายในระดับกฎกระทรวง (Ministerial Regulation) ที่เกี่ยวกับเงื่อนไขของการขอออกใบอนุญาต ดำเนินกิจกรรมที่เกี่ยวข้องต่ออาวุธที่มีอำนาจทำลายล้างสูง	เช่น ข้อมูลของการบังคับทางกฎหมายทั้งทางแพ่งและทางอาญาในกรณีที่มีบุคคลหรือหน่วยงานได้ทำการฝ่าฝืน

ที่มาของข้อมูลในตาราง³²⁶

³²⁶ Security Council Committee established pursuant to resolution 1540 (2004), "Section III - Operative paragraph 3 (a),(b) Account for/Secure/Physically protect NW, CW and BW, including Related Materials in the Approved 1540 Matrix Template" (2020), Available from <https://www.un.org/en/sc/1540/national-implementation/1540-matrices.shtml>

ตารางที่ 4 : ข้อมูลของรัฐที่เกี่ยวข้องกับความมาตรการเพื่อการควบคุมการผ่านแดน การส่งออก การนำเข้า การเอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การเอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
1 การควบคุมชายแดนเพื่อตรวจจับ ยับยั้ง ป้องกัน และต่อต้านการค้าอาวุธที่ผิดกฎหมาย	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
2 การบังคับใช้กฎหมายเพื่อตรวจจับ ยับยั้ง ป้องกัน และต่อต้านการค้าอาวุธที่ผิดกฎหมาย	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
3 มาตรการตรวจจับการควบคุมชายแดน (Border control detection measures)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	(Security Service) เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
4 การควบคุมนายหน้า (Control of brokering)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
5 กฎหมายควบคุมการส่งออก (Export control)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบ	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมาย

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
legislation in place)	หรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	กฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
6 ข้อกำหนดและการขออนุญาต (Licensing provisions and Authority)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบ หรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
7 รายการควบคุมวัสดุอุปกรณ์และเทคโนโลยี	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบ หรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงาน	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies)

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
	ตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
8 การถ่ายโอนเทคโนโลยีที่จับต้องไม่ได้ (Intangible technology transfers)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการค้าเงินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
9 วิธีการจัดส่ง (Inclusion of means of delivery)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการ	เช่น ข้อมูลการค้าเงินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือ

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
	รักษาความปลอดภัย (Security Service)	หน่วยงานบริการรักษาความปลอดภัย (Security Service)
10 การควบคุมของผู้ใช้ปลายทาง (End-user controls)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
11 สัญญาเพื่อหลีกเลี่ยงข้อโต้แย้งเกี่ยวกับสิ่งที่ก่อให้เกิดข้อพิพาททางกฎหมาย (Catch all clause)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
12 การควบคุมการขนส่ง (Transit control)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
13 การควบคุมการขนส่งทางเรือ (Trans-shipment control)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
14 การควบคุมการส่งออกอีกครั้ง (Re-export control)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน

รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ	ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในรัฐ	ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ
	(Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	(Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
15 ควบคุมการจัดหาเงินทุนสำหรับการส่งออก / การขนส่งซึ่งจะนำไปสู่การแพร่กระจาย (Control over financing of exports/Transshipments that would contribute to proliferation)	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)
16 ควบคุมบริการที่เกี่ยวข้องกับการส่งออก / การขนส่งที่จะนำไปสู่การแพร่กระจายรวมถึงการขนส่ง (Control over services related to exports/ Transshipments that would contribute to proliferation including	เช่น ข้อมูลที่เกี่ยวข้องกับการออกกฎระเบียบหรือข้อบังคับจากหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงาน	เช่น ข้อมูลการดำเนินการบังคับตามกฎหมายของหน่วยงานควบคุมชายแดน (Border management agencies) หน่วยงานตรวจคนเข้าเมือง (Immigration) หน่วยงาน

<p>รายการที่จะมีการออกกฎหมายและมาตรการของหน่วยงานเพื่อควบคุมการผ่านแดน การส่งออก การนำเข้า การโอนซึ่งอาวุธที่มีอำนาจทำลายล้างสูงและวัสดุที่เกี่ยวข้องกับอาวุธ</p>	<p>ข้อมูลหรือเอกสารของกฎหมายที่บังคับใช้ในประเทศ</p>	<p>ข้อมูลหรือเอกสารของการบังคับตามกฎหมายที่ใช้ในรัฐ</p>
<p>transportation)</p>	<p>ศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)</p>	<p>หน่วยงานศุลกากร (Customs) หรือหน่วยงานบริการรักษาความปลอดภัย (Security Service)</p>

ที่มาของข้อมูลในตาราง³²⁷

³²⁷ Security Council Committee established pursuant to resolution 1540 (2004), "Section III - Operative paragraph 3 (c),(d) and related matters from Operative paragraph 6 Controls of NW, CW and BW, including Related Materials in the Approved 1540 Matrix Template" (2020), Available from <https://www.un.org/en/sc/1540/national-implementation/1540-matrices.shtml>

3.5.5 ความช่วยเหลือระหว่างประเทศและคำแนะนำ

การปฏิบัติตามพันธกรณีทั้งเรื่องจัดทำข้อมูลเพื่อรายงานต่อคณะกรรมการลงโทษ หรือ กระบวนการในการออกกฎหมายเพื่ออนุวัติการตามพันธกรณี คณะมนตรีความมั่นคงได้สนับสนุน แผนงานให้กับคณะกรรมการลงโทษเพื่อรวบรวมข้อมูลการสำรวจประสบการณ์ที่แบ่งปัน และ บทเรียนที่ได้เรียนรู้ ระหว่างรัฐและองค์กรระหว่างประเทศทั้งระดับภูมิภาคและอนุภูมิภาค ทั้งเสนอ ให้องค์การระหว่างประเทศที่เกี่ยวข้องต่อการปราบปรามการแพร่ขยายของอาวุธที่มีอานุภาพทำลาย ล้ำสูงได้เสนอคำแนะนำในการดำเนินการตามพันธกรณีมาเป็นตัวอย่างให้แก่รัฐในบางรัฐที่ยังไม่ได้ ดำเนินการตามพันธกรณีอย่างเพียงพอ ซึ่งอาจจะเกิดจากการขาดประสบการณ์ องค์ความรู้ในการ ออกกฎหมายรวมทั้งระเบียบข้อบังคับต่างๆ ดังนั้นข้อเสนอขององค์การระหว่างประเทศหรือภูมิภาค มีส่วนสำคัญให้การชี้แนะทางการดำเนินการตามพันธกรณีให้แก่รัฐให้ปฏิบัติตามได้อย่างมี ประสิทธิภาพ

3.5.5.1 องค์การระหว่างประเทศ

1. ทบวงการพลังงานปรมาณูระหว่างประเทศ (International Atomic Energy Agency: IAEA)

สำนักงานกฎหมายของ IAEA ได้นำเสนอเอกสารทางกฎหมายเกี่ยวกับการป้องกันและการไม่ แพร่กระจายตลอดจนคู่มือปฏิบัติของ IAEA ปี 2003 เกี่ยวกับกฎหมายนิวเคลียร์ (Handbook on Nuclear Law) คู่มือดังกล่าวประกอบด้วยแบบจำลองข้อความทางกฎหมายที่มีคำอธิบายประกอบ เกี่ยวกับการไม่แพร่ขยายอาวุธนิวเคลียร์ (Legal texts relating to nuclear non-proliferation) และบทลงโทษของการใช้หรือครอบครองวัสดุนิวเคลียร์อย่างผิดกฎหมาย (Penalization of the illicit activities) โดยตัวกระทำที่ไม่ใช่รัฐ ในปี 2010 IAEA ได้ออกหนังสือ "Handbook on Nuclear Law - Implementing Legislation"³²⁸ เล่มที่สองซึ่งเน้นการร่างกฎหมาย ซึ่งเป็นครั้งแรก ในการเสนอรูปแบบตัวอย่างของบทบัญญัติที่ครอบคลุมทุกแง่มุมของกฎหมายนิวเคลียร์

³²⁸ International Atomic Energy Agency, "Handbook on Nuclear Law" (2010), Available from https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1456_web.pdf

2. องค์การห้ามอาวุธเคมี (Organisation for the Prohibition of Chemical Weapons) ฝ่ายกฎหมายได้จัดทำ “กฎหมายแม่บทแบบจำลอง (Model decree)”³²⁹ เพื่อจัดตั้งหน่วยงานระดับชาติสำหรับการดำเนินการตามอนุสัญญาอาวุธเคมีในรูปแบบบทบัญญัติประมวลกฎหมาย และชุดปฏิบัติตามกฎหมายระดับชาติ (National legislation implementation kit) ที่มาพร้อมกับข้อความและคำอธิบายที่ละเอียด ด้วยความร่วมมือกับสถาบันเพื่อการฝึกอบรมและการวิจัยแห่งสหประชาชาติ (UNITAR) OPCW และองค์การแห่งรัฐแคริบเบียนตะวันออก (OECS) ได้พัฒนาแบบแผนการดำเนินการเพื่อรวมการควบคุมด้านความปลอดภัยของสารเคมีและยาฆ่าแมลงและสิ่งแวดล้อมเข้ากับข้อกำหนดของอนุสัญญาอาวุธเคมี

3. สำนักงานกิจการลดอาวุธแห่งสหประชาชาติ (United Nations Office for Disarmament Affairs: UNODA)

ในการประชุมทบทวนครั้งที่หกที่รัฐภาคีของอนุสัญญาอาวุธชีวภาพ ได้ตัดสินใจเกี่ยวกับมาตรการที่เฉพาะเจาะจงและเป็นรูปธรรมเพื่อเสริมสร้างการปฏิบัติตามอนุสัญญารวมถึงการสร้างหน่วยสนับสนุนการดำเนินการ (Implementation support unit) มีหน้าที่เก็บรักษา ดำเนินมาตรการเสริมสร้างความเชื่อมั่นในรูปแบบอิเล็กทรอนิกส์ในภาษาราชการทั้งหมดและทำให้พร้อมใช้งานบนเว็บไซต์ (www.unog.ch/bwc)

Implementation

The Geneva Branch of the United Nations Office for Disarmament Affairs (UNODA) is the implementing agency for the current Council Decision, which aims to support implementation of the BWC on the international, regional and national levels through six major projects:

1. Promoting universal adherence to the BWC
2. Capacity building in support of BWC implementation
3. Fostering biosecurity networks in the Global South
4. Supporting the inter-sessional programme and preparations for the Ninth BWC Review Conference
5. Strengthening preparedness of States Parties to prevent and respond to attacks involving biological agents
6. Enabling tools for awareness-raising, education and engagement

ซึ่งฐานข้อมูลในเว็บไซต์นี้ประกอบด้วยเครื่องมือออนไลน์จำนวนมากและฐานข้อมูลที่มีรายละเอียดของมาตรการระดับชาติที่อาจเกี่ยวข้องกับอนุสัญญานี้รวมถึงบทสรุปของมาตรการและ

³²⁹ Organisation for the Prohibition of Chemical Weapons, "Model decree on the establishment of a National Authorities", (2010), Available from <https://www.opcw.org/documents/model-decree-establishment-national-authority>

ลิงก์ไปยังเนื้อหาทั้งหมดของมาตรการหากเป็นไปได้ นอกจากนี้หน่วยงานระหว่างประเทศอื่น ๆ อีกหลายแห่งได้จัดทำคู่มือหรือเอกสารที่คล้ายคลึงกันที่เกี่ยวข้องกับอนุสัญญานี้ อาทิ สำนักงานเพื่อการลดอาวุธแห่งสหประชาชาติได้จัดทำคู่มือการมีส่วนร่วมในมาตรการเสริมสร้างความเชื่อมั่นของอนุสัญญาอาวุธชีวภาพ "Guide to Participating in the Confidence- Building Measures of the Biological Weapons Convention (December 2009)"

4. คณะกรรมการกาชาดระหว่างประเทศและองค์การตำรวจอาชญากรรมระหว่างประเทศ

คณะกรรมการกาชาดระหว่างประเทศได้ร่างกฎหมายต้นแบบ (Model law) คือ "พระราชบัญญัติการก่ออาชญากรรมทางชีวภาพและอาวุธสารพิษ"³³⁰ สำหรับรัฐในการนำไปใช้เป็นตัวอย่างหรือต้นแบบของการปฏิบัติตามพันธกรณี

ส่วนในปี 2010 INTERPOL ได้ตีพิมพ์คู่มืออ้างอิงฉบับที่สองคือ "Bioterrorism Incident Pre-Planning and Response Guide"³³¹ เพื่อใช้ในการป้องกันการก่อการร้ายทางชีวภาพ และการเตรียมความพร้อมรวมถึงการออกกฎหมายการรักษาความปลอดภัยตัวแทนความปลอดภัยทางชีวภาพและความปลอดภัยทางชีวภาพ INTERPOL กำลังพัฒนารฐานข้อมูล Bioincident ซึ่งจะมีข้อมูลเกี่ยวกับอุปกรณ์ตรวจจับและสารชีวภาพหรือสารพิษที่ถูกขโมยหรือหายไปและสามารถเข้าถึงได้ผ่านระบบสื่อสาร I-24/7

5. สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ

สำนักงานสหประชาชาติว่าด้วยยาเสพติด ได้จัดทำคู่มือนิติบัญญัติด้านกฎหมายเกี่ยวกับอนุสัญญาต่อต้านการก่อการร้ายสากลและพิธีสาร เสนอคำอธิบายและรูปแบบของกฎหมายที่มีคำอธิบายประกอบเพื่อดำเนินการตามอนุสัญญาต่อต้านการก่อการร้ายทั้งหมด นอกจากนี้สำนักงานยังได้เผยแพร่ "Guide for Legislative Incorporation of the Provisions of the Universal Legal Instruments against Terrorism"³³² และได้ร่างกรอบกฎหมายที่เกิดขึ้นใหม่สำหรับการต่อต้านการ

³³⁰ International Committee of the Red Cross, "Model law: the Biological and Toxin Weapons Crimes Act" (2005), Available from <https://international-review.icrc.org/articles/model-law-biological-and-toxin-weapons-crimes-act>

³³¹ INTERPOL, "Bioterrorism Incident Pre-Planning and Response Guide" (2020), Available from <https://www.interpol.int/en/Crimes/Terrorism/Bioterrorism>

³³² United Nations Office on Drugs and Crime, "Guide for Legislative Incorporation of the Provisions of the Universal Legal Instruments against Terrorism" (2008), Available from https://www.unodc.org/documents/terrorism/Publications/Legislative_Guide_Universal_Legal_Regi_me/English.pdf

ก่อนการร้ายทางนิวเคลียร์ นอกจากนี้ยังขอแนะนำอื่นที่ถูกเพิ่มในฐานข้อมูล (www.unodc.org/tldb) และกฎหมายที่เกี่ยวข้อง

6. คณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Financial Action Task Force : FATF)

Financial Action Task Force (FATF) ได้จัดรวบรวมรวมข้อแนะนำในเรื่องการจัดการจัดหาเงินทุนเพื่อการแพร่กระจายอาวุธในเอกสาร "FATF Recommendations" และนอกจากนี้ FATF ยังได้เผยแพร่รายงานการจัดการจัดหาเงินทุนเพื่อการแพร่กระจาย (Proliferation Financing Report)³³³ ซึ่งจะเป็นการศึกษาเกี่ยวกับวิธีการและเทคนิคที่ใช้ในการจัดหาเงินทุนในการขยายจำนวนรวมถึงตัวอย่างกรณีเฉพาะและมาตรการที่ประเทศต่างๆดำเนินการเพื่อต่อสู้กับกิจกรรมนี้ นอกจากนี้ยังเกี่ยวข้องกับภาระผูกพันในการจัดหาเงินทุนและบริการสำหรับการค้ามนุษย์ที่ผิดกฎหมาย

3.5.5.2 องค์การส่วนภูมิภาค

1. Organization for Security and Co-operation in Europe

ได้จัดทำคู่มือแนวปฏิบัติที่ดีสำหรับการดำเนินการตามข้อมติ 1540/2004 (Best practices guide for implementing resolution 1540) ซึ่งรัฐต่างๆในภูมิภาคได้ส่งรายงานและแบ่งปันประสบการณ์ของการดำเนินการตามข้อมติ ซึ่งประโยชน์ต่อรัฐที่กำลังดำเนินการตามให้สามารถมีแบบตัวอย่างเพื่อการศึกษาจะนำไปประยุกต์ใช้ในการดำเนินการปฏิบัติ³³⁴

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

³³³ The Financial Action Task Force, "Typologies Report on Proliferation Financing" (2008), Available from

<https://www.fatfgafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf>

³³⁴ Organization for Security and Co-operation in Europe, "BEST PRACTICE GUIDE ON UN SECURITY COUNCIL RESOLUTION (UNSCR) 1540" (2009), Available from

<https://www.osce.org/files/f/documents/d/0/41446.pdf>

3.6 ตารางสรุปมาตรการการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ

การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ชนิด/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อดีที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
การแบ่งปันข้อมูลต่อมาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรม				
<p>ความร่วมมือระหว่าง กระบวนการยุติธรรม</p>	<p>ข้อดีที่ 1373/2001 ข้อดีที่ 2178/2014 ข้อดีที่ 2322/2016 ข้อดีที่ 2396/2017</p>	<p>รัฐสมาชิกจะต้องมีการร่วมมือในการแบ่งปันข้อมูลและ พยานหลักฐานที่เกี่ยวข้องกับคดีการก่อการร้ายผ่านความ ร่วมมือระหว่างประเทศที่ระดับพหุภาคี ทวิภาคี ภูมิภาค หรืออนุภูมิภาค โดยกระบวนการของการแบ่งปันข้อมูลมี ขั้นตอนว่ารัฐจะต้องอาศัยความตกลงที่ว่าด้วยความ ช่วยเหลือซึ่งกันและกัน (Mutual legal assistance agreement) โดยจะต้องกำหนดให้มีหน่วยงานซึ่งจะทำ หน้าที่เป็นคนกลางในกระบวนการแบ่งปันข้อมูลและ พยานหลักฐาน (Central Authority) แต่ทั้งนี้การกำหนด กระบวนการภายในก็ขึ้นอยู่กับรัฐว่าจะกำหนดให้หน่วยงานใดมี หน้าที่ดังกล่าว เช่น อัยการ หรือ หน่วยสืบสวนสอบสวน</p>	<p>1. หน่วยงานกลาง (Central Authority) ของ รัฐสมาชิก 2. หน่วยงานบังคับใช้ กฎหมาย 3. หน่วยงานอัยการ</p>	<p>1. Addendum to the 2015 Madrid Guiding Principles ซึ่งใน Guiding Principle 14</p>


การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ชื่อมติ/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อมติที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
การแบ่งปันข้อมูลเพื่อป้องกันการเข้าถึงแหล่งการเงินของการก่อการร้าย				
ข้อมูลเพื่อการอารยทรัพย์สิน ของกลุ่มก่อการร้าย	ข้อมติที่ 1267/1999 ข้อมติที่ 1989/2011	รัฐสมาชิกแห่งสหประชาชาติมีพันธกรณีที่จะต้องจัดหา (Supply) ซึ่งข้อมูลที่จำเป็นต่อการปราบปรามกลุ่มก่อการร้ายให้แก่คณะกรรมการลงโทษกลุ่มก่อการร้ายอัลไคเดะ (Al-Qaida Sanctions Committee) เพื่อเป็นเหตุผลให้ การดำเนินการกำหนดรายชื่อ (Reasons for listing) การ ทบทวนรายชื่อบุคคลหรือกลุ่มบุคคล (Reviewing) และ การเพิกถอนรายชื่อบุคคลหรือกลุ่มบุคคล (Delisting)	1. หน่วยงานในการป้องกัน และปราบปรามการฟอก เงินและการต่อต้านการ สนับสนุนเงินแก่การก่อการ ร้าย 2. คณะกรรมการลงโทษ กลุ่มก่อการร้ายอัลไคเดะ	1. มาตรฐานสากลที่ ครอบคลุมซึ่งรวมอยู่ใน คำแนะนำสี่สิบข้อของ Financial Action Task Force เกี่ยวกับการฟอกเงิน และ FATF Nine ข้อเสนอแนะพิเศษเกี่ยวกับ การจัดหาเงินทุนของ ผู้ก่อการร้าย 2. ข้อมติที่ 2368/2017
ข้อมูลเพื่อการปราบปราม กิจกรรมการมีส่วนร่วมทางการเงิน กับการก่อการร้าย	ข้อมติที่ 1373/2001 ข้อมติที่ 2170/2014 ข้อมติที่ 2199/2015	รัฐถูกกำหนดให้มีการดำเนินการแบ่งปันข้อมูลเพื่อ ต่อไปได้และป้องกันกิจกรรมการมีส่วนร่วมทางการเงิน การก่อการร้าย (Financial engagement to terrorism) ทั้งระดับภายในและระหว่าง ประเทศ อาทิ การบริการกระเป๋าสเงินดิจิทัล การ บริการสินทรัพย์เสมือน การระดมทุนผ่านระบบ	1. หน่วยงานในการป้องกัน และปราบปรามการฟอก เงินและการต่อต้านการ สนับสนุนเงินแก่การก่อการ ร้าย 2. หน่วยข่าวกรองทาง	1. ข้อมติที่ 1267/1999 2. ข้อมติที่ 1373/2001 3. Guidance for a risk-based approach virtual assets and virtual asset service providers

การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ข้อคดี/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อคดีที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
	<p>CHULALONGKORN UNIVERSITY</p>	<p>อินเทอร์เน็ต โดยในกระบวนการของการแบ่งปันข้อมูล รัฐจะกำหนดหน่วยงานสำคัญหลักอยู่สองหน่วยงานคือ หน่วยข่าวกรองทางการเงิน (Financial intelligence unit) มีอำนาจหน้าที่ในการแบ่งปันข้อมูลกับผู้มีส่วนเกี่ยวข้องทั้งภาครัฐ เอกชนผู้ให้บริการทำธุรกรรมการเงิน และสถาบันการเงิน ที่อยู่ในประเทศไทยและต่างประเทศ โดยหน่วยงานป้องกันและปราบปรามการฟอกเงิน (Anti-Money Laundering Regulator) มีหน้าที่รับข้อมูลที่จะได้จากการวิเคราะห์แล้วจากหน่วยข่าวกรองทางการเงินเพื่อการดำเนินการสอบสวนและบังคับใช้กฎหมาย เช่น ยึด आयทรัพย์สิน ระบุบัญชี</p>	<p>การเงิน (Financial intelligence units) 3. ผู้ให้บริการโทรคมนาคม (Telecommunication service providers) 4. ผู้ให้บริการกระเป๋าเงินดิจิทัล (Digital wallet providers) 5. สถาบันทางการเงิน 6. หน่วยธุรกิจและผู้ประกอบอาชีพที่มีใช้สถาบันการเงิน 7. ผู้ให้บริการสินทรัพย์เสมือน</p>	<p>4. Standards of Financial Action Task Force: Fundraising through social media – FATF 5. Global recommendation in preventing the financing of foreign terrorist fighters</p>

การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ข้อคดี/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อคดีที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
การแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย				
ข้อมูลในการควบคุมชายแดน ให้ได้มีประสิทธิภาพ (Effective border controls)	ข้อคดีที่ 2178/2014 ข้อคดีที่ 2322/2016 ข้อคดีที่ 2396/2017	รัฐสมาชิกจะต้องหาช่องทางทางการสื่อสารเพื่อทำการแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องทั้งหมด เช่น สำนักงานตรวจคนเข้าเมือง (Immigration) กรมศุลกากร (Customs) สำนักงานความมั่นคงชายแดน (Border security) หรือหน่วยงานบังคับใช้กฎหมาย (Law enforcement) รัฐสมาชิกจะต้องแก้ไขจุดบกพร่องของการแบ่งปันข้อมูลระหว่างหน่วยงานภายในของรัฐตน เพราะถือว่าเป็นอุปสรรคต่อการดำเนินมาตรการควบคุมชายแดนให้ได้มีประสิทธิภาพ และจะต้องมีการแบ่งปันข้อมูลที่เกี่ยวข้องเกือบทุกด้านของข้อมูลผู้โดยสาร ข้อมูลสินค้า รวมไปถึงข้อมูลที่ใช้ในการสืบสวนสอบสวน ข้อมูลการวิเคราะห์ความเสี่ยงของเจ้าหน้าที่หน่วยลาดตระเวน และข้อมูลของการมีส่วนร่วมในการปฏิบัติการข้ามพรมแดนพิเศษ (Special cross-border operational engagement information) ทั้งหมดนี้จะต้องมีการดำเนินการที่	1. สำนักงานตรวจคนเข้าเมือง (Immigration) 2. กรมศุลกากร (Customs) 3. สำนักงานความมั่นคงชายแดน (Border security) 4. หน่วยงานบังคับใช้กฎหมาย (Law enforcement) 5. ศูนย์ความร่วมมือชายแดน (Border Cooperation Centres)	1. ข้อคดีที่ 1373/2001 2. Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of Foreign Terrorist Fighters

การแบ่งปันข้อมูลใน มาตรการการต่อต้านการก่อ การร้าย	ข้อมติ/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อมติที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
		ทันเวลาที่ (Timely) และแม่นยำ (Accurate) เพื่อ ประโยชน์ต่อการทำงานของหน่วยงานอื่นที่ต้องการเข้าถึง ข้อมูล ณ เวลานั้น		
การตรวจบุคคลที่เดินทางเข้า ประเทศด้วยข้อมูลผู้โดยสาร ล่วงหน้า ข้อมูลการบันทึกของ ผู้โดยสาร และข้อมูลลักษณะ เฉพาะตัวบุคคล	ข้อมติที่ 2178/2014 ข้อมติที่ 2309/2016 ข้อมติที่ 2396/2017	รัฐสมาชิกสหประชาชาติจะต้องกำหนดช่องทาง แบ่งปันข้อมูล อาทิ ข้อมูลผู้โดยสารล่วงหน้า ข้อมูล การบันทึกของผู้โดยสาร และข้อมูลลักษณะ เฉพาะตัวของนักท่องเที่ยว ระหว่างหน่วยงาน ควบคุมชายแดน (Border Authorities) กับบริษัท สายการบิน (Airline) ภายในประเทศ โดยมี กระบวนการของการแบ่งปันข้อมูลอยู่สองระดับคือ ระดับภายในประเทศ จะต้องมีการแบ่งปันข้อมูล ข้อมูลผู้โดยสารล่วงหน้า ข้อมูลการบันทึกของ ผู้โดยสาร และข้อมูลลักษณะเฉพาะตัวของ นักท่องเที่ยว ระหว่างหน่วยงานควบคุมชายแดน ของรัฐกับบริษัทสายการบินที่บริการภายในประเทศ เพื่อตรวจจับการเดินทางขาเข้าประเทศ ขาออก	1. บริษัทสายการบิน (Air carriers) 2. สำนักงานตรวจคนเข้า เมือง (Immigration) 3. กรมศุลกากร (Customs) 4. สำนักงานความมั่นคง ชายแดน (Border security) 5. หน่วยงานบังคับใช้ กฎหมาย (Law enforcement) 6. ศูนย์ความร่วมมือ ชายแดน (BCCs)	1. ข้อมติที่ 1373/2001 2. ข้อมติที่ 2322/2016 3. Guiding principle 19 ของ Madrid Guiding Principles 4. Annex 9 to the Convention on International Civil Aviation

การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ข้อมติ/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อมติที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
	ข้อมติ/ปี	<p>ประเทศไทย รวมถึงการเปลี่ยนแปลงที่สนามบินของ ผู้ก่อการร้าย และระดับระหว่างประเทศ หน่วยงาน ควบคุมชายแดนของรัฐจะต้องแบ่งปันข้อมูล ผู้โดยสารล่วงหน้า และข้อมูลการบินที่กักของ ผู้โดยสารผ่านการประสานงานเพื่อจัดการชายแดน ระหว่างประเทศ (International coordinated border management) ไปยังหน่วยงานควบคุม ชายแดนของประเทศที่เป็นปลายทางหรือประเทศที่ เป็นจุดเปลี่ยนผ่านของเที่ยวบินนั้นๆ</p>		
ข้อมูลบุคคลที่อยู่ในรายชื่อเฝ้า ระวังและฐานข้อมูล (Watch lists and database)	ข้อมติที่ 2396/2017	<p>บรรดารัฐสมาชิกสหประชาชาติจะต้องพัฒนา “Watch lists and database” เพื่อตรวจจับผู้ก่อการร้ายที่ทราบ และอยู่ในรายชื่อ ผู้ต้องสงสัยที่เกี่ยวข้องต่อก่อการร้าย รวมทั้งนักรบต่างชาติ นักบต่างชาติที่จะเดินทางไปร่วมฝึก รบหรือกลับคืนสู่ประเทศต้นทาง รวมทั้งการคัดกรองบุคคล ที่เดินทาง ประเมินความเสี่ยงของบุคคลที่เกี่ยวข้องต่อการ ก่อการร้าย รวมทั้งการดำเนินการสืบสวนสอบสวนบุคคล</p>	<ol style="list-style-type: none"> 1. หน่วยงานบังคับใช้ กฎหมาย (Law enforcement) 2. หน่วยงานมั่นคง ชายแดน (Border security) 3. ศุลกากร (Customs) 	<ol style="list-style-type: none"> 1. ข้อมติที่ 1373/2001 2. ข้อมติที่ 2178/2014 3. ข้อมติที่ 2309/2016 4. “Annex to the letter dated 28 December 2018 from the Chair of the Security Council

การแบ่งปันข้อมูลใน มาตกรรมการต่อต้านการก่อ การร้าย	ข้อมติ/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อมติที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
		<p>โดยทั้งนี้การดำเนินการดังกล่าวของรัฐสมาชิกจะต้องเป็นไปตามกฎหมายภายในและเคารพต่อพันธกรณีระหว่างประเทศที่ว่าด้วยสิทธิมนุษยชน</p> 	<p>4. ทหาร (Military) 5. หน่วยข่าวกรอง (Intelligence agency) 6. INTERPOL</p>	<p>Committee” Guiding Principle ที่ 2 ว่าด้วยเรื่อง การพัฒนาระบบ Watch lists and database การต่อต้านการก่อการร้ายแบบบูรณาการ (Integrated counter terrorism)</p>
การแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้าย				
<p>การแบ่งปันข้อมูลผ่าน ฐานข้อมูลขององค์การตำรวจ อาชญากรรมระหว่างประเทศ</p>	<p>ข้อมติที่ 1373/2001 ข้อมติที่ 2178/2014 ข้อมติที่ 2309/2016</p>	<p>รัฐสมาชิกถูกกำหนดให้จะต้องเชื่อมต่อดูฐานข้อมูลกลางขององค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL Databases) เพื่อทำการแบ่งปันข้อมูลอันเป็นประโยชน์แก่การบังคับใช้กฎหมายแบบเรียลไทม์ต่อการดำเนินการเพื่อต่อต้านการก่อการร้าย โดยรัฐจะต้องกำหนดสำนักงานกลางแห่งชาติที่เรียกว่า “National</p>	<p>1. หน่วยงานบังคับใช้กฎหมายของรัฐ 2. สำนักงานกลางแห่งชาติ (National Central Bureaus) 3. INTERPOL</p>	

การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ข้อมติ/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อมติที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
		<p>Central Bureau” ซึ่งจะต้องมีหน้าที่หลักคือเป็น ศูนย์กลางรวบรวมข้อมูลและแบ่งปันข้อมูล และยัง มีหน้าที่เป็นจุดประสานงาน กับ INTERPOL และ หน่วยงานบังคับใช้กฎหมายภายในประเทศในการ ดำเนินมาตรการบังคับใช้กฎหมาย อาทิ จับกุม บุคคลในหมาย หรือดำเนินการทางกฎหมายอื่นๆ</p>		
การแบ่งปันข้อมูลต่อการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงเพื่อใช้ในการก่อการร้าย				
<p>การให้ข้อมูลการดำเนินการ ตามข้อมติต่อคณะกรรมการ ตามข้อมติที่ 1540</p>	<p>ข้อมติที่ 1540/2004 ข้อมติที่ 1673/2004 ข้อมติที่ 1810/2008 ข้อมติที่ 1977/2011 ข้อมติที่ 2055/2012 ข้อมติที่ 2325/2016</p>	<p>ข้อมติกำหนดให้บรรดารัฐต่างๆ ดำเนินมาตรการ ป้องกันการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้าง สูง (WMDs) ตลอดจนดำเนินการควบคุมการ จัดส่ง วัสดุประกอบอาวุธ จากตัวกระทำการที่มีไซ่ รัฐโดยกระบวนการของการแบ่งปันข้อมูลคือ รัฐ จะต้องกำหนดจุดติดต่อแห่งชาติที่จะต้องรวบรวม ข้อมูลจากหน่วยงานระดับชาติทั้งหมด เพื่อแบ่งปัน ข้อมูลแก่คณะกรรมการลงโทษตามรายการที่</p>	<p>1. หน่วยงานที่เกี่ยวข้องใน การดำเนินมาตรการของรัฐ สมาชิก 2. หน่วยงานควบคุมการ นำเข้าหรือส่งออกสินค้า 3. หน่วยงานควบคุม ขยายแดน (Border control) 4. หน่วยงานศุลกากร (Customs) 5. บริษัทผู้ให้บริการด้าน</p>	<p>ข้อมติที่ 1373/2001</p>

การแบ่งปันข้อมูลใน มาตรการต่อต้านการก่อ การร้าย	ข้อมติ/ปี	สาระสำคัญของการแบ่งปันข้อมูล	ผู้มีส่วนเกี่ยวข้อง (Stakeholders) อาทิ หน่วยงานของรัฐ ภาคเอกชน	ข้อมติที่เกี่ยวข้องหรือ เอกสารอื่นที่เกี่ยวข้อง
	<p>CHULALONGKORN UNIVERSITY</p>	<p>ปรากฏใน The Matrix ซึ่งประกอบด้วยข้อมูลทั้ง 4 ประการคือ ข้อมูลของรัฐในการเข้าร่วมเป็นภาคีของอนุสัญญาต่อต้านการแพร่ขยายอาวุธอานุภาพทำลายล้างสูง ข้อมูลของรัฐในการออกกฎหมายและบังคับใช้กฎหมายการต่อต้านการแพร่ขยายอาวุธอานุภาพทำลายล้างสูง ข้อมูลของรัฐในการดำเนินมาตรการควบคุมภายในเพื่อการต่อต้านการแพร่ขยายอาวุธอานุภาพทำลายล้างสูง ข้อมูลของรัฐในการดำเนินการประเมินมาตรการควบคุมการผ่านแดนการส่งออก การนำเข้า การโอนไปซึ่งอาวุธและวัสดุที่เกี่ยวข้องกับอาวุธอานุภาพทำลายล้างสูง</p>	<p>การขนส่ง (Carrier companies) 6. บริษัทผู้ให้บริการขนส่งทางเรือ (Shipping companies) 7. คณะกรรมการตามข้อมติที่ 1540</p>	

สรุปท้ายบท

เมื่อได้ทำการศึกษาถึงมาตรการการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงมาแล้วในบทนี้จะสามารถสรุปได้ว่า การแบ่งปันข้อมูลถือเป็นกลไกหนึ่งในการขับเคลื่อนการดำเนินมาตรการต่อต้านการก่อการร้ายในแขนงต่างๆ อันได้แก่ มาตรการความร่วมมือด้านกระบวนการยุติธรรม มาตรการปราบปรามแหล่งการเงิน มาตรการควบคุมการเดินทาง มาตรการบังคับตามกฎหมาย และมาตรการต่อต้านการแพร่ขยายของอาวุธที่มีอานุภาพทำลายล้างสูง ซึ่งข้อพิจารณาของผู้เขียนมาจาก 2 ประเด็น คือ

ประเด็นแรก รูปแบบ (Form) ของมาตรการการแบ่งปันข้อมูล จากการพิจารณาการแบ่งปันข้อมูลในมาตรการต่อต้านการก่อการร้ายต่างๆ ที่ได้ทำการศึกษามาได้บ่งชี้ จะพบว่าไม่ได้มีความแตกต่างกันมากนักในหลายกรณี โดยทั่วไปแล้วตัวรูปแบบของมาตรการการแบ่งปันข้อมูลมีลักษณะของการให้รัฐสมาชิกกำหนดช่องทางความร่วมมือ (Cooperations) หรือช่องทางการประสานงาน (Coordination) ทั้งในระดับระหว่างประเทศ และภายในประเทศ กำหนดให้มีการออกกฎหมาย (Legislation) ที่ให้อำนาจชัดเจนทั้งในรูปแบบกฎหมายสารบัญญัติและกระบวนการกำหนดให้มีการมอบหมายหน่วยงานให้อำนาจหน้าที่ (Competent authorities) ในการดำเนินการแบ่งปันข้อมูลกับผู้มีส่วนเกี่ยวข้องต่างๆ (Stakeholders) ซึ่งสิ่งเหล่านี้ได้สะท้อนให้เห็นว่าตัวรูปแบบ (Form) ของการแบ่งปันข้อมูลนั้นได้แสดงให้เห็นภาพของ “โครงสร้างของมาตรการแบ่งปันข้อมูล” ซึ่งเป็นโครงสร้างของมาตรการการแบ่งปันข้อมูลที่มีลักษณะทั่วไปและสามารถพบได้ในอนุสัญญาหรือความร่วมมือระหว่างประเทศต่างๆ และเมื่อโครงสร้างของมาตรการแบ่งปันข้อมูลถูกนำไปจับกับเนื้อหา (Content) ของมาตรการต่อต้านการก่อการร้ายแขนงต่างๆ โครงสร้างนั้นก็จะเป็นกลไกในการขับเคลื่อนมาตรการเหล่านั้น

ประเด็นที่สอง เนื้อหา (Content) ของมาตรการแบ่งปันข้อมูลอันหมายถึงด้านสารบัญญัติและด้านกระบวนการนั้นมีความแตกต่างกันไปตามแต่ว่าการแบ่งปันข้อมูลนั้นจะได้ถูกนำไปจับกับมาตรการต่อต้านการก่อการร้ายในเรื่องใด ดังเช่น ในมาตรการความร่วมมือด้านกระบวนการยุติธรรม สารบัญญัติของข้อมูลจะเป็นข้อมูลที่สามารถนำไปเป็นพยานหลักฐาน หรือพยานในรูปแบบดิจิทัลที่ใช้ในการดำเนินกระบวนการยุติธรรม กระบวนการของการแบ่งปันข้อมูลจะมีหน่วยงานกลาง (Central authority) เป็นหน่วยงานที่จะทำหน้าที่คอยช่วยเหลือ ในมาตรการปราบปรามแหล่งการเงินจะมีกระบวนการแบ่งปันข้อมูลที่แตกต่างกันคือหน่วยข่าวกรองทางการเงินจะทำหน้าที่แบ่งปันข้อมูล และส่งให้หน่วยป้องกันและปราบปรามการฟอกเงินทำหน้าที่บังคับใช้กฎหมายและดำเนินการสืบสวนสอบสวน ในมาตรการควบคุมการเดินทาง สารบัญญัติของข้อมูลคือข้อมูลที่ครอบคลุมเกี่ยวข้องกับตัวผู้โดยสาร ซึ่งกระบวนการแบ่งปันข้อมูลจะมีบริษัทสายการบินเป็นภาคเอกชนที่เข้ามาเกี่ยวข้องด้วย ตัวอย่างเหล่านี้แสดงให้เห็นว่าตัวเนื้อหา (Content) ของมาตรการแบ่งปันข้อมูลจะเปลี่ยนแปลงไปตาม

การทำหน้าที่เป็นกลไกในมาตรการต่อต้านการก่อการร้ายในเรื่องนั้นๆ นั้นเองซึ่งสอดคล้องกับแนวคิดที่ว่า การแบ่งปันข้อมูลจะเกิดผลสัมฤทธิ์ในการปราบปรามการก่อการร้ายได้ ก็ต่อเมื่อการแบ่งปันข้อมูลนั้นเป็นหนทางหนึ่งที่น่าไปสู่การ "ลงมือดำเนินการ" (Take action) ซึ่งสะท้อนในอยู่ในรูปของมาตรการต่อต้านการก่อการร้ายต่างๆ ที่ได้กล่าวมาในบทนี้

ทั้งนี้จากข้อสรุปในบทนี้จึงนำไปสู่การวิเคราะห์ในบทถัดไปถึงปัญหาและผลกระทบของการดำเนินมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ ทั้งในแง่ของปัญหาด้านกระบวนการทางกฎหมายและการบังคับใช้กฎหมายในการดำเนินการของรัฐสมาชิก ตลอดจนทั้งผลกระทบที่เกิดขึ้นกับภาคธุรกิจและผลกระทบต่อผู้มีส่วนเกี่ยวข้องที่เป็นเจ้าของข้อมูล



บทที่ 4

ปัญหาและช่องทางของการดำเนินมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของ คณะมนตรีความมั่นคงแห่งสหประชาชาติ

จากบทที่ผ่านมาผู้เขียนได้อธิบายถึงโครงสร้างของมาตรการแบ่งปันข้อมูลว่ารัฐสมาชิกสหประชาชาติมีพันธกรณี สารบัญญัติ และกระบวนการของการดำเนินมาตรการแบ่งปันข้อมูลอย่างไร ซึ่งการแบ่งปันข้อมูลนั้นเป็นกลไกที่สำคัญเพื่อเข้าไปเสริมการดำเนินมาตรการต่อต้านการก่อการร้ายในด้านอื่นๆ ของคณะมนตรีความมั่นคงให้มีประสิทธิภาพยิ่งขึ้น อาทิ มาตรการความร่วมมือในกระบวนการยุติธรรม มาตรการยับยั้งการเข้าถึงแหล่งการเงิน มาตรการตรวจจับการเดินทาง มาตรการการบังคับในทางกฎหมาย มาตรการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง

ดังนั้นในบทนี้จะได้อธิบายถึงปัญหาที่เกิดขึ้นของบรรดารัฐสมาชิกสหประชาชาติที่ถูกสะท้อนมาในระหว่างการดำเนินมาตรการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย ทั้งในส่วนที่เป็นปัญหาทางด้านกระบวนการและการบังคับซึ่งกฎหมาย มากไปกว่านั้นผลกระทบของการดำเนินมาตรการแบ่งปันข้อมูลที่เกิดขึ้นต่อภาคธุรกิจ และผลกระทบต่อผู้มีส่วนเกี่ยวข้องที่เป็นเจ้าของข้อมูล

4.1 ปัญหาและแนวปฏิบัติจากการดำเนินมาตรการแบ่งปันข้อมูลของรัฐ

ในการดำเนินมาตรการแบ่งปันข้อมูลของบรรดารัฐต่างๆ หากมีปัญหาเกิดขึ้นทั้งในแง่ของกระบวนการในทางกฎหมายและการบังคับใช้กฎหมาย ประเด็นปัญหาเหล่านี้จะถูกรายงานออกมาจากรัฐและสามารถหยิบยกเป็นข้อพิจารณาให้แก่รัฐอื่นๆ ในการดำเนินมาตรการแบ่งปันข้อมูลให้ได้มีประสิทธิภาพมากยิ่งขึ้น ในทางกลับกันประสบการณ์หรือแนวทางการแก้ไขปัญหาของรัฐหนึ่งก็สามารถถูกพิจารณาเป็นคำแนะนำในการช่วยเหลือการดำเนินมาตรการแบ่งปันข้อมูลของรัฐอื่นๆ ที่ประสบปัญหาได้พบช่องทางในการแก้ไขปัญหา

4.1.1 ปัญหากระบวนการทางกฎหมาย

1. ปัญหาต่อการแบ่งปันข้อมูลในกระบวนการยุติธรรมเพื่อต่อต้านการก่อการร้าย

- ขาดการกำหนดฐานความผิดทางกฎหมายต่อการก่อการร้าย

ในการดำเนินมาตรการแบ่งปันข้อมูลต่อมาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรมหลายประเทศประสบปัญหาการขาดความสอดคล้องกันของระบอบกฎหมายภายใน อาทิ การแบ่งปันข้อมูลหรือพยานหลักฐานของผู้ที่มีความสงสัยว่าจะกระทำความผิดในฐานะก่อ

การร้าย จะไม่เกิดประสิทธิภาพต่อการไหลลื่นของข้อมูล หากฐานความผิดว่าด้วยการก่อการร้ายมิได้ ถูกกำหนดว่าผิดกฎหมายในทุกๆเขตอำนาจ³³⁵ ของประเทศภายใต้ความร่วมมือนั้น ซึ่งทุกประเทศที่อยู่ภายใต้ความร่วมมือในการปราบปรามการก่อการร้ายจะต้องตกลงกันกำหนดองค์ประกอบของฐานความผิดว่าด้วยการก่อการร้ายที่เหมือนกัน และสอดคล้องต่อหลักความผิดตามกฎหมายของทั้ง 2 ประเทศ (Principle of double criminality) เพื่อความสะดวกแก่การประสานความร่วมมือในด้านกระบวนการยุติธรรม

- ปัญหาของเขตอำนาจรัฐต่อการแบ่งปันข้อมูลพยานหลักฐานทางอิเล็กทรอนิกส์

นอกจากนี้เงื่อนไขในทางเขตอำนาจเป็นอุปสรรคต่อการแบ่งปันข้อมูล และพยานหลักฐานทางอิเล็กทรอนิกส์ ในการดำเนินกระบวนการยุติธรรมในคดีที่เกี่ยวข้องกับระบบอินเทอร์เน็ตและโซเชียลมีเดีย เนื่องจากข้อมูลที่จะสามารถนำมาเป็นพยานหลักฐานอาจจะถูกผลิตขึ้นที่ใดก็ได้ หรือภายใต้เขตอำนาจใดก็ได้ จึงเป็นข้อท้าทายของการดำเนินมาตรการแบ่งปันข้อมูลต่อมาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรมที่แต่หลายประเทศจะต้องกำหนดว่ารัฐใดจะมีเขตอำนาจในการเข้าถึงข้อมูล อาทิ รัฐที่เป็นที่จัดเก็บข้อมูล (the State in which the data are stored) รัฐเจ้าของสัญชาติของบริษัทที่ถือข้อมูล (the State of nationality of the corporation holding the data) รัฐเจ้าของสัญชาติของเจ้าของข้อมูล (the State of nationality of the data owner) รัฐที่ข้อมูลได้ถูกสร้างขึ้น (the State in which the data are created)

ซึ่งในปัจจุบันยังคงเป็นปัญหาในหลายภูมิภาคของความร่วมมือและส่งผลให้พนักงานสืบสวนสอบสวน และอัยการ อาจเข้าถึงข้อมูลและหลักฐานทางอิเล็กทรอนิกส์ได้อย่างจำกัด เนื่องจากในแต่ละรัฐอาจมีเกณฑ์ที่แตกต่างกันในการกำหนดว่ารัฐนั้นมีเขตอำนาจเหนือข้อมูล อย่างไรก็ตามมีตัวอย่างของบริษัท Facebook ที่ได้ทำ “Guidelines for Cooperation with Law Enforcement Worldwide, Preservation of Data, and Emergency Requests” เปิดช่องทางให้หน่วยงานบังคับใช้กฎหมายหรือหน่วยงานที่เกี่ยวข้องจากรัฐที่ได้รับบริการของบริษัท สามารถส่งคำร้องให้มีการแบ่งปันหรือช่วยเหลือทางข้อมูล ซึ่งจะต้องไปตามเงื่อนไขของทางบริษัท Facebook ดังที่ได้ อรรถาธิบายไปในบทที่ 3

³³⁵ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp. 18-22

2. ปัญหาต่อการแบ่งปันข้อมูลการเงินเพื่อต่อต้านการก่อการร้าย

- ขาดกฎหมายเฉพาะเอาผิดกับการเข้าถึงเงินทุนของการก่อการร้ายรูปแบบใหม่ๆ

ช่องว่างของกระบวนการทางกฎหมายของประเทศสมาชิกในการต่อต้านการจัดหาเงินทุนของการก่อการร้ายและมาตรการในการอายัดทรัพย์สินของผู้ก่อการร้าย ในบางรัฐสมาชิกไม่มีการออกกฎหมายที่เฉพาะ ใหม่ๆ เพื่อขัดขวางและป้องกันการสนับสนุนทางการเงินของการก่อการร้ายที่ปัจจุบันยิ่งทวีความต้องการที่จะฟอกเงินและสรรหาการเข้าถึงแหล่งเงินด้วยวิธีใหม่ๆ หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ของรัฐสมาชิกมีบทบาทสำคัญให้การเข้าถึงข้อมูลการเงินต่างๆของการก่อการร้ายในรูปแบบใหม่ รวมทั้งการเข้าถึงข้อมูลจากผู้มีส่วนเกี่ยวข้องใหม่ๆ อาทิ ธนาคารผู้ให้บริการด้านการเงินให้รูปแบบดิจิทัล เอกชนผู้ให้บริการโทรคมนาคม หรือผู้ให้บริการสินทรัพย์เสมือนในบางประเทศหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ได้มีการพัฒนาศักยภาพในการจัดการ ต่อการเข้าถึงแหล่งเงินของการก่อการร้ายในรูปแบบใหม่ ทั้งนี้มีข้อเสนอมากมายของคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Financial Action Task Force – FATF) รวมทั้งได้กำหนดมาตรการการปกป้องการฟอกเงินหรือการสนับสนุนเงินของการก่อการร้าย

- การขาดนโยบายกำหนดความเสี่ยงการทำธุรกรรมที่เสี่ยงต่อการก่อการร้ายของรัฐ

ในหลายรัฐสมาชิกขาดการประเมินความเสี่ยงด้านการก่อการร้ายทางการเงิน กล่าวคือ หน่วยงานของรัฐสมาชิกที่เกี่ยวข้องต่อการปราบปรามการเงินของการก่อการร้ายจะต้องมีการกำหนดแผนการเกี่ยวกับความเสี่ยงทางการเงินของการก่อการร้ายอย่างรอบด้านของภาคเศรษฐกิจ ที่คาดว่าจะมีความเสี่ยงต่อการจัดหาเงินทุนของการก่อการร้าย เช่น ธนาคาร บริษัทผู้ให้บริการการทำธุรกรรมทางการเงิน และรวมถึงภาคเศรษฐกิจที่มีความเสี่ยงที่มีใช้ภาคการเงินอื่นๆ เช่น ภาคธุรกิจการก่อสร้าง (Construction sectors) ภาคธุรกิจสินค้าโภคภัณฑ์ (Commodities sectors) ภาคธุรกิจเภสัชกรรม (Pharmaceutical sectors) เมื่อมีแผนการประเมินความเสี่ยงด้านการเงินของการก่อการร้ายแห่งชาติ³³⁶ จะส่งผลให้หน่วยงานที่มีหน้าที่ปราบปรามการเงินของการก่อการร้ายสามารถกำหนดกรอบการทำงานที่ชัดเจนว่าจะต้องมีการแบ่งปันข้อมูลการทำธุรกรรมทางการเงินของการก่อการร้ายในด้านต่างๆ จากใครบ้างและแผนการเกี่ยวกับความเสี่ยงทางการเงินของการก่อการร้ายจะต้องมีการทบทวน

³³⁶ Security Council, "Letter dated 27 December 2019 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2019), pp. 66-68

อยู่ตลอดเวลาและประเมินถึงความเสี่ยงใหม่ของการเข้าถึงแหล่งเงินของการก่อการร้ายโดยอาศัยการเก็บข้อมูลจากทุกภาคส่วน จึงจะส่งผลให้มาตรการปราบปรามการเงินของการก่อการร้ายมีประสิทธิภาพมากยิ่งขึ้น

3. ปัญหาต่อการแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย

- การขาดทรัพยากรบุคคลและองค์ความรู้ของรัฐ

ปัญหาของการดำเนินกระบวนการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า และข้อมูลการบินที่ของผู้โดยสาร ในบางรัฐสมาชิกไม่ได้มีโครงสร้างพื้นฐานในการพัฒนาระบบการแบ่งปันข้อมูล ในแง่ของทรัพยากรบุคคลและความสามารถ หน่วยงานของรัฐที่มีหน้าที่รับผิดชอบขาดซึ่งบุคลากรที่มีองค์ความรู้ความสามารถในการพัฒนาระบบการแบ่งปันข้อมูล อาทิ การใช้ การวิเคราะห์ การเก็บรักษาข้อมูล การลบ การประมวลผลข้อมูล และการแบ่งปันข้อมูล ในขงแห่งกระบวนการทางกฎหมายคือ บางรัฐสมาชิกไม่ได้กำหนดกลไกทางกฎหมายให้หน่วยงานสามารถเข้าถึงข้อมูลภาคเอกชนที่จำเป็นต่อการคัดกรองนักเดินทาง³³⁷ อาทิ บริษัทสายการบินที่อยู่ภายใต้เขตอำนาจ หรือบริษัทขนส่งสินค้าระหว่างประเทศ มากไปกว่านั้นคือบางรัฐสมาชิกเกิดปัญหาว่าภาคเอกชนเองไม่มีศักยภาพในการพัฒนาระบบการแบ่งปันข้อมูลให้แก่หน่วยงานของรัฐ ทั้งนี้คำแนะนำขององค์การการบินพลเรือนระหว่างประเทศให้มีการจัดการประชุมเชิงปฏิบัติการ³³⁸ ระหว่างหน่วยงานของรัฐสมาชิกและสมาคมภาคเอกชนสายการบิน ทั้งในระดับภายในประเทศและระดับภูมิภาค และออกคู่มือคำแนะนำรัฐสมาชิกในการดำเนินการตามมาตรการแบ่งปันข้อมูลในการตรวจจับการเดินทางของผู้ก่อการร้าย

<https://www.icao.int/Security/FAL>

³³⁷ Security Council, "Letter dated 27 December 2019 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2019), pp. 291-293

³³⁸ International Civil Aviation Organization, "Facilitation Programmes" (2021), Available from <https://www.icao.int/Security/FAL/Pages/default.aspx>

International Civil Aviation Organization, "Annex 9 - Facilitation" (2021), Available from <https://www.icao.int/Security/FAL/ANNEX9/Pages/default.aspx>

International Civil Aviation Organization, "ICAO Traveller Identification Programme (TRIP) Strategy" (2021), Available from <https://www.icao.int/Security/FAL/TRIP/Pages/default.aspx>

อ้างอิงที่มาของรูปภาพ <https://www.icao.int/Security/FAL>

- การขาดเทคนิคในการพัฒนาช่องทางการแบ่งปันข้อมูลของรัฐ

การดำเนินการมาตรการแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย กุญแจสำคัญในการกำหนดกระบวนการก็คือความเร็วของการแบ่งปันข้อมูลระหว่างหน่วยงานที่มีหน้าที่เกี่ยวข้องต่อการตรวจคนเข้าเมืองของรัฐและภาคเอกชน อาทิ สายการบินผู้ให้บริการ ในประสบการณ์ของหลายรัฐสมาชิกประสบปัญหาในกระบวนการดำเนินการแบ่งปันข้อมูลที่ล่าช้าและเป็นอุปสรรคที่สำคัญในการออกมาตรการบังคับ ซึ่งในบทเรียนของรัฐสมาชิกที่สามารถแก้ปัญหาเหล่านี้ได้นั้น กล่าวคือมีการพัฒนาระบบแจ้งเตือนที่ใช้งานได้ตลอดเวลา (Functioning round-the-clock alert system) ที่ใช้ภายในภูมิภาคเพื่อให้แน่ใจว่ามีการแบ่งข้อมูลที่ทันท่วงที่ทั้งระดับระหว่างหน่วยงานของรัฐภายในประเทศและเอกชน³³⁹ จนถึงระดับระหว่างประเทศกับหน่วยงานของรัฐต่างประเทศภายในภูมิภาค เพื่อให้เกิดการไหลเวียนของข้อมูลที่มีประสิทธิภาพและเป็นประโยชน์ต่อการออกมาตรการบังคับได้ทันท่วงที่ โดยทั้งนี้รัฐสมาชิกในภูมิภาคนั้นได้จัดตั้งฐานข้อมูลส่วนกลาง เพื่อเป็นกลไกอำนวยความสะดวกในการแลกเปลี่ยนข้อมูลและประสานข้อมูลกันระหว่างประเทศภายในภูมิภาคและระหว่างหน่วยงานบังคับใช้กฎหมายของรัฐต่างๆ รวมทั้งหน่วยงานความมั่นคง และหน่วยงานบริหารข้อสังเกตของผู้เขียนคือ ประเทศที่สามารถพัฒนาระบบมาตรการแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้ายได้อย่างมีประสิทธิภาพนั้นเป็นเพราะประเทศเหล่านั้นมีทรัพยากรในการลงทุนของภาครัฐ รวมทั้งการมีทรัพยากรทางบุคคลที่มีความรู้ความสามารถจะเข้าไปทำหน้าที่เป็นฟันเฟืองขับเคลื่อนกระบวนการเหล่านี้ ซึ่งอาจจะเป็นไปได้ยากสำหรับกลุ่มประเทศกำลังพัฒนาที่ขาด

³³⁹ ETIAS.info, "Schengen Information System: New rules to strengthen security in the EU" (2018), Retrieved from <https://www.etias.info/schengen-information-system-security-eu>

แคลนทั้งทรัพยากรการเงินและบุคคล³⁴⁰ ดังนั้นข้อท้าทายเหล่านี้จึงจะเป็นส่วนเพิ่มเติมในการพิจารณาการออกมาตรการเพิ่มเกี่ยวกับการแบ่งปันข้อมูลเพื่อยับยั้งการเดินทางของผู้ก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติต่อไป

4. ปัญหาการแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมาย

- ขาดการเชื่อมต่อฐานข้อมูลกับองค์การตำรวจอาชญากรรมระหว่างประเทศ

ปัญหากระบวนการทางกฎหมายในหลายรัฐสมาชิกคือ มีการเชื่อมต่อที่ไม่เพียงพอ และไม่ได้ใช้ประโยชน์อย่างเต็มที่จากฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศ เช่น ฐานข้อมูลเกี่ยวกับเอกสารการเดินทางที่ถูกขโมยและสูญหาย (Database on stolen and lost travel documents) ในหลายรัฐสมาชิกขาดการจัดตั้งหน่วยงานเพื่อการสื่อสารระหว่างสำนักงานกลางแห่งชาติ (INTERPOL's National Central Bureau) นำมาสู่การขาดการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานรัฐกับองค์การตำรวจอาชญากรรมระหว่างประเทศ³⁴¹ และส่งผลกระทบต่อการทำงานบังคับใช้กฎหมายของรัฐชาติซึ่งข้อมูลในการดำเนินมาตรการบังคับต่อผู้ก่อการร้าย ดังนั้นกระบวนการเหล่านี้ถือว่าเป็นโครงสร้างพื้นฐานสำคัญให้แก่มาตรการการแบ่งปันข้อมูลเพื่อการบังคับใช้กฎหมายบรรลุผลอย่างมีประสิทธิภาพ

- ขาดการกำหนดรายชื่อของบุคคลที่มีความเสี่ยงกับการก่อการร้าย

ในกระบวนการแบ่งปันข้อมูลเพื่อกำหนดบุคคลในรายชื่อเฝ้าระวังในฐานข้อมูลต่างๆ นั้น ประเทศสมาชิกจำนวนหนึ่งยังไม่ได้กำหนดรายชื่อบุคคลเฝ้าระวัง และพัฒนาฐานข้อมูลในการกำหนดรายชื่อผู้ก่อการร้ายที่รู้จักและต้องสงสัย (Known and suspected terrorist names) เป็นของตัวเอง เพื่อที่จะให้หน่วยงานการบังคับใช้กฎหมาย หน่วยงานความมั่นคงชายแดน หน่วยงานศุลกากรทหาร หน่วยข่าวกรอง ทั้งภายในประเทศของตน และหน่วยงานเหล่านี้ของต่างประเทศภายใต้ความร่วมมือได้ดำเนินมาตรการกักกรองบุคคลที่เดินทางเข้า เปลี่ยนผ่าน เติมนอกประเทศ รวมทั้งดำเนินการมาตรการประเมินความเสี่ยงและทำการสืบสวนสอบสวน ซึ่งบุคคลที่ถูกกำหนดในรายชื่อ

³⁴⁰ Security Council, "Letter dated 15 December 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp. 156

³⁴¹ Security Council, "Letter dated 12 November 2014 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2014), pp. 15

เผ่าละวัง การที่มีรัฐสมาชิกจำนวนหนึ่งไม่ได้กำหนดรายชื่อบุคคลเผ่าละวัง และพัฒนาฐานข้อมูลของในการกำหนดรายชื่อผู้ก่อการร้ายที่รู้จักและต้องสงสัยในระดับชาติของตน นำมาซึ่งการขาดประสิทธิภาพต่อการดำเนินมาตรการบังคับในการป้องกัน การระบุซึ่งตัวบุคคล และการตรวจจับผู้ก่อการร้าย ดังนั้นการมีรายชื่อเผ่าละวังและฐานข้อมูลจะช่วยให้บรรดารัฐสามารถแบ่งปันข้อมูลผ่านกลไกทวิภาคีและพหุภาคีกับหน่วยงานของรัฐต่างประเทศที่เกี่ยวข้องเพื่อดำเนินการบังคับตลอดจนทำการสืบสวนสอบสวน³⁴²

5. ปัญหาการแบ่งปันข้อมูลต่อการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง

- ขาดการจัดตั้งหน่วยงานประสานงานกลางในการรวบรวมข้อมูล

ปัญหาในกระบวนการของการรายการข้อมูลต่อคณะกรรมการตามข้อมติที่ 1540 ในแบบของ “The matrix” ที่คณะกรรมการตามข้อมติที่ 1540 ได้รับรองขึ้นมานั้น ได้ระบุชื่อรายการของการดำเนินมาตรการซึ่งจะเป็นข้อมูลในระดับชาติอย่างเป็นทางการของบรรดารัฐสมาชิกที่จะประกอบไปด้วยสองทัศนะ คือ 1. ทัศนะด้านการปฏิบัติการในเรื่องของการออกกฎหมาย (Legislative compliance viewpoint) และ 2. ทัศนะด้านการปฏิบัติการในเรื่องของการบังคับใช้กฎหมาย (Enforce compliance viewpoint) ตามรายงานของคณะกรรมการตามข้อมติได้ระบุว่าหลายรัฐสมาชิกยังมีได้กำหนดกระบวนการรวบรวมข้อมูลภายในประเทศที่ชัดเจน³⁴³ และทั้งไม่มีการจัดตั้งหน่วยงานที่มีความรับผิดชอบเฉพาะในการปราบปรามการแพร่ขยายของอาวุธ หรือเป็นจุดประสานงานกับคณะกรรมการตามข้อมติที่ 1540 ดังนั้นปัญหาที่เกิดขึ้นจากประเทศเหล่านี้คือ นำมาซึ่งการได้ข้อมูลที่ขาดประสิทธิภาพ กล่าวคือ ข้อมูลไม่มีความรอบด้าน ข้อมูลไม่มีมาจากแผนการดำเนินงานโดยตรงของหน่วยงานที่มีความรับผิดชอบภายในรัฐ เช่น ข้อมูลการควบคุมการขนส่ง นำเข้า และส่งออก ทั้งในแง่ของการออกกฎหมาย และการบังคับใช้กฎหมาย มิได้สะท้อนถึงการดำเนินการตามพันธกรณีในเรื่องการปราบปรามการแพร่ขยายของอาวุธอย่างแท้จริง³⁴⁴ จึงส่งผลกระทบต่อการใช้ข้อมูลดังกล่าวจะถูกใช้ใน

³⁴² Security Council, "Letter dated 5 February 2020 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2002) concerning counter-terrorism", the President of the Security Council (2014), pp. 15-16

³⁴³ Security Council, "Letter dated 8 July 2008 from the Chair of the Security Council Committee established pursuant to resolution 1540 (2004) concerning counter-terrorism", the President of the Security Council (2008), pp. 12-21

³⁴⁴ Peter Crail, "Report of implementing UN security council resolution 1540 and A Risk-Based Approach," *Nonproliferation Review* 13, no. 2 (July 2006), https://www.vertic.org/media/assets/nim_docs/background%20articles/Crail_risk-based%20assessment_1540.pdf

การวิเคราะห์ของคณะกรรมการตามข้อมติเพื่อประเมินถึงสภาพปัญหาของการแพร่ขยายซึ่งอาวุธที่แท้จริงในประเทศดังกล่าวว่ามีความเสี่ยงมากน้อยเพียงใด

- การขาดทรัพยากรบุคคลและองค์ความรู้ของรัฐ

ในการส่งรายงานการออกกฎหมายและการควบคุมอาวุธที่มีอำนาจทำลายล้างสูงนั้น จำเป็นอย่างยิ่งที่หน่วยงานจะต้องมีบันทึกและเก็บข้อมูลเหล่านั้นไว้ แต่ในทางปฏิบัติแล้วบางประเทศไม่มีความสามารถในการเก็บข้อมูลทั้งที่เป็นข้อมูลทางกฎหมาย และข้อมูลที่เป็นสถิติของการดำเนินมาตรการบังคับเพื่อป้องกันการแพร่ขยายของอาวุธที่มีอำนาจทำลายล้างสูง ปัญหาที่พบคือหน่วยงานของรัฐขาดซึ่งทรัพยากรบุคคลในการทำหน้าที่ดังกล่าว ข้อมูลการดำเนินมาตรการบางอย่าง เป็นความลับของรัฐที่ไม่สามารถเผยแพร่ได้เพราะเป็นข้อมูลที่เกี่ยวข้องกับผลประโยชน์ของรัฐและภาคอุตสาหกรรมภายในประเทศที่ดำเนินกิจการเกี่ยวข้องกับวัสดุที่สามารถพัฒนาเป็นอาวุธที่มีอำนาจทำลายล้างสูง รวมไปถึงจนถึงภาครัฐเองที่ขาดซึ่งองค์ความรู้ต่อการดำเนินการรวบรวมข้อมูลตามที่ถูกกำหนดไว้ในแบบฟอร์มจากคณะกรรมการลงโทษ

4.1.2 ปัญหาการบังคับใช้กฎหมาย

1. ปัญหาต่อการแบ่งปันข้อมูลในกระบวนการยุติธรรม

- ขาดการกำหนดหน่วยงานกลางอย่างชัดเจน (Central National Authority)

ความร่วมมือระหว่างประเทศในกระบวนการยุติธรรมหลายประเทศมิได้จัดตั้งหน่วยงานกลางอย่างชัดเจนซึ่งจะมีหน้าที่คอยเป็นผู้รับการประสานงานหรือให้ความร่วมมือทางข้อมูลรวมทั้งพยานหลักฐานแก่ประเทศต่างๆที่อยู่ภายใต้ความร่วมมือในการปราบปรามการก่อการร้าย รวมทั้งเป็นจุดติดต่อเพื่อการสื่อสารอย่างไม่เป็นทางการเพื่อเตรียมรับคำขอ (Focal point to initiate informal communication to prepare a request)³⁴⁵ ปัญหาที่ถูกสะท้อนมาจากประเทศที่ไม่มีหน่วยงานกลางนั้นในบางประเทศกำหนดให้มีคณะกรรมการบริหาร (Executive Committee) ที่มีเจ้าหน้าที่รัฐที่มาจากหลายๆกระทรวงทำหน้าที่เสมือนเป็นหน่วยงานกลางอย่างไม่เป็นทางการ แต่ปัญหาที่มักเกิดขึ้นคือการดำเนินงานของคณะกรรมการบริหารเป็นไปอย่างล่าช้าต่อการตอบรับหรือสนองซึ่งคำขอทางข้อมูลหรือพยานหลักฐานจากประเทศผู้เป็นคนร้องขอข้อมูลหรือพยานหลักฐาน ซึ่งเป็นคำตอบ

³⁴⁵ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 431-432

ที่ชัดเจนว่ารัฐควรจะต้องจัดตั้งหน่วยงานกลางเพื่อทำหน้าที่การประสานงานและให้ความร่วมมือต่อการปราบปรามการก่อการร้ายและเพื่อให้เกิดประสิทธิภาพอันสูงสุดต่อการดำเนินมาตรการแบ่งปันข้อมูล

- ขาดการทบทวนความตกลงที่ว่าด้วยความช่วยเหลือซึ่งกันและกัน (Mutual legal assistance agreement)

ในความตกลงที่ว่าด้วยความช่วยเหลือซึ่งกันและกันของบางพหุภาคี หรือทวิภาคีมีการกำหนดกลไกของการช่วยเหลือทางข้อมูลในรูปแบบยุคก่อนอิเล็กทรอนิกส์ (The pre-electronic era) เพื่อรับรองการแบ่งปันข้อมูลในเฉพาะรูปแบบข้อมูลกายภาพ (Physical information) อาทิ เอกสาร หนังสือรับรอง เป็นต้น แต่ในยุคปัจจุบันนั้นเป็นยุคของข้อมูลอิเล็กทรอนิกส์ (Electronic data era) ที่สามารถข้ามพรมแดนหลายประเทศผ่านทางอินเทอร์เน็ตในหน่วยมิลลิวินาที ซึ่งกลไกในความตกลงที่ว่าด้วยความช่วยเหลือซึ่งกันและกันแบบเดิมไม่ได้สอดคล้องต่อการพัฒนาทางเทคโนโลยี และเป็นอุปสรรคต่อการดำเนินมาตรการปราบปรามการก่อการร้ายให้มีประสิทธิภาพ ดังนั้นรัฐสมาชิกควรจะต้องมีการทบทวนความตกลงที่ว่าด้วยความช่วยเหลือซึ่งกันและกัน ที่ตนมีพันธกรณี และปรับเปลี่ยนข้อตกลงให้สอดคล้องกับปัจจุบัน คณะกรรมาธิการการต่อต้านการก่อการร้าย สนับสนุนให้รัฐเพิ่มขีดความสามารถในการให้ความช่วยเหลือซึ่งกันและกัน เช่น การพัฒนาศักยภาพเครือข่ายความร่วมมือที่ดำเนินการตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์³⁴⁶

2. ปัญหาต่อการแบ่งปันข้อมูลการเงินของการก่อการร้าย

- ขาดการกำหนดหน่วยข่าวกรองทางการเงิน (Financial intelligence unit)

บางรัฐสมาชิกไม่ได้จัดตั้งหน่วยงานที่เปรียบเสมือนเป็นกลไกของหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ในการเข้าถึงข้อมูลการเงินของการก่อการร้าย กล่าวคือมิได้จัดตั้งหน่วยข่าวกรองทางการเงิน (ที่สามารถเป็นตัวกลางที่มีบทบาทสำคัญในการระบุตัวผู้ก่อการร้ายและป้องกันกิจกรรมทางการเงินของพวกเขา) หน่วยข่าวกรองเป็นกลไกกลางเพื่อให้เกิดการพัฒนาความร่วมมือระหว่างภาครัฐบาลและสถาบันการเงินเอกชน เพื่อการรับรู้ข้อมูลซึ่งเกี่ยวข้องกับรายการกิจกรรมที่น่าสงสัย หน่วยข่าวกรองทางการเงินจะ

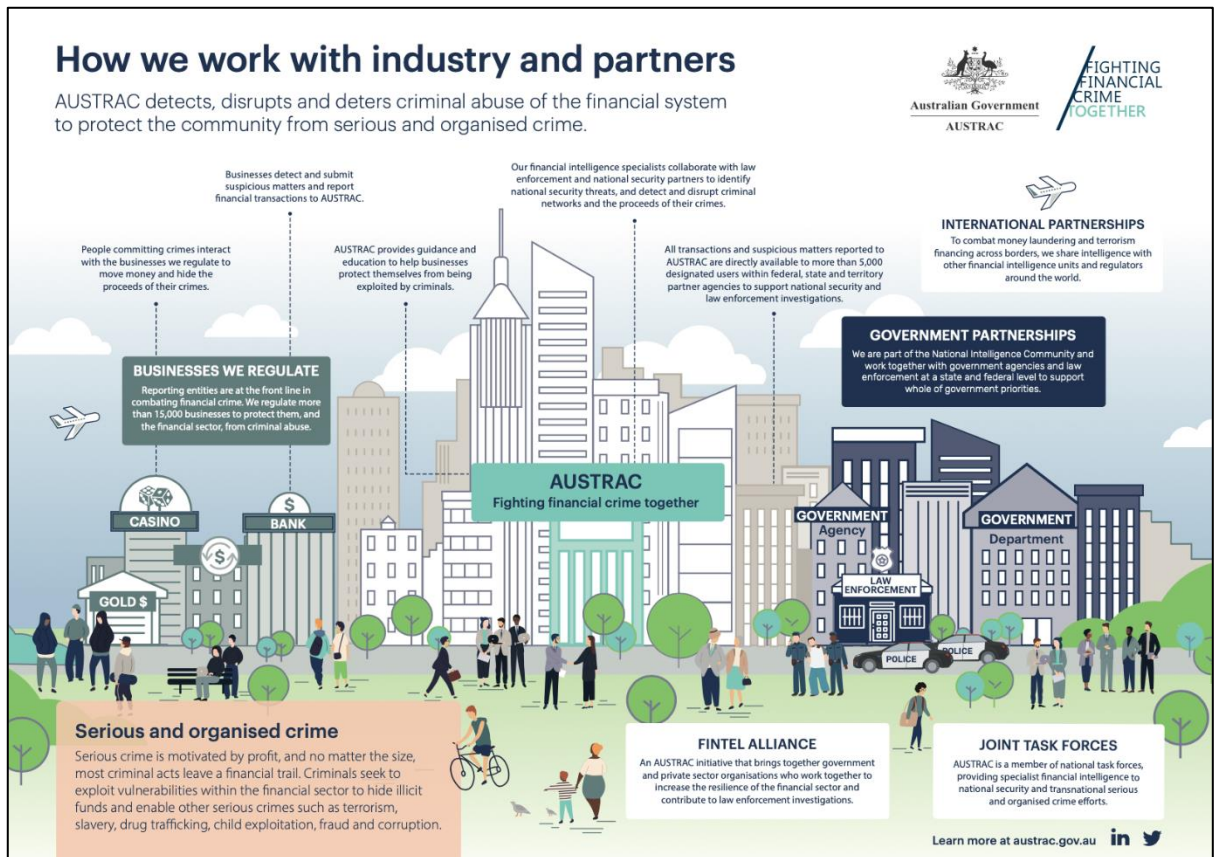
³⁴⁶ “The Committee may wish to call upon Member States to invest more effort in enhancing their capacities to provide mutual legal assistance. It may also wish to encourage States to develop and implement informal channels of communication, including the development of cooperation networks that operate 24 hours a day, 7 days a week”, Ibid, pp. 431-432

รับรู้ข้อมูลเส้นทางการเงินของผู้ก่อการร้ายผ่านสถาบันทางการเงินที่สแกนบัญชีหลายล้านบัญชีในระบบของตน รวมทั้งข้อมูลกิจกรรมการเงินอื่นผ่านบริษัทเอกชนที่ให้บริการการทำธุรกรรมทางการเงิน เพื่อรวบรวมข่าวกรองทางการเงินในการออกมาตรการบังคับ รวมทั้งเป็นที่ปรึกษาในการดำเนินมาตรการแก่สถาบันทางการเงิน และบริษัทเอกชน

- ขาดการกำหนดแผนงานบูรณาการร่วมกันระหว่างหน่วยข่าวกรองกับหน่วยบังคับใช้กฎหมาย

หน่วยงานภายในของรัฐสมาชิกไม่มีความสามารถหรือช่องทางในการประสานงานระหว่างกัน ซึ่งกระบวนการแบ่งปันข้อมูลนั้นหน่วยข่าวกรองทางการเงิน จะทำงานร่วมกับหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย ในการใช้ข้อมูลมาวิเคราะห์เพื่อดำเนินมาตรการบังคับแก่เส้นทางการเงินของผู้ก่อการร้าย แต่ในกระบวนการของบางรัฐสมาชิกยังขาดช่องทางอื่นที่จะเปิดทางในหน่วยงานทั้งสองนี้เข้าถึงข้อมูลในด้านอื่นๆ ที่อาจจะไม่มีหน้าที่เกี่ยวข้องต่อการต่อต้านการก่อการร้าย เพราะบางข้อมูลอาจจะเป็นประโยชน์แก่การออกมาตรการบังคับ เช่น การไม่มีช่องทางในการประสานทางข้อมูลกับหน่วยงานที่เกี่ยวข้องต่อการตรวจคนเข้าเมือง³⁴⁷ การไม่มีช่องทางในการเข้าถึงข้อมูลของบุคคลในเรื่องการประกันสังคม และข้อมูลรายการบันทึกภาษี เป็นต้น ดังนั้นรัฐสมาชิกจะต้องแน่นอนใจว่าได้กำหนดช่องทางแบ่งปันข้อมูลระหว่างหน่วยงานของภาครัฐต่างๆ กับหน่วยข่าวกรองทางการเงินและหน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย เพื่อเข้าถึงข้อมูลที่เกี่ยวข้องในการจัดหาเงินทุนของการก่อการร้าย หรือกำหนดแผนการว่าด้วยการต่อต้านการก่อการร้ายโดยรวม เพื่อให้ทุกหน่วยงานภายในรัฐได้รับการบูรณาการให้ความร่วมมือแก่กันและกัน ตัวอย่างของการบูรณาการในการกำหนดกำหนดแผนการว่าด้วยการต่อต้านการก่อการร้ายโดยรวม ผู้เขียนขอยกตัวอย่างแผนผังแสดงการทำงานของหน่วยงานต่างๆที่มีความรับผิดชอบต่อการปราบปรามการเงินของการก่อการร้ายของประเทศออสเตรเลีย

³⁴⁷ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 412-413



อ้างอิงที่มาของรูปภาพ https://www.austrac.gov.au/sites/default/files/2020-05/AUSTRAC%20Infographic_how%20we%20work%20with%20industry%20and%20partners_New.pdf

3. ปัญหาต่อการแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย

- ขาดประสิทธิภาพในการพัฒนาระบบการแบ่งปันข้อมูลผู้โดยสาร

ในแง่ของการบังคับใช้กฎหมายในการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า และข้อมูลการบินที่ของผู้โดยสาร ในบางรัฐยังคงมีปัญหาต่อการแบ่งปันข้อมูลที่มีอยู่ในระบบคอมพิวเตอร์แบบเต็มรูปแบบ (Fully computerized) จึงส่งผลให้หน่วยงานที่มีหน้าที่รับผิดชอบในการแบ่งปันข้อมูล อาทิ สำนักงานตรวจคนเข้าเมือง กรมศุลกากร สำนักงานความมั่นคงชายแดน หรือหน่วยงานบังคับใช้กฎหมาย และศูนย์ความร่วมมือชายแดน ไม่มีประสิทธิภาพในการแบ่งปันข้อมูลระหว่างหน่วยงานด้วยกันเอง หรือแบ่งปันข้อมูลกับภาคเอกชน เช่น บริษัทสายการบิน ทั้งนี้ยังส่งผลต่อการตรวจจับบุคคลที่อยู่ในรายชื่อเฝ้าระวัง ที่มีปรากฏอยู่ในฐานข้อมูลต่างๆทั้งของรัฐอื่น หรือขององค์การระหว่างประเทศ จึงเป็นอุปสรรคในแง่ของการใช้เวลาตรวจสอบที่มากขึ้น และหน่วยงานที่มีหน้าที่รับผิดชอบมิสามารถดำเนินมาตรการบังคับได้อย่างท่วงที เช่น ในกรณีที่มีรัฐก่อนหน้าได้รับข้อมูลผู้โดยสารล่วงหน้า

ข้อมูลการบันทึกของผู้โดยสารซึ่งเมื่อทำการตรวจสอบกับฐานข้อมูลต่างๆ ได้แสดงถึงความเสี่ยงที่น่ากังวลเกี่ยวกับการก่อการร้ายของผู้โดยสารบนเที่ยวบิน³⁴⁸ เมื่อข้อมูลถูกแบ่งปันมายังรัฐที่มีได้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพ อาจจะทำให้หน่วยงานของรัฐนั้นมิได้อยู่ในสถานะที่มีความพร้อมที่จะวิเคราะห์ข้อมูลและดำเนินมาตรการบังคับต่อผู้โดยสารบนเที่ยวบินนั้นได้อย่างมีประสิทธิภาพและทัน่วงที

จากปัญหาการบังคับใช้กฎหมายในประเด็นแรกสะท้อนว่าผู้มีส่วนได้เสีย ทั้งหน่วยงานของรัฐที่เกี่ยวข้อง กับบริษัทเอกชนไม่มีศักยภาพมากพอในการแบ่งปันข้อมูลเพื่อดำเนินมาตรการบังคับ ทั้งนี้มีข้อพิจารณาที่ถูกละเลยมาจากการดำเนินการของบรรดารัฐสมาชิกแล้วประสบปัญหาในแง่ของการบังคับใช้กฎหมายคือ หน่วยงานของรัฐสมาชิกกับบริษัทเอกชนมิได้กำหนด “การเรียงลำดับผลตอบแทน” ในการดำเนินมาตรการบังคับใช้กฎหมายที่ชัดเจน กล่าวคือ

หน่วยงานของรัฐสมาชิกกับบริษัทเอกชนจะต้องร่วมกันในการพัฒนาศักยภาพของการกำหนดความเสี่ยง และต้องมีการกำหนดมาตรการบังคับร่วมกันในการตอบโต้กับความเสี่ยงนั้น ในข้อนี้ผู้เชี่ยวชาญมีความเห็นว่าหน่วยงานของรัฐนั้นเป็นผู้กำหนดมาตรการทางกฎหมายก็จริง แต่การดำเนินการดังกล่าวเป็นไปได้หากปราศจากความร่วมมือกับภาคเอกชน ดังนั้นเอกชนจึงเป็นตัวละครที่สำคัญที่จะเสริมรัฐให้ดำเนินมาตรการอย่างมีประสิทธิภาพ จำเป็นที่จะต้องอาศัยความร่วมมือกับเอกชนในทุกๆขั้นตอนของการดำเนินการ ตั้งแต่การกำหนดความเสี่ยง การกำหนดมาตรการตอบโต้

หน่วยงานของรัฐสมาชิกที่เกี่ยวข้องกับบริษัทเอกชนต้องมีการพัฒนาความสามารถของบุคลากรผู้ที่จะดำเนินมาตรการแบ่งปันข้อมูลเพื่อได้รับรู้ถึงแนวทางในการดำเนินมาตรการบังคับร่วมกัน ซึ่งอาจจะอยู่ในรูปแบบของการอบรมเชิงปฏิบัติการ แลกเปลี่ยนการทำงาน หรือการจัดหลักสูตรการฝึกอบรมร่วมกัน³⁴⁹ การอบรมเหล่านี้จะนำไปสู่การที่บุคลากรของหน่วยงานรัฐ และเอกชนจะทำความเข้าใจและเรียนรู้ต่อการปรับปรุงทรัพยากรทางเทคโนโลยีและนวัตกรรม เพื่อดำเนินมาตรการแบ่งปันข้อมูล

³⁴⁸ Security Council, "Letter dated 18 January 2016 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2016), pp. 31,51

³⁴⁹ Security Council, "Letter dated 27 December 2019 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2019) concerning counter-terrorism", the President of the Security Council (2016), pp. 291-301

4. ปัญหาการแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมาย

- ขาดการกำหนดหน่วยต่อต้านการก่อการร้ายเฉพาะกิจ (Specialized counter-terrorism units)

ปัญหาของการบังคับใช้กฎหมายของการแบ่งปันข้อมูลคือ รัฐสมาชิกจำนวนมากมิได้จัดตั้งหน่วยต่อต้านการก่อการร้ายเฉพาะกิจ (Specialized counter-terrorism units)³⁵⁰ ที่เปรียบเสมือนกลไกของการบังคับต่อการแบ่งปันข้อมูล ไม่มีการออกกฎหมายภายในที่กำหนดโครงสร้างให้หน่วยงานบังคับใช้กฎหมายต่างๆ แบ่งปันข้อมูลเพื่อดำเนินการบังคับร่วมกัน รวมทั้งการฝึกอบรมเจ้าหน้าที่บังคับใช้กฎหมาย (Training of law enforcement officials) และการใช้ฐานข้อมูลขององค์การตำรวจอาชญากรรมระหว่างประเทศในการปรับปรุงการแจ้งเตือนและความสามารถในการตอบโต้ต่อการโจมตีของผู้ก่อการร้ายในระดับภายในประเทศ³⁵¹ ทั้งนี้บทเรียนของรัฐบาลสมาชิกในการบังคับใช้กฎหมายอีกแห่งหนึ่งคือ รัฐบาลสมาชิกจำนวนมากมิได้จัดตั้งหน่วยเฉพาะกิจก็จริง แต่ได้มีการกำหนดกลไกทางนิติบัญญัติในด้านข่าวกรองทั้งในหน่วยงานจากต่างประเทศ และภายในประเทศ ที่สำคัญคือรัฐบาลสมาชิกจำนวนมากกำลังโปรโมทการฝึกอบรมในประเด็นที่เกี่ยวข้องกับการต่อสู้กับผู้ก่อการร้าย โดยอาศัยความร่วมมือระหว่างประเทศกับรัฐต่างๆ และบางรัฐได้กำหนดช่องทางในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐในทุกระดับ ตลอดทั้งชุมชนท้องถิ่น และภาคเอกชน

4.1.3 แนวปฏิบัติทางกฎหมายของประเทศไทย

ในรายงานการต่อต้านการก่อการร้ายแต่ละประเทศ ปี ค.ศ. 2019 (Country reports on terrorism 2019) ของกระทรวงการต่างประเทศสหรัฐอเมริกา (The United States Department of State) ภาพรวมของการดำเนินมาตรการปราบปรามการก่อการร้ายของประเทศไทยถูกจัดอยู่ในระดับที่ดีขึ้น เนื่องจากประเทศไทยเองมิได้เผชิญปัญหาเกี่ยวกับการก่อการร้ายของกลุ่มก่อการร้ายข้ามชาติ (Transnational terrorist groups) แต่เหตุความรุนแรงที่เกิดขึ้นนั้นจำกัดอยู่แค่การก่อเหตุความไม่สงบของชาวชาติพันธุ์ (Ethno-nationalist insurgents) ในสี่จังหวัดชายแดนภาคใต้ของประเทศไทยเท่านั้น อย่างไรก็ตามหน่วยงานที่เกี่ยวข้องต่อการรักษาความมั่นคงของประเทศไทยมีกังวลเกี่ยวกับศักยภาพของกลุ่มจัดตั้งรัฐอิสลามแห่งอิรักและ Levant (ISIL (Da'esh) ในการแทรกซึมเข้าร่วมกับกลุ่มผู้ก่อความไม่สงบในสี่จังหวัดชายแดนภาคใต้ของประเทศไทย ทั้งนี้ในรายงานระบุว่า

³⁵⁰ “ประเทศไทยเองพยายามที่จะออกกฎหมายพระราชบัญญัติการปราบปรามการก่อการร้ายและจัดตั้งหน่วยงานด้วยเฉพาะขึ้น”

³⁵¹ Security Council, "Letter dated 2 September 2015 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism", the President of the Security Council (2015), pp. 99-100

จากข้อมูลของเจ้าหน้าที่ความมั่นคงของประเทศไทยได้ยืนยันว่าไม่มีหลักฐานใด ๆ ในปัจจุบันถึงความเชื่อมโยงในการปฏิบัติการระหว่างกลุ่มในประเทศกับเครือข่ายการก่อการร้ายระหว่างประเทศ³⁵²

ประเด็นการออกกฎหมาย แม้ว่าประเทศไทยกำลังร่างพระราชบัญญัติต่อต้านการก่อการร้ายฉบับใหม่ ซึ่งมีจุดมุ่งหมายเพื่อรวบรวมกฎหมายที่เกี่ยวข้องกับการต่อต้านการก่อการร้ายที่มีอยู่ให้เป็นเอกสารฉบับเดียว ซึ่งในอดีตที่ผ่านมาทำให้บังคับฐานความผิดว่าด้วยการก่อการร้ายให้เป็นไปตามประมวลกฎหมายอาญา เมื่อปลายปี พ.ศ. 2561 สภานิติบัญญัติแห่งชาติ (National Legislative Assembly of Thailand) ยังมิได้พิจารณาผ่านร่างกฎหมาย และในปัจจุบันปี พ.ศ. 2563 รัฐสภาแห่งราชอาณาจักรไทยตามรัฐธรรมนูญแห่งราชอาณาจักรไทยปีพุทธศักราช 2560 ก็ยังคงมิได้ผ่านร่างกฎหมายดังกล่าวเช่นกัน

ประเด็นการบังคับใช้กฎหมาย ในมาตรการการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายหน่วยงานที่เกี่ยวข้องของประเทศไทยได้ดำเนินการทางกฎหมายเพื่อให้สอดคล้องต่อพันธกรณีระหว่างประเทศไทยมีซึ่งสามารถแบ่งได้ตามหัวข้ออธิบายดังต่อไปนี้

1. การแบ่งปันข้อมูลทางกระบวนการยุติธรรม

ในเรื่องความร่วมมือระหว่างประเทศเกี่ยวกับคดีการก่อการร้ายนั้นประเทศไทยได้มีกลไกการบังคับทางกฎหมายภายในคือ

- 1.) พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535
- 2.) พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา (ฉบับที่ 2) พ.ศ. 2559
- 3.) ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2537

โดยกฎหมายได้ให้อำนาจ “สำนักงานอัยการสูงสุด” เป็นหน่วยงานกลาง (Central National Authority)³⁵³ ซึ่งจะมีหน้าที่คอยเป็นผู้รับการประสานงานหรือให้ความร่วมมือทางข้อมูลรวมทั้งพยานหลักฐานแก่ประเทศต่างๆที่อยู่ภายใต้ความร่วมมือในการปราบปรามการก่อการร้าย รวมทั้งเป็นจุดติดต่อเพื่อการสื่อสารอย่างไม่เป็นทางการเพื่อเตรียมคำขอ (Focal point to initiate informal communication to prepare a request)

³⁵² United States Department of State, *Country Reports on Terrorism 2019 - Thailand* (JUNE 24, 2020), <https://www.state.gov/wp-content/uploads/2020/06/Country-Reports-on-Terrorism-2019-2.pdf>

³⁵³ มาตรา 6 ระบุว่า ให้อัยการสูงสุดหรือผู้ซึ่งอัยการสูงสุดมอบหมายเป็นผู้ประสานงานกลาง ที่มา พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535

รายชื่อประเทศ/องค์การระหว่างประเทศที่มีสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกัน ในเรื่องทางอาญากับไทย				
ประเทศ	วันลงนาม	สถานที่ลงนาม	วันมีผลใช้บังคับ	
๑. สหรัฐอเมริกา	๑๙ มีนาคม ๒๕๒๙	กรุงเทพฯ	๑๐ มิถุนายน ๒๕๓๖	
๒. สหราชอาณาจักรบริเตนใหญ่ และไอร์แลนด์เหนือ	๑๒ กันยายน ๒๕๓๗	กรุงเทพฯ	๑๐ กันยายน ๒๕๔๐	
๓. แคนาดา	๓ ตุลาคม ๒๕๓๗	กรุงออตตาวา	๓ ตุลาคม ๒๕๓๗	
๔. สาธารณรัฐฝรั่งเศส	๑๑ กันยายน ๒๕๔๐	กรุงปารีส	๑ มิถุนายน ๒๕๔๓	
๕. ราชอาณาจักรนอร์เวย์	๒๐ พฤษภาคม ๒๕๔๒	นครแบร์เกน	๒๒ กันยายน ๒๕๔๓	
๖. สาธารณรัฐประชาชนจีน	๒๑ มิถุนายน ๒๕๔๖	จังหวัดเชียงใหม่	๒๐ กุมภาพันธ์ ๒๕๔๘	
๗. สาธารณรัฐเกาหลี	๒๕ สิงหาคม ๒๕๔๖	กรุงโซล	๖ เมษายน ๒๕๔๘	
๘. สาธารณรัฐอินเดีย	๘ กุมภาพันธ์ ๒๕๔๗	จังหวัดภูเก็ต	๗ มิถุนายน ๒๕๔๗	
๙. สาธารณรัฐโปแลนด์	๒๖ กุมภาพันธ์ ๒๕๔๗	กรุงเทพฯ	๔ ตุลาคม ๒๕๕๒	
๑๐. สาธารณรัฐสังคมนิยม ประชาธิปไตยศรีลังกา	๓๐ กรกฎาคม ๒๕๔๗	กรุงเทพฯ	๓๐ พฤษภาคม ๒๕๕๕	
๑๑. สาธารณรัฐเปรู	๓ ตุลาคม ๒๕๔๘	กรุงลิมา	๓ ตุลาคม ๒๕๔๘	
๑๒. ราชอาณาจักรเบลเยียม	๑๒ พฤศจิกายน ๒๕๔๘	กรุงเทพฯ	๒๓ กรกฎาคม ๒๕๕๓	
๑๓. ออสเตรเลีย	๒๗ กรกฎาคม ๒๕๔๙	กรุงกัวลาลัมเปอร์	๑๘ มิถุนายน ๒๕๕๒	
๑๔. สมาคมประชาชาติแห่งเอเชีย ตะวันออกเฉียงใต้ (อาเซียน)	๒๙ พฤศจิกายน ๒๕๔๗	กรุงกัวลาลัมเปอร์	๓๑ มกราคม ๒๕๕๖ (สำหรับไทย)	
๑๕. ยูเครน	๕ มิถุนายน ๒๕๖๐	กรุงเทพฯ	๙ สิงหาคม ๒๕๖๒	

สถานะ ณ เดือนกรกฎาคม ๒๕๖๒

ที่มารูปภาพ : <https://treaties.mfa.go.th/กฎหมายระหว่างประเทศ/ความร่วมมือทางอาญา>

ทั้งนี้ประเทศไทยได้มีสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันระหว่างประเทศไทยกับประเทศต่างๆ ซึ่งสามารถเข้าไปดูรายชื่อสนธิสัญญาที่ได้กรมสนธิสัญญาและกฎหมายกระทรวงการต่างประเทศ³⁵⁴

³⁵⁴ อาจารย์ ดร. ชัชชม อรรถภิญญ์ อธิบดีอัยการ, เอกสารประกอบการสอนวิชาวิธีพิจารณาความอาญาชั้นสูง, หัวข้อ ความร่วมมือระหว่างประเทศในเรื่องทางอาญา (Mutual Legal Assistance in Criminal Matters), (สำนักงานต่างประเทศสำนักงานอัยการสูงสุด, 2018).

ความเห็นของผู้เขียนมีข้อสังเกตอยู่ว่าสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันระหว่างประเทศไทยกับประเทศต่างๆ หลายฉบับยังมิได้ถูกทบทวน (Review) ถึงเนื้อหาเพื่อให้สอดคล้องต่อการแบ่งปันข้อมูลในปัจจุบัน เช่น การแบ่งปันข้อมูลดิจิทัล หรือพยานหลักฐานทางอิเล็กทรอนิกส์

2. การแบ่งปันข้อมูลทางการเงินของการก่อการร้าย

ประเทศไทยได้มีกลไกตามกฎหมายในการดำเนินมาตรการแบ่งปันข้อมูลที่เกี่ยวข้องกับการเงินของการก่อการร้ายโดยมีหน่วยงานบังคับใช้กฎหมาย (Law enforcement) คือ สำนักงานป้องกันและปราบปรามการฟอกเงิน (Anti-Money Laundering Office) หรือ ปปง. ทั้งนี้ได้มีอำนาจหน้าที่ตามกฎหมายเสมือนเป็นหน่วยข่าวกรองทางการเงิน (Financial intelligence unit) อีกด้วย โดยอาศัยอำนาจตามกฎหมายดังต่อไปนี้คือ

1. พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒

2. พระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. ๒๕๕๙

โดยที่กฎหมายดังกล่าวให้อำนาจหน้าที่สำนักงานป้องกันและปราบปรามการฟอกเงิน (Anti-Money Laundering Office) มีอำนาจในการเก็บ รวบรวมข้อมูล และพยานหลักฐานเพื่อดำเนินการเกี่ยวกับการยึดอายัด หรือริบทรัพย์สินตามกฎหมายป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง หรือตามกฎหมายอื่น³⁵⁵ มากกว่าสำนักงานป้องกันและปราบปรามการฟอกเงิน (Anti-Money Laundering Office) มีอำนาจในการเข้าถึงข้อมูล หรือให้ซึ่งข้อมูลแก่คณะกรรมการลงโทษตามข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติเพื่อดำเนินมาตรการในการยึดอายัด หรือริบทรัพย์สินของบุคคลตามรายชื่อบุคคลที่ถูกกำหนด (UN Sanction List)

³⁵⁵ มาตรา 22 (4) ของพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559



รายชื่อบุคคลที่ถูกกำหนด

แห่ง พ.ร.บ. ป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559



รายชื่อบุคคลที่ถูกกำหนด
ตามมาตรา 6 และมาตรา 15
(UN Sanction List)



รายชื่อบุคคลที่ถูกกำหนด
ตามมาตรา 7
(Thailand List)

▶ รายชื่อบุคคลที่ถูกกำหนด กลุ่ม Al-Qaida

▶ รายชื่อบุคคลที่ถูกกำหนด กลุ่ม Taliban

▶ รายชื่อบุคคลที่ถูกกำหนด กลุ่ม DPRK

▶ รายชื่อบุคคลที่ถูกกำหนด กลุ่ม IRAN

ที่มาของรูปภาพ : <https://www.amlo.go.th/index.php/th/>

โดยพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง พ.ศ. 2559 มาตรา 6 บัญญัติว่า “ในกรณีที่มีมติของหรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติกำหนดรายชื่อบุคคล คณะบุคคล นิติบุคคล หรือองค์กรใดเป็นผู้ที่มีการกระทำความผิดเป็นการก่อการร้าย และสำนักงานเห็นว่ามติหรือประกาศดังกล่าวไม่ขัดต่อรัฐธรรมนูญและกฎหมายไทย ให้สำนักงานดำเนินการ ประกาศรายชื่อนั้นเป็นบุคคลที่ถูกกำหนดเพื่อดำเนินการให้เป็นไปตามมติหรือประกาศดังกล่าว การเพิกถอนรายชื่อของบุคคลที่ถูกกำหนดตามวรรคหนึ่ง ให้กระทำได้เมื่อมีมติของหรือประกาศ ภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติอันเป็นผลให้ต้องเพิกถอนรายชื่อผู้นั้นออกจากรายชื่อบุคคลที่ถูกกำหนดแล้ว”

และมาตรา 15 บัญญัติไว้ว่า “ในกรณีที่มีมติของหรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติกำหนดรายชื่อบุคคล คณะบุคคล นิติบุคคล หรือองค์กรใดเป็นผู้กระทำการอันเกี่ยวข้องกับการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง และสำนักงานเห็นว่ามติหรือประกาศดังกล่าวไม่ขัดต่อรัฐธรรมนูญและกฎหมายไทยให้สำนักงานประกาศรายชื่อนั้นเป็นบุคคลที่ถูกกำหนดเพื่อดำเนินการให้เป็นไปตามมติหรือประกาศดังกล่าวการเพิกถอนรายชื่อของบุคคลที่ถูกกำหนดตามวรรคหนึ่ง ให้กระทำได้เมื่อมีมติของหรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติอันเป็นผลให้ต้องเพิกถอนรายชื่อผู้นั้นออกจากรายชื่อบุคคลที่ถูกกำหนดแล้ว”

3. การแบ่งปันข้อมูลเพื่อการบังคับทางกฎหมายและการตรวจบุคคลเข้าเมือง

หน่วยงานบังคับใช้กฎหมายของไทย อาทิ สำนักงานตำรวจแห่งชาติ (the Royal Thai Police) กรมสอบสวนคดีพิเศษ (the Department of Special Investigation) และกองทัพไทย (the Thai military) ได้มีมาตรการบังคับในการตรวจจับ ยับยั้ง ตอบสนองต่อเหตุการณ์ก่อการ และบังคับใช้กฎหมายในคดีที่เกี่ยวข้องกับการก่อการร้าย ทั้งนี้ความร่วมมือและการประสานงานระหว่างหน่วยงานภายในประเทศไทยนั้นยังมีข้อจำกัดในเรื่องการแบ่งปันข้อมูล และการกำหนดขอบเขตของหน้าที่ระหว่างหน่วยงานบังคับใช้กฎหมาย และหน่วยทหาร ในเรื่องความรับผิดชอบในการต่อต้านการก่อการร้าย ในการแบ่งปันข้อมูลที่เกี่ยวข้องกับการก่อการร้ายระหว่างประเทศ

สำนักงานตำรวจแห่งชาติมีหน่วยงานในสังกัด คือ สำนักงานตรวจคนเข้าเมือง และกรมสอบสวนคดีพิเศษ ได้มีกลไกในการเข้าถึงข้อมูลและแบ่งปันข้อมูลผ่านเครื่องมือขององค์การตำรวจอาชญากรรมระหว่างประเทศ โดยได้จัดทำร่างความตกลงระหว่างสำนักงานกลางแห่งชาติตำรวจสากลประเทศไทยและสำนักงานตำรวจแห่งชาติว่าด้วยการเข้าถึงระบบข้อมูลข่าวสารองค์การตำรวจสากลโดยตรง (Agreement between the INTERPOL National Central Bureau for Thailand in Bangkok and Royal Thai Police on Direct Access to the INTERPOL Information System) และคณะรัฐมนตรีมีมติเห็นชอบและอนุมัติตามที่สำนักงานตำรวจแห่งชาติเสนอ³⁵⁶ ดังนี้

- “1. เห็นชอบในการจัดทำความตกลงระหว่างสำนักงานกลางแห่งชาติตำรวจสากลประเทศไทย (ตำรวจสากลกรุงเทพ) และสำนักงานตำรวจแห่งชาติว่าด้วยการเข้าถึงระบบข้อมูลข่าวสารองค์การตำรวจสากลโดยตรง (Agreement between the INTERPOL National Central Bureau for Thailand in Bangkok and Royal Thai Police on Direct Access to the INTERPOL Information System)
2. มอบหมายให้ผู้บัญชาการตำรวจแห่งชาติหรือผู้ที่ผู้บัญชาการตำรวจแห่งชาติมอบหมายเป็นผู้ลงนามความตกลงดังกล่าว
3. อนุมัติให้สำนักงานตำรวจแห่งชาติสามารถดำเนินการแก้ไขปรับปรุงร่างความตกลงฯ ในส่วนที่ไม่ใช่สาระสำคัญหากมีความจำเป็นต้องมีการแก้ไข ในภายภาคหน้าโดยไม่ต้องเสนอคณะรัฐมนตรีพิจารณาให้ความเห็นชอบอีกครั้ง”³⁵⁷

³⁵⁶ Nationthailand NEWS, "Cabinet okays Interpol-DSI draft agreement", (February 24, 2021), Retrieved from <https://www.nationthailand.com/in-focus/30403008>

³⁵⁷ มติชน, กรมเห็นชอบร่างความตกลงของดีเอสไอเข้าถึงฐานข้อมูลตำรวจสากล ยกเว้นบังคับใช้กฎหมายระหว่างประเทศ (กุมภาพันธ์ 2564), https://www.matichon.co.th/politics/news_2593283. มติชน, "กรมเห็นชอบร่างความตกลงของดีเอสไอเข้าถึงฐานข้อมูลตำรวจสากล ยกเว้นบังคับใช้กฎหมายระหว่างประเทศ," (กุมภาพันธ์ 2564). https://www.matichon.co.th/politics/news_2593283

สำหรับฐานข้อมูลที่ได้รับอนุญาตให้เข้าถึงโดยตรงประกอบด้วย 9 ฐานข้อมูล ดังนี้

1. เรื่องเอกสารการเดินทางที่ถูกขโมยหรือสูญหาย (Stolen and Lost Travel Document -SLTD)
2. เอกสารราชการที่ถูกขโมย (Stolen Administrative Document)
3. ภาพการแสวงหาประโยชน์ทางเพศจากเด็กระหว่างประเทศ (IChild Sexual Exploitation Images -ICSE)
4. ระบบจัดการบันทึกและการติดตามอาวุธผิดกฎหมาย (Illicit arms records management system -iARMS)
5. เอกสารการเดินทาง (Edison TD)
6. ตารางหมายเลขอ้างอิงอาวุธปืน ขององค์การตำรวจสากล (INTERPOL Firearms Reference Table -IFRT)
7. ฐานข้อมูลแจ้งเตือนระบบดิจิทัล ขององค์การตำรวจสากลเกี่ยวกับเอกสาร (The Digital INTERPOL Alert)
8. ระบบข้อมูลอาชญากรรมขององค์การตำรวจสากล (INTERPOL's Criminal Information System (ICIS)
- ระบบข้อมูลกระสุนปืน ปดอกรกระสุนปืน ขององค์การตำรวจสากล (INTERPOL Ballistic Information Network)

ทั้งนี้ประเทศไทยได้เริ่มรวบรวมข้อมูลและวิเคราะห์ข้อมูลผู้โดยสารล่วงหน้า และข้อมูลการบันทึกของผู้โดยสาร บนเที่ยวบินเชิงพาณิชย์ที่สนามบินนานาชาติทุกแห่งในประเทศ โดยการอาศัยอำนาจตามตามพระราชบัญญัติการเดินอากาศ เพื่อออกข้อบังคับของคณะกรรมการการบินพลเรือน ฉบับที่ 87 ว่าด้วยการอำนวยความสะดวกเพื่อตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า ข้อที่ 2 (2) บัญญัติว่า “เพื่อประโยชน์ในการอำนวยความสะดวกในการเดินทางผ่านแดนและการตรวจปล่อย เพื่อการเข้าออกราชอาณาจักร ของอากาศยาน ผู้โดยสาร ผู้ประจำหน้าที่ เจ้าหน้าที่ประจำอากาศยาน และสัมภาระ ณ สนามบินอนุญาตที่ให้บริการระหว่างประเทศ ให้ดำเนินการดังต่อไปนี้ ให้เจ้าของหรือผู้จดทะเบียนอากาศยาน หรือผู้ดำเนินการเดินอากาศ จัดเก็บข้อมูล ผู้โดยสารล่วงหน้า และข้อมูลผู้ประจำหน้าที่ในอากาศยานล่วงหน้า ในทุกเที่ยวบินและนำส่งทางอิเล็กทรอนิกส์ ไปยังระบบข้อมูลการตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า และส่งไปยังระบบของเจ้าหน้าที่ผู้มีอำนาจ”³⁵⁸

กล่าวคือสายการบินผู้ให้บริการภายใต้เขตอำนาจของรัฐไทยจะต้องเก็บข้อมูลผู้โดยสารล่วงหน้า และข้อมูลการบันทึกของผู้โดยสาร เพื่อแบ่งปันให้แก่หน่วยงานที่มีอำนาจในการตัดสินใจให้อนุญาตหรือไม่ให้อนุญาตบุคคลเดินทางเข้ามาในราชอาณาจักร หรือออกไปซึ่งจากราชาอาณาจักร

³⁵⁸ ข้อบังคับของคณะกรรมการการบินพลเรือน ฉบับที่ 87 ว่าด้วยการอำนวยความสะดวกเพื่อตรวจสอบและคัดกรองผู้โดยสารล่วงหน้า ข้อที่ 2 (2)

4. การแบ่งปันข้อมูลต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงที่ใช้ในการก่อการร้าย

หน่วยงานที่มีอำนาจหน้าที่รับผิดชอบในการให้ข้อมูลการดำเนินการตามข้อมติที่ 1540/2004 กับคณะกรรมการลงโทษตามข้อมติที่ 1540 (Security Council Committee established pursuant to resolution 1540 (2004) คือ กรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ ประเทศไทย และคณะผู้แทนถาวรไทยประจำสหประชาชาติ ณ นครนิวยอร์ก เป็นหน่วยงานติดต่อระดับชาติ และเป็นผู้รับผิดชอบในการรวบรวมข้อมูลของประเทศไทยในการดำเนินมาตรการการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงโดย “National Focal Points” ของประเทศไทยต่อการดำเนินการมาตรการซึ่งประกอบไปด้วย³⁵⁹

- 1.) กระทรวงกลาโหมเป็นหน่วยงานระดับชาติ ในการควบคุมและกำกับซิปินาอาวุธ อาวุธธรรมดาและวัสดุที่เกี่ยวข้อง
- 2.) สำนักงานปรมาณูเพื่อสันติ (The Office of Atoms or Peace) เป็นหน่วยงานระดับชาติ ในการกำกับดูแลและควบคุมอาวุธนิวเคลียร์และรังสีและวัสดุที่เกี่ยวข้อง
- 3.) กระทรวงอุตสาหกรรมเป็นหน่วยงานระดับชาติในการควบคุมและกำกับอาวุธเคมีและวัสดุที่เกี่ยวข้อง
- 4.) กระทรวงสาธารณสุขเป็นหน่วยงานระดับชาติในการควบคุมและกำกับอาวุธชีวภาพและวัสดุที่เกี่ยวข้อง
- 5.) กระทรวงพาณิชย์เป็นหน่วยงานระดับชาติในการกำกับดูแลและควบคุมรายการสินค้าสองทาง (Dual use items)

และมีกฎหมายที่เกี่ยวข้องต่อการดำเนินการต่อต้านการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงเพื่อใช้ในการก่อการร้ายคือ

1. พระราชบัญญัติศุลกากร (พ.ศ. 2469)
2. พระราชบัญญัติควบคุมการส่งออกอาวุธยุทโธปกรณ์และสงครามการดำเนินการ
3. พระราชบัญญัติพลังงานปรมาณูเพื่อสันติ (พ.ศ. 2504)
4. กฎกระทรวงซึ่งออกตามคำสั่งแห่งชาติ คณะปฏิรูปการปกครองชุดที่ 37 (พ.ศ. 2519)
5. พระราชบัญญัติการส่งออกและนำเข้าสินค้า (พ.ศ. 2522)
6. พระราชบัญญัติควบคุมโรค (พ.ศ. 2523)

³⁵⁹ Security Council Committee established pursuant to resolution 1540 (2004), "Note verbale dated 5 November 2004 from the Permanent Mission of Thailand to the United Nations", the Chairman of the Committee, Available from <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/665/64/PDF/N0466564.pdf>

7. พระราชบัญญัติควบคุมอาวุธสงคราม (พ.ศ. 2530)
8. พระราชกฤษฎีกาควบคุมการส่งออกอาวุธยุทโธปกรณ์และการทำสงคราม
9. พระราชบัญญัติวัตถุอันตราย (พ.ศ. 2535)
10. พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (พ.ศ. 2542)
11. พระราชบัญญัติควบคุมโรคสัตว์ (พ.ศ. 2544)
12. พระราชบัญญัติเชื้อโรคและสารพิษ (พ.ศ. 2544)
13. ประมวลกฎหมายอาญา

4.2 ผลกระทบของภาคธุรกิจในการดำเนินมาตรการแบ่งปันข้อมูล

หากจะกล่าวถึงผลกระทบของการก่อการร้ายต่อภาคเศรษฐกิจก็สามารถที่จะได้คำตอบอย่างชัดเจนว่าการก่อการร้ายมีนัยยะสำคัญของการสร้างความเสียหายต่อเศรษฐกิจเป็นอย่างมาก ซึ่งต้นทุนมูลค่าความเสียหายทางเศรษฐกิจนั้นสามารถวัดได้จากการสูญเสียทรัพยากรมนุษย์ (Human resource lost) รวมทั้งทรัพย์สินที่ถูกทำลายจากเหตุก่อการร้ายที่ส่งผลกระทบโดยตรงต่อการประเมินมูลค่าการเติบโตของเศรษฐกิจในแง่ของการผลิตอย่างชัดเจน ทั้งนี้ยังไม่รวมถึงผลกระทบทางด้านอารมณ์ (Emotional toll) ที่เกิดขึ้นกับเหยื่อการก่อการร้าย ญาติ เพื่อนสนิท ผู้รอดชีวิต รวมทั้งผู้คนที่อาศัยในพื้นที่ที่ถูกก่อการร้ายล้วนเป็นปัจจัยของการเกิดผลกระทบต่อภาคการผลิตในระบบเศรษฐกิจอย่างปฏิเสธมิได้³⁶⁰

มากไปกว่านั้นในการดำเนินมาตรการปราบปรามการก่อการร้ายก็สร้างผลกระทบต่อภาคเศรษฐกิจด้วยเช่นกัน อันเป็นผลมาจากการกระทำของภาครัฐในการดำเนินมาตรการปราบปราม และเอกชนเองจำเป็นต้องเพิ่มเติม “ต้นทุนอ้อม (Indirect costs)” เพื่อป้องกันตนเองจากผลกระทบของการโจมตีของผู้ก่อการร้าย หรือเพื่อป้องกันการโจมตีของผู้ก่อการร้าย ซึ่งค่าใช้จ่ายอันเป็นต้นทุนอ้อมที่เกิดขึ้นต่อภาคธุรกิจนั้นสามารถพิจารณาแบ่งออกเป็น 2 ทางหลักๆ คือ “ต้นทุนในการรักษาความปลอดภัย (Cost of security investment)” และ “ต้นทุนค่าเสียโอกาส (Opportunity costs)”³⁶¹ ที่เกิดขึ้นโดยที่ภาคเอกชนเองต้องให้ความร่วมมือ หรืออยู่ภายใต้ระเบียบข้อบังคับจากภาครัฐในการดำเนินมาตรการปราบปรามการก่อการร้าย ความจำเป็นในการต่อต้านการก่อการร้ายของภาครัฐนั้นจะบรรลุผลอย่างมีประสิทธิภาพได้ ภาคเอกชนที่ดำเนินกิจการภายใต้เขตอำนาจ

³⁶⁰ David Gold, "Economics of Terrorism - Economic Aspects of Fighting Terrorism," *Graduate Program in International Affairs New School University* (2015), https://www.files.ethz.ch/isn/10698/doc_10729_290_en.pdf

³⁶¹ Friedrich Schneider, Tilman, and Daniel,, "The Economics of Terrorism and Counter-Terrorism: A Survey," *Economics of Security Working Paper - German Institute for Economic Research* no. 45 (2011).

จำเป็นต้องให้ความร่วมมือกับมาตรการปราบปรามการก่อการต่างๆด้วย ซึ่งผลที่ตามมาก็คือการเพิ่มขึ้นทางอ้อมของภาคเอกชนนั่นเอง

4.2.1 ต้นทุนของมาตรการรักษาความปลอดภัย

ในกระบวนการดำเนินมาตรการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้ายของรัฐ จำที่จะต้องให้บริษัทเอกชนที่อยู่ภายใต้เขตอำนาจปฏิบัติตามมาตรการในการปราบปรามการก่อการร้าย โดยส่วนใหญ่แล้วบริษัทเอกชนจะต้องเพิ่มต้นทุนในเรื่องของการรักษาความปลอดภัยให้สอดคล้องกับนโยบายต่อต้านของภาครัฐ โดยเฉพาะภาคธุรกิจที่ดำเนินกิจการเกี่ยวกับอุตสาหกรรมขนส่ง ที่ถูกผลกระทบจากระเบียบข้อบังคับของรัฐให้กลุ่มอุตสาหกรรมเหล่านี้มีการดำเนินการเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัย จากการที่การก่อการร้ายส่วนใหญ่ที่เกิดจะมุ่งเน้นการโจมตีไปที่โครงสร้างพื้นฐานสาธารณะ และการขนส่งสาธารณะ บริษัทที่ดำเนินกิจการที่เกี่ยวข้องกับการขนส่งทางการบิน การขนส่งทางเรือ การขนส่งทางถนน การขนส่งทางรถไฟ จำเป็นจะต้องเพิ่มต้นทุนในแง่การกำหนดมาตรการความปลอดภัยที่สอดคล้องกับระเบียบข้อบังคับในการปราบปรามการก่อการร้ายของรัฐ จากต้นทุนของบริษัทเอกชนที่เพิ่มขึ้นมานั้น จึงส่งผลกระทบต่อผู้ใช้บริการมีภาระที่จะต้องจ่ายค่าธรรมเนียมของการบริการที่เพิ่มขึ้นไปด้วยอยู่ในรูปแบบของ “Security surcharges”³⁶²

ในการศึกษาผลกระทบของบริษัทที่ให้บริการเกี่ยวกับการขนส่งทางการบิน ในประเทศสหรัฐอเมริกา ภายหลังเหตุการณ์วินาศกรรมได้มีกฎระเบียบข้อบังคับว่าสายการบินดำเนินการหาช่องทางการแบ่งปันข้อมูลผู้โดยสารล่วงหน้า และข้อมูลบันทึกการเดินทางของผู้โดยสาร ให้แก่หน่วยงานบังคับใช้กฎหมายที่มีอำนาจหน้าที่เกี่ยวข้องกับการตรวจคนเข้าเมืองเพื่อดำเนินมาตรการปราบปรามการก่อการร้าย อาทิ ในการแบ่งปันข้อมูลบริษัทเอกชนจะต้องสร้างโครงข่ายการเชื่อมต่อเพื่อการแบ่งปันข้อมูลในรูปแบบของ “Passenger Data Single Window” กับหน่วยงานของรัฐ³⁶³ รวมทั้งบริษัทเอกชนต้องพัฒนาระบบการเก็บข้อมูลผู้โดยสารด้วยตัวเอง เป็นต้น [ดังตัวอย่างนี้ชี้ให้เห็นว่าภาระของการเพิ่มต้นทุนตกอยู่ที่บริษัทเอกชน มีรายงานตัวเลขว่าบริษัทสายการบินต่างๆ เพิ่มค่าบริการเที่ยวบิน ขึ้นไปถึง 8 ดอลลาร์ต่อผู้โดยสารหนึ่งคน หรือในการบริการการขนส่งสินค้าทางอากาศราคาถูกปรับค่าบริการเพิ่มขึ้นมาที่ 0.10 - 0.15 ดอลลาร์ต่อ 1 กิโลกรัมของน้ำหนักสินค้าที่ถูกขนส่งอันเป็นผลมาจากที่บริษัทผู้ให้บริการมีต้นทุนที่เพิ่มขึ้นในการกำหนดมาตรการรักษาความปลอดภัยในสอดคล้องต่อมาตรการในการปราบปรามการก่อการร้ายของภาครัฐ

³⁶² Ibid, p.59-60

³⁶³ International Civil Aviation Organization, "Annex 9 to the Convention on International Civil Aviation Facilitation", Fifteenth Edition, (October 2017), p. 9-1 CHAPTER 9. Passenger data exchange systems, Available from https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

4.2.2 ต้นทุนค่าเสียโอกาส

ต้นทุนค่าเสียโอกาส³⁶⁴ ที่เกิดขึ้นกับเอกชนในการที่ภาครัฐดำเนินมาตรการปราบปรามการก่อการร้ายที่เคร่งครัดที่ให้ภาคธุรกิจที่เกี่ยวข้องกับการขนส่งทางการบิน การขนส่งทางเรือ การขนส่งทางถนน การขนส่งทางรถไฟ จำเป็นจะต้องเพิ่มต้นทุนในแง่การกำหนดมาตรการความปลอดภัยที่สอดคล้องกับระเบียบข้อบังคับในการปราบปรามการก่อการร้ายของรัฐ เมื่อการดำเนินการปราบปรามการก่อการร้ายแล้วรัฐในหลายๆด้านมีความเข้มแข็งขึ้น เช่น มาตรการตรวจคนเดินทางเข้าเมืองที่มีระเบียบและขั้นตอนที่เพิ่มขึ้นในมาตรการรักษาความปลอดภัย มั่นนำมาสู่ผลกระทบต่อภาคอุตสาหกรรมการขนส่งทางการบิน

รายงานผลการวิจัยของ Blalock et al. (2007)³⁶⁵ แสดงให้เห็นว่าการที่รัฐมีมาตรการดำเนินการตรวจคัดกรองบุคคลเข้าเมือง สัมภาระของบุคคลในสหรัฐอเมริกาหลังเหตุการณ์วินาศกรรม 9/11 ส่งผลกระทบให้ความต้องการในการเดินทางทางอากาศลดลงอย่างมาก (Considerable reduction in demand)³⁶⁶ แม้ว่าจะทำการควบคุมปัจจัยกระทบอื่น ๆ ซึ่งอาจส่งผลกระทบต่อความต้องการในการเดินทางทางอากาศแล้วก็ตาม รายงานผลการวิจัยนี้แสดงให้เห็นว่ามาตรการต่อต้านการก่อการร้ายของภาครัฐ ส่งผลกระทบการเติบโตของรายได้ของภาคอุตสาหกรรมการบิน รวมถึงความสามารถในการทำกำไรของอุตสาหกรรมในอนาคต มากไปกว่านั้นภาคอุตสาหกรรมท่องเที่ยวเองก็ได้รับผลกระทบจากสูญเสียรายได้จากการต้องดำเนินมาตรการรักษาความปลอดภัยตามนโยบายของภาครัฐ ซึ่งส่งผลจากภาคอุตสาหกรรมที่ต้องกำหนดขั้นตอนของการรักษาความปลอดภัยให้แก่นักท่องเที่ยว ผู้นำทัวร์ ตลอดจนการมีเครื่องมือตามมาตรการตรวจสอบความปลอดภัยของสัมภาระของผู้เดินทาง

ธุรกิจที่เกี่ยวข้องกับการจัดหาแรงงานที่มีทักษะเฉพาะข้ามชาติก็ได้รับผลกระทบจากการดำเนินมาตรการปราบปรามการก่อการร้ายจากการที่ภาครัฐได้เพิ่มขั้นตอนของการพิจารณาออกเอกสารอนุญาตให้เข้าประเทศ อนุญาตให้เข้ามาทำงานในประเทศ กระบวนการที่เข้มงวดเหล่านี้ส่งผลกระทบต่อการจัดหาแรงงานที่มีทักษะเฉพาะข้ามชาติ ที่จำเป็นต้องผ่านขั้นตอนการพิจารณาในการออกเอกสารที่ยากขึ้น นักท่องเที่ยวธุรกิจ เช่น กลุ่มนักท่องเที่ยวไปเพื่อประชุม อบรม ดูงาน หรือต่อยอดธุรกิจนอกสถานที่ ที่เดินทางเข้ามาทำงานที่ประเทศสหรัฐอเมริกาหลังจากการมีมาตรการรักษาความปลอดภัยที่เกี่ยวข้องกับการปราบปรามการก่อการร้ายมีแนวโน้มที่จะไม่กลับมาทำธุรกิจใน

³⁶⁴ ต้นทุนค่าเสียโอกาส (Opportunity cost) คือ มูลค่าของผลตอบแทนจากกิจกรรมที่สูญเสียโอกาสไปในการเลือกทำกิจกรรมอย่างหนึ่ง ที่มา: www.posttoday.com/aec/trade

³⁶⁵ Kadiyali Blalock, D.H. Simon, , "The impact of post-9/11 airport security measures on the demand for air travel," *Journal of Law & Economic* (2007).

³⁶⁶ Schneider, "The Economics of Terrorism and Counter-Terrorism: A Survey."

ประเทศอีก³⁶⁷ และในอีกหลายคนเลือกที่จะเดินทางไปทำธุรกิจในประเทศอื่นแทน ซึ่งธุรกิจที่อยู่ ประกอบกิจการที่เกี่ยวข้องก็เกิดการสูญเสียทุนต้นทางโอกาสจากการที่ต้องยึดถือมาตรการปราบปรามการก่อการร้ายจากภาครัฐ

เมื่อมาตรการตรวจคนเข้าเมืองมีความซับซ้อนมากขึ้น ส่งผลให้การขออนุญาตออกเอกสารอนุญาตเดินทางเข้าประเทศ³⁶⁸ มีตัวเลขที่ลดลงร้อยละ 32 เป็นผลมาจากขั้นตอนการขอวีซ่าที่ยากขึ้นหลังเกิดเหตุการณ์วินาศกรรม 9/11 ทั้งในอุตสาหกรรมที่เกี่ยวข้องในการขนส่งเชื้อโรค (The transport of pathogens) ในสหรัฐอเมริกาได้ถูกมาตรการปราบปรามการก่อการร้าย ปิดกั้นโอกาสในการวิจัยทางชีวการแพทย์ในหลาย ๆ ด้าน รวมถึงการวิจัยที่อาจนำไปสู่กิจกรรมที่เกี่ยวข้องกับการป้องกันทางชีวภาพ (Bio-defense related activities) ซึ่งมีค่าเสียโอกาสทางธุรกิจ และอาจส่งผลต่อการเติบโตของภาคการผลิตในระยะยาวที่เป็นไปได้³⁶⁹

4.3 ผลกระทบต่อผู้มีส่วนเกี่ยวข้องที่เป็นเจ้าของข้อมูล

ในการดำเนินมาตรการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย จำเป็นที่จะต้องอาศัยข้อมูลจากผู้มีส่วนเกี่ยวข้องต่างๆ เช่น ภาคธุรกิจผู้ให้บริการเทคโนโลยีการสื่อสาร สถาบันทางการเงิน และบริการธุรกรรมทางการเงิน หรือตัวปัจเจกชนเองให้เข้ามาเป็นส่วนหนึ่งในกระบวนการของการปราบปรามการก่อการร้าย อย่างไรก็ตามหากเกิดผลกระทบขึ้นกับบุคคลที่สามซึ่งเป็นเจ้าของข้อมูลผู้เกี่ยวข้องเหล่านี้จะมีการคุ้มครองและการแก้ไขอย่างไร

4.3.1 ภาคธุรกิจผู้ให้บริการเทคโนโลยีการสื่อสาร

ในการดำเนินมาตรการป้องกันและปราบปรามการก่อการร้ายจำเป็นอยู่แล้วที่ภาครัฐจะต้องอาศัยข้อมูลต่างๆ ในการวิเคราะห์และดำเนินมาตรการป้องกัน และในหลายประเทศก็มีข้อเท็จจริงที่ปรากฏอย่างชัดเจนว่ารัฐได้พึ่งพาข้อมูลของภาคเอกชน (Private sector) ในการดำเนินการเฝ้าระวังการก่อการร้ายไม่มากนักน้อย บางรัฐอาศัยกลไกทางกฎหมายเป็นวิธีการหนึ่งในการเข้าถึงข้อมูลภาคธุรกิจที่เป็นเป้าหมายแรกของการที่รัฐจะอาศัยข้อมูลเพื่อดำเนินการป้องกันการก่อการร้ายได้แก่ กลุ่มธุรกิจที่เกี่ยวข้องกับการให้บริการสื่อสารโทรคมนาคม (Telecommunications service

³⁶⁷ David Gold, "Economics of Terrorism - Economic Aspects of Fighting Terrorism," in *Graduate Program in International Affairs New School University* (2015).

³⁶⁸ Daniel Altman, "Uncertain Economy Hinders Highly Precise Supply System," *New York Times* March 15, 2003, <https://www.nytimes.com/2003/03/15/business/uncertain-economy-hinders-highly-precise-supply-system.html>.

³⁶⁹ Edward Alden, "No Entry: Tougher Visa Controls are Creating Barriers to American Business," *Financial Times* July 2, 2004, <https://www.ft.com/content/aa713a54-80a6-4117-83f8-3d610cd872e6>

providers) และบริการอินเทอร์เน็ต (Internet service) โดยทั่วไปแล้วรัฐเป็นเจ้าของสัมปทานคลื่นความถี่ให้แก่บริษัทเอกชนในการประกอบกิจการด้านสื่อสารโทรคมนาคม โดยอาจจะมีการกำหนดเงื่อนไขทางกฎหมายถึงการขอเข้าถึงข้อมูลซึ่งเป็นประโยชน์ต่อการดำเนินการบังคับใช้กฎหมายและมาตรการป้องกันภัยต่างๆ ของรัฐ มากกว่านั้นในบางรัฐกำหนดข้อบังคับทางกฎหมายเปิดช่องให้หน่วยงานของรัฐสามารถเข้าถึงการดักฟัง (Wiretap-ready)³⁷⁰ การให้บริการของบริษัทเหล่านี้ อันเป็นสิ่งที่น่ากังวลถึงผลกระทบที่เกิดขึ้นกับตัวของบริษัทเอกชนเอง และรวมไปถึงเจ้าของข้อมูลอย่างผู้รับบริการต่อความเสี่ยงที่จะถูกสอดแนมโดยรัฐ

4.3.1.1 การปกป้องข้อมูลของผู้รับบริการ

การหลีกเลี่ยงความเสี่ยงของกลุ่มธุรกิจที่เกี่ยวข้องกับการให้บริการสื่อสารโทรคมนาคม (Telecommunications service providers) ในการละเมิดซึ่งข้อมูลของผู้รับบริการนั้น บริษัทจะต้องมีแผนกำหนดมาตรการปกป้องและแก้ไขปัญหาที่เกิดขึ้นต่อข้อมูลที่เกี่ยวข้องกับผู้รับบริการในทุกแง่มุมของการดำเนินธุรกิจของตน ในตัวอย่างประเทศภูมิภาคยุโรปบริษัทเหล่านี้รวมตัวกันจัดตั้งเป็น สมาคมผู้ประกอบการเทคโนโลยีการสื่อสาร (Information and communication technology business group association) และกำหนดมาตรฐานในการป้องกันและแก้ไขผลกระทบด้านสิทธิมนุษยชนของผู้รับบริการให้สอดคล้องกับหลักการของสหประชาชาติว่าด้วยธุรกิจกับสิทธิมนุษยชน (United Nations Guiding Principles on Business and Human Rights) และมีผลใช้บังคับตลอดการดำเนินงานทั่วโลกของกลุ่มบริษัทในสมาคม ไม่ว่าจะได้ให้บริการอยู่ที่ใดในโลก บริษัทผู้ให้บริการเทคโนโลยีการสื่อสารและบริการอินเทอร์เน็ตควรจะต้องจัดทำคำแถลงนโยบายของบริษัทถึงความมุ่งมั่นในการยึดถือและเคารพสิทธิของผู้รับบริการในทุกๆ ขั้นตอนของการให้บริการ เพื่อให้ความมั่นใจแก่ลูกค้าในการใช้บริการ รวมถึงนโยบายตรวจสอบวิเคราะห์ที่เหมาะสมเพื่อการประเมิน ป้องกันข้อมูลของลูกค้า หากในกรณีของบริษัทมีความจำเป็นจะต้องแบ่งปันข้อมูลลูกค้าแก่ภาครัฐ ในกรณีที่มีระเบียบข้อบังคับกำหนดให้ต้องทำที่ชัดเจน บริษัทควรจะต้องกำหนดเงื่อนไขดังกล่าวในข้อตกลงการใช้บริการ (Term of service) ให้ชัดเจนเพื่อเป็นการประกอบการตัดสินใจของผู้รับบริการว่ายอมรับในเงื่อนไขหรือไม่³⁷¹

เมื่อบริษัทถูกร้องขอจากภาครัฐในการเข้าถึงข้อมูลของผู้รับบริการ โดยหากบริษัทเห็นว่าการร้องขอนั้นปฏิบัติไม่สอดคล้องกับกฎเกณฑ์ที่กฎหมายกำหนด หรืออาจจะนำไปสู่การละเมิดซึ่งสิทธิของผู้รับบริการ บริษัทหรือสมาคมอาจอ้างหลักการและมาตรฐานที่ได้ถูกกำหนดชี้แจงต่อภาครัฐ หรือ

³⁷⁰ European Digital Rights, *The Slide from 'Self-Regulation' to Corporate Censorship* (January 2011), www.edri.org/files/EDRI_selfreg_final_20110124.pdf

³⁷¹ United Nations General Assembly, *International Principles on the Application of Human Rights to Communications Surveillance* (2014), <https://en.necessaryandproportionate.org/text>

แสดงความกังวลต่อการกระทำของภาครัฐ หากเห็นว่าจะต้องดำเนินการอย่างไม่มีเงื่อนไขก็ควรตีความข้อร้องขอของรัฐบาลให้แคบที่สุด หรือกำหนดให้แสดงคำสั่งศาลก่อนที่จะทำการดำเนินการตามคำขอของภาครัฐ รวมไปถึงจนถึงสื่อสารกับผู้รับบริการอย่างโปร่งใสเกี่ยวกับการที่บริษัทจะต้องปฏิบัติตามข้อเรียกร้องของรัฐ

4.3.1.2 การกำหนดมาตรการเยียวยา

ในการให้บริการของภาคธุรกิจผู้ให้บริการเทคโนโลยีการสื่อสารนั้นสิ่งสำคัญที่จะต้องมอบให้ผู้รับบริการคือ การการันตีด้วยความโปร่งใสถึง การเก็บข้อมูล การใช้ข้อมูล หรือการรวบรวมข้อมูลของผู้รับบริการจะถูกดำเนินการในขั้นตอนที่มีความปลอดภัย ดังนั้นบริษัทควรมีช่องทางในการแจ้งข้อกังวลของผู้รับบริการ รวมถึงแจ้งการขอให้ลบหรือแก้ไขเปลี่ยนแปลงข้อมูลของผู้รับบริการ ในกรณี que บริษัทผู้ให้บริการเทคโนโลยีการสื่อสารมีส่วนทำให้เกิดผลกระทบต่อสิทธิของผู้รับบริการ ทางบริษัทควรจะต้องมีกลไกให้ความรับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว กำหนดกระบวนการของการเยียวยาที่สอดคล้องกับกฎหมาย ตัวอย่างในการปฏิบัติของบางบริษัทได้กำหนดให้มีช่องทางความช่วยเหลือและเยียวยาแบบรวดเร็ว (Remediation at the earliest possible stage) เพื่อปกป้องและจำกัดวงกว้างของผลกระทบและความเสียหายที่เกิดขึ้นต่อข้อมูลผู้รับบริการ หรือกำหนดซึ่งองค์กรที่จะมาเป็นกลไกพิเศษ (Operational-level grievance mechanisms)³⁷² เพื่อรับร้องทุกข์จากการให้บริการของบริษัทที่สร้างผลกระทบต่อผู้รับบริการ โดยกระบวนการเหล่านี้จะประโยชน์อย่างมากกับผู้รับบริการที่อาศัยอยู่ในประเทศที่มีกลไกการคุ้มครองสิทธิที่ไม่มีประสิทธิภาพ

ผู้เขียนมีความเห็นว่าเป็นไปไม่ได้อย่างแน่นอนถ้าภาครัฐจะดำเนินมาตรการป้องกันและปราบปรามการก่อการร้ายโดยปราศจากการขอเข้าถึงข้อมูลต่างๆ อันจะเป็นประโยชน์ในการดำเนินการป้องกัน ซึ่งข้อมูลเหล่านั้นส่วนมากเป็นของบริษัทเอกชนผู้ให้บริการสื่อสารโทรคมนาคม (Telecommunications service providers) และบริการอินเทอร์เน็ต (Internet service) หากรัฐมีการอ้างถึงกลไกทางกฎหมายด้วยแล้วยากมากที่บริษัทเอกชนที่อยู่ภายใต้เขตอำนาจของรัฐจะหลีกเลี่ยงปฏิเสธการดำเนินการ แต่ทั้งนี้ทั้งนั้นบริษัทเอกชนที่ประกอบการในธุรกิจประเภทนี้ สามารถที่จะรวมตัวกันจัดตั้งเป็นสมาคมและมีประกาศเจตจำนงหรือการกำหนดมาตรฐานในการให้ความร่วมมือกับภาครัฐเป็นของตนเอง เพื่อเป็นวิธีการต่อรองกับรัฐในรูปแบบหนึ่ง ซึ่งจะเกิดขึ้นได้จากการที่กลุ่ม

³⁷² European Agency for Fundamental Rights, "Surveillance by Intelligence Services," *Fundamental Rights Safeguards and Remedies in the EU*. Vol. II: Field Perspectives and Legal Update, Luxembourg, Publications Office of the European Union (2017), <https://www.statewatch.org/media/documents/news/2015/nov/eu-fra-2015-surveillance-intelligence-services.pdf>

บริษัทผู้ประกอบการในธุรกิจประเภทนี้เล็งเห็นผลประโยชน์ของการคุ้มครองผู้รับบริการและให้ความสำคัญกับสิทธิของผู้รับบริการ อย่างไรก็ตามหากบริษัทเอกชนได้เป็นส่วนหนึ่งของการทำให้เกิดความเสียหายหรือกระทบจากการให้บริการของตน จำเป็นที่จะต้องมีการกำหนดมาตรการเยียวยา และการแก้ไขปัญหาต่อผู้รับบริการทั้งในระยะสั้นและในระยะยาวสำหรับการบริการใหม่ๆที่จะเกิดขึ้นในอนาคต

4.3.2 สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงิน

สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินนับว่ามีบทบาทสำคัญในการเป็นผู้เกี่ยวข้องในการดำเนินกระบวนการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของรัฐ เมื่อพิจารณาจะพบว่ารัฐต้องการเข้าถึงข้อมูลการทำธุรกรรมทางการเงินที่มีความเสี่ยงเกี่ยวข้องกับการก่อการร้ายเพื่อที่รัฐจะสามารถบังคับใช้กฎหมายในการต่อต้านการก่อการร้ายได้ สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินจึงเป็นแนวหน้าสำคัญที่รัฐจะใช้ข้อมูลเหล่านั้นเพื่อการสกัดกั้นการเงินของการก่อการร้าย

4.3.2.1 หน้าที่ในการคุ้มครองผลประโยชน์ของลูกค้า

สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินต่างมีพันธะขั้นพื้นฐาน (Fundamental obligations) ของการให้บริการกับลูกค้าในหลายๆด้าน อาทิ การให้การปฏิบัติที่เป็นธรรม (Fair treatment) แก่ลูกค้า โดยที่ห้ามไม่ให้สถาบันเลือกปฏิบัติต่อลูกค้าด้วยเหตุผลด้านเพศ อายุ ศาสนา เชื้อชาติ หรือการให้ความเป็นส่วนตัวแก่ลูกค้า (Privacy) โดยสถาบันทางการเงินมีหน้าที่จะต้องเก็บรักษาข้อมูลส่วนบุคคล ข้อมูลของการทำธุรกรรมของลูกค้า ลูกค้ามีสิทธิที่จะได้รับการคุ้มครองจากการสื่อสารทุกประเภทซึ่งจะละเมิดความเป็นส่วนตัวของพวกเขา ข้อมูลส่วนบุคคลของลูกค้าควรถูกเก็บเป็นความลับแม้ว่าลูกค้าคนดังกล่าวจะได้เลิกใช้บริการกับสถาบันการเงินไปนานแล้ว อาทิ การปิดบัญชี การยกเลิกสัญญาการทำธุรกิจต่างๆกับสถาบันทางการเงิน เว้นแต่พวกเขาจะให้ความยินยอมกับสถาบันการเงินเป็นการเฉพาะหรือข้อมูลของลูกค้าดังกล่าวนี้จะต้องให้ไว้กับสถาบันภายใต้การมีกฎหมายบังคับ รวมถึงการเก็บข้อมูลลูกค้าเพื่อวัตถุประสงค์ทางธุรกิจของสถาบัน เช่น ข้อมูลเครดิต ข้อมูลการทำสินเชื่อต่างๆ³⁷³

แต่อย่างไรก็ตามจากกรณีการดำเนินกระบวนการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของรัฐที่จำเป็นจะต้องอาศัยข้อมูลบางอย่างของสถาบันทางการเงินโดยเฉพาะอันเป็นข้อมูลของลูกค้าในหลายๆด้าน อาทิ ข้อมูลประวัติเจ้าของบัญชี ข้อมูลประวัติการทำธุรกรรมย้อนหลัง ข้อมูลการโอนหรือการได้รับมาซึ่งทรัพย์สิน ข้อมูลประเภทของทรัพย์สิน โดยทั้งนี้ก่อนสถาบันทางการเงินและ

³⁷³ ET Bureau Preeti Kulkarni, "Five basic rights for bank customers laid down," (Dec 22, 2014).

เอกชนผู้ให้บริการธุรกรรมทางการเงินจะได้มอบข้อมูลเหล่านี้ให้กับภาครัฐในการดำเนินการปราบปรามการก่อการร้าย สถาบันและเอกชนจะต้องแน่อนใจว่ารัฐมีกรอบกฎหมายในการคุ้มครองต่อการไม่ต้องรับผิด (Non-liability law) อันมาจากการที่สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินได้ปฏิบัติตามกรอบของกฎหมายในการส่งต่อซึ่งข้อมูลของลูกค้าเพื่อการดำเนินมาตรการป้องกันและปราบปรามการก่อการร้าย แต่ทั้งนี้การดำเนินการดังกล่าว สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินไม่มีอำนาจหน้าที่ในการดำเนินการนอกเหนือจากที่กฎหมายได้กำหนดไว้ หากสถาบันและบริษัทเอกชนได้ดำเนินการนอกเหนือจากการที่กฎหมายกำหนดนั้นถือว่าการละเมิดต่อสิทธิประโยชน์ของลูกค้า และหากเกิดความเสียหายต่อลูกค้าประการใด สถาบันการเงินและเอกชนดังกล่าวจำเป็นต้องมีมาตรการเยียวยาแก่ลูกค้าต่อไป³⁷⁴

4.3.2.2 การปฏิบัติตามข้อกำหนดการป้องกันการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย

สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินในหลายๆประเทศ แม้ว่าจะมีข้อตกลงในการปกป้องผลประโยชน์ของลูกค้าผู้รับบริการ แต่สถาบันและเอกชนกลับมีหน้าที่ที่จะต้องดำเนินการตามกฎหมายป้องกันและปราบปรามการฟอกเงินและการต่อต้านการก่อการร้าย โดยทั้งนี้ก็เพื่อเป็นประโยชน์ต่อสถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินที่จะไม่ตกเป็นเครื่องมือ หรือเป็นตัวกลางในการสนับสนุนการก่อการร้าย ในบรรดากฎหมายที่เกี่ยวข้องต่อการปราบปรามได้กำหนดให้สถาบันและเอกชนจะต้องตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence)³⁷⁵ แน่ใจว่าจะต้องรวมไปถึงการเก็บข้อมูลของลูกค้าเพื่อให้สถาบันสามารถระบุตัวตนและพิสูจน์ทราบตัวตนของลูกค้าได้ นำข้อมูลมาวิเคราะห์เพื่อจัดระดับความเสี่ยงด้านการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้าย และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูงของลูกค้า โดยอาจจะพิจารณาจากข้อมูลลูกค้า เช่น ประเทศ/สัญชาติ การประกอบธุรกิจ และการใช้ผลิตภัณฑ์ การรับบริการกับสถาบัน โดยทั้งนี้ในแต่ละครั้งของการตรวจสอบจะต้องได้รับอนุมัติจากผู้บริหารระดับสูงของธนาคาร หรือเจ้าหน้าที่ที่ได้รับการแต่งตั้งขึ้นเป็นการเฉพาะ ดำเนินการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า และการทบทวนข้อมูลลูกค้าอย่างสม่ำเสมอ

³⁷⁴ Isabel Frommelt Alyson J. K. Bailes, "Security and the responsibilities of the public and private sectors," in *Business and Security Public-Private Sector Relationships in a New Security Environment* (Oxford University Press, 2004).

³⁷⁵ Bangkok Bank, "Anti-Money Laundering and Counter Terrorism Financing (AML/CFT) Policy", Retrieved from <https://www.bangkokbank.com/en/About-Us/Corporate-Governance/Anti-Money-Laundering-Policy>

สถาบันและเอกชนจะต้องทำการรายงานหรือแบ่งปันซึ่งข้อมูลอันเป็นประโยชน์แก่การดำเนินการของหน่วยงานป้องกันและปราบปรามการฟอกเงิน รวมถึงการรายงานธุรกรรมที่มีเหตุอันควรสงสัย หรือรายงานข้อมูลอื่นใดที่เกี่ยวข้องของลูกค้าต่อหน่วยงานป้องกันและปราบปรามการฟอกเงิน ซึ่งขั้นตอนการรายงานหรือแบ่งปันข้อมูลจะถือเป็นความลับโดยที่จะไม่เปิดเผยให้กรรมการพนักงาน ลูกจ้าง ตัวแทนในการรับรู้ข้อเท็จจริง อย่างไรก็ตามในหลายสถาบันและเอกชนผู้ให้บริการได้กำหนดและชี้แจงถึงขั้นตอนในการดำเนินการเหล่านี้ ลงในเงื่อนไขการให้บริการทางการเงิน (Terms and conditions financial services) เพื่อทำความเข้าใจกับลูกค้าก่อนว่าสถาบันจำเป็นต้องดำเนินการกับข้อมูลของลูกค้าอย่างไรบ้าง

4.3.2.3 การเยียวยาความเสียหายต่อลูกค้า

ในกรณีที่สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินได้เปิดเผยข้อมูลของลูกค้า (Disclose information) โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล หรือมีกฎหมายและระเบียบข้อบังคับที่จะกำหนดให้ต้องเปิดเผยอันเป็นประโยชน์ต่อการดำเนินมาตรการปราบปรามการก่อการร้าย การกระทำเหล่านี้ถือว่าสถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินได้ละเมิดหน้าที่ของการเก็บข้อมูลความลับและผลประโยชน์ของลูกค้า (Violation of its duty of secrecy) สถาบันและเอกชนนั้นจะต้องให้การรับผิดชอบต่อความเสียหายทั้งสิ้นที่เกิดขึ้นแก่ลูกค้าผู้เป็นเจ้าของข้อมูล อย่างไรก็ตามกรณีการเปิดเผยข้อมูลลูกค้าของสถาบันการเงินในหลายประเทศนั้นพบว่าสถาบันการเงินให้จ่ายค่าความเสียหายและการเยียวยาเป็นจำนวนที่น้อยนิดมาก (Nominal damages) เพราะในการดำเนินกระบวนการยุติธรรมลูกค้าผู้เป็นเจ้าของข้อมูลอันที่ได้ถูกเปิดเผยจากสถาบันการเงินนั้น ไม่สามารถพิสูจน์ในชั้นศาลถึงความเสียหายทางการเงินที่เกิดอย่างแท้จริงของตน (Actual financial damage) และสถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินพยายามปฏิเสธความรับผิดชอบที่เกิดขึ้นอันอยู่นอกขอบเขตและอำนาจหน้าที่ของสถาบัน³⁷⁶

อย่างไรก็ตามในแนวปฏิบัติหลายประเทศมีการกำหนดระเบียบและข้อกำหนดของการดำเนินการให้บริการของสถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินว่าหาก ในกรณีที่สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินได้เปิดเผยข้อมูลของลูกค้า (Disclose information) โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล สถาบันและเอกชนดังกล่าวจะต้องแสดงความรับผิดชอบและดำเนินการให้มีมาตรการเยียวยาและทดแทนอันสอดคล้องกับข้อบังคับว่าด้วยความเสียหายตามสัญญา (Contract damage rule) ลูกค้าจะต้องได้รับการเยียวยาและทดแทนจากความ

³⁷⁶ Robert B. Wessling, "Banking: Disclosure of Records: The Duty of a Bank as to Customer Information," *Michigan Law Review* Vol. 60, no. 6 (Apr., 1962), <https://www.jstor.org/stable/1286777>

เสียหายที่เกิดขึ้นจากการละเมิดโดยตรง (Directly from breach) และความเสียหายได้เกิดขึ้นจากการละเมิดโดยอ้อม (Indirect injuries) โดยประเมินจากคาดการณ์ล่วงหน้าที่สมเหตุสมผล

ความเห็นของผู้เขียนสรุปได้ว่า มาตรการแบ่งปันข้อมูลเพื่อการปราบปรามแหล่งการเงินที่เกี่ยวข้องต่อการก่อการร้ายนั้นมีความจำเป็นอย่างมากที่จะต้องอาศัยข้อมูลจากผู้มีส่วนเกี่ยวข้องต่างๆ โดยเฉพาะสถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินที่เป็นเจ้าของข้อมูลการทำธุรกรรมทางการเงินที่อาจจะนำไปสู่การตรวจสอบและดำเนินบังคับใช้กฎหมายในการต่อต้านการก่อการร้าย ทั้งนี้สถาบันทางการเงินและเอกชนผู้ให้บริการธุรกรรมทางการเงินเองก็ควรจะต้องมีการดำเนินการคุ้มครองข้อมูลอันเป็นผลประโยชน์ของลูกค้ายจากการที่จะได้รับผลกระทบ ไปพร้อมกับการช่วยเหลือข้อมูลต่อภาครัฐในการดำเนินมาตรการต่อต้านการก่อการร้ายอย่างได้สัดส่วนและมีการกำหนดมาตรการเยียวยาที่ชัดเจนในกรณีที่เกิดความเสียหายแก่ลูกค้าผู้รับบริการ

4.3.3 ปัจเจกชน

4.3.3.1 ปัญหาด้านสิทธิความเป็นส่วนตัว

หากมองย้อนหลังไปในช่วงแรกระหว่างปี ค.ศ. 1999 – 2003³⁷⁷ ของข้อมติการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงมิได้ให้ความสำคัญของการดำเนินการต่อต้านการก่อการร้ายให้สอดคล้องกับพันธกรณีว่าด้วยสิทธิมนุษยชนเท่าที่ควร เพราะมีข้อสังเกตในทางกฎหมายว่าหากคณะมนตรีความมั่นคงได้ตัดสินใจรับรองข้อมติโดยดำเนินการภายใต้หมวดที่เจ็ดแล้วนั้น สถานะของพันธกรณีตามข้อมติดังกล่าวจะมีลักษณะที่เหนือกว่าพันธกรณีระหว่างประเทศอื่นๆ อันเป็นไปตามข้อที่ 103 ของกฎบัตรสหประชาชาติ (The prevailing character) ซึ่งไม่ได้บังคับใช้เฉพาะพันธกรณีตามกฎบัตรสหประชาชาติเท่านั้น แต่ยังรวมไปถึงคำตัดสิน ที่ถูกรับรองจากองค์กรที่มีอำนาจหน้าที่ตามกฎหมายประชาชาติอีกด้วย³⁷⁸

นั่นจึงหมายความว่ารัฐสมาชิกสหประชาชาติจะต้องปฏิบัติตามพันธกรณีตามข้อมติว่าด้วยการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงมาเป็นลำดับแรก จากพันธกรณีระหว่างประเทศ

³⁷⁷ "In addition to the limited levels of law enforcement and criminal justice cooperation in terrorism cases, there have been a number of well-publicized extrajudicial and unlawful counter-terrorism cooperation practices that have fallen short of key international human rights, rule of law and due process protections" *From* Anton du plessis, "A snapshot of international criminal justice cooperation against terrorism since 9/11," in *Counter-Terrorism Strategies in a Fragmented International Legal Order* (Cambridge University Press, July 2013).

³⁷⁸ Pierre-Marie Dupuy, "The Constitutional Dimension of the Charter of the United Nations Revisited," in *Max Planck Yearbook of United Nations Law Online* (01 Jan 1997).

อื่นๆ เช่น พันธกรณีในเรื่องสิทธิมนุษยชน³⁷⁹ และมากไปกว่านั้นไม่มีหน่วยงานระหว่างประเทศใดมีฐานอำนาจทางกฎหมายที่จะสามารถทำการพิจารณา (Judicial review) ถึงความชอบด้วยกฎหมาย (Legality) ของข้อมติว่าด้วยการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงได้ และเป็นที่ปฏิเสธไม่ได้อีกว่าข้อมติว่าด้วยการปราบปรามการก่อการร้ายมีส่วนในการสร้างผลกระทบต่อสิทธิของบุคคล ตัวอย่างถูกสะท้อนออกมาจากศาลยุติธรรมแห่งสหภาพยุโรป (Court of Justice of the European Union) ในคดี “Yassin Abdullah Kadi v. Council of the European Union and Commission of the European Communities” ซึ่งศาลชั้นต้น (the Court of First Instance) ได้มีความเห็นบางช่วงว่า “ด้วยตัวของคณะมนตรีความมั่นคงควรยึดถือความสอดคล้องตามบทบัญญัติพื้นฐานของหลักกฎหมายเด็ดขาด (The fundamental peremptory provisions of Jus cogens)” กล่าวคือแม้ว่าพันธกรณีของคณะมนตรีความมั่นคงจะมีสถานะที่เหนือกว่าพันธกรณีอื่น แต่ไม่ได้หมายความว่า จะอยู่เหนือหลักกฎหมายเด็ดขาด (Jus cogens) อันเป็นแนวทางเดียวกับการยึดถือปฏิบัติของรัฐในสังคมนานาชาติ และทั้งนี้เพื่อเป็นการปิดกั้นโอกาสที่จะใช้องค์การระหว่างประเทศในการหลีกเลี่ยงการปฏิบัติตามหลักกฎหมายเด็ดขาด³⁸⁰

อย่างไรก็ตามในทางกฎหมายแล้วศาล ECJ ในคดีนี้ไม่ได้มีฐานทางอำนาจในการพิจารณา ข้อมติคณะมนตรีความมั่นคงว่าชอบด้วยกฎหมายหรือไม่ และปัจจุบันยังไม่มียุติการระหว่างประเทศใดที่มีฐานอำนาจทางกฎหมายอย่างเป็นทางการในการพิจารณาความชอบด้วยกฎหมายของข้อมติคณะมนตรีความมั่นคง แม้กระทั่งศาลยุติธรรมระหว่างประเทศ (International Court of Justice) เองซึ่งเป็นองค์กรหลักของสหประชาชาติก็ได้มีฐานอำนาจที่ปรากฏทั้งในกฎบัตรสหประชาชาติและธรรมนูญศาลยุติธรรมระหว่างประเทศ (Statute of the International Court of Justice)³⁸¹

จุฬาลงกรณ์มหาวิทยาลัย

³⁷⁹ "As indicated previously, the obligations imposed by UNSC Resolutions would have priority over those derived from particular conventional law, in virtue of what is provided in Article 103 of the Charter" *From* Luis Miguel Hinojosa Martínez, "The Legislative Role of the Security Council in Its Fight against Terrorism: Legal, Political and Practical Limits," *The International and Comparative Law Quarterly* Vol. 57, no. 2 (Apr., 2008).

³⁸⁰ Andrea Bianchi, "Assessing the Effectiveness of the UN Security Council's Anti-terrorism Measures: The Quest for Legitimacy and Cohesion," *The European Journal of International Law* Vol. 17 no. 5 (2007).

³⁸¹ "Julian Arato มีความเห็นว่ามีเพียงคณะมนตรีความมั่นคงเท่านั้นที่จะอยู่ในสถานะที่จะกำหนดให้มีการทบทวนการตัดสินใจ (Decision) ของตัวเองหรือวินิจฉัยว่าคณะมนตรีความมั่นคงมีอำนาจสอดคล้องกับกฎบัตรสหประชาชาติหรือไม่ ลักษณะนี้สามารถเทียบเคียงอำนาจขององค์กรด้านตุลาการที่ว่า Compétence de la compétence หรือ Judicial Kompetenz-kompetenz" *ที่มาของความเห็น* : Julian Arato, "Constitutionality and constitutionalism beyond the state: Two perspectives on the material constitution of the United Nations," in *Oxford University Press and New York University School of Law* (2012).

ภายหลังจากการเกิดข้อถกเถียงของปัญหาผลกระทบด้านสิทธิมนุษยชนจากมาตรการต่อต้านการก่อการร้าย คณะมนตรีความมั่นคงแห่งสหประชาชาติมีการทบทวนปัญหาดังกล่าว และทำการปรับและรับรองข้อมติว่าด้วยการต่อต้านการก่อการร้ายเพิ่มเติมที่ได้พยายามเน้นย้ำว่า การดำเนินมาตรการต่อต้านการก่อการร้ายของเหล่ารัฐสมาชิกในทุกๆวิธีการนั้น (All means) จะต้องสอดคล้องกับพันธกรณีว่าด้วยสิทธิมนุษยชน โดยในบทที่สามที่ผ่านมาผู้เขียนได้กล่าวถึงพันธกรณีของรัฐสมาชิกสหประชาชาติในการดำเนินการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายตามมาตราต่างๆ จะสังเกตเห็นว่าการดำเนินการแบ่งปันข้อมูลบางอย่างนั้น ข้อมติของคณะมนตรีความมั่นคงแห่งสหประชาชาติได้มีการกำหนดชัดเจนว่า “การดำเนินการนั้นจะต้องสอดคล้องต่อพันธกรณีว่าด้วยสิทธิมนุษยชน” อาทิ การแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย หรือการแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้าย

ดังนั้นจึงชี้ให้เห็นว่าพันธกรณีของรัฐสมาชิกในการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้ายนั้น หลีกเลียงมิได้ที่จะไม่ปฏิบัติตามการพันธกรณีว่าด้วยสิทธิมนุษยชน โดยเฉพาะอย่างยิ่งพันธกรณีการแบ่งปันข้อมูลว่าด้วยการต่อต้านการก่อการร้ายนั้นโดยสารบัญญัติและวิธีดำเนินการ มีแนวโน้มว่าจะกระทบต่อสิทธิความเป็นส่วนตัวส่วนบุคคล (Right to privacy) จากการที่รัฐได้แบ่งปันข้อมูลตามมาตราดังกล่าวโดยอาศัยข้อมูลส่วนบุคคล หรือบุคคลที่สามทั้งที่อาจจะเกี่ยวข้องหรือไม่ได้เกี่ยวข้องต่อการก่อการร้าย มิว่าการแบ่งปันข้อมูลของรัฐนั้นจะอยู่ในลักษณะภายในประเทศหรือระหว่างประเทศก็ตามจำเป็นที่จะต้องสอดคล้องต่อพันธกรณีว่าด้วยสิทธิมนุษยชน จึงนำมาสู่เนื้อหาในหัวข้อนี้ที่จะวิเคราะห์และแจกแจงเงื่อนไขของคณะมนตรีความมั่นคงเองที่ได้กำหนดให้รัฐสมาชิกจะต้องเคารพพันธกรณีระหว่างประเทศว่าด้วยสิทธิมนุษยชนพร้อมกับการดำเนินการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้าย และแนวทางการปกป้องสิทธิความเป็นส่วนตัวส่วนบุคคลจากคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ

1. ปัญหาจากกระบวนการ

ภายหลังจากการออกข้อมติว่าด้วยการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติในช่วงหลังเหตุการณ์ก่อการร้ายสากลที่เกิดขึ้นในประเทศอเมริกา ในกระบวนการการดำเนินมาตรการต่อต้านการก่อการร้ายในหลายอย่างตามข้อมติของคณะมนตรีความมั่นคง ที่ถูกดำเนินการ (Implement) โดยเหล่ารัฐสมาชิกของสหประชาชาตินั้น ขาดไปซึ่งข้อกำหนดสำหรับการประเมินผลกระทบด้านสิทธิมนุษยชนอย่างครอบคลุม เพราะรัฐเหล่านั้นมีมุมมองว่าการมีอยู่ของการก่อการร้ายนั้นคือภัยคุกคามความมั่นคงของชาติ ดังนั้นกระบวนการการดำเนินมาตรการต่อต้านการ

ก่อนการร้ายจึงถูกสะท้อนของมาในประโยคที่ว่า “With us or with the terrorists”³⁸² กล่าวคือ หากต้องการจะมีสังคมที่ปราศจากการก่อการร้าย ประชาชนจะต้องให้ความร่วมมือจากการดำเนินมาตรการของรัฐ แม้ว่ากระบวนการในบางขั้นตอนจะกระทบต่อสิทธิของปัจเจกบุคคลอย่างบางก็ตาม

ในที่ประชุม “The First Security Council Open Debate on Counter Terrorism” ในวันที่ 18 January ปี ค.ศ. 2002 นายโคฟี อันนัน เลขาธิการแห่งสหประชาชาติในขณะนั้น (Secretary-General Kofi Annan) ได้ยื่นคำแถลงการณ์ต่อคณะมนตรีความมั่นคงแห่งสหประชาชาติกรณีที่มีการรับรองข้อมติว่าด้วยการต่อต้านการก่อการร้ายที่ 1373/2001 ข้อมติดังกล่าว เปิดช่องให้รัฐสมาชิกสามารถดำเนินกระบวนการปราบปรามการก่อการร้ายที่ก่อให้เกิดการลดทอนสิทธิมนุษยชน และขอเรียกร้องให้คณะมนตรีความมั่นคงและรัฐสมาชิกสหประชาชาติมีดำเนินมาตรการต่อต้านการก่อการร้ายในระยะยาวควบคู่ไปกับการเคารพหลักสิทธิมนุษยชนและความยุติธรรมตามสังคมนานาชาติ³⁸³

ทั้งนี้ นายโคฟี อันนัน เลขาธิการแห่งสหประชาชาติได้กล่าวถึงคณะกรรมการต่อต้านการก่อการร้าย ที่ถูกจัดตั้งตามข้อมติที่ 1373/2001 ควรจะต้องมีหน้าที่นอกเหนือการสังเกตการดำเนินตามข้อมติของบรรดารัฐสมาชิกแล้ว ยังควรจะต้องมีหน้าที่ในการประเมินการดำเนินการตามข้อมติของรัฐสมาชิกให้สอดคล้องต่อพันธกรณีว่าด้วยสิทธิมนุษยชน ซึ่งต่อมาภายหลังหนึ่งปีจากที่ประชุมการรับฟังปัญหาจากหน่วยงานภายในสหประชาชาติที่เกี่ยวข้องกับการดำเนินมาตรการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงที่อาจจะกระทบต่อเรื่องสิทธิมนุษยชนนั้น คณะมนตรีความมั่นคงแห่งสหประชาชาติได้รับรองข้อมติที่สำคัญคือ ข้อมติที่ 1456/2003 จึงมีสาระสำคัญดังต่อไปนี้

ประการแรก กล่าวคือมีการเรียกร้อง (Calls upon) บรรดารัฐสมาชิกต้องมีความแน่ใจว่า มาตรการต่างๆ ของตนที่ได้ดำเนินการเกี่ยวข้องต่อการต่อต้านการก่อการร้ายนั้นจะต้องสอดคล้อง (Comply) หรือมีพันธกรณีภายใต้กฎหมายระหว่างประเทศรับรอง อาทิ สนธิสัญญา อนุสัญญาว่าด้วยการต่อต้านการก่อการร้าย รวมถึงข้อมติของคณะมนตรีความมั่นคงในการต่อต้านการก่อการร้าย³⁸⁴

ประการที่สอง บรรดารัฐสมาชิกต้องมีความแน่ใจว่ามาตรการต่างๆ ของตนที่ควรนำมาใช้ต่อต้านการเกี่ยวข้องต่อการต่อต้านการก่อการร้ายนั้นจะต้องสอดคล้อง กฎหมายระหว่างประเทศ

³⁸² Human Rights Council, "Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders", from Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, (March 2019), pp. 5-10

³⁸³ Security Council, "The first security council open debate on counter terrorism", Addressing security council, secretary-general calls on counter-terrorism committee to develop long-term strategy to defeat terror, (18 January 2002), Retrieved from <https://www.un.org/press/en/2002/SC7276.doc.htm>

³⁸⁴ United Nations Security Council Resolution 1456/2003, pp 6

อาทิ กฎหมายสิทธิมนุษยชนระหว่างประเทศ กฎหมายมนุษยธรรมระหว่างประเทศ และกฎหมายว่าด้วยผู้ลี้ภัย

ดังนั้นในพันธกรณีในการแบ่งปันข้อมูลของรัฐสมาชิก ซึ่งถือว่าเป็นหนึ่งในมาตรการเพื่อการดำเนินการต่อต้านการก่อการร้าย จึงหลีกเลี่ยงมิได้ที่รัฐสมาชิกจะต้องปฏิบัติให้สอดคล้อง ตามการพันธกรณีว่าด้วยสิทธิมนุษยชน มากไปกว่านั้นคณะมนตรีความมั่นคงได้รับรองข้อมติที่ 2178/2014 ซึ่งเป็นข้อมติที่สะท้อนว่ามีผลผูกพันตามกฎหมายอย่างชัดเจน กล่าวคือข้อมติได้อำนาจตามกฎหมายว่าด้วยสิทธิมนุษยชนที่เข้มงวด และระบุว่าในความร่วมมือระหว่างประเทศ ผ่านการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายทั้งในรูปแบบความตกลงพหุภาคี หรือความตกลงทวิภาคี รัฐสมาชิกจะต้องดำเนินการตามพันธกรณีของตนภายในกฎหมายระหว่างประเทศ ขณะเดียวกันนั้นก็ต้องเคารพ ต่อกฎหมายสิทธิมนุษยชนระหว่างประเทศ และเสรีภาพขั้นพื้นฐาน

2. ปัญหาจากการบังคับ

ตามรายงานของ “Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism”³⁸⁵ ได้ยืนยันว่าการบังคับใช้มาตรการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้ายตามเหล่าข้อมติของคณะมนตรีความมั่นคง (Security Council-mandated information-sharing measures) โดยบรรดารัฐสมาชิกสหประชาชาติ ในบางรัฐมีการดำเนินการแบ่งปันข้อมูลในระดับระหว่างประเทศ หรือภายในประเทศ รวมทั้งมีการจัดเก็บข้อมูลบุคคลโดยหน่วยงานของภาครัฐดังกล่าวนี้มีแนวโน้มอย่างมากที่จะละเมิดพันธกรณีระหว่างประเทศว่าด้วยเรื่องสิทธิความเป็นส่วนตัว ตามกฎหมายสิทธิมนุษยชนระหว่างประเทศทั้งในรูปแบบของกฎหมายอย่างอ่อน หรือทั้งพันธกรณีระหว่างประเทศที่มีผลผูกพัน

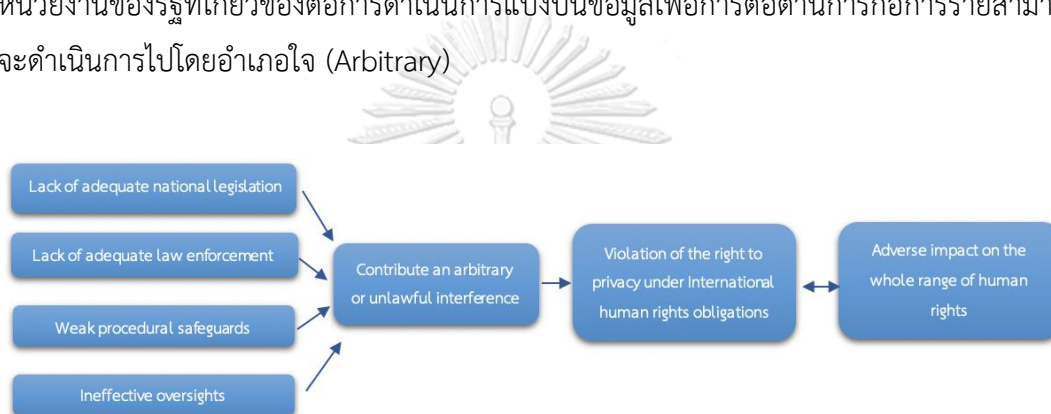
ตามบริบทของการบังคับใช้มาตรการของการแบ่งปันข้อมูลตามคณะมนตรีความมั่นคงนั้น มีส่วนที่จะสร้างให้เกิดการบุกรุกความเป็นส่วนตัว³⁸⁶ เช่น การดำเนินการบังคับใช้กฎหมายเพื่อเข้าถึงข้อมูลบุคคลอย่างมิชอบด้วยกฎหมาย และนำไปสู่การเกิดผลกระทบต่อการดำเนินการปกป้องสิทธิที่หลากหลาย ซึ่งในการดำเนินมาตรการต่อต้านการก่อการร้ายในหลายๆรัฐสมาชิกล้วน การแบ่งปันข้อมูลและจัดเก็บข้อมูลของบุคคลมิได้สอดคล้องต่อพันธกรณีของหลักการสิทธิมนุษยชน อาทิ พันธกรณีในการเคารพสิทธิความเป็นส่วนตัว (Obligation to respect) พันธกรณีในการปกป้องสิทธิ

³⁸⁵ United Nations Human Rights Council, "Information-sharing in the framework of preventing and countering terrorism and the concerns such measures present in relation to the protection and promotion of human rights with particular focus on the right to privacy", The Special Rapporteur on the promotion and protection of human rights (2017), p. 3-5

³⁸⁶ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (30 June 2014), pp. 47

ความเป็นส่วนตัว (Obligation to protect) และพันธกรณีในการเติมเต็มสิทธิความเป็นส่วนตัว (Obligation to fulfill)

โดยทั้งหมดนั้นเกิดจากการที่รัฐสมาชิกขาดไปซึ่งกฎหมายภายในชาติ (Lack of adequate national legislation) ที่บัญญัติให้มีการคุ้มครองต่อสิทธิความเป็นส่วนตัวอย่างเพียงพอ และขาดไปซึ่งการบังคับใช้กฎหมายภายในชาติ (Lack of adequate law enforcement) ที่เพียงพอต่อการคุ้มครองต่อสิทธิความเป็นส่วนตัว มากไปกว่านั้นบางรัฐสมาชิกมีขั้นตอนของการป้องกันการละเมิดสิทธิความเป็นส่วนตัวที่อ่อน (Weak procedural safeguards)³⁸⁷ และการกำกับดูแลการละเมิดสิทธิความเป็นส่วนตัวที่ไม่มีประสิทธิภาพ (Ineffective oversight) ซึ่งปัญหาเหล่านี้สามารถนำไปสู่การที่หน่วยงานของรัฐที่เกี่ยวข้องต่อการดำเนินการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้ายสามารถที่จะดำเนินการไปโดยอำเภอใจ (Arbitrary)



ข้อกังวลของทั้งสมาชิกใหญ่แห่งสหประชาชาติ และคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ ได้ระบุว่าสิทธิในความเป็นส่วนตัว ถือเป็นหลักการหนึ่งที่สำคัญของสังคมประชาธิปไตย และมีบทบาทที่เครื่องยืนยันถึงการใช้สิทธิเสรีภาพในการแสดงออกของบุคคล (Right to freedom of expression) ที่สามารถใช้สิทธิได้โดยปราศจากการแทรกแซง (Interference) รวมทั้งสิทธิอื่นที่เกี่ยวข้อง³⁸⁸ เช่น สิทธิที่จะมีเสรีภาพในการชุมนุมโดยสงบและการสมาคม (The rights to freedom of peaceful assembly) ดังนั้นหากมีการละเมิดสิทธิความเป็นส่วนตัว (Right to privacy) เสียแล้วจะส่งผลกระทบต่อสิทธิมนุษยชนทั้งปวง เช่น สิทธิในเสรีภาพและ

³⁸⁷ United Nations Human Rights Council, "Information-sharing in the framework of preventing and countering terrorism and the concerns such measures present in relation to the protection and promotion of human rights with particular focus on the right to privacy", The Special Rapporteur on the promotion and protection of human rights (2017), p. 3

³⁸⁸ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (23 March 2017), p. 1-5

ความปลอดภัยของร่างกาย (Right to liberty and security of person) หรือสิทธิในสุขภาพ (Right to health)

4.3.3.2 แนวทางการป้องกันทางกฎหมายและข้อเสนอแนะ

สิทธิในความเป็นส่วนตัว ในช่วงแรกของการพัฒนาแนวคิดในความเป็นส่วนตัวนั้น ก่อนจะได้ริเริ่มและรับรองไว้ในกฎหมายสิทธิมนุษยชนระหว่างประเทศภายหลังจากสงครามโลกครั้งที่สองในหลายประเทศมีการรับรองเอาไว้ในรัฐธรรมนูญอันเป็นกฎหมายที่สูงที่สุดในประเทศที่กล่าวถึงสิทธิของประชาชนโดยทั่วไป ซึ่งการรับรองสิทธิความเป็นส่วนตัว ในระบบกฎหมายภายใน ช่วงแรกสะท้อนให้เห็นว่ารัฐให้การการันตี ว่าบุคคลจะไม่ถูกรบกวนจากผู้บังคับใช้กฎหมายที่ผิดกฎหมาย การรบกวนต่อที่พักเคสสถาน การรบกวนต่อข้อความจดหมายโต้ตอบ หรือการค้นตัวบุคคลที่ปราศจากเหตุผลอันสมควร³⁸⁹

อย่างไรก็ตามภายหลังจากสงครามโลกครั้งที่สองแง่มุมของการรับรองสิทธิความเป็นส่วนตัว ในฐานะสิทธิมนุษยชนที่เป็นเสรีภาพขั้นพื้นฐาน ได้ถูกพัฒนาอย่างมีนัยยะสำคัญ กล่าวคือมุ่งคุ้มครองบุคคลในลักษณะที่เป็นเจ้าของร่างกาย หรือเจ้ากรรมสิทธิ์ที่อยู่อาศัยเพียงอย่างเดียว แต่ได้ขยายขอบเขตของการคุ้มครองไปถึง ชื่อเสียงของบุคคล พื้นที่ระยะห่างของบุคคลกับสังคม และมีการรับรองว่าความเป็นส่วนตัวเป็นศักดิ์ศรีของบุคคล มากไปกว่านั้นในยุคปัจจุบันซึ่งเป็นยุคของเทคโนโลยีสารสนเทศ ความเป็นเจ้าของข้อมูลของบุคคล หรือข้อมูลการทำกิจกรรมต่างๆผ่านเทคโนโลยีสารสนเทศก็ควรจะต้องได้รับความคุ้มครองเช่นกัน³⁹⁰ พันธกรณีระหว่างประเทศว่าด้วยสิทธิความเป็นส่วนตัว ได้ปรากฏอยู่ในตราสารระหว่างประเทศทั้งที่มีผลผูกพันทางกฎหมาย และไม่มีความผูกพันทางกฎหมายแต่ทั้งหมดก็ได้สร้างบรรทัดระหว่างประเทศว่าด้วยเรื่องของการปกป้องคุ้มครองสิทธิความเป็นส่วนตัวดังนี้

1. กฎหมายสิทธิมนุษยชนระหว่างประเทศ

กฎหมายสิทธิมนุษยชนระหว่างประเทศสามารถแบ่งออกเป็น 2 ประเภทหลักๆคือ กฎหมายสิทธิมนุษยชนที่มุ่งคุ้มครองสิทธิมนุษยชนทั่วไป (General international law on human rights) ซึ่งจะมุ่งการคุ้มครองไปที่เสรีภาพ ร่างกาย และความคิดของบุคคล เช่น สิทธิในการมีชีวิต สิทธิส่วนบุคคล เสรีภาพทางความคิดและความเชื่อทางศาสนา ตลอดจนสิทธิพลเมืองและสิทธิทางการเมืองต่างๆ อาทิ เสรีภาพทางความคิด และการแสดงออก เสรีภาพในการชุมนุมโดยสงบ และสิทธิในการมี

³⁸⁹ Maria Nicole Cleis Oliver Diggelmann, "How the Right to Privacy Became a Human Right," in *Human Rights Law Review* (Published by Oxford University Press, 7 July 2014).

³⁹⁰ Dunstan Allison-Hope, "The Right to Privacy, 70 Years On" (2018), Retrieved from <https://www.bsr.org/en/our-insights/blog-view/human-rights-to-privacy-70-years-on>

ส่วนร่วมในกิจการสาธารณะ ซึ่งจะแตกต่างจากกฎหมายสิทธิมนุษยชนที่คุ้มครองสิทธิมนุษยชนที่มีลักษณะเฉพาะเจาะจง (Specific international law on human rights)³⁹¹ ที่มุ่งเน้นการคุ้มครองไปที่เรื่องที่มีลักษณะเฉพาะเจาะจง หรือเป็นการดำเนินการและผลักดันของหน่วยงานระหว่างประเทศที่มีอำนาจหน้าที่ หรือความรับผิดชอบในเรื่องใดเรื่องหนึ่งโดยเฉพาะ อาทิ กฎหมายสิทธิมนุษยชนระหว่างประเทศที่ว่าด้วยการคุ้มครองความอยู่รอดของมนุษย์และการกระทำที่กระทบต่อศักดิ์ศรีแห่งความเป็นมนุษย์ กฎหมายสิทธิมนุษยชนระหว่างประเทศที่ว่าด้วยแรงงาน กฎหมายสิทธิมนุษยชนระหว่างประเทศที่ว่าด้วยผู้ลี้ภัย เป็นต้น

ดังนั้นจากที่ได้บรรยายไปในข้างต้นจะพบว่าสิทธิส่วนบุคคล นั้นได้ถูกคุ้มครองอยู่ภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศที่มุ่งคุ้มครองทั่วไป (General international law on human rights) ซึ่งจะสามารถพิจารณาข้อบทในตราสารระหว่างประเทศว่าด้วยสิทธิมนุษยชนเหล่านี้

- สิทธิความเป็นส่วนตัวตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights)

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนถูกยกร่างในระหว่างปี ค.ศ. 1946-1948 เมื่อถูกประกาศ จึงที่เป็นที่ชัดเจนว่าได้บัญญัติว่า สิทธิในความเป็นส่วนตัวถูกรับรองในความหมายของสิทธิมนุษยชนสากล เมื่อพิจารณาจะสังเกตได้ว่าข้อที่ 12 ยังคงรับรองถือแนวคิดพื้นฐานว่าด้วยความเป็นส่วนตัวคือบุคคลจะต้องไม่ถูกรบกวนโดยพลการจากภาครัฐต่อความเป็นส่วนตัว การรบกวนต่อที่พักเคหสถาน การรบกวนต่อข้อความจดหมายได้ตอบ ซึ่งได้ขยายกรอบคิดของคำว่าความเป็นส่วนตัวรวมถึงเกียรติยศและชื่อเสียงด้วย ในตอนท้ายของข้อที่ 12 จะได้รับรองอย่างชัดเจนว่า การปกป้องจากการรบกวนได้แสดงอย่างเป็นนัยยะว่ารัฐมีหน้าที่ในการเคารพเสรีภาพจากการถูกรบกวนของบุคคล³⁹²

- สิทธิความเป็นส่วนตัวตามกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights)

ข้อบทที่ว่าด้วยสิทธิความเป็นส่วนตัวในกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองถูกรับรอง หลังจากการประกาศปฏิญญาสากลว่าด้วยสิทธิมนุษยชนถูกยกร่างในระหว่างปีมากกว่า 17 ปี ในข้อที่ 17 ของกติกามีความแตกต่างจากข้อที่ 12 ของปฏิญญาสากลดังนี้

³⁹¹ ศารทูล สันติวาสะ, "กฎหมายสิทธิมนุษยชนในกฎหมายระหว่างประเทศ," in กฎหมายสิทธิมนุษยชน, ed. บรรณาธิการ รุ่งพงษ์ ชัยนาม (นนทบุรี : สำนักพิมพ์มหาวิทยาลัยสุโขทัยธรรมมาธิราช, พ.ศ. 2554).

³⁹² Oliver Diggelmann, "How the Right to Privacy Became a Human Right."

ซึ่งเมื่อสิ่งที่สามารถพิจารณาได้ถึงความแตกต่างอย่างชัดเจนระหว่างตราสารระหว่างประเทศที่ว่าด้วยเรื่องสิทธิความเป็นส่วนตัวทั้งสองฉบับนี้คือ ในกติกาไม่ได้มีข้อห้ามเรื่องการรบกวนโดยพลการ จากภาครัฐต่อความเป็นส่วนตัวเพียงอย่างเดียว แต่มีส่วนเพิ่มเติมมาอีกคือ การรบกวนโดยมิชอบด้วยกฎหมาย จากภาครัฐ ซึ่งสะท้อนให้เห็นว่ารัฐภาคีมีพันธกรณีที่จะต้องรับรองข้อกำหนดเกี่ยวกับการกระทำที่ผิดกฎหมายในการรบกวนสิทธิความเป็นส่วนตัว³⁹³ ทั้งกรณีที่บุคคลถูกรบกวนสิทธิความเป็นส่วนตัวจากการกระทำของหน่วยงานภาครัฐ หรือกรณีที่บุคคลถูกรบกวนสิทธิความเป็นส่วนตัวจากการกระทำของภาคเอกชน

ตามข้อวินิจฉัยที่ 16 ของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ (CCPR General Comment No. 16 - Article 17 Right to Privacy) นัยยะการตีความของคำว่า “ไม่ชอบด้วยกฎหมาย” ในข้อที่ 17 ของกติกาสากลนั้นหมายความว่า ต้องไม่มีการกระทำการรบกวน ใดๆเกิดขึ้น ยกเว้นเสียว่าการกระทำการรบกวนนั้นคาดได้ว่ากระทำไปตามกฎหมาย ซึ่งจะต้องเป็นกฎหมายที่ถูกตราขึ้นเพื่ออนุญาตให้มีการกระทำการรบกวนนั้นโดยเฉพาะ³⁹⁴ สังเกตได้จากข้อวินิจฉัยที่ใช้คำว่า “The law” การกระทำการรบกวนที่นอกเหนือจากกฎหมายกำหนดไว้เฉพาะ ถือว่าอยู่ในขอบเขตของคำว่า “ไม่ชอบด้วยกฎหมาย” ทั้งสิ้น

ดังนั้นจึงสามารถอธิบายได้ว่าการรบกวนสิทธิส่วนบุคคลที่ได้รับอนุญาตให้กระทำได้จากรัฐนั้น จะต้องกระทำภายในขอบเขตที่กฎหมายได้อนุญาตในเรื่องนั้นๆอย่างเฉพาะเจาะจง

ประการแรก กฎหมายการอนุญาตดังกล่าวนั้นจะต้องมีเปิดช่องให้เจ้าพนักงานรัฐมีการใช้อำนาจตามดุลยพินิจ (Discretion of decision-maker) ของตนมากเกินไปในการกระทำการรบกวนต่อสิทธิความเป็นส่วนตัว

ประการที่สอง กฎหมายการอนุญาตดังกล่าวนั้นจะต้องบัญญัติถึงรายละเอียดเงื่อนไขของสถานการณ์ (Precise circumstances) ที่จะมีการอนุญาตให้รัฐทำการรบกวนต่อสิทธิความเป็นส่วนตัว ซึ่งผู้ที่มีอำนาจตัดสินใจจะอนุญาตหรือไม่อนุญาตจะต้องเป็นไปตามที่กฎหมายกำหนดเท่านั้น และการกระทำการรบกวนต่อสิทธิส่วนบุคคลจะถูกพิจารณาเป็นไปตามรายกรณี (Case-by-case basis)³⁹⁵

³⁹³ Oliver Diggelmann and Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", *Human Rights Law Review* (Published by Oxford University Press, 7 July 2014), p 449-451

³⁹⁴ Human Rights Committee, "CCPR General Comment No. 16 - Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation" (8 April 1988), Available from <https://www.refworld.org/docid/453883f922.html>

³⁹⁵ Melissa Castan Jenny Schultz, Sarah Joseph,, "How the Right to Privacy Became a Human Right," in *Human Rights Law Review* (Published by Oxford University Press, 7 July 2014).

ประการสุดท้าย การออกกฎหมายอนุญาตจะต้องสอดคล้องต่อเป้าหมาย (Aims) และวัตถุประสงค์ (Objectives) ของบทบัญญัติข้อที่ 17 ของกติกาสากลด้วย

- การอนุญาตจำกัดสิทธิความเป็นส่วนตัว (Permissible limitations on right to privacy) การรบกวนต่อสิทธิความเป็นส่วนตัวของบุคคลสามารถทำได้เท่าที่กฎหมายระหว่างประเทศว่าด้วยสิทธิมนุษยชนในที่นี้คือกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ได้กำหนดว่า การรบกวนห้ามเป็นไปในกรณีที่ไม่ชอบด้วยกฎหมาย และห้ามเป็นไปโดยผลการ

คำว่า “ไม่ชอบด้วยกฎหมาย” ในข้อที่ 17 ของกติกาสากลนั้นหมายความว่า ต้องไม่มีการกระทำการรบกวนใดๆเกิดขึ้น ยกเว้นเสียว่าการกระทำรบกวนนั้นคาดได้ว่ากระทำไปตามกฎหมายซึ่งจะต้องเป็นกฎหมายที่ถูกตราขึ้นเพื่ออนุญาตให้มีการกระทำการรบกวนนั้นโดยเฉพาะ³⁹⁶ อย่างไรก็ตามในกรณีที่มีการอนุญาตให้มีการรบกวนสิทธิความเป็นส่วนตัวของบุคคลภายใต้กฎหมายภายในที่บัญญัติขึ้นการเฉพาะนั้นได้ขัดแย้ง กับบทบัญญัติ จุดมุ่งหมาย วัตถุประสงค์ ของกติการะหว่างประเทศ การอนุญาตให้มีการรบกวนสิทธิความเป็นส่วนตัวของบุคคลถือว่าเป็นไปโดยมิชอบด้วยกฎหมาย³⁹⁷

ส่วนคำว่า “โดยผลการ” ในข้อที่ 17 ของกติกาสากลนั้นหมายความว่า จะต้องไม่มีการอนุญาตให้มีการรบกวนสิทธิความเป็นส่วนตัวของบุคคลภายใต้กฎหมายภายในที่บัญญัติขึ้นการเฉพาะที่ไม่สอดคล้องกับบทบัญญัติ จุดมุ่งหมาย วัตถุประสงค์ ของกติการะหว่างประเทศ และการอนุญาตให้มีการรบกวนสิทธิความเป็นส่วนตัวของบุคคลจะต้องมีเหตุผลอันควรโดยพิจารณาจากสถานการณ์นั้นๆเป็นกาลเฉพาะ³⁹⁸

เมื่อพิจารณาจากบทบัญญัติในข้อที่ 17 ของกติกาสากลมิได้ระบุถึงประโยคที่ว่าด้วยการจำกัด (Limitations clause) อย่างแจ่มชัด ซึ่งการจะบอกแนวทางของการจำกัดสิทธิความเป็นส่วนตัวทั้งสองประการนั้นกล่าวคือ การจำกัดที่ชอบด้วยกฎหมาย และไม่เป็นไปโดยอำเภอใจ ถูกสร้างขึ้นในเอกสารที่ชื่อว่า “Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights” ซึ่งคณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติได้ร่างออกมาจากแนวปฏิบัติและข้อวินิจฉัย (CCPR General Comment) ซึ่งประกอบ

³⁹⁶ Human Rights Committee, "CCPR General Comment No. 16 - Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation" (8 April 1988), Available from <https://www.refworld.org/docid/453883f922.html>

³⁹⁷ United Nations Human Rights Council, "The right to privacy in the digital age", *Report of the Office of the United Nations High Commissioner for Human Rights* (30 June 2014), p. 21

³⁹⁸ Human Rights Committee, "CCPR General Comment No. 16 - Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation" (8 April 1988), pp.4, Available from <https://www.refworld.org/docid/453883f922.html>

ไปด้วย ข้อที่ 16, 27, 29, 34 และ 31 ตลอดจนสะท้อนออกมาจากการสังเกตแนวกฎหมายจากคดีพิพาทของประเทศและภูมิภาคจากมุมมองจากผู้เชี่ยวชาญ³⁹⁹ ซึ่งสามารถสรุปออกมาเป็นข้อดังต่อไปนี้

- การจำกัดต้องถูกกำหนดโดยกฎหมาย (Limitations shall be prescribed by law)

การจำกัดสิทธิความเป็นส่วนตัวจะต้องถูกกำหนดโดยกฎหมาย ซึ่งกฎหมายนั้นจะต้องเป็นกฎหมายที่บัญญัติการอนุญาตให้จำกัดไว้โดยเฉพาะ กฎหมายนั้นจะต้องสามารถเข้าถึงได้มีความชัดเจนและกำหนดสารบัญญัติตลอดจนวิธีการหรือกระบวนการอย่างละเอียดโดยที่บุคคลทั่วไปสามารถทราบถึงกระบวนการ และหน้าที่ความรับผิดชอบของเจ้าพนักงานตามที่บัญญัติได้ระบุไว้ถึงการมีอำนาจดำเนินการสอดส่องข้อมูล และขอบเขตของการดำเนินการภายใต้สถานการณ์เฉพาะ⁴⁰⁰ สุดท้ายกฎหมายการจำกัดนั้นจะต้องมีบทบัญญัติเกี่ยวกับการเยียวยาที่มีประสิทธิภาพ (Effective remedies) ในกรณีที่เกิดการจำกัดที่มีขอบด้วยกฎหมาย หรือเกิดการดำเนินกฎหมายที่ไม่เหมาะสม

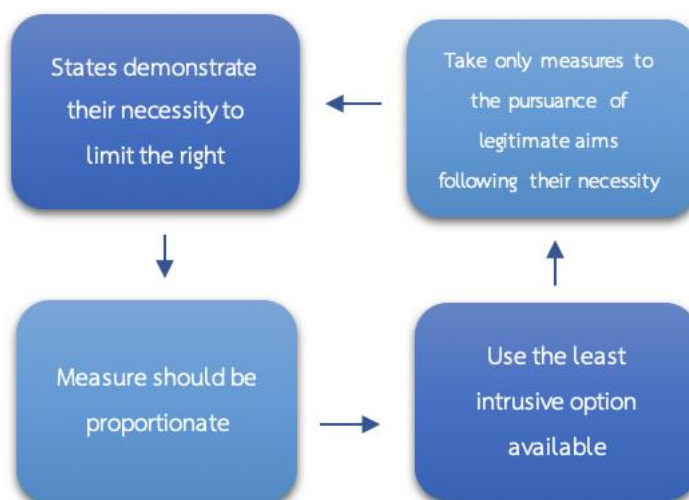
- การจำกัดต้องมีความจำเป็นและได้สัดส่วน (Limitations must be necessary and proportionate)

ในการจำกัดสิทธิความเป็นส่วนตัวตามกติกาสากล รัฐภาคีจะต้องแสดงให้เห็นถึงความจำเป็น (Necessity) ของการมาตรการจำกัดที่จะใช้ ตลอดทั้งรัฐภาคีจะต้องคำนึงถึงการดำเนินมาตรการที่จะต้องได้สัดส่วน (Proportionate) และสอดคล้องตามจุดมุ่งหมายที่ถูกต้อง (Legitimate aims) โดยการคำนึงถึงหน้าที่ของการปกป้องอันต่อเนื่องของสิทธิตามกติกาสากล หรือกล่าวอีกนัยหนึ่งได้ว่า มาตรการการจำกัดนั้นจะต้องมีความจำเป็น และการได้สัดส่วนของการใช้มาตรการ รัฐสมาชิกจะต้องเลือกใช้มาตรการที่คาดได้ว่าสมส่วนกับเหตุความจำเป็นของตน⁴⁰¹ และจะต้องดำเนินมาตรการนั้นบนการตัดสินใจว่าเป็นตัวเลือกที่พิจารณาแล้วว่าจะเกิดการถูกล้ำต่อสิทธิความเป็นส่วนตัวของบุคคลน้อยที่สุด

³⁹⁹ United Nations Human Rights Council, *The right to privacy in the digital age* (30 June 2014).

⁴⁰⁰ The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, I. Limitation Clauses

⁴⁰¹ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (30 June 2014), p. 23



มากไปกว่านั้นในการจำกัดสิทธิความเป็นส่วนตัว รัฐภาคีจะต้องกล่าวอ้างถึงความจำเป็นตามวัตถุประสงค์ในการดำเนินมาตรการที่ชอบด้วยกฎหมาย หรือวัตถุประสงค์ที่ถูกต้อง ของกติกาสากล รวมทั้งกฎหมายสิทธิมนุษยชนระหว่างประเทศอื่นๆ อาทิ เพื่อปกป้องความมั่นคงของชาติ ความปลอดภัยสาธารณะ ความสงบเรียบร้อยของประชาชน⁴⁰² สุขอนามัย ศีลธรรม หรือเพื่อเป็นไปในการปกป้องสิทธิมนุษยชนและเสรีภาพของบุคคลอื่น ทั้งนี้มาตรการการจำกัดสิทธิความเป็นส่วนตัวดังกล่าวจะต้องแสดงถึงความเป็นไปได้ ของการบรรลุซึ่งวัตถุประสงค์ในการดำเนินมาตรการปกป้องที่ได้กล่าวอ้าง⁴⁰³

- การห้ามเลือกปฏิบัติ (Prohibition of discrimination)

การจำกัดสิทธิความเป็นส่วนตัวจะต้องดำเนินการให้สอดคล้องต่อหลักการที่ว่าด้วยการไม่เลือกปฏิบัติ (Non-discrimination) ของกฎหมายสิทธิมนุษยชนระหว่างประเทศ⁴⁰⁴ หรือในกติกาสากล ข้อที่ 2.1 ได้บังคับหลักการไม่เลือกปฏิบัติใช้กับสิทธิเสรีภาพที่ถูกรับรองในกติกาตลอดทั้งการจำกัดสิทธิใดๆ โดยปราศจากการแบ่งแยกใดๆ อาทิ เชื้อชาติ ผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมือง หรือความคิดเห็นอื่นใด เผ่าพันธุ์แห่งชาติ หรือสังคม ทรัพย์สิน กำเนิด หรือ

⁴⁰² Australian human rights commission, "Permissible limitations on rights" (2020), retrieved from <https://humanrights.gov.au/our-work/rights-and-freedoms/permissible-limitations-rights>

⁴⁰³ Office of the United Nations High Commissioner for Human Rights, "Human Rights, Terrorism and Counter-terrorism Fact Sheet No. 32", (2003), p. 24, Retrieved from <https://www.refworld.org/docid/48733ebc2.html>

⁴⁰⁴ Australian human rights commission, "Lawful Limits on Fundamental Freedoms" (2020), retrieved from <https://humanrights.gov.au/our-work/publications/human-rights-brief-no-4>

สถานะอื่นๆ⁴⁰⁵ หากการจำกัดสิทธิส่วนบุคคลไม่สอดคล้องต่อหลักการที่ว่าด้วยการไม่เลือกปฏิบัติ ถือได้ว่าการจำกัดดังกล่าวมิชอบด้วยกฎหมาย และการรบกวนสิทธิส่วนตัวที่ได้กระทำไปนั้นถือว่ากระทำไปโดยพลการ

2. ข้อเสนอแนะของคณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติ

ในหัวข้อนี้ผู้เขียนจะอธิบายถึงข้อเสนอแนะของคณะกรรมการสิทธิมนุษยชนในการวางหลักปฏิบัติการปกป้องสิทธิความเป็นส่วนตัวในขณะที่รัฐรวมถึงเอกชนได้ดำเนินกิจกรรมที่เกี่ยวข้องต่อการแบ่งปันข้อมูลเพื่อการต่อต้านการก่อการร้าย ที่ผ่านมาในบทที่สามเรื่องพันธกรณีผู้เขียนได้แสดงให้เห็นว่ารัฐสมาชิกของสหประชาชาติมีหน้าที่จะต้องทำการแบ่งปันข้อมูลในรายการมาตรการต่างๆ ของการต่อต้านการก่อการร้ายอย่างไรบ้าง ซึ่งทั้งนี้ภาคเอกชนที่ได้ทำกิจการภายใต้เขตอำนาจของรัฐก็มีหน้าที่ที่จะต้องอำนวยความสะดวกบางอย่างที่จำเป็นต่อการดำเนินการต่อต้านการก่อการร้ายให้แก่ภาครัฐ ซึ่งการกระทำทั้งหมดของภาครัฐและเอกชนส่งผลต่อการกระทบต่อสิทธิความเป็นส่วนตัวส่วนบุคคลหรือเอกชนที่เป็นเจ้าของข้อมูลตามข้อกังวลของคณะกรรมการสิทธิมนุษยชนตามประเด็นในรายงานดังต่อไปนี้

- การแก้ไขปัญหาการเข้าถึงข้อมูลบุคคลจากเอกชนผู้ให้บริการโดยหน่วยงานของรัฐ

การแบ่งปันข้อมูลเพื่อยับยั้งการเข้าถึงแหล่งการเงินของการก่อการร้าย ได้ปรากฏว่าหน่วยงานของรัฐ อาทิ หน่วยข่าวกรองทางการเงิน หน่วยงานป้องกันและปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนเงินแก่การก่อการร้าย เจ้าหน้าที่อัยการหรือเจ้าหน้าที่ฝ่ายตุลาการ ได้ทำการแลกเปลี่ยนข้อมูลจากภาคเอกชน เช่น ข้อมูลการบริการสินทรัพย์เสมือน ข้อมูลการบริการกระเป๋าเงินดิจิทัล ข้อมูลการระดมทุนผ่านระบบอินเทอร์เน็ต โดยภาคเอกชน ผู้ให้บริการโทรคมนาคม ผู้ให้บริการกระเป๋าเงินดิจิทัล ผู้ให้บริการสินทรัพย์เสมือน

จากมาตรการดังที่กล่าวมานั้นได้เป็นข้อกังวลอย่างร้ายร้ายของคณะกรรมการสิทธิมนุษยชนว่าการแบ่งปันข้อมูลดังกล่าวระหว่างหน่วยงานของรัฐและเอกชน จะส่งผลต่อการละเมิด พันธกรณีที่จะต้องปกป้องสิทธิความเป็นส่วนตัวส่วนบุคคล ทั้งนี้ยังอาจจะก่อให้เกิดการกระทำที่หลีกเลี่ยง ต่อกระบวนการของการป้องกัน (Procedural safeguards)⁴⁰⁶ การละเมิดสิทธิความเป็นส่วนตัวส่วนบุคคล ในรายงานของคณะกรรมการสิทธิมนุษยชนได้ให้รายละเอียดบางส่วนว่า มีตัวอย่างของบางรัฐมีคำสั่งในทางบริหารต่อการขอเข้าถึงข้อมูลเหล่านี้จากการเก็บของภาคเอกชนผู้ให้บริการอย่างจำนวน

⁴⁰⁵ International Covenant on Civil and Political Rights, Article 2

⁴⁰⁶ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (3 August 2018), p. 13, 18

มาก ทั้งนี้รัฐได้กำหนดภาระหน้าที่เชิงบังคับให้ต่อภาคเอกชนผู้ให้บริการภายใต้เขตอำนาจของตน อาทิ บริษัทโทรคมนาคม และผู้ให้บริการอินเทอร์เน็ตในการเก็บรักษาข้อมูลส่วนบุคคลไว้เกินระยะเวลาที่ควรจะเป็น โดยในบางรัฐมีการออกกฎหมายเพื่อเรียกร้องให้ภาคเอกชนทำการรวบรวมและจัดเก็บข้อมูลของบุคคลทั้งหมดอย่างตามอำเภอใจ⁴⁰⁷ ต่อข้อมูลที่เกี่ยวข้องกับการสื่อสารทางอิเล็กทรอนิกส์ทุกรูปแบบซึ่งเกินความจำเป็นต่อการให้บริการของภาคเอกชน ทั้งนี้การกระทำดังกล่าวอาจสร้างความเสี่ยงของข้อมูลส่วนบุคคลที่อาจจะตกไปอยู่ในมือของบุคคลที่สาม เช่น อาชญากร ฝ่ายตรงข้ามทางการเมือง คู่แข่งทางธุรกิจ ทั้งนี้คำสั่งหรือกฎหมายดังกล่าวถูกพิจารณาว่าไม่เป็นไปตามหลักความจำเป็น และได้สัดส่วน

- การแก้ไขปัญหการจัดเก็บข้อมูลลักษณะเฉพาะตัวของบุคคล

ในพันธกรณีของการแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้าย หน่วยงานของรัฐรวมทั้งภาคเอกชน อาทิ ผู้ให้บริการสนามบิน หรือสายการบิน ได้พัฒนาระบบในการรวบรวมข้อมูลผู้โดยสารล่วงหน้า ข้อมูลการบินของผู้โดยสาร หรือข้อมูลลักษณะเฉพาะตัวของนักท่องเที่ยว อาทิ ข้อมูลชีวประวัติบุคคล และข้อมูลชีวภาพบุคคล เช่น ลายนิ้วมือ , ลายฝ่ามือ, ดีเอ็นเอ, รูปทรงใบหน้า, เสียง, จอประสาทตาเรตินา, รูปแบบม่านตา, การจดจำใบหน้า, สแกนร่างกาย, รูปทรงของมือ ทั้งนี้เพื่อเป็นไปตามวัตถุประสงค์ของการแบ่งปันข้อมูลเพื่อตรวจจับการเดินทางของผู้ก่อการร้ายตามมาตรการต่อต้านการก่อการร้ายของรัฐต่างๆ

ความกังวลของคณะมนตรีสิทธิมนุษยชนที่สะท้อนออกมาจากรายงานที่สังเกตการณ์ดำเนินการเช่นนี้ของบรรดารัฐสมาชิกสหประชาชาติว่าในบางประเทศได้บางประเทศได้สร้างฐานข้อมูลส่วนบุคคลขนาดใหญ่ ที่จัดเก็บข้อมูลดังกล่าวอย่างมากมาย และอำเภอใจ เพื่อวัตถุประสงค์อันหลากหลายที่รัฐได้กล่าวอ้างตั้งแต่ การต่อต้านการก่อการร้าย รักษาความมั่นคงแห่งชาติ การจัดการชายแดน และการสอบสวนทางคดีอาญาที่จะต้องการระบุตัวบุคคล ทั้งนี้รัฐได้ใช้ข้อมูลเหล่านี้เพื่อวิเคราะห์บุคคลผ่านการติดตั้งกล้องโทรทัศน์วงจรปิด ในสถานที่ เช่น เมืองใหญ่ สถานีรถไฟ หรือสนามบิน เพื่อจดจำใบหน้าบุคคลและระบุตัวตนของบุคคลอย่างอัตโนมัติได้ทันที⁴⁰⁸ สิ่งเหล่านี้สะท้อนออกมาเป็นรายงานของคณะมนตรีสิทธิมนุษยชนว่าด้วยเรื่องการละเมิดสิทธิความเป็นส่วนตัวของบุคคลจากการใช้เทคโนโลยีการจัดเก็บข้อมูลลักษณะเฉพาะตัวของบุคคล ซึ่งข้อมูลดังกล่าวมีความอ่อนไหวเป็นพิเศษ (Particularly sensitive) เนื่องจากมีความเชื่อมโยงอย่างแยกไม่ออกกับบุคคลใดบุคคลหนึ่ง และชีวิตของบุคคลนั้นมีโอกาสที่จะถูกล่วงละเมิดอย่างร้ายแรง ตัวอย่างเช่น การขโมย

⁴⁰⁷ Human Rights Committee, "Concluding observations on the initial report of South Africa", International Covenant on Civil and Political Rights Report, (27 April 2016), pp. 42-43

⁴⁰⁸ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (3 August 2018), p. 14

ข้อมูลประจำตัวโดยอาศัยข้อมูลทางชีวภาพ ถูกใช้เพื่อวัตถุประสงค์ในการติดตามและระบุตัวตนบุคคลที่ไม่ชอบด้วยกฎหมาย ซึ่งเป็นเรื่องยากมากที่จะเยียวยาความเสียหายและอาจส่งผลกระทบต่อสิทธิของแต่ละบุคคลอย่างร้ายแรง⁴⁰⁹

เมื่อพิจารณาถึงความเสียหายเหล่านี้ รัฐควรให้ความสนใจเป็นพิเศษกับมาตรการที่สอดคล้องต่อหลักการว่าด้วยความจำเป็นและการได้สัดส่วนในการรวบรวมข้อมูลไบโอเมตริกซ์ เมื่อเทียบกับข้อมูลภูมิหลังในรายงาน เป็นเรื่องที่น่ากังวลอย่างมากที่บางรัฐกำลังดำเนินมาตรการที่ใช้ข้อมูลไบโอเมตริกซ์จำนวนมากโดยไม่ได้มีการป้องกันทางกฎหมาย และขั้นตอนการปกป้องที่เพียงพอ

- การแก้ไขปัญหาการแบ่งปันข้อมูลข่าวกรองและพยานหลักฐาน

การแบ่งปันข้อมูลต่อมาตรการความร่วมมือระหว่างประเทศในกระบวนการยุติธรรม และการแบ่งปันข้อมูลเพื่อการดำเนินการบังคับในทางกฎหมายต่อการก่อการร้าย รัฐบาลในหลายประเทศได้จัดทำความร่วมมือระหว่างประเทศเพื่อแบ่งปันข้อมูลข่าวกรองที่เกี่ยวข้องของบุคคล นอกกรอบการควบคุมของกฎหมาย โดยปราศจากการกำกับดูแลที่เพียงพอ ทั้งในเรื่องของความร่วมมือระหว่างประเทศในกระบวนการดำเนินคดีอาญา การแบ่งปันข้อมูลของบุคคลที่อาจถูกใช้เพื่อเป็นพยานหลักฐานอิเล็กทรอนิกส์ หรือข้อมูลข่าวกรอง ภายใต้กรอบการดำเนินการมาตรการต่อต้านการก่อการร้ายที่อาจกระทบต่อสิทธิความเป็นส่วนบุคคลของบุคคล

การแบ่งปันข้อมูลดังเช่น พยานหลักฐานอิเล็กทรอนิกส์ หรือข้อมูลข่าวกรอง ภายใต้การดำเนินการมาตรการต่อต้านการก่อการร้าย การที่รัฐใช้วิธีการเช่นนี้นั้นมีแนวโน้มที่จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่รัฐอาจใช้เป็นแนวทาง เพื่อหลีกเลี่ยงข้อจำกัดทางกฎหมายภายในประเทศ อาทิ ในบางประเทศตามการรายงานของคณะมนตรีสิทธิมนุษยชน ได้ทำการรวบรวมข้อมูล หรือการวิเคราะห์ข้อมูล ที่ใช้เป็นข่าวกรอง หรือพยานหลักฐานในคดี โดยอาศัยเขตอำนาจของประเทศที่สามซึ่งมีการป้องกันสิทธิความเป็นส่วนตัวที่อ่อนแอ ทั้งยังมีการแลกเปลี่ยนข้อมูลผ่านช่องทางทางกฎหมาย⁴¹⁰ ของประเทศต้นทางของข้อมูลตลอดจนประเทศปลายทางของข้อมูลการกระทำทั้งหมดนั้นถูกชี้ว่ารัฐนั้นได้ล้มเหลวในการมีมาตรการที่มีประสิทธิภาพในการปกป้องบุคคลที่อยู่ภายใต้เขตอำนาจของตน จาก

⁴⁰⁹ United Nations Human Rights Council, "Information-sharing in the framework of preventing and countering terrorism and the concerns such measures present in relation to the protection and promotion of human rights with particular focus on the right to privacy", The Special Rapporteur on the promotion and protection of human rights (2017), p. 4-5

⁴¹⁰ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (30 June 2014), p. 28-30

การเข้าถึงข้อมูลที่ผิดกฎหมายโดยหน่วยงานรัฐ หรือหน่วยงานธุรกิจอื่นในการละเมิดพันธกรณีด้านสิทธิมนุษยชนว่าด้วยสิทธิความเป็นส่วนตัว⁴¹¹

การแบ่งปันข้อมูลข่าวกรองที่ไม่สอดคล้องกับกฎหมายและพันธกรณีระหว่างประเทศนั้นสะท้อนถึงปัญหาทางด้านการละเมิดสิทธิมนุษยชนอย่างร้ายแรงตามมา เช่น การละเมิดสิทธิมนุษยชนอย่างเป็นระบบโดยกระบวนการยุติธรรม ข่าวกรองที่รัฐหนึ่งได้รับจากอีกรัฐหนึ่งอาจตามมาด้วยการละเมิดกฎหมายระหว่างประเทศรวมถึงการซ้อมทรมาน และการปฏิบัติอื่น ๆ ที่โหดร้ายไร้มนุษยธรรมหรืออ่ำยศักดิ์ศรี (Other cruel, inhuman or degrading treatment)⁴¹² ความเสี่ยงต่อการละเมิดสิทธิมนุษยชนที่เกิดจากการแบ่งปันข่าวกรองนั้นเพิ่มสูงขึ้น จากการที่รัฐนั้นขาดความโปร่งใส ความรับผิดชอบ⁴¹³ และการกำกับดูแลจัดการการแบ่งปันข่าวกรองในปัจจุบันจึงจำเป็นที่รัฐจะต้องมี "Proper statutory footing" และสอดคล้องต่อหลักความชอบด้วยกฎหมายภายใต้กฎหมายสิทธิมนุษยชนระหว่างประเทศ⁴¹⁴

- การแก้ไขปัญหาการสอดแนมมวลชน (Mass surveillance)

การสอดแนมมวลชน หรือการสอดแนมชนิดที่แพร่หลายครอบคลุมประชากรทั้งหมดหรือครอบคลุมประชากรจำนวนมาก อาทิ การสกัดกั้นการสื่อสาร รวบรวม จัดเก็บ และวิเคราะห์ ข้อมูลของผู้ใช้ทั้งหมดที่เกี่ยวข้องกับวิธีการสื่อสารที่หลากหลาย เช่น ข้อมูลอีเมล ข้อมูลโทรศัพท์ และวิดีโอคอล ข้อความ และเว็บไซต์ที่เยี่ยมชม โดยส่วนใหญ่แล้วรัฐบาลมักเป็นผู้สอดแนม โดยมากจะลักลอบทำ แต่อาจจะมีการแจ้งบริษัทเอกชนภายนอก การสอดแนมนั้นอาจชอบด้วยกฎหมายหรือไม่ก็ได้ และอาจจำเป็นต้องอาศัยการให้อำนาจจากศาลหรือหน่วยงานอิสระอื่นหรือไม่ก็ได้ จากรายงานของคณะกรรมการสิทธิมนุษยชนการสอดแนมมวลชนโดยหน่วยงานของรัฐ มักอ้างความชอบธรรม ว่ามีความจำเป็นต้องทำเพื่อต่อต้านการก่อการร้าย เพื่อป้องกันไม่ให้เกิดความไม่สงบในสังคม รักษาความมั่นคง

⁴¹¹ General Assembly, *Promotion and protection of human rights and fundamental freedoms while countering terrorism* (23 September 2014).

⁴¹² United Nations Human Rights Council, "The right to privacy in the digital age", *Report of the Office of the United Nations High Commissioner for Human Rights* (3 August 2018), p. 21

⁴¹³ Human Rights Committee, "Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland", *International Covenant on Civil and Political Rights Report*, (17 August 2015), pp. 24

⁴¹⁴ Human Rights Committee, "Concluding observations on the seventh periodic report of Sweden", *International Covenant on Civil and Political Rights Report*, (28 April 2016), pp. 36

ของชาติ (National security) ปรากฏภาพโป๊เด็ก (Child sexual exploitation images) และ ปกป้องเด็ก⁴¹⁵

ในปัจจุบันการสอดแนมมวลชน ถูกวิพากษ์วิจารณ์อย่างกว้างขวางว่าละเมิดความเป็นส่วนตัว และจำกัดสิทธิพลเมืองและสิทธิทางการเมือง รวมทั้งผิดกฎหมายระหว่างประเทศหรือกฎหมายรัฐธรรมนูญ ซึ่งมีความกังวลว่าถ้าการสอดแนมมวลชนมีอัตราที่เพิ่มขึ้นเรื่อย ๆ ผลลัพธ์อาจนำไปสู่ การที่รัฐนั้นใช้อำนาจเผด็จการ ผู้คิดต่างทางการเมืองอาจจะถูกทำลายโดยปฏิบัติการสอดแนมมวลชน ซึ่งการปฏิบัติสอดแนมมวลชนในลักษณะต่างๆ⁴¹⁶ ถูกห้ามโดยกฎหมายสิทธิมนุษยชนระหว่างประเทศ เมื่อพิจารณาความจำเป็นเฉพาะ และวิเคราะห์สัดส่วนของการกระทำไม่ได้สอดคล้องต่อบริบทของใช้ มาตรการดังกล่าวเพื่อต่อต้านการก่อการร้าย รักษาความมั่นคง หรือความสงบเรียบร้อย ตามที่ศาล สิทธิมนุษยชนแห่งยุโรปได้เคยชี้ให้เห็นว่า "ระบบการสอดส่องอย่างลับๆที่สร้างขึ้นเพื่อปกป้องความ มั่นคงของชาติอาจบ่อนทำลายหรือทำลายระบอบประชาธิปไตย"⁴¹⁷

- การกำหนดกระบวนการการป้องกัน (Procedural safeguards)

การกำหนดกระบวนการการป้องกันปัญหาการละเมิดสิทธิส่วนบุคคล รวมทั้งการละเมิด ข้อมูลส่วนตัวของบุคคลนั้น ข้อเสนอแนะของคณะมนตรีสิทธิมนุษยชนคือรัฐจะต้องกำหนดมาตรการการ ป้องกันกิจกรรมที่เกี่ยวข้องกับการสอดส่องข้อมูลส่วนตัวของบุคคลทุกประเภท และจะต้องดำเนินการ บนพื้นฐานของกฎหมาย เป็นที่น่าสังเกตว่าในรัฐหลายประเทศ การเก็บ การใช้ การแบ่งปันซึ่งข้อมูล ส่วนบุคคลในการดำเนินงานของหน่วยงานข่าวกรอง หรือหน่วยงานบังคับใช้กฎหมายนั้นถูกกำหนด เป็นข้อยกเว้นในบทบัญญัติของกฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัวของข้อมูล อย่างไรก็ตาม รัฐจะต้องกำหนดขอบเขตของข้อยกเว้นที่ชัดเจน ควรจำกัดขอบเขตของข้อยกเว้นโดยสอดคล้องและ ยึดตามหลักการของความจำเป็น (Principles of necessity) และความเป็นสัดส่วน (Principles of proportionality)⁴¹⁸ ด้วยเหตุนี้ในการออกกฎหมายจึงต้องมีการอธิบายลักษณะของการกระทำ ความผิดที่ชัดเจน การให้เหตุผลที่คลุมเครือและกว้างเกินไป เช่น การกำหนดข้อยกเว้นของการเข้าถึง ข้อมูลส่วนบุคคลในกรณีที่เป็นไปเพื่อการรักษา “ความมั่นคงของชาติ” นั้น รัฐจะต้องแจกแจงคำ

⁴¹⁵ The Electronic Frontier Foundation, "Surveillance Technologies" (2020), Retrieved from <https://www.eff.org/issues/mass-surveillance-technologies>

⁴¹⁶ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (3 August 2018), p. 17

⁴¹⁷ "The European Court of Human Rights has pointed out, "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it" *from* Roman Zakharov v. Russia, para. 232.

⁴¹⁸ Accessnow, "A human rights response to government hacking" (September 2016), Available from <https://www.accessnow.org/cms/assets/uploads/2016/09/Gov-Hacking-Three-Pager.pdf>

จำกัดความของ “ความมั่นคงของชาติ” ในกฎหมายดังกล่าวนั้น มิฉะนั้นจะถือว่ากฎหมายดังกล่าว มิได้มีความชัดเจนที่เพียงพอ และการเข้าถึงข้อมูลส่วนตัวของบุคคลจะต้องอยู่บนพื้นฐานของความสงสัยที่สมเหตุสมผล (Reasonable suspicion)⁴¹⁹

- การกำหนดหน่วยงานในการให้อนุญาตและการกำกับดูแลที่เป็นอิสระ (Independent authorization and oversight)

การกำหนดหน่วยงานอิสระที่จะมาเป็นกลไกในการอนุญาตและการกำกับดูแล (Oversight bodies) ซึ่งการเข้าถึงข้อมูลส่วนบุคคล โดยหน่วยงานนี้จะต้องมีอำนาจหน้าที่ในการเข้าตรวจสอบและทบทวน ในทุกขั้นตอน ของการเข้าถึงข้อมูลส่วนบุคคลทั้งจากการดำเนินงานของหน่วยงานภาครัฐ อาทิ หน่วยงานบังคับใช้กฎหมาย และบริษัทเอกชน หน่วยงานอิสระที่จะมาเป็นกลไกในการอนุญาตและการกำกับดูแลการเข้าถึงข้อมูลส่วนบุคคลนั้น จะต้องถูกอาจจะจัดตั้งให้เป็นหน่วยงานที่อยู่ภายใต้กำกับของฝ่ายตุลาการ (Judicial oversight) หรืออยู่ภายใต้กำกับของฝ่ายนิติบัญญัติ (Parliamentary oversight)⁴²⁰ ทั้งนี้ก็เพื่อสร้างความมั่นใจว่าหน่วยงานดังกล่าวมีอิสระเพียงพอจากอำนาจฝ่ายบริหาร (Independent from administration) ทั้งนี้อำนาจหน้าที่ของหน่วยงานอาจจะถูกแบ่งออกเป็น 2 ลักษณะใหญ่ๆ คือ

1. อำนาจหน้าที่ในการอนุญาตต่อการเข้าถึงข้อมูลส่วนบุคคลทั้งจากหน่วยงานของรัฐและบริษัทภาคเอกชน และ

2. อำนาจหน้าที่ในการกำกับดูแลตรวจสอบแบบเชิงรุกและสังเกตการทำงานของคณะทำงานที่มีอำนาจในการเฝ้าระวังการละเมิดข้อมูลส่วนตัวของบุคคล ตลอดทั้งดำเนินการทบทวนอย่างเป็นระยะและพัฒนาความสามารถทางเทคโนโลยีในการเฝ้าระวังการละเมิดนั้น⁴²¹

หน่วยงานบังคับใช้กฎหมายของภาครัฐที่มีประวัติของการขอเข้าถึงข้อมูลส่วนตัวของบุคคล หรือการละเมิดข้อมูลส่วนตัวของบุคคล จะต้องรายงานข้อมูลการดำเนินการทั้งหมดที่จำเป็นและมีประสิทธิภาพเพียงพอสำหรับการตรวจสอบการกำกับดูแลข้อมูลส่วนบุคคล เมื่อมีการร้องขอเกิดขึ้น โดยให้หน่วยงานบังคับใช้กฎหมายจะต้องส่งรายงานต่อหน่วยงานกำกับดูแลข้อมูลส่วนบุคคลอย่าง

⁴¹⁹ United Nations Office on Drugs and Crime, "Unspecific references to national security", *International human rights and cyber crime law* (2020), Retrieved from <https://www.unodc.org/e4j/fr/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html>

⁴²⁰ United Nations Human Rights Council, "The right to privacy in the digital age", *Report of the Office of the United Nations High Commissioner for Human Rights* (3 August 2018), pp. 39-40

⁴²¹ United Nations General Assembly Resolution 71/199, pp. 5 (d)

รวดเร็ว มากไปกว่านั้นหากหน่วยงานบังคับใช้กฎหมายของภาครัฐ ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนตัวของบุคคลแล้วนั้น จะต้องเก็บบันทึกการดำเนินการของการเข้าถึงข้อมูลบุคคลและปฏิบัติตามมาตรการเฝ้าระวัง ที่ถูกกำหนดขึ้นโดยหน่วยงานกำกับดูแลข้อมูลส่วนบุคคลในทุกๆขั้นตอนของการดำเนินงาน

นอกจากนี้หน่วยงานกำกับดูแลข้อมูลส่วนบุคคล จะต้องดำเนินการกระบวนการกำกับดูแลที่โปร่งใส และอยู่ภายใต้การตรวจสอบข้อเท็จจริงของสาธารณชนที่เหมาะสม และอำนาจการตัดสินใจของหน่วยงานกำกับดูแลจะต้องมีกฎหมายเปิดช่องให้มีการขออุทธรณ์คำสั่ง หรือได้รับการตรวจสอบอย่างอิสระ

สุดท้ายคือการปฏิบัติตามหลักการว่าด้วยความโปร่งใส (Principle of transparency) เพื่อให้ประชาชนทั่วไปได้ทำการพิจารณา ทำความเข้าใจ ข้อดี และข้อจำกัดของการดำเนินงานของหน่วยงาน เช่น ผู้ที่เคยถูกละเมิดข้อมูลส่วนตัวควรได้รับการแจ้ง และได้รับคำอธิบายเหตุผลที่สมเหตุสมผลแก่พวกเขาเพื่อให้ทราบถึงความจำเป็นในการแทรกแซงสิทธิความเป็นส่วนตัวของพวกเขา พวกเขาควรมีสิทธิในการเปลี่ยนแปลง หรือลบข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้อง⁴²² หรือสิทธิที่จะขอให้ทำการลบซึ่งข้อมูลที่ไม่มีความจำเป็นอีกต่อไปในดำเนินการสอบสวนของหน่วยงานบังคับใช้กฎหมายในปัจจุบัน หรือในขั้นตอนระหว่างรอการดำเนินการ

- การเยียวยาเจ้าของข้อมูลผู้ถูกละเมิดสิทธิส่วนบุคคล

ผู้เสียหายต่อการละเมิดความเป็นส่วนตัว หรือการถูกละเมิดจากการกระทำโดยหน่วยงานของรัฐ หรือองค์กรธุรกิจ จะต้องสามารถเข้าถึงการเยียวยาที่ประสิทธิภาพ (Effective remedy) รัฐไม่เพียงแต่มีภาระหน้าที่ในการตรวจสอบความรับผิดชอบ และการแก้ไขปัญหาสำหรับการละเมิดสิทธิมนุษยชนที่กระทำโดยหน่วยงานของรัฐเท่านั้น แต่ยังรวมถึงการถูกละเมิดจากภาคธุรกิจด้วย ทั้งนี้รัฐจำเป็นต้องมีการกำหนดขั้นตอนทางกฎหมายเพื่อให้ผู้เสียหายที่ถูกภาคธุรกิจละเมิดสิทธิมนุษยชนสามารถเข้าถึงการเยียวยาที่มีประสิทธิภาพได้เช่นกัน⁴²³

ในแต่ละครั้งของกรณีการละเมิดข้อมูลส่วนบุคคลนั้น รัฐจะต้องมีกระบวนการของการตรวจสอบในลักษณะเฉพาะแต่ละกรณีไป ซึ่งผู้เสียหายจะต้องสามารถเข้าถึงการร้องขอการเยียวยาโดยอาจจะผ่าน กลไกการร้องทุกข์ที่ถูกกำหนดขึ้นโดยรัฐ (State-based grievance

⁴²² United Nations High Commissioner for Human Rights, "A Human Rights Based Approach to Data Leaving No One Behind in the 2030 Agenda for Sustainable Development", Guidance Note to Data Collection and Disaggregation (2019), Available from <https://www.ohchr.org/Documents/Issues/HRIIndicators/GuidanceNoteonApproachtoData.pdf>

⁴²³ United Nations Human Rights Council, "The right to privacy in the digital age", Report of the Office of the United Nations High Commissioner for Human Rights (3 August 2018), pp. 50-57

mechanisms)⁴²⁴ อาจจะไม่อยู่ในรูปแบบของกลไกที่อยู่ภายใต้อำนาจของศาล (Judicial mechanisms) หรืออาจจะไม่อยู่ภายใต้อำนาจศาล (Non-judicial mechanisms) ก็ได้ทุกนี้ขึ้นอยู่กับว่ากลไกนั้นถูกสร้างขึ้นมาให้มีความสามารถที่มีประสิทธิภาพเพียงพอในการเข้าตรวจสอบการละเมิดข้อมูลส่วนตัวและทำงานภายใต้บริบทของเทคโนโลยีการสื่อสารสารสนเทศ (Information Communication Technology context) หรืออาจมอบหมายหน้าที่ให้แก่หน่วยงานอิสระที่มีอำนาจในการตรวจสอบแนวทางปฏิบัติด้านความเป็นส่วนตัวของข้อมูลของรัฐและเอกชน เช่น หน่วยงานด้านความเป็นส่วนตัวและการปกป้องข้อมูล⁴²⁵ เป็นต้น

4.3.3.3 แนวปฏิบัติทางกฎหมายประเทศไทยในการปกป้องสิทธิความเป็นส่วนตัว

เมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 ประเทศไทยได้ผ่านกฎหมายฉบับหนึ่งคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 วัตถุประสงค์หลักของการบัญญัติกฎหมายนี้คือ เป็นเพิ่มความน่าเชื่อถือในมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ในเรื่องการค้าระหว่างประเทศ และการทำธุรกิจระหว่างประเทศ หากประเทศไทยจำเป็นต้องมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อเพิ่มโอกาสและความเชื่อมั่นจากต่างประเทศ และอาจรวมไปถึงประชาคมโลกที่กำลังตื่นตัวเรื่อง Data Protection⁴²⁶

อย่างไรก็ตามแม้ว่าชื่อของ "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562" เมื่อพิจารณาได้แล้ว สามารถคาดเดาได้ว่ากฎหมายฉบับนี้มุ่งเน้นไปที่ “การคุ้มครอง” ข้อมูลส่วนบุคคล แต่ใจความสำคัญของกฎหมายฉบับนี้ กลับมุ่งเน้นไปที่องค์กร หน่วยงาน หรือนิติบุคคลให้มี “มาตรฐาน” ในการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมและเพียงพอ เมื่อมีความจำเป็นต้องขอใช้ข้อมูลส่วนบุคคลของผู้บริโภค ทั้งนี้ก็เพื่อเป็นการป้องกันความเสี่ยงที่จะมีผลกระทบไปถึงการรักษา ความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูลส่วนบุคคล ที่ก่อให้เกิดแนวโน้มให้เกิดผลกระทบเชิงลบหรือความเสียหายในระดับบุคคลหรือองค์กร⁴²⁷

⁴²⁴ Human Rights Council, "Improving accountability and access to remedy for victims of business-related human rights abuse", Report of the United Nations High Commissioner for Human Rights (10 May 2016), pp. 1-7

⁴²⁵ Human Rights Council, "Improving accountability and access to remedy for victims of business-related human rights abuse through State-based non-judicial mechanisms", Report of the United Nations High Commissioner for Human Rights (14 May 2018), pp. 4-12

⁴²⁶ ACInfotec, "สรุปใจความสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ผู้ประกอบการควรรู้" (2019), Retrieved from <https://www.acinfotec.com/2019/07/23/data-protection-law-2562/>

⁴²⁷ สุนทรีย์ ส่งเสริม, "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562", สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (2018), Retrieved from https://www.bot.or.th/Thai/PaymentSystems/PSA_Oversight

1. สาระสำคัญและกระบวนการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประเด็นแรก ในมาตรา 23 และมาตรา 30 – 35 พระราชบัญญัติฉบับนี้ได้กล่าวถึงสิทธิของเจ้าของข้อมูล (Data subject right) อาทิ สิทธิที่จะต้องได้รับการแจ้งให้ทราบ (Right to be informed) สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล (Right of access) สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability) สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคล (Right to object) สิทธิในการขอให้ลบหรือทำลาย หรือขอให้ข้อมูลส่วนบุคคลของตนนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ (Right to erasure and right to be forgotten) สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to restrict processing) สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right to rectification) และสิทธิในการให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น กล่าวคือ ต้องขออนุมัติจากเจ้าของข้อมูลก่อน เช่น หากแอปพลิเคชันหนึ่งจะเก็บข้อมูลบัตรเครดิตของเราไว้ในระบบ ก็ต้องมีข้อความให้เรากดยืนยันเพื่อยินยอม พร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวม และการใช้ หากเราไม่ยินยอมให้ใช้ข้อมูลบัตรเครดิต ผู้ให้บริการแอปพลิเคชันนั้นก็ไม่สามารถใช้ข้อมูลบัตรเครดิตของเราได้

ประเด็นที่สอง ในมาตรา 37 ของพระราชบัญญัติฉบับนี้ได้กล่าวถึง หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (The Data Controller) มีหน้าที่ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Appropriate security measures) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวน มาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีนั้นได้เปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และผู้ควบคุมข้อมูลส่วนบุคคล (The Data Controller) จะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด ระยะเวลาการเก็บรักษาหรือลบข้อมูลที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม ซึ่งข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลนั้นร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลนั้นได้ถอนความยินยอม⁴²⁸

⁴²⁸ สำนักงานคุ้มครองข้อมูลส่วนบุคคล, "สรุปสาระสำคัญ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562" (2019), Available from

<http://www.oic.go.th/FILEWEB/CABINFOCENTER32/DRAWER083/GENERAL/DATA0000/00000166.PDF>

ประเด็นที่สาม ในมาตรา 40 ของพระราชบัญญัติฉบับนี้ได้กล่าวถึงผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ว่าจะต้องมีหน้าที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครอง ข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ ประการต่อมาคือการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Appropriate security measures) เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ รวมทั้ง แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และจัดทำและเก็บรักษาซึ่งบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

2. หน่วยงานที่ถูกกำหนดขึ้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ในการกำหนดมาตรฐานในการเก็บรวบรวมข้อมูล การใช้ และการเปิดเผยข้อมูลส่วนบุคคล รวมถึงให้ความรู้และฝึกอบรมเจ้าหน้าที่ภาครัฐ เอกชน และบุคคลทั่วไปให้มีความเข้าใจและสามารถรักษาข้อมูลส่วนบุคคลอย่างปลอดภัย โดยที่มาของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะเป็นไปตาม มาตรา 8 และ 9



อ้างอิงรูปภาพจาก : <https://www.mdes.go.th/mission/detail/2320-คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล>

โดยมาตรา 16 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ คณะกรรมการคุ้มครองฯ มีหน้าที่และอำนาจคือ⁴²⁹

⁴²⁹ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, "คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล" (2019), Retrieved from <https://www.mdes.go.th/mission/detail/2320-คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล>

- 1.) จัดทำแผนแม่บทการดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม
- 2.) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนแม่บทข้อ 1 รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนแม่บทดังกล่าว
- 3.) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามพระราชบัญญัติฯ
- 4.) ออกประกาศหรือระเบียบ เพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัติฯ
- 5.) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ
- 6.) ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ
- 7.) เสนอแนะต่อคณะรัฐมนตรีให้มีการตรา หรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- 8.) เสนอแนะต่อคณะรัฐมนตรีในการตราพระราชกฤษฎีกาหรือทบทวนความเหมาะสมของพระราชบัญญัติฯ อย่างน้อยๆรอบ 5 ปี
- 9.) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัติฯ
- 10.) ศึกษาค้นคว้าและวิจัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัติฯ
- 11.) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน
- 12.) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- 13.) ปฏิบัติการอื่นใดตามที่พระราชบัญญัติฯ หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการคุ้มครองฯ

3. ขอบเขตของการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติฉบับนี้ใช้บังคับแก่การให้ความคุ้มครองข้อมูลส่วนบุคคล (Personal Data) ตามมาตราที่ 6 ได้แก่ ข้อมูลที่เกี่ยวข้องดังต่อไปนี้ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ และไม่รวมข้อมูลของนิติบุคคล

เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล ฯลฯ

- | | |
|------|--|
| (1) | ชื่อ-นามสกุล หรือชื่อเล่น |
| (2) | เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาจะสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล) |
| (3) | ที่อยู่, อีเมล, เลขโทรศัพท์ |
| (4) | ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID |
| (5) | ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, พัลมเอกซ์เรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม |
| (6) | ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน |
| (7) | ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด, เชื้อชาติ, สัญชาติ, น้ำหนัก, ส่วนสูง, ข้อมูลตำแหน่งที่อยู่ (location), ข้อมูลการแพทย์, ข้อมูลการศึกษา, ข้อมูลทางการเงิน, ข้อมูลการจ้างงาน |
| (8) | ข้อมูลหมายเลขอ้างอิงที่เก็บไว้ในไมโครฟิล์ม แม้ไม่สามารถระบุไปถึงตัวบุคคลได้ แต่หากใช้ร่วมกับระบบดัชนีข้อมูลอีกระบบหนึ่งก็จะสามารถระบุไปถึงตัวบุคคลได้ ดังนั้นข้อมูลไมโครฟิล์มจึงเป็นข้อมูลส่วนบุคคล |
| (9) | ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง |
| (10) | ข้อมูลบันทึกต่างๆที่ใช้ติดตามตรวจสอบกิจกรรมต่างๆของบุคคล เช่น log file |
| (11) | ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่นในอินเทอร์เน็ต |

อ้างอิงรูปภาพ : Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

รวมไปทั้งข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data) ตามมาตรา 26 ข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ทั้งนี้ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

- | |
|--|
| (1) เชื้อชาติ |
| (2) เผ่าพันธุ์ |
| (3) ความคิดเห็นทางการเมือง |
| (4) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา |
| (5) พฤติกรรมทางเพศ |
| (6) ประวัติอาชญากรรม |
| (7) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต |
| (8) ข้อมูลสภาพแรงงาน |
| (9) ข้อมูลพันธุกรรม |
| (10) ข้อมูลชีวภาพ |
| (11) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด |

อ้างอิงรูปภาพ : Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

และพระราชบัญญัติฉบับนี้ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล 2 ลักษณะ คือ

1. บุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักร
 2. มีผลใช้บังคับถึงกรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร หากมี (1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่ (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร
4. การไม่ใช้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในมาตราที่ 4 ของพระราชบัญญัติได้วางข้อการไม่ใช้บังคับกฎหมายนี้กับกิจกรรมดังต่อไปนี้ คือ

- 1.) การเก็บรวบรวมใช้หรือเปิดเผยเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้น
- 2.) การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ (The duties to maintain state security) ความมั่นคงทางการคลังของรัฐ (Financial security of the state) การรักษาความปลอดภัยของประชาชน (Public safety) การป้องกันและปราบปรามการฟอกเงิน (The prevention and suppression of money laundering) นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)
- 3.) การเก็บรวบรวมเพื่อกิจการสื่อสารมวลชนงานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

4.) สภาผู้แทนราษฎร วุฒิสภา รัฐสภา คณะกรรมการ ตามอำนาจและหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา และคณะกรรมการ

5.) การพิจารณาพิพากษาคดีของศาล การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ การดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6.) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจ ข้อมูลเครดิต

5. วิเคราะห์กฎหมายของประเทศไทยกับข้อเสนอการคุ้มครองสิทธิส่วนบุคคล

ประเด็นการบังคับใช้ เมื่อพิจารณาการบังคับใช้กฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทยแล้วจะพบว่า กฎหมายดังกล่าวไม่ได้คุ้มครองข้อมูลที่เกี่ยวข้องต่อการดำเนินมาตรการซึ่งกับการรักษาความมั่นคงของรัฐ (The duties to maintain state security) การรักษาความปลอดภัยของประชาชน (Public safety) และป้องกันและปราบปรามการฟอกเงิน (The prevention and suppression of money laundering) ซึ่งไม่มีความชัดเจนในบทบัญญัติทางกฎหมายว่าข้อมูลส่วนบุคคลที่ใช้ในการดำเนินมาตรการต่อต้านการก่อการร้ายของหน่วยงานรัฐหรือการปราบปรามการก่อการร้ายของหน่วยงานรัฐนั้นได้อยู่ในขอบเขตของการบังคับตามกฎหมายนี้หรือไม่

อย่างไรก็ตามหากมีการใช้ดุลยพินิจของหน่วยงานบังคับใช้กฎหมายว่าข้อมูลส่วนบุคคลที่ใช้ในการดำเนินมาตรการต่อต้านการก่อการร้ายอยู่ในขอบเขตของการดำเนินมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงของรัฐ การรักษาความปลอดภัยของประชาชน และป้องกันและปราบปรามการฟอกเงิน ซึ่งเป็นข้อยกเว้นของการบังคับใช้กฎหมายฉบับนี้ คำถามต่อไปจึงมีอยู่ว่าการออกกฎหมายดังกล่าวมีการอธิบายลักษณะ หรือการให้เหตุผลที่คลุมเครือและกว้างเกินหรือไม่ ในกรณีการกำหนดข้อยกเว้นในการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่เป็นไปเพื่อการรักษา “ความมั่นคงของชาติ” ตามบัญญัติในกฎหมายนั้น ควรจะต้องแจกแจงคำจำกัดความของ “ความมั่นคงของชาติ” หรือไม่ เพื่อให้บทบัญญัติเกิดความชัดเจนที่เพียงพอและสมเหตุสมผลในการปฏิบัติงานของหน่วยงานบังคับใช้กฎหมาย และเป็นการกำจัดดุลพินิจของหน่วยงานบังคับใช้กฎหมาย โดยเฉพาะหน่วยงานที่มีอำนาจหน้าที่ในการเข้าถึงข้อมูลส่วนบุคคลเพื่อดำเนินมาตรการต่อต้านการก่อการร้าย

มากกว่านั้นมาตราที่ 4 ของพระราชบัญญัติฉบับนี้ไม่ได้บัญญัติถึงข้อมูลที่ทำเนิการโดยภาคเอกชนที่มีส่วนเกี่ยวข้องต่อการดำเนินการตามมาตรการที่การรักษาความมั่นคงของรัฐ การรักษาความปลอดภัยของประชาชน และป้องกันและปราบปรามการฟอกเงิน ซึ่งอาจจะหมายความรวมถึงมาตรการการปราบปรามการก่อการร้ายด้วย เพราะมาตรการแบ่งปันข้อมูลที่ได้รณธิบายมาในบทที่สามข้างต้นนั้นแล้ว จะพบว่าภาคเอกชนเองก็มีส่วนสำคัญในการเก็บ ใช้ วิเคราะห์ และแบ่งปัน

ข้อมูลทั้งที่เป็น ข้อมูลทั่วไป (General information) ข้อมูลส่วนบุคคล (Personal information) หรือข้อมูลที่มีลักษณะอ่อนไหว (Sensitive information) ให้แก่หน่วยงานของรัฐที่มีอำนาจในการปราบปรามการก่อการร้ายอยู่นั้นเอง ซึ่งสามารถตั้งคำถามต่อไปได้อีกว่าในมาตรการการใช้ข้อมูลส่วนบุคคลเพื่อดำเนินการต่อต้านการก่อการร้ายของรัฐ หากมีบริษัทเอกชนเข้าไปเป็นส่วนหนึ่งในกลไกของการดำเนินมาตรการต่อต้านการก่อการร้ายแล้วนั้น บริษัทเอกชนนั้นจะอยู่ภายใต้ข้อยกเว้นของมาตรา 4 ของพระราชบัญญัติคุ้มครองสิทธิส่วนบุคคลหรือไม่ เพราะโดยส่วนตัวผู้เขียนแล้วเมื่อพิจารณาที่ตัวบทกฎหมายก็ได้บัญญัติขอบเขตของการไม่ใช้บังคับในกรณีที่บริษัทเอกชนเป็นส่วนหนึ่งของกลไกการปราบปรามการก่อการร้าย หรือมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงของรัฐ (The duties to maintain state security) การรักษาความปลอดภัยของประชาชน (Public safety) และป้องกันและปราบปรามการฟอกเงิน (The prevention and suppression of money laundering) ดังนั้นบริษัทเอกชนนั้นจำเป็นต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอยู่นั้นเอง

ประเด็นของกระบวนการ เมื่อพิจารณาถึงสาระสำคัญและกระบวนการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะพบว่ามุ่งเน้นไปที่องค์กร หน่วยงาน หรือนิติบุคคลให้มี “มาตรฐาน” ในการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมและเพียงพอ เมื่อมีความจำเป็นต้องขอใช้ข้อมูลส่วนบุคคลของผู้บริโภค ทั้งนี้ก็เพื่อเป็นการป้องกันความเสี่ยงที่จะมีผลกระทบต่อ การรักษา ความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน ของข้อมูลส่วนบุคคล ที่ก่อให้เกิดแนวโน้มให้เกิดผลกระทบเชิงลบหรือความเสียหายในระดับบุคคลหรือองค์กร

นั่นหมายความว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะเน้นไปที่การควบคุมภาคธุรกิจไม่ให้ละเมิดข้อมูลส่วนบุคคลมากกว่าจะเป็นการควบคุมหน่วยงานของภาครัฐไม่ให้ละเมิดซึ่งข้อมูลส่วนบุคคล ทั้งนี้สังเกตได้จากการที่มาตรา 4 การไม่บังคับใช้พระราชบัญญัติในมาตรการที่เกี่ยวข้องกับการรักษาความมั่นคงของรัฐ การรักษาความปลอดภัยของประชาชน และป้องกันและปราบปรามการฟอกเงินมากกว่านั้นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่มีอำนาจตามกฎหมายฉบับนี้มีที่มาของการแต่งตั้งจากฝ่ายบริหาร ซึ่งถือว่าขาดคุณสมบัติความเป็นอิสระเมื่อพิจารณาตามหลักเกณฑ์ข้อแนะนำของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติในการให้ความคุ้มครองซึ่งสิทธิส่วนบุคคล จะพบว่าเงื่อนไขตามข้อแนะนำ คือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่จะมาเป็นหน่วยงานกำกับดูแลข้อมูลส่วนบุคคล จะต้องมิใช่บุคคลที่ถูกแต่งตั้งมาจากฝ่ายบริหาร แต่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนั้นจะต้องถูกออกแบบเหมือนเป็นกลไกอิสระ เช่น อาจมาจากการแต่งตั้งโดยอำนาจนิติบัญญัติ หรืออำนาจยุติธรรม เป็นต้น

ดังนั้นจึงสรุปได้ว่ากฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทยได้เน้นไปที่การออกแบบกลไกในการคุ้มครองข้อมูลส่วนบุคคลจากการกระทำที่เป็นการ

ละเมิดของภาคเอกชน และการกำหนดมาตรการฐานของบริษัทเอกชนในการเข้าถึงข้อมูลเสียมากกว่าจะเป็นกลไกในการคุ้มครองข้อมูลส่วนบุคคลจากการกระทำที่อาจเป็นการละเมิดจากหน่วยงานรัฐหรือหน่วยงานบังคับใช้กฎหมายที่อ้างการดำเนินการเพื่อรักษาความมั่นคงแห่งชาติ

4.3.4 ผลกระทบในมิติอื่นที่เกี่ยวข้องกับการแบ่งปันข้อมูล

การแบ่งปันข้อมูลได้เป็นกลไกที่ช่วยให้การบังคับใช้มาตรการปราบปรามการก่อการร้ายอื่นบรรลุซึ่งผลขึ้นมาได้ ซึ่งในมาตรการที่ได้มีการบังคับใช้เหล่านั้นบางมาตรการได้สร้างผลกระทบต่อบุคคลที่ถูกสงสัยว่าได้เกี่ยวข้องต่อการก่อการร้าย และภายหลังได้รับการพิสูจน์ว่าไม่มีส่วนเกี่ยวข้องกันแต่อย่างใด จึงนำมาสู่คำถามว่าคณะมนตรีความมั่นคงหรือรัฐเองที่บังคับใช้มาตรการเหล่านี้มีการคุ้มครองหรือมาตรการเยียวยาอย่างไร

4.3.4.1 ปัญหาของผู้ถูกกล่าวหาว่าเกี่ยวข้องกับก่อการร้ายโดยมิชอบ

ในมาตรการอายัดทรัพย์สินของกลุ่มก่อการร้าย กำหนดให้รัฐต้องให้ข้อมูลทรัพย์สินของบุคคล หรือข้อมูลบุคคลแก่คณะกรรมการลงโทษ เพื่อดำเนินการกำหนดรายชื่อบุคคลที่เกี่ยวข้องกับกลุ่มก่อการร้ายเพื่อการคว่ำบาตร (UN sanction list) และเพื่อหน่วยงานบังคับใช้กฎหมายของรัฐมีหน้าที่ดำเนินการอายัดเงินทุนและทรัพย์สินของบุคคลที่อยู่ในรายชื่อ ปัญหาได้เกิดขึ้นว่ามีกรณีของบุคคลที่ได้ปรากฏชื่ออยู่ในรายชื่อการคว่ำบาตร อันนำมาสู่การถูกดำเนินการบังคับกับทรัพย์สิน หรือนำมาซึ่งการสูญเสียชื่อเสียงโดยที่ตนไม่ได้รับการพิสูจน์ความบริสุทธิ์ตามกระบวนการยุติธรรมจากการที่รัฐนั้นได้อ้างถึงการมีหน้าที่จะต้องปฏิบัติตามพันธกรณีของคณะมนตรีความมั่นคงตามกฎหมายบัตรสหประชาชาติ กรณีที่เกิดขึ้น เช่น Liban Hussein ชื่อของเขาถูกปรากฏอยู่ในรายชื่อการคว่ำบาตร หลังจากเกิดเหตุการณ์วินาศกรรมก่อการร้ายที่นิวยอร์ก ทั้งนี้เขาถูกดำเนินมาตรการอายัดทรัพย์สินที่อยู่ในธนาคาร และในเวลาต่อมาปรากฏว่าชื่อของเขาถูกถอดออกจากรายชื่อคว่ำบาตรเพียงเพราะทางประเทศอเมริกาได้รับข้อมูลที่คลาดเคลื่อน⁴³⁰ Abousfan Abdelrazik เป็นชาวซูดาน (Sudanese) ที่มีสถานะเป็นพลเมืองแคนาดาได้ถูกควบคุมตัวโดยปราศจากการตั้งข้อกล่าวหาตามกฎหมายจากหน่วยงานบังคับใช้กฎหมายประเทศซูดานในขณะที่เขาเดินทางไปประเทศบ้านเกิด เพราะชื่อเขาได้

⁴³⁰ CanWest, "Canada: Government pay out of court settlement to falsely accused "terrorist" suspect" (October 2, 2003), Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/utflr62&div=6&g_sent=1&casa_token=

ปรากฏอยู่ในรายชื่อการคว่ำบาตร ทั้งยังถูกประเทศเจ้าของสถานะพลเมืองของเขาอย่างแคนาดา ปฏิเสธที่จะให้เดินทางกลับเข้ามาในประเทศ⁴³¹

จากกรณีดังกล่าวมาในข้างต้นนั้นหากภายหลังได้รับการพิสูจน์ว่าบุคคลเหล่านี้ไม่ได้มีส่วน เกี่ยวข้องกับการก่อการร้าย หรือชื่อของพวกเขาที่ได้ปรากฏในรายชื่อคว่ำบาตรมาจากข้อมูลที่มีความ คาดเคลื่อน ผลกระทบจากความผิดพลาดดังกล่าวที่ได้เกิดขึ้นกับบุคคลที่ได้ปรากฏอยู่ในรายชื่อเหล่านี้ ใครจะเป็นผู้รับผิดชอบ หรือจะได้รับมาตรการการเยียวยาจากใคร เพราะรัฐเองอาจกล่าวอ้างได้ว่า เป็นพันธกรณีที่จะต้องปฏิบัติและเป็นพันธกรณีที่อยู่เหนือพันธกรณีระหว่างประเทศในเรื่องอื่น แม้แต่ พันธกรณีด้านสิทธิมนุษยชน ประเทศที่เป็นผู้กำหนดรายชื่อการคว่ำบาตรได้กระทำในนามคำสั่งของ คณะมนตรีความมั่นคงที่อาศัยอำนาจตามหมวดที่เจ็ดมีผลผูกพันบรรดารัฐต่างๆ โดยที่คณะมนตรี ความมั่นคงมีความคึกักกันจากกระบวนการทางกฎหมายภายในทุกประเทศ จึงนำมาสู่แนวทางข้อเสนอ ของมาตรการเยียวยาบุคคลผู้ถูกกล่าวหาว่าเกี่ยวข้องกับก่อการร้ายโดยมิชอบ

4.3.4.2 ข้อเสนอสำหรับการเยียวยา

ในข้อเท็จจริงจากปัญหาที่เกิดขึ้นเหล่านี้สามารถศึกษาเป็นแนวทางเพื่อให้ข้อเสนอแนะการเยียวยา บุคคลผู้ได้รับความเสียหาย ประเด็นแรก แนวปฏิบัติของคณะมนตรีความมั่นคงคือไม่มีการกำหนด มาตรการอย่างเป็นทางการสำหรับการเยียวยาบุคคลผู้ถูกกล่าวหาว่าเกี่ยวข้องกับก่อการร้ายโดยมิชอบ หรือถูกกำหนดไว้ในรายชื่อการคว่ำบาตร ประเด็นที่สอง แนวปฏิบัติภายในบางประเทศได้กำหนดให้มี Ombudsperson เพื่อกำหนดการเยียวยาบุคคลที่ได้รับผลกระทบจากมาตรการอายัดทรัพย์สินตาม ข้อมติที่ 1267/1999 โดยศาลสูงสุดของสหราชอาณาจักรได้พิจารณาว่าดำเนินการตามข้อมติที่ 1267/2001 ในการกำหนดรายชื่อและอายัดทรัพย์สินบุคคลไม่มีความสอดคล้องกับหลักสุกษณิติ กระบวน (Due process)⁴³² อย่างไรก็ตามมีผู้ตั้งข้อสงสัยว่ากระบวนการเยียวยาของประเทศอังกฤษ เป็นการเยียวยาผู้รับผลกระทบจริง แต่หาใช่เป็นการเยียวยาข้อบกพร่องของกระบวนการกำหนด รายชื่อและอายัดทรัพย์สินบุคคล หรือแนวปฏิบัติของประเทศแคนาดาศาลสูงสุดมีมาตรการเยียวยา แก่บุคคลที่อยู่ในรายชื่อ แต่อย่างไรก็ตามชื่อของเขาไม่ได้ถูกลบจากรายชื่อการคว่ำบาตรของ สหประชาชาติอันเป็นผลให้ทางรัฐบาลแคนาดาจำเป็นต้องยึดอายัดทรัพย์สิน หรือระงับบัญชี ธนาคารของเขาต่อไป จนภายหลังชื่อของเขาได้ถูกลบออกจากรายชื่อการคว่ำบาตรของสหประชาชาติ

⁴³¹ Farnaz Mirshahi, "The UN 1267 Sanctions Regime: Due Process and Intelligence Evidence", A thesis submitted in conformity with the requirements for the degree of Masters in Law, (Faculty of Law University of Toronto, 2012), p. 25-27

⁴³² Jared Genser & Kate Barth, "When Due Process Concerns Become Dangerous: The Security Council's 1267 Regime and the Need for Reform" (2010)

โดยปราศจากการเยียวยาจากสหประชาชาติ แต่กลับเป็นศาลภายในประเทศแคนาดาเองที่ให้การเยียวยา

ในความเห็นของผู้เขียนมองเป็นประเด็นว่า คณะมนตรีความมั่นคงควรจะต้องมีมาตรการเยียวยาบุคคลที่ได้รับผลกระทบต่อการดำเนินมาตรการของตน อาจจะไม่เฉพาะเรื่องการก่อการร้าย แต่รวมถึงเรื่องอื่นๆด้วย โดนอาจจะกำหนดช่องทางการเยียวยาไว้ให้เป็นหน้าที่ของคณะกรรมการลงโทษที่ในปัจจุบันมีหน้าที่หลักคือควบคุมการดำเนินการตามข้อมติอย่างเดียว อาศัยกลไกการกำหนดช่องทางเยียวยาอื่นอย่างเช่น ปรับปรุงกระบวนการเยียวยาตาม 1503 Procedure ของคณะมนตรีสิทธิมนุษยชนให้มีอำนาจมากขึ้นในการเป็นช่องทางรับการเยียวยามากกว่าจะเป็นแค่ช่องทางการสื่อสารของรายบุคคล (Individual Communications) ประการที่สอง ประเทศที่ดำเนินมาตรการตามข้อมติคณะมนตรีความมั่นคงควรจะต้องคำนึงถึงผลกระทบที่อาจจะเกิดและควรกำหนดช่องทางการเยียวยาจากผู้ที่ได้รับผลกระทบ มากกว่าจะเป็นอ้างว่าเป็นหน้าที่ตามพันธกรณีที่จะต้องทำนั่นเอง



สรุปท้ายบท

เมื่อได้ทำการวิเคราะห์ในบทนี้จะได้ผลการวิเคราะห์ว่าปัญหาที่พบระหว่างการดำเนินมาตรการแบ่งปันข้อมูลของบรรดาระัฐสมาชิกทั้งในแง่ของกระบวนการในทางกฎหมายก็ดี และการบังคับใช้กฎหมายก็ดีประเด็นปัญหาเหล่านี้ที่ถูกรายงานออกมาจากรัฐหนึ่ง สามารถหยิบยกเป็นข้อพิจารณาให้แก่รัฐสมาชิกอื่นๆ ในการดำเนินมาตรการแบ่งปันข้อมูลให้ได้มีประสิทธิภาพภายใต้กรอบการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคง ในขณะที่เดียวกันนั้นประสบการณ์หรือแนวทางปฏิบัติการแก้ไขปัญหาของรัฐสมาชิกก็สามารถถูกพิจารณาเป็นตัวอย่างคำแนะนำหรือแบบอย่างในการช่วยเหลือการดำเนินมาตรการแบ่งปันข้อมูลของรัฐอื่นๆ ที่อาจประสบปัญหาอยู่ได้พบคู่ทางในการแก้ไขปัญหา

ตลอดจนข้อพิจารณาของการคำนึงถึงผลกระทบของภาคธุรกิจที่ทำการภายใต้เขตอำนาจของรัฐนั้นๆ จากในการดำเนินมาตรการต่อต้านการก่อการร้าย และผลกระทบขึ้นกับบุคคลที่สามซึ่งเป็นเจ้าของข้อมูลโดยมีการกำหนดการคุ้มครองและการแก้ไขปัญหายังไร รวมถึงการละเมิดซึ่งสิทธิความเป็นส่วนตัวของปัจเจกบุคคลโดยรัฐต้องมีแนวทางการปฏิบัติเพื่อการปกป้องตามพันธกรณีของกฎหมายสิทธิมนุษยชนระหว่างประเทศ ควบคู่ไปกับยึดปฏิบัติตามคำแนะนำของคณะมนตรีสิทธิมนุษยชนแห่งสหประชาชาติ

จากการศึกษาและวิเคราะห์มาในบทนี้ได้คำตอบให้กับข้อสมมุติฐานที่ได้ตั้งไว้ว่าการดำเนินมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายจะสามารถเกิดการบังคับไปได้อย่างมีประสิทธิภาพหรือไม่นั้น จำเป็นที่จะต้องอาศัยการกำหนดกระบวนการและกลไกภายในรัฐ เช่น หากรัฐไม่ได้มีกำหนดหน่วยงานที่เป็นกลไกในการดำเนินกระบวนการแบ่งปันข้อมูล กระบวนการแบ่งปันข้อมูลนั้นก็จะไม่เกิดการบังคับใช้อย่างมีประสิทธิภาพ อันจะนำไปสู่ผลกระทบต่อการ Take action ของมาตรการต่อต้านการก่อการร้ายต่างๆ ตามที่ได้ศึกษามา

บทที่ 5 บทสรุปและเสนอแนะ

บทสรุป

พันธกรณีในการแบ่งปันข้อมูลของคณะมนตรีความมั่นคงแห่งสหประชาชาตินั้นจะเกิดขึ้นโดยอาศัยความร่วมมือของรัฐสมาชิกในการตระหนักถึงปัญหาของภัยก่อการร้าย ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบต่อสังคมระหว่างประเทศ การดำเนินมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายนั้น รัฐใดรัฐหนึ่งจะกระทำการไปเพียงลำพังมิได้ ต้องอาศัยความร่วมมือกันเพื่อที่จะบรรลุผลในการปราบปรามการก่อการร้ายให้ไปได้ด้วยดี การแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายนั้นมิได้เพิ่งมาปรากฏอยู่ในบริบทของคณะมนตรีความมั่นคงแห่งสหประชาชาติเป็นครั้งแรก แต่ได้เคยปรากฏอยู่ในข้อบท (Provisions) ของตราสารระหว่างประเทศว่าด้วยการต่อต้านการก่อการร้ายอยู่แล้ว ตั้งแต่ช่วง ค.ศ. 1963 แต่ด้วยปัญหาขอบเขตของสารบัญญัติ และกระบวนการของการแบ่งปันข้อมูลที่มีได้มีความชัดเจนมากนัก ส่งผลให้เกิดช่องว่างให้รัฐบางรัฐกล่าวอ้างเพื่อที่จะมิให้ความร่วมมือทางข้อมูลเพื่อการต่อต้านการก่อการร้าย ตลอดทั้งตราสารระหว่างประเทศหลายฉบับพบว่าไม่ได้ถูกสนับสนุนในการเข้าร่วมเป็นภาคีจากรัฐในสังคมนระหว่างประเทศมากที่ควร หรือขาดไปซึ่งการสนับสนุนที่เป็นสากล (Universal supports) อาจด้วยเพราะปัจจัยทางกฎหมายต่างๆ อาทิ ความไม่ชัดเจนของปัญหาค่านิยมของการก่อการร้าย และการกำหนดกระบวนการบังคับที่ไม่มีประสิทธิภาพเท่าที่ควร

ปัญหาเหล่านี้นำมาสู่การบูรณาการเพิ่มเติมของมาตรการแบ่งปันข้อมูลในการต่อต้านการก่อการร้ายโดยสะท้อนออกมาจากข้อมติของคณะมนตรีความมั่นคงตั้งแต่ทศวรรษที่ ค.ศ. 1990-2020 คือ การที่คณะมนตรีความมั่นคงได้มุ่งให้รัฐสมาชิกดำเนินมาตรการต่อต้านการก่อการร้ายกันโดยอาศัยบทบาทของความร่วมมือ (Cooperation) หรือ การประสานงาน (Coordination) ระหว่างกัน ทั้งในระดับระหว่างประเทศ (International level) และระดับภายในประเทศ (Domestic level) มาตรการแบ่งปันข้อมูลภายใต้กรอบของการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคง ได้สร้างความชัดเจนในขอบเขตพันธกรณีของข้อมูลที่รัฐจะต้องดำเนินการแบ่งปัน มากไปกว่านั้นสารบัญญัติของข้อมูลมีขอบเขตที่กว้างมากขึ้นจากเดิมที่เคยถูกกำหนดในตราสารระหว่างประเทศ ในขณะที่เดียวกันก็มีความยืดหยุ่นต่อการนำข้อมูลเหล่านั้นไปปรับใช้ในการดำเนินมาตรการต่อต้านการก่อการร้ายในส่วนต่างๆ กระบวนการในมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงแห่งสหประชาชาติ มีการกำหนดเป็นที่ชัดเจนและเป็นขั้นตอนมากขึ้น ซึ่งมีการกำหนดกระบวนการของการบูรณาการร่วมกันระหว่างหน่วยงานภายในของรัฐที่มีอำนาจหน้าที่เฉพาะ ตลอดจนสร้างความร่วมมือกับบริษัทเอกชนให้เป็นหนึ่งผู้เกี่ยวข้องในกระบวนการแบ่งปันข้อมูล ยิ่งไป

กว่านั้นคณะมนตรีความมั่นคงมีความพยายามที่จะบูรณาการกลไกอื่นๆให้เข้ามาเป็นเครื่องมือส่งเสริมต่อกระบวนการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้าย โดยเครื่องมือเหล่านั้นอาจจะอยู่ในรูปของข้อเสนอแนะจากหน่วยงานระหว่างประเทศ องค์การระหว่างประเทศ เอกสารกำหนดมาตรฐานสากลหรือเครื่องมือ อาทิสถานข้อมูลขององค์การระหว่างประเทศต่างๆที่อาจมีบทบาทสำคัญให้การบูรณาการเพิ่มเติมกับการดำเนินมาตรการต่อต้านการก่อการร้าย

บทบาทนำในการดำเนินมาตรการปราบปรามการก่อการร้ายของคณะมนตรีความมั่นคงเป็นที่ปฏิเสธมิได้ว่ามีผลประโยชน์ทางการเมืองของประเทศมหาอำนาจที่เป็นสมาชิกถาวรของคณะมนตรีอยู่ ซึ่งในช่วงเริ่มแรกของการรับรองข้อมติต่างๆได้มุ่งเน้นไปเพียงเพื่อการปราบปรามการก่อการร้ายอย่างเข้มข้นโดยปราศจากการคำนึงถึงผลกระทบในด้านมิติอื่นๆ เช่น การเคารพต่ออำนาจอธิปไตยของรัฐ การเคารพในหลักการขั้นพื้นฐานที่ว่าด้วยสิทธิมนุษยชน จึงเป็นเหตุผลให้เลขาธิการแห่งสหประชาชาติซึ่งแต่เดิมมีบทบาทเพียงแคเป็นผู้เฝ้ามองและสังเกตการณ์มาโดยตลอดนั้น ได้ริเริ่มแนวคิดของการปฏิรูปสถาปัตยกรรมมาตรการต่อต้านการก่อการร้าย (Reform counter terrorism architecture) ให้สอดคล้องกับบริบทของการต่อต้านการร้ายที่เปลี่ยนแปลงไป ขณะเดียวกันก็คำนึงถึงผลกระทบในด้านมิติอื่นๆ จึงส่งผลมาสู่การดำเนินมาตรการแบ่งปันข้อมูลที่มีแนวทางที่สอดคล้องกับนโยบายการปฏิรูปสถาปัตยกรรมดังกล่าว วิเคราะห์ได้จากบทบาทของมาตรการแบ่งปันข้อมูลที่จะพบว่าคณะมนตรีความมั่นคงเองก็ยึดถือแนวปฏิบัติของการเคารพหลักการขั้นพื้นฐานที่ว่าด้วยสิทธิมนุษยชนดังที่ปรากฏให้เห็นในข้อมติหลายๆฉบับว่ามีการกำหนดให้บรรดารัฐต่างๆ ดำเนินมาตรการต่อต้านการก่อการร้ายโดยจะต้องสอดคล้องกับพันธกรณีระหว่างประเทศในด้านสิทธิมนุษยชนเสมอ ทั้งนี้ในเรื่องของกระบวนการของการแบ่งปันข้อมูล คณะมนตรีความมั่นคงกับหน่วยงานภายใต้การทำงานของคณะมนตรีเองก็ได้มีข้อเสนอแนะ หรือหลักการปฏิบัติที่เน้นชัดถึงการที่รัฐจะต้องกำหนดกระบวนการแบ่งปันข้อมูลที่เคารพต่อหลักสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลโดยยึดตามหลักการที่ว่าด้วยความจำเป็นและการได้สัดส่วนของการเข้าถึงข้อมูลส่วนตัวของบุคคล

การรับรองข้อมติเพื่อการปราบปรามการก่อการร้ายของคณะมนตรีความมั่นคงตามแนวคิด “Smart Sanctions” นั้นอธิบายได้ว่าหลังสงครามเย็นยุติ พัฒนาการของ Sanction ของคณะมนตรีความมั่นคงในช่วงปี ค.ศ. 1990 – ค.ศ. 1995 นั้นมีการดำเนินการ Sanction ที่มีลักษณะที่เรียกว่า “Global sanction” หรือ “Sanction แบบเบ็ดเสร็จ” ซึ่งสร้างผลกระทบมากมายโดยเฉพาะอย่างยิ่งในเรื่องของผลกระทบด้านมนุษยธรรม (Humanitarian consequences) ต่อประชากรที่อยู่ภายใต้การดำเนินการ Sanction นำมาสู่การเริ่มทดลองใช้มาตรการ “Smart sanction” ของคณะมนตรีความมั่นคง เช่น การกำหนดโครงการด้านการช่วยเหลือทางมนุษยธรรม หรือการยกเว้นการคว่ำบาตรสินค้าบางอย่างที่จำเป็นต่อการดำรงชีวิตของมนุษย์ จนถึงในช่วงปี ค.ศ. 2000 เป็นต้นมา แนวปฏิบัติในการลงโทษของคณะมนตรีความมั่นคงได้ยกเลิกการ Sanction แบบเบ็ดเสร็จ และแก้ไข

เปลี่ยนแปลงการ Sanction ให้เป็น “Targeted Sanction” หรือ “Smart sanction” มากขึ้นเพื่อหลีกเลี่ยงผลร้าย (Adverse consequences) ที่จะเกิดขึ้นกับประชากรโดยรวม เมื่อพิจารณากับข้อมติที่เกี่ยวข้องกับการต่อต้านการก่อการร้ายทั้งหลายแล้วนั้นจะพบว่าข้อมติเหล่านั้นมีลักษณะคำนึงถึงผลกระทบด้านมนุษยธรรม (Humanitarian consequences) ต่อประชากรโดยรวม ซึ่งสามารถพิจารณาได้จากการที่ข้อมติว่าด้วยการต่อต้านการก่อการร้ายนั้นได้มีลักษณะของการกำหนดเป้าหมาย (Targeted) ในการดำเนินมาตรการ เช่น การกำหนดรายชื่อบุคคลในการลงโทษทางการเงิน (Name lists of financial sanction) การห้ามเดินทางของบุคคลที่เกี่ยวข้องกับการก่อการร้าย (Targeted travel bans) ซึ่งแต่เดิมใน Sanction แบบเบ็ดเสร็จนั้นจะห้ามทุกวิธีการในการเดินทาง (Ban on all means of transportation)

หากจะพิจารณาต่อไปอีกว่ามาตรการแบ่งปันข้อมูลซึ่งถือเป็นกลไกหนึ่งของการต่อต้านการก่อการร้ายของคณะมนตรีความมั่นคงได้สอดคล้องกับแนวทาง “Smart Sanction” ของคณะมนตรีความมั่นคงหรือไม่นั้น ผู้เขียนวิเคราะห์ได้ว่าหากย้อนกลับไปพิจารณาที่ตัวข้อมติว่าด้วยการต่อต้านการก่อการร้าย (Counter Terrorism Resolutions) แล้วนั้น ไม่มีข้อมติใดเลยที่คณะมนตรีความมั่นคงได้ระบุว่าเป็นการใช้อำนาจตาม ข้อ 41 และ ข้อ 42 หรือระบุในข้อมติว่าเป็นการ Sanction เพราะคณะมนตรีระมัดระวังอย่างมากในการที่จะไม่ระบุข้อบทตามกฎบัตรลงไปในเรื่องข้อมติว่าดำเนินการต่อต้านการก่อการร้ายต่างๆ นั้นว่าได้ใช้อำนาจจากข้อบทใด แต่จะระบุอย่างกว้างๆ ในข้อมตินั้นๆ ว่าได้กระทำการภายใต้หมวดที่เจ็ด “Acting under Chapter VII of the Charter of the United Nations” ดังนั้นจึงมีคำถามต่อไปอีกว่าแล้วมาตรการแบ่งปันข้อมูลที่อยู่ในข้อมติว่าด้วยการต่อต้านการก่อการร้ายนั้นมีความเหมาะสม (Qualify) ที่จะเป็นการ Sanction หรือไม่ สามารถวิเคราะห์ได้ว่าแท้จริงแล้วนั้น “Sanction” เป็นคำที่ถูกเรียกขึ้นมาเองโดยพิจารณาจากการใช้อำนาจของคณะมนตรีความมั่นคง อย่างไรก็ตาม ข้อที่ 39, 41 และ 42 ในกฎบัตรก็มิได้ปรากฏถ้อยคำว่าเป็นการ Sanction เพียงแต่เป็นการดำเนินการให้การคุกคามต่อสันติภาพ (Threats to the Peace) หรือการละเมิดสันติภาพ (Breaches of the Peace) นั้นยุติหรือสิ้นสุดลง การกระทำอันคุกคามหรือละเมิดเหล่านั้นอาจจะเกิดขึ้นโดยการกระทำของรัฐเอง หรือตัวกระทำที่ไม่มีใช้รัฐ (Non-state actors) โดยมาตรการการแบ่งปันข้อมูลนั้นหัวใจหลักคือการทำให้รัฐสมาชิกมีความร่วมมือ (Cooperation) ต่อกันในการต่อต้านการก่อการร้ายซึ่งก็คือเป็นการดำเนินการชนิดหนึ่งตามกลไกของหมวดที่เจ็ด เพื่อที่จะให้การคุกคามต่อสันติภาพ (Threats to the Peace) ในที่นี้กล่าวคือภัยการก่อการร้ายนั้นยุติหรือสิ้นสุด ทั้งนี้สอดคล้องกับถ้อยคำของข้อที่ 39 ที่ระบุว่า “Shall make decide what measure to maintain or restore international peace and security” ซึ่งก็ถือได้ว่าความร่วมมือในการดำเนินมาตรการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายก็เป็นหนึ่งใน “Measure” ตามนัยของข้อ 39 ที่จะนำไปสู่การป้องกันและขจัดตัดตอนการก่อการร้าย ดังนั้น

มาตรการแบ่งปันข้อมูลจึงไม่ใช่การ Sanction แต่เป็นเพียงมาตรการหนึ่งภายใต้กลไกของหมวดที่เจ็ด ในการยุติภัยก่อการร้ายซึ่งจะต้องอาศัย “มาตรการ” (ซึ่งตรงกับข้อบทที่ 39 กฎบัตรสหประชาชาติใช้ คำว่า “Measure”) อันที่มีความหลากหลาย เช่น การลงโทษ (Sanction), ความร่วมมือ (Cooperation), การป้องกัน (Prevention), การตอบโต้ (Retaliation)

ส่วนประโยชน์ของมาตรการแบ่งปันข้อมูลที่เกิดขึ้นมานั้น ถูกสะท้อนออกมาจากการ ดำเนินการของรัฐ ซึ่งก่อให้เกิดช่องทางของการแบ่งปันข้อมูลใหม่ๆ ทั้งผ่านบทบาทของความร่วมมือ และการประสานงาน บรรดารัฐได้ข้อมูลสำคัญจากการแบ่งปัน และสามารถนำไปใช้เพื่อเสริมประสิทธิภาพ ของการดำเนินมาตรการการก่อการร้ายในแขนงต่างๆ อาทิ การแบ่งปันข้อมูลเพื่อนำข้อมูลนั้นไปเป็น พยานหลักฐานหรือข้อเท็จจริงในการดำเนินกระบวนการยุติธรรม ทั้งข้อมูลที่เป็นการสืบสวนสอบสวน หรือข้อมูลที่น่าไปเป็นพยานหลักฐานในการนำผู้กระทำความผิดเข้าสู่กระบวนการยุติธรรม ยิ่งไปกว่า นั้นในการแบ่งปันข้อมูลเส้นทางการเงินของบุคคลที่เป็นที่สงสัยหรือมีความเกี่ยวข้องว่าจะ เป็น ผู้ก่อการร้ายหรือผู้สนับสนุนการก่อการร้าย หน่วยงานบังคับใช้กฎหมายที่มีหน้าที่ให้การอายัดการเงิน สามารถดำเนินการบังคับโดยอาศัยจากการพิจารณาข้อมูลที่ได้จากการแบ่งปันระหว่างผู้มีส่วน เกี่ยวข้องทั้งหลาย อาทิ หน่วยงานของรัฐด้วยกันเอง ธนาคาร หรือบริษัทเอกชนที่ให้บริการด้าน การเงิน ตลอดทั้งการแบ่งปันข้อมูลของผู้เดินทางระหว่างประเทศนั้นสามารถที่จะเป็นประโยชน์ต่อ การตรวจจับการเดินทางของผู้ก่อการร้าย เครือข่ายการก่อการร้าย และข้อมูลนั้นสามารถที่จะช่วยให้ หน่วยงานที่มีหน้าที่บังคับตามกฎหมายได้ดำเนินการอย่างทันท่วงที

ดังนั้นแล้วมาตรการแบ่งปันข้อมูลมีวัตถุประสงค์สำคัญเพื่อให้รัฐสมาชิกสหประชาชาติ ร่วมมือกัน โดยที่รัฐไม่มีความจำเป็นที่จะต้องห่วงหาพันข้อมูลอีกต่อไป และประสิทธิภาพของมาตรการ การแบ่งปันข้อมูลเพื่อการป้องกันและปราบปรามการก่อการร้ายทั้งหมดจะเกิดขึ้นนั้น ก็ขึ้นอยู่กับ ความสามารถของบรรดารัฐต่างๆ ในการดำเนินการภายในรัฐ ตลอดทั้งมีความร่วมมือในการแบ่งปัน ข้อมูลในระดับระหว่างประเทศ

ข้อเสนอแนะ

1. ในการกำหนดกระบวนการของการแบ่งปันข้อมูลของบรรดารัฐต่างๆ ตามข้อมติของคณะ มนตรีความมั่นคงแห่งสหประชาชาตินั้น ในบางครั้งข้อมติดังกล่าวก็มิได้ระบุว่ารัฐจะต้องดำเนินกระบวนการ อย่างไรที่ชัดเจน จึงจำเป็นที่รัฐจะต้องอาศัยและยึดถือหลักเกณฑ์ของการกำหนดกระบวนการในทาง ปฏิบัติจากหน่วยงานที่มีความเกี่ยวข้อง หรือองค์กรระหว่างประเทศที่มีความเกี่ยวข้อง ซึ่งอาจจะได้ กำหนดออกมาอยู่ในรูปแบบของ ข้อปฏิบัติ (Practices) คำแนะนำ (Recommendation) หรือ หลักการ (Principle) ซึ่งเอกสารเหล่านี้ไม่มีสถานะผลผูกพันในทางกฎหมาย (Legal binding) แต่

ยังคงมีลักษณะเป็นกฎหมายแบบอ่อน (Soft law) ที่อาจจะสร้างบรรทัดฐานในการปฏิบัติต่อไปก็ได้ ทั้งนี้การปฏิบัติตามข้อแนะนำต่าง ๆ นั้นก็เพื่อจำกัดขอบเขตของรัฐในการใช้ดุลยพินิจในการกำหนดกระบวนการของการแบ่งปันข้อมูลที่อาจจะไปก่อให้เกิดกระทบต่อพันธกรณีระหว่างประเทศในด้านอื่น เช่น สิทธิของบุคคลที่เป็นเจ้าของข้อมูลอันนำไปสู่ปัญหาทางด้านสิทธิมนุษยชน

2. กระบวนการของการเข้าถึงข้อมูลบางอย่าง บรรดารัฐต่าง ๆ มีความจำเป็นอย่างมากที่จะต้องกำหนดหน่วยงานภายในรัฐตนที่มีอำนาจและหน้าที่ในการเข้าถึงข้อมูลเพื่อการต่อต้านการก่อการร้าย ซึ่งความจำเป็นของการกำหนดหน่วยงานเหล่านี้เสมือนไปเสริมกลไกของการแบ่งปันข้อมูลระหว่างหน่วยงานของรัฐเอง หรือระหว่างบริษัทเอกชนที่มีส่วนเกี่ยวข้อง เช่น ในมาตรการแบ่งปันข้อมูลเพื่อการตรวจสอบเส้นทางการเงินของการก่อการร้ายนั้น ผู้เขียนเห็นว่ารัฐควรที่จะกำหนดหน่วยข่าวกรองทางการเงิน (Financial intelligence unit) ซึ่งแยกอำนาจหน้าที่ออกมาจากหน่วยบังคับใช้กฎหมายในการอายัดการเงินของการก่อการร้าย (Counter-terrorist financing regulator) แต่ทั้งนี้หน่วยงานทั้งสองจะต้องทำงานภายใต้การบูรณาการร่วมกัน จะช่วยเสริมประสิทธิภาพของการดำเนินมาตรการแบ่งปันข้อมูลเพื่อการอายัดทางการเงินของการก่อการร้าย มากไปกว่านั้นรัฐอาจจะเลือกใช้เครื่องมือขององค์การระหว่างประเทศอื่น เช่น ฐานข้อมูลกลางของการองค์การตำรวจอาชญากรรมระหว่างประเทศเพื่อเป็นช่องทางตัวกลางในการแบ่งปันข้อมูลระหว่างประเทศ และสามารถเข้าถึงข้อมูลที่จำเป็นในการบังคับใช้กฎหมายซึ่งในปัจจุบันองค์การตำรวจอาชญากรรมระหว่างประเทศได้มีการพัฒนาฐานข้อมูลที่เกี่ยวข้องกับอาชญากรรมในหลากหลายรูปแบบโดยทั้งนี้รวมถึงการก่อการร้ายด้วย

3. ข้อเสนอต่อการกำหนดมาตรการเยียวยาต่อผู้ที่ได้รับผลกระทบจากการแบ่งปันข้อมูลเพื่อต่อต้านการก่อการร้ายจากผู้มีส่วนเกี่ยวข้องในกระบวนการทั้งที่เป็นภาครัฐและเป็นบริษัทเอกชน ผู้ที่ได้รับผลกระทบจะต้องมีช่องทางในการได้รับการเยียวยาที่มีประสิทธิภาพ รัฐและเอกชนไม่เพียงแต่มีภาระหน้าที่ที่จะต้องประกันความรับผิดชอบและการเยียวยาชดเชยสำหรับการละเมิดสิทธิของบุคคลที่สาม ในทางปฏิบัติแล้วบ่อยครั้งที่ผู้ที่ได้รับความเสียหายขาดองค์ความรู้ต่อการเข้าถึงขั้นตอนการเยียวยา จึงเสนอให้รัฐควรแจ้งต่อผู้ที่ได้รับผลกระทบจากการดำเนินมาตรการการแบ่งปันข้อมูลที่ได้สร้างความเสียหาย และแจ้งถึงขั้นตอนของการเยียวยาจากภาครัฐ เช่นเดียวกับกับบริษัทเอกชนที่ควรแจ้งให้ลูกค้าทราบเมื่อเกิดการละเมิดข้อมูลของลูกค้าจนเกิดความเสียหายและชี้แจงถึงกระบวนการของการเยียวยาและชดเชยจากบริษัท ทั้งนี้ก็ขึ้นอยู่กับว่าผู้ที่ได้รับกระทบหรือได้รับความเสียหายจะพอใจกับมาตรการเยียวยาหรือการชดเชยที่ได้รับหรือไม่ หากไม่ก็เป็นสิทธิของผู้ที่ได้รับผลกระทบในการดำเนินการทางกฎหมายต่อไป

บรรณานุกรม

- Alain Pellet, Alina Miron. "Sanctions." In *In the Max Planck Encyclopedia of Public International Law (Mpepil)* edited by Edited under the Direction of Rüdiger Wolfrum, 16: Published under the Auspices of the Max Planck Institute for Comparative Public Law and International Law, 2011.
- Alden, Edward. "No Entry: Tougher Visa Controls Are Creating Barriers to American Business." *Financial Times*, July 2, 2004. <https://www.ft.com/content/aa713a54-80a6-4117-83f8-3d610cd872e6>
- Altman, Daniel. "Uncertain Economy Hinders Highly Precise Supply System." *New York Times* March 15, 2003. <https://www.nytimes.com/2003/03/15/business/uncertain-economy-hinders-highly-precise-supply-system.html>.
- Alyson J. K. Bailes, Isabel Frommelt. "Security and the Responsibilities of the Public and Private Sectors." In *Business and Security Public-Private Sector Relationships in a New Security Environment*, 71-75: Oxford University Press, 2004.
- Arato, Julian. "Constitutionality and Constitutionalism Beyond the State: Two Perspectives on the Material Constitution of the United Nations." In *Oxford University Press and New York University School of Law*, 652, 2012.
- Bassiouni, M. Cherif. "The Weakness of Existing International Law in Addressing Terrorism", Legal Control of International Terrorism: A Policy-Oriented Assessment." *Harvard International Law Journal* Vol. 49 No. 1 (2002): 88-89.
- Bianchi, Andrea. "Assessing the Effectiveness of the Un Security Council's Anti-Terrorism Measures: The Quest for Legitimacy and Cohesion." *The European Journal of International Law* Vol. 17 no. 5 (2007).
- Biersteker, Thomas J. "Counter-Terrorism Measures Undertaken under Un Security Council Auspices." *Business and Security: Public-Private Sector* (2003): 71 <https://www.sipri.org/sites/default/files/files/books/SIPRI04BaiFro/SIPRI04BaiFro05.pdf>
- Blalock, Kadiyali, D.H. Simon, . "The Impact of Post-9/11 Airport Security Measures on

- the Demand for Air Travel." *Journal of Law & Economic* (2007): 50.
- Blank, Laurie. "Creating a More Effective Tool for the Enforcement of International Law." *Article from Emory University* (1995): 164-65.
- Carnero, Rosa Giles. "Terrorist Acts in the Configuration of the Threat to International Peace and Security." 2012.
http://rabida.uhu.es/dspace/bitstream/handle/10272/15562/TERRORIST_ACTS%20_AS_THREATS.pdf?sequence=2
- Catano, Victor, and Jeffery Gauger. "Information Fusion: Intelligence Centers and Intelligence Analysis." In *Information Sharing in Military Operations*, edited by ed. Anthony J, p. 17. Cham: Springer Nature, 2017.
- Chee, Foo Yun. "Twitter Suspended 166,153 Accounts for Terrorism Content in Second Half 2018." *REUTERS*, 2019. <https://www.reuters.com/article/us-twitter-security/twitter-suspended-166153-accounts-for-terrorism-content-in-second-half-2018-idUSKCN1SF1LN>
- Conforti, Benedetto. "International Law and the Role of Domestic Legal Systems." *American journal of international law* 88 (Martinus Nijhoff Publishers 1993): 34.
- Corera, Gordon. "Facebook Reveals Measures to Remove Terrorist Content." *BBC News*, 2017. <https://www.bbc.com/news/technology-40290258>
- Crail, Peter. "Report of Implementing Un Security Council Resolution 1540 and a Risk-Based Approach." *Nonproliferation Review* 13, no. 2 (July 2006): 378-79.
https://www.vertic.org/media/assets/nim_docs/background%20articles/Crail_risk-based%20assessment_1540.pdf
- Damjanović, Dragan Z. *Types of Information Warfare and Examples of Malicious Programs of Information Warfare*. Republic of Serbia, 2017.
- Dupuy, Pierre-Marie. "The Constitutional Dimension of the Charter of the United Nations Revisited." In *Max Planck Yearbook of United Nations Law Online* 11-15, 01 Jan 1997.
- Economides, Constantin P. "The Sources of International Responsibility - Obligations of Means and Obligations of Result - the Traditional Meaning of Obligations of Means or Conduct and Obligations of Result." In *The Law of International Responsibility*, edited by Alain Pellet Edited By James Crawford, Simon Olleson,

- Kate Parlett 375: Published Oxford Commentaries on International Law, 20 May 2010.
- Einsiedel, Sebastian von. "International Conventions in Assessing the Un's Efforts to Counter Terrorism." (October 2016): 1
- European Agency for Fundamental Rights. "Surveillance by Intelligence Services." *Fundamental Rights Safeguards and Remedies in the EU*. Vol. II: Field Perspectives and Legal Update, Luxembourg, Publications Office of the European Union (2017).
<https://www.statewatch.org/media/documents/news/2015/nov/eu-fra-2015-surveillance-intelligence-services.pdf>
- European Digital Rights. *The Slide from 'Self-Regulation' to Corporate Censorship*. (January 2011). www.edri.org/files/EDRI_selfreg_final_20110124.pdf
- Gabriel H. Oosthuizen, Elizabeth Wilmschurst. "Terrorism and Weapons of Mass Destruction: United Nations Security Council Resolution 1540." *Chatham House international law programme* (September, 2014): 2.
- General Assembly. *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*. (23 September 2014).
- Goh, Leanne. "Malaysia Will Set up Centre to Counter Is Propaganda." *Thestar.com.my*, 2015. <https://www.thestar.com.my/news/nation/2015/10/10/malaysia-will-set-up-centre-to-counter-is-propaganda>.
- Gold, David. "Economics of Terrorism - Economic Aspects of Fighting Terrorism." *Graduate Program in International Affairs New School University* (2015): 2.
https://www.files.ethz.ch/isn/10698/doc_10729_290_en.pdf
- . "Economics of Terrorism - Economic Aspects of Fighting Terrorism." In *Graduate Program in International Affairs New School University*, 4-5, 2015.
- Gómez, Juan Miguel del Cid. "A Financial Profile of the Terrorism of Al-Qaeda and Its Affiliates." *Perspectives on terrorism* 8, 4 (2010): 24.
- Gowlland-debbas, Vera. "Collective Security Revisited in Light of the Flurry over Un Reform an International Law Perspective." *International Law and the Quest for its Implementation* (2007): 251-77
- Gurin, Joel, Laura Manley, and Oleg Petrov. "New Discussion Paper: How Open Data Can

- Drive Sustainable Development." 34, no. 1 (2015): 11-18.
www.blogs.worldbank.org/digital-development.
- Happold, Matthew. "Security Council Resolution 1373 and the Constitution of the United Nations." In *Current Legal Developments - Leiden Journal of International Law* 596: under the Foundation of the Leiden Journal of International Law, 2003.
- Hausler, Kristin. "The Evolution Role of the United Nations Security Council and the Protection of Culture Heritage in the Event of Armed Conflict." 2018.
<http://www.qil-qdi.org/cultural-heritage-security-council-resolution-2347-matters>.
- Jacobson, Michael. "Terrorist Financing and the Internet." In *Studies in Conflict & Terrorism, Bruce Hoffman*, 354 Washington, D.C., USA, 2010.
- Jankowski, Barbara. "Information Sharing among Military Operational Staff: The French Officers' Experience." In *Information Sharing in Military Operations*, edited by ed. Anthony J., p. 73. Cham: Springer Nature, 2017.
- Jenny Schultz, Melissa Castan, Sarah Joseph.. "How the Right to Privacy Became a Human Right." In *Human Rights Law Review* 449-51: Published by Oxford University Press, 7 July 2014.
- KEATINGE, Tom. "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses." In *Director of the Centre for Financial Crime and Security Studies*, 21: Royal United Services Institute, 2018.
- Kinchin, Niamh. "According to Law in the Context of the Unsc's Targeted Sanctions, in Administrative Justice in the Un: Procedural Protections, Gaps and Proposals for Reform." Chap. Topic 6.2. Elgar Publishing, 2018.
- Marcinko, Marcin. "The Evolution of Un Anti-Terrorist Conventions Towards the Universal Treaty-Based Model of Combating Terrorism." *Groningen Journal of International Law* vol 6(1) of Terrorism and International Law (2014): 77.
- Martinez, Luis Miguel Hinojosa. "The Legislative Role of the Security Council in Its Fight against Terrorism: Legal, Political and Practical Limits." *The International and Comparative Law Quarterly* Vol. 57, no. 2 (Apr., 2008).
- Morphet, Sally. "Resolutions and Vetoes in the Un Security Council: Their Relevance and Significance." In *Review of International Studies*, 344-46: Published by

Cambridge University Press October, 1999.

Oliver Diggelmann, Maria Nicole Cleis. "How the Right to Privacy Became a Human Right." In *Human Rights Law Review* 441-43 Published by Oxford University Press, 7 July 2014.

pleassis, Anton du. "A Snapshot of International Criminal Justice Cooperation against Terrorism since 9/11." In *Counter-Terrorism Strategies in a Fragmented International Legal Order* 31: Cambridge University Press, July 2013.

Preeti Kulkarni, ET Bureau. "Five Basic Rights for Bank Customers Laid Down." Dec 22, 2014.

Rosand, Eric. "Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism." In *The American Journal of International Law* 97 No. 2 (Published by: Cambridge University Press, Apr ,2003): 333-34.

Schneider, Friedrich, Tilman, and Daniel,. "The Economics of Terrorism and Counter-Terrorism: A Survey." *Economics of Security Working Paper - German Institute for Economic Research* no. 45 (2011): 54.

Security Council. *Eighth Report of the Secretary-General on the Threat Posed by Isil (Da'esh) to International Peace and Security and the Range.* (2019).

———. *Fifth Report of the Secretary-General on the Threat Posed by Isil (Da'esh) to International Peace and Security and the Range.* (2017).

———. *Ninth Report of the Secretary-General on the Threat Posed by Isil (Da'esh) to International Peace and Security and the Range.* ((2019).

———. *Second Report of the Secretary-General on the Threat Posed by Isil (Da'esh) to International Peace and Security and the Range.* (2016).

Soeters, Joseph. "Information Sharing in Military and Security Operations." In *Information Sharing in Military Operations*, edited by ed. Anthony J., p. 5. Cham: Springer Nature, 2017.

United Nations General Assembly. *International Principles on the Application of Human Rights to Communications Surveillance.* (2014).

<https://en.necessaryandproportionate.org/text>

United Nations Human Rights Council. *The Right to Privacy in the Digital Age.* (30 June 2014).

United Nations Office on Drugs and Crime. *Basic Principles of International Cooperation against Terrorism*. (2009).

https://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/English.pdf

———. *The Practical Guide for Requesting Electronic Evidence across Borders*. (2019).

<https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html>

United States Department of State. *Country Reports on Terrorism 2019 - Thailand*.

(JUNE 24, 2020). <https://www.state.gov/wp-content/uploads/2020/06/Country-Reports-on-Terrorism-2019-2.pdf>

Vervaele, John A. E. "Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the Us and the Netherlands: Emergency Criminal Law?". (2005).

<https://www.utrechtlawreview.org/articles/10.18352/ulr.1>

Wakabayashi, Daisuke. "Youtube Sets New Policies to Curb Extremist Videos." *The New York Times*, 2017. <https://www.nytimes.com/2017/06/18/business/youtube-terrorism.html>

Waqas. "Twitter Suspends 125,000 Accounts for Promoting Terrorist Acts." In *Hackread Cyber Security Intelligence*, 2016.

Wessling, Robert B. "Banking: Disclosure of Records: The Duty of a Bank as to Customer Information." *Michigan Law Review* Vol. 60, no. 6 (Apr., 1962).

<https://www.jstor.org/stable/1286777>

Woodward, John. *A Former Cia Operations Officer, "Biometrics: Facing up to Terrorism*. (2001).

Yuen, Stacey. "Terror Financiers Are Using Social Media Propaganda" (December, 2017), Cnbc News." <https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html>

ดวงเด่น นาคสีหราช. หลักกฎหมายระหว่างประเทศแผนกคดีเมือง. พิมพ์ครั้งที่ 2: กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, ปี พ.ศ. 2562.

ทิพวันต์, นาดยา. "ข้อมติขององค์การระหว่างประเทศในฐานะที่เป็นบ่อเกิดของกฎหมายระหว่างประเทศ." วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, พ.ศ. 2534.

นาคสีหราช, ดวงเด่น. หลักกฎหมายระหว่างประเทศแผนกคดีเมือง. Edited by พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: สำนักพิมพ์วิญญู

ชน, ปี พ.ศ. 2562.

นาดยา ทิพวันต์. ข้อคิดขององค์การระหว่างประเทศในฐานะที่เป็นบ่อเกิดของกฎหมายระหว่างประเทศ. วิทยานิพนธ์ นิติศาสตรมหา
บัณฑิต มหาวิทยาลัยธรรมศาสตร์, พ.ศ. 2534.

มดิชน. ครม.เห็นชอบร่างความตกลงของดีเอสไอเข้าถึงฐานข้อมูลตำรวจสากล ยกกระดับบังคับใช้กฎหมายระหว่างประเทศ. (กุมภาพันธ์
2564). https://www.matichon.co.th/politics/news_2593283.

———. "ครม.เห็นชอบร่างความตกลงของดีเอสไอเข้าถึงฐานข้อมูลตำรวจสากล ยกกระดับบังคับใช้กฎหมายระหว่างประเทศ."

กุมภาพันธ์ 2564. https://www.matichon.co.th/politics/news_2593283

ร้อยตำรวจเอกเมือง พรหมเกษา. "สถานะเหนือกว่าของพันธกรณีตามกฎหมายระหว่างประเทศต่อพันธกรณีตามข้อตกลง ตามกฎหมายระหว่าง
ประเทศอื่น : กรณีศึกษาข้อคิดคณะมนตรีความมั่นคงว่าด้วยการต่อต้านการก่อการร้ายและคำวินิจฉัยของศาลยุติธรรมแห่ง
สหภาพยุโรป." วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2555.

วิลาสินี หมายเจริญศรี. "การเข้าเป็นภาคีสันธิสัญญาว่าด้วยการค้าอาวุธ ค.ศ. 2013 ของประเทศไทย : ปัญหาและลู่ทาง." จุฬาลงกรณ์
มหาวิทยาลัย, พ.ศ. 2559.

ศารทูล สันติवासะ. "กฎหมายสิทธิมนุษยชนในกฎหมายระหว่างประเทศ." In กฎหมายสิทธิมนุษยชน, edited by บรรณาธิการ รุ่ง
พงษ์ ชัยนาม: นนทบุรี : สำนักพิมพ์มหาวิทยาลัยสุโขทัยธรรมาราช, พ.ศ. 2554.

สายเชื้อ, สุทธิพร. "ปัญหาและอุปสรรคในการดำเนินการตามมาตรการในพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงิน
แก่การก่อการร้าย พ.ศ. 2556 : ศึกษากรณีธุรกิจประกันชีวิต." หน้า 144, จุฬาลงกรณ์มหาวิทยาลัย, ปีพ.ศ. 2558.

สุทธิพร สายเชื้อ. ""ปัญหาและอุปสรรคในการดำเนินการตามมาตรการในพระราชบัญญัติป้องกันและปราบปรามการสนับสนุนทางการเงิน
แก่การก่อการร้าย พ.ศ. 2556 : ศึกษากรณีธุรกิจประกันชีวิต." จุฬาลงกรณ์มหาวิทยาลัย, ปีพ.ศ. 2558.

หมายเจริญศรี, วิลาสินี. "การเข้าเป็นภาคีสันธิสัญญาว่าด้วยการค้าอาวุธ ค.ศ. 2013 ของประเทศไทย : ปัญหาและ ลู่ทาง."
จุฬาลงกรณ์มหาวิทยาลัย, พ.ศ. 2559.

อาจารย์ ดร. ชัชชม อรรถภิญญ์ อธิบดีอัยการ. เอกสารประกอบการสอนวิชาวิธีพิจารณาความอาญาชั้นสูง. หัวข้อ ความร่วมมือระหว่าง
ประเทศในเรื่องทางอาญา (Mutual Legal Assistance in Criminal Matters). สำนักงานต่างประเทศ
สำนักงานอัยการสูงสุด, 2018.



จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ประวัติผู้เขียน

ชื่อ-สกุล	ธีรพันธุ์ แก้วคง
วัน เดือน ปี เกิด	30 พฤษภาคม พ.ศ. 2538
สถานที่เกิด	กรุงเทพมหานครฯ
วุฒิการศึกษา	สำเร็จการศึกษาระดับประถมศึกษาจากโรงเรียนสุนทรวัฒนา และระดับมัธยมศึกษาจากโรงเรียนชัยภูมิภักดีชุมพล สำเร็จการศึกษาระดับอุดมศึกษาปริญญาตรี นิติศาสตรบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยมหาสารคาม และประกาศนียบัตรหลักสูตร English for Academic Purposes จาก English Language Centre, University of New England ประเทศออสเตรเลีย จากนั้นจึงได้เข้าศึกษาต่อในหลักสูตรนิติศาสตรมหาบัณฑิต หมวดกฎหมายระหว่างประเทศ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ระหว่างการศึกษาได้เคยเป็นผู้ช่วยผู้วิจัยแก่ ศาสตราจารย์ ดร.ชุมพร ปัจจุบันงานในโครงการศึกษาการเข้าร่วมอนุสัญญาระหว่างประเทศว่าด้วยการควบคุมและจัดการน้ำอับเฉาและตะกอนจากเรือ
ที่อยู่ปัจจุบัน	Email : teerapan.pope@gmail.com