รายงานการศึกษาวิจัย

การปรับปรุงระเบียบ กฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

เสนอ

สำนักงานกิจการยุติธรรม

กระทรวงยุติธรรม

โดย

นายฐนันดร์ศักดิ์ บวรนันทกุล และคณะ

คณะสังคมศาสตร์และมนุษยศาสตร์

มหาวิทยาลัยมหิดล

2549

กิตติกรรมประกาศ

รายงานการศึกษาวิจัย เรื่อง **การปรับปรุงระเบียบกฎหมายที่เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม** นี้ สำเร็จลุล่วงได้ด้วยดี จากความเมตตาช่วยเสนอแนะ แนะนำและชี้แนะแนวทางจากท่านวิศิษฏ์ วิสิษฏ์สรอรรถ ผู้อำนวยการสำนักงานกิจการยุติธรรม และท่านผู้อำนวยการสำนักวิจัยและพัฒนากระบวนการยุติธรรม สำนักงานกิจการยุติธรรม ท่านวัลลภ นาคบัว ซึ่งกรุณาให้แนวทางและข้อคิดที่เป็นประโยชน์อย่างยิ่งต่อทิศทางในการศึกษา คณะผู้วิจัยขอกราบขอบพระคุณในความกรุณาเป็นอย่างยิ่ง

ขอขอบพระคุณผู้บริหารและผู้แทนจากหน่วยงานต่างๆ ทั้งจากกระทรวงยุติธรรมโดยตรง หน่วยงานขึ้นตรงต่อรัฐมนตรีว่าการกระทรวงยุติธรรม หน่วยงานต่างๆในกระบวนการยุติธรรมโดยตรงและหน่วยงานที่เกี่ยวข้อง ที่ท่านได้กรุณาสละเวลาเข้าร่วมการประชุมเชิงปฏิบัติการทั้ง 2 ครั้ง (บางท่านได้กรุณาสละเวลาให้สัมภาษณ์ในการศึกษาในครั้งนี้) รวมทั้งผู้บริหารและผู้แทนจากองค์กรและหน่วยงานต่างๆที่เป็นประโยชน์อย่างยิ่ง ทำให้การศึกษามีความสมบูรณ์อย่างยิ่ง คณะผู้วิจัยขอขอบพระคุณอย่างยิ่งในความเอื้อเฟื้อและการมีส่วนร่วม รวมถึงความเมตตาที่กรุณาให้ข้อมูลที่เป็นประโยชน์ในการศึกษาครั้งนี้

น้องๆผู้ประสานงานจากสำนักงานกิจการยุติธรรม ได้แก่ น้องยุ้ย (จิรารัตน์ วรวัฒน์ธำรง) และน้องปู (เปรมมิศา หนูเรืองงาม) ที่ช่วยเหลือดูแลประสานการดำเนินการตลอดจนคุณสำราญฯ และคณะกรรมการตรวจฯ ที่ได้ให้ข้อสังเกตและข้อเสนอแนะที่เป็นประโยชน์ต่อการแก้ไข ปรับปรุง การศึกษา และการดำเนินการให้สำเร็จลุล่วงไปด้วยดี คณะทำงานขอขอบคุณในความช่วยเหลือดูแลประสานการดำเนินการและความมีน้ำใจต่างๆ

คณะผู้วิจัย

บทคัดย่อ

ชื่อเรื่อง : **การปรับปรุงระเบียบ กฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม**

ผู้วิจัย : **นายฐนันดร์ศักดิ์ บวรนันทกุล และคณะ**

ปีที่ทำวิจัย : **เมษายน 2550**

การศึกษาวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อสำรวจการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรม ตามแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551) ศึกษาวิเคราะห์ ปัญหาและอุปสรรค และกฎ ระเบียบ ข้อบังคับ และกฎหมายของหน่วยงานในกระบวนการยุติธรรมต่อการเชื่อมโยง ข้อมูล และ การนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรม ตลอดจนเสนอแนะแนวทางการปรับปรุงแก้ไขระเบียบและกฎหมายต่าง ๆที่เป็นอุปสรรคต่อการเชื่อมโยงและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรม

วิธีการดำเนินการวิจัยใช้การศึกษาเอกสาร (Documentary Research) และการสนทนากลุ่ม (focus group seminars) โดยผู้เข้าร่วมเป็นผู้แทนและผู้ปฏิบัติงานที่เกี่ยวข้อง (The Stakeholders) ในหน่วยงานของกระบวนการยุติธรรม ตลอดจนการสัมภาษณ์บุคคลที่ปฏิบัติงานที่เกี่ยวข้องโดยตรง

ผลการศึกษาพบว่า หน่วยงานในกระบวนการยุติธรรมส่วนใหญ่ ยังไม่ได้มีการเชื่อมโยง แลกเปลี่ยนหรือบูรณาการข้อมูลร่วมกันจะมีเชื่อมโยงกันบ้างเพียงไม่กี่หน่วยงาน บางหน่วยงานฐานข้อมูลมูลอยู่ในระหว่างการพัฒนาปรับปรุง ปัญหาและอุปสรรคในการเชื่อมโยงข้อมูล ได้แก่ การขาดนโยบายที่ชัดเจนว่า ควรจะจัดเก็บข้อมูลอะไรบ้าง และขาดความต่อเนื่องในการดำเนินการ ขาดหน่วยงานที่เป็นเจ้าภาพหลักในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการประมวลผล งบประมาณที่สูง และงานด้านเทคโนโลยีสารสนเทศไม่ใช่งานหลักของหน่วยงาน การขาดแคลนบุคลากรที่มีความรู้เฉพาะด้านการเปลี่ยนแปลงเทคโนโลยีที่รวดเร็ว มิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก ขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ความน่าเชื่อถือน้อย ข้อมูลจำนวนมากขาดการปรับปรุงให้เป็นปัจจุบัน ขาดการคุ้มครอง

ส่วนบุคคล การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ การขาดความพร้อมสำหรับการบูรณาการ

ในด้านกฎ ระเบียบ และกฎหมายที่เกี่ยวข้องพบว่า หน่วยงานในกระบวนการยุติธรรมส่วนใหญ่ ไม่มีกฎ ระเบียบ เกี่ยวกับการเชื่อมโยงแลกเปลี่ยนข้อมูลโดยเฉพาะ แต่มีกฎหมายที่ทั้งเป็นปัญหาและอุปสรรคต่อการเชื่อมโยง ตั้งแต่บทบัญญัติตามกฎหมายรัฐธรรมนูญ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 พ.ร.บ.ประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามทุจริต พ.ศ.2542 มาตรา 25 และมาตรา 120 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 เป็นต้น และ กฎ ระเบียบ และกฎหมายที่เอื้ออำนวยต่อการเชื่อมโยงข้อมูล อาทิ พระราชบัญญัติว่าด้วยธุรกรรมอิเลคโทรนิคส์ พ.ศ. 2544 ระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาฯ พ.ศ. 2545 อย่างไรก็ตาม กฎ ระเบียบ กฎหมายที่เกี่ยวข้องกับการเชื่อมโยง การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม อาจจำแนกเป็น 4 กลุ่ม คือ กฎหมายที่เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม กฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล กฎหมายทรัพย์สินทางปัญญา และกฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ข้อเสนอแนะ จากการศึกษาในด้านกลไกการดำเนินการทั่วไป ได้แก่ การเริ่มเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระทรวงยุติธรรมขยายความร่วมมือไปยังหน่วยงานที่สังกัด และหน่วยงานภายนอก มีการจัดทำคู่มือการดำเนินการ (Code of Practice) จัดตั้งคณะทำงานทางเทคนิค (liaison officers) เวียนไปดูแลประสานงานแต่ละหน่วยงาน ในด้านกฎ ระเบียบ จัดทำระเบียบการเชื่อมโยงข้อมูลภายในกระทรวง (ประกาศกระทรวง) เสนอแก้กฎหมายที่เกี่ยวข้องและในระยะยาวควรตรากฎหมายระดับพระราชบัญญัติการเชื่อมโยงแลกเปลี่ยน และบูรณาการข้อมูลด้านกระบวนการยุติธรรมออกมาใช้โดยตรง โดยใช้มาตรการทางกฎหมายในเชิงการบริหารจัดการ

คำสำคัญ (Key words): เทคโนโลยีสารสนเทศ (Information Technology) การบูรณาการข้อมูลในกระบวนการยุติธรรม (Integration of Criminal Justice Information) กฎหมาย การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (Justice Information Sharing Laws)

ABSTRACT

Research Title: Improving Regulations and Laws for Enhancing the Use of Criminal Justice Information in Thailand

Researcher : Tanansak Borwornnuntakul and Colleques.

Date : April 2007

The objectives of this study were to survey the communication of criminal justice information in relevant governmental organizations under the National Master Plan for Criminal Justice Information Technology Paper.1 (B.E. 2548-2551), delineating not only the problems and obstacles but also the existing rules, regulations and laws, including proposals for problem solving as well as improving such procedures.

Methods for collecting data included documentary research and focus group seminars among criminal justice stakeholders, including interviews with those who are directly working on such criminal justice information technology.

The results of this study revealed that there were only a few criminal justice units collaborating on criminal justice information sharing. In addition, there still remain various problems and obstacles such as, a lack of a clear-cut policy on justice data sharing, an absence of a key central unit, inadequate finance, lack of information technology experts, no standardized formats, a general unawareness of information database, a lack of intention by the CEO, a lack of readiness for integration etc.

As for the relevant regulations and laws, generally speaking, there are four classifications as follows: the laws concerned with the integration of criminal justice information, personal data protection law, intellectual property law, and computer misuse laws. The Thai criminal justice system is currently lacking some essential legal provisions for justice information sharing such as a specific justice integration law and personal data protection law. In addition, existing legal provisions are causing obstacles for achieving, including The Constitution of The Kingdom of Thailand, The Government Information Act B.E. 2540, the Organic law not only regarding the Committee for Prevention and Suppression of Money Laundering Act but also the National Committee for the Prevention and Suppression of Corruption etc. Be that as it may, there are some contributing provisions for data sharing laws such as The Electronic Activities Act of B.E. 2544, the Regulation of The General Attorney on Criminal Procedures B.E.2545.,etc. As a matter of fact, we can apply such laws to enhance criminal justice integration.

The recommendations for this study are to develop the communication among the internal departments in the justice ministry and extend this to similar mission organizations and relevant criminal outsider organizations, to formulate a Code of Practice, to set up liaison officers for cooperating in the procedure, to pass a ministerial announcement (as administrative law) for criminal justice information sharing and enact specific acts for the connecting, sharing and integrating of criminal justice information in terms of administrative and management legal measures.

KEY WORDS : Information Technology / Integration of Criminal Justice Information / Justice Data Sharing

สารบัญ

บทที่			หน้า
1	**บทนำ**		**1**
	1.1	หลักการและเหตุผล	1
	1.2	วัตถุประสงค์	3
	1.3	เป้าหมาย	3
	1.4	วิธีดำเนินการศึกษา	4
	1.5	ผลที่คาดว่าจะได้รับ	4
2	**แนวคิดการบูรณาการและการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม**		**6**
	2.1	การนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กร	8
	2.2	ข้อมูลสารสนเทศในกระบวนการยุติธรรม	15
	2.3	การคุ้มครองข้อมูล (Data Protection)	29
	2.4	การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์	34
	2.5	การบูรณาการข้อมูลด้านการบริหารงานยุติธรรม	42
	2.6	เทคโนโลยีสารสนเทศและการบูรณาการข้อมูลด้านงานยุติธรรมของไทย	45
3	**กฎหมาย กฎและระเบียบที่เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม**		**63**
	3.1	หลักและแนวคิดทางกฎหมาย	63
		1. กฎหมายเกี่ยวกับการเชื่อมต่อ แลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม	63
		2. กฎหมายคุ้มครองข้อมูลส่วนบุคคล	65
		3. กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	76
		4. กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในการกระทำผิด	81
	3.2	กฎหมายต่างประเทศ	88
		(ก) กลุ่มประเทศ Common Law	88
		1. ประเทศสหรัฐอเมริกา	88
		2. ประเทศอังกฤษ หรือสหราชอาณาจักร	111
		3. ประเทศสวีเดน	128

สารบัญ (ต่อ)

บทที่		หน้า
	4. ประเทศแคนาดา	137
	5. ประเทศออสเตรเลีย	145
	6. ประเทศนิวซีแลนด์	152
	(ข) กลุ่มประเทศ Civil Law	157
	2.1 กฎหมายคุ้มครองข้อมูลในฐาน ข้อมูลอิเลกทรอนิกส์ของสหภาพยุโรป	157
	1. ประเทศฝรั่งเศส	161
	2. ประเทศญี่ปุ่น	168
	3. ประเทศเนเธอร์แลนด์	185
	4. ประเทศสิงคโปร์	189
	5. ประเทศไทย	193
	ก. กฎหมายที่เป็นอุปสรรคต่อการเชื่อมโยงข้อมูลระหว่างหน่วยงาน ในกระบวนการยุติธรรม	198
	ข. กฎหมายที่เอื้ออำนวยต่อการเชื่อมโยงข้อมูลระหว่างหน่วยงาน ในกระบวนการยุติธรรม	200
4	**การวิเคราะห์ข้อมูล**	**236**
	4.1 การวิเคราะห์ปัญหา อุปสรรค ของการเชื่อมโยงข้อมูลระหว่างหน่วยงาน ในกระบวนการยุติธรรม	236
	4.2 การวิเคราะห์ปัญหาทางด้านกฎหมาย	241
	4.3 การวิเคราะห์การประยุกต์กับแผนแม่บท	255
5	**บทสรุปและเสนอแนะ**	**283**
	5.1 บทสรุป	283
	5.2 ข้อเสนอแนะ	294
บรรณานุกรม		**297**

สารบัญ (ต่อ)

หน้า

ภาคผนวก **309**

ภาคผนวก 1: สรุปผลการประชุมเชิงปฏิบัติการ ครั้งที่ 1 เพื่อรับฟังความคิดเห็นเกี่ยวกับการเชื่อมต่อข้อมูล ปัญหาและอุปสรรคที่เกี่ยวข้อง 310

ภาคผนวก 2: สรุปผลการประชุมเชิงปฏิบัติการ ครั้งที่ 2 เพื่อรับฟังความคิดเห็นเกี่ยวกับประเด็น ทางกฎหมายที่เกี่ยวข้อง 325

ภาคผนวก 3: สรุปผลการประชุมสัมมนา ครั้งที่ 3 เพื่อเผยแพร่และรับฟังความคิดเห็น เกี่ยวกับร่างรายงานฉบับสมบูรณ์ 334

ภาคผนวก 4: รายชื่อผู้เข้าร่วมการประชุมเชิงปฏิบัติการ ครั้งที่ 1 2 และการประชุมสัมมนา ครั้งที่ 3 341

คณะทำงาน **356**

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ตามแผนแม่บทกระบวนการยุติธรรมแห่งชาติ พ.ศ. 2547-2549 กำหนดให้มีการพัฒนาและอำนวยความยุติธรรมอย่างเป็นระบบ มีประสิทธิภาพ รวดเร็ว โปร่งใสตรวจสอบได้ โดยหน่วยงานในกระบวนการยุติธรรมจะต้องบูรณาการเป้าหมายและกระบวนการทำงานให้สอดคล้องและเป็นไปในทิศทางเดียวกัน รวมทั้งพัฒนาประสิทธิภาพการบริหารจัดการของหน่วยงานยุติธรรมด้วยการลดขั้นตอนการปฏิบัติให้สะดวก รวดเร็ว มีประสิทธิภาพ และใช้ทรัพยากรร่วมกัน

การนำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในกระบวนการยุติธรรมเพื่อช่วยให้มีการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้องรวมถึงการมีและใช้ข้อมูลดังกล่าวร่วมกันระหว่างหน่วยงาน จะส่งผลให้การทำงานของหน่วยงานในกระบวนการยุติธรรมเป็นอย่างสะดวก รวดเร็ว ถูกต้อง และมีประสิทธิภาพยิ่งขึ้น นอกจากนี้การสามารถเข้าถึงและใช้ข้อมูลที่มีอยู่แล้วของหน่วยงานใดหน่วยงานหนึ่งโดยหน่วยงานที่ต้องการใช้ข้อมูลไม่ต้องดำเนินการกรอกข้อมูลใหม่ ทำให้หน่วยงานนั้นๆได้รับและได้ใช้ข้อมูลที่มีความคลาดเคลื่อนน้อยที่สุด อันจะนำไปสู่หนทางที่จะอำนวยความยุติธรรมให้แก่ประชาชนอีกหนทางหนึ่งและการที่หน่วยงานต่างๆจะได้รับหรือได้ใช้ข้อมูลเหล่านั้นจากการเชื่อมโยงข้อมูลระหว่างหน่วยงานยุติธรรมได้ก็จักต้องมีการส่งต่อข้อมูลที่หน่วยงานนั้นๆมีอยู่ให้แก่กันและกัน ทั้งนี้เพื่อให้เกิดการบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรมอย่างแท้จริง แต่ในทางปฏิบัติการส่งต่อข้อมูลระหว่างหน่วยงานในกระบวนยุติธรรมอาจมีปัญหาและอุปสรรคเกิดขึ้นได้ นอกจากนี้การดำเนินงานในกระบวนการยุติธรรมในปัจจุบันยังต้องเป็นไปตามขั้นตอนและวิธีการที่กฎ ระเบียบ ข้อบังคับ หรือกฎหมายที่แต่ละหน่วยงานได้กำหนดขึ้น ซึ่งอาจเป็นอีกสาเหตุหนึ่งที่ก่อให้เกิดความล่าช้าและเป็นอุปสรรคต่อการส่งต่อข้อมูลและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรม

นอกจากนี้ แผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551) ยังได้กำหนดยุทธศาสตร์ที่สำคัญหลายประการ โดยมุ่งหมายให้หน่วยงานในกระบวนการยุติธรรม (ซึ่งรวมถึงศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติ

กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน กรมบังคับคดี สถาบันนิติวิทยาศาสตร์ และกรมคุ้มครองสิทธิและเสรีภาพ) จัดทำฐานข้อมูลสารสนเทศที่เกี่ยวข้องกับอำนาจหน้าที่ของแต่ละหน่วยงานในรูปแบบของข้อมูลอิเล็กทรอนิกส์โดยใช้มาตรฐานทางเทคโนโลยีสารสนเทศขั้นต่ำร่วมกันเพื่อประโยชน์ในการบูรณาการข้อมูลและใช้ข้อมูลร่วมกัน (ทั้งนี้แผนแม่บทฯกำหนดให้ใช้มาตรฐานที่สามารถเรียกใช้ข้อมูลผ่านโปรแกรมประยุกต์แบบ Web-based) แผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติมุ่งสร้างบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรมโดยเชื่อมโยงข้อมูลสารสนเทศของหน่วยงานต่างๆ ในกระบวนการยุติธรรมเข้าด้วยกันโดยผ่านฐานข้อมูลกลาง (Centralized Sever) และศูนย์แลกเปลี่ยนข้อมูล (Data Exchange Centre หรือ DXC) เพื่อให้หน่วยงานในกระบวนการยุติธรรมสามารถใช้ข้อมูลสารสนเทศที่เกี่ยวข้องร่วมกันได้ กล่าวคือ หน่วยงานหนึ่งจัดทำข้อมูลสารสนเทศอิเล็กทรอนิคส์ที่อยู่ในความรับผิดชอบโดยตรงของตนและหน่วยงานอื่นที่ต้องใช้ข้อมูลสารสนเทศที่หน่วยงานแรกจัดทำไว้แล้วโดยไม่จำเป็นที่หน่วยงานอื่นนั้นต้องจัดทำข้อมูลสารสนเทศอิเล็กทรอนิกส์ซ้ำซ้อนกัน ในการนี้ ข้อมูลสารสนเทศอิเล็กทรอนิกส์ที่จะจัดทำขึ้นและบูรณาการหรือเชื่อมโยงกันประกอบด้วยข้อมูลที่เกี่ยวข้องกับงานด้านต่างๆรวมทั้งงานด้านการป้องกันและปราบปรามอาชญากรรม การพิจารณาคดี การดำเนินงานตามคำพิพากษา และการคุ้มครองสิทธิเสรีภาพของประชาชน ซึ่งข้อมูลในแต่ละด้านมีหลากหลาย เช่น ข้อมูลด้านการป้องกันและปราบปรามอาชญากรรม การพิจารณาคดี การดำเนินงานตามคำพิพากษา และการคุ้มครองสิทธิเสรีภาพของประชาชน ซึ่งข้อมูลในแต่ละด้านมีหลากหลาย เช่น ข้อมูลด้านการป้องกันและปราบปรามอาชญากรรมประกอบด้วยข้อมูลเกี่ยวกับการแจ้งความ การกระทำความผิด การจับกุม ประวัติผู้ต้องสงสัย ผู้ต้องหาและพยาน การสอบสวนและคำให้การ ประวัติอาชญากร ประวัตินักโทษและบุคคลพ้นโทษ หมายจับ ลายพิมพ์นิ้วมือ ข้อมูลนิติเวช ทะเบียนยานพาหนะ ฯลฯ

ดังนั้น เพื่อให้มีการดำเนินการตามยุทธศาสตร์ในแผนแม่บทเทคโนโลยีสารสนเทศและเกิดผลสัมฤทธิ์อย่างเป็นรูปธรรม จำเป็นต้องมีการศึกษา ทบทวน และแก้ไขกฎ ระเบียบ ข้อบังคับ และกฎหมายต่างๆที่เป็นอุปสรรคต่อการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมเพื่อนำผลการศึกษา แนวคิด และแนวทางปฏิบัติงานเพื่อการปรับปรุงระเบียบ กฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรมดังกล่าว มาใช้เป็นข้อมูลประกอบการพิจารณาในการจัดให้มีการศึกษาวิเคราะห์ในรายละเอียดเกี่ยวกับการดำเนินการที่มีอยู่ในปัจจุบันและการ

ดำเนินการใหม่ให้มีความเป็นเอกภาพและสอดคล้องกับการดำเนินการระหว่างองค์กรโดยคำนึงถึงผลประโยชน์ของชาติและความเหมาะสมที่สุด (Best Practices for Thailand) เป็นสำคัญต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อสำรวจว่าการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมตามแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551) มีปัญหาและอุปสรรคอย่างไร และกฎ ระเบียบ ข้อบังคับ และกฎหมายของหน่วยงานในกระบวนการยุติธรรมก่อให้เกิดปัญหาและอุปสรรคต่อการเชื่อมโยงข้อมูลและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมอย่างไร

1.2.2 เพื่อศึกษาวิเคราะห์สภาพปัญหาและอุปสรรคของการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมและการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานของหน่วยงานในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

1.2.3 เพื่อนำเสนอแนวทางในการปรับปรุง แก้ไขกฎ ระเบียบ ข้อบังคับ หรือกฎหมายต่างๆที่เป็นอุปสรรคต่อการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมและการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานของหน่วยงานในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้อง

1.3 เป้าหมาย

1.3.1 การดำเนินการเชื่อมโยงข้อมูลระหว่างหน่วยงานสำหรับการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรมเดิมที่มีอยู่ ได้รับการปรับปรุงให้เหมาะสมยิ่งขึ้นหรือมีการยกร่างการดำเนินการเฉพาะด้าน หรือจัดทำข้อกำหนดอื่นๆ ที่เหมาะสมเพื่อรองรับการดำเนินงานการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

1.3.2 ปรับปรุงกฎ ระเบียบ กฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม ยกร่างการดำเนินการเฉพาะด้านหรือจัดทำร่างข้อกำหนดอื่นๆ (Code of Practice) ที่เหมาะสมเพื่อรองรับการดำเนินงาน

1.3.3 การจัดทำร่างนโยบาย มาตรการ ระเบียบ ข้อกำหนด ที่เหมาะสมใน ว่าด้วยปรับปรุงระเบียบกฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

1.4 วิธีดำเนินการศึกษา

แนวทางในการศึกษาวิจัยในครั้งนี่แบ่งออกเป็น 2 ขั้นตอน คือ

1.4.1 **การวิจัยเอกสาร (Documentary Research)** เป็นการศึกษาทบทวนวรรณกรรมที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลด้านกระบวนการยุติธรรมของไทยและของต่างประเทศ รวมทั้งศึกษากฎหมายต่างๆที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการดังกล่าว

1.4.2 **การศึกษางานสนาม (Field Research)**เป็นการดำเนินการภายหลังจากการศึกษาและทบทวนวรรณกรรมจนได้กรอบแนวคิดและแนวทางต่างๆ จากนั้นนำแนวคิดไปเก็บข้อมูลภาคสนาม แนวทางการดำเนินการนี้ดำเนินการโดยใช้การประชุมกลุ่ม (Focus group seminar) และใช้การสัมภาษณ์บุคลากรที่ปฏิบัติงานเกี่ยวข้องกับหน่วยงานต่างๆในกระบวนการยุติธรรม

1.5 ผลที่คาดว่าจะได้รับ

1.5.1 ทำให้ทราบถึงปัญหาและอุปสรรคที่เกิดขึ้นจากกฎ ระเบียบ ข้อบังคับและกฎหมายของหน่วยงานในกระบวนการยุติธรรมและที่ไม่ได้เกิดขึ้นจากกฎ ระเบียบ ข้อบังคับและกฎหมายของหน่วยงานว่าก่อให้เกิดปัญหาและอุปสรรคต่อการเชื่อมโยงข้อมูลและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมอย่างไร

1.5.2 ทำให้ทราบถึงแนวทางในการปรับปรุง แก้ไขกฎ ระเบียบ ข้อบังคับหรือกฎหมายต่างๆที่เป็นอุปสรรคต่อการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมและการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานของหน่วยงานในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้อง

นอกจากนี้จะทำให้กระทรวงยุติธรรมสามารถมีกรอบการดำเนินการและมาตรการที่เหมาะสมสำหรับแนวทางการปฏิบัติงานปรับปรุงระเบียบกฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม ภายใต้หลักการของการเป็นหุ้นส่วนความร่วมมือ (Partnership) และว่าด้วยกิจกรรมการดำเนินการต่าง ๆและการปรับปรุงระเบียบกฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรมตามหลักเกณฑ์ที่กำหนดไว้

บทที่ 2
แนวคิดเกี่ยวกับการบูรณาการและการแลกเปลี่ยนข้อมูล ด้านกระบวนการยุติธรรม

โครงการปรับปรุง ระเบียบ กฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรมนี้มีความมุ่งหมายที่จะศึกษาสำรวจ การเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรม ศึกษาปัญหาและอุปสรรคในการเชื่อมโยงตลอดจนศึกษา กฎ ระเบียบ ข้อบังคับ และกฎหมายของหน่วยงานในกระบวนการยุติธรรมที่เกี่ยวข้อง เพื่อทำการวิเคราะห์การเชื่อมโยงข้อมูล ปัญหา อุปสรรคในการดำเนินการและกฎระเบียบ กฎหมายที่เกี่ยวข้องกับการเชื่อมโยง การแลกเปลี่ยน และการบูรณาการเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม ซึ่งก่อนที่จะศึกษาประเด็นทางกฎหมายจำเป็นจะต้องทำความเข้าใจถึง แนวคิด หลักการที่เกี่ยวข้องกับการบูรณาการและการแลกเปลี่ยนข้อมูลโดยการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรมอันจะเป็นพื้นฐานในการวิเคราะห์ในประเด็นที่เกี่ยวข้องต่อไป

การเชื่อมโยง การแลกเปลี่ยนข้อมูล และการบูรณาการข้อมูล ข้อเท็จจริง และข้อมูลสารสนเทศในกระบวนการยุติธรรม สามารถกระทำได้จากความร่วมมือของหน่วยงานและองค์กรต่างๆในกระบวนการยุติธรรม ได้ทำการส่งมอบและแลกเปลี่ยนข้อมูลที่สำคัญและจำเป็นเพื่อนำไปใช้ประโยชน์ในบทบาทหน้าที่และการปฏิบัติงานขององค์กรต่อไป

ในยุคปัจจุบัน ความก้าวหน้าทางด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศรวมไปถึงการใช้สื่ออิเล็กทรอนิกส์ในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งในรูปแบบของเครือข่ายอินเตอร์เน็ต ได้รับการพัฒนามากขึ้นอย่างต่อเนื่องและรวดเร็ว ประเทศต่างๆจำเป็นต้องมีการพัฒนาปรับปรุง ตลอดจนนำมาปรับใช้ในการปฏิบัติงานในองค์กรต่างๆโดยเฉพาะของรัฐให้ดำเนินไปอย่างมีประสิทธิภาพ ซึ่งก็รวมถึงการเชื่อมต่อ การบูรณาการและการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรมด้วย ดังนั้น สิ่งที่ต้องคำนึงถึงควบคู่ไปกับความเจริญก้าวหน้าของเทคโนโลยีและการดำเนินการทางด้านนี้เพิ่มเติมก็คือ การดูแลรักษาความปลอดภัยต่อเครื่องคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมการใช้งาน โปรแกรมระบบ ข้อมูลสารสนเทศ การบริหารการจัดการ รวมไปถึงตัวผู้ใช้ ผู้ควบคุม ระบบและผู้บริหาร เป็นต้น[1] ทั้งนี้เพื่อป้องกัน

[1] Chance, Clifford. **Data Protection** p.15

และควบคุมไม่ให้เกิดการลอกเลียนแบบ การปลอมหรือเปลี่ยนแปลง การบุกรุกการทำงาน การนำไปใช้โดยไม่ได้รับอนุญาต ตลอดจนการทำลายไม่ให้สามารถปฏิบัติงานได้ในรูปแบบของอาชญากรรมทางคอมพิวเตอร์ที่เพิ่มจำนวนสูงขึ้นอยู่ตลอดเวลาทั้งในสหรัฐเมริกาและในสหภาพยุโรป รวมทั้งไม่ว่าจะเป็นการคิดค้นสร้างโปรแกรมไวรัสคอมพิวเตอร์ชนิดต่างๆ ออกมาทำลายข้อมูลของบริษัทชั้นนำมากมาย หรือการถอดรหัสหมายเลขบัตรเครดิตของบุคลอื่นมาใช้ในการถอนเงินหรือโอนเงินของบุคคลนั้นๆ มาเป็นของตนเอง

สำหรับประเทศไทยนั้นได้ก้าวเข้าสู่สังคมเทคโนโลยีสารสนเทศอย่างหลีกเลี่ยงไม่ได้ เพราะแต่ละประเทศในภูมิภาคต่างๆ ได้เร่งพัฒนาศักยภาพขีดความสามารถด้านเทคโนโลยีสารสนเทศประเทศได้ดียิ่งขึ้น นอกจากนี้จากการสร้างความร่วมมือทางด้านเศรษฐกิจขึ้นระหว่างสหรัฐอเมริกา แคนนาดา และเม็กซิโก เป็นเขตการค้าเสรีแห่งอเมริกาเหนือ หรือ North American Free Trading Areas (NAFTA) หรือจะเป็นการร่วมมือกันทางด้านเศรษฐกิจระหว่างกลุ่มประเทศอาเซียนกลายเป็นเขตการค้าเสรีอาเซียน หรือ Asian Free Trading Areas (AFTA) เป็นต้น ด้วยเหตุผลประการนี้เองทำให้ประเทศไทยจำเป็นต้องพัฒนาภารกิจหลักที่สำคัญ 3 ประการ[2] คือ การลงทุนพัฒนาโครงสร้างพื้นฐานทางสารสนเทศแห่งชาติ การลงทุนพัฒนาคุณภาพทรัพยากรมนุษย์ที่มีทักษะทางด้านเทคโนโลยีสารสนเทศ และการลงทุนพัฒนาการปกครองที่ดี เพื่อสร้างความได้เปรียบทางด้านต่างๆ แก่ประเทศของเรา

อย่างไรก็ตาม การพัฒนาปัจจัยทั้งหมดให้เกิดประสิทธิภาพและประสิทธิผลมากที่สุดนั้น ตัวแปรสำคัญขึ้นอยู่กับการปรับปรุงระบบ หน่วยงานของรัฐและสถานที่ราชการทุกแห่งจะต้องมีความพร้อมทั้งในส่วนของบุคลากรที่มีความรู้ความสามารถในการใช้เทคโนโลยีและในส่วนของเครื่องมือและอุปกรณ์เทคโนโลยีสารสนเทศ นอกจากนี้รัฐจะต้องมีฐานข้อมูลของรัฐ ไม่ว่าจะเป็นข้อมูลสถิติของจำนวนประชากร สังคม เศรษฐกิจ ศิลปวัฒนธรรม การศึกษา การสาธารณสุข ฯลฯ เพื่อประโยชน์ในการวางแผน คาดการณ์ และเตรียมการ โดยรัฐจะต้องดำเนินการให้ประชาชนสามารถติดต่อราชการได้ด้วยสื่ออิเล็กทรอนิกส์ในสถานที่ราชการทุกแห่งเท่าที่จะเป็นไปได้ ขณะเดียวกันข้อมูลสาธารณะจะต้องสามารถเปิดกว้างสำหรับการค้นคว้าของประชาชนโดยผ่านสื่ออิเล็กทรอนิกส์เช่นกันตามเงื่อนไขการเจริญเติบโตของประเทศความก้าวหน้าทางด้านข้อมูลกฎหมาย

---

[2] ปทีป เมธาคุณวุฒิ. **แนวทางการออกกฎหมายคุ้มครองข้อมูลและสารสนเทศส่วนบุคคลในประเทศไทย.** หน้า.1

แต่เนื่องจากสภาพทางด้านเศรษฐกิจในยุคเทคโนโลยีสารสนเทศนี้ ทำให้เกิดการแข่งขันกันในทุกๆ ด้าน การใช้เทคโนโลยีทางด้านคอมพิวเตอร์และสารสนเทศ เพื่อการจัดเก็บข้อมูลจำนวนมากๆ รวมทั้งข้อมูลส่วนบุคคลที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของ ซึ่งสามารถนำมารวบรวม ตรวจสอบ วิเคราะห์ แสดงผลและทำสำเนาโดยใช้แผ่นเทปหรือดิสเก็ตได้อย่างรวดเร็ว ข้อมูลและสารสนเทศส่วนบุคคลจึงเป็นสิทธิส่วนบุคคลที่ผู้ใดจะละเมิดไม่ได้ ดังนั้น ข้อมูลและข้อสนเทศต่างๆในกระบวนการยุติธรรมก็เช่นเดียวกัน ส่วนใหญ่จะเป็นข้อมูลที่มีผลเกี่ยวกับการดำเนินคดีกับผู้ที่เกี่ยวข้อง ดังนั้น เพื่อให้การรวบรวมข้อมูลเกี่ยวกับบุคคลการดำเนินการต่างๆในกระบวนการยุติธรรม การพัฒนาและปรับปรุงกฎระเบียบและกฎหมายที่เกี่ยวข้องจึงมีความจำเป็นต้องทำการศึกษาถึงมาตรการทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง ซึ่งเกี่ยวโยงถึงโครงสร้างพื้นฐานของเทคโนโลยีสารสนเทศ (Information Technology Infrastructure) และสถาปัตยกรรมของข้อมูลในกระบวนการยุติธรรม (Criminal Justice Data Architectures) และแนวคิดในการนำเอาระบบเทคโนโลยีคอมพิวเตอร์ไปใช้เก็บและประมวลข้อมูลก่อน

2.1 การนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กร

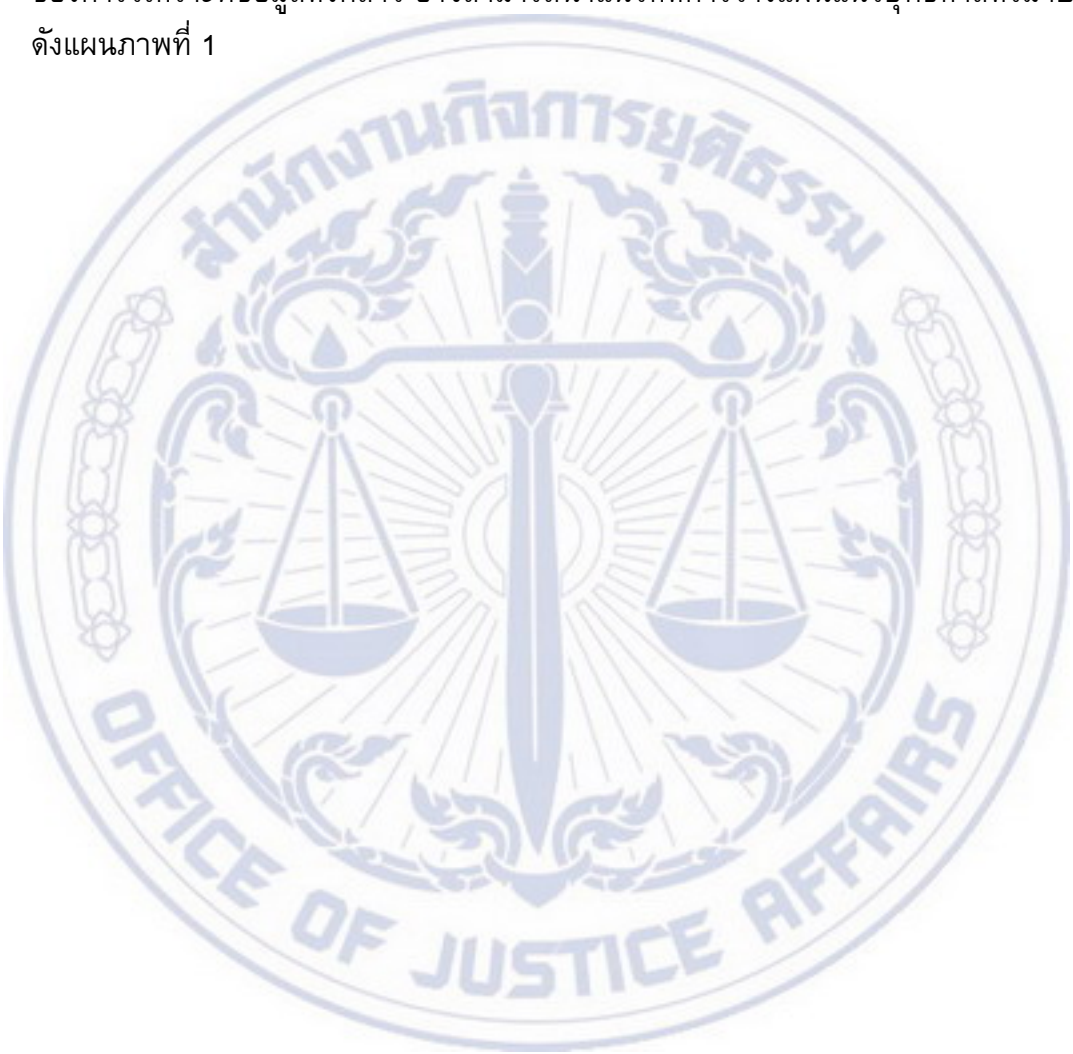
แนวคิดในการทำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กรเป็นแนวคิดที่มีความสำคัญอย่างยิ่ง เพราะจะเป็นการใช้ความก้าวหน้าทางเทคโนโลยีมาใช้ในการจัดเก็บ และประมวลข้อมูล ตลอดจนจัดทำระบบเพื่อการค้นคว้าอ้างอิงและการประสานการดำเนินการต่างๆ โดยเฉพาะอย่างยิ่งองค์กรในกระบวนการยุติธรรมนั้นเป็นหน่วยงานที่ต้องมีใครจัดเก็บ และประมวลข้อมูลที่เกี่ยวกับผู้กระทำผิด พฤติกรรมการกระทำผิด ผู้เสียหาย การดำเนินคดีและการบังคับใช้กฎหมายต่างๆให้มีประสิทธิภาพ และที่สำคัญอย่างยิ่ง เทคโนโลยีสารสนเทศที่นำมาใช้ในองค์กรในกระบวนการยุติธรรมจะเอื้อต่อการจัดการความรู้ในกระบวนการยุติธรรม (Criminal Justice Knowledge Management) ต่อไปในอนาคต

การนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กรให้มีประสิทธิภาพเป็นเรื่องที่จะต้องมีการวางแผนการดำเนินการให้เหมาะสม ตั้งแต่เริ่มต้นลำดับขั้น คือ เริ่มจากขั้นการริเริ่ม[3] (Initiation) ที่องค์กรเริ่มร่างนโยบายเพื่อจัดสรรทรัพยากรคอมพิวเตอร์ แล้วเข้าสู่ขั้นของการบูรณาการ (Integration) ซึ่งเป็นการใช้วิทยาการด้านคอมพิวเตอร์เข้ามาเชื่อมโยงกันให้เป็นระบบสามารถแลกเปลี่ยนข้อมูลและใช้ข้อมูลร่วมกันได้ ภายในหน่วยงาน ซึ่งขั้นตอนการบริหารงาน

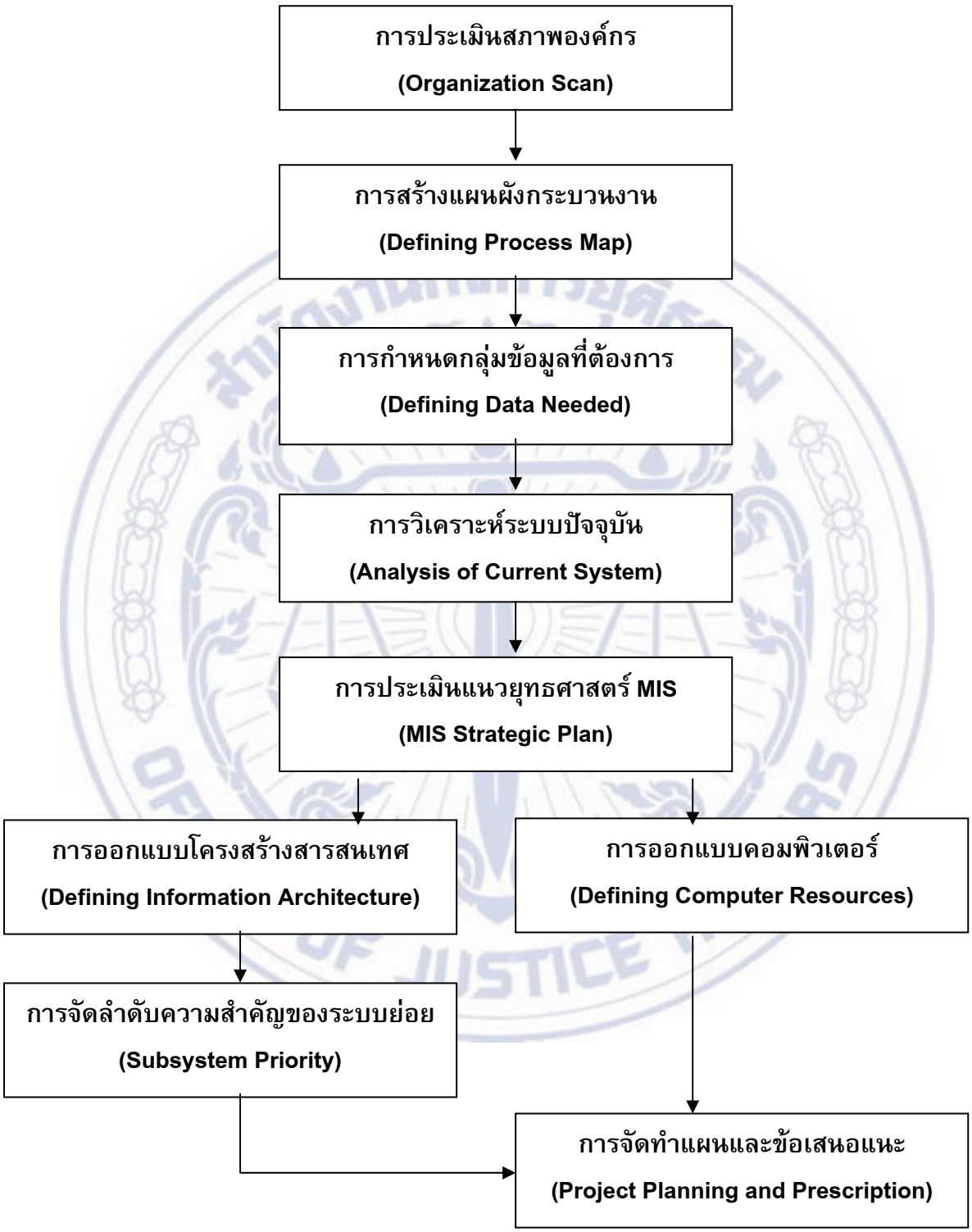
---

[3] ดำรง วัฒนา. **การนำระบบสารสนเทศไปใช้ในการปรับปรุงการบริการภาครัฐ.** หน้า 20-21.

ส่วนวิทยาการฐานข้อมูล และโทรคมนาคม จนถึงขั้นสุดท้ายที่บรลุถึงขั้นวุฒิภาวะ (Maturity) ที่ผู้บริหารระดับต่าง ๆ ตระหนักถึงความสำคัญของการนำไปใช้งานอย่างเป็นระบบเพื่อการบริหารงานขององค์การ ดังนั้นหน่วยงานจึงจะต้องสำรวจข้อมูลและวิเคราะห์ข้อมูลในระดับขั้นการบูรณาการนี้ เพื่อนำไปวางแผนระบบข้อมูลวิทยาคอมพิวเตอร์ และกำลังคน ตลอดจนการบริหาร ฯลฯ ได้เหมาะสม เพื่อเป็นพื้นฐานในการพัฒนาในระดับขั้นต่อไป ซึ่งในกระบวนการของการวิเคราะห์ข้อมูลดังกล่าว อาจสามารถนำแนวคิดการวางแผนแนวยุทธศาสตร์มาปรับใช้ ดังแผนภาพที่ 1



แผนภูมิที่ 1 : แสดงกระบวนการวางแผนยุทธศาสตร์ด้านระบบสารสนเทศ



ที่มา : เอกสารเรื่อง “การนำระบบสารสนเทศไปใช้ในการปรับปรุงการบริการภาครัฐ

2.1.1 นิยามและคำจำกัดความของข้อมูลและฐานข้อมูล (Data and Database Definitions)

ข้อมูลนั้นมีอยู่หลากหลายตามประเภทของงานที่สร้างสรรค์ขึ้น มีการให้นิยามความหมายแตกต่างกันไปบ้าง แต่ก็มีองค์ประกอบคล้ายๆ กัน ใน Webster's New World Dictionary ได้ให้นิยามคำว่า ข้อมูล (Data) ว่าหมายถึง สิ่งที่แสดงถึงข้อเท็จจริง (Facts) หรือแนวความคิด (Concept) หรือข้อแนะนำ (Instructions) อย่างเป็นทางการและเหมาะสม หรืออาจจะเป็นการแสดงออกถึงคุณลักษณะ (Characters) หรือปริมาณ (Analog quantities) ที่มีหรืออาจมีความหมาย[4] เมื่อมีข้อมูลแล้ว ถ้าไม่จัดไว้ให้เป็นระเบียบในเรื่องหรือหมวดเดียวกันก็จะยุ่งยากต่อการค้นหาเพื่อนำมาใช้ (Utilization) จึงมีวิธีจัดการเกี่ยวกับข้อมูล (Data or Data item management) ซึ่งทำให้ทราบว่าข้อมูลนั้นๆ อยู่ในที่ใด

ข้อมูลแต่ละเรื่องอาจมีประโยชน์ต่อบุคคลบางคน หรือบางสถาบันก็ได้ แต่ข้อมูลอย่างเดียวกันอาจจะไม่เป็นประโยชน์ต่อคนอื่นๆ ก็ได้ ข้อมูลที่ไม่เป็นประโยชน์นี้เรียกว่าข้อมูลดิบ (Raw data) แต่ข้อมูลดิบก็อาจเป็นประโยชน์เมื่อนำไปผ่านการประมวลผล (Data processing system) หรือ ระบบจัดทำเกี่ยวกับข้อมูล (Data manipulation) โดยทำให้ข้อมูลดิบอยู่ในรูปแบบที่กะทัดรัด (Compact) ทำให้มีความหมายนำมาใช้สอยได้ เมื่อได้ข้อมูลของแต่ละเรื่อง ซึ่งอาจมีเป็นจำนวนมาก จึงมีวิธีเก็บรวบรวมไว้ด้วยกัน เรียกว่า ฐานข้อมูล (Database)

ฐานข้อมูล (Database) หมายถึง การรวบรวมข้อมูลที่จะใช้ร่วมกันเข้าด้วยกัน โดยใช้เครื่องจักรกลเข้ามาช่วย และในองค์กรมีการกำหนดรูปแบบที่แน่นอนของข้อมูลที่ใช้ร่วมกันเหล่านี้ มีการจัดลำดับตามคุณค่าของข้อมูลแต่ละประเภทเพื่อสะดวกในการใช้สอย โดยอาจจะมีการรวบรวมภายใต้การควบคุมจากศูนย์กลางเดียวกัน จากนิยามดังกล่าว ฐานข้อมูลจึงไม่รวมข้อมูลที่ไม่เป็นทางการ ข้อมูลส่วนบุคคล หรือ ข้อมูลที่เก็บรวบรวมไว้ด้วยมือ (Manual)

ทั้งนี้ ข้อมูล (Data) นั้นก็หมายความรวมถึงข้อเท็จจริง (Fact) ต่างๆ ทั้งที่อยู่ในรูปของข้อความ (Text) รูปภาพ (Image) สูตร (Formula) และสื่อผสม (Multimedia) นอกจากนี้ข้อมูลดังกล่าวไม่จำเป็นต้องมีความหมายในตัวมันเอง หรือจะมีความหมายหรือมูลค่าก็ต่อเมื่อมีการนำไปผ่านกระบวนการ (Data processing) ก็ตาม

---

[4] Adam, Eric J. *"Second Coming for Electronic Data Interchange."* **World Trade** p.36.

เมื่อวิทยาการเจริญขึ้น มีการใช้เครื่องมืออิเล็กทรอนิกส์ อย่างเช่น คอมพิวเตอร์ในการจัดเก็บข้อมูล นับแต่มีการปฏิวัติคอมพิวเตอร์เพื่อการค้าทำให้เกิดความเป็นระเบียบ (Formalization) มากขึ้น และรูปแบบของข้อมูลที่จัดเก็บนั้นก็เปลี่ยนไป สามารถรวมเรียกได้ว่าข้อมูลและฐานข้อมูลทางอิเล็กทรอนิกส์ (Electronic database) ฐานข้อมูลอิเล็กทรอนิกส์นี้ง่ายต่อการนำข้อมูลมาใช้และการทำซ้ำ ทั้งยังรวดเร็วกว่าการเก็บข้อมูลในฐานข้อมูลที่เป็นกระดาษ โดยที่ฐานข้อมูลแต่ละเรื่องแยกเป็นเอกเทศภายในองค์กรนั้นๆ และระบบฐานข้อมูลอิเล็กทรอนิกส์ยังเป็นเอกเทศจากระบบคอมพิวเตอร์โดยรวมขององค์กรอีกด้วย และถ้าหากมีการพัฒนาข้อมูลและฐานข้อมูลอย่างเต็มรูปแบบ คือการนำข้อมูลมาจัดลำดับตามคุณค่าของข้อมูล โดยที่คุณค่าของข้อมูลก็ขึ้นกับข้อมูลแต่ละประเภท ก็จะเป็นการเพิ่มคุณค่าของข้อมูลที่ได้เก็บรวบรวมไว้ให้มากขึ้นอีกด้วย

ในระบบข้อมูลขนาดใหญ่ เราจะพบว่าข้อมูลในแต่ละแฟ้มข้อมูลจะเกี่ยวข้องกัน เราจึงมีการนำแฟ้มข้อมูลที่เกี่ยวข้องกันนั้นมารวมเข้าไว้ด้วยกัน ด้วยหลักการทางการจัดการฐานข้อมูล ซึ่งทำให้การเก็บข้อมูลนั้นไม่ซ้ำซ้อนกัน และสามารถเรียกใช้ข้อมูลได้อย่างรวดเร็ว แต่ทั้งนี้ไม่ได้หมายความว่าในองค์กรหนึ่งๆ จะต้องมีระบบฐานข้อมูลระบบเดียวกัน แต่หมายความว่าข้อมูลทั้งหมดที่อยู่ในระบบฐานข้อมูลจะต้องมีความสัมพันธ์กัน

2.1.2 โครงสร้างและองค์ประกอบของข้อมูลอิเล็กทรอนิกส์ (Data in Electronic Form) โครงสร้างและองค์ประกอบของข้อมูลอิเล็กทรอนิกส์จะประกอบด้วย[5]

1. บิท (Binary digit : bit) เป็นส่วนประกอบหน่วยที่เล็กที่สุดของข้อมูลที่คอมพิวเตอร์สามารถทำความเข้าใจ ได้ประกอบด้วยตัวเลขฐานสองสองตัว คือ 0 และ 1 แทนสถานะของการทำงานสองลักษณะคือ การเปิด-ปิดวงจร อันเป็นหลักการทำงานขั้นพื้นฐานของระบบดิจิตอล

2. หน่วยข้อมูล (Data item) เป็นส่วนที่เล็กที่สุดของข้อมูลที่ผู้ใช้รู้จักประกอบด้วย ตัวอักขระหรือสัญลักษณ์พิเศษ แต่ไม่มีความหมายในตัวเอง

3. ฟิลด์ข้อมูล (Field) เป็นการนำหน่วยข้อมูลมารวมเข้าไว้ด้วยกัน ทำให้สามารถสื่อความหมายได้

---

[5] Josph N.Ulman,Jr. and Jay R.Gould **Technical Report** p.59

4.ระเบียนข้อมูลหรือเรคคอร์ด (Record) เป็นการบันทึกรวบรวมเอาฟิลด์หลายๆ ฟิลด์ที่สัมพันธ์กันเข้าไว้ด้วยกัน

5. แฟ้มข้อมูลหรือไฟล์ข้อมูล (File) คือ การรวบรวมข้อมูลหลายๆ ระเบียนเข้าไว้ด้วยกัน โดยมักจะเรียงลำดับระเบียนเพื่อให้สะดวกต่อการค้นหาและจะมีฟิลด์หนึ่งฟิลด์ที่ใช้สำหรับการอ้างอิงระเบียน ซึ่งเรียกว่า คีย์ฟิลด์ (key field) แต่จะต้องไม่มีการเก็บข้อมูลซ้ำกันในแต่ละคีย์ฟิลด์ของทุกระเบียน โดยทั่วไปแฟ้มข้อมูลแบ่งเป็น 2 ประเภท คือ

(1) แฟ้มข้อมูลหลัก (Master file) หมายถึง แฟ้มข้อมูลที่ใช้เก็บข้อมูลที่สนใจจะเป็นแฟ้มข้อมูลถาวร มีการเปลี่ยนแปลงน้อย

(2) แฟ้มข้อมูลชั่วคราว (Transaction file) เป็นแฟ้มข้อมูลที่ใช้เก็บข้อมูลที่มีการเปลี่ยนแปลงบ่อยๆ

ก.โครงสร้างและองค์ประกอบของฐานข้อมูลอิเล็กทรอนิกส์ (Electronic Database System) ประกอบด้วย

1. ข้อมูล (Data) ข้อมูลที่ถูกเก็บอยู่ในระบบฐานข้อมูลนั้น มีอยู่มากมายหลายประเภท การเก็บบันทึกข้อมูลเหล่านั้นอย่างเป็นระบบ จึงจำเป็นต้องมีการจำแนกประเภทของข้อมูลเพื่อที่จะสามารถกำหนดเรคอร์ดและฟิลด์ในระบบฐานข้อมูลได้ และยังจำเป็นที่จะต้องมีกลไกภายในที่บำรุงรักษาข้อมูลที่เก็บบันทึกไว้นั้น จนสามารถรู้ได้ว่าส่วนประกอบเฉพาะแต่ละส่วนนั้นเก็บบันทึกอยู่ที่ไหน นอกจากนี้จะต้องทราบวิธีการใส่หรือเพิ่มข้อมูลลงในฐานข้อมูล แก้ไขจัดเรียงข้อมูล ดึงข้อมูลทั้งหมดหรือบางส่วนออกจากฐานข้อมูล ดังนั้นการจัดระบบฐานข้อมูลจึงมีความจำเป็นสำหรับการจัดเตรียมบริการให้กับผู้ใช้ได้เข้าถึงข้อมูลอย่างสะดวก

2. ฮาร์ดแวร์ (Hardware) เป็นอุปกรณ์ที่ใช้ในการเก็บข้อมูลต่างๆ และเรียงข้อมูลให้เป็นลำดับเพื่อสะดวกในการนำข้อมูลมาใช้

3. ซอฟแวร์ (Software) เป็นคำสั่งที่ใช้ควบคุมการรับส่งข้อมูลในแต่ละระดับ เพื่อให้สามารถเพิ่ม ลบ ค้นหาข้อมูล และเปลี่ยนแปลงข้อมูล ทำให้การจัดการเก็บข้อมูลสะดวกและง่ายดายขึ้นมาก

4. ผู้ใช้ (Users) มี 3 ส่วน คือ

4.1 ผู้เขียนโปรแกรมประยุกต์ในภาษาต่างๆที่ใช้คู่กับระบบฐานข้อมูล

4.2 ผู้ปฏิบัติงานระบบฐานข้อมูล เป็นผู้รู้วิธีการและสามารถใช้อุปกรณ์ต่างๆ ได้อย่างคล่องแคล่วเพื่อจัดการเก็บข้อมูล

4.3 ผู้ควบคุมดูแลระบบทั้งหมด ไม่ว่าจะเป็นเรื่องการออกแบบระบบการจัดการเรื่องฮาร์ดแวร์ หรือ ทรัพยากรอื่นๆ ทั้งยังเป็นผู้กำหนดคัดเลือกผู้ที่จะเข้ามาใช้งานในระบบ หรือใช้งานข้อมูลแต่ละส่วน

แม้ว่าจะมีการกำหนดนิยามและคำจำกัดความของข้อมูลและฐานข้อมูล รวมทั้งโครงสร้างและองค์ประกอบของข้อมูลและฐานข้อมูลกันไว้แล้ว แต่ในความเป็นจริงการกำหนดนิยาม โดยเฉพาะอย่างยิ่งนิยามของฐานข้อมูลว่าเป็น “การรวบรวมข้อมูลที่จะใช้รวมกันเข้าด้วยกัน” นั้นกว้างมากจนอาจมองไม่ออกเลยว่าฐานข้อมูลนั้นมีความสำคัญอย่างไรต่อการพัฒนาเศรษฐกิจและสังคมของมนุษย์ และจำเป็นมากน้อยเพียงใดจึงต้องบัญญัติกฎหมายเพื่อคุ้มครองสิทธิของข้อมูลนั้นๆ

สำหรับการให้บริการฐานข้อมูลบนอินเตอร์เน็ตนั้น ผู้ให้บริการมักจะมีกลยุทธ์ป้องกันฐานข้อมูลของตนเอง (Self-help) ดังนี้

ก.การใช้รหัสลับ (Passwords) โดยเว็บไซต์ส่วนใหญ่มักจะให้ผู้ใช้บริการสามารถเข้าถึงฐานข้อมูลที่จำกัด เพื่อเป็นตัวอย่างเท่านั้น หากต้องการใช้ฐานข้อมูลอย่างไม่มีข้อจำกัดก็จำเป็นต้องสมัครเป็นสมาชิก และผู้ใช้บริการก็จะได้รับรหัสลับเพื่อเข้าถึงฐานข้อมูลได้

ข.เว็บไซต์ที่สืบค้นข้อมูลเท่านั้น (Search only web sites) กล่าวคือ ผู้ใช้จะต้องแสดงความต้องการสิ่งที่ตนเองต้องการค้นหา แล้วผู้ใช้บริการเว็บไซต์นั้นจะเป็นคนทำการสืบค้นฐานข้อมูลนั้นให้และจะแสดงผลการสืบค้นให้ผู้ใช้บริการทราบ

ค.บางฐานข้อมูลมีรายได้จากการจำหน่ายรายชื่อ (Clearinghouses) แทนที่จะเก็บค่าบริการจากผู้ใช้ ตัวอย่างที่เห็นได้ชัดคือ เว็บไซต์หางาน ซึ่งบริษัทที่ต้องการประกาศโฆษณาหาคนงานจะเป็นผู้จ่ายค่าโฆษณานั้น

ง.การขายพ่วง (Product Ties) กล่าวคือ ในหลายเว็บไซต์ได้นำเสนอฐานข้อมูลเพื่อต้องการจำหน่ายหรือโฆษณาผลิตภัณฑ์หรือบริการหลักของตน (Core business) มากกว่าตัวผลิตภัณฑ์ฐานข้อมูลนั้นเอง

จากกรณีตัวอย่างของฐานข้อมูลที่กล่าวมานั้น จะเห็นได้ว่ามีฐานข้อมูลเพียงบางประเภทเท่านั้นที่ต้องการความคุ้มครองในรูปของกฎหมาย และโดยทั่วไปผู้ให้บริการฐานข้อมูลที่เกี่ยวกับข้อมูลของรัฐบาล และการศึกษาที่มีอยู่ในปัจจุบันนั้น มักจะมีเป้าหมายในการกระจายความรู้หรือข้อมูลในฐานข้อมูลเป็นเป้าหมายหลักมากกว่าผลประโยชน์ทางการค้า จึงมักไม่มีการ

จัดเก็บค่าบริการจากผู้ใช้หรือกาจจัดเก็บในราคาต่ำ โดยเฉพาะรัฐบาลส่วนใหญ่มักมีนโยบายทางด้านเทคโนโลยีสารสนเทศในทำนองว่ารัฐบาลมีหน้าที่ให้บริการข้อมูลและสารสนเทศพื้นฐานแก่ประชาชน ดังนั้นรัฐบาลมักเป็นผู้จัดทำฐานข้อมูลเอง โดยไม่การจัดเก็บค่าบริการแก่ผู้ใช้แต่ประการใด

2.2 ข้อมูลสารสนเทศในกระบวนการยุติธรรม

ในอดีตข้อมูลสารสนเทศในกระบวนการยุติธรรมมีการจัดแบ่งโดยมีการแบ่งระดับอาชญากรรมโดยใช้เกณฑ์ความร้ายแรง Crime Seriousness Scales เป็นการกำหนดระดับความรุนแรงของอาชญากรรมโดยการให้น้ำหนักของอาชญากรรมในแง่ของความสัมพันธ์ความรุนแรงที่เกิดขึ้น การรวบรวมและการรายงานข้อมูลเหล่านั้น จึงเป็นการรวบรวมและนำเสนอในรูปของประเภทของการประกอบอาชญากรรมเป็นหลัก ซึ่งการดำเนินการแม้ว่าจะเริ่มต้นที่ฝรั่งเศส แต่การดำเนินการที่เป็นระบบเกิดขึ้นที่สหรัฐอเมริกา โดยมีการจัดแบ่งการดำเนินการดังนี้

1.UCR crime index

แบบรายงานการประกอบอาชญากรรม (Uniform Crime Report : UCR) เป็นแบบรายงานการประกอบอาชญากรรมที่รู้จักกันดีของเอฟบีไอของอเมริกา เป็นการเก็บข้อมูลด้านสถิติการก่ออาชญากรรม โดยหน่วยเอฟ บี ไอ ได้รวบรวมข้อมูลจากกรมตำรวจอเมริกามากกว่า 16000 หน่วย ซึ่งนอกจากจะมีข้อมูลบรรจุแล้วยังมีการวิเคราะห์เกี่ยวกับดัชนีอาชญากรรม (index crime) มีการจัดประเภทการประกอบอาชญากรรมประเภทต่างๆ เช่น การฆ่าผู้อื่น ทำร้ายร่างกาย วางเพลิง โจรกรรมรถยนต์ เป็นต้น โดยมีตารางระบุลักษณะการประกอบอาชญากรรมด้วย ข้อมูลเหล่านี้จะมีการตีพิมพ์เผยแพร่รายปีจำแนกตามพื้นที่ด้วย แบบรายงาน UCR นี้ยังให้ข้อมูลเกี่ยวกับจำนวนและลักษณะส่วนบุคคล (อายุ ชาติพันธุ์ เพศ)

วิธีการที่ใช้ในการรวบรวมข้อมูล UCR ค่อนข้างจะมีความซับซ้อน เนื่องจากในแต่ละเดือน หน่วยงานที่ทำหน้าที่ในการบังคับใช้กฎหมาย ได้รายงานตัวเลขและข้อมูลการประกอบอาชญากรรมที่ได้รับแจ้ง ข้อมูลทั้งหมดเป็นข้อมูลที่ได้จากการแจ้งความโดยผู้เสียหาย อย่างไรก็ตาม หากการสืบสวนสอบสวนไม่คืบหน้าไม่มีการดำเนินการใดๆ ข้อมูลก็จะถูกตัดออกไป[6] ดังนั้น ข้อมูลที่รายงานจึงเป็นข้อมูลที่รู้ตัวผู้กระทำผิดอย่างแท้จริง “(actual offense known)”

---

[6] Larry J. Siegel. **Criminology’ Theories, Patterns and Typologies.** p.46

UCR ใช้วิธีการ 3 วิธีในการแสดงข้อมูลด้านการประกอบอาชญากรรม กล่าวคือ ประการแรก จำนวนผู้ประกอบการอาชญากรรมที่มีการรายงานต่อเจ้าหน้าที่ตำรวจและถูกจับกุมจะมีการรายงานอย่างหยาบๆ เช่น จำนวนผู้ถูกฆาตกรรมในปี 2005 เท่ากับ...คน) และประการที่สอง แสดงอัตราการเปลี่ยนแปลงเป็นอัตราร้อยละ เพื่อชี้ให้เห็นว่ามีการประกอบอาชญากรรมเพิ่มสูงขึ้นหรือลดลง ประการสุดท้าย จะแสดงอัตราการเกิดอาชญากรรม โดยคำนวณจากหนึ่งแสนคน ตามสูตรคือ

<u>จำนวนผู้ประกอบอาชญากรรม</u> X 100,000 = อัตราการเกิดอาชญากรรม
จำนวนพลเมืองทั้งหมด

อย่างไรก็ตามการเก็บรวบรวมข้อมูลแบบ UCR ก็ยังประสบปัญหาหลายประการคือ

1. อาชญากรรมในระดับประเทศ (federal crime) ไม่ได้มีการรายงาน

2. การรายงานข้อมูลเป็นเรื่องของความสมัครใจของหน่วยงาน ดังนั้นความถูกต้องเที่ยงตรง และความสมบูรณ์ของข้อมูลก็ยังขาดไป

3. หน่วยงานที่รายงานไม่ใช่ทุกหน่วย/ สถานีตำรวจ

4. การประมาณค่าการประกอบอาชญากรรม FBI ใช้การคาดประมาณ

5. อาชญากรคนหนึ่งอาจก่ออาชญากรรมหลายประเภท แต่มีการรายงานเฉพาะอาชญากรรมรุนแรงเท่านั้น เช่น อาชญากรที่ถูกจับอาจกระทำผิดทั้งมีการข่มขืน การโจรกรรม การฆาตกรรม

6. รวมเอาการกระทำผิดฐานพยายามกระทำผิด กับการกระทำความผิดสำเร็จเข้าด้วยกัน

7. การให้ความหมาย ขอบเขต ของการประกอบอาชญากรรมในแต่ละมลรัฐแตกต่างกัน

8. แยกการลงการกระทำให้สมคบกันกระทำความผิด

จากปัญหาและอุปสรรคต่างๆก็ได้มีการพยายามเพิ่มในรายละเอียดของการกระทำลงไป เช่น จากการข่มขืน (rape) ก็เป็นการข่มขืนโดยใช้กำลังประทุษร้าย (Forcible rape) เป็นต้น และมีการพยายามพัฒนาแบบรายงานใหม่ในรูป National Incident-Based Reporting System (NIBRS) ขึ้นมาแทน

2. NCVS

NCVS เป็นตัวย่อของแบบสำรวจระดับชาติถึงการตกเป็นเหยื่ออาชญากรรม (The National Crime Victimization Survey : NCVS) เนื่องจาก การเก็บข้อมูลจากผู้เสียหายหรือเหยื่อจากการประกอบอาชญากรรมจะเป็นข้อมูลที่พาดพิงไปถึง ลักษณะ สาเหตุ ประเภท และพฤติกรรมการประกอบอาชญากรรมด้วย ข้อมูลที่ได้มาจากการสอบถามเหยื่อหรือผู้เคราะห์ร้าย เนื่องจากในอดีต ไม่ได้มีการสอบถามและเก็บข้อมูลเหยื่อ และข้อมูลผู้เสียหายก็จะเป็นข้อมูลที่ใช้ปิดช่องว่างจากการถูกโจมตีว่า การเก็บข้อมูลจากการประกอบอาชญากรรม (The dark figures of crime)

ในการดำเนินการสำรวจถึงการตกเป็นเหยื่ออาชญากรรม เริ่มครั้งแรกเริ่มในปี ค.ศ. 1966 โดยสำรวจจากหนึ่งแสนครัวเรือน โดยเป็นหนึ่งในโครงการดำเนินการของกรรมาธิการของประธานาธิบดีว่าด้วยการบังคับใช้กฎหมายและการบริหารงานยุติธรรม (The President's Commission on Law Enforcement and The Administration of Justice) คณะกรรมาธิการชุดนี้ได้พยายามจะเอาผู้นำหน่วยที่เกี่ยวข้องกับการบังคับใช้กฎหมาย และนักวิชาการผู้เชี่ยวชาญ มาทำงานร่วมกันเพื่อพัฒนาภาพรวมของปัญหาอาชญากรรมที่เกิดขึ้นในสหรัฐอเมริกาและพยายามที่จะดูว่า กระบวนการยุติธรรมที่มีอยู่ตอบสนองหรือดำเนินการกับการก่ออาชญากรรมอย่างไร ซึ่งผลจากการสำรวจพบว่า การก่ออาชญากรรมที่เกิดขึ้นในสหรัฐอเมริกานั้นมีผู้ที่ตกเป็นเหยื่อสูงกว่าที่เคยคาดประมาณกันไว้ โดยที่ผู้ที่ตกเป็นเหยื่อจำนวนไม่น้อยที่ไม่ได้ไปแจ้งความ เนื่องจากสาเหตุต่างๆ เช่น ความหวาดกลัว ความอับอาย การคิดว่าแจ้งไปก็ไม่เกิดประโยชน์อะไร [7]

ต่อมาได้มีการพัฒนาแบบสำรวจนี้ให้มีมาตรฐานมากยิ่งขึ้นมีการนำไปขยายการจัดเก็บมากยิ่งขึ้น ใช้เทคนิคต่างๆ ในการวิเคราะห์มากขึ้น ทำให้ข้อมูลที่ได้รับสามารถนำมาจัดเก็ฐประมวลผลอย่างเป็นระบบและใช้งานมากยิ่งขึ้น

NCVS เป็นกลุ่มความผิดที่ถูกเลือกมาเพื่อใช้วัดความเปลี่ยนแปลงในจำนวนและอัตราของอาชญากรรมที่ได้รับการรายงานจากหน่วยงานที่บังคับกฎหมายของรัฐบาล UCR Crime Index ได้ถูกแนะนำครั้งแรกโดยผู้อำนวยการหน่วยตำรวจสืบสวนกลาง J. Edgar Hoover ในรายงาน Uniform Crime Reporting : Report of the Consultant Committee (September 1958) ซึ่งข้อแนะนำได้รับการยอมรับโดยหน่วยงาน FBI และ Crime Index คือ

---

[7] Alfred Blumstein, Jacqueline Cohen, and Richard Rosenfeld "Trend and Deviance in Crime Rates: A Comparison of UCR and NCUS data for Burglary and Robbery" **Criminology 29** p.237

ความผิด Part I ซึ่งประกอบไปด้วย อาชญากรรมที่มีความรุนแรง (Violent Crime) ได้แก่ ฆาตกรรมและฆ่าผู้อื่นโดยไม่เจตนา ข่มขืนโดยใช้กำลังประทุษร้าย ชิงทรัพย์ ทำร้ายร่างกายผู้อื่นเป็นอันตรายสาหัส และอาชญากรรมที่มุ่งต่อทรัพย์สิน (Property Crime) ได้แก่ ลักทรัพย์ในเคหะสถาน ลักทรัพย์ โจรกรรมรถยนต์ – รถจักรยานยนต์ วางเพลิง รวมทั้งสิ้น 7 ประเภท ซึ่งทั้งหมดเป็นความผิดที่ได้รับการพิจารณาว่า

1. เป็นความผิดร้ายแรง

2. มีความถี่ในการเกิดขึ้นโดยหน่วยงานตำรวจได้รับรายงานเกี่ยวกับความผิดนั้นอย่างสม่ำเสมอ

3. เป็นความผิดที่มีการกระจายการเกิดขึ้นทั่วประเทศ

4. สามารถเก็บข้อมูลลักษณะความผิดที่เกิดขึ้นได้อย่างถูกต้องสามารถนำมาคำนวณ

5. เป็นความผิดที่สะท้อนให้เห็นถึงปัญหาของการบังคับใช้ Common Law ของประเทศ

UCR ได้กำหนดประเภทของข้อความผิดออกเป็นสองประเภท คือ Index crime ซึ่งเป็นความผิดร้ายแรง ในครั้งแรกเป็นความผิดหลัก 7 ประเภท จนกระทั่งเมื่อเดือนตุลาคม 1978 สภาคองเกรทได้ผ่านกฎหมายให้การวางเพลิงได้รับการบรรจุเข้ามาอยู่ในกลุ่ม 1 ที่เป็นความผิดร้ายแรงรวมเป็น 8 ประเภทด้วยกัน

ส่วนกลุ่มที่สอง Non-index crime เป็นความผิดอาญาทั่วไปจำนวน 20 ความผิด เช่น ทำร้ายร่างกาย การทำลายทรัพย์สิน การพนัน เมาสุราอาละวาด เป็นต้น

3.NCVRS

เนื่องจากวัตถุประสงค์ของการศึกษา NCVS นี้มุ่งเน้นไปยังอาชญากรรมที่ไม่ถูกบันทึกโดยหน่วยงานที่บังคับใช้กฎหมายของทางการเป็นสำคัญ ดังนั้นการวัดจึงมีบางส่วนที่ทับซ้อนกันกับ UCR แต่ไม่เหมือนกันในกลุ่มของความผิด โดย NCVRS จะรวมอาชญากรรมทั้งที่ถูกรายงานและไม่ถูกรายงานไปยังหน่วยงานที่บังคับใช้กฎหมายเข้าไว้ด้วยกัน เช่น NCVS จะไม่นำความผิดร้ายแรงที่อยู่ใน UCR คือ homicide, arson, commercial crimes และ อาชญากรรมต่อเด็กที่มีอายุต่ำกว่า 12 เข้ามารวม ในขณะที่ UCR ก็ไม่มีความผิดประเภท simple assault และ sexual assaults ที่นอกเหนือจาก forcible rape มารวม ซึ่งเป็นความ

แตกต่างกันในการแบ่งประเภทความผิดของทั้งสองวิธี ต่อมา NCVS ได้มีการเปลี่ยนแปลงในเรื่องของการแบ่งกลุ่มความผิด โดยเฉพาะอย่างยิ่งการเปลี่ยนแปลงในเรื่องของการลักทรัพย์ในอาชญากรรมต่อบุคคลไปสู่การลักทรัพย์อาชญากรรมต่อทรัพย์สิน ซึ่งรูปแบบเดิม การลักทรัพย์ถูกจัดไว้ในกลุ่มอาชญากรรมต่อบุคคลหรือครัวเรือน ขึ้นอยู่กับสถานที่เกิดเหตุ

อย่างไรก็ตาม ในปัจจุบันระบบข้อมูลด้านงานยุติธรรม (Criminal Justice Information System) อาจจะจำแนกโดยทั่วไปได้ 2 ประเภท คือ

1) ข้อมูลที่มีการรายงานต่อสาธารณะ (Public record information) ข้อมูลเหล่านี้ได้แก่ รายงานการโจรกรรมทรัพย์สิน รายงานการจับกุม รายชื่อผู้กระทำผิดทางเพศ เป็นต้น

2) ข้อมูลการสืบสวนสอบสวน (Investigative system) โดยปกติข้อมูลการสืบสวนสอบสวนมักจะเป็นข้อมูลที่ยังไม่สามารถเปิดเผยได้ เนื่องจากยังอยู่ในระหว่างการดำเนินการสืบสวนสอบสวน เช่น รายชื่อผู้ต้องสงสัย ผู้ให้ข้อมูล ผู้เสียหาย พยาน เป็นต้น ข้อมูลเหล่านี้ บางครั้งมีรายละเอียดเกี่ยวกับตัวบุคคล เช่น วัน เดือน ปีเกิด สัญชาติ เชื้อชาติ หรือรายละเอียดส่วนบุคคล เป็นต้น ข้อมูลเหล่านี้บางครั้งก็เป็นข้อมูลเชิงเทคนิค เช่น ลายพิมพ์นิ้วมือ เป็นต้น ข้อมูลกลุ่มนี้อาจเป็นข้อมูลในหน่วยงานของกระบวนการยุติธรรมที่สามารถดำเนินการแลกเปลี่ยน และหรือบูรณาการข้อมูลได้ และรัฐบาลและมลรัฐต่างๆ เช่น ในสหรัฐอเมริกา ได้พยายามให้มีการแยกฐานข้อมูลที่ระบุ DNA หรือ DNA identification data base ออกมาโดยเฉพาะ นอกจากนี้ยังมีฐานข้อมูลในกลุ่มที่สองนี้บางประเภทที่ไม่สามารถเปิดเผยได้ เช่น ข้อมูลเกี่ยวกับการโจรกรรมต่างๆ เป็นต้น

ในสหรัฐอเมริกานั้น หากจำแนกหน่วยงานในกระบวนการยุติธรรมในระดับประเทศ ระดับมลรัฐ และระดับท้องถิ่น รวมกันทุกเขตมีหน่วยงานถึง 19,000 หน่วย ในขณะที่หน่วยงานของตำรวจมีเกือบ 200 หน่วย ซึ่งหน่วยงานต่างๆเหล่านี้ ทั้งตำรวจ อัยการ ศาล ราชทัณฑ์ คุมประพฤติ หน่วยสืบสวนสอบสวนพิเศษ เช่น FBI ต้องการข้อมูลที่จัดเก็บในระบบฐานข้อมูล การเชื่อมต่อและการบูรณาการข้อมูลเพื่อใช้ในระดับชาติทั้งสิ้น สิ่งที่ต้องกระทำให้เกิดขึ้นก็คือ ความถูกต้องของข้อมูล (Accuracy) การตรวจสอบและดำเนินการให้ถูกต้อง บุคคลผู้ที่มีสิทธิเข้ามาใช้วัตถุประสงค์ของการเก็บและใช้ข้อมูล ระยะเวลาในการเก็บ ระบบการป้องกันการนำเอาข้อมูลเหล่านี้ไปใช้ในทางที่ผิด การดำเนินการเหล่านี้ยังรวมถึงข้อคำถามที่ว่า ข้อมูลชนิดหรือประเภทใดที่ควรจะเปิดเผยต่อสาธารณะได้ ไม่ว่าโดยทั่วไปหรือผ่านระบบ Internet และการเชื่อมโยงและบูรณาการข้อมูลอย่างไรในอนาคต เพื่อให้การพัฒนามีประสิทธิภาพยิ่งขึ้น

ในส่วนของระบบข้อมูลที่มีการบูรณาการและจัดทำเครือข่ายที่ดำเนินการในสหรัฐอเมริกาในปัจจุบัน ได้แก่[8]

1. NLETS (The National Law Enforcement Telecommunications Systems)

NLETS เป็นเครือข่ายระดับชาติที่เชื่อมข้อมูลกับรัฐต่างๆ และหน่วยงานของรัฐบาลกลางเข้าด้วยกัน เพื่อการแลกเปลี่ยนข้อมูลด้านกระบวนการยุติธรรมทั้งหมดในแต่ละมลรัฐ จะมีหน่วยงานแนวหน้าหลักที่รับผิดชอบในการดูแลระบบการสื่อสารทางไกลเกี่ยวกับการบังคับใช้กฎหมายและถ่ายทอดส่งต่อข้อมูลไปยังทุกหน่วยที่เกี่ยวข้องรายย่อยๆในมลรัฐ ซึ่งในการเชื่อมโยงดังกล่าวมีหน่วยงานด้านกระบวนการยุติธรรม ที่มีหน้าที่บังคับใช้กฎหมายราว 102 แห่งในแต่ละมลรัฐที่สามารถสื่อและใช้ระบบข้อมูลเหล่านี้

หน่วยงานที่เข้ามามีบทบาทในการใช้ข้อมูลเหล่านี้ได้แก่ ตำรวจ อัยการ คุมประพฤติ หน่วยพักการลงโทษ เป็นต้น หน่วยงานต่างๆเหล่านี้ พบว่ามีการเข้าใช้มากกว่า 1 ล้านตรั้ง และในแต่ละวัน มีผู้เข้าใช้สูงถึง 327,000 ราย

ข้อมูลต่างๆที่เกี่ยวข้องกับกระบวนการยุติธรรมที่จัดเก็บโดย NLETS ได้แก่

1) ข้อมูลการจดทะเบียนยานพาหนะ (Vehicle Registration Information)

2) ข้อมูลใบอนุญาตขับขี่ (Drivers License Information)

3) ทะเบียนประวัติอาชญากร (Criminal History Records)

4) ข้อมูลการจดทะเบียนเรือและรถสำหรับวิ่งในหิมะ (Boat and Snowmobile Registration)

5) ข้อมูลการคุมประพฤติและการพักการลงโทษ (Parole and Probation Information)

6) ข้อมูลด้านการกระทำความผิดทางเพศ (Sex Offender Registration Information)

อย่างไรก็ตาม ข้อมูลบางประเภท เช่น เรือ และ รถวิ่งในหิมะ หรือ ข้อมูลการคุมประพฤติและพักการลงโทษอาจเป็นข้อมูลที่ไม่ได้มีในทุกมลรัฐ (บางมลรัฐไม่มีคลอง หรือแม่น้ำที่จะสัญจรทางเรือ หรือ การใช้รถวิ่งในหิมะ ส่วนข้อมูลเกี่ยวกับคดีทางเพศนั้น ถือเป็นข้อมูลสำคัญ เพราะผู้ก่อคดีทางเพศมักจะก่อคดีซ้ำ (Recidivism) และมักใช้เพื่อเฝ้าระวังการกระทำผิด

---

[8] Dunworth Terrance *"Criminal Justice and the it Revolution"* **Federal Probation** p.4.

นอกจากข้อมูลหลักเหล่านี้แล้ว NLETS ยังมีข้อมูลอื่นๆที่เชื่อมต่อ สามารถเข้าถึงและใช้ประโยชน์ได้ในการดำเนินการด้านกระบวนการยุติธรรม เช่น

- ข้อมูลด้านอาวุธปืน (A TF Gun Tracking Data)
- ข้อมูล FAA Tracking Information
- ข้อมูล FAA Aircraft Registration Data
- ข้อมูล National Impound Vehicle File
- ข้อมูลด้านดัชนีชี้วัดยาเสพติด (National Drug Pointer Index)
- ข้อมูลเกี่ยวกับวัตถุมีพิษและอันตราย (Hazardous Material Information)
- ข้อมูลของศูนย์สนับสนุนการบังคับใช้กฎหมาย (INN's Law Enforcement Support Center)

ยังมีข้อมูลที่ได้เชื่อมต่อและสามารถเก็บได้จากแคนาดา โดยใช้ระบบ NLETS คือ

- ข้อมูลบุคคลที่ต้องการตัว (Wanted Persons)
- ข้อมูลยานพาหนะที่จดทะเบียนและถูกโจรกรรม (Stolen and Registered Vehicles)
- แฟ้มข้อมูลใบอนุญาตขับขี่ (Driver License Files)
- แฟ้มการโจรกรรม (Stolen Articles Files)
- แฟ้มอาวุธปืนที่ถูกโจรกรรม (Stolen Gun Files)
- แฟ้มการโจรกรรมทรัพย์ (Stolen Securities Files)
- แฟ้มเรือที่ถูกโจรกรรม (Stolen Boats Files)
- ทะเบียนประวัติอาชญากร (Criminal History Records)

หน่วยงานที่มีอำนาจเข้าใช้ NLETS ได้แก่ สมาชิกเหล่านี้

- มลรัฐ 50 มลรัฐ District of Columbia และเปอร์โตริโก้
- U.S. Department of State.
- FBI
- Treasury Enforcement Communications System (TECS)
- ศุลกากรสหรัฐ
- IRS Inspection Service
- Bureau of Alcohol Tobacco and Firearms
- กระทรวงยุติธรรมสหรัฐอเมริกา
- หน่วยปราบยาเสพติด (DEA : Drug Enforcement Administration)
- หน่วยตรวจคนเข้าเมืองและสัญชาติ(Immigration and Naturalization Service)

- U.S. Marshal's Service
- ตำรวจสากล (Interpol)
- หน่วยตรวจสอบ Postal Inspection Service
- กระทรวงกลาโหม (Department of Defense)
- หน่วย U.S. Secret Service
- ศูนย์ต่อต้านการแสวงหาประโยชน์จากเด็กและเด็กหาย (National Center for Missing and Exploited Children)
- กระทรวงมหาดไทย (Department of The Interior)
- กองทัพ (Department of the Army)
- หน่วยประกันภัยอาชญากรรม National Insurance Crime Bureau (NICB)
- สำนักงานศาลยุติธรรมอเมริกา(Administrative Office of the U.S. Courts)
- หน่วยรักษาความปลอดภัยชายฝั่ง (U.S. Coast Guards)
- หน่วยคุ้มครองรัฐ (Federal Protective Service)
- องค์กรทหารผ่านศึก (Veterans Administration)
- ตำรวจตระเวนชายแดนแคนาดา (Royal Canadian Mounted Police)
- หน่วยข่าวกรอง El Paso Intelligence Center (EPIC)

นอกจากหน่วยงานหลักต่อไปนี้แล้ว ยังมีหน่วยงานที่ไม่ใช่สมาชิก (Non – membered authorized) แต่ก็สามารถเข้าใช้ข้อมูลที่บูรณาการเหล่านี้ได้ เช่นกัน คือ

- National Institutes of Health, Protection & Security Management Branch
- U.S. Department of Agriculture, Office of Inspector General
- U.S. Department of Agriculture, Office of Inspector General
- U.S. Government Printing Office, Investigation & Security
- U.S. Department of Transportation, Odometer Fraud Division
- National Gallery of Art (Security Division)
- American Samoa Police
- Federal Aviation Administration
- Amtrak Police
- Federal Emergency Management Administration (FEMA)
- Financial Crimes Enforcement Network (Fin CEN)

2. ศูนย์ข้อมูลเครือข่ายอาชญากรรมระดับชาติ FBI (The FBI.s National Crime Information Center (NCIC) Network)

ศูนย์ข้อมูลนี้ เริ่มดำเนินการมานานแล้ว โดยเริ่มตั้งแต่ปี 1967 และมาปรับปรุงใหม่จนเป็นมาตรฐานในปี 2000 โดยเป็นชุด NCIC Version 2000 เป็นศูนย์ที่สร้างตัวชี้วัดระดับชาติ เกี่ยวกับข้อมูลด้านการโจรกรรม การประกันและข้อมูลด้านกระบวนการยุติธรรม ทั้งหมดที่หน่วยบังคับใช้กฎหมายทุกหน่วยจากทั่วประเทศต้องส่งข้อมูลให้ ทุก 12 วินาที จะมีการเปลี่ยนข้อมูลที่เข้ามาเกี่ยวกับบุคคลและทรัพย์สิน ซึ่งตำรวจทุกหน่วยจะรายงานเข้ามา รวมทั้งหน่วยงานอื่นๆ เช่น สำนักงานบังคับคดี อัยการ เป็นต้น ดังนั้น สามารถตรวจสอบรายการบุคคลหาย ทรัพย์สินถูกโจรกรรม และอื่นๆ ศูนย์ข้อมูลนี้จะมีผู้ใช้ต่อวันสูงถึง 2 ล้านราย ข้อมูลส่วนใหญ่จะถูกจำแนกเป็น 2 ส่วน คือ

1) ข้อมูลเกี่ยวกับบุคคล ข้อมูลเกี่ยวกับบุคคลจะประกอบด้วย

- รายงานบุคคลที่ต้องการตัว (Wanted Person Repords) ทั้งเด็กเยาวชนกระทำผิด และผู้ใหญ่
- รายงานคนต่างชาติ (Foreign Fugitive Reports)
- รายงานคนสูญหาย (Missing Person Reports)
- ข้อมูลคำสั่ง (Protective Order Data)
- บุคคลอันตราย (Persons of Possible Danger to Secret Services, Protectees)
- ข้อมูลทะเบียนประวัติอาชญากรทางเพศ (Sex Offenders Registration Data)
- บุคคลที่ได้รับการปล่อยตัวภายใต้การแนะนำ (Persons of Supervised Release)
- แก๊งอาชญากรรมที่ใช้ความรุนแรงและองค์กรก่อการร้าย (Violent Gang and Terrorist Organization and (Members) Data

ในเครือข่ายของ NCI C Network ยังจัดให้สามารถเข้าถึงการระบุตัวบุคคลระหว่างรัฐ โดยใช้หลัก FBI’s Interstate Identification Index (III)

โดยมีข้อมูลทะเบียนประวัติอาชญากรรมใน FBI หรือ แต่ละมลรัฐเฉพาะ ในขณะเดียวกัน ข้อมูลต่างๆที่เกี่ยวข้องเกี่ยวกับทะเบียนประวัติอาชญากร ก็จะมีการส่งเข้ามาเก็บในฐานข้อมูล เครือข่ายนี้จากรัฐต่างๆด้วย ซึ่งการดำเนินการต่างๆใช้รูปแบบเดียวกันและ

ทำการส่งเข้ามากระบบก็จะบันทึก ปรับเปลี่ยนโดยอัตโนมัติ ซึ่งก็จะลดภาระงานของ FBI ลงด้วย

3. ศูนย์ข้อมูลเครือข่ายงานยุติธรรมของ FBI (The FBI.s Criminal Justice Information Services Wide Area Network (CJIS WAN)

ศูนย์เครือข่ายข้อมูลนี้ได้เริ่มต้นเปิดดำเนินการในเดือนกรกฎาคมปี 1999 เพื่อเชื่อมโยงกับรัฐต่าง ๆ ในการบูรณาการข้อมูลด้านลายพิมพ์นิ้วมือของ FBI's Integrated Automated Fingerprint Identification Systems. (IAFIS) ระบบ WAN นี้ ได้เชื่อมต่อกันในแต่ละมลรัฐซึ่งอนุญาตให้มีการส่งลายพิมพ์นิ้วมือ ทางอิเลคโทรนิคส์ไปให้ FBI เก็บรวบรวมและเทียบเคียงกับทะเบียนประวัติได้ และยังมีการเก็บรวบรวมข้อมูลเกี่ยวกับลายนิ้วแฝง จากพื้นที่ต่าง ๆซึ่งสามารถดำเนินการเปรียบเทียบและดำเนินการได้รู้ตัวบุคคลภายในเวลา 2 ชั่วโมง โดยการประสานการทำงานกับห้องปฏิบัติการ FBI Laboratory รวมทั้งข้อมูลประกอบในด้าน DNA ที่มลรัฐต่าง ๆดำเนินการและจัดส่งให้ FBI การดำเนินการในระบะยาวจะได้มีการดำเนินการเพื่อให้เป็นเครือข่ายที่สมบูรณ์ที่สุดต่อไป

1) ข้อมูลด้านทรัพย์สินที่ถูกโจรกรรม ซึ่งจะประกอบด้วย

- การโจรกรรมยานพาหนะ (Stolen Vehicles)
- ยานพาหนะที่ใช้ในการกระทำผิด
- ใบอนุญาตขับขี่ที่ถูกโจรกรรม
- เรือที่ถูกโจรกรรม
- ทรัพย์สินที่ถูกโจรกรรม
- อาวุธปืนที่ถูกโจรกรรม
- อาวุธปืนเถื่อน
- เป็นต้น

4. ระบบเครือข่ายอื่น ๆ (Other Systems and Telecommunications Networks)

ระบบเครือข่ายอื่นๆนี้ สามารถจำแนกออกได้เป็น 2 กลุ่ม คือ[9]

(ก) ระบบระดับชาติ (National – System) ที่สนับสนุนหน่วยงานรัฐในระดับท้องถิ่นและรัฐบาลกลางจะประกอบด้วยระบบฐานข้อมูลและเครือข่ายต่อไปนี้ คือ

---

[9] Miller, J, FBI Shares Crime Data. **Government Computing News** p.21

- CODIS เป็นการรวมเอา DNA Index System และดัชนีระดับชาติของข้อมูลด้าน DNA แต่อย่างไรก็ตาม ระบบนี้จำกัดเฉพาะข้อมูลและพยานหลักฐานที่ได้จากสถานที่เกิดเหตุเท่านั้น

- NIBIN เป็นการบูรณาการข้อมูลเครือข่ายประเภท National Integrated Ballistics Information Network เป็นความพยายามที่จะกำหนดฐานข้อมูลเกี่ยวกับอาวุธ BATF และ FBI

- NDPIX (National Drug Pointer Index) เป็นฐานข้อมูลด้านดัชนีชี้วัดยาเสพติดระดับชาติ วางระบบชี้วัดที่อนุญาตให้มลรัฐต่างๆ รัฐบาลท้องถิ่นและหน่วยงานจากรัฐบาลกลางได้กำหนดในกรณีที่เกิดมีการสงสัยในระหว่างการสืบสวน

- UCR / NIBRS เป็นระบบที่รู้จักกันดี คือ การวางรูปแบบการรายงานข้อมูลอาชญากรรมระดับประเทศ หรือ National Uniform Crime Report System เป็นระบบการรายงานข้อมูลอาชญากรรมโดยใช้กระบวนการทางสถิติเข้าช่วย แต่ก็ไม่ได้รวมเอาข้อมูลที่ระบุตัวบุคคลเฉพาะเข้ามาไว้ด้วย

- NICS – National Instant Criminal Background Check System for pre – sale firearm background เป็นฐานข้อมูลที่เกี่ยวข้องกับผู้จัดจำหน่ายอาวุธปืน และตรวจสอบกับผู้ที่มีอาวุธปืนไว้ในครอบครอง

- LEO–Law Enforcement On–Line เป็นข้อมูลส่วนหนึ่งที่เกี่ยวข้องกับการฝึกอบรม และการสร้างความปลอดภัยแก่สาธารณะ

(ข) ระบบรัฐบาลกลาง (Federal – System) เป็นระบบที่ให้การสนับสนุนกิจกรรมด้านงานยุติธรรมแก่หน่วยงานรัฐบาลกลางในหน่วยต่างๆ แต่ระบบนี้จะเอื้อเฉพาะระดับรัฐบาลกลางเท่านั้น จะประกอบด้วย

- TECS – Treasury Enforcement Communications System

- DRUGX – a เป็นฐานข้อมูลข่าวกรองของหน่วยปราบยาเสพติดสหรัฐอเมริกา (DEA) ที่ใช้เพื่อการร่วมมือในการปราบปรามยาเสพติด

- JABS – Joint, Automated Booking System เป็นระบบการที่เริ่มดำเนินตั้งแต่ปี 1999 เพื่อให้หน่วยงานของรัฐบาลกลางได้แลกเปลี่ยนข้อมูลเกี่ยวกับการจับกุมและเชื่อมโยงข้อมูลอื่นๆกับหน่วยงาน FBI (ด้าน IAFIS)

- NIPC'S เป็นฐานข้อมูลป้องกันโครงสร้างพื้นฐานระดับชาติ (National Infrastructure Protection Center Data)

- IDEN – INS's เป็นฐานข้อมูลเกี่ยวกับคนต่างด้าวเข้าเมืองทุกประเภททั้งถูกและผิดกฎหมาย

- Fin CEN – เป็นเครือข่ายเกี่ยวกับอาชญากรรมทางด้านเศรษฐกิจ (Financial Crime Enforcement Network)

(ค) ระดับมลรัฐ (State – System) ภูมิภาคและท้องถิ่น จะประกอบด้วย

- ระบบทะเบียนประวัติอาชญากรรม
- ข้อมูลบุคคลที่ต้องการและทรัพย์สินที่ถูกโจรกรรมระดับรัฐและท้องถิ่น
- ระบบข้อมูลเกี่ยวกับราชทัณฑ์ระดับมลรัฐ
- ระบบศาลระดับมลรัฐและท้องถิ่น
- ระบบห้องปฏิบัติการมลรัฐ
- ระบบการจดทะเบียนยานพาหนะและใบขับขี่
- ระบบงานยุติธรรมเกี่ยวกับเด็กและเยาวชนกระทำผิด
- ระบบการคุมประพฤติ ระบบการพักการลงโทษ และการแนะนำผู้ถูกปล่อยตัว
- ระบบการบริหารจัดการเรือนจำ
- ระบบอัยการ

(ง) ระดับหลายมลรัฐ (Multi – State System) ประกอบด้วย

- RISS (Regional Information Sharing System)
- WIN (Western Identification Network) เป็นการประมวลข้อมูลในมลรัฐแถบตะวันตก
- SWBS ADIS – (Southwest Border States Anti – Drug Information System)
- GREAT – Gang Reporting , Evaluation and Tracking System เป็นฐานข้อมูลเกี่ยวกับการสืบสวน สอบสวน ผู้ต้องสงสัยที่เป็นสมาชิกของเพื่อนร่วมแก๊งค์ ฐานข้อมูลนี้ได้รับความร่วมมือจากสำนักงานนายอำเภอของลอส แองเจิลลิส แต่ก็สามารถเข้าถึงได้จากทั่วโลก

2.2.1 การแลกเปลี่ยนข้อมูลด้านกระบวนการยุติธรรมกับการใช้เทคโนโลยีเพื่อการป้องกัน (Information Sharing and Prevention Technology)

แม้ว่ากระแสการดำเนินการเกี่ยวกับการก่อการร้ายจะมีบทบาทต่อการเร่งเร้าให้มีการแลกเปลี่ยนข้อมูลในหน่วยงานด้านกระบวนการยุติธรรม หน่วยบังคับกฎหมายและด้านความมั่นคง แต่การพัฒนาการแลกเปลี่ยนข้อมูลด้านกระบวนการยุติธรรม และการบูรณาการ

ข้อมูลด้านกระบวนการยุติธรรมก็เกิดขึ้นมาก่อนหน้านี้แล้ว โดยมีการทุ่มเททรัพยากรในด้านกระบวนการยุติธรรมเพื่อพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี (Technological infrastructures) เพื่อเอื้อต่อการแลกเปลี่ยนข้อมูลที่สำคัญๆ นอกจากนี้ระบบการบูรณาการข้อมูลด้านงานยุติธรรมหรือ The integrated justice information system ได้ถูกกำหนดขึ้นเพื่อให้การแลกเปลี่ยนข้อมูลเป็นไปในกรอบของความถูกต้อง ชัดเจนรวดเร็ว ในวงการกระบวนการยุติธรรม และยังส่งเสริมในด้านการลดค่าใช้จ่าย แต่มีประสิทธิภาพ การบูรณาการจึงมีทั้งแนวดิ่ง (Vertical) และแนวราบ (Horizontal Approach)

ในการดำเนินการที่เกี่ยวกับการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม ด้านการป้องกันอาชญากรรม รัฐบาลได้จัดทำเครือข่ายระดับชาติ (a national criminal intelligence network) ที่ชื่อ “RISS.NET” หรือ “The Regional Information Sharing Systems Network” โดยความร่วมมือกับ FBI (Federal Bureau of Investigations Database) และกระทรวงกลาโหม (Department of Defense) รวมทั้งกระทรวงความมั่นคงแห่งมาตภูมิ (Department of Homeland Security)[10] แม้การสร้างเครือข่ายดังกล่าวจะยังไม่ใช่ต้นแบบในการบูรณาการข้อมูลด้านงานยุติธรรมทั้งหมดในอนาคต แต่ก็เป็นก้าวแรกของการสร้างเครือข่ายในการแลกเปลี่ยนและการบูรณาการข้อมูลด้านอาชญากรรม

แนวโน้มและทิศทางการดำเนินการการเป็นหุ้นส่วนในภารกิจด้านงานยุติธรรม อาจกล่าวได้ว่า มีแนวโน้มในเชิงของการป้องกันอาชญากรรม มากกว่าการปราบปรามอาชญากรรม สหรัฐอเมริกาเป็นประเทศที่มีประสบการณ์อย่างดีในการเรียนรู้การดำเนินการเช่นนี้ เพราะในอดีต สหรัฐอเมริกาวางนโยบายในการทำสงครามกับอาชญากรรม (War on Crime) แต่เมื่อดำเนินการผ่านไปราว 2 ทศวรรษ ก็เริ่มตระหนักจากผลการประเมินว่า ต้องทุ่มเท และสูญเสียทรัพยากรต่างๆ(resources)และงบประมาณมหาศาล จึงหันมาทำการศึกษาวิจัยและปรับเปลี่ยนระเบียบวาระด้านนโยบาย (Policy Agenda) หันเหมาที่การสร้างความร่วมมือ การขยายเครือข่าย (Network) การเป็นหุ้นส่วน (Partnership) เพื่อป้องกันอาชญากรรม

ลักษณะและรูปแบบการป้องกันอาชญากรรมแบบดั้งเดิมจะใช้วิธีการเช่น การตรวจตรา (techniques of surveillance) การพยายามขัดขวางหรือสร้างอุปสรรคในการก่ออาชญากรรม (Incapacitation) และเน้นที่การจับกุมเรื่อง อาวุธ แก๊งค์ และยาเสพติด (Guns

---

[10] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. **Mission possible: Strong governance for the integration of justice information systems** p.25

gangs and drugs) แต่ในรอบ 10 ปีที่ผ่านมา มีการปรับเปลี่ยนนโยบายและยุทธศาสตร์ ที่สำคัญคือ ตามข้อเท็จจริงแล้ว สหรัฐอเมริกาเองไม่มีหน่วยงานด้านใดที่รับผิดชอบโดยเฉพาะในด้านการป้องกันอาชญากรรม หรือแม้กระทั่งการกำหนดเป็นระเบียบวาระแห่งชาติด้านการป้องกันอาชญากรรม (a national crime prevention agenda) ปัจจุบันมีการนำเอาระบบการบูรณาการข้อมูล (Information integration systems)ใช้เทคโนโลยี เชิงการป้องกัน (Prevention technology) การเป็นหุ้นส่วนในการบังคับใช้กฎหมาย (Law enforcement partnerships) และการจัดทำโครงการมุ่งเป้า (Targeted interventions) เป็นต้น

ในมลรัฐต่าง ๆของอเมริกาและเทศบาลในท้องถิ่นก็ยังได้มีการพัฒนาระบบการบูรณาการเพื่อแลกเปลี่ยนข้อมูลระหว่างหน่วยงานด้านงานยุติธรรม เช่น JUSTIS (The Integrated Justice Information System) ที่ District of Columbia ที่วอชิงตัน ดีซี ได้พัฒนาขึ้นได้เปิดโอกาสให้มีการแลกเปลี่ยนและการใช้ข้อมูลด้านงานยุติธรรม ถึง 13 หน่วยงาน ไม่ว่าจะเป็นด้านศาลยุติธรรม เรือนจำ คุมประพฤติ องค์กรบริการสงเคราะห์บุคคล และหน่วยงานด้านการบังคับใช้กฎหมาย[11]

JUSTIS จะใช้หลักการถ่ายโอนข้อมูลโดยที่หน่วยงานใด ๆที่เกี่ยวข้องสามารถจะเรียกใช้ข้อมูลที่เกี่ยวข้องได้ และในขณะเดียวกันก็สามารถผลักข้อมูล (Pushed) จากหน่วยงานตรงให้เข้าไปยังหน่วยงานอื่น ๆได้ เช่น ศาลสูงสามารถเรียกข้อมูลจากหน่วยงานของอัยการไปใช้ได้ นอกจากนี้ USTISยังรวมทั้งข้อมูลการอภิปรายและการประชุมต่าง ๆเพื่อพัฒนาให้เกิดความรู้สึกว่าเป็นวงการเดียวกัน แต่ต่างองค์กรที่ทำงานด้านกระบวนการยุติธรรม (a sense of community among officials from different agencies and promote collaboration around justice-related issues) เมืองนิวยอร์ค มหานครวอชิงตันดีซี รัฐเพ็นซิลวาเนีย ได้วางแผนที่จะใช้ต้นแบบของ JUSTIS เพื่อพัฒนาระบบการแลกเปลี่ยนข้อมูลเพื่อป้องกันอาชญากรรม และการป้องกันมาตภูมิ

ในขณะที่มีการชื่นชมเกี่ยวกับระบบบูรณาการของการแลกเปลี่ยนข้อมูลด้านกระบวนยุติธรรมและงานยุติธรรม ก็มีคำถามเกิดขึ้นว่า **เราจะใช้ข้อมูลจากการบูรณาการดังกล่าวให้เกิดประสิทธิภาพได้อย่างไร** ตำรวจชิคาโก (The Chicago Police Department (CPD) ก็เป็นผู้นำในการดำเนินการเพื่อให้คำตอบดังกล่าวโดยการพัฒนาระบบการแลกเปลี่ยนข้อมูลที่เรียกว่า “CLEAR Program” (Chicago Law Enforcement Analysis and Reporting) โดยการนำเอามาใช้กลางปี 1990 ร่วมกับการพัฒนาโครงการตำรวจชุมชน ตามยุทธศาสตร์

---

[11] Criminal Justice Coordinating Council 2002 p.28

The Chicago Alternative Policing Strategy หรือ CAPs ซึ่งเป็นการนำเอาความร่วมมือของตำรวจและสมาชิกของชุมชน ตลอดจนผู้แทนจากหน่วยงานต่างๆมาร่วมกันกำหนดและแก้ไขปัญหาที่เกิดขึ้นจากเพื่อนบ้านอย่างมีประสิทธิภาพ โครงการ CLEAR นี้ได้

2.3 การคุ้มครองข้อมูล (Data Protection)

การจัดเก็บ ประมวลผลข้อมูลและการจัดทำข้อมูลเทคโนโลยีสารสนเทศ เป็นสิ่งที่ดำเนินการไม่ยากในระหว่างหน่วยงานและองค์กร แต่การจำแนกและให้ความคุ้มครองข้อมูลจากการนำไปแสวงหาผลประโยชน์และการก่อให้เกิดการเสียหายกับบุคคลที่เกี่ยวข้องโดยเฉพาะข้อมูลส่วนบุคคล จำเป็นจะต้องมีกระบวนการและมาตรการทางกฎหมายในการคุ้มครองซึ่งในต่างประเทศ นอกจากจะมีมาตรการทางกฎหมายในการคุ้มครองการเข้าใช้ข้อมูลโดยไม่ถูกต้องแล้วยังมีการให้ความคุ้มครองข้อมูลในฐานะที่ระบบฐานข้อมูลที่จัดทำขึ้นก็ถือเป็นทรัพย์สินทางปัญญาประเภทหนึ่ง[12] ที่จะต้องได้รับการดูแล

เมื่อพิจารณาฐานข้อมูลที่สรุปได้อย่างกว้างๆ ว่าเป็นการรวบรวมข้อมูลหรือสารสนเทศอย่างเป็นระบบระเบียบ (Organized collection of information) หรือชุดข้อมูลที่ได้รับการจัดเรียงเป็นหมวดหมู่อย่างดีจะเห็นได้ว่ามีคุณสมบัติคาบเกี่ยวและสามารถนับได้ว่าเป็นทรัพย์สินทางปัญญา ซึ่งในแง่ของกฎหมายแล้ว หมายถึง สิทธิอันเกิดขึ้นจากผลงานทางความคิด เช่น แนวความคิดเกี่ยวกับสิ่งประดิษฐ์ บทกวี วรรณกรรม คอมพิวเตอร์โปรแกรม เป็นต้น มากกว่าจะหมายถึงตัวผลิตผลที่จะได้สร้างสรรค์ขึ้น ดังนั้นคำว่าทรัพย์สินทางปัญญา จึงหมายถึง สิทธิตามกฎหมายซึ่งได้มีการกำหนดขึ้นอันเกี่ยวด้วยกับผลผลิตจากปัญญาของมนุษย์โดยขึ้นอยู่กับองค์ประกอบของฐานข้อมูลนั้นๆ อย่างเช่น หากเป็นการรวบรวมหรือจัดการเกี่ยวกับข้อมูลที่ต้องใช้ความอุตสาหพยายามอย่างมาก และในบางกรณีจะต้องใช้ความคิดสร้างสรรค์เพื่อให้แก้ปัญหาให้ลุล่วงไปได้ ด้วยคุณสมบัติดังกล่าวจึงทำให้ฐานข้อมูลจำพวกได้รับความคุ้มครองในฐานะทรัพย์สินทางปัญญาภายใต้กฎหมายลิขสิทธิ์[13] เช่น งานที่ถือว่ามีคุณภาพใกล้เคียงกับงานวรรณกรรม (Literary works) อาจได้รับความคุ้มครองลิขสิทธิ์ในข้อใดข้อหนึ่งดังต่อไปนี้

---

[12] ปารเมศ บุญญานันท์ **กฎหมายคุ้มครองข้อมูลในฐานข้อมูลอิเลคโทรนิกส์** หน้า 20

[13] Wright, Benjamin, and Jane L, Winn., **The Law of Electronic Commerce.** P.39

1. เนื้อหาที่จะได้รับการคัดเลือกมารวมไว้ (Selection of the content)
2. การประสานกันของเนื้อหาทั้งหมด (Internal co-ordination of the content)
3. การจัดลำดับความสัมพันธ์ขององค์ประกอบทั้งหมดของฐานข้อมูล
4. เนื้อหาของงานนั้นๆ เองโดยตรง (The content itself)

ในกรณีของฐานข้อมูลมักจะได้รับความคุ้มครองทั้งหมด เนื่องจากข้อมูลที่ประกอบกันขึ้นเป็นฐานข้อมูล ซึ่งมักจะเป็นข้อมูลสาธารณะ (Public knowledge) หรือเป็นเพียงข้อเท็จจริง (Mere facts) และข้อมูลที่มีความพิเศษ (Unique Information) ที่ทำให้ฐานข้อมูลนั้นมีคุณสมบัติที่โดดเด่นออกมาจากการเป็นแต่เพียงสมุดรวบรวมข้อมูลตามลำดับก่อนหลัง ยกตัวอย่างเช่น หากเราต้องการสร้างฐานข้อมูลรายชื่อผู้ค้าอุปกรณ์คอมพิวเตอร์ โดยต้องการสำรวจความสนใจของผู้ประกอบการในตลาด และหากรายใดสนใจก็จะอนุญาตให้ผู้รวบรวมนำชื่อและที่อยู่ของผู้ประกอบการนั้น รวมไว้ในฐานข้อมูลที่จัดลำดับด้วยความอุตสาหะได้ แต่หากงานมีเพียงแค่นี้ ก็จะไม่ได้รับความคุ้มครองลิขสิทธิ์ผู้รวบรวมเพิ่มส่วนแจกแจงคุณสมบัติของผู้ประกอบการแต่ละรายลงไป ซึ่งถือว่าเป็นข้อมูลที่มีความพิเศษ อาจทำให้งานชิ้นนี้ได้รับความคุ้มครองก็ได้เนื่องจากศาลเห็นว่าผู้รวบรวมมีความพยายามในการสร้างผลงาน จึงไม่ควรที่จะให้ผู้อื่นฉกฉวยผลประโยชน์ในแง่ธุรกิจไปได้[14]

นอกจากนี้การพิจารณาว่างานชิ้นใด เข้าข่ายเป็นทรัพย์สินทางปัญญาและสมควรจะได้รับความคุ้มครองนั้น ยังนิยมที่จะอ้างถึงคำตัดสินของศาลในกรณีที่คล้ายๆ กันอีกด้วย ดังกรณีตัวอย่าง Rural Telephone v. Feist Publications ที่มีชื่อเสียง

ดังนั้น ระบบฐานข้อมูลด้านกระบวนการยุติธรรมที่จัดทำขึ้นในต่างประเทศนอกจากรัฐจะต้องมีกลไกในการดำเนินการเพื่อปกป้องข้อมูลมิให้ถูกนำไปใช้เพื่อแสวงหาผลประโยชน์และก่อให้เกิดความเสียหายแล้วยังจะต้องให้การคุ้มครองถึงลักษณะด้านทรัพย์สินทางปัญญาอันเกี่ยวข้องกับกฎหมายลิขสิทธิ์ของข้อมูลข่าวสารในกระบวนการยุติธรรมนั้นด้วย

2.3.1 แนวทางการให้ความคุ้มครองข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์ของต่างประเทศ

ข้อมูลต่างๆที่จัดเก็บในฐานข้อมูลอิเลคโทรนิคส์นั้นเป็นข้อมูลที่จะต้องให้การคุ้มครองถึงลักษณะด้านทรัพย์สินทางปัญญาด้วย ซึ่งแนวทางการให้ความคุ้มครองข้อมูลของสหรัฐอเมริกามีหลักในการพิจารณาให้ความคุ้มครองข้อมูลที่มีผู้สร้างสรรค์ขึ้นอยู่ 4 แนวทาง[15]

---

[14] Wright, Benjamin, and Jane L, Winn., Ibid.p.42

[15] ปารเมศ บุญญานันท์ **อ้างแล้ว** หน้า 26-34

1.หลักทฤษฎี Sweat of the brow

2.หลักกฎหมาย Misappropriation

3.หลักกฎหมาย Unfair Competition

4.หลักกฎหมาย Trade Secret

อย่างไรก็ตาม กฎหมายรัฐธรรมนูญบัญญัติของสหรัฐอเมริกา ได้กล่าวถึงการที่จะให้ความคุ้มครองข้อมูลตามหลักกฎหมายลิขสิทธิ์ ไว้ว่า ข้อมูลนั้นต้องมีคุณสมบัติเป็นความริเริ่มหรือมีความคิดสร้างสรรค์ที่เกิดจากสติปัญญา ซึ่งกฎหมายลิขสิทธิ์ของสหรัฐอเมริกามีจุดกำเนิดมาจากทฤษฎี “Sweat of the brow” ซึ่งเป็นกฎหมายของประเทศสหราชอาณาจักร ที่ให้ความคุ้มครอง

1. หลักทฤษฎี Sweat of the brow

ศาลของสหรัฐอเมริกาได้ใช้หลักทฤษฎี “Sweat of the brow” ในการพิจารณาพิพากษาคดีเกี่ยวกับข้อมูล ซึ่งมีหลักในการให้ความคุ้มครองทรัพย์สินทางปัญญาของงาน คดี Banks v. Mcdivitt, ซึ่งศาลได้วางหลักเกี่ยวกับข้อมูลที่จะได้รับความคุ้มครองว่า งานรวบรวมข้อมูลนั้นต้องเกิดจากความคิดริเริ่ม หรือความคิดสร้างสรรค์ใหม่ จนกระทั่งต่อมาได้ถือเป็นจุดเริ่มต้นการบัญญัติ

2. หลักกฎหมาย Misappropriation

ศาลของสหรัฐอเมริกายังได้พิจารณาพิพากษา ให้ความคุ้มครองข้อมูลตามหลักกฎหมายอื่นอีก เช่น การให้ความคุ้มครองข้อมูลตามหลักกฎหมาย Misappropriation ซึ่งเป็นรูปแบบของกฎหมายที่ให้ความคุ้มครองแก่ข้อมูลเกี่ยวกับการค้าที่มีการลงทุนในการสร้างสรรค์ที่มีคุณสมบัติกว้างขวางกว่า แต่ประเด็นของลิขสิทธิ์ สิทธิบัตร หรือเครื่องหมายการค้า นั่นคือการที่มีการปฏิบัติต่อกันอย่างไม่เป็นธรรม การนำทรัพย์สินของผู้อื่นไปใช้ เพื่อหาผลประโยชน์แต่เพียงประการเดียวโดยไม่เป็นธรรมต่อเจตนาอันสุจริต (goodwill) และชื่อเสียงของผู้ที่เป็นเจ้าของนั้น

หลักกฎหมายของสหรัฐอเมริกาที่ใช้ให้ความคุ้มครองข้อมูลต่างๆ อยู่ในปัจจุบันนี้ จะคุ้มครองข้อมูลที่เกิดขึ้นจากความริเริ่มใหม่ ความคิดสร้างสรรค์ใหม่ โดยที่ข้อมูลนั้นผู้รวบรวมได้ใช้ความมานะพยายาม ความวิริยะอุตสาหะสร้างขึ้น และเมื่อมีการราบรวมข้อมูลไว้เป็นหมวดหมู่ เพื่อให้สะดวกในการเก็บการนำกลับมาใช้ ที่เรียกว่า “ฐานข้อมูล” ก็จะต้องมีการปรับปรุงกฎหมายให้คุ้มครองฐานข้อมูลอีกด้วย ในประเทศสหรัฐอเมริกาจะใช้คำพิพากษาของศาลมาเป็นหลักช่วยในการพิจารณา

3. หลักกฎหมาย Unfair Competition

กฎหมายที่ให้ความคุ้มครองแก่ข้อมูลในสหรัฐอเมริกา คือ กฎหมายการแข่งขันที่ไม่เป็นธรรม (Unfair Competition Law) เป็นกฎหมายที่ประกอบด้วย การชดใช้ค่าเสียหายเนื่องจากการนำข้อมูลในรูปแบบของการสื่อสารอิเล็กทรอนิกส์ไปแสวงหากำไรทางการค้า รวมทั้งการนำข้อมูลทางการค้าไปใช้โดยไม่เสมอภาค จนก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลที่แท้จริง

4. หลักกฎหมาย Trade Secret

ความลับทางการค้า (Trade Secret) เป็นข้อมูลข่าวสารที่มีความเกี่ยวพันกันกับคุณค่าของข้อมูลผู้ที่ละเมิดความลับทางการค้าต้องชดใช้ค่าเสียหาย พระราชบัญญัติอาชญากรรมทางเศรษฐกิจ (The Economic Act of 1996) ของสหรัฐอเมริกาได้ขยายขอบเขตของความลับทางการค้า ให้รวมถึงรูปแบบทุกรูปแบบ และทุกประเภทของการเงิน ธุรกิจ วิทยาศาสตร์ เทคนิค เศรษฐกิจ หรือ วิศวกรรมข้อมูลข่าวสาร ศาลสูงของรัฐอิลินอย ให้ความหมายความลับทางการค้า คือ กระบวนการเครื่องมือ กลไกของการใช้ประโยชน์ของข้อมูลข่าวสารโดยบุคคลในธุรกิจ คดีที่พิจารณาจากศาลสูงของสหรัฐกำหนดไว้ว่า ความลับทางการค้าจำเป็นต้องเก็บความลับและไม่เป็นที่เปิดเผยต่อสาธารณชนหรือ ไม่เป็นที่รู้กันในการค้าหรือธุรกิจ

2.3.2 แนวทางการให้ความคุ้มครองฐานข้อมูล

ข้อมูลที่ถูกเก็บรวบรวมในฐานข้อมูลจะได้รับการคุ้มครองหรือไม่ พิจารณาเป็นเรื่องๆ ไปเช่นกัน โดยใช้ปัจจัยต่างๆ ในการพิจารณา เช่น ข้อมูลนั้นจะต้องใช้ความพยายามสร้างขึ้นมามากน้อยเพียงใด มีอุปสรรคยุ่งยากแค่ไหน มีการลงทุนสูงหรือไม่ และอาศัยจากคดีที่ศาลได้พิจารณาพิพากษาไว้เป็นบรรทัดฐาน

การที่กฎหมายแยกแยะความแตกต่างระหว่างข้อเท็จจริง (Facts) กับการรวบรวมข้อเท็จจริงนั้น (Factual compilations) นั้นเป็นหลักสำคัญขั้นพื้นฐานของกฎหมายลิขสิทธิ์ ด้วยเหตุผลที่ว่า ข้อเท็จจริง (Facts) นั้นไม่ได้ถูกสร้างสรรค์ขึ้นอย่างงานต้นแบบ ยิ่งไปกว่านั้น การสร้างสรรค์ (Creation) การค้นพบ (Discovery) ก็มีความแตกต่างกัน

จากบทบัญญัติกฎหมายคุ้มครองฐานข้อมูลสหรัฐอเมริกา เมื่อผลคำพิพากษาของคดี Feist ในปี 1991 ออกมาว่าไม่ให้ความคุ้มครองแก่ข้อมูลที่รวบรวมมาโดยไม่แสดงความคิดสร้างสรรค์ หรือ ความคิดริเริ่มที่ควรได้รับความคุ้มครองทางกฎหมาย ทำให้เกิดผลกระทบต่อ

อุตสาหกรรมฐานข้อมูลของสหรัฐอเมริกาที่มีบทบาทต่อเศรษฐกิจโดยรวมของประเทศ ดังนั้น สหรัฐอเมริกานำเสนอกฎหมายให้ความคุ้มครองแก่ฐานข้อมูลต่อองค์การทรัพย์สินทางปัญญาโลก[16] เรียกว่า United States Proposal For Sui Generis Protection of Database เพื่อให้องค์การทรัพย์สินทางปัญญาโลก นำหลักการตามข้อเสนอไปร่างเป็นสนธิสัญญาคุ้มครองฐานข้อมูลแก่ประเทศสมาชิก เพื่อประโยชน์ใช้ในระดับนานาชาติ คงจะเป็นการประสบความได้เปรียบในการคุ้มครองฐานข้อมูลของสหรัฐอเมริกาต่อไปในอนาคตและได้มีกฎหมายเสนอให้สภาคองเกรสพิจารณาอีก 4 ฉบับในเวลาต่อมาคือ

การประชุมสภาคองเกรสครั้งที่ 104 ปี 1997 นายโคเบล (Coble) สมาชิกผู้แทนราษฎรสภาคองเกรสของสหรัฐอเมริกาได้เสนอ หลักกฎหมายให้ความคุ้มครองแก่การลงทุนในฐานข้อมูล (The Database Investment and Intellectual Property Antipiracy Act 1996: House of Representative 3531) เป็นพระราชบัญญัติว่าด้วยกฎหมายการลงทุนและป้องกันฐานข้อมูลในทรัพย์สิน หลักกฎหมายฉบับนี้ได้วางรูปแบบความคุ้มครองฐานข้อมูลเป็นแบบเดียวกันกับกฎหมายที่เสนอต่อองค์การทรัพย์สินทางปัญญาโลก การให้ปกป้องการลงทุนในอุตสาหกรรมฐานข้อมูล แต่ผลปรากฏว่าสภาคองเกรสยังไม่อนุมัติให้เป็นกฎหมาย เพราะพบความบกพร่องหลายประการ อาทิ คำจำกัดความกว้างและคลุมเครือ ไม่แบ่งแยกประเภทความคุ้มครอง ครั้นประชุมสภาคองเกรส

การประชุมคองเกรส ครั้งที่ 105 ปี 1998 มีการนำเสนอกฎหมายให้สภาพิจารณาความคุ้มครองแก่การรวบรวมข้อมูล (Collections of Information Anti-piracy Act: H.R. 2652) โดยกำหนดรูปแบบความคุ้มครองให้เด่นชัดขึ้นและแก้ข้อผิดพลาดจากหลักกฎหมายที่เสนอต่อสภาครั้งก่อน ปรากฏผลขั้นต้นว่า ผ่านขั้นพิจารณาชั้นสภาคองเกรสแล้ว จึงนำเสนอให้คณะวุฒิสภาพิจารณา แต่ก็ยังไม่ได้ออกมาบัญญัติเป็นกฎหมายให้ความคุ้มครองอีก เพราะช่วงระยะเวลาในการพิจารณาของคณะวุฒิสภาดังกล่าว มีการเสนอความคุ้มครองแก่ลิขสิทธิ์แห่งสหัสวรรษดิจิตอล จึงทำให้กฎหมายที่เสนอให้ความคุ้มครองแก่การรวบรวมข้อมูลนั้นตกไป

จนกระทั่ง การประชุมสภาคองเกรสสมัยที่ 106 ปี 1999 สมาชิกสภาผู้แทนก็นำเสนอกฎหมาย 2 ฉบับ คือ หลักกฎหมายป้องกันการนำข้อมูลไปใช้ไม่เหมาะสม (Collections of Information Anti-piracy Act: H.R. 354) โดยขัดเกลาตัวหลักกฎหมายเดิมให้มีผลคุ้มครองและได้แก้ไขเพิ่มเติมเรื่องการนำเอาข้อมูลไปใช้โดยไม่เหมาะสม (Federal of Misappropriation) ที่เกี่ยวข้องกับการรวบรวมข้อมูล และกฎหมายกำหนดให้ความคุ้มครองและ

---

[16] ปารเมศ บุญญานันท์ **อ้างแล้ว** หน้า 48

เปิดโอกาสให้ผู้บริโภคและผู้ลงทุนเข้าถึงในข้อมูล (Consumer and Investor Access to Information Act: House of Representatives 1858) กำหนดรูปแบบสนับสนุนการค้าอิเล็กทรอนิกส์แก่ผู้บริโภคผ่านฐานข้อมูลอิเล็กทรอนิกส์รวมทั้งฐานข้อมูลทางการตลาดย่อมได้รับความคุ้มครองตามกฎหมาย เน้นการให้ความคุ้มครองการเผยแพร่โดยการทำซ้ำข้อมูล (Prohibition against distribution of duplicates) วางหลักกำหนดเน้นถึงการค้าระหว่างประเทศที่ผ่านระบบการสื่อสารข้อมูลจะต้องกระทำโดยผู้มีอำนาจให้เผยแพร่ข้อมูล

ในปัจจุบันหลายประเทศได้ออกกฎหมายคุ้มครองในรูปของกฎหมายเกี่ยวกับการป้องกันการใช้คอมพิวเตอร์ไปในทางที่ผิด (Anti misuse computer Acts) ซึ่งก็จะเป็นกฎหมายที่มีมาตรการในการคุ้มครองฐานข้อมูลที่จัดขึ้นอีกส่วนหนึ่ง

2.4การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์(Electronic Data Interchange–EDI)

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์หรือ EDI เป็นความก้าวหน้าทางการส่งข้อมูลทางธุรกิจ เช่น คำสั่งซื้อจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่ง โดยทางเทคนิคแล้วข้อความ EDI (EDI message) จะถูกส่งด้วยวิธีเดียวกันกับ E-mail ข้อความ EDI สามารถบันทึกบนสื่ออิเล็กทรอนิกส์หรือกระดาษได้เหมือนกับ E-mail เทคโนโลยี EDI ได้รับการพัฒนาขึ้นราวทศวรรษที่ 1970 เพื่อใช้ในอุตสาหกรรมการขนส่งและได้รับความนิยมในช่วงทศวรรษ 1980 เมื่อสามารถนำมาพัฒนาปรับใช้ได้กับอุตสาหกรรมการผลิตและการค้าปลีก[17] ระบบ EDI สามารถใช้ประโยชน์ในระบบกาคลังที่เรียกว่า Just-in-time, Streamlined acquisition และระบบการจัดจำหน่าย (Distribution System) ซึ่งเป็นประโยชน์ต่อกระบวนการปฏิรูปการทำงานของบริษัท

2.4.1 ความหมายการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Electronic Data Interchange – EDI)

EDI เป็นคำย่อมาจากคำว่า “การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” (Electronic Data Interchange) สาเหตุที่ EDI เป็นเรื่องของ “อิเล็กทรอนิกส์” เพราะเป็นขั้นตอนและ

---

[17] ไชยวัฒน์ บุนนาค และ ไพบูลย์ อมรภิญโญเกียรติ. *“ความรู้เบื้องต้นและปัญหาข้อกฎหมายเกี่ยวกับการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์.”* ใน **เอกสารประกอบการสัมมนาเรื่อง ปัญหาข้อกฎหมายที่เกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์ในสังคมยุคเทคโนโลยีสารสนเทศ.** หน้า 1 – 2

กระบวนการที่เกี่ยวกับการทำงานของระบบคอมพิวเตอร์ การใช้คำว่า “ข้อมูล” (Data) เนื่องจากเป็นข้อมูลสารสนเทศโดยทั่วไปทุกประเภทและเกี่ยวกับการแลกเปลี่ยนข้อมูลระหว่างบุคคล ความเคลื่อนไหวของข้อมูลระหว่างบุคคลที่ใช้ EDI จะเรียกโดยรวมว่า ข้อความ (Transaction) และสัญญาณ (signal) ต่างๆ ที่ประกอบเป็น EDI จะเรียกรวมกันว่า “Transaction Set”

EDI นั้นมีประโยชน์ทางธุรกิจหลายประการ สามารถเป็นวิธีทางอิเล็กทรอนิกส์สำหรับการเจรจรและก่อให้เกิดสัญญาระหว่างคู่ค้าที่ใช้ EDI เช่น วิธีใช้ EDI ในรูปแบบเดิมมักจะทำกันระหว่างคู่ค้าที่มีความใกล้ชิดในระบบปิดที่มีความสัมพันธ์ทางธุรกิจมายาวนานและต่อเนื่อง การใช้ EDI จะเกิดประสิทธิภาพก็ต่อเรื่องคู่ค้าจำเป็นต้องทำการติดต่อกันในรูปแบบที่คล้ายและซ้ำกันอย่างต่อเนื่อง เพื่อลดความล่าช้าและสามารถทำการสื่อสารตอบโต้กันได้อย่างทันที

นอกจากนั้น EDI ยังเป็นการสื่อสารทางธุรกิจที่จำเป็นต้องมีข้อมูลที่มีรูปแบบ (Format) ที่ชัดเจน ซึ่งได้จัดเตรียมและวางรูปแบบตามมาตรฐานที่ตกลงกันไว้ล่วงหน้าระหว่างคู่ค้า และการที่ต้องทำเป็นรูปแบบ (Format) นั้น เนื่องจาก

1) เพื่อลดความคลุมเครือของการติดต่อสื่อสารที่ต้องทำเป็นประจำ มาตรฐาน EDI จึงต้องมีรายละเอียดระบุถึงความหมายของคำที่ใช้ในการส่งข้อมูลอย่างชัดเจน

2) เพื่อประโยชน์ในการอ้างอิงภายหลัง ระบบการจัดเก็บเอกสารและรักษาความปลอดภัยควรทำอย่างระมัดระวังและให้มีเนื้อหาตามที่ต้องการ

ข้อความ EDI ประกอบด้วยกลุ่มของข้อมูลที่เป็นรูปแบบ (Set of formatted data) ระหว่างคู่ค่า การรับ การส่ง และการยืนยันชุดข้อมูลดังกล่าวจะเรียกว่า “EDI Transaction” กล่าวคือ ผู้ส่งข้อมูล สื่อ (Carrier) ยอมรับและยืนยันความถูกต้องของข้อมูล จากนั้นสื่อจะทำการส่งข้อมูลไปยังผู้รับ โดยผู้รับจะรับและยืนยันความถูกต้องของข้อมูลที่ได้รับ กระบวนการดังกล่าวนี้มีความรวดเร็วกว่าวีการใช้กระดาษในรูปแบบเดิมอย่างมาก

EDI สามารถส่งระหว่างผู้รับและผู้ส่งทางเครื่องคอมพิวเตอร์ทั้งของผู้รับและผู้ส่ง (point – to – point) หรือส่งในรูปแบบดิสเก็ตที่มีข้อมูล EDI อยู่ก็ได้ (Tape – to – Tape Exchange) หรือเชื่อมผ่านสายโทรศัพท์หรือเครือข่ายโทรคมนาคมอื่นๆ ก็ได้ นอกจากนั้นยังสามารถส่งผ่านเครือข่ายคอมพิวเตอร์ (Intermediary computer network0 ที่เรียกว่าเครือข่ายเสริม (Value – added Network) เครือข่ายบุคคลที่สาม (Third Party Network) หรือผู้ให้บริการ EDI (EDI Service Provider) ผู้ให้บริการ EDI จะให้บริการในการเก็บและส่งข้อมูล ตรวจสอบสถานะและมาตรฐานของข้อมูล เก็บข้อมูลไว้เพื่อการตรวจสอบ แปลข้อมูลจากมาตรฐานหนึ่งไป

เป็นอีกมาตรฐานหนึ่ง เช่น มาตรฐานในระบบปิดไปเป็นมาตรฐานในระบบเปิด หรือให้บริการที่เกี่ยวข้องอื่นๆ ในขณะที่การบริหาร e-mail เป็นที่แพร่หลายในปัจจุบันมีส่วนทำให้บทบาทของ EDI ลดลง EDI จึงได้รับการพัฒนาให้ใช้บนเครือข่ายอินเตอร์เน็ตได้ ส่งผลให้การใช้งานประหยัด สะดวกและรวดเร็วมากยิ่งขึ้น[18]

จะเห็นได้ว่า EDI แตกต่างจากรูปแบบการสื่อสารทางอิเล็กทรอนิกส์อื่นๆ คือ โครงสร้างและระบบของข้อมูลที่ถ่ายโอนกันและวิธีการที่ข้อมูลถูกบันทึกได้รับการคุ้มครอง

ในสังคมยุคข้อมูลข่าวสารในปัจจุบัน การสื่อสารอิเล็กทรอนิกส์ในรูปแบบต่างๆ ได้รับการพัฒนาอย่างรวดเร็ว โดยใช้คอมพิวเตอร์เป็นสื่อกลางในการติดต่อระหว่างกัน เดิมใช้โทรศัพท์และโทรสารในการแลกเปลี่ยนข้อมูลได้พัฒนามาเป็นการแลกเปลี่ยนข้อมูลโดยผ่านเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมต่อระหว่างกันทั่วโลก และมีมาตรฐานการรับส่งข้อมูลโดยส่งเป็นตัวอักษร ภาพ และเสียง ซึ่งคนทั่วไปมักจะเรียกการสื่อสารวิธีนี้ว่า การสื่อสารด้วยระบบอินเตอร์เน็ต การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) เป็นหลักและใช้การสื่อสารระบบอินเตอร์เน็ตเช่นเดียวกัน ทั้งนี้เนื้อหาคือมาตรฐาน องค์ประกอบ และการทำงานของการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) โดยมีสาระสำคัญ ดังต่อไปนี้

รูปแบบมาตรฐานของ EDI สามารถแบ่งได้ 4 ระบบใหญ่ ดังนี้

1) ระบบ Generic EDI

เป็นระบบที่มีการกำหนดโครงสร้างของข้อมูลที่จะแลกเปลี่ยนระหว่างกันแบบกว้างๆเป็นการทั่วไป โดยการกำหนดโครงสร้างดังกล่าวต้องเป็นไปตามมาตรฐานของหน่วยงานที่กำหนดขึ้น (Standard Bodies) ซึ่งขึ้นอยู่กับความสมารถของอุปกรณ์คอมพิวเตอร์และมาตรฐานของอุตสาหกรรมที่ใช้สื่ออิเล็กทรอนิกส์ในขณะนั้นมาตรฐาน EDI ที่เป็นนิยมและยอมรับเป็นการสากลทั่วไป คือ ANSI X 12 และ EDIFACT

2) ระบบ Industry Convention EDI

เป็นระบบที่กำหนดโครงสร้าง EDI เพื่ออุตสาหกรรมแต่ละประเภทโดยเฉพาะ โดยอุตสาหกรรมแต่ละประเภทจะมีโครงสร้างหรือมาตรฐานของข้อมูล EDI ที่แตกต่างกัน เช่น อุตสาหกรรมรถยนต์ อุตสาหกรรมต่างๆ ที่แตกต่างกัน เช่น อุตสาหกรรมรถยนต์ อุตสาหกรรมวัตถุเคมีภัณฑ์ เป็นต้น

---

[18] Eric J. Adam, **Ibid** p.36

3) ระบบ Proprietary EDI

เป็นระบบที่องค์กรแต่ละองค์กรกำหนดโครงสร้างของเอกสาร เพื่อใช้เองภายในองค์กรของตน ผู้ที่จะติดต่อกับองค์กรนั้นก็ต้องใช้แบบฟอร์มโครงสร้าง EDI ขององค์กรนั้น เช่น บริษัทสยามแม็คโคร จำกัด (มหาชน) บริษัทไทยน้ำทิพย์ จำกัด ซึ่งเป็นผู้ประกอบการเกี่ยวกับสินค้าอุปโภคบริโภค ก็จะมีการกำหนด EDI FORM มาใช้กับองค์กรของตน เป็นต้น

4) ระบบ Finance EDI

เป็นระบบการแลกเปลี่ยนข้อมูลด้านการรับจ่ายเงินและส่งผ่านข้อมูลต่างๆ ระหว่างหน่วยองค์กรธุรกิจกับองค์กรด้านการเงินต่างๆ เช่น ระบบการโอนเงินระหว่างธนาคารทางอิเล็กทรอนิกส์ (BAHTNET) ซึ่งเป็นระบบ EDI ของธนาคารแห่งประเทศไทย เป็นผู้กำหนดมาตรฐานแบบฟอร์มขึ้น เพื่อให้เกิดความรวดเร็วในการโอนเงินระหว่างธนาคารภายในประเทศแทนการใช้เช็คในอดีต

ในส่วนขององค์ประกอบของ EDI โดยทั่วไปล้วEDIจะมีองค์ประกอบสำคัญ 3 ส่วน คือ

1) ผู้ใช้บริการ (Trading Partner)

เป็นองค์กรหรือบุคคลที่ต้องการส่งข้อมูลซึ่งมักเป็นผู้ใช้บริการลำดับสุดท้าย (End User) และต้องมีอย่างน้อย 2 ฝ่ายที่ต้องการส่งผ่านข้อมูลโดยใช้คอมพิวเตอร์ที่มีโปรแกรมใช้งานในการแปลงข้อมูลแบบฟอร์มหรือมาตรฐานเป็นตัวเชื่อมระหว่างกันโดยข้อมูลที่ส่งนั้นเป็นไปตามแบบฟอร์มหรือมาตรฐานที่ตกลงกันโดยส่งข้อมูลผ่านผู้ให้บริการ หรือ VAN ของตน

2) ผู้ให้บริการระบบ EDI (Value – added Network – VANs)

ทำหน้าที่ให้บริการส่งข้อมูลระหว่างผู้ใช้บริการในเครือข่ายของตนหรือเชื่อมต่อกับ VAN อื่นโดยตัวกลางในการผ่านข้อมูลให้กับผู้ใช้บริการ (End User) ทั้งสองฝ่ายโดยเก็บข้อมูลของผู้ใช้บริการอยู่ใน Mailbox ในเครือข่ายของตน

3) ศูนย์กลางการรับส่งข้อมูล (GATEWAY)

เป็นจุดเชื่อมต่อระหว่าง VAN ต่างๆ กับหน่วยงานของรัฐบาล โดยปกติรัฐบาลของแต่ละประเทศมักจะเป็นผู้ควบคุมหรือตั้งตัวแทนมาควบคุมศูนย์กลางหรือ GATEWAY เพื่อทำหน้าที่เป็นศูนย์กลางการรับข้อมูลแห่งชาติ (National Gateway) ให้กับ VAN ต่างๆ ในการเชื่อมโยงกับหน่วยงานของราชการ

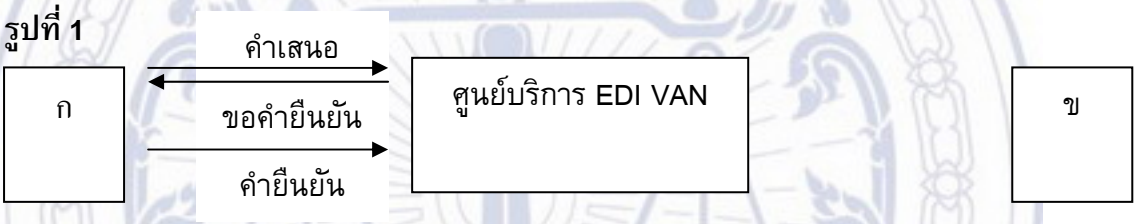
กระบวนการทำงานของ EDI แบ่งเป็น 2 ระบบใหญ่ ดังนี้

1) การทำงานแบบ Communication Network

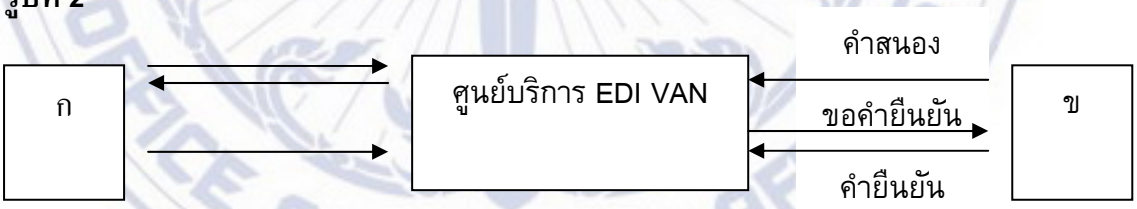
การส่งข้อมูลแบบนี้ VAN จะทราบถึงรายละเอียดข้อมูลของผู้ใช้บริการ (End User) เช่น ผู้ใช้บริการ ก. ต้องการติดต่อส่งข้อมูลไปยังผู้ใช้บริการ ข. ก. ต้องส่งผ่านข้อมูลมายัง VAN ของตน และข้อมูลนั้นจะถูกส่งผ่านไปยัง VAN ของ ข. (กรณีอยู่คนละ VAN) โดยการแลกเปลี่ยนหรือส่งผ่านข้อมูลกันนั้นจะมีการตรวจสอบข้อมูลกลับไปมาระหว่าง VAN และผู้ใช้บริการทั้งสอง ทำให้ VAN จะทราบข้อมูลที่ผู้ใช้บริการส่งผ่านระหว่างกัน ซึ่งระบบนี้ไม่เป็นที่นิยมมากนัก

แผนภาพการทำงานของระบบ Communication Network

รูปที่ 1



รูปที่ 2

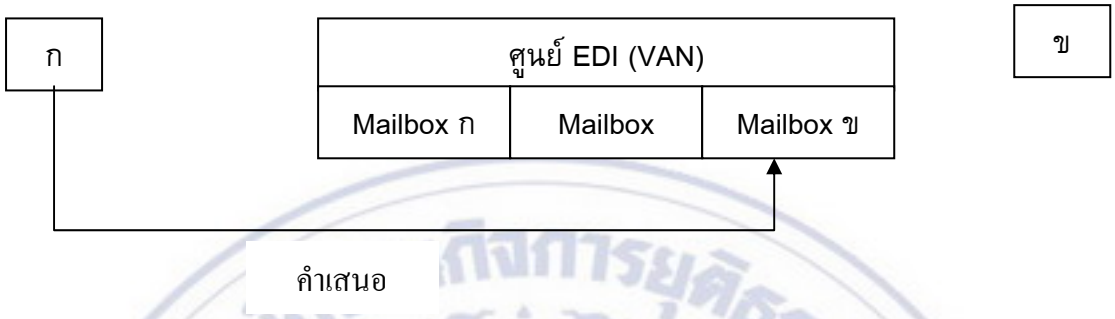


2) การทำงานแบบ EDI Service

แตกต่างกับระบบแรก คือ เมื่อผู้ใช้บริการส่งข้อมูลมายัง VAN ที่ให้บริการข้อมูลดังกล่าวจะถูกบันทึกโดยโปรแกรมคอมพิวเตอร์ของ VAN นั้นภายใต้ตู้ไปรษณีย์อิเล็กทรอนิกส์ (Mailbox) ของผู้ใช้บริการแต่ละรายซึ่งเป็นหน่วยความจำเล็กในเครื่อง EDI Service เพื่อรอใช้ผู้ที่ต้องการรับข้อมูลข่าวสารอีกฝ่ายมารับไปเองจาก Mailbox ของ VAN จึงทำให้หน้าที่เป็นเพียงบุรุษไปรษณีย์เท่านั้น โดยไม่ทราบถึงรายละเอียดของข้อมูลที่ส่งผ่านระหว่างผู้ใช้บริการทั้งสองฝ่าย

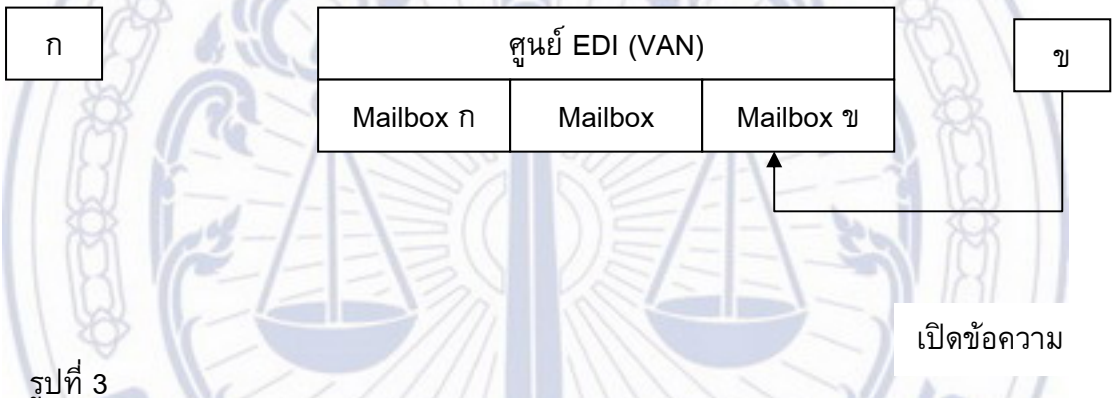
แผนภาพการทำงานของระบบ EDI Service

รูปที่ 1



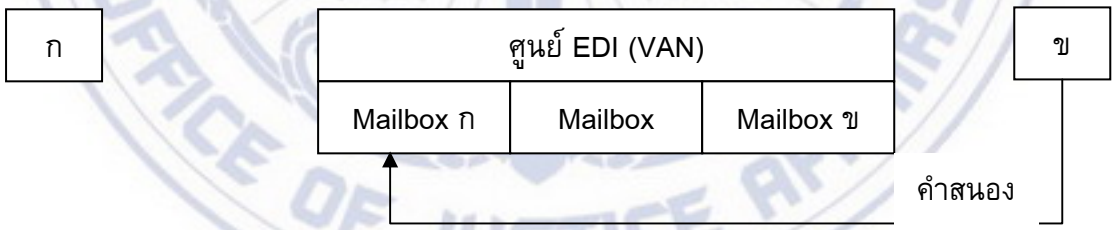
คำเสนอ

รูปที่ 2



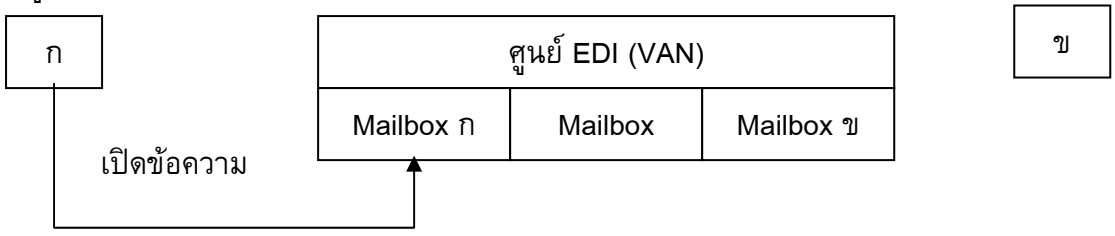
เปิดข้อความ

รูปที่ 3



คำสนอง

รูปที่ 4



เปิดข้อความ

สำหรับการรักษาความลับของข้อมูลนั้น การรักษาความลับของข้อมูลข่าวสารของผู้ใช้บริการ EDI โดยปกติจะใช้วิธีการเข้ารหัส (Encryption) โดยผู้ใช้บริการทั้งสองฝ่ายมักจะมีกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) เพื่อป้องกันการเปลี่ยนแปลงข้อมูลข่าวสารการส่งข้อมูล รวมถึงป้องกันไม่ให้บุคคลภายนอกทราบถึงข้อมูลที่ส่งระหว่างกัน นอกจากนี้ยังมีระบบลายมือชื่ออิเล็กทรอนิกส์ หรือ Digital Signature ซึ่งเป็นการแปลงข้อมูลคอมพิวเตอร์เป็นรหัสเฉพาะบุคคลเพื่อป้องกันข้อมูลนั้นมิให้บุคคลภายนอกล่วงรู้ได้ โดยผู้ใช้บริการ EDI นั้น มักใช้ทั้งสองระบบควบคู่ในการส่งผ่านข้อมูลในแต่ละครั้ง

2.4.2 ประโยชน์ของการใช้สื่ออิเล็กทรอนิกส์ (EDI)[19]

ก.ประโยชน์จากการใช้ภายในและระหว่างหน่วยงาน

1) ลดระยะเวลาในการส่งผ่านข้อมูล เนื่องจากสามารถยกเลิกการส่งผ่านข้อมูลทางไปรษณีย์และระบบการส่งผ่านภายในของหน่วยงานได้ทั้งหมด

2) ลดค่าใช้จ่ายด้านการจัดการข้อมูลและการส่งข้อมูล (ไปรษณีย์และระบบภายในองค์กร) ซึ่งรวมทั้งค่าใช้จ่ายในส่วนของบุคลากร ค่าไปรษณีย์ กระดาษและอุปกรณ์อื่นๆ ที่เกี่ยวข้อง

3) ลดความผิดพลาดของข้อมูลที่มีการแลกเปลี่ยนกัน โดยเฉพาะในส่วนของการพิมพ์ซ้ำซึ่งไม่มีความจำเป็นเมื่อนำ EDI มาใช้

4) มีการตอบรับทันทีระหว่างผู้ส่งและผู้รับข้อมูล ซึ่งเป็นการลดความเสี่ยงในการดำเนินธุรกิจลงไปอย่างมาก ซึ่งทำให้ผู้รับและผู้ส่งสามารถวางแผนดำเนินการธุรกิจต่างๆ ได้ดีขึ้น

5) การควบคุมสินค้าคงเหลือ (Inventory) ทำได้อย่างมีประสิทธิภาพขึ้น คือ สามารถควบคุมให้เหลือน้อยที่สุดไปจนถึงการนำระบบ Just – In – Time มาใช้

6) สร้างความสัมพันธ์ที่ดีระหว่างองค์กรที่แลกเปลี่ยนข้อมูลด้วย EDI ด้วยกัน เนื่องจากเกิดความสะดวก ประหยัด และรวดเร็วกว่าการดำเนินธุรกิจกับหน่วยงานที่ไม่ได้ใช้ EDI

7) สามารถบริการลูกค้าได้ดียิ่งขึ้น ทั้งในเรื่องของความถูกต้องและความรวดเร็วในการตอบสนองความต้องการของลูกค้า ตั้งแต่เรื่องของการซื้อสินค้า การจัดส่งและการบริการหลังการขาย

---

[19] สุธรรม อยู่ในธรรม และคณะ. **แนวทางการพัฒนากฎหมายแลกเปลี่ยนข้อมูลด้วยสื่ออิเล็กโทรนิกส์ .** หน้า 36.

กล่าวได้ว่า การนำ EDI มาใช้เป็นประโยชน์ต่อองค์การอย่างมาก ไม่เฉพาะในเรื่องกาลดต้นทุนการผลิตและลดความผิดพลาดต่างๆ เท่านั้น แต่ยังเป็นผลดีต่อการวางแผนธุรกิจและการบริการต่อลูกค้า จึงทำให้ EDI ได้รับความนิยมมากขึ้นในปัจจุบัน

ข. ประโยชน์ที่เกิดจากการใช้ระหว่างอุตสาหกรรม

จากความต้องการใช้ระบบอิเล็กทรอนิกส์เพื่อการส่งผ่านและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ทำให้บริษัทขนาดใหญ่หลายบริษัทในอุตสาหกรรมต่างๆ พยายามที่จะกำหนดมาตรฐานของการส่งผ่านข้อมูลดังกล่าวของตนขึ้น ทำให้พบปัญหาที่ตามมา คือ บริษัทคู่ค้าเป็นจำนวนมากที่ต้องการติดต่อกับบริษัทขนาดใหญ่ที่มีมาตรฐานการแลกเปลี่ยนข้อมูลที่แตกต่างกัน ต่างก็มีความยุ่งยากในการจัดทำระบบคอมพิวเตอร์เพื่อการติดต่อดังกล่าว ไม่ว่าจะเป็นเรื่องของ

1) อุปกรณ์ส่วนประกอบคอมพิวเตอร์ (ต้องเป็นระบบเดียวกันทั้งที่เป็นบริษัทผู้ส่งข้อมูลและบริษัทผู้รับข้อมูล)

2) โปรแกรมใช้งานระบบการแลกเปลี่ยนข้อมูล(ต้องเป็นระบบเดียวกัน)

3) Protocol เพื่อการติดต่อระหว่างเครื่องต้องเหมือนกัน

4) ความเร็วของการส่งผ่านข้อมูลต้องเหมือนกัน

5) สายโทรศัพท์ (ที่ใช้เพื่อการแลกเปลี่ยนข้อมูล) ต้องว่างอยู่เสมอ

ข้อมูลและการป้อนข้อมูลต้องเป็นมาตรฐานเดียวกัน

ทำให้เกิดความสับสน ทั้งยังเป็นการเพิ่มเติมต้นทุนและความยุ่งยากในการจัดการ เนื่องจากบริษัทคู่ค้าจำเป็นต้องมีคอมพิวเตอร์หลายระบบเพื่อเชื่อมโยงเข้ากับบริษัทขนาดใหญ่แต่ละแห่ง

การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI)ในกระบวนการยุติธรรมก็เป็นแนวทางในการแลกเปลี่ยนข้อมูลเกี่ยวกับการดำเนินการป้องกันและปราบปรามอาชญากรรมระหว่างหน่วยงานที่บังคับใช้กฎหมายและการดำเนินคดี ทั้งนี้เป็นหลักและใช้การสื่อสารระบบอินเตอร์เน็ตเช่นเดียวกัน ทั้งนี้เนื้อหาคือมาตรฐาน องค์ประกอบ และการทำงานของการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (EDI) สามารถใช้ในการดำเนินการในช่วงแรกของการดำเนินการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมของอเมริกาก่อนจะพัฒนาในรูปแบบที่เป็นอยู่ในปัจจุบัน

2.5 การบูรณาการข้อมูลด้านการบริหารงานยุติธรรม (Integration of Criminal Justice Information System)

สำหรับประเภทข้อมูลพื้นฐานที่ต้องจัดเก็บในรูปแบบอิเล็กทรอนิกส์เพื่อประโยชน์ในการบูรณาการข้อมูลและการบริหารจัดการกระบวนการยุติธรรม ประกอบด้วยข้อมูลที่เกี่ยวข้องกับงานด้านการป้องกันและปราบปรามอาชญากรรม ข้อมูลด้านการพิจารณาคดี ข้อมูลด้านการดำเนินงานตามคำพิพากษา และข้อมูลด้านการคุ้มครองสิทธิเสรีภาพของประชาชนรวมทั้งข้อมูลเพื่อการวางแผน กำหนดนโยบาย ศึกษาวิจัยและพัฒนาระบบงานยุติธรรมที่จะช่วยทำให้การบริหารงานกระบวนการยุติธรรมเป็นไปอย่างมีประสิทธิภาพ ทันสถานการณ์ และเกิดประสิทธิผลต่อการแก้ไขปัญหาต่างๆในสังคม

ส่วนหลักการบูรณาการข้อมูลสารสนเทศกระบวนการยุติธรรมที่เหมาะสมคือ สร้างศูนย์เชื่อมโยงข้อมูลครอบคลุมระบบฐานข้อมูลที่มีอยู่เดิม โดยใช้สถาปัตยกรรมระบบเทคโนโลยีสารสนเทศแบบกระจาย (Distributed Databases Architecture) ซึ่งฐานข้อมูลของทุกหน่วยงานจะยังคงอยู่ที่เดิม เฉพาะข้อมูลที่แลกเปลี่ยนจะถูกเก็บในรูปแบบมาตรฐานเดียวกัน และมีหน่วยงานกลางหรือศูนย์แลกเปลี่ยนข้อมูล (DATA EXCHANGE CENTER) หรือ DXC ทำหน้าที่บริหารจัดการข้อมูล โดยจัดเก็บข้อมูลในลักษณะ METADATA ซึ่งจะระบุหน่วยงานเจ้าของข้อมูล ประเภทและรูปแบบข้อมูล สิทธิการเข้าถึง และวิธีขอข้อมูล รวมทั้งตรวจสอบสิทธิผู้ขอใช้และให้บริการตามขั้นตอนที่กำหนดไว้ ทั้งนี้ผู้มีสิทธิเข้าถึงข้อมูลสามารถใช้บริการจากทุกสถานที่ที่แบบ ONE-STOP SERVICE โดยเรียกใช้ผ่านโปรแกรมประยุกต์แบบ WEB-BASED ทั่วไป เพื่อเข้าสู่ระบบ DXC ซึ่งเป็นเครือข่ายเฉพาะที่มีความปลอดภัยสูง

การบูรณาการระบบข้อมูลด้านงานยุติธรรม (Justice Information System Integration : JISI)ไม่ใช่แนวคิดใหม่แต่อย่างใด หน่วยงานต่างๆในกระบวนการยุติธรรมได้เล็งเห็นความสำคัญของการบูรณาการระบบข้อมูลเพื่อแบ่งปันข้อมูล เอกสาร และภาพต่างๆ โดยมีการจัดทำโครงการและแผนต่างๆ ระบบการบูรณาการได้ช่วยให้การปรับปรุงไม่เพียงแต่คุณภาพของความถูกต้องของข้อมูลต่างๆเท่านั้น แต่ยังช่วยให้การวินิจฉัย และการตัดสินต่างๆได้ดำเนินไปอย่างเหมาะสมและถูกต้องอีกด้วย ขจัดหรือลดทั้งข้อผิดพลาดและระยะเวลาในการเข้าถึงข้อมูลโดยเฉพาะในประเด็นที่มีความสำคัญต่อการตัดสิน ผู้ที่ปฏิบัติงานที่เกี่ยวข้องในกระบวนการยุติธรรมหลากหลายสามารถเข้าถึงและใช้ข้อมูลเดียวกันแม้จะอยู่ห่างไกลจากศูนย์ข้อมูล

อย่างไรก็ตาม แนวคิดเรื่อง การบูรณาการระบบข้อมูลด้านงานยุติธรรมหรือ JISI นั้นก็ยังแตกต่างกันออกไป ขอบเขตของข้อมูลให้เป็นเอกภาพ การให้นิยามความหมายและประเภทข้อมูลก็ยังหลากหลายแตกต่างกันออกไป [20]

ในหลายกรณีอาจจะมีหน่วยงานใดเพียงหน่วยงานเดียวที่รับดำเนินการจากระบบข้อมูลต่างๆที่หลากหลาย เช่น กระทรวงความปลอดภัยสาธารณะ (Department of Public Safety : DPS) ที่จะเป็นหน่วยงานหรือองค์กรที่รวบรวมบูรณาการข้อมูลด้านประวัติการขับขี่รถยนต์และประวัติอาชญากร รวมไปถึงการบูรณาการระบบข้อมูลอาชญากรรมหรือฐานข้อมูลลายนิ้วมือ ซึ่งต่อมาเมื่อมีการปรับปรุงประสิทธิภาพและประสิทธิผลทำให้ระบบการสื่อสารข้อมูลต่างๆ เป็นไปได้อย่างรวดเร็ว และสามารถใช้ในระดับนานาชาติได้

ยังมีโครงการอื่นๆ ซึ่งมีการบูรณาการระบบข้อมูลระหว่างหน่วยงานที่มีบทบาทหน้าที่แตกต่างกัน แต่ต้องการที่จะแลกเปลี่ยนข้อมูลสำคัญในกระบวนการยุติธรรม เช่น ระบบข้อมูลสารสนเทศด้านกระบวนการยุติธรรมของเท็กซัส หรือ CJIS (Texas Criminal Justice Information System) โดยดำเนินการประสานแฟ้มข้อมูลร่วมกับทะเบียนประวัติอาชญากรรมคอมพิวเตอร์ หรือ CCH (The Computerized Criminal History) ที่ดำเนินการโดยกระทรวงความมั่นคงสาธารณะ (DPS) ความพยายามที่จะสร้างความร่วมมือในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานตรวจคนเข้าเมืองกับFBIด้านลายพิมพ์นิ้วมือ มาตรฐานการจัดเก็บข้อมูลในระดับชาติ การพัฒนาระบบข้อมูลข่าวสารด้านกระบวนการยุติธรรมของมลรัฐแคนซัสซิตี้ที่เป็นโครงการต้นแบบ หรือโปรแกรมระบบการบริหารจัดการข้อมูลด้านคดีของศาลที่เป็นมาตรฐาน รวมทั้งระบบรายงานข้อมูลของท้องถิ่น เหล่านี้เป็นต้น

2.5.1 ปัญหาและอุปสรรคประมวลผลข้อมูลเกี่ยวกับกระบวนการยุติธรรม

จากการศึกษาเกี่ยวกับการประมวลผลข้อมูลเกี่ยวกับ กระบวนการยุติธรรม และการนำเอาระบบข้อมูลเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมนั้น พบว่า ประสบปัญหาและอุปสรรคดังต่อไปนี้[21]

---

[20] SEARCH 2001

[21] Dawes et al 2003; SEARCH, 2001 b

หน่วยงานในกระบวนการยุติธรรมมีหลากหลายมากเกินไปและความต้องการของหน่วยงานก็แตกต่างกัน ทำให้การกำหนดมาตรฐานและการประมวลผลข้อมูล แตกต่างกันออกไป เช่น องค์กรตำรวจมีความต้องการและใช้ข้อมูลเกี่ยวกับการสืบสวนและจับกุม แต่ในองค์กรศาลไม่ต้องการข้อมูลที่เกี่ยวกับการสืบสวน เป็นต้น ดังนั้น ทำให้การประมวลผลมีความยุ่งยาก และล่าช้า เพราะอาจจะต้องมีการจำแนกเป็นข้อมูลประเภท primary, secondary เป็นต้น

1. บางองค์กรในกระบวนการยุติธรรมยังไม่ให้ความสำคัญและจัดสรรงบประมาณให้น้อย ทำให้การดำเนินการเป็นไปอย่างล่าช้าและเชื่อมโยงข้อมูลได้ยาก เนื่องจากหลายๆองค์กรในกระบวนการยุติธรรม มองว่า หน่วยงานด้านเทคโนโลยีสารสนเทศเป็นหน่วยงานสนับสนุนการทำงานไม่ใช่หน่วยงานหลัก และหน่วยงานตนเองก็อาจไม่จำเป็นต้องใช้ข้อมูลที่ได้จากการเก็บและประมวลผล ดังนั้นจึงไปมุ่งให้ความสำคัญกับการปฏิบัติงานหลัก

2. หน่วยงานบางหน่วยงานยังมีขนาดเล็กเกินไปที่จะมีการจ้างบุคลากรที่มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศมาประมวลผลข้อมูลในกระบวนการยุติธรรม และการเป็นหน่วยงานเล็ก ข้อมูลน้อย การจ้างบุคลากรมาประจำเป็นการไม่คุ้มค่าใช้จ่ายในการดำเนินการองค์กร

3. การขาดการวางแผนระยะยาวในการดำเนินการ การจัดสรรงบประมาณอาจพิจารณาให้ไม่ต่อเนื่องให้เฉพาะบางปี ทำให้การประมวลผลก็ขาดความต่อเนื่องตามไปด้วย

4. การมีข้อจำกัดในด้านบุคลากรและการออกแบบเพื่อนำมาใช้งานหรือใช้ประโยชน์อย่างจริงจัง เนื่องจากการเก็บรวบรวมและแลกเปลี่ยนข้อมูลตลอดจนการบูรณาการข้อมูลในองค์กรจำเป็นจะต้องอาศัยบุคลากรที่มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้านมาเป็นผู้ช่วยวางแผนและออกแบบระบบให้เหมาะสมกับองค์กรและการใช้งาน ซึ่งองค์กรหลายองค์กรในกระบวนการยุติธรรมก็ขาดบุคลากรด้านนี้โดยตรง การจัดหาจึงเป็นเพียงอุปกรณ์มาประจำ

5. การประสบปัญหาในด้านความเสี่ยงต่างๆ ปัญหาความเสี่ยงต่างๆที่เกิดขึ้นมีหลายประการ โดยเฉพาะอย่างยิ่ง จากด้าน ข้อมูลส่วนบุคคล (privacy) และ เรื่องความปลอดภัยของข้อมูล (security) [22]นอกจากนี้ยังมีปัญหาความเสี่ยงอื่นๆตามมา อาทิ เช่น ความถูกต้องของข้อมูล การสร้างข้อจำกัดในการใช้ การเข้าไปใช้ข้อมูลโดยไม่ได้รับอนุญาต หรือไม่มีอำนาจอาชญากรรมคอมพิวเตอร์ เป็นต้น

---

[22] Peter Csonka 2001

6. ความหวาดกลัวในปัญหาเกี่ยวกับความรับผิด (liability) หากมีความผิดพลาดเกิดขึ้นกับข้อมูล โดยเฉพาะหากตนเองต้องรับผิดชอบโดยตรง ซึ่งความรับผิดจะเกิดขึ้นกับตน ซึ่งจะสร้างความยุ่งยากในการปฏิบัติงานในองค์กร ดังนั้น การดำเนินการประมวลผลและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม จึงดูเหมือนจะสร้างความยุ่งยากลำบากใจมากกว่า จึงไม่ให้ความสนใจในการดำเนินการ

ปัญหาต่างๆเหล่านี้ บางปัญหาก็ได้รับการแก้ไข เช่น ในปัญหาที่เกี่ยวพันกับงบประมาณ หากองค์กรใดสนใจสมัครเข้าร่วมในการดำเนินการ ก็จะมีการจัดสรรงบประมาณให้จำนวนหนึ่ง (โดยมีการประเมินผล) และให้ผู้เชี่ยวชาญในการวางแผนระบบเข้าไปช่วยวางแผนในหน่วยงาน เป็นต้น

2.6 เทคโนโลยีสารสนเทศและการบูรณาการข้อมูลด้านงานยุติธรรมของไทย

ปัจจุบันหน่วยงานในกระบวนการยุติธรรมที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานมีทั้งสิ้น 14 หน่วยงาน ได้แก่

- ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติ
- กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ
- สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
- สำนักงานป้องกันและปราบปรามการฟอกเงิน
- สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด
- กรมสอบสวนคดีพิเศษ
- สำนักงานอัยการสูงสุด
- สำนักงานศาลยุติธรรม
- กรมราชทัณฑ์
- กรมคุมประพฤติ
- กรมพินิจและคุ้มครองเด็กและเยาวชน
- กรมบังคับคดี
- สถาบันนิติวิทยาศาสตร์
- กรมคุ้มครองสิทธิและเสรีภาพ

2.6.1 การเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมของไทย

การเชื่อมโยง ข้อมูลระหว่างหน่วยงานในกระบวนยุติธรรมและการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการดำเนินการ ซึ่งจากการศึกษาและการประมวลข้อมูลจากการสัมภาษณ์จากการประชุมเชิงปฏิบัติการเพื่อรับฟังข้อมูล ข้อเท็จจริง ข้อมูลต่างๆ ที่เกี่ยวข้องสามารถวิเคราะห์ได้ดังนี้ (รายละเอียดปรากฏในภาคผนวก ก.)

1. ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาติ

ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาติ ปัจจุบัน เปลี่ยนชื่อเป็น “ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ ทำหน้าที่เป็นศูนย์กลางในการดำเนินการเกี่ยวกับการจัดเก็บข้อมูลต่างๆที่เกี่ยวข้องกับการปฏิบัติงานของตำรวจ เป็นหน่วยงานระดับกองบังคับการที่ทำหน้าที่เป็นหน่วย ด้านระบบเทคโนโลยีสารสนเทศของสำนักงานตำรวจแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาตินั้น ปัจจุบันมีฐานข้อมูลบางส่วนของกองทะเบียนประวัติอาชญากร (ทว.) บางส่วน ที่เก็บรักษาไว้ที่ศูนย์เทคโนโลยีกลาง สำนักงานตำรวจแห่งชาติ และมีข้อมูลด้านยาเสพติด รวมทั้งบุคคลที่ขึ้นทะเบียนเป็นบุคคลต้องห้าม (Block lists) เท่านั้น ส่วนการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมอื่นๆยังไม่มี ไม่ว่าจะเป็นสำนักงานป้องกันและปราบปรามการทุจริตแห่งชาติ (ปปช.) สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กรมสอบสวนคดีพิเศษ (DSI) สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน กรมบังคับคดี สถาบันนิติวิทยาศาสตร์ กรมคุ้มครองสิทธิและเสรีภาพ เป็นต้น ซึ่งศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาตินั้น ยังมีความต้องการเชื่อมโยงหรือบูรกณาการข้อมูลอย่างยิ่ง กับหน่วยงานอื่นๆ ในกระบวนการยุติธรรม เพราะข้อมูลเหล่านั้นจะเป็นประโยชน์สำหรับการปฏิบัติงานของเจ้าหน้าที่ตำรวจทั้งในด้านการป้องกัน และปราบปรามอาชญากรรม ทั้งประเทศและสามารถนำไปใช้ในการจัดทำนโยบายและแผนของสำนักงานตำรวจแห่งชาติได้ ตามความมุ่งหมายของการจัดตั้งศูนย์ฯต่อไป

ปัญหาในการดำเนินการ คือ ขาดนโยบายที่ชัดเจนว่า ควรจะจัดเก็บข้อมูลอะไรบ้าง และขาดความต่อเนื่องในการดำเนินการ หน่วยงานนี้เป็นหน่วยงานทางด้านเทคนิค ซึ่งบทบาทความสำคัญทั้งในด้านบุคลากร งบประมาณและการดำเนินการ ยังอยู่ในขั้นเตรียมความพร้อมสำหรับความร่วมมือในการเชื่อมโยง หรือบูรณาการข้อมูลเทคโนโลยีสารสนเทศด้านงานยุติธรรมกับหน่วยงานอื่นๆ

สำหรับปัญหาที่เกี่ยวข้องกับกฎ ระเบียบ สำหรับการดำเนินการนั้น ในปัจจุบันสำนักงานตำรวจแห่งชาติและทางศูนย์เองไม่ได้มีกฎ ระเบียบ เป็นการเฉพาะไม่ว่าจะเป็นการเอื้ออำนวยหรือเป็นอุปสรรค การใช้กฎหมายก็จะใช้กฎหมายข้อมูลข่าวสารทางราชการโดยทั่วไปและในกรณีที่มีหน่วยงานแจ้งขอข้อมูลเข้ามาเป็นการเฉพาะก็ขึ้นอยู่กับดุลพินิจของผู้บังคับบัญชาที่จะอนุญาตให้ใช้ข้อมูลข่าวสารเหล่านั้น

2. กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ

กองทะเบียนประวัติอาชญากร หรือรู้จักกันในนาม “ทว.” เป็นหน่วยงานที่มีบทบาทสำคัญที่จะเก็บรวบรวมข้อมูลบุคคลที่ก่ออาชญากรรมที่เกี่ยวข้อง โดยเป็นข้อมูลจากการพิมพ์ลายนิ้วมือและลักษณะพฤติกรรมการประกอบอาชญากรรม ซึ่งข้อมูลที่จัดเก็บเป็นข้อมูลสำคัญที่หน่วยงานต่างๆในกระบวนการยุติธรรมจำเป็นจะต้องอาศัยประกอบการจัดทำสำนวนและการดำเนินคดี ซึ่งในการดำเนินการเก็บรวบรวมและประมวลข้อมูลนั้นอาศัยข้อมูลจากสถานีตำรวจต่างๆได้ดำเนินการจัดส่งมาเก็บไว้ มีการประมวลและจัดเก็บเป็นหมวดหมู่รวมทั้งจัดเก็บในฐานข้อมูลทางอิเลคโทรนิคส์

กองทะเบียนประวัติอาชญากร ได้มีการเชื่อมโยงข้อมูลกับหน่วยงานหลายหน่วยงาน คือ สำนักงานป้องกันและปราบปรามยาเสพติด (ปปส.) กรมราชทัณฑ์ กรมคุมประพฤติ เป็นหลัก ส่วนหน่วยงานอื่นๆ ในกระบวนการยุติธรรมยังไม่ได้มีการดำเนินการเชื่อมโยงข้อมูลแต่อย่างใด

สำหรับหน่วยงานที่กองทะเบียนประวัติอาชญากรต้องการที่จะเชื่อมโยงข้อมูลด้วยมากที่สุด คือ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม เนื่องจากต้องการทราบผลของการดำเนินคดี ซึ่งผลดังกล่าวจะเป็นประโยชน์ต่อกองทะเบียนประวัติอาชญากร ในแง่ของการปรับปรุงข้อมูลให้มีความทันสมัยและถูกต้อง

ปัญหาที่กองทะเบียนประวัติอาชญากร ประสบในด้านของการเชื่อมโยงข้อมูลก็คือ ความต้องการข้อมูลที่เป็นประโยชน์ในคดี แต่มีการจัดส่งทางโทรสาร (Fax) หรือ ทาง E- Mail ซึ่งข้อมูลเหล่านี้ ศาลจะรับฟังเป็นพยานหลักฐาน (พยานเอกสาร) ได้หรือไม่อย่างไรในทางคดีอาญา

ส่วนปัญหาทางกฎหมายที่เกี่ยวข้องก็คือ มีข้อมูลจำนวนมากที่กองทะเบียนประวัติอาชญากรจัดเก็บ และมีการดำเนินการเตรียมในระบบฐานข้อมูลเทคโนโลยีสารสนเทศแล้ว แต่ข้อมูลเหล่านั้น ยังต้องถือเป็นความลับส่วนบุคคลที่ไม่สามารถจัดส่งให้หน่วยงานอื่นๆ

ได้ เนื่องจาก ข้อมูลของบุคคลเหล่านี้ (ยัง) เป็นข้อมูลเกี่ยวกับ “ผู้ต้องหา” ไม่ใช่จำเลย ซึ่งในกฎหมายแม่บท เช่น กฎหมายรัฐธรรมนูญกำหนดว่า ผู้ต้องหาหรือแม้จำเลยนั้น ต้องสันนิษฐานว่าเป็นผู้บริสุทธิ์อยู่ การเปิดเผยข้อมูลส่วนบุคคลอาจจะนำไปสู่การถูกฟ้องร้อง ตามประมวลกฎหมายอาญา มาตรา 157[23] และตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420[24], 423[25] เรื่องละเมิด และหมิ่นประมาทได้

หากมีข้อตกลงระหว่างหน่วยงานในกระบวนการยุติธรรมชัดเจน ให้ถือเป็นการดำเนินการที่ชัดเจน ก็อาจเป็นข้อยกเว้นได้ และทางกองทะเบียนประวัติอาชญากรก็ได้มีการเตรียมดำเนินการปรับปรุงระเบียบการใช้ข้อมูลดังกล่าว แต่อยู่ในระหว่างการดำเนินการอยู่ อย่างไรก็ตามในส่วนของบุคลากรผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูล ยังมีความกังวลในเรื่องของการเชื่อมโยงข้อมูล เพราะนั่นหมายความว่า ข้อมูลที่อยู่ในครอบครองและถูกเก็บไว้ จะถูกใช้โดยหน่วยงานอื่นๆซึ่งหากไม่มีกฎหมายมารองรับให้เกิดความชัดเจน เกรงว่าจะถูกฟ้องร้องดำเนินคดีได้ เพราะการจัดเก็บข้อมูล เป็นการจัดเก็บตามที่กฎหมายให้อำนาจ แต่การใช้ข้อมูลยังมีความไม่ชัดเจนหากมีบุคคลหรือหน่วยงานอื่นๆเอาไปใช้

กองทะเบียนประวัติอาชญากรมุ่งที่จะเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรมในลักษณะที่เป็นทั้งผู้ให้และเป็นทั้งผู้ใช้ แต่ก็อยากที่จะเริ่มการเชื่อมโยงข้อมูลกับหน่วยงานที่จำเป็น และมีระบบข้อมูลคล้ายคลึงกันก่อน จากนั้น หากมีการดำเนินการที่ได้ผลจึงจะค่อยๆขยายออกไปกับหน่วยงานอื่นๆสร้างระบบโดยเฉพาะกับกรมราชทัณฑ์ หรือสถาบันนิติวิทยาศาสตร์ เป็นต้น ข้อมูลเกี่ยวกับการกระทำผิดซ้ำ เป็นข้อมูลสำคัญ เพราะหากมีการพัฒนาและเชื่อมโยงฐานข้อมูลจากการกระทำผิดซ้ำแล้ว หน่วยงานอื่นๆจะสามารถนำไปใช้ประโยชน์ได้อย่างมากมาย และหน่วยงานที่เคยติดต่อประสานกันในสำนักงานตำรวจ

---

[23] **มาตรา 157** ผู้ใดเป็นเจ้าพนักงานปฏิบัติหรือละเว้นการปฏิบัติหน้าที่โดยมิชอบเพื่อให้เกิดความเสียหายแก่ผู้หนึ่งผู้ใดหรือปฏิบัติหรือละเว้นการปฏิบัติหน้าที่โดยทุจริตต้องระวางโทษจำคุกตั้งแต่ 1 ปีถึง 10 ปี.....

[24] **มาตรา 420** ผู้ใดจงใจหรือประมาทเลินเล่อทำต่อบุคคลอื่นโดยผิดกฎหมายทำให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

[25] **มาตรา 423** ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนกับความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใดๆอันเกิดจากการนั้นแม้ทั้งเมื่อตนไม่รู้ว่าข้อความนั้นไม่จริงหากแต่ควรจะได้รู้

ผู้ใดส่งข่าวสารอันตนไม่ได้รู้ว่าเป็นความจริงหากว่าตนเองหรือผู้รับข่าวสารนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสารเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่

แห่งชาติ คือ สำนักงานตรวจคนเข้าเมือง (ตม.) ซึ่งตม.เองก็เชื่อมโยงข้อมูลกับสำนักงานปปส. อยู่แล้ว หากร่วมมือกันก็จะขยายเครือข่ายไปได้ หรือ หน่วยงานนอกกระบวนการยุติธรรม เช่น กระทรวงต่างประเทศ ก็เป็นหน่วยงานที่หากมีการเชื่อมโยงข้อมูลด้วยกันแล้วจะเป็นประโยชน์อย่างยิ่งในการปฏิบัติงาน

3. กรมพินิจและคุ้มครองเด็กและเยาวชน

กรมพินิจและคุ้มครองเด็กและเยาวชน เป็นหน่วยงานระดับกรมสังกัดกระทรวงยุติธรรม มีบทบาทมีอำนาจหน้าที่พิทักษ์และคุ้มครองสิทธิเด็กและเยาวชนที่กระทำความผิด ส่งเสริมความมั่นคงของสถาบันครอบครัวและชุมชนโดยใช้กระบวนการยุติธรรมทางเลือก กระบวนการยุติธรรมเชิงสมานฉันท์ การหันเหคดีออกจากกระบวนการยุติธรรม และมาตรการอื่นๆ ดำเนินการด้าน คดีอาญา คดีครอบครัว กำกับการปกครองและการบำบัดแก้ไข ฟื้นฟู ป้องกัน พัฒนาและสงเคราะห์ ตลอดจนการติดตามประเมินผลเด็กและเยาวชน ฯลฯ

ในด้านการเชื่อมโยงข้อมูลระหว่างงานในกระบวนการยุติธรรม และการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการดำเนินการนั้น มีการเชื่อมโยงเพียง 4 หน่วยงาน คือ

1. กองทะเบียนประวัติอาชญากร (ทว.) สำนักงานตำรวจแห่งชาติ ในด้านการตรวจสอบประวัติและการดำเนินการ เรื่อง การลบทะเบียนประวัติอาชญากรของเด็กและเยาวชนที่กระทำผิดหรือถูกดำเนินการในกระบวนการยุติธรรมออกจากฐานข้อมูลประวัติอาชญากร

2. สำนักงานยุติธรรม การดำเนินการเป็นการใช้ฐานข้อมูลด้านการดำเนินคดี ผลคำพิพากษาของสำนักงานศาลยุติธรรม เพื่อดำเนินการในส่วนของกรมพินิจและคุ้มครองเด็กและเยาวชน อย่างไรก็ตาม ในปัจจุบัน ยังเป็นเพียงแค่ด้านการตรวจสอบเฉพาะราย ไม่สามารถดำเนินการตรวจสอบ โดยใช้ฐานข้อมูลด้านสารสนเทศ

3. กรมราชทัณฑ์ กรมพินิจและคุ้มครองเด็กและเยาวชน ใช้ฐานข้อมูลด้านผลการดำเนินการหลังคำพิพากษา ในกรณีที่เกี่ยวข้องกับเด็กและเยาวชนที่ศาลมีคำพิพากษาให้ไปอยู่ในความดูแลของกรมราชทัณฑ์

4. กรมคุมประพฤติ ในส่วนที่เกี่ยวข้องเป็นการที่กรมพินิจและคุ้มครองเด็กและเยาวชน ใช้ฐานข้อมูลด้านผลการคุมประพฤติ ในกรณีที่ผู้กระทำความผิดเป็นเด็ก หรือเยาวชนเพื่อนำผลไปประกอบการดำเนินงานด้านการสืบเสาะ ข้อเท็จจริง ของเด็กและเยาวชนที่ถูกจับกุมดำเนินคดีในชั้นสถานพินิจ

ในด้านของปัญหาด้านกฎ ระเบียบ และกฎหมายที่เกี่ยวข้องของกรมพินิจและคุ้มครองเด็กและเยาวชน อาจจะเป็นปัญหาที่เกี่ยวข้องกับเรื่องอนุสัญญาสิทธิเด็ก ข้อ 40 พระราชบัญญัติจัดตั้งศาลเยาวชนและครอบครัวและวิธีพิจารณาคดีเยาวชนและครอบครัว พ.ศ. 2534 มาตรา 93 [26] ในส่วนอื่นๆที่เกี่ยวข้องกับข้อมูลข่าวสารก็จะใช้พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 เป็นหลัก ซึ่งหากพิจารณาโดยรวมแล้วจะเห็นว่ากฎหมายที่เกี่ยวข้องมีแนวโน้มที่จะเป็นอุปสรรคต่อข้อมูลการกระทำความผิดของเด็กและเยาวชน

4. กรมราชทัณฑ์

มีอำนาจหน้าที่ปฏิบัติต่อผู้กระทำผิดให้เป็นไปตามคำพิพากษาหรือคำสั่งตามกฎหมายโดยดำเนินการตามกฎหมายว่าด้วยการราชทัณฑ์และกฎหมายอื่นที่เกี่ยวข้อง กำหนดแนวทางปฏิบัติต่อผู้ต้องขังให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ นโยบายของกระทรวง หลักอาชญาวิทยา และหลักทัณฑวิทยา ตลอดจนข้อกำหนดมาตรฐานขั้นต่ำสำหรับปฏิบัติต่อผู้ต้องขังและข้อเสนอแนะในเรื่องที่เกี่ยวข้องขององค์การสหประชาชาติ ดำเนินการเกี่ยวกับการสวัสดิการและการสงเคราะห์แก่ผู้ต้องขัง จัดทำและประสานแผนงานของกรมให้เป็นไปตามนโยบายและแผนแม่บทของกระทรวง รวมทั้งกำกับ เร่งรัด ติดตาม และประเมินผลการปฏิบัติงานตามแผนงานของหน่วยงานในสังกัดกรม

กรมราชทัณฑ์ได้มีการเชื่อมโยงระบบเพื่อการสืบค้นข้อมูล 13 หลัก กับศูนย์ทะเบียนราษฎรฯ นอกจากนี้ยังมีการเชื่อมโยงและดำเนินการตามแผนแม่บทเทคโนโลยีสารสนเทศ กระทรวงยุติธรรม

ในส่วนของการใช้เทคโนโลยีสารสนเทศของหน่วยงานนั้น กรมราชทัณฑ์ไม่ได้ขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม กรมราชทัณฑ์มีการจัดทำและมีนโยบายในด้านการใช้เทคโนโลยีสารสนเทศที่ชัดเจน แต่ขาดการดำเนินการอย่างจริงจังและต่อเนื่องประกอบกับการเปลี่ยนแปลงรัฐบาลที่ทำให้การพัฒนากระบวนการยุติธรรมของประเทศดำเนินไปอย่างล่าช้า ซึ่งก็ส่งผลกระทบต่อการใช้เทคโนโลยีสารสนเทศด้วย และเห็นด้วยว่า ในการดำเนินการยังขาดหน่วยงานที่เป็นเจ้าภาพหลัก ในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการ

---

[26] มาตรา 93 ห้ามมิให้ผู้ใดบันทึกภาพ แพร่ภาพ พิมพ์รูปหรือบันทึกเสียง แพร่เสียงของเด็กหรือเยาวชนซึ่งต้องหาว่ากระทำความผิดหรือโฆษณาข้อความซึ่งปรากฏในทางสอบสวนของพนักงานสอบสวนหรือในทางพิจารณาคดีของศาลที่อาจทำให้บุคคลอื่นรู้จักตัว ชื่อตัว ชื่อสกุลของเด็กหรือเยาวชนนั้นหรือโฆษณาข้อความเปิดเผยประวัติ การกระทำความผิดหรือสถานที่ สถานทำงาน หรือสถานศึกษาของเด็กหรือเยาวชนนั้น

ประมวลผล หากมีหน่วยงานที่เป็นเจ้าภาพหลักในการบูรณาการข้อมูลจะช่วยประสานงานให้หน่วยงานของแต่ละหน่วยงานมีข้อมูลที่ถูกต้อง เหมาะสม และทันเวลา

การดำเนินการบูรณาการข้อมูลในกระบวนการยุติธรรมนั้น จำเป็นอย่างยิ่งที่ผู้บริหารระดับสูงต้องให้ความสำคัญอย่างยิ่ง ในขณะที่ ปัญหาด้านงบประมาณก็มีส่วนสำคัญทั้งๆที่รู้และเข้าใจในบทบาทงานด้านเทคโนโลยีสารสนเทศแต่การต้องใช้งบประมาณที่สูง และงานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน เป็นภาระงานที่ยังรองได้ อันส่งผลกระทบต่อเนื่องที่ทำให้ขาดความพร้อมทางด้านอุปกรณ์ต่างๆของทุกหน่วยงานในกระบวนการยุติธรรม มากน้อยแตกต่างกันไป ประกอบกันปัญหารการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน เนื่องจาก การเปลี่ยนแปลงเทคโนโลยีที่รวดเร็ว และบุคลากรที่เก่งจริงก็ไปอยู่ในภาคเอกชน

ส่วนด้านปัญหาการเก็บรวบรวมข้อมูลที่มีความซับซ้อนนั้น ปัญหานี้มีสาเหตุจากการที่แต่ละหน่วยงานจะจัดเก็บกันเอง โดยมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ต่างฝ่ายต่างจัดเก็บ ก็ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก เพราะยังขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ส่งผลตามมาทำให้ข้อมูลมีความน่าเชื่อถือน้อย เพราะมีข้อมูลจำนวนมากที่ขาดการปรับปรุง เปลี่ยนแปลง ข้อมูลให้เป็นปัจจุบัน จัดเก็บแล้วก็ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน

ด้านการคุ้มครองข้อมูลก็เป็นสิ่งที่จำเป็นเพราะถือว่าข้อมูลของบุคคลที่เป็นความลับส่วนบุคคล เป็นสิ่งที่เป็นผลเสียได้สำหรับบุคคลนั้น การเคารพสิทธิ์ในข้อมูลส่วนบุคคลจึงต้องมีอยู่และให้การคุ้มครอง

ปัญหาหลักอื่นๆก็คือ การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ ซึ่งก็ส่งผลให้หลายๆหน่วยงานจึงขาดความพร้อม เพื่อการบูรณาการ ปัญหาอื่นๆก็คือ ปัญหาด้านงบประมาณ ซึ่งรัฐบาลไม่จัดให้ กรมราชทัณฑ์ต้องจัดเจียดมาดำเนินการเอง ซึ่งในส่วนนี้ก็ต้องขึ้นกับผู้บริหารกรมราชทัณฑ์ว่าจะมีการดำเนินการและนโยบายอย่างไร

กรมราชทัณฑ์มีความคาดหวังว่า สำหรับฐานข้อมูลของกรมราชทัณฑ์นั้นอย่างน้อยก็จะต้องมีข้อมูล หรือ ประวัติผู้ต้องขัง ในปีพ.ศ. 2545 กรมราชทัณฑ์ได้มอบหมายให้จุฬาลงกรณ์มหาวิทยาลัย และสถาบันเทคโนโลยีพระจอมเกล้าฯ ทำการวิเคราะห์ระบบงานเพื่อสามารถที่จะเชื่อมโยงข้อมูลเข้าออกได้ ซึ่งกรมราชทัณฑ์เตรียมความพร้อมในด้านการ

บูรณาการไว้ว่าจะต้องมีข้อมูล โดยเฉพาะเรื่องลายนิ้วมือ เนื่องจากในข้อมูลบางอย่าง เช่น หมายศาลไม่มีเลข 13 หลัก การมีการทำ Finger Print ที่เก็บรวบรวมข้อมูลได้ถึง 2 แสนคน และสามารถเรียกใช้ข้อมูลได้โดยระบบ real time[27]

ในการเชื่อมโยงข้อมูลนั้นกรมราชทัณฑ์ ได้ลงนามความร่วมมือ (MOU) กับหน่วยงานด้านกระบวนการยุติธรรมในจังหวัดนนทบุรี เป็นโครงการนำร่อง และถือเป็นขั้นแรก (Phase I) ในขณะเดียวกันก็มีการจัดทำ DXC โดยมาตั้ง Brokerที่กรมราชทัณฑ์

ด้านกฎหมายและระเบียบที่เกี่ยวข้องนั้น ในตัวกฎหมาย คือ พระราชบัญญัติราชทัณฑ์ พ.ศ.2479 เอง ไม่ได้มีการระบุถึงการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมแต่เน้นที่การบริหารจัดการ และสิทธิของผู้ต้องขัง กฎหมายที่ใช้ก็จะเป็นพระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 254

5. กรมบังคับคดี

มีอำนาจหน้าที่ดำเนินการยึดทรัพย์สิน อายัดทรัพย์สิน จำหน่ายทรัพย์สิน บังคับคดีล้มละลายบุคคลธรรมดาตามคำสั่งศาล บังคับคดีล้มละลายนิติบุคคล บังคับคดีล้มละลายกิจการพิเศษ บังคับคดีฟื้นฟูกิจการของลูกหนี้ ชำระบัญชีห้างหุ้นส่วนบริษัทหรือนิติบุคคลในฐานะผู้ชำระบัญชี ตาม คำสั่งศาล รับวางทรัพย์จากลูกหนี้หรือผู้มีสิทธิวางทรัพย์ ดำเนินการประเมินราคาทรัพย์ ดำเนินการตรวจสอบสิทธิทางบัญชีของผู้มีส่วนได้เสียเพื่อรับส่วนแบ่งจากคดี ตรวจสอบค่าใช้จ่ายและเรียกเก็บค่าธรรมเนียมการบังคับคดี

กรมบังคับคดีมีฐานข้อมูลที่เกี่ยวข้องกับทรัพย์สินที่ดำเนินการขายทอดตลาดและข้อมูลที่เกี่ยวข้อง แต่ก็ไม่ได้มีการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรมแต่อย่างใด ในส่วนของข้อมูลข่าวสารโดยปกติกรมบังคับคดีก็มีการปิดประกาศแจ้งข้อมูลที่เกี่ยวข้องเพื่อให้ผู้มีส่วนได้เสียมาดำเนินการ ในส่วนของกฎระเบียบที่เกี่ยวข้องกรมบังคับคดีไม่ได้มีการออกระเบียบเฉพาะเรื่องที่จะเอื้ออำนวยต่อการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ ไม่ว่าจะเป็นหน่วยงานในกระบวนการยุติธรรมหรือไม่และในการปฏิบัติงานทั่วไปก็จะยึดการดำเนินการตามหลักกฎหมายของพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 และให้เป็นดุลพินิจของผู้บังคับบัญชาระดับสูงที่เกี่ยวข้อง

---

[27] สัมภาษณ์คุณชาญ วชิรเดช. หัวหน้าศูนย์ทะเบียนประวัติผู้ต้องขัง กองแผนงาน กรมราชทัณฑ์ วันที่11 กุมภาพันธ์ 2550.

6. กรมคุ้มครองสิทธิและเสรีภาพ

มีอำนาจหน้าที่จัดระบบการบริหารจัดการด้านคุ้มครองสิทธิและเสรีภาพของประชาชน ดำเนินการและส่งเสริมการคุ้มครองสิทธิและเสรีภาพของประชาชน การระงับข้อพิพาทในสังคม ส่งเสริม พัฒนา และประสานงานกับภาครัฐและภาคเอกชนทั้งในและต่างประเทศ จัดทำระบบมาตรการและดำเนินการช่วยเหลือประชาชนที่ตกเป็นเหยื่ออาชญากรรม รวมทั้งจำเลยที่ถูกดำเนินคดีอาญาโดยมิได้เป็นผู้กระทำความผิดตามกฎหมายว่าด้วยค่าตอบแทนผู้เสียหายและค่าทดแทนและค่าใช้จ่ายแก่จำเลยในคดีอาญา ส่งเสริมและศึกษาวิจัยเพื่อการพัฒนาในด้านการคุ้มครองสิทธิและเสรีภาพ ติดตามและประเมินผลการดำเนินการด้านการคุ้มครองสิทธิและเสรีภาพ ปรับปรุงและแก้ไขกฎหมาย กฎ หรือข้อบังคับในด้านการคุ้มครองสิทธิและเสรีภาพส่งเสริม ดำเนินการ และปฏิบัติการตามแผนปฏิบัติการด้านสิทธิมนุษยชน และดำเนินการคุ้มครองพยานตามกฎหมายว่าด้วยการคุ้มครองพยานในคดีอาญา

ในการเชื่อมโยงข้อมูลในส่วนของกรมคุ้มครองสิทธิและเสรีภาพนั้น เนื่องจากเป็นหน่วยงานใหม่ การเชื่อมโยงข้อมูลในหน่วยงานด้านกระบวนการยุติธรรม ยังไม่ได้เกิดขึ้นชัดเจน แต่ก็มีการเตรียมการเพื่อรองรับตามแผนแม่บทเทคโนโลยี กระทรวงยุติธรรม ส่วนที่มีการเชื่อมโยงก็จะเป็นสำนักงานทะเบียนราษฎร์ เพื่อดำเนินการตรวจสอบและค้นหาข้อมูลในการดำเนินการด้านการจ่ายค่าทดแทน และการคุ้มครองพยาน ซึ่งหน่วยงานในกระบวนการยุติธรรมที่อยากจะเชื่อมโยงเร็วที่สุดก็คือ สำนักงานศาลยุติธรรม เพราะจะสะดวกต่อการปฏิบัติงาน ในความต้องการแล้ว ประสงค์อยากจะเชื่อมกับทุกหน่วยงานในกระบวนการยุติธรรม และนอกหน่วยงานในกระทรวงยุติธรรม เช่น สำนักงานผู้ตรวจการแผ่นดินรัฐสภา เพราะภาระงานของกรมเชื่อมโยงกัน และภาระงานก็หลากหลายมากในการที่จะต้องประสานข้อมูลกับหน่วยงานอื่นๆให้มากที่สุดเท่าที่จะทำได้ โดยเฉพาะด้านสิทธิมนุษยชน และด้านของผู้เสียหายซึ่งเป็นข้อมูลที่สำนักงานตำรวจแห่งชาติ มีการจัดทำทะเบียนประวัติอาชญากร แต่ทะเบียนประวัติผู้เสียหาย ยังไม่ได้มีการดำเนินการอย่างเป็นระบบแต่อย่างใด กรมคุ้มครองสิทธิและเสรีภาพ เนื่องจากเป็นหน่วยงานใหม่ในกระทรวงยุติธรรม ดังนั้น การเชื่อมโยงข้อมูลในด้านงานยุติธรรมจะดำเนินการตามแผนแม่บทกระทรวงยุติธรรม และจะพยายามพัฒนาฐานข้อมูลของตนเอง ปัจจุบันมีข้อมูลบางส่วนที่เกิดจากการปฏิบัติงานแต่ยังไม่ได้จัดทำฐานเพื่อเชื่อมโยงข้อมูล

โดยภารกิจงานของกรมคุ้มครองสิทธิเสรีภาพมีภารกิจเกี่ยวข้องที่หลากหลายและมากมาย อย่างไรก็ตามทางกรมฯ ก็ยังไม่ได้มีการออกระเบียบมาเป็นพิเศษโดยเฉพาะที่เกี่ยวข้องกับการแลกเปลี่ยน หรือเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ การดำเนินการก็จะนำเอา

หลักเกณฑ์ตามพรบ.ข้อมูลข่าวสารทางราชการพ.ศ. 2540 มาใช้ ซึ่งไม่ได้มีปัญหาหรืออุปสรรคในเชิงกฎหมายแต่อย่างใด

7. สถาบันนิติวิทยาศาสตร์

มีอำนาจหน้าที่รับผิดชอบงานธุรการของคณะกรรมการมาตรฐานงานด้านนิติวิทยาศาสตร์ และคณะกรรมการบริหารกิจการด้านนิติวิทยาศาสตร์ รวมทั้งศึกษา รวบรวมและวิเคราะห์ข้อมูลต่าง ๆ ที่เกี่ยวกับงานของคณะกรรมการทั้งสองคณะ แต่งตั้งและเพิกถอนการแต่งตั้งรวมทั้งกำกับดูแลการปฏิบัติหน้าที่ของผู้ช่วยผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์ให้เป็นไปตามหลักเกณฑ์ มาตรฐาน และจรรยาบรรณ รับเรื่องราวร้องทุกข์จากบุคคลซึ่งได้รับความเสียหายจากการประพฤติผิดหลักเกณฑ์ มาตรฐาน หรือจรรยาบรรณของผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์ ฯลฯ

ในส่วนของการเชื่อมโยงข้อมูลของสถาบันนิติวิทยาศาสตร์กับหน่วยงานอื่นๆในกระบวนการยุติธรรมนั้น สถาบันนิติวิทยาศาสตร์ มีการจัดทำโครงการพัฒนาด้านเทคโนโลยีสารสนเทศ เพื่อรองรับการปฏิบัติงาน และการดำเนินการตามแผนแม่บทเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม โดยเฉพาะอย่างยิ่ง เพื่อให้สอดรับกับการดำเนินการจัดตั้งและพัฒนาศูนย์บุคคลสูญหาย เนื่องจากสถาบันนิติวิทยาศาสตร์นั้น เป็นหน่วยงานที่มีบทบาทในด้านข้อมูลเกี่ยวกับวัตถุพยาน ซึ่งผลการตรวจห้องปฏิบัติการจะส่งผลต่อคดี หน่วยงานของสถาบันติวิทยาศาสตร์จึงประสงค์จะให้ระบบฐานข้อมูลเป็นระบบปิด ซึ่งการจะเชื่อมโยงข้อมูลได้มากน้อยเพียงใด ก็ขึ้นอยู่กับผู้บริหารเป็นหลัก

ด้านกฎหมายและกฎระเบียบที่เกี่ยวข้องนั้น สถาบันนิติวิทยาศาสตร์ไม่ได้มีการจัดทำขึ้นโดยเฉพาะกฎหมายที่ใช้ก็จะมีกฎหมายแม่ คือ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ.2540 เป็นหลัก ควบคู่กับการใช้ดุลพินิจของผู้บริหารของสถาบันในการให้ข้อมูล

8. กรมสอบสวนคดีพิเศษ

กรมสอบสวนคดีพิเศษ มีอำนาจหน้าที่รับผิดชอบในงานธุรการของคณะกรรมการคดีพิเศษ คณะอนุกรรมการที่แต่งตั้งโดยคณะกรรมการคดีพิเศษ และคณะกรรมการที่ปรึกษาการบริหารงานบุคคลพนักงานสอบสวนคดีพิเศษ ป้องกัน ปราบปราม สืบสวน และสอบสวนคดีพิเศษตามกฎหมายและตามหลักเกณฑ์ที่คณะกรรมการคดีพิเศษประกาศ กำหนด หรือตามมติของคณะกรรมการคดีพิเศษ ศึกษารวบรวมและวิเคราะห์ข้อมูลเพื่อประโยชน์แก่การปฏิบัติหน้าที่ของคณะกรรมการ คดีพิเศษ จัดให้มีการศึกษาอบรมเพื่อพัฒนาระบบงานการสืบสวนและสอบสวน พัฒนาความรู้และประเมินสมรรถภาพการปฏิบัติ

หน้าที่ของพนักงานสอบสวนคดีพิเศษ เจ้าหน้าที่คดีพิเศษ และข้าราชการกรมสอบสวนคดีพิเศษ ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและตามกฎหมายอื่นอันเกี่ยวกับความผิดทางอาญาที่เป็นคดีพิเศษ และดำเนินการเกี่ยวกับงานกฎหมายและระเบียบในความรับผิดชอบของกรมและกฎหมายอื่นที่เกี่ยวข้อง

กรมสอบสวนคดีพิเศษมีข้อมูลระบบงานการสืบสวนและสอบสวนแต่ไม่สามารถเชื่อมต่อข้อมูลกับหน่วยงานอื่นๆได้ เนื่องจากข้อมูลต่างๆที่เกี่ยวข้องในคดีเป็นข้อมูลที่มีผลกระทบอย่างสูงต่อการดำเนินคดี อย่างไรก็ตาม กรมสอบสวนคดีพิเศษก็สามารถที่จะใช้ข้อมูลในฐานะที่เป็นผู้ใช้จากหน่วยงานบางหน่วยเช่น ข้อมูลจากฐานทะเบียบราษฎร์ หรือเป็นการติดต่อประสานขอข้อมูลจากหน่วยราชการอื่นๆเพื่อการสอบสวนดำเนินคดี กรมสอบสวนคดีพิเศษมิได้มีการออกระเบียบที่เป็นการเอื้ออำนวยหรือเป็นปัญหาและอุปสรรคต่อการเชื่อมโยงข้อมูลกับหน่วยงานอื่นในกระบวนการยุติธรรม และกฎหมายเฉพาะของหน่วยงานกับบทบาทหน้าที่ในการปฏิบัติงาน ทำให้เป็นปัญหาอุปสรรคในการที่จะเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆในฐานะที่เป็นผู้ให้ข้อมูล

9. กรมคุมประพฤติ

มีอำนาจหน้าที่ดำเนินการสืบเสาะและพินิจ ควบคุมและสอดส่อง แก้ไขฟื้นฟูและสงเคราะห์ผู้กระทำผิดในชั้นก่อนฟ้อง ชั้นพิจารณาคดีของศาล และภายหลังที่ศาลมีคำพิพากษาตามที่กฎหมายกำหนด ดำเนินการฟื้นฟูสมรรถภาพผู้ติดยาเสพติดในระบบบังคับรักษาตามกฎหมายว่าด้วยการฟื้นฟูสมรรถภาพผู้ติดยาเสพติด ส่งเสริมสนับสนุนเกี่ยวกับการดำเนินการแก้ไขฟื้นฟูและสงเคราะห์ผู้กระทำผิดในชุมชน พัฒนาระบบ รูปแบบ และวิธีการปฏิบัติต่อผู้กระทำผิดในชุมชน จัดทำและประสานแผนงานของกรมให้สอดคล้องกับนโยบายและแผนแม่บทของกระทรวง เร่งรัด ติดตามและประเมินผลการปฏิบัติงานของหน่วยงานในสังกัด เสริมสร้าง สนับสนุน และประสานงานให้ภาคประชาสังคมเข้ามามีส่วนร่วมในการปฏิบัติต่อผู้กระทำผิด และป้องกันสังคมจากอาชญากรรม รวมทั้งให้สามารถรวมเป็นเครือข่ายเพื่อดำเนินภารกิจดังกล่าว

กรมคุมประพฤติมีฐานข้อมูลและมีการเชื่อมโยงข้อมูลกับหลายหน่วยงาน เนื่องจากภารกิจและการดำเนินการของกรมคุมประพฤตินั้นมีความหลากหลายและจำเป็นจะต้องเกี่ยวข้องกับหน่วยงานในกระบวนการยุติธรรมไม่ว่าจะเป็นสำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ ฯลฯ และยังมีการเชื่อมโยงข้อมูลที่เกี่ยวข้องกับหน่วยงานอื่นๆเช่น สำนักทะเบียนราษฎร์ สำนักงานปปส. เป็นต้น

ในส่วนของปัญหาและอุปสรรคด้านกฎหมาย กรมคุมประพฤติมิได้มีการออกระเบียบเป็นการเฉพาะว่าด้วยการแลกเปลี่ยนและเชื่อมโยงข้อมูล หากแต่เป็นการประสานงานกับหน่วยงานที่เกี่ยวข้องและขอข้อมูลเพื่อใช้ในการปฏิบัติงานในการดำเนินการจึงใช้พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ.2540 กับดุลพินิจของผู้บังคับบัญชาในการให้ข้อมูลกับหน่วยงานที่ประสานงานเพื่อใช้ข้อมูลร่วมกัน

10. สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด

เป็นส่วนราชการที่อยู่ในบังคับบัญชาขึ้นตรงต่อรัฐมนตรี มีอำนาจหน้าที่ดำเนินการตามกฎหมายว่าด้วยการป้องกันและปราบปรามยาเสพติด กฎหมายว่าด้วยมาตรการในการปราบปราม ผู้กระทำความผิดเกี่ยวกับยาเสพติด และกฎหมายอื่น ๆ ที่เกี่ยวเนื่องกับการป้องกันและปราบปราม ยาเสพติด หรือการแก้ไขปัญหาเกี่ยวกับยาเสพติด ดำเนินการเกี่ยวกับงานเลขานุการของ คณะกรรมการป้องกันและปราบปรามยาเสพติดและคณะกรรมการตรวจสอบทรัพย์สิน รวมทั้งงานเลขานุการของคณะกรรมการที่ปรึกษา และคณะอนุกรรมการที่คณะกรรมการป้องกันและปราบปราม ยาเสพติดแต่งตั้ง หรือคณะอนุกรรมการที่คณะกรรมการตรวจสอบทรัพย์สินแต่งตั้ง ประเมิน สถานการณ์การดำเนินงานและให้ข้อเสนอแนะด้านนโยบายยุทธศาสตร์ แผน และงบประมาณในการดำเนินงานด้านป้องกันและแก้ไขปัญหายาเสพติด อำนวยการ เร่งรัด กำกับ ติดตามการดำเนินงานด้านป้องกันและแก้ไขปัญหายาเสพติดให้เป็นตามนโยบาย แผน และงบประมาณ ให้ข้อเสนอแนะด้านยุทธศาสตร์และประสานความร่วมมือกับต่างประเทศด้านยาเสพติด พัฒนาและสนับสนุนวิชาการด้านการป้องกันและแก้ไขปัญหายาเสพติดแก่หน่วยงานทั้งภาครัฐและเอกชน ส่งเสริมและสนับสนุนด้านพัฒนาองค์กร ทรัพยากรบุคลากร ข้อมูลสารสนเทศ กฎหมาย และระเบียบที่เกี่ยวข้องกับการป้องกันและแก้ไขปัญหายาเสพติด ปฏิบัติงานด้านการรณรงค์และประชาสัมพันธ์ต่อต้านยาเสพติด

ในทางปฏิบัติสำนักงาน ปปส.เป็นทั้งผู้ให้ข้อมูลและผู้รับข้อมูล โดยหน่วยงานในกระบวนการยุติธรรมที่ได้มีการเชื่อมโยงข้อมูลแล้ว ได้แก่ สำนักงานคณะกรรมการป้องกันการฟอกเงิน (ปปง.) กรมสอบสวนคดีพิเศษ (DSI) ในขณะที่บางหน่วยงานยังไม่มีการเชื่อมต่ออีกหลายหน่วยงาน

สำนักงานปปส. มีการจัดทำฐานข้อมูลด้านยาเสพติดมาตั้งแต่ปี พ.ศ. 2506 แต่เป็นระบบปิดมีการกำหนดระบบรักษาความปลอดภัย ต่อมาก็มีการปรับเปลี่ยนเป็นระบบเปิดแต่ก็ยังมีระบบการรักษาความปลอดภัยของข้อมูลที่เข้มข้น มีการสอบถามหน่วยงานที่ใช้ข้อมูลทุกๆ 6 เดือน เพื่อตรวจสอบผู้ที่ใช้ ในการดำเนินการโดยเฉพาะด้านทะเบียนยาเสพติด มีการนำเข้ามูลเข้าฐานเอง หน่วยงานที่ประสานงานใกล้ชิด ได้แก่ สำนักงานตรวจคนเข้าเมือง

สำนักงานตำรวจแห่งชาติ และกองทะเบียนประวัติอาชญากร ในการพัฒนาระบบใหม่ๆ ควรต้องมีการสำรวจและดูความต้องการของหน่วยงานและข้อมูลเพื่อสามารถดำเนินการเชื่อมโยงได้อย่างเหมาะสม ตลอดรวมทั้งกรมคุมประพฤติ

สำนักงานป้องกันและปราบปรามยาเสพติดใช้กฎหมายที่เกี่ยวข้องในการปฏิบัติงานสำหรับการแลกเปลี่ยนข้อมูล หรือการเชื่อมโยงข้อมูลจากพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ.2540 ส่วนตัวกฎหมายของปปส.เองไม่ได้มีบทบัญญัติใดที่เอื้ออำนวยต่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรมและไม่ได้ออกระเบียบมาเป็นการเฉพาะสำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานใดๆในกระบวนการยุติธรรม อย่างไรก็ตาม ข้อมูลที่หน่วยงานพิจารณาเห็นว่าเป็นข้อมูลที่เป็นความลับและมีผลต่อการสืบสวน สอบสวน ในคดียาเสพติดก็เป็นดุลพินิจของผู้บังคับบัญชาระดับสูงที่จะอนุญาตหรือไม่อนุญาตให้เปิดเผยหรือให้ข้อมูลเหล่านั้น

11. สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน

เป็นส่วนราชการที่อยู่ในบังคับบัญชาของรัฐมนตรีว่าการกระทรวงยุติธรรม มีอำนาจหน้าที่ดำเนินการให้เป็นไปตามมติของ คณะกรรมการป้องกันและปราบปรามการฟอกเงินและคณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน รวบรวม ติดตาม ตรวจสอบ ศึกษา และวิเคราะห์รายงานและข้อมูลต่าง ๆ เกี่ยวกับการทำธุรกรรม เก็บรวบรวมพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

สำนักงานคณะกรรมการปปง.ได้ประสานความร่วมมือกับกระทรวงเทคโนโลยีและสารสนเทศ ในการช่วยดำเนินการบูรณาการซอฟแวร์ HMC ในการแปลงฐานข้อมูล เนื่องจากข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของสำนักงานปปง.เป็นข้อมูลที่มีผลกระทบและอาจเกิดความเสียหายทั้งต่อบุคคลหรือองค์กรธุรกิจได้

ซึ่งหากมีการออกระเบียบมารองรับก็สามารถเชื่อมโยงข้อมูล ได้โดยอาจจะมีกฎหมาย 2 ฉบับที่สามารถใช้ได้คือ ร่างพรบ. ธุรกรรมอิเลคโทรนิคส์ และร่างพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ ดังนั้น หากมีการเชื่อมโยงข้อมูลกับหน่วยงานในกระบวนการยุติธรรม ก็จะต้องมีกฎหมายหรือระเบียบฯ โดยเฉพาะมารองรับ เพราะที่มีการดำเนินการอยู่ในปัจจุบัน มีเพียงเลขาธิการ ปปง.และผู้ที่ได้รับมอบหมายเท่านั้นที่มีอำนาจในการอนุญาตให้บุคคลอื่นเข้าถึงข้อมูลของปปง.ซึ่งกฎหมายที่กำหนดให้เฉพาะเลขาธิการสำนักงาน

คณะกรรมการปปง.เท่านั้นเป็นผู้มีอำนาจเปิดเผยข้อมูลเป็นบทบัญญัติที่ค่อนข้างเป็นอุปสรรคต่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรม

12. สำนักงานอัยการสูงสุด

เป็นส่วนราชการที่อยู่ในบังคับบัญชาของรัฐมนตรีว่าการกระทรวงยุติธรรม มีอำนาจหน้าที่เกี่ยวกับการดำเนินคดีอาญาทั้งปวง ดำเนินคดีแพ่ง และให้คำปรึกษาด้านกฎหมายแก่รัฐบาลและหน่วยงานของรัฐ และอำนาจหน้าที่ตามที่กำหนดไว้ในกฎหมาย

สำนักงานอัยการสูงสุดได้จัดทำสารบบคดีด้านอิเลคโทรนิคส์ โดยมีการจัดเก็บฐานข้อมูลเป็นของตนเอง และมีการเชื่อมโยงข้อมูลกับสำนักงานศาลยุติธรรม สำนักงานป้องกันและปราบปรามยาเสพติด สำนักงานตำรวจแห่งชาติ (เฉพาะกรณีการฟ้องด้วยวาจา) และสำนักงานผู้ตรวจการแผ่นดินรัฐสภา สำนักงานอัยการสูงสุด มีขอบเขตการจำกัดการเก็บข้อมูลแต่ก็จะเก็บข้อมูลครบถ้วนในกลุ่มที่ดำเนินการในขณะนี้ก็อยู่ในระหว่างการดำเนินการเกี่ยวกับข้อมูลทางคดี

ในด้านกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องนั้นก็ใช้ระเบียบของอัยการสูงสุด (พ.ศ. 2545) เป็นกรอบในการดำเนินการซึ่งโดยทั่วไปเนื้อหาของระเบียบมีลักษณะที่เอื้ออำนวยต่อการที่สามารถนำมาใช้ในการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรม โดยเฉพาะข้อ 19 [28] นอกจากนี้ ในการดำเนินการหากมีการประสานขอข้อมูลมาที่สำนักงานอัยการสูงสุด หากเป็นข้อมูลในสำนวนคดีก็อาจใช้พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ.2540 ควบคู่ไปด้วย ส่วนการจะให้ข้อมูลหรือไม่แก่ฝ่ายใดนั้นก็จะให้เป็นดุลพินิจของผู้บริหารฯ (อธิบดีอัยการฯ)

---

[28] ระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ (ฉบับที่ 7) พ.ศ. 2545 ข้อ 19 (การยืมหรือคัดสำเนา)

การยืม หรือคัดสำเนาการสอบสวนให้ดำเนินการได้ดังต่อไปนี้

1) สำนวนการสอบสวนคดีที่เสร็จเด็ดขาดแล้ว หากพนักงานสอบสวนหรือส่วนราชการที่เกี่ยวข้อง ประสงค์จะขอยืมหรือขอคัดค้านสำเนาสำนวนทั้งหมดหรือบางส่วนไปเพื่อใช้ประโยชน์ในราชการแล้ว ให้หัวหน้าพนักงานอัยการอนุญาตให้ยืมหรือให้คัดสำเนาไปได้

2) สำนวนการสอบสวนคดีที่ยังไม่เสร็จเด็ดขาด หากผู้เกี่ยวข้องประสงค์จะขอยืมหรือคัดสำเนาสำนวนทั้งหมดหรือบางส่วนเพื่อใช้ประโยชน์ในราชการแล้ว ให้หัวหน้าพนักงานอัยการพิจารณา หากเห็นว่าไม่เป็นการขัดข้องหรือเสียหายแก่การดำเนินคดี ให้อนุญาตให้ยืมหรือคัดสำเนาไปได้

13.สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตและประพฤติมิชอบแห่งชาติ(ปปช.)

สำนักงานปปช.นั้น มีกฎหมายที่ให้อำนาจชัดเจน คือ พระราชบัญญัติประกอบรัฐธรรมนูญ ซึ่งในการทำงาน ปปช.สามารถอ้างพระราชบัญญัติประกอบรัฐธรรมนูญดังกล่าว ขอข้อมูลได้ทุกหน่วยงานและทุกประเภทของเอกสาร ซึ่งแม้บางหน่วยงาน เช่น สำนักงานประกันสังคม

ในการเชื่อมโยงข้อมูลจะไม่มีการเชื่อมโยงข้อมูลรายเรื่อง แต่จะเชื่อมโยงตามความจำเป็นเท่านั้น ใช้ระบบการเชื่อมโยงคล้ายกับของกรมสรรพากร มีการจัดทำฐานเก็บติดตั้งระบบอิเลคโทรนิคส์ เพื่อสร้าง Security ผู้ที่ใช้เกี่ยวข้องก็จะมี Card อิเลคโทรนิคส์ เพื่อสร้าง Security ผู้ที่ใช้เกี่ยวข้องก็จะมี Card จึงจะเข้าไปได้ อย่างไรก็ดี การจะขอข้อมูลก็อาจทำได้เป็นรายเรื่อง ปปช.เองก็อยากจะเชื่อมโยงข้อมุลกับหลายๆหน่วยงาน เช่น สำนักทะเบียนราษฎร กรมการขนส่งทางบก เป็นต้น เพราะการเชื่อมโยงก็ช่วยในการปฏิบัติงานของ ปปช. ให้รวดเร็วได้เช่นกัน เช่น กรณีการต้องเดินทางไปสอบสวนหรือตรวจสอบต่างจังหวัด ถ้ามีการเชื่อมโยงสามารถเข้าไปค้นหาได้เร็วยิ่งขึ้น ในหลักการเป็นสิ่งที่ดีเพียงแต่ต้องระมัดระวังเรื่องความปลอดภัยเท่านั้น

14. สำนักงานศาลยุติธรรม

สำนักงานศาลยุติธรรมนั้นในทางปฏิบัติได้มีการยึดถือแนวทางการดำเนินการโดยใช้ประมวลกฎหมายวิธีพิจารณาความแพ่งมาตรา 54 ที่ระบุว่า ผู้ที่จะคัดสำเนาได้จะต้องเป็นคู่ความในคดี หรือพยานเท่านั้น ทำให้เกิดปัญหาว่า การแลกเปลี่ยน การเชื่อมโยง หรือการบูรณาการข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรม จะสามารถทำได้มากน้อยแค่ไหน ในส่วนของสำนักงานศาลยุติธรรมเอง ไม่ได้มีการออกกฎหรือระเบียบภายในของสำนักงานศาลยุติธรรมเป็นการเฉพาะ การดำเนินการโดยทั่วไปก็จะอาศัยพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 เป็นหลักด้วยเช่นกัน อย่างไรก็ตาม ในการขอหรือเชื่อมโยงข้อมูลก็อาจจะประสบปัญหาเช่นกัน เพราะต้องยึดตามหลักกฎหมายที่ว่า การขอข้อมูลงานคดีก็ต้องถือว่า เป็นคู่ความในคดี ดังนั้น หากไม่ใช่ เป็นคู่ความในคดี ก็อาจจะไม่สามารถกระทำได้ ในส่วนนี้จึงอาจจะกระทบต่อการเชื่อมต่อข้อมูล

2.6.2 ปัญหาหลักในการพัฒนาเทคโนโลยีสารสนเทศกระบวนการยุติธรรมของไทย

ในการพัฒนาและนำเอาระบบเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมของไทยยังประสบปัญหาและอุปสรรคต่างๆหลายประการ จากข้อมูลข้างต้นสามารถสรุปปัญหา

หลักๆทั้งที่เป็นจุดอ่อนและข้อจำกัดในการพัฒนาเทคโนโลยีสารสนเทศกระบวนการยุติธรรม อาจจะสรุปได้ 2 ประเด็น คือ ปัญหาด้านพื้นฐานและปัญหาด้านระบบเทคโนโลยีสารสนเทศ[29]

ประเด็นที่ปัญหาที่ 1 : ปัญหาด้านพื้นฐาน

การใช้เทคโนโลยีสารสนเทศของหน่วยงานในกระบวนการยุติธรรม มีปัญหาด้านพื้นฐานหลักๆ ได้แก่

1.1 ขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม ในปัจจุบัน แม้ว่าหน่วยงานในกระบวนการยุติธรรม มีความคิดและความต้องการที่จะแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น แต่ยังไม่มีการกำหนดแนวทางที่ชัดเจนร่วมกันในเรื่องมาตรฐาน ทั้งในด้านวิธีการ เทคโนโลยี และแนวทางการปฏิบัติ การแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นจึงยังไม่เกิดขึ้น

1.2 ขาดหน่วยงานที่เป็นเจ้าภาพในการดำเนินงานบูรณาการข้อมูล แม้ว่าหน่วยงานในกระบวนการยุติธรรม จะเห็นความสำคัญของการนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานให้เกิดประสิทธิภาพ แต่ยังขาดแกนนำหรือเจ้าภาพรับผิดชอบในการดำเนินงานให้เกิดการบูรณาการข้อมูลอย่างเป็นรูปธรรม

1.3 ขาดการสนับสนุนจากผู้บริหารระดับสูง ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ หรือ CIO ไม่เข้าใจความต้องการหรือการสนับสนุนการใช้เทคโนโลยีสารสนเทศในการทำงานให้มีความคล่องตัวสูงขึ้น

1.4 ขาดงบประมาณในการดำเนินงาน ขาดงบประมาณในการจัดซื้ออุปกรณ์ที่เหมาะสม รวมถึงการได้มาซึ่งอุปกรณ์ที่ไม่สามารถทำงานได้ตามที่คาดหวัง

1.5 ขาดความพร้อมด้านอุปกรณ์ บางหน่วยงานยังไม่มีความพร้อมด้านอุปกรณ์ และยังต้องการ การจัดซื้อเพิ่มเติมเพื่อให้สามารถเข้าร่วมแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ในระบบของกระบวนการยุติธรรมได้

1.6 ขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน ปัญหานี้มีอยู่เกือบทุกหน่วยงานในกระบวนการยุติธรรม ทำให้งานที่ทำอยู่ไม่พัฒนาเท่าที่ควร หรือพัฒนาระบบงานออกมาได้ไม่เหมาะสมกับงานที่ทำ จากการสำรวจบุคลากรด้านเทคโนโลยีสารสนเทศของ

---

[29] **แผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1** พ.ศ.2552-2555 หน้า 24-26

หน่วยงานในกระบวนการยุติธรรม จำนวนทั้งสิ้น 117 คน พบว่า บุคลากรส่วนใหญ่มีความสามารถในการใช้งานเฉพาะ Word Processor กับ Microsoft Windows เท่านั้น

1.7 จัดเก็บข้อมูลซ้ำซ้อน แต่ละหน่วยงานต่างจัดเก็บข้อมูลเฉพาะภายในหน่วยงานของตนเองไม่มีการแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆ ที่ต้องการใช้ข้อมูลในลักษณะเดียวกัน การแลกเปลี่ยนข้อมูลต้องทำเป็นหนังสือราชการ ทำให้เกิดความล่าช้า

1.8 ข้อมูลขาดความสมบูรณ์และรวบรวมยาก ข้อมูลบางประเภทยากแก่การรวบรวมและขาดความสมบูรณ์ จึงไม่สามารถให้หน่วยงานอื่นนำไปใช้ได้

1.9 ข้อมูลมีความน่าเชื่อถือได้น้อย ข้อมูลที่ใช้ในหน่วยงานบางประเภทยังไม่สามารถเชื่อถือได้ 100 % ทั้งนี้ จากการยอมรับของหน่วยงานเจ้าของข้อมูลนั้นเอง หน่วยงานจึงไม่ยินยอมให้นำข้อมูลออกเผยแพร่

1.10 ปัญหาจากสิทธิส่วนบุคคล พ.ร.บ.พระราชบัญญัติข้อมูลข่าวสารทางราชการพ.ศ. 2540 เป็นเงื่อนไขสำคัญที่หน่วยงานต่างๆ ไม่สามารถเผยแพร่ข้อมูลได้ เพราะเกรงการถูกฟ้องร้อง

ประเด็นปัญหาที่ 2 : ปัญหาด้านระบบเทคโนโลยีสารสนเทศ

ด้านเทคโนโลยีสารสนเทศของหน่วยงานในกระบวนการยุติธรรม ขณะนี้ยังมี**ปัญหาเชิงระบบ**ที่ต้องแก้ไขและพัฒนาอีกหลายประการ ได้แก่

1.ระบบงานปัจจุบันไม่สามารถรองรับความต้องการของผู้ใช้ในหน่วยงานได้

2.ระบบไม่ได้รับการออกแบบให้รองรับการขอใช้งานจากหน่วยงานภายนอกอื่นๆ

3.ระบบงานมีความหลากหลาย ทำให้การเชื่อมโยงหรือแลกเปลี่ยนข้อมูลไม่สามารถทำได้หรือต้องเสียค่าใช้จ่ายสูง

4.การจัดเก็บ หรือส่งข้อมูลยังทำเป็นระบบเอกสาร ข้อมูลที่มีอยู่ในหลายๆ หน่วยงานต้องมีการขออนุญาต ก่อนส่งออก หรือแม้ว่าจะอยู่ในรูปแบบคอมพิวเตอร์แล้ว ก็ยังไม่สามารถส่งออกได้โดยตรง

5.ขาดมาตรฐานทางเทคโนโลยีในการแลกเปลี่ยนข้อมูล

6.ระบบเครือข่าย : ไม่สามารถรองรับการเชื่อมต่อจากหน่วยงานภายนอก

โดยสรุป ปัญหาและอุปสรรคของการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรมของไทย ได้แก่ การขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม ขาดการดำเนินการอย่างจริงจังและต่อเนื่องประกอบกับการเปลี่ยนแปลงรัฐบาลที่ทำให้การพัฒนากระบวนการยุติธรรมของประเทศดำเนินไปอย่างล่าช้า ซึ่งก็ส่งผลกระทบต่อการใช้เทคโนโลยีสารสนเทศด้วย ในการดำเนินการยังขาดหน่วยงานที่เป็นเจ้าภาพหลักในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการประมวลผล หากมีหน่วยงานที่เป็นเจ้าภาพหลักในการบูรณาการข้อมูลจะช่วยประสานงานให้หน่วยงานของแต่ละหน่วยงานมีข้อมูลที่ถูกต้องเหมาะสม และทันเวลา

ผู้บริหารระดับสูงยังไม่ให้ความสำคัญเท่าที่ควร ในขณะที่ ปัญหาด้านงบประมาณก็มีส่วนสำคัญ ทั้งๆที่รู้และเข้าใจในบทบาทงานด้านเทคโนโลยีสารสนเทศแต่การต้องใช้งบประมาณที่สูง และงานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน เป็นภาระงานที่ยังรอได้ อันส่งผลกระทบต่อเนื่องที่ทำให้ขาดความพร้อมทางด้านอุปกรณ์ต่างๆของทุกหน่วยงานในกระบวนการยุติธรรมมากน้อยแตกต่างกันไป ประกอบกับปัญหารการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน เนื่องจาก การเปลี่ยนแปลงเทคโนโลยีที่รวดเร็ว และบุคลากรที่เก่งจริง ก็ไปอยู่ในภาคเอกชน

ส่วนด้านปัญหาการเก็บรวบรวมข้อมูลที่มีความซับซ้อนนั้น ปัญหานี้มีสาเหตุจากการที่แต่ละหน่วยงานจะจัดเก็บกันเอง โดยมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ต่างฝ่ายต่างจัดเก็บ ก็ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก เพราะยังขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ส่งผลตามมาทำให้ข้อมูลมีความน่าเชื่อถือน้อย เพราะมีข้อมูลจำนวนมากที่ขาดการปรับปรุง เปลี่ยนแปลง ข้อมูลให้เป็นปัจจุบัน จัดเก็บแล้วก็ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน

ด้านการคุ้มครองข้อมูลก็เป็นสิ่งที่จำเป็นเพราะถือว่าข้อมูลของบุคคลที่เป็นความลับส่วนบุคคล เป็นสิ่งที่เป็นผลเสียได้สำหรับบุคคลนั้น การเคารพสิทธิ์ในข้อมูลส่วนบุคคลจึงต้องมีอยู่และให้การคุ้มครอง

ปัญหาหลักอื่นๆก็คือ การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ ซึ่งก็ส่งผลให้หลายๆหน่วยงานจึงขาดความพร้อม เพื่อการบูรณาการ

บทที่ 3
กฎหมาย กฎและระเบียบที่เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

การใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรมจะมีลักษณะพิเศษเฉพาะ เนื่องจากข้อมูลข้อสนเทศต่าง ๆที่อยู่ในองค์กรกระบวนการยุติธรรมต่าง ๆนั้น เป็นข้อมูลที่มีผลกระทบอย่างยิ่งต่อชีวิต ร่างกาย ทรัพย์สิน หากไม่มีการจัดทำระบบและการปกป้องคุ้มครองข้อมูลที่ดีพอรวมไปทั้งยังเป็นข้อมูลที่อาจจะก่อให้เกิดความเสียหายโดยตรงและทางอ้อมแก่ผู้เกี่ยวข้องด้วย การมีมาตรการทางกฎหมายมาให้การคุ้มครองหรือเอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศ จะส่งผลให้การดำเนินการมีประสิทธิภาพ นอกจากนี้ บางประเทศไม่ได้มีกฎหมายออกมาโดยเฉพาะก็พยายามนำกฎหมายที่มีอยู่มาปรับใช้

ประเทศต่าง ๆได้มีมาตรการทางกฎหมายทั้งกฎหมายที่ออกโดยฝ่ายนิติบัญญัติและกฎหมายของฝ่ายบริหารที่เกี่ยวข้องมาปกป้องคุ้มครองในรูปแบบต่าง ๆ ซึ่งเนื้อหาในบทนี้จะได้ทำการทบทวนและประมวลตลอดจนศึกษาวิเคราะห์ ทั้งในส่วนของต่างประเทศและในส่วนของประเทศไทยที่มีอยู่และที่เกี่ยวข้องเพื่อเป็นฟื้นฐานในการทำความเข้าใจและการวิเคราะห์ต่อไป

จากการศึกษากฎหมายและระเบียบต่าง ๆที่เกี่ยวข้องกับการเชื่อมโยงการแลกเปลี่ยนและการบูรณาการข้อมูลด้านกระบวนการยุติธรรมทั้งจากของไทยและของต่างประเทศ สามารถจำแนกกฎหมายและระเบียบต่างเหล่านั้น ออกได้เป็น 4 กลุ่มใหญ่ คือ

1.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

2.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

3.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

4.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

3.1.1 หลักและแนวคิดทางกฎหมาย

(1) กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

กฎหมายที่เกี่ยวข้องกับการเชื่อมโยง การแลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมมีรากฐานแนวคิดมาจากการที่หน่วยงานที่ทำหน้าที่บังคับใช้กฎหมาย

(Law Enforcement Agency) มีความจำเป็นที่จะต้องประสานการใช้ข้อมูลร่วมกันเพื่อให้การปฏิบัติงานบรรลุเป้าหมายโดยเร็วขึ้นทั้งที่ข้อมูลบางประเภทที่หน่วยงานเก็บรักษาเป็นข้อมูลที่เป็นความลับเกี่ยวข้องกับตัวบุคคลซึ่งองค์กรที่ดูแลรักษาข้อมูลต้องเก็บรักษาและมีความรับผิดชอบหากมีการนำมาใช้และก่อให้เกิดความเสียหายแก่ผู้ใดผู้หนึ่ง มาตรการทางกฎหมายจึงเป็นบทบัญญัติที่จำเป็นจะต้องออกมารองรับเพื่อให้หน่วยงานต่างๆสามารถที่จะเชื่อมโยงข้อมูลที่ตนเองมีอยู่และเก็บรักษามาปฏิบัติงานร่วมกับองค์กรหรือหน่วยงานอื่นๆ นอกจากนี้ข้อมูลข่าวสารในปัจจุบันได้ถูกเก็บรักษาไว้ในฐานข้อมูลและเป็นข้อมูลในทางอิเล็กทรอนิคส์ซึ่งจำเป็นต้องมีกฎหมายมารองรับและระบุความถูกต้องทั้งในการเข้าถึงข้อมูลและการใช้ข้อมูลตลอดจนการเก็บรักษาความลับ การเข้าถึงข้อมูล การรักษาความปลอดภัย ประเภทของข้อมูลและระยะเวลาในการจัดเก็บ

เนื่องจากความก้าวหน้าทางเทคโนโลยีมีการเปลี่ยนแปลงรวดเร็วมาก และในการดำเนินการใดๆที่เกี่ยวข้องมีความจำเป็นที่จะต้องอาศัยบุคคลที่มีความรู้ความเชี่ยวชาญเฉพาะทาง ดังนั้น ในการดำเนินการที่เกี่ยวข้องกับมาตรการทางกฎหมาย ประเทศที่ใช้ประมวลกฎหมาย (Civil Law) จึงมักจะใช้การออกกฎหมายเฉพาะในเชิงการบริหารจัดการในรูปของพระราชบัญญัติ (act) ออกมาใช้ โดยมีการตั้งคณะกรรมการเฉพาะกิจ (ad hoc Committee) หรือ อาจจะมีการตั้งเป็นคณะทำงาน (task force) ที่ประกอบด้วยตัวแทนจากหน่วยงานบังคับกฎหมายที่เกี่ยวข้องมาดำเนินการร่วมกัน[30] รวมทั้งบางประเทศก็ใช้ทั้งการตั้งคณะกรรมการเฉพาะกิจมาทำหน้าที่คณะกรรมการในเชิงนโยบายและเชิงการบริหาร แต่ก็มีการตั้งคณะทำงานให้มาเป็นอนุกรรมการ ซึ่งการดำเนินการในลักษณะนี้มีความเหมาะสมกับการเปลี่ยนแปลงทางเทคโนโลยี และการกำหนดแนวทางการปฏิบัติในเชิงเทคนิคแก่หน่วยงานตลอดรวมทั้งการแก้ปัญหาต่างๆที่เกิดขึ้น ได้รวดเร็วและมีประสิทธิภาพ

ในขณะที่การดำเนินการในกลุ่มประเทศ Common Law จะมีแนวทางที่แตกต่างออกไป คือ จะเป็นการพิจารณาออกกฎหมายรับรองการดำเนินการขององค์กร โดยจะออกกฎหมายของรัฐบาลกลางและเชิงประสานบังคับให้หน่วยงานในระดับท้องถิ่นประสานให้ความร่วมมือในการประสานการปฏิบัติการ เช่น กรณีของเรื่องการก่อการร้าย (Terrorism) ก็จะมีการออกกฎหมาย The Patriot Act ขึ้นมา เพื่อให้หน่วยงานด้านความมั่นคง FBI หรือหน่วยงานรัฐสภา คณะกรรมการเฉพาะกิจ สามารถประสานข้อมูลเพื่อการปฏิบัติการโดยเฉพาะ ใน

---

[30] Cresswell, A.M. and Connelly D. **Reconnaissance study. Developing a business case for the integration of criminal justice information** p.99

ขณะเดียวกันก็ใช้แนวการวินิจฉัย หรือ คำตัดสินของศาลมาใช้เป็นแนวปฏิบัติ เช่น ในคดี Katz v. US. 389. US. 347 (1967) เป็นกรณีที่ยึดเอาการตีความของรัฐธรรมนูญ ฉบับแก้ไขครั้งที่ 4 (The Fourth Amendment) ที่ระบุว่า จะให้การคุ้มครองกับการตรวจค้น จับกุมที่ปราศจากเหตุอันควร (unreasonable searches and seizures)[31] เป็นต้น

การที่ประเทศ Common Law อย่างเช่น สหรัฐอเมริกา หรืออังกฤษ พิจารณาเห็นว่า ในการป้องกันและปราบปรามอาชญากรรมนั้น บางครั้งข้อมูลที่เชื่อมโยง หรือแลกเปลี่ยนในกระบวนการยุติธรรมเท่านั้นหาเพียงพอไม่ จำเป็นจะต้องมีการได้รับข้อมูลจากองค์กรภายนอกกระบวนการยุติธรรมที่เป็นองค์กรหรือหน่วยงานเอกชน ซึ่งสามารถให้ข้อมูลได้ เช่น บริษัทโทรศัพท์เอกชน หรือ บริษัทที่ให้บริการสื่อสารด้าน internet หน่วยงานของรัฐสามารถใช้กฎหมาย The Communications Assistance for Law Enforcement Act (CALEA 1994) โดยการขอศาลให้ออกทั้งการดักฟังโทรศัพท์ การตรวจสอบการสื่อสารทางอิเลคโทรนิกส์ ในกรณีที่มีเหตุอันควร (probable case) ที่จะเชื่อได้ว่ามีการประกอบอาชญากรรม[32] ในขณะที่ในการดำเนินการก็จะมีการแจ้งในที่ประชุม เช่น ที่ประชุมผู้ว่าการรัฐเกี่ยวกับการบูรณาการและการขอความร่วมมือในการให้ข้อมูลเกี่ยวกับงานยุติธรรม ของ The Nationa Governers' Association Center for Best Practice : Developing an Implementing Plan for Justice Information System Integration , ณ กรุง Washington D.C. (May 2001) เป็นต้น

ดังนั้น การเชื่อมโยง การแลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมจำเป็นต้องมีการออกกฎหมายที่เอื้อต่อการเชื่อมโยงข้อมูลเพื่อให้ผู้ที่ปฏิบัติงานเกิดความรู้สึกมั่นใจในการปฏิบัติงานและจะเป็นผลที่ดีต่อการทำงานร่วมกันจากหน่วยบังคับใช้กฎหมายที่จะประสานการทำงานให้มีประสิทธิภาพ เกิดทัศนคติที่ดีต่อการยอมแลกเปลี่ยนข้อมูลที่ตนเองมีอยู่รวมทั้งการตรวจสอบกฎ ระเบียบที่เป็นปัญหาและอุปสรรคต่อการเชื่อมโยงด้วย

(2) กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Information)หมายถึง ข้อความใดๆที่เกี่ยวกับบุคคลธรรมดาอันระบุตัว หรืออาจจะระบุตัวบุคคลนั้นได้ การที่จะถือว่าข้อมูลข่าวสารใดเป็น

---

[31] Hennepin County Criminal Justice System Information Integration Project.p.24

[32] Dawes, S. *Interagency Information Sharing: Expected Benefits, Manageable Risks*. **Journal of Policy Analysis and Management** p. 379.

ข้อมูลข่าวสารส่วนบุคคลนั้นตามหลักกฎหมายที่ได้รับการยอมรับนานาประเทศว่าจะสามารถคุ้มครองสิทธิส่วนบุคคลได้มากกว่านั้นจะประกอบด้วยองค์ประกอบ 2 ประการสำคัญ คือ[33]

1) ข้อมูลนั้นจะต้องเป็นข้อมูลข่าวสารที่เกี่ยวข้องกับตัวสิ่งเฉพาะตัวบุคคล คือ ข้อมูลข่าวสารที่เป็นเรื่องเฉพาะตัวของบุคคลและมีผลเฉพาะตัวไม่เกี่ยวข้องกับบุคคลภายนอก

1.1 คุณสมบัติติดตัวของบุคคล ซึ่งอาจเป็นคุณสมบัติที่ติดตัวบุคคลไปตลอดชีวิตหรือลักษณะทางพันธุกรรมของบุคคล เช่น เชื้อชาติ กลุ่มเลือด สีผิว สีตา ลายพิมพ์นิ้วมือ ความพิการของร่างกายที่มีมากตั้งแต่เกิด อันมีลักษณะติดตัวไปจนวันตาย หรือเป็นสิ่งเฉพาะตัวของบุคคลที่เป็นคุณสมบัติที่สามารถเปลี่ยนแปลงได้ตามกาลเวลา เช่น น้ำหนัก อายุ ส่วนสูง วุฒิการศึกษา ความสามารถ เป็นต้น

1.2 การประเมินคุณค่าในตัวบุคคล เช่น ทัศนคติการประเมินความประพฤติและความเห็นเกี่ยวกับกับการกระทำต่างๆของบุคคล เนื่องจากข้อมูลข่าวสารเหล่านี้เป็นสื่อให้เห็นถึงความ คิด ความสามารถ และการแสดงออกถึงความมีตัวตนของบุคคลได้

1.3 แนวความคิด ความเชื่อ พฤติกรรมซึ่งอาจเปลี่ยนแปลงไปตามวัยและวันเวลา เช่น ความสนใจทางการเมืองความสนใจทางเพศ ความรักหรือความชอบความสามารถ

2) ข้อมูลนั้นจะต้องเป็นข้อมูลข่าวสารที่สามารถพิสูจน์ตัวบุคคลได้ กล่าวคือ สิ่งที่บอก ลักษณะ ที่ทำให้รู้จักบุคคลจากข้อมูลข่าวสารนั้นได้ หรือเรียกได้ว่าเป็นข้อมูลที่บอกถึงความเป็นตัวตนของบุคคล ได้แก่

1.1 เครื่องหมายบ่งชี้ตัวบุคคล เช่นชื่อ นามสกุล ฉายาหรือนามแฝงหรือเลขรหัส

1.2 ลักษณะทางกายภาพของบุคลภายนอก เช่นความสูงต่ำ ดำขาว ความสมบรูณ์ หรือความพิการทางกายภาพ

1.3 ข้อเท็จจริงต่างๆที่สามารถแสดงได้ว่าเป็นบุคคลหรือข้อเท็จจริงที่เกี่ยวข้องกับบุคคล เช่นยศ ตำแหน่ง หน้าที่การงานซึ่งเป็นสถานะที่ต้องแสดงออกได้ชัดว่าหมายถึง ผู้ที่ดำรงตำแหน่ง ดังกล่าวในขณะนั้น

1.4 ข้อมูลที่เป็นลักษณะเป็นการประเมินคุณค่าของบุคคล ทัศนคติต่อบุคคล การประพฤติปฏิบัติและการกระทำต่างๆของบุคคล ซึ่งข้อมูลข่าวสารเหล่านี้เป็นสิ่งที่สื่อให้เห็นถึงความคิดของบุคคลสามารถแสดงออกถึงความมีตัวตนของบุคคลได้ทั้งสิ้น

---

[33] Chance, Clifford. **Data Protection.** P.18

จากองค์ประกอบของข้อมูลข่าวสารส่วนบุคคลดังกล่าว เมื่อพิจารณาต่อมาถึงการแบ่งประเภทของข้อมูลส่วนบุคคลที่มีอยู่หลายรูปแบบ และหลายลักษณะนั้นก็มีความพยายามในการจัดแบ่งประเภทของข้อมูลให้ชัดเจนยิ่งขึ้น ซึ่งกล่าวโดยกว้างๆ ได้ว่าการแบ่งประเภทของข้อมูลข่าวสารส่วนบุคคลนั้นหลักการทั่วไปที่ได้รับการยอมรับจะขึ้นอยู่กับประเมินประเภทของข้อมูลในประเด็นความอ่อนไหว ที่จะส่งผลกระทบต่อเจ้าของข้อมูลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้น โดยสามารถแบ่งได้ออกเป็น 3 ระดับ ดังนี้

1.ข้อมูลที่มีความอ่อนไหวระดับสูง (High sensitivity –HS) ข้อมูลประเภทนี้ได้แก่ข้อมูลรายละเอียดส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศหรือข้อเท็จจริงด้านอื่นๆในชีวิตของบุคคลซึ่งสามารถ กล่าวได้ว่าเป็นเรื่องส่วนตัว หรือลับเฉพาะซึ่งเป็นข้อมูลที่ไม่ควรเปิดเผย

2. ข้อมูลที่มีความอ่อนไหวระดับกลาง (Moderate sensitivity-Ms)นี่เป็นข้อมูลที่ความอ่อนไหวมากในแง่ที่ว่าโอกาสที่จะก่อให้เกิดความเสียหายเมื่อข้อมูลถูกนำไปใช้ในทางที่ผิดอยู่ในระดับสูง ข้อมูลประเภทนี้ครอบคลุมข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล ซึ่งมีความครอบคลุมทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางนี้ ก็เช่นเดียวกับข้อมูลที่มีความอ่อนไหวระดับสูง คือไมควรถูกเก็บรวบรวมโดยสิ้นเชิง

3. ข้อมูลที่มีความอ่อนไหวระดับต่ำ (Low sensitivity-Ls) ข้อมูลประเภทนี้เป็นข้อมูลที่เกี่ยวข้องกับบุคคล เป็นข้อมูลที่มีความอ่อนไหวเนื่องด้วยข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น ดั้งนั้นข้อมูลเกี่ยวกับนายจ้างคนเก่าช่วยปูทางให้เข้าถึงข้อมูลที่มีความอ่อนไหวระดับสูงยิ่งขึ้นไป

ในต่างประเทศจึงได้มีการออกกฎหมายไว้เพื่อคุ้มครองข้อมูลและสิทธิส่วนบุคคลนั้นเรียกว่า Data Protection Act และ Privacy Act [34]โดยจะคุ้มครองตั้งแต่ข้อมูลทั่วไปของบุคคลนั้น ได้แก่ ชื่อ นามสกุล ที่อยู่ ระดับการศึกษา อาชีพ เป็นต้น จนถึงข้อมูลที่เป็นความลับ เช่น ประวัติทางการแพทย์ ประวัติทางวินัย ประวัติทางอาชญากรรม เป็นต้น การนำเอาระบบเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมเป็นสิ่งที่ดีและมีความเหมาะสมแต่ก็ควรต้องมีการออกกฎหมายมาคุ้มครองระบบฐานข้อมูลเหล่านั้นให้มีความเหมาะสมต่อไปด้วย

---

[34] ปทีป เมธาคุณวุฒิ, อ้างแล้ว หน้า 2

ในกลุ่มสหภาพยุโรปมีแนวทางการคุ้มครองตาม(The EU Directive 95/46/EC) เกิดขึ้นโดยคณะกรรมาธิการ(European Commission)แห่งประชาคมเศรษฐกิจยุโรป (European Economic Community) ที่ได้มีข้อเสนอแนะ (Recommendation) เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับอนุสัญญาของคณะมนตรีแห่งยุโรป(Commission Recommendation : Relating to the Council of Europe Convention for the Protection of individuals with regard to Automatic Processing of Personal Data) เพื่อประกันสิทธิขั้นพื้นฐานของประชาชน ดังนั้นสหภาพยุโรป จึงได้กำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เทียบเท่ากันในยุโรป โดยใช้อนุสัญญาของคณะมนตรีแห่งยุโรปเป็นแนวทางในการยกร่างกฎหมาย ทั้งนี้ เพื่อให้กฎหมายอยู่ในลักษณะเป็นเอกภาพทั่วทั้งยุโรป (for the purpose of creation a uniform level of data protection in Europe) ข้อตกลงนี้กำหนดให้ประเทศสมาชิกต้องบัญญัติกฎหมายภายในให้เป็นไปตาม Detective ภายในสามปีนับแต่ Directive 95/46/EC ได้แก้ไขปรับปรุงแล้วเสร็จ ดังนั้น เมื่อ Directive 95/46/EC แก้ไขปรับปรุงแล้วเสร็จเมื่อวันที่ 24 ตุลาคม ค.ศ. 1995 ประเทศสมาชิกจึงต้องออกกฎหมายภายในให้แล้วเสร็จภายในวันที่ 24 ตุลาคม ค.ศ. 1998

ขอบเขตของ Directive ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งการประมวลผลโดยอัตโนมัติและการประมวลผลด้วยวิธีการ Manual สำหรับการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการ Manual นั้น ข้อมูลส่วนบุคคลที่ถูกประมวลผลด้วยวิธีนี้ต้องเป็นส่วนหนึ่งหรือมีเจตนาที่จะให้เป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล (Filling System เช่น ระบบการจัดเก็บข้อมูลประวัติคนไข้ของโรงพยาบาลต่างๆ) อย่างไรก็ตาม กฎหมายไม่ใช้บังคับกับการประมวลผลข้อมูลโดยบุคคลธรรมดาในกรณีของ A purely personal or household activity ทั้งนี้สาระสำคัญของสหภาพยุโรปนี้มีดังต่อไปนี้[35]

ก. ข้อมูลที่กฎหมายคุ้มครอง คือ ข้อมูลส่วนบุคคล (Personal Data) ซึ่งหมายความว่า ข้อเท็จจริงหรือรายละเอียดใดๆ ที่เกี่ยวกับบุคคลธรรมดา (Natural Person) ที่ถูกระบุตัวหรือสามารถถูกระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมบุคคลที่ถูกระบุตัวหรือสามารถถูกระบุตัวจากข้อมูลดังกล่าว ตามกฎหมายนี้เรียก Data Subject กรณีของบุคคลที่ถูกระบุตัว (Identified person) จะเป็นกรณีที่ระบุตัวบุคคลดังกล่าวได้จากชื่อของบุคคลนั้น ส่วนกรณีของบุคคลที่สามารถถูกระบุตัว (Identified person) เป็นกรณีที่สามารถระบุตัวบุคคลดังกล่าวได้จากข้อมูลใดโดยใช้วิธีการที่สมเหตุสมผล (Reasonable) โดยเฉพาะจากข้อมูลดังต่อไปนี้ เลขบัตรประจำตัวประชาชนซึ่งถือเป็นกรณีระบุโดยตรง ส่วนการระบุโดยอ้อมก็เช่น การระบุตัวบุคคล

---

35 Chance, Clifford. Ibid p.42

โดยอาศัยข้อมูลเกี่ยวกับลักษณะเฉพาะ ถือเป็นกรณีระบุโดยตรง ส่วนการระบุโดยอ้อมก็เช่น การระบุตัวบุคคลโดยอาศัยข้อมูลเกี่ยวกับลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสังคม เป็นต้น

ข. การดำเนินการที่กฎหมายควบคุม คือ การประมวลผลข้อมูล (Processing) ซึ่งหมายความว่า การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีการอัตโนมัติหรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึกการจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การค้นคืน consultation การใช้ การเปิดเผยโดยการส่งผ่าน การเผยแพร่ (dissemination) หรือโดยวิธีการอื่นๆ ที่ทำให้เข้าถึงข้อมูลได้ การจัดกลุ่มหรือการรวมข้อมูล การขัดขวาง การลบ หรือการทำลายข้อมูล

เมื่อพิจารณาจากคำนิยามคำว่า “ข้อมูลส่วนบุคคล” ซึ่งเป็นสิ่งที่กฎหมายประสงค์จะคุ้มครอง จะเห็นว่ากฎหมายมุ่งประสงค์จะคุ้มครองเฉพาะข้อมูลส่วนบุคคลของบุคคลธรรมดาเท่านั้น ดังนั้น นิติบุคคลจึงมิได้รับความคุ้มครองตามกฎหมายนี้ บุคคลที่ถูกควบคุมคือ ผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผลข้อมูล (Processor) ซึ่งผู้ควบคุมข้อมูลหมายความว่าบุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่ของรัฐ หน่วยงานหรือองค์กรอื่นใด โดยโดยลำพังหรือร่วมกับผู้อื่นกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือกฎเกณฑ์ของรัฐสมาชิกหรือของสหภาพยุโรป ผู้ควบคุมข้อมูลหรือวิธีการแต่งตั้งหรือเลือกตั้งเป็นผู้ควบคุมข้อมูลอาจถูกกำหนดโดยกฎหมายภายในของรัฐสมาชิก หรือกฎหมายของสหภาพยุโรป

ส่วนผู้ประมวลผลข้อมูล หมายความว่า บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่ของรัฐ หน่วยงานหรือองค์กรอื่นใดซึ่งประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล แต่ทั้งนี้ก็มีข้อยกเว้นทั่วไปในการควบคุม 2 กรณี คือ

(1) การประมวลผลในกิจกรรมที่อยู่นอกขอบเขตของ Community Law เช่น กิจกรรมเกี่ยวกับนโยบายต่างประเทศและความมั่นคง หรือการประมวลผลในกิจกรรมของรัฐที่เกี่ยวกับกฎหมายอาญา เป็นต้น

(2) การประมวลผลโดยบุคคลธรรมดาเพื่อกิจกรรมส่วนตัว (Purely Personal and Household Activity)

ค.หน้าที่ของบุคคลที่ถูกควบคุม Directive กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งแก่ Supervisory Authority ก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติ โดยในการแจ้งนั้นต้องประกอบด้วยรายการข้อมูลดังนี้

(1) ชื่อที่อยู่ของผู้ควบคุมข้อมูลและผู้แทน (ถ้ามี)

(2) วัตถุประสงค์ของการประมวลผล

(3) ประเภทของข้อมูลที่เก็บ

(4) ผู้รับข้อมูล

(5) วัตถุประสงค์ของการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

(6) ข้อมูลเบื้องต้นเกี่ยวกับมาตรการที่ใช้เพื่อรักษาความปลอดภัยในการประมวลผลข้อมูล

ทั้งนี้ก่อนการประมวลผลข้อมูล Directive กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้วยกฎหมาย ซึ่งการประมวลผลเช่นใดถึงจะเรียกว่าชอบด้วยกฎหมายนั้น Directive ได้กำหนดไว้ 7 กรณี[36] ดังนี้

(1) ได้รับความยินยอมจากเจ้าของข้อมูล (Unambiguous Consent of Data Subject)

(2) เป็นกรณีจำเป็นเพื่อปฏิบัติตามสัญญาหรือเป็นการดำเนินการก่อนเข้าทำสัญญา

(3) ตามที่กฎหมายกำหนด

(4) เพื่อรักษาชีวิตของเจ้าของข้อมูล (Vital Interest)

(5) เพื่อปฏิบัติภารกิจที่ผลประโยชน์ของสาธารณะหรือจำเป็นต่อการปฏิบัติหน้าที่ของเจ้าพนักงาน

(6) เพื่อประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลที่สาม และการประมวลผลดังกล่าวไม่เป็นการกระทบกระเทือนต่อประโยชน์ของการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลโดยเฉพาะสิทธิในความเป็นส่วนตัว

ง.หลักการทั่วไปเกี่ยวกับการประมวลผลข้อมูล Directive กำหนดว่าประเทศสมาชิกต้องปฏิบัติต่อไปนี้ในการดำเนินการต่อข้อมูลส่วนบุคคล อันได้แก่

(1) ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย

(2) ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (specified, explicit and legitimate purposes) นอกจากนี้จะต้องไม่มี

---

[36] สุธรรม อยู่ในธรรมและคณะ **แนวทางการพัฒนากฎหมายแลกเปลี่ยนข้อมูลด้วยสื่ออิเล็กทรอนิกส์ในประเทศไทย.** หน้า 56

การประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่การประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์

(3) ข้อมูลส่วนบุคคลต้องมีความเพียงพอ (adequate) ไม่มากเกินจำเป็น (not excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น

(4) ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และกรณีจำเป็นต้องเป็นปัจจุบันด้วย

(5) ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลไว้นานเกินไป อีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

นอกจากนี้ตามข้อตามข้อตกลงได้กำหนดให้มีข้อมูลชนิดพิเศษ (Sensitive Data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลจาก

(1) การทำลายข้อมูลโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย

(2) การสูญเสียข้อมูลโดยอุบัติเหตุ

(3) การแก้ไขเปลี่ยนแปลงโดยอุบัติเหตุ

(4) การเปิดเผยหรือการเข้าถึงโดยปราศจากอำนาจ และ

(5) ป้องกันการประมวลผลที่มิชอบด้วยกฎหมายทุกรูปแบบ

การพิจารณาถึงความเหมาะสมที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลนั้นต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นจากการประมวลผล และลักษณะของข้อมูลที่ทำการประมวลผล

โดยสรุปข้อกำหนดของ EU ได้กำหนดให้รัฐสมาชิกอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักทั่วไป ดังนี้

(1) ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

(2) การประมวลผลจะทำได้เท่าที่จำเป็นในการทำนิติกรรมสัญญาใดๆ ของผู้เป็นเจ้าของข้อมูลเท่านั้น

(3) การประมวลผลจะต้องอยู่ภายใต้กรอบของกฎหมาย

(4) การประมวลผลจะต้องกระทำเพื่อปกป้องผลประโยชน์สำคัญของผู้เป็นเจ้าของข้อมูล

(5) การประมวลผลจำเป็นที่จะต้องกระทำเพื่อผลประโยชน์ของสาธารณะ หรือในการดำเนินงานของหน่วยงานของรัฐที่ได้รับมอบหมายให้เป็นผู้ควบคุมข้อมูลหรือเปิดเผยข้อมูลต่อบุคคลที่สาม

(6) การประมวลผลที่จำเป็นและอยู่ภายใต้กรอบของกฎหมายจะต้องไม่กระทบต่อผลประโยชน์ หรือสิทธิขั้นพื้นฐานของผู้เป็นเจ้าของข้อมูล

ทั้งนี้ตามข้อกำหนดของสหภาพยุโรปยังได้ให้ความสำคัญเกี่ยวกับความลับและความมั่นคง รวมถึงข้อยกเว้นในการเปิดเผยข้อมูลกรณีที่มิได้นำข้อมูลไปใช้ประโยชน์สาธารณะแต่นำไปใช้เพื่อประโยชน์ส่วนตัว และกำหนดเกี่ยวกับเรื่องความเสียหายที่เกิดขึ้นต่อ ผู้เป็นเจ้าของข้อมูล เมื่อมีการประมวลผลโดยไม่ชอบด้วยกฎหมายและการเปิดเผยข้อมูลจะต้องไม่ละเมิดต่อความมั่นคงของรัฐ

จ. การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ Directive ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลเพื่อประมวลผลหรือเจตนาที่จะประมวลผลไปยังประเทศที่มิได้เป็นสมาชิกสหภาพยุโรป เว้นแต่ ประเทศที่รับข้อมูลจะได้ให้ความคุ้มครองข้อมูลส่วนบุคคลใน “ระดับที่เพียงพอ (Adequate Level)” อย่างไรก็ตาม Directive ก็กำหนดข้อยกเว้นไว้ เช่น ได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล หรือการส่งหรือโอนข้อมูลส่วนบุคคลจำเป็นเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลและผู้ควบคุมข้อมูลเป็นคู่กรณีต่อกันหรือเพื่อปฏิบัติการให้เป็นไปตามข้อตกลงก่อนเข้าทำสัญญาตามคำร้องขอของเจ้าของข้อมูล

ฉ.สิทธิของเจ้าของข้อมูล Directive ได้กำหนดสิทธิของเจ้าของข้อมูลที่สำคัญๆ ไว้ดังนี้

(1) สิทธิได้รับแจ้งข้อมูลตามที่กฎหมายกำหนดเมื่อถูกเก็บรวบรวมข้อมูล

(2) สิทธิเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตน

(3) สิทธิแก้ไขข้อมูลส่วนบุคคลที่เกี่ยวกับตนให้ถูกต้อง

ช.องค์กรที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย Directive วางแนวทางให้ประเทศสมาชิกสหภาพยุโรป (European Union) กำหนดให้มีองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความเป็นอิสระไว้ในกฎหมายคุ้มครองของแต่ละประเทศ ซึ่งประเทศสมาชิกส่วนใหญ่ก็จะกำหนดไว้ในรูปของ Commissioner ซึ่ง Directive กำหนดให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอย่างน้อยต้องกำหนดอำนาจหน้าที่ดังต่อไปนี้ให้กับบุคคลหรือองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมาย คือ

(1) อำนาจในการสืบสวน เช่น อำนาจในการเข้าถึงและเก็บรวบรวมข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ของผู้ควบคุมดูแล

(2) อำนาจในการแทรกแซง เช่น อำนาจในการออกคำสั่งขัดขวาง ลบหรือทำลายข้อมูล หรือ การห้ามการประมวลผลข้อมูลชั่วคราว

(3) รับคำร้องทุกข์เกี่ยวกับการดำเนินการที่เป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลและวินิจฉัยคำร้องทุกข์ดังกล่าว

(4) จัดทำรายงานการปฏิบัติงานและเผยแพร่รายงานดังกล่าวต่อสาธารณะ

(5) ผู้ควบคุมดูแลและเจ้าหน้าที่ของผู้ควบคุมดูแลต้องรักษาความลับของข้อมูลที่มี Confidential ซึ่งตนได้เข้าถึงเนื่องจากการปฏิบัติหน้าที่

นอกจากข้อตกลงของสหภาพยุโรปแล้ว กลุ่มประเทศทวีปยุโรปได้มีแนวทางอีกข้อหนึ่งของการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามข้อตกลงของรัฐสภายุโรป ซึ่ง ข้อตกลงดังกล่าว (Convention of Council of Europe) ได้ประกาศใช้เมื่อปี ค.ศ. 1984 มีบทบัญญัติถึงการคุ้มครองสิทธิความเป็นส่วนตัว และการคุ้มครองข้อมูลข่าวสารส่วนบุคคล การประมวลผลโดยวิธีอัตโนมัติและการเปิดเสรีของการไหลเวียนข้อมูลระหว่างประเทศ โดยมีหลักการสำคัญๆ ได้แก่

1) หลักการเก็บรวบรวมข้อมูล การประมวลผลข้อมูลต้องดำเนินการโดยถูกต้อง และการเปิดเผยต้องทำด้วยเจตนาที่สุจริต

2) หลักการกำหนดระยะเวลาในการใช้ข้อมูล เมื่อสิ้นสุดความจำเป็นในการใช้ข้อมูลต้องยกเลิกการจัดเก็บทันที

3) หลักการจัดเก็บและการประมวลผลต้องทำภายใต้วัตถุประสงค์ และเพียงเท่าที่จำเป็น

4) หลักความถูกต้องของข้อมูลข่าวสาร ต้องมีคุณภาพ และมีการปรับปรุงให้ทันสมัยอยู่เสมอ

5) หลักการรักษาความปลอดภัยของข้อมูลข่าวสาร มาตรการการคุ้มครองข้อมูลข่าวสารตามกฎหมายและให้ความคุ้มครองในทางเทคนิค

ภายใต้ข้อตกลงของรัฐสภายุโรปนี้ เพื่อควบคุมการคุ้มครองให้เป็นไปตามกฎหมาย จึงได้มีการกำหนดให้มีองค์กรที่ชื่อ The Council of European's Committee ทำหน้าที่คอยดูแลการละเมิดสิทธิส่วนบุคคลอันเกิดจากการละเมิดข้อมูลข่าวสารส่วนบุคคลด้วย

สหประชาชาติได้วางแนวทางในการประมวลผลแฟ้มข้อมูลส่วนบุคคลทางคอมพิวเตอร์ของสหประชาชาติขึ้นมา แนวทางนี้ได้รับการจัดทำขึ้นเมื่อวันที่ 14 ธันวาคม 1990 โดยสมัชชาใหญ่แห่งสหประชาชาติได้มีมติกำหนดแนวทางในการประมวลผลแฟ้มข้อมูลส่วนบุคคลทางคอมพิวเตอร์ (Guidelines Concerning Computerized Personal Data Files) ขึ้น เพื่อให้ประเทศสมาชิกปฏิบัติหลักเกณฑ์ในการกำหนดมาตรฐานขั้นต่ำเกี่ยวกับบัญญัติกฎหมายภายในของรัฐดังต่อไปนี้

(1) หลักเกี่ยวกับความชอบธรรมในการประมวลผลข้อมูล(Principle of Lawfulness and Fairness) ข้อมูลที่ได้รับการประมวลผลจะต้องได้มาโดยชอบธรรม และชอบด้วยกฎหมาย ทั้งนี้ โดยไม่ขัดหรือแย้งกับกฎบัตรสหประชาชาติ (Charter of the United Nations)

(2) หลักความถูกต้อง (Principle of Accuracy) บุคคลที่มีหน้าที่รับผิดชอบในการเก็บรักษาข้อมูลจะต้องทำการตรวจสอบข้อมูลตลอดเวลาเพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บนั้นถูกต้อง เพื่อมิให้เกิดความผิดพลาด

(3) หลักในการกำหนดวัตถุประสงค์พิเศษในการจัดเก็บข้อมูล (Principle of the Purpose-specification)

ก.ข้อมูลส่วนบุคคลต้องจัดเก็บและรวบรวมอย่างพอเพียง ตามวัตถุประสงค์ที่กำหนดไว้เป็นพิเศษ

ข.ห้ามมิให้มีการใช้ข้อมูลหรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

ค.ระยะเวลาในการจัดเก็บจะต้องไม่เกินไปกว่าวัตถุประสงค์ที่กำหนดไว้เป็นพิเศษ

(4) หลักในการเข้าถึงข้อมูลส่วนบุคคล (Principle of Interested-person Access) บุคคลมีสิทธิที่จะเข้าถึงข้อมูลของตนเองโดยการแสดงหลักฐานสำคัญเพื่อแสดงว่าตนเป็นใคร

(5) หลักในการไม่เลือกปฏิบัติ (Principle of Non-discrimination)ในการจัดทำข้อยกเว้น จะต้องไม่มีการเลือกปฏิบัติไม่ว่าบุคคลนั้นจะมีสัญชาติ เชื้อชาติ ศาสนา เพศ ความเห็นทางการเมือง ความคิด ความเชื่อ หรือความเป็นสมาชิกภาพ สถาบัน หรือสมาชิกภาพองค์กร แตกต่างกันก็ตาม

(6) การกำหนดข้อยกเว้น (Power to make exceptions)ข้อห้ามในการเปิดเผยข้อมูล จะไม่นำไปบังคับใช้หากกระทบต่อความมั่นคงของรัฐความสงบเรียบร้อยของประชาชน การสาธารณสุข หรือศีลธรรม รวมทั้งเสรีภาพของบุคคลอื่น

(7) หลักความปลอดภัย (Principle of Security) จะต้องมีการนำมาตรการที่เหมาะสมมาใช้เพื่อป้องกันแฟ้มข้อมูลส่วนบุคคล ทั้งจากเหตุอันอาจเกิดขึ้นตามธรรมชาติ ความเสียหายอันเกิดจากการกระทำของมนุษย์ เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การนำข้อมูลไปใช้โดยไม่ชอบหรือการใส่โปรแกรมไวรัสเข้าไปในระบบคอมพิวเตอร์เพื่อทำลายล้างข้อมูล

(8) หลักการตรวจสอบและบทลงโทษ (Supervision and Sanctions) กฎหมายภายในของทุกประเทศจะต้องกำหนดให้มีระบบการตรวจสอบการปฏิบัติตามหลักเกณฑ์ข้างต้น และจะต้องกำหนดบทลงโทษทางอาญาและบทปรับในกรณีที่มีการล่วงละเมิดเกิดขึ้น

(9) หลักการส่งข้อมูลไปต่างประเทศ (Transborder Data Flows)ในการส่งข้อมูลข้ามไปต่างประเทศจะต้องทำโดยเสรี และมีหลักประกันความปลอดภัยสำหรับข้อมูลดังกล่าว

(10) หลักการบังคับใช้ (Field of Application) หลักการข้างต้นจะต้องถูกใช้บังคับกับทั้งการประมวลผลของภาครัฐและภาคเอกชนจากแนวทางของกฎหมายระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่นำเสนอมาข้างต้นจะเห็นได้ว่าต่างก็มีหลักการสำคัญที่คล้ายคลึงกันหลายประการ ไม่ว่าจะเป็นหลักความยินยอมของเจ้าของข้อมูล หลักวัตถุประสงค์ในการจัดเก็บ หลักการคุ้มครองข้อมูลข่าวสารส่วนบุคคล หลักการรักษาความปลอดภัยในการนำไปใช้ เป็นต้น ทั้งนี้ความสัมพันธ์ที่เกี่ยวข้องของข้อตกลงระหว่างประเทศในเรื่องการคุ้มครองข้อมูลข่าวสารส่วนบุคคล ซึ่งจะเข้ามาเกี่ยวพันกับกฎหมายภายในประเทศต่างๆ จะมีประเด็นสำคัญอยู่ที่ ภายใต้ข้อตกลงและสนธิสัญญาระหว่างประเทศก็มีหลักการสำคัญที่ห้ามการส่งข้อมูลส่วนบุคคลระหว่างประเทศ (International data transfers or Transborder data flows) โดยกำหนดให้ประเทศที่ดำเนินการแลกเปลี่ยนข้อมูลนั้นจะกระทำได้ต่อเมื่อประเทศนั้นๆ ต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือมีมาตรฐานในการคุ้มครองที่เพียงพอ

ฉะนั้นแล้วจากเงื่อนไขนี้จึงเป็นมาตรการป้องกันปัญหาการคุ้มครองข้อมูลส่วนบุคคลในทางระหว่างประเทศที่สำคัญ และบังคับให้ประเทศต่างๆ ต้องพัฒนากฎหมายของตนให้มีมาตรฐานสากลทัดเทียมกันไปด้วย รวมทั้งยังเป็นการสร้างและรักษามาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลให้อยู่ในระดับเดียวกัน เพื่อความปลอดภัยและเป็นอันหนึ่งอันเดียวกันของเกณฑ์มาตรฐาน และเพื่อลดปัญหาช่องว่างในการคุ้มครองสิทธิเสรีภาพบุคคลในเรื่องนี้ให้น้อยลงมากที่สุด ดังนั้นบทบัญญัติระหว่างประเทศเหล่านี้จึงมีความสำคัญที่ทุกประเทศต้องให้ความสนใจและปฏิบัติตาม และนั้นก็ส่งผลให้กลายเป็นกรอบกติการะหว่างประเทศ ที่ประเทศไทยจะต้องนำมาใช้ตรวจสอบและพัฒนากฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลให้ได้มาตรฐานดังที่กล่าวมาแล้วข้างต้น

(3) กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

กฎหมายทรัพย์สินทางปัญญา เป็นมาตรการทางกฎหมายประการหนึ่งที่ถูกนำเข้ามาปรับใช้กับการคุ้มครองฐานข้อมูลโดยถือว่าฐานข้อมูลที่จัดทำขึ้นใหม่ควรเป็นสิ่งที่มีกฎหมายให้การรองรับและถือเป็นการสร้างสรรค์ จึงควรได้รับการคุ้มครองจากกฎหมายทรัพย์สินทางปัญญา ดังนั้นในกรณีที่มีการจัดทำฐานข้อมูลขึ้นมาเฉพาะเพื่อการแลกเปลี่ยนเชื่อมโยงหรือบูรณาการข้อมูลในกระบวนการยุติธรรม ฐานข้อมูลเหล่านั้นจึงถือเป็นทรัพย์สินทางปัญญาของหน่วยงานหรือองค์กรที่ดำเนินการและควรมีมาตรการทางกฎหมายโดยเฉพาะกฎหมายลิขสิทธิ์มาให้การรับรองและคุ้มครอง

เมื่อพิจารณาฐานข้อมูลที่สรุปได้อย่างกว้างๆว่าเป็นการรวบรวมข้อมูลหรือสารสนเทศอย่างเป็นระบบระเบียบ(Organized collection of information)หรือชุดข้อมูลที่ได้รับการจัดเรียงเป็นหมวดหมู่อย่างดีจะเห็นได้ว่ามีคุณสมบัติคาบเกี่ยวและสามารถนับได้ว่าเป็นทรัพย์สินทางปัญญา ซึ่งในแง่ของกฎหมายแล้ว หมายถึงสิทธิอันเกิดขึ้นจากผลงานทางความคิด เช่น แนวความคิดเกี่ยวกับสิ่งประดิษฐ์ บทกวี วรรณกรรม คอมพิวเตอร์โปรแกรม เป็นต้น มากกว่าจะหมายถึงตัวผลิตผลที่จะได้สร้างสรรค์ขึ้น ดังนั้นคำว่าทรัพย์สินทางปัญญา จึงหมายถึง สิทธิตามกฎหมายซึ่งได้มีการกำหนดขึ้นอันเกี่ยวด้วยกับผลผลิตจากปัญญาของมนุษย์ โดยขึ้นอยู่กับองค์ประกอบของฐานข้อมูลนั้นๆ อย่างเช่น หากเป็นการรวบรวมหรือจัดการเกี่ยวกับข้อมูล ที่ต้องใช้ความอุตสาหพยายามอย่างมากและในบางกรณีจะต้องใช้ความคิดสร้างสรรค์เพื่อให้แก้ปัญหาให้ลุล่วงไปได้ ด้วยคุณสมบัติดังกล่าวจึงทำให้ฐานข้อมูลจำพวกได้รับความคุ้มครองในฐานะทรัพย์สินทางปัญญาภายใต้กฎหมายลิขสิทธิ์ เช่น งานที่ถือว่ามีคุณภาพใกล้เคียงกับงานวรรณกรรม (Literary works) อาจได้รับความคุ้มครองลิขสิทธิ์ในข้อใดข้อหนึ่งดังต่อไปนี้

1.เนื้อหาที่จะได้รับการคัดเลือกมารวมไว้ (Selection of the content)

2.การประสานกันของเนื้อหาทั้งหมด (Internal co-ordination of the content)

3.การจัดลำดับความสัมพันธ์ขององค์ประกอบทั้งหมดของฐานข้อมูล (Arrangement of all elements of the database)

4.เนื้อหาของงานนั้นๆ เองโดยตรง (The content itself)

ในกรณีของฐานข้อมูลมักจะได้รับความคุ้มครองทั้งหมด เนื่องจากข้อมูลที่ประกอบกันขึ้นเป็นฐานข้อมูล ซึ่งมักจะเป็นข้อมูลสาธารณะ (Public knowledge) หรือเป็นเพียงข้อเท็จจริง (Mere facts) และข้อมูลที่มีความพิเศษ (Unique Information) ที่ทำให้ฐานข้อมูลนั้นมีคุณสมบัติที่โดดเด่นออกมาจากการเป็นแต่เพียงสมุดรวบรวมข้อมูลตามลำดับก่อนหลัง ยกตัวอย่างเช่น หากเราต้องการสร้างฐานข้อมูลรายชื่อผู้ค้าอุปกรณ์คอมพิวเตอร์ โดยต้องการสำรวจความสนใจของผู้ประกอบการในตลาด และหากรายใดสนใจก็จะอนุญาตให้ผู้รวบรวมนำชื่อและที่อยู่ของผู้ประกอบการนั้น รวมไว้ในฐานข้อมูลที่จัดลำดับด้วยความอุตสาหะได้ แต่หากงานมีเพียงแค่นี้ ก็จะไม่ได้รับความคุ้มครองลิขสิทธิ์ผู้รวบรวมเพิ่มส่วนแจกแจงคุณสมบัติของผู้ประกอบการแต่ละรายลงไป ซึ่งถือว่าเป็นข้อมูลที่มีความพิเศษ อาจทำให้งานชิ้นนี้ได้รับความคุ้มครองก็ได้เนื่องจากศาลเห็นว่าผู้รวบรวมมีความพยายามในการสร้างผลงาน จึงไม่ควรที่จะให้ผู้อื่นฉกฉวยผลประโยชน์ในแง่ธุรกิจไปได้ นอกจากนี้การพิจารณาว่างานชิ้นใด เข้าข่ายเป็นทรัพย์สินทางปัญญาและสมควรจะได้รับความคุ้มครองนั้น ยังนิยมที่จะอ้างถึงคำตัดสินของศาลในกรณีที่คล้ายๆ กันอีกด้วย ดังกรณีตัวอย่าง Rural Telephone v. Feist Publications ที่มีชื่อเสียง

ดังนั้น ระบบฐานข้อมูลด้านกระบวนการยุติธรรมที่จัดทำขึ้นในต่างประเทศนอกจากรัฐจะต้องมีกลไกในการดำเนินการเพื่อปกป้องข้อมูลมิให้ถูกนำไปใช้เพื่อแสวงหาผลประโยชน์และก่อให้เกิดความเสียหายแล้วยังจะต้องให้การคุ้มครองถึงลักษณะด้านทรัพย์สินทางปัญญาอันเกี่ยวข้องกับกฎหมายลิขสิทธิ์ของข้อมูลข่าวสารในกระบวนการยุติธรรมนั้นด้วย

ลิขสิทธิ์ (Copyright) เป็นประเภทหนึ่งของทรัพย์สินทางปัญญา (Intellectual Property) โดยในทางกฎหมายมิใช่หมายความถึงทรัพย์ในแง่ที่มีรูปร่างสามารถจับต้องได้ตามกฎหมาย โดยมีระยะคุ้มครองที่แน่นอนในการกระทำการต่างๆ เช่น การจำหน่าย การจัดพิมพ์ การเผยแพร่ ในงานต้นฉบับหรือส่วนใดส่วนหนึ่งของงาน[37] หรือตามแนวของ WIPO ลิขสิทธิ์

[37] an exclusive legal right, held for a certain number of years, to print, publish, sell, broadcast, perform, film or record an original work or any part of it

หมายถึง การให้ความคุ้มครองตามกฎหมายแก่ผู้สร้างสรรค์งานอันมีลิขสิทธิ์ซึ่งได้สร้างสรรค์ขึ้นมา โดยประกอบด้วยสิทธิทางเศรษฐกิจและสิทธิทางศีลธรรม[38] หรือในอนุสัญญาเบอร์นฉบับ Berlin Act 1908, ข้อ 2 ได้ให้คำอธิบายการคุ้มครองงานวรรณกรรมและศิลปกรรมไว้ดังนี้ “งานวรรณกรรมและศิลปกรรมหมายรวมถึง งานใดๆ ไม่ว่าจะเป็นงานวรรณกรรมวิทยาศาสตร์หรือศิลปกรรม หรืองานในรูปหรือลักษณะใดๆ” ...

ส่วนข้อตกลง TRIPS ในภาคผนวก 1 ซีได้กล่าวถึง ลิขสิทธิ์โดยอ้อมว่า ลิขสิทธิ์และสิทธิเกี่ยวเนื่องเป็นประเภทหนึ่งของทรัพย์สินทางปัญญาในข้อ 1 วรรค 2 (For the purposes of this Agreement, the term “intellectual property” refers to all categories of intellectual property that are the subject of Sections 1 through 7 of Part II”

สำหรับสนธิสัญญาลิขสิทธิ์ของ WIPO แม้ไม่ได้กล่าวถึงความหมายของลิขสิทธิ์ไว้ชัดเจน แต่ใช้วิธีการอ้างถึงอนุสัญญาเบอร์นและขยายงานอันมีลิขสิทธิ์บางประเภทที่อนุสัญญาเบอร์นไม่มี ซึ่งเป็นวิธีการแก้ปัญหาที่ง่ายที่สุด โดยทั่วไปแล้วงานทุกงานที่เกิดจากความคิดสร้างสรรค์ย่อมเป็นงานมีลิขสิทธิ์ทั้งสิ้น ไม่ว่าจะจัดประเภทไว้หรือไม่ก็ตาม เพียงแต่ปัญหาที่เกิดขึ้นและไม่ยุตินั้นเป็นผลเนื่องจากลิขสิทธิ์มีความเกี่ยวข้องกับผลประโยชน์และเป็นแหล่งเศรษฐกิจและมีผลต่อการค้า ดังนั้น การให้ความคุ้มครองลิขสิทธิ์ไม่ว่าตามแนวกฎหมายใดๆ จำต้องมีลักษณะของคำนิยามจำกัดอยู่ในเรื่องของ **“งานอันมีลิขสิทธิ์และสิทธิของผู้สร้างสรรค์ที่จะได้รับความคุ้มครองตามกฎหมาย”**

ลิขสิทธิ์เป็นทรัพย์สินประเภทหนึ่งโดยจัดเป็นวัตถุไม่มีรูปร่าง แต่มีราคาและถือเอาได้ตามกฎหมาย ไม่ว่ายุคสมัยใด ลิขสิทธิ์จึงมีวัตถุแห่งสิทธิเป็นนามธรรมกล่าวคือ ผลงานสร้างสรรค์ต่างๆ ซึ่งไม่สามารถยึดถือหรือครอบครองได้ที่เกิดจากการใช้สติปัญญา ความรู้ความสามารถ และแรงงานสามารถแสดงออกซึ่งความคิดในรูปแบบที่มีลักษณะเฉพาะหรือเอกลักษณ์ของตน ไม่ใช่ผลิตผลเกิดจากการใช้ความคิดรูปแบบที่ลอกเลียนมา และงานนั้นเป็นงานที่กฎหมายภายในของแต่ละประเทศกำหนดให้ความคุ้มครองย่อมให้ถือเป็นงานอันพึงมีลิขสิทธิ์ได้ และลักษณะของสิทธิในลิขสิทธิ์เป็นสิทธิผู้เดียว (Exclusive rights) โดยมีวัตถุแห่งสิทธิเป็นอำนาจหวงกันมิให้ผู้อื่นมาละเมิดสิทธิของตน ซึ่งเมื่อพิจารณาวัตถุแห่งลิขสิทธิ์ ตั้งแต่อดีตจนถึงปัจจุบันจะพบความแตกต่างอย่างเห็นได้ชัดในเนื้อหาที่จะให้ความคุ้มครองซึ่งเป็นไปตามสถานการณ์ทั้งด้านเศรษฐกิจ สังคม และการค้าระหว่างประเทศเป็นสำคัญ เช่น อนุสัญญา

---

[38]Copyright it’s the legal protection extended to the owner of the rights in an original work that he has created. It comprised two main sets of rights : the economic rights and the moral rights

เบอร์นตั้งแต่ ค.ศ.1886 จนถึง ค.ศ.1971 มีวัตถุแห่งลิขสิทธิ์ที่ “งานวรรณกรรมและศิลปกรรม” (literary and artistic works) โดยแต่ละฉบับจะเป็นการเพิ่มเติมการให้ความคุ้มครองงานอันมีลิขสิทธิ์ว่ามีงานใดบ้าง เช่น อนุสัญญาเบอร์น 1886 มิได้ให้คำจำกัดความของงานแปลไว้ แต่ในอนุสัญญาเบอร์น 1908 ได้ขยายงานที่ให้ความคุ้มครองรวมถึงการแปล การดัดแปลงและงานลักษณะอื่นไว้ ในมาตรา 2 ดังนี้ “…Translations, adaptations, arrangements of music and other reproductions in an altered form of literary or artistic work…” หรือในข้อตกลง TRIPS หรือสนธิสัญญาลิขสิทธิ์ของ WIPO เองต่างต้างถึงวัตถุแห่งลิขสิทธิ์ไว้คล้ายกับอนุสัญญาเบอร์น แต่ได้มีการขยายความคุ้มครองเรื่องของโปรแกรมคอมพิวเตอร์ และฐานข้อมูลไว้เช่นกัน และวัตถุแห่งลิขสิทธิ์ที่เกิดขึ้นใหม่ของสนธิสัญญาลิขสิทธิ์ของ WIPO ได้แก่ การบริหารข้อมูลและข้อมูล อิเล็กโทรนิคไว้เป็นการเฉพาะ

สำหรับฐานข้อมูลหรือการรวบรวมข้อมูล (Collective Data หรือ Complication of Data) ได้มีการบัญญัติไว้ในข้อ 5 กล่าวคือ การรวบรวมข้อมูลหรือวัตถุใดไม่ว่าในรูปแบบใดเนื่องจากการคัดเลือกหรือเรียบเรียงเนื้อหาที่เป็นการสร้างสรรค์ทางปัญญาย่อมได้รับการคุ้มครอง แต่ไม่คลุมถึงตัวข้อมูลเอง[39] ซึ่งหมายความว่า การให้ความคุ้มครองภายใต้ข้อนี้จำกัดเฉพาะข้อมูลที่ใช้ความคิดสร้างสรรค์ (Intellectual Creations) ในการคัดเลือกหรือเรียบเรียงข้อมูลหรือวัตถุใดซึ่งอยู่ในรูปแบบใด (in any form) ก็คำว่า รูปแบบใดก็ได้นี้สามารถตีความรองรับถึงการรวบรวมข้อมูลหรือฐานข้อมูลในรูปอิเลคโทรนิคได้ ตัวอย่างของงานที่เรียกว่าฐานข้อมูล

อย่างไรก็ตาม งานอันมีลิขสิทธิ์เดิมยังคงได้รับการคุ้มครองตามสิทธิ ที่มีอยู่ก่อนนี้เหมือนเดิม ส่วนการถูกรวบรวมให้อยู่ในฐานข้อมูลอันใหม่นี้ไม่ได้ทำให้สิทธิต่างๆ ที่มีอยู่เดิมนั้นถูกกระทบแต่อย่างใด นอกจากนี้ข้อความอันเป็นที่ยอมรับได้กล่าวไว้ในข้อ 5 ว่า บทบัญญัติในข้อ 5 นี้จะมีเนื้อหาที่สอดคล้องกับข้อ 2(5) ของอนุสัญญาเบอร์น ที่ว่า”การรวบรวมงานวรรณกรรมหรือศิลปกรรมเช่น สารานุกรม โดยวิธีการคัดเลือกและรวบรวมเนื้อหาที่ใช้สติปัญญาสร้างสรรค์ย่อมได้รับความคุ้มครอง.....” ทั้งสองข้อตกลงได้ให้ความสำคัญในเรื่อง “การเลือกและการเรียบเรียงเนื้อหา” เหมือนกัน แต่ต่างกันที่ถ้อยคำที่ใช้ซึ่งภาษาในสนธิสัญญาลิขสิทธิ์ใช้คำ “กว้างกว่า” ในอนุสัญญาเบอร์น กล่าวคือ ในสนธิสัญญาใช้คำว่า “ไม่ว่าในรูปแบบใด” (in any

---

[39] Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copy right subsisting in the data or material contained in the compilation.

from) ซึ่งหมายรวมถึง งานในรูปดิจิตอลไม่ว่าจะเป็นภาพหรือเสียง แต่ในอนุสัญญาเบอร์นระบุเพียงการคัดเลือกและเรียบเรียงเนื้อหาของงานวรรณกรรมหรือศิลปกรรมซึ่งทำให้ไม่คลุมถึงงานดิจิตอลที่มีความสำคัญในยุค 2000 นี้

ถ้อยคำในสนธิสัญญานี้ยังคล้ายกับข้อ 10(2) ของ TRIPS ที่กล่าวว่า “การรวบรวมข้อมูลหรือวัตถุใด ไม่ว่าจะอยู่ในรูปแบบที่เครื่องอ่านได้หรือในรูปแบบอื่นซึ่งเป็นการสร้างสรรค์ทางปัญญา โดยการคัดหรือเรียบเรียงจะได้รับความคุ้มครอง” หากพิจารณาเนื้อหาการให้ความคุ้มครองย่อมมีลักษณะคล้ายคลึงกันเพียงแต่ถ้อยคำที่ใช้มีความต่างกัน กล่าวคือ ถ้อยคำที่ใช้ในสนธิสัญญานี้ใช้คำว่า”ไม่ว่าในรูปแบบใด” แต่ข้อตกลง TRIPS นี้ใช้คำว่า “ในรูปแบบที่เครื่องอ่านได้หรือในรูปแบบอื่น” ซึ่งเมื่อเทียบกันแล้วจะพบว่า จุดมุ่งหมายของทั้งสองนั้นไม่แตกต่างกันเพราะมีลักษณะการใช้ถ้อยคำกว้างๆ ในการคุ้มครองงานประเภทนี้เหมือนกัน ซึ่งคาดว่า เป็นการเตรียมความพร้อมในการรับมือกับข้อมูลในยุคดิจิตอล

ส่วนข้อความในท้ายประโยคของข้อ 5 ของสนธิสัญญาที่กำหนดว่า **“จะไม่ครอบคลุมถึงข้อมูลหรือวัตถุและจะไม่กระทบต่อลิขสิทธิ์ที่มีอยู่เดิม”** หากพิจารณาเปรียบเทียบจะพบว่า เนื้อหาและหลักการมีลักษณะใกล้เคียงกับข้อ 2(5) ของอนุสัญญาเบอร์น กล่าวคือ งานรวบรวมเป็นงานลิขสิทธิ์ ถ้ามีการเลือกและเรียบเรียง โดยที่แต่ละงานวรรณกรรมหรือศิลปกรรมใดที่เป็นงานลิขสิทธิ์อยู่แต่เดิมก็จะไม่ได้รับความคุ้มครอง (without prejudice to the copyright in eac of the works forming part of such collections) แต่ต่างกันที่ถ้อยคำของงาน โดยสนธิสัญญานี้ใช้คำว่า “ข้อมูลหรือวัตถุใด” ซึ่งเป็นคำกว้างๆ แต่ในอนุสัญญาเบอร์นใช้คำว่า “งานวรรณกรรมและศิลปกรรม”

สำหรับวรรคท้ายของข้อตกลง TRIPS มีความสอดคล้องในเรื่องหลักการเดียวกับวรรคท้ายของสนธิสัญญานี้โดยวรรคท้ายของข้อตกลง TRIPS ระบุว่า การคุ้มครองเช่นว่านี้จะไม่ขยายคลุมถึงข้อมูลหรือวัตถุโดยตัวของมันเอง (Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.) ซึ่งหมายความว่า การคุ้มครองงานรวบรวมข้อมูลหรือฐานข้อมูลนี้จะไม่ขยายไปคลุมถึงข้อมูลซึ่งไม่ใช่งานลิขสิทธิ์ในตนเอง

จากข้อสังเกตที่กล่าวมาแล้วข้างต้นสามารถสรุปได้ว่าฐานข้อมูลที่จะได้รับความคุ้มครองตามข้อ 5 จำต้องประกอบด้วย

1. ข้อมูลหรือวัตถุใดซึ่งเป็นงานลิขสิทธิ์อยู่แล้วและ

2. ข้อมูลเหล่านั้นได้มีการคัดลอกหรือเรียบเรียงข้อมูลในฐานข้อมูลโดยใช้ปัญญาสร้างสรรค์ขึ้นมาใหม่

การรวบรวมข้อมูลทางด้านกระบวนการยุติธรรมหรือการจัดทำฐานข้อมูลที่เกี่ยวกับงานยุติธรรมหรือวัตถุใดไม่ว่าในรูปแบบใด เช่น ซีดี หรือโสตทัศนูปกรณีต่าง ๆ เนื่องจากการคัดเลือกหรือเรียบเรียงเนื้อหาที่เป็นเนื้อหาที่ตนเองดูแลและรับผิดชอบก็น่าจะถือเป็นเป็นการสร้างสรรค์ทางปัญญาควรได้รับการคุ้มครอง ซึ่งนั่นหมายความว่าในกรณีที่กระทรวงยุติธรรมเป็นผู้ที่บูรณาการข้อมูลด้านงานยุติธรรมแล้วน่าจะถือเป็นเป็นการสร้างสรรค์ทางปัญญาควรได้รับการคุ้มครองจากกฎหมายทรัพย์สินทางปัญญาด้วย แม้ว่าในตัวกฎหมายทรัพย์สินทางปัญญาของไทยยังไม่ได้ระบุชัดเจน แต่หากพิจารณาจากการที่บทบัญญัติต่าง ๆที่กล่าวมาแล้วจะเห็นได้ว่าได้มีการให้การคุ้มครองฐานข้อมูลและการบูรณาการข้อมูลแทบทั้งสิ้น เพราะถือว่าเป็นการสร้างสรรค์ผลงาน การให้มีมาตรการทางกฎหมายทรัพย์สินทางปัญญาน่าจะเป็นผลดีมากกว่า

(4) กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในการกระทำความผิด (Computer Misuse Laws)

ฐานข้อมูลที่เกี่ยวกับกระบวนการยุติธรรมเป็นฐานข้อมูลที่มีบทบาทและความสำคัญอย่างยิ่งทั้งต่อการดำเนินคดี การสร้างความยุติธรรม และผลกระทบต่อชีวิตร่างกาย ทรัพย์สิน ของบุคคลที่เกี่ยวข้องไม่ว่าจะเป็นโจทก์ จำเลย พยาน และผู้เกี่ยวข้องอื่นๆ ซึ่งหากมีผู้ที่สามารถนำข้อมูลเหล่านั้นไปใช้ประโยชน์โดยมิชอบจากการลักลอบเข้าถึงข้อมูลโดยไม่ถูกต้อง (Hacking) จึงควรมีมาตรการทางกฎหมาย มาตรการคุ้มครองโดยเฉพาะต่อการกระทำความผิดต่อคอมพิวเตอร์ให้เป็นอาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่ง ซึ่งทำให้เกิดผลกระทบต่อกฎหมายอาญาของประเทศต่าง ๆทั่วโลก กล่าวคือ การกระทำดังกล่าวอยู่นอกขอบเขตของกฎหมายที่ใช้บังคับอยู่ ทำให้ไม่เป็นความผิดอาญา เนื่องจากกฎหมายอาญาของประเทศต่าง ๆล้วนแล้วแต่เน้นให้ความคุ้มครองแก่วัตถุที่มีรูปร่าง (tangible or corporeal objects) เช่น ทรัพย์ เป็นต้น เมื่อการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่าง ๆเป็นการกระทำต่อวัตถุที่ไม่มีรูปร่าง (intangible or incorporeal objects) ได้แก่ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ดังนั้น การกระทำความผิดต่อคอมพิวเตอร์จึงไม่เป็นความผิดอาญา[40]

---

[40] องอาจ เทียนหิรัญ. “**อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์.**” หน้า 46

ขณะนี้ มีการกระทำความผิดต่อคอมพิวเตอร์ใน 6 รูปแบบที่สำคัญ[41]ได้แก่ การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (unauthorized access to information system) การดักข้อมูลคอมพิวเตอร์ (interception) การจารกรรมข้อมูลคอมพิวเตอร์ (computer espionage) การทำให้เกิดความเสียหายต่อคอมพิวเตอร์ (computer sabotage) การปลอมข้อมูลคอมพิวเตอร์ (computer forgery) และการฉ้อโกงทางคอมพิวเตอร์ (computer fraud)

ปัจจุบัน ประเทศต่างๆที่มีความเจริญก้าวหน้าทางเทคโนโลยีทางการติดต่อสื่อสารและคอมพิวเตอร์ เช่น ประเทศสหรัฐอเมริกา อังกฤษ เยอรมัน และกลุ่มประเทศสหภาพยุโรปต่างกำหนดให้การกระทำความผิดต่อคอมพิวเตอร์ในรูปแบบต่างๆเป็นความผิดอาญา เพื่อให้ความคุ้มครองคุณลักษณะ (properties) ของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ซึ่งได้แก่ ความลับ (confidentiality) ความครบถ้วน (integrity) และความสามารถในการใช้ประโยชน์ได้ (availability) ของสิ่งต่างๆดังกล่าว และการให้ความคุ้มครองสิทธิในทรัพย์สินของเจ้าของทรัพย์สิน

แม้ว่าในขณะนี้จะยังไม่มีคำนิยามคำว่า “อาชญากรรมทางคอมพิวเตอร์” ที่เป็นสากล แต่เพื่อให้สะดวกต่อการทำความเข้าใจเรื่องอาชญากรรมทางคอมพิวเตอร์ โดยเฉพาะอย่างยิ่ง เรื่องการกระทำความผิดต่อคอมพิวเตอร์ บทบาทของคอมพิวเตอร์ที่เข้าไปมีส่วนเกี่ยวข้องกับการกระทำความผิดเป็น 3 ลักษณะ[42] คือ

1.คอมพิวเตอร์ในฐานะที่เป็นวัตถุแห่งการกระทำความผิด (computers as the target of the crime) ในกรณีนี้คือการกระทำความผิดในรูปแบบต่างๆต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ การดักข้อมูลคอมพิวเตอร์ การจารกรรมข้อมูลคอมพิวเตอร์ การทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ เป็นต้น

2.คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือที่ใช้ในการกระทำความผิด (computers as a tool in the commission of a crime) การกระทำในกรณีนี้ คือการกระทำความผิดรูปแบบเดิม แต่ผู้กระทำได้ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เพื่อให้

---

[41] เชิดพันธ์ อุปนิสากร. “ความรับผิดทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต.”หน้า 24

[42] นัยนรัตน์ งามแสง. “**อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเทอร์เน็ต.**” หน้า 58

สามารถกระทำความผิดได้โดยสะดวก หรือมีประสิทธิภาพมากยิ่งขึ้น (If a computer is a tool of the crime, the computer is used to commit and old crime in a high – tech way) เช่น การเผยแพร่ภาพลามกอนาจาร การพนันที่ผิดกฎหมาย การละเมิดลิขสิทธิ์ การฟอกเงิน เป็นต้น

3.คอมพิวเตอร์ในฐานะที่มีส่วนเกี่ยวข้องกับการกระทำความผิด (computers as incidental to crime) การกระทำในกรณีนี้ คอมพิวเตอร์จะมีส่วนเกี่ยวข้องกับการกระทำความผิดไม่ว่าทางใดทางหนึ่ง โดยการใช้คอมพิวเตอร์จะทำให้การกระทำผิดเป็นไปด้วยความสะดวกและมีประสิทธิภาพยิ่งขึ้น อย่างไรก็ดี บทบาทของคอมพิวเตอร์นั้นไม่มีความสำคัญถึงขนาดที่ ถ้าไม่มีคอมพิวเตอร์แล้ว ความผิดจะไม่สามารถเกิดขึ้นได้เลย กล่าวอีกนัยหนึ่ง แม้จะไม่มีการใช้คอมพิวเตอร์ การกระทำความผิดนั้นก็ยังคงสามารถเกิดขึ้นได้อยู่ดี เช่น การใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับลูกค้ายาเสพติด ลูกค้าที่เล่นการพนัน เป็นต้น

รูปแบบการกระทำความผิดต่อคอมพิวเตอร์

ขณะนี้ มีการกระทำความผิดต่อคอมพิวเตอร์ 6 รูปแบบที่สำคัญ ได้แก่ การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ การดักข้อมูลคอมพิวเตอร์ การจารกรรมข้อมูลคอมพิวเตอร์ การทำให้เกิดความเสียหายต่อคอมพิวเตอร์ การปลอมข้อมูลคอมพิวเตอร์ และการฉ้อโกงทางคอมพิวเตอร์ โดยการกระทำความผิดต่อคอมพิวเตอร์ในรูปแบบต่างๆดังกล่าว ส่วนใหญ่เริ่มเกิดขึ้นจากการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจก่อน แล้วจึงมีการกระทำความผิดรูปแบบอื่นต่อไป

1.การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ

การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (unauthorized access to information system) หมายถึง การเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์โดยปราศจากอำนาจ

แต่เดิมคำว่า"การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ" เป็นคำที่ใช้เรียกการเข้าถึงสิ่งต่างๆดังกล่าว โดยผู้กระทำไม่มีเจตนาที่จะก่อให้เกิดความเสียหายใดๆ เช่น การจารกรรม ข้อมูลความลับทางการค้า การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ การฉ้อโกง และการก่อวินาศกรรมทางคอมพิวเตอร์ เป็นต้น แต่ผู้กระทำเข้าถึงคอมพิวเตอร์เพียงเพราะต้องการเอาชนะระบบรักษาความปลอดภัยของคอมพิวเตอร์ ต้องการได้รับการยอมรับจากเพื่อนฝูงว่าตนมีความสามารถทางคอมพิวเตอร์

วิธีการเข้าถึงคอมพิวเตอร์มีหลายวิธี ตั้งแต่วิธีการง่ายๆไปจนถึงวิธีการยากๆ เช่น การแอบดูรหัสผ่าน (password) การใช้เครื่องมือพิเศษดักรหัสผ่านจากสายโทรศัพท์หรือคอมพิวเตอร์ การออกแบบให้โปรแกรมนั้นสามารถค้นหารหัสผ่านของผู้อื่น เป็นต้น

การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจทำให้เกิดผลกระทบต่อความลับของข้อมูล ดังที่ได้กล่าวแล้วว่า ความลับ หมายถึง สภาวะที่ไม่มีผู้อื่นสามารถเข้าถึงข้อมูลได้นอกจากเจ้าของข้อมูล โดยเจ้าของข้อมูลมีสิทธิเด็ดขาดในการควบคุมการเข้าถึงหรือเปิดเผยข้อมูลนั้น เมื่อพิจารณาลักษณะของความลับแล้ว อาจกล่าวได้ว่า ความลับเป็นเรื่องส่วนตัวของมนุษย์ทุกผู้ทุกนาม

เมื่อพิจารณาเรื่องการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ จะเห็นว่านอกจากจะกระทบต่อความลับของข้อมูลแล้ว ยังทำให้เกิดผลกระทบต่อกฎหมายอาญาของประเทศต่างๆทั่วโลกด้วย เนื่องจากการกระทำดังกล่าวอยู่นอกขอบเขตความรับผิดทางอาญา กล่าวคือ แม้ว่าการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจจะมีลักษณะคล้ายกับการบุกรุก แต่เพราะเป็นการเข้าถึงทางอิเล็กทรอนิกส์ มิได้มี “การเข้าไป” ทางกายภาพ (real property) อันเป็นองค์ประกอบของความผิดฐานบุกรุกแต่อย่างใด การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ จึงไม่เป็นความผิดฐานบุกรุก

ในเรื่องของการกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิดกฎหมายอาญาของแต่ละประเทศบัญญัติองค์ประกอบของความผิดฐานนี้ไว้ไม่เหมือนกัน เช่น บางประเทศกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเพียงอย่างเดียวเป็นความผิด เช่น กฎหมายอังกฤษ ออสเตรเลีย เดนมาร์ก กรีก และมลรัฐต่างๆส่วนใหญ่ในประเทศสหรัฐอเมริกา เป็นต้น บางประเทศกำหนดให้การเข้าถึงคอมพิวเตอร์จะเป็นความผิดต่อเมื่อมีองค์ประกอบอย่างอื่นด้วย เช่น ผู้กระทำมีเจตนาที่จะกระทำความผิดอย่างอื่นภายหลังจากการเข้าถึงคอมพิวเตอร์ เช่น กฎหมายฝรั่งเศส แคนาดา อิสราเอล นิวซีแลนด์ หรือเป็นการเข้าถึงคอมพิวเตอร์ที่มีการติดตั้งระบบรักษาความปลอดภัย เช่น กฎหมายเยอรมัน เนเธอร์แลนด์ นอร์เวย์ หรือเป็นการเข้าถึงคอมพิวเตอร์แล้วผู้กระทำได้ไปซึ่งข้อมูล หรือกระทำการต่างๆ เช่น แก้ไขเปลี่ยนแปลง หรือทำให้ข้อมูลเสียหาย เช่น กฎหมายของบางมลรัฐในประเทศสหรัฐอเมริกา เป็นต้น

การดักข้อมูลคอมพิวเตอร์ (Computer interception) คือ การดักข้อมูลคอมพิวเตอร์หรือสิ่งต่างๆที่ได้มาจากการปฏิบัติงานของระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เช่น คลื่นอิเล็กทรอนิกส์ (Electromagnetic radiation) เป็นต้น การดักข้อมูล

คอมพิวเตอร์อาจกระทำได้สองวิธี วิธีแรก คือ การเข้าถึงระบบคอมพิวเตอร์โดยตรงแล้วจึงดักข้อมูลคอมพิวเตอร์ วิธีที่สอง คือ การใช้เครื่องดักข้อมูล (eltctronic eavesdropping devices) ซึ่งเป็นการอาศัยเทคโนโลยีสมัยใหม่ดักข้อมูลคอมพิวเตอร์ โดยที่ผู้ดักข้อมูลไม่จำเป็นต้องเข้าถึงระบบคอมพิวเตอร์เลย เพียงแต่วางเครื่องดักข้อมูลไว้ในระยะที่สามารถดักข้อมูลได้ก็พอแล้ว

เมื่อพิจารณาถึงลักษณะและวิธีการดักข้อมูลแล้ว จะเห็นว่า การดักข้อมูลสามารถกระทำได้โดยง่ายและสะดวกมากกว่าการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ และการตรวจพบการกระทำความผิดดังกล่าวก็เป็นเรื่องยาก เนื่องจากผู้กระทำไม่จำเป็นต้องเข้าถึงระบบคอมพิวเตอร์ และข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ก็มิได้ถูกแก้ไขเปลี่ยนแปลง หรือเกิดความเสียหายแต่อย่างใด ทำให้ไม่มีร่องรอยการกระทำความผิด ผลของการดักข้อมูลคือ การทำให้เกิดผลกระทบต่อความลับของข้อมูล

การให้ความคุ้มครองความลับในการติดต่อสื่อสารนั้น โดยปกติมีกฎหมายให้ความคุ้มครองในเรื่องนี้อยู่แล้ว ได้แก่ กฎหมายที่เกี่ยวกับการควบคุมการดักฟังข้อมูลจากระบบการติดต่อสื่อสารต่างๆ เช่น กฎหมายห้ามการดักฟังโทรศัพท์ (wire tapping) และการดักข้อมูลในระหว่างการติดต่อสื่อสาร (interception of data communications) แต่ปัญหาที่เกิดขึ้น คือ กฎหมายเหล่านี้ให้ความคุ้มครองเฉพาะกรณีที่เป็นการติดต่อสื่อสารกันทางคำพูดหรือสัญญาณต่างๆจากการติดต่อสื่อสารทางระบบคอมพิวเตอร์ด้วย

การจารกรรมข้อมูลคอมพิวเตอร์

ก่อนที่จะมีการจารกรรมข้อมูลคอมพิวเตอร์ ได้มีการจารกรรมข้อมูลของบุคคลอื่นอยู่แล้วเช่น การจารกรรมข้อมูลทางอุตสาหกรรม ข้อมูลทางเศรษฐกิจ ความลับทางการค้า ข้อมูลส่วนตัวของบุคคล เป็นต้น เมื่อเทคโนโลยีทางการติดต่อสื่อสารและคอมพิวเตอร์มีความเจริญก้าวหน้ามากขึ้น โดยเฉพาะความสามารถในการเก็บ เข้าถึง และประมวลผลข้อมูลของคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ จึงทำให้เกิดความนิยมในการนำข้อมูลต่างๆตั้งแต่ข้อมูลทั่วๆไป จนถึงข้อมูลที่มีความสำคัญไปเก็บไว้ในคอมพิวเตอร์ ด้วยเหตุนี้ คอมพิวเตอร์จึงกลายเป็นเป้าหมายในการกระทำความผิดแห่งใหม่ที่มีเสน่ห์ดึงดูดใจบรรดาอาชญากรทั้งหลาย

เมื่อพิจารณาลักษณะของการจารกรรมข้อมูลคอมพิวเตอร์แล้ว จะเห็นว่า การกระทำนี้ทำให้เกิดความเสียหายต่อความเป็นความลับของข้อมูลและการจารกรรมข้อมูลมีลักษณะคล้ายกับการลักทรัพย์ อย่างไรก็ดี เมื่อพิจารณาความรับผิดทางอาญาสำหรับการจารกรรมทางคอมพิวเตอร์แล้ว จะเห็นว่า ความผิดฐานลักทรัพย์ไม่สามารถนำมาใช้กับการ

จารกรรมข้อมูลคอมพิวเตอร์ได้ เนื่องจาก “ไม่มีการเอาไป หรือพรากไปซึ่งกรรมสิทธิ์และการครอบครองข้อมูล” กล่าวคือ การจารกรรมข้อมูลคอมพิวเตอร์มิได้ส่งผลกระทบต่อกรรมสิทธิ์และการครอบครองข้อมูลของเจ้าของข้อมูลคอมพิวเตอร์แต่อย่างใด เจ้าของข้อมูลยังคงมีสิทธิ์ต่างๆดังกล่าวอยู่ตลอดเวลา

การทำให้เกิดความเสียหายต่อคอมพิวเตอร์

การทำให้เกิดความเสียหายต่อคอมพิวเตอร์ คือ การกระทำด้วยวิธีการใดๆ เช่น การนำเข้า แก้ไขเปลี่ยนแปลง ลบ ทำลาย เป็นต้น เพื่อทำให้เกิดความเสียหายต่างๆ เช่น การรบกวน การขัดขวาง การแทรกแซง การหยุดการทำงาน หรือการทำให้เกิดความเสียหายอย่างอื่นต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ การกระทำนี้อาจเรียกอีกอย่างหนึ่งว่า “การก่อวินาศกรรมทางคอมพิวเตอร์” (Computer sabotage)

มูลเหตุจูงใจในการกระทำความผิดโดยใช้โปรแกรมที่ลักษณะอันตรายนี้อาจเป็นไปเพื่อการต้องการแก้แค้น การกรรโชกทรัพย์ หรือการก่อการร้าย เป็นต้น ต่อมา วิธีการกระทำความผิดได้เปลี่ยนแปลงไป กล่าวคือ ผู้กระทำความผิดหันมานิยมใช้โปรแกรมคอมพิวเตอร์ที่มีคุณสมบัติและความสามารถในการลบ ทำลาย รบกวน ขัดขวาง หรือทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ได้อย่างมากมายและภายในเวลาอันรวดเร็ว โดยเรียกโปรแกรมที่มีลักษณะดังกล่าวว่า “โปรแกรมที่มีลักษณะอันตราย” (Crash programs) โดยความเสียหายที่เกิดขึ้นมิได้เป็นความเสียหายทางกายภาพเหมือนเช่นความเสียหายที่เกิดขึ้นจากการทำให้เกิดเสียรูปแบบเดิม แต่เป็นความเสียหายต่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ซึ่งเรียกว่าเป็น “ความเสียหายต่อสิ่งที่ไม่มีรูปร่าง” (Logical damage)

เมื่อพิจารณาลักษณะของการทำให้เกิดความเสียหายต่อคอมพิวเตอร์แล้วจะเห็นว่า ทำให้เกิดผลกระทบต่อความครบถ้วน และความสามารถในการใช้ประโยชน์ได้ของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ และการกระทำดังกล่าวมีลักษณะคล้ายกับการทำให้เสียทรัพย์ แต่การที่ความผิดฐานทำให้เสียทรัพย์ตามกฎหมายของประเทศต่างๆให้ความคุ้มครองเฉพาะแก่สิ่งที่มีรูปร่างเท่านั้น เมื่อข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ไม่ใช่สิ่งที่มีรูปร่าง การกระทำนั้นจึงไม่เป็นความผิดฐานทำให้เสียทรัพย์

การปลอมข้อมูลคอมพิวเตอร์

การปลอมข้อมูลคอมพิวเตอร์ (Computer forgery) คือการกระทำด้วยวิธีการใดๆ เช่น การปลอมข้อมูลคอมพิวเตอร์ทั้งหมด หรือแต่บางส่วน การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ที่แท้จริง การรบกวนการทำงานของระบบคอมพิวเตอร์ หรือการกระทำด้วยวิธีการอย่างอื่น เพื่อให้ผู้อื่นหลงเชื่อว่าข้อมูลนั้นเป็นข้อมูลที่แท้จริง

เมื่อพิจารณาถึงลักษณะของการปลอมข้อมูลคอมพิวเตอร์แล้ว จะเห็นว่านอกจากจะส่งผลกระทบต่อความครบถ้วนของข้อมูลแล้ว ยังส่งผลกระทบต่อกฎหมายอาญาของประเทศต่างๆอีกด้วย เนื่องจากความผิดฐานปลอมเอกสารตามกฎหมายอาญาของประเทศต่างๆครอบคลุมถึงเฉพาะกรณีที่เป็นการกระทำต่อข้อความที่สามารถอ่านได้ด้วยนัยน์ตา (Readability of statements) ที่ถูกนำมารวบรวมไว้ในเอกสารเท่านั้น มิได้รวมถึงการกระทำต่อข้อมูลคอมพิวเตอร์ด้วย

การฉ้อโกงทางคอมพิวเตอร์

The National Crime Authority ประเทศออสเตรเลีย กล่าวถึงเรื่องการฉ้อโกงทางคอมพิวเตอร์ว่า ปัญหาเรื่องการฉ้อโกงทางการเงินที่กำลังเกิดขึ้นกับภาคเอกชนในขณะนี้กำลังอยู่ในความสนใจของผู้เกี่ยวข้องทั้งหลาย แม้ว่าการประเมินค่าความเสียหายที่เกิดขึ้นจากการกระทำความผิดประเภทนี้เป็นเรื่องยาก แต่จากการประเมินค่าความเสียหายจากแหล่งข้อมูลต่างๆพบว่า ปัญหานี้เป็นปัญหาใหญ่ที่กำลังเกิดขึ้นทั่วโลก ทั้งอินเตอร์เนทและการทำพาณิชย์อิเล็กทรอนิกส์ได้เป็นปัจจัยที่ทำให้ปัญหาเรื่องการฉ้อโกงทางคอมพิวเตอร์ได้ขยายตัวเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่ง อินเตอร์เนทนั้น เป็นสถานที่ที่ดึงดูดใจให้มีการซื้อขายข้อมูลเกี่ยวกับบัตรเครดิต และมีการใช้ซาลามิเทคนิค (Salami technique) เป็นจำนวนมาก

เนื่องจากลักษณะของการกระทำที่เป็นการกระทำด้วยวิธีการใดๆต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ซึ่งทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม และเป็นเหตุให้ผู้กระทำได้ไปซึ่งทรัพย์สินหรือประโยชน์อื่นใดจากผู้อื่นโดยมิชอบด้วยกฎหมาย จึงเรียกการกระทำในลักษณะนี้ว่า “การฉ้อโกงทางคอมพิวเตอร์” (Computer fraud)

การฉ้อโกงทางคอมพิวเตอร์อาจแบ่งออกได้เป็น 2 ประเภทใหญ่ๆ คือ การฉ้อโกงข้อมูล (Data frauds) และการฉ้อโกงโปรแกรม (Programming frauds)

การฉ้อโกงข้อมูล คือ การกระทำต่างๆต่อข้อมูลในขั้นตอนต่างๆขณะที่คอมพิวเตอร์กำลังทำงาน ได้แก่ การแก้ไขเปลี่ยนแปลงข้อมูลที่จะนำเข้าไปในคอมพิวเตอร์ (Input data) การแก้ไขเปลี่ยนแปลงข้อมูลที่อยู่ในระบบคอมพิวเตอร์ โดยอาจเป็นกระทำในขณะที่คอมพิวเตอร์กำลัง ประมวลผล (Data processing) อยู่ หรือในขณะที่ข้อมูลกำลังอยู่ในขั้นตอนของการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์ก็ได้ และการแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลที่ถูกนำออกมาแล้ว (Output data)

เมื่อพิจารณาลักษณะของการฉ้อโกงทางคอมพิวเตอร์แล้ว จะเห็นว่า นอกจากจะส่งผลกระทบต่อ “สิทธิในทรัพย์สิน” ของเจ้าของทรัพย์สินแล้ว การฉ้อโกงทางคอมพิวเตอร์ยังส่งผลกระทบต่อกฎหมายอาญาของประเทศต่างๆอีกด้วย เนื่องจากความผิดฐานฉ้อโกงตามกฎหมายดังกล่าวสามารถใช้ดำเนินคดีกับการกระทำที่วัตถุแห่งการกระทำเป็น “มนุษย์” เท่านั้น ดังนั้น เมื่อการฉ้อโกงทางคอมพิวเตอร์เป็นการกระทำที่กระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ การกระทำนั้นจึงไม่เป็นความผิดฐานฉ้อโกง

3.1.2 กฎหมายต่างประเทศ

ก.กลุ่มประเทศ Common Law

1) ประเทศสหรัฐอเมริกา

1.1 การบูรณาข้อมูลด้านกระบวนการยุติธรรมของสหรัฐอเมริกา

การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมของสหรัฐอเมริกานั้น ไม่ว่าจะเป็นระดับรัฐบาลกลาง มลรัฐ หรือท้องถิ่น ก็จะมีการออกกฎหมายมารองรับในการแลกเปลี่ยนข้อมูลและการบูรณาการข้อมูลทั้งสิ้น กฎ ระเบียบ และ/หรือ กฎหมายของรัฐบาลกลาง อาจจะถูกมลรัฐ หรือ ท้องถิ่น นำไปใช้เป็นแนวทาง หรือ อาจถูกยกเว้นบางหลักเกณฑ์ หากขาดความเหมาะสมกับท้องถิ่นใดๆ เว้นแต่กฎ ระเบียบ หรือกฎหมายนั้นจะถูกจำกัดว่า ห้ามออกข้อยกเว้น หรือ ระบุไว้โดยเฉพาะว่า จะต้องมีองค์ประกอบ แม้ว่ากฎหมายของรัฐบาลกลางส่วนใหญ่จะมีข้อจำกัดในการเข้าถึงข้อมูลอิเลคโทรนิคส์ แต่ก็มีกฎหมายที่ได้ตราไว้ในอำนาจอย่างเป็นกลาง และเขียนไว้อย่างกว้างๆ

กฎหมายหลักของอเมริกาที่ตราไว้อย่างกว้างๆ และให้อำนาจในการบูรณาการและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรมได้แก่ The Code of Federal Regulations (CFR) โดยอยู่ในหมวด 28 CFR Part 23 : Criminal Justice History Information กระทรวงยุติธรรมของสหรัฐอเมริกา โดย Office of Justice Programs ได้นำมา

ประยุกต์ออกระเบียบควบคุมการดำเนินการเกี่ยวกับระบบข่าวกรองทางอาชญากรรม หรือ Criminal Intelligence System โดยดำเนินการร่วมภายใต้กฎหมาย The Omnibus Crime Control and Safe Streets Act of 1968 กฎหมายดังกล่าวได้มีการตราให้มีการดำเนินการออกแบบในการรับข้อมูล การเก็บรวบรวม และประมวลผลข้อมูลทั้งข้อมูลส่วนบุคคล และข้อมูลจากองค์กรต่างๆ บนฐานของหลักการที่เชื่อได้ว่าเป็นกิจกรรมการดำเนินการที่เกี่ยวข้องกับการประกอบอาชญากรรม (28 CFR S23.3 (b)) ระเบียบเหล่านั้น มีข้อสังเกตว่า ข้อมูลที่มีหลักฐานหรือเชื่อได้ว่า เป็นเครือข่าย (network) กับการประกอบอาชญากรรมก็สามารถที่จะดำเนินการเก็บรวบรวมข้อมูลได้ อย่างไรก็ตาม การเก็บรวบรวมข้อมูลก็จะต้องเป็นไปตามหลักการเรื่อง “intelligence Project” ที่ระบุว่า องค์กรใดๆหรือหลายๆองค์กรอาจรวบรวมและเก็บรักษาข้อมูลของบุคคลใด (individual) เฉพาะเมื่อมีเหตุผลอันควรสงสัยว่า บุคคลนั้นเกี่ยวข้องกับการประกอบอาชญากรรม หรือกิจกรรมที่เกี่ยวข้องกับอาชญากรรม[43] และข้อมูลนั้นต้องเกี่ยวข้องกับศาสนา การเมือง สมาคม หรือ ทัศนคติทางสังคม หรือ การดำเนินการใดๆ หากไม่มีความเกี่ยวข้องโดยตรงกับการประกอบอาชญากรรมจะไม่อนุญาตให้มีการรวบรวม โดยในการรวบรวมข้อมูลดังกล่าวต้องมีหลักฐานและข้อเท็จจริงเพียงพอที่จะเชื่อว่า บุคคลดังกล่าวเกี่ยวพันกับการประกอบอาชญากรรมหรือ มีส่วนรู้เห็น (28 CFR S23.20 (a)-(c))

การปกครองของประเทศสหรัฐอเมริกาประกอบด้วยรัฐบาลสหพันธรัฐ (Federal government) และรัฐบาลมลรัฐ (state government) ส่วนองค์กรทางด้านงานยุติธรรม ได้แก่ ตำรวจ อัยการ เรือนจำ ศาล ซึ่งแบ่งออกได้เป็นหลายระดับตั้งแต่ระดับสหพันธ์รัฐ ไปจนถึงมลรัฐ เขตและท้องถิ่น ทำให้การบริหารงานยุติธรรมของประเทศมีความซับซ้อน เนื่องจากความพร้อมทางเทคโนโลยีสานสนเทศไม่เท่ากัน รัฐบาลกลางและรัฐบาลท้องถิ่นใช้ซอฟแวร์แบบปิด หรือเป็นระบบเฉพาะของตนเองทำให้การเชื่อมโยงสานสนเทศเป็นไปได้ยาก นอกจากนี้ยังประสบปัญหาด้านกฎหมายในเรื่องความลับของข้อมูลส่วนบุคคลหรือ Privacy act

เพื่ออำนวยความสะดวกในการแลกเปลี่ยนข้อมูล กระทรวงยุติธรรมได้ดำเนินการจัดตั้งศูนย์ข้อมูลวิสาหกิจบริหารจัดการโดยส่วนกลาง อาทิเช่น ระบบอาชญายุติธรรม (CJIS) ศูนย์ข้อมูลอาชญากรรมแห่งชาติ (NCIC) และระบบข้อมูลที่รวบรวมลายพิมพ์นิ้วมือ (IAFIS) ศูนย์ข้อมูลดังกล่าวมีคณะทำงานดูแลตลอด 24 ชั่วโมง และให้บริการผ่านระบบเครือข่าย ทั้งแบบที่มีชั้นความลับสูง (classified) และแบบทั่วไป (SBU) ซึ่งหน่วยงานระดับท้องถิ่น รัฐและสหพันธรัฐสามารถขอใช้บริการได้

---

[43] Aspin Criminal Justice and Information Technology p.25

กระทรวงยุติธรรมยังได้จัดทำโครงสร้างข้อมูลมาตรฐานสำหรับกระบวนการยุติธรรม ที่เรียกว่า (Global Justice XML) ซึ่งนำเอาเทคโนโลยี XML มาใช้เป็นมาตรฐานในการแลกเปลี่ยนข้อมูล สำหรับหน่วยงานทั้งภาครัฐและเอกชนในการใช้ข้อมูลร่วมกันในระดับมลรัฐทั่วประเทศ มาตรฐาน Global Justice XML กำหนดส่วนประกอบสำคัญ[44] ดังต่อไปนี้

1. ความสัมพันธ์ของข้อมูลในขั้นตอนต่างๆ ของกระบวนการทำงาน (workflow)
2. เหตุการณ์ที่มักนำไปสู่การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน
3. หน่วยงานที่เกี่ยวข้องกับการส่งหรือรับ
4. เงื่อนไขและ ปัจจัย ที่ส่งผลต่อทิศทางการแลกเปลี่ยนข้อมูล
5. ข้อมูลข่าวสารที่แลกเปลี่ยนกันในกระบวนการทำงาน ได้แก่
   - หน่วยข้อมูลย่อยที่มีการแลกเปลี่ยน ได้แก่ ชื่อ นามสกุล เลขประกันสังคม เลขบัตรประจำตัว วันเกิดเหตุ ชื่อหน่วยงานต้นเรื่อง เป็นต้น
   - ชุดข้อมูล กลุ่มรายละเอียดย่อยๆ ที่เกี่ยวพันกันอย่างมีเหตุผล เช่น หลักฐานข้อมูลส่วนบุคคล ข้อกล่าวหา ข้อมูลคดี ข้อมูลความประพฤติ
   - เอกสารในรูปของกระดาษหรือสื่ออิเล็กทรอนิกส์ที่ประกอบด้วยชุดข้อมูลและรายละเอียดปลีกย่อย

เพื่อส่งเสริมการใช้มาตรฐานข้อมูล global Justice XML สมาคมข้อมูลสารสนเทศและสถิติแห่งชาติ หรือ SEARCH ได้สนับสนุนโครงการสร้างแบบจำลองการแลกเปลี่ยนข้อมูลยุติธรรม ซึ่งมุ่งเน้นการพัฒนาระบบบูรณาการข้อมูล และการนำไปสู่อนุวัติการ (implement) ทั่วประเทศ โดยผ่านระบบรักษาความปลอดภัยที่ต้องอาศัยการระบุตำแหน่งในการเข้าถึงข้อมูล คณะทำงานในโครงการได้พัฒนาเครือข่ายจำลองและวิธีการดึงข้อมูลรายละเอียดทั้งในแง่ของกระบวนการ เหตุการณ์ หน่วยงาน ข้อมูล และลักษณะการแลกเปลี่ยนที่สัมพันธ์กับการบูรณาการข้อมูลยุติธรรม ผลงานจากโครงการดังกล่าวได้เริ่มทดลองใช้งานแล้วใน 5 รัฐ คือ โคโลราโด แคนซัส มินเนโซต้า นิวเม็กซิโก และเพนซิลเวเนีย พร้อมทั้งได้เผยแพร่ไปยังศาลปกครองอีกกว่า 20 เขต

ภารกิจอีกประการของกระทรวงยุติธรรม คือ การรวบรวมข้อมูลสถิติที่เกี่ยวข้องกับอาชญากรรม อาชญากร เหยื่อผู้เคราะห์ร้าย และการทำงานของกระบวนการยุติธรรมในหลายๆระดับของรัฐบาล และนำเอาข้อมูลสถิติที่รวบรวมได้มาทำการวิเคราะห์ในด้านต่างๆ ตีพิมพ์ผลการวิเคราะห์และแสดงผลต่อหน่วยงานราชการและประชาชน

---

[44] ร่างแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 หน้า 14

นอกจากนี้รัฐบาลยังส่งเสริมให้มีการนำเทคโนโลยีแบบเปิด มาใช้ร่วมกับระบบเซิร์ฟเวอร์ที่มีราคาย่อมเยา แทนระบบปิดแบบเก่าที่ผูกขาดโดยผู้จำหน่ายเพียงไม่กี่ราย การพัฒนาระบบสารสนเทศใหม่มุ่งเน้นการใช้ซอฟต์แวร์มาตรฐาน (commercial-off-the-shelf) และหลีกเลี่ยงการพัฒนาระบบเฉพาะซึ่งยากแก่การดูแลรักษา การพัฒนาเทคโนโลยีสารสนเทศตามหลักการดังกล่าวจะส่งผลให้การแลกเปลี่ยนข้อมูลและการทำงานของแต่ละหน่วยงานเป็นไปได้ง่ายขึ้น

ยังมีแนวทางในการเก็บข้อมูลในกระบวนการยุติธรรมอีกประเภทหนึ่ง คือ “Biometrics” โดยแนวการดำเนินการแบบไบโอเมตทริคส์เป็นการเก็บรวบรวมข้อมูลด้านรูปพรรณสันฐาน ที่จะระบุตัวบุคคลหรือระบุเอกลักษณะของบุคคล เนื่องจากในอดีตเราใช้ลายพิมพ์นิ้วมือ (finger printing) เป็นการระบุเอกลักษณ์ของบุคคล (personel identification) และใช้มาเป็นนับศตวรรษ อย่างไรก็ตาม การใช้แนวทางแบบไบโอเมติคส์นี้จะให้ความชัดเจนและความรวดเร็วในการระบุตัวได้ชัดเจนมากกว่า โดยการใช้เทคนิคที่ ได้แก่ Facial recognition, iris scaning, retinal scanning และ voice recognition

การประยุกต์เทคนิคด้านการ biometric technology ที่นำมาใช้เร็วๆนี้ ในอเมริกาก็คือ การจัดระบบความปลอดภัยแก่โรงเรียน หรือ school safety โรงเรียนหลายๆแห่งใน New Jersey ใช้การทดสอบที่เรียกว่า T – PASS (Testing the Teacher – Parent Authorization Security System) ซึ่งในการนี้ กระทรวงยุติธรรมของสหรัฐอเมริกาได้จัดสรรงบประมาณ และดำเนินการเพื่อสร้างความปลอดภัยให้แก่โรงเรียนต่างๆ โดยการใช้เทคโนโลยีแบบ iris recognition technology มีระบบการทำงานคล้ายๆกับลายพิมพ์นิ้วมือในส่วนที่มีการจัดทำฐานข้อมูล (data base) โดยการบันทึกภาพม่านกระจกตาของบุคคล และเก็บรวมไว้ในฐานข้อมูลจากนั้นก็เชื่อมโยงเข้ากับข้อมูลส่วนบุคคล และกระทรวงยุติธรรมของสหรัฐได้มอบหมายให้ Maryland – based company 21st Century Solution (JUSTNET n.d) เป็นผู้ดำเนินการประเมินโครงการนี้

นอกจาก Biometric technology ยังมีการใช้ Bioagent detection ซึ่งในส่วนนี้ได้รับการสนับสนุนจากกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of homeland security) เพื่อใช้ในกลยุทธ์เพื่อการป้องกันอาชญากรรม เดิมแนวทางนี้ใช้ในการตรวจสอบโรคแอนแทรกซ์ (anthrax) แต่ได้นำมาประยุกต์ใช้เพื่อเก็บข้อมูลในการระบุยาเสพติดที่ผิดกฎหมาย เช่น กัญชา และโคเคน ตัวอย่างการนำเอามาใช้ คือ Aerosol Drug Detection and Identification Research Project ซึ่งใช้การพ่นสเปรย์เพื่อตรวจหายาเสพติดต่างๆในสถานที่ต่างๆเช่น โรงเรียน ซึ่งสามารถตรวจได้ทั้ง เฮโรอีน กัญชา โคเคน และแอมเฟตามีน

ความมุ่งหมายในการค้นหาก็คือ การเก็บข้อมูลตั้งแต่แรกเริ่มว่า พบยาเสพติดประเภทใด และที่ใด เช่น โต๊ะเรียน ห้องน้ำ สถานที่ใดเป็นสถานที่หลักที่ใช้มั่วสุมเสพยาเสพติด (the main locations of durg use) ความถี่ที่พบ เป็นต้น อย่างไรก็ตามปัญหาที่พบก็คือ เจ้าหน้าที่ที่ปฏิบัติงานที่โรงเรียนยังขาดความเข้าใจในการใช้เทคโนโลยีเพื่อการสืบสวนเหล่านี้ และอาจจะประสบปัญหากฎหมายที่เกี่ยวข้อง เมื่อเร็วๆนี้ The National Institute of Justice ได้วางนโยบายในการเก็บข้อมูลด้านงานยุติธรรมโดยใช้เทคโนโลยีดำเนินการด้วย

เราอาจกล่าวได้ว่า การตระหนักและเฝ้าระวังถึงการก่อการร้ายได้ส่งผลดีต่อเนื่องมาถึงการใช้เทคโนโลยีในการแลกเปลี่ยนข้อมูล ในกระบวนการยุติธรรม และการวางแผนการบูรณาการข้อมูลเพื่อป้องกันอาชญากรรม ทั้งการทบทวนแนวทางและข้อมูลเดิม การใช้วิธีการและเทคโนโลยีใหม่ๆ รวมไปถึงการมีหุ้นส่วนกับชุมชนในการร่วมดำเนินการ ทุกองค์กรยอมรับในหลักการร่วมกันว่า การแลกเปลี่ยนข้อมูลในระบบกระบวนการยุติธรรมนั้นจะทำให้เกิดความปลอดภัยแก่สังคมโดยส่วนรวม

ประวัติและพัฒนาการการบูรณาการข้อมูลระบบสารสนเทศในกระบวนการยุติธรรมในสหรัฐอเมริกานั้น อาจจำแนกได้เป็น 5 ยุคด้วยกัน คือ[45]

1. ยุคเริ่มต้น 100 ปี (ค.ศ. 1830 – 1930)
2. ยุคกรรมาธิการ Wickersham Commission (ค.ศ. 1931 – 1965)
3. ยุคกรรมาธิการของประธานาธิบดี (ค.ศ. 1965 – 1968)
4. ยุคการตรากฎหมายรัฐบาลกลาง (ค.ศ. 1968 – 1994)
5. ยุคปัจจุบัน (ค.ศ. 1995 – ปัจจุบัน)

1. ยุคเริ่มต้น 100 ปี (Historical Background The First 100 years)

โดยข้อเท็จจริงแล้ว ความต้องการข้อมูลเกี่ยวกับการประกอบอาชญากรรม ไม่ว่าจะเป็นตัวอาชญากรรม การประกอบอาชญากรรมและการลงโทษ นับมาตั้งแต่ก่อนสองศตวรรษที่ผ่านมา ซึ่งในปี ค.ศ. 1978 เดคเคอร์ (Decker) ได้ระบุว่า นักปรัชญาการเมืองเจ้าของแนวคิดทฤษฎีอรรถประโยชน์นิยม อย่าง เบนแธม (Teremy Bentham) ได้เคยพยายามรวบรวมข้อมูลเกี่ยวกับนักโทษชาวอังกฤษ (British prisoners) มาตั้งแต่ปี ค.ศ. 1778 แล้วแต่

---

[45] Dunworth Terrance *"Criminal Justice and the it Revolution"* **Federal Probation**. P.4

ก็ปรากฏหลักฐานว่าระบบสถิติข้อูลการประกอบอาชญากรรมของฝรั่งเศสที่ดำเนินการโดย Guerry ในปี ค.ศ. 1833 และ Quetelet ซึ่งได้วิพากษ์ระบบการจัดเก็บข้อมูลทางสถิติเกี่ยวกับอาชญากรรมของฝรั่งเศสว่ามีจุดอ่อนและจุดแข็งในด้านใดบ้าง เป็นข้อมูลที่มีการจัดเก็บรวบรวมและดำเนินการอย่างเป็นระบบมากกว่า

เดคเคอร์ได้ให้ข้อสังเกตว่า ในสหรัฐอเมริกานั้นความพยายามที่จะพัฒนาระบบข้อมูลเกี่ยวกับอาชญากรรมต้องสืบค้นย้อนหลังไปราวศตวรรษครึ่ง (ประมาณ 150 ปี) ในปี ค.ศ. 1834 แมสซาชูเซส เป็นมลรัฐแรกที่เริ่มต้นรวบรวมข้อมูลเกี่ยวกับการประกอบอาชญากรรม ในเวลาเดียวกันกับที่รัฐบาลกลางก็ได้เริ่มดำเนินการ และในปี ค.ศ. 1835 ได้มีการจัดทำสำมะโน (Census) เริ่มแรกเกี่ยวกับข้อมูลผู้ประกอบอาชญากรรม ซึ่งในเวลาต่อมาก็ได้กลายมาเป็นต้นแบบการจัดทำสำมะโนในด้านอาชญากรรมในเวลาต่อมา ต้นปี ค.ศ. 1900 ได้มีข้อมูลจากการรายงานของตำรวจที่ถูกเก็บรวบรวมและจัดหมวดหมู่เพื่อรายงานเป็นสถิติการประกอบอาชญากรรม (Criminal Statistical Reports) รวมไปถึงการเริ่มดำเนินการเกี่ยวกับข้อมูลด้านผู้ต้องขังโดยหน่วยงานของรัฐบาลกลาง และฝ่ายศาลก็มีการจัดการรวบรวมทำสถิติเกี่ยวกับรายงานของศาลตีพิมพ์เผยแพร่ โดยสำนักงานอัยการสูงสุดของอเมริกา [46]

อย่างไรก็ตาม แม้ว่าข้อมูลการรวบรวมต่างๆ เหล่านั้นจะกลายเป็นบรรทัดฐานและมาตรฐานการขยายการเก็บรวบรวมข้อมูลต่างๆ ก็ตาม แต่ข้อมูลต่างๆ เหล่านั้นกลับถูกใช้เพียงแค่ 2 ลักษณะ คือ เป็นข้อมูลประกอบการพิจารณาคดีศาลและเป็นข้อมูลเพื่อประกอบการตัดสินใจในการอนุมัติงบประมาณ และการจัดสรรทรัพยากรต่างๆ ให้แก่หน่วยงานที่เกี่ยวข้องเท่านั้น ยังไม่ถูกนำมาใช้แลกเปลี่ยนและบูรณาการข้อมูลร่วมกันแต่อย่างใด ข้อมูลเหล่านั้นยังถูกจำแนกการจัดเก็บเป็นข้อมูลเกี่ยวกับการประกอบอาชญากรรมในเขตเมืองด้วย ทั้งนี้อาจจะเป็นเพราะหน่วยงานที่ทำหน้าที่ในการบังคับใช้กฎหมายยังขาดทรัพยากรต่างๆ และขาดความสนใจที่จะรวบรวมและประมวลข้อมูล รวมทั้งความรอบรู้ในการประกอบอาชญากรรมอื่นๆ ที่ยากและซับซ้อน ยังขาดและควมล้าหลังของสภาพแวดล้อมของกระบวนการยุติธรรมในท้องถิ่นต่างๆ

ในปี ค.ศ. 1920 The International Association of Chiefs of Police (IACP) ได้ตอบสนองความต้องการในการเก็บรวบรวมข้อมูลโดยการจัดทำแบบฟอร์ม (uniform) ที่เป็นระบบในการรวบรวมสถิติการประกอบอาชญากรรมที่สามารถนำไปใช้ได้ทั่วประเทศ โดย

---

[46] The Office of the U.S., Attorney General p.27

การพัฒนารูปแบบของแบบฟอร์มที่เรารู้จักกันดี คือ UCRs (Uniform Crime Reporting System) หน่วยงานในกรมตำรวจได้กระตุ้นให้มีการเก็บรวบรวมข้อมูลเกี่ยวกับการประกอบอาชญากรรมในรูปแบบที่เป็นมาตรฐาน ในปี 1930 IACP ได้ร่วมมือกับรัฐบาลกลางในการถ่ายโอนข้อมูลตามระบบนี้ให้กับ FBI (Federal Bureau of Investigation) และ UCR report ได้รวมข้อมูลจาก 1002 เมือง โดยร้อยละ 83 มีจำนวนอาชญากรรมเพิ่มขึ้นมากกว่า 25,000 ราย

2. ยุคกรรมาธิการ Wickersham Commission (ค.ศ. 1931 – 1965)

ในปี 1929 เป็นช่วงปีเดียวกับที่มีการเริ่มดำเนินการ UCR ประธานาธิบดีฮูเวอร์ (Hoover) ได้แต่งตั้งคณะกรรมาธิการ National Commission on Law Observance and Enforcement ซึ่งคณะกรรมาธิการชุดนี้รู้จักกันในนาม “Wickersham Commission” อันเป็นการตั้งชื่อตามชื่อของประธานคณะกรรมาธิการคือ George W. Wickersham ได้ทำการศึกษาและประเมินผลระบบกระบวนการยุติธรรมของประเทศ แม้ว่าก่อนหน้านี้จะมีการพยายามศึกษา และประเมินผลกระบวนการยุติธรรมในรอบ 10 ปีก็ตาม แต่คณะกรรมมาธิการชุดนี้ถือเป็นชุดระดับชาติ

ในเดือนมิถุนายน 1930 ได้มีการจัดทำรายงาน 13 ฉบับ และหนึ่งในจำนวนนั้นมีรายงานว่าด้วยสถิติอาชญากรรมเพื่อเป็นการประเมินและตรวจสอบความถูกต้องชัดเจน และการจัดทำระบบสถิติอาชญากรรมในระดับชาติและในกระบวนการยุติธรรม รายงานดังกล่าวได้สะท้อนให้เห็นถึงอิทธิพลของงานด้าน IACP และ UCR อย่างไรก็ตาม สมาชิกของคณะกรรมาธิการก็ต้องให้รายงานได้พัฒนาก้าวหน้าไปมากกว่าของ UCR โดยการสร้างระบบประมวลผลข้อมูลระดับชาติเกี่ยวกับโทษ ข้อมูลด้านศาล ด้านตำรวจ รายงานต่าง ๆดังกล่าวยังได้มีการจัดเก็บสำรองเกี่ยวกับสถิติอาชญากรรมไว้อย่างเป็นระบบ และมีการตีความข้อมูลเพื่อนำไปใช้ประโยชน์ทางด้านนโยบาย

3.ยุคกรรมาธิการประธานาธิบดี (Presidential Commission)

ระบบข้อมูล UCR นั้นอาจจะเรียกได้ว่าเป็นระบบข้อมูลที่ได้รับการยอมรับว่ามีขอบข่ายระดับชาติ แต่ก็ยังมีความก้าวหน้าและพัฒนาไปไม่มากนัก ในปี 1938 สำนักงานศาลยุติธรรมของสหรัฐ (The Administrative Office of the U.S. Courts) ได้มีการจัดเก็บรวบรวมข้อมูลระบบการลงโทษและระบบการดำเนินคดีของศาลโดยมีการจัดตั้งหน่วยงานใหม่ขึ้นมารองรับ ในการทำหน้าที่รวบรวมและประมวลผลข้อมูล รวมถึงการรายงานข้อมูลที่เป็นปัจจุบัน

ในปี 1965 ประธานาธิบดีจอห์นสัน ได้จัดตั้งคณะกรรมาธิการ ชื่อ “Commission on Law Enforcement and Administration of Justice” เพื่อให้ดำเนินการวิเคราะห์ข้อมูลด้านอาชญากรรม คณะกรรมาธิการชุดนี้มีอำนาจในการดำเนินการอย่างไม่จำกัด ซึ่งในการดำเนินการตรวจสอบระบบข้อมูลข่าวสารและสถิตินั้น รองผู้อำนวยการคณะกรรมาธิการ คือ Henry Ruth ได้กล่าวว่า เมื่อคณะกรรมาธิการเริ่มทำงานตรวจสอบจริงดูเหมือนว่าข้อมูลในด้านกระบวนการยุติธรรมไม่ได้ปรากฏอยู่จริงและจากการสุ่มสำรวจข้อมูลจากบ้านเรือนต่างๆ หลายๆแห่งก็พบว่า มีข้อมูลจำนวนมากไม่ได้มีการแจ้งความกับตำรวจ ซึ่งก็หมายความว่า ข้อมูลที่แจ้งระบุใน UCR ก็จะเป็นเสมือนแค่ยอดปลายของภูเขาน้ำแข็ง ซึ่งก็ยังไม่ใช่ข้อมูลที่จะบอกได้ถึงระดับการก่ออาชญากรรมที่แท้จริงของประเทศ ซึ่งคณะกรรมาธิการชุดนี้ระบุว่า หน่วยงานที่จะทำหน้าที่เก็บรวบรวมและพัฒนาข้อมูลควรจะเป็น National Criminal Justice Statistics Center มากกว่าจะเป็นตำรวจ และศูนย์ข้อมูลนี้ควรจะทำหน้าที่ในการจัดเตรียมข้อมูลและสนับสนุนข้อมูลต่างๆเหล่านี้แก่หน่วยงานรัฐในด้านกระบวนการยุติธรรมเพื่อให้มีการนำเอาข้อมูลนี้ไปใช้และช่วยให้บรรลุวัตถุประสงค์ในงานของหน่วยงาน

4. ยุคการตรากฎหมายของรัฐบาลกลาง (Federal Legislation: 1968–1994)

ผลพวงของงานของกรรมาธิการดังกล่าวก่อให้เกิดการผ่านกฎหมาย Omnibus Crime Control and Safe Street Act of 1968 เพื่อเป็นต้นแบบของการบังคับใช้กฎหมายทั้งในระดับมลรัฐและระดับท้องถิ่น กฎหมายฉบับดังกล่าว ได้กำหนดให้มีการจัดตั้งสำนักบริหารช่วยในการบังคับใช้กฎหมาย หรือ The Law Enforcement Assistance Administration ตั้งแต่ปี 1968 จนกระทั่งในปี 1974 จึงได้มีการจัดตั้ง National Institute of Law Enforcement and Criminal Justice (ซึ่งปัจจุบันก็คือ National Institute of Justice) และ National Justice Information and Statistics Service (ปัจจุบันคือ Bureau of Justice Statistics) โดยมี LEAA ให้การช่วยเหลือและในปี 1973 มีการจัดทำ National Crime Survey

1.2 กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

โดยข้อเท็จจริงแล้ว แม้ว่าสหรัฐอเมริกาจะมีการแลกเปลี่ยนข้อมูลเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม แต่ก็มิได้มีกฎหมายเฉพาะในการการแลกเปลี่ยนข้อมูลเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม อย่างไรก็ตาม สหรัฐอเมริกาเป็นประเทศที่มีระบบกฎหมายแบบ Common law ที่มีการพัฒนาและออกกฎหมายและสามารถปรับมารองรับการจัดทำฐานข้อมูลและการเชื่อมต่อบูรณาการข้อมูลในกระบวนการยุติธรรม โดยมีการกำหนด

มาตการต่างๆพบกฎหมายที่จำเป็นและวางแนวทางการดำเนินการอย่างเป็นระบบ ซึ่งกฎหมายเหล่านี้ได้แก่

1) The Crime Identification Technology Act of 1998 (CITA), Pub. L. No. 105-251, 112 Stat.1871 (1998), codified at 42 USC Section 14601 et seq.;

กฎหมายฉบับนี้เป็นกฎหมายของสหรัฐอเมริกาที่มีบทบัญญัติที่ครอบคลุมเกี่ยวกับการเชื่อมต่อและการบูรณาการข้อมูลและรวมทั้งการแลกเปลี่ยนข้อมูลในหน่วยงานในกระบวนการยุติธรรมมากที่สุด ฉบับหนึ่ง โดยเน้นการแลกเปลี่ยนและการบูรณาการข้อมูลในหน่วยงานในกระบวนการยุติธรรม ซึ่งเป็นหน่วยงานที่จะต้องใช้ข้อมูลร่วมกันทั้งในการป้องกันและการปราบปรามอาชญากรรม และการดำเนินคดีซึ่งสหรัฐอเมริกามีการออกกฎหมายนี้ โดยมุ่งให้มีผลต่อการปรับปรุงประสิทธิภาพการดำเนินการด้านกระบวนการยุติธรรมที่เน้นเกี่ยวกับเทคโนโลยีสารสนเทศ คือ ***The Crime Identification Technology Act 1998*** โดยกฎหมายฉบับนี้ได้ให้รัฐสภาตัดงบประมาณรายจ่ายจำนวน 250 ล้านเหรียญอเมริกันต่อปี ติดต่อกันเป็นเวลา 5 ปี (รวมราว 1.25 พันล้านเหรียญอเมริกัน) เพื่อให้มลรัฐต่างๆ ได้ส่งเสริมการบูรณาการข้อมูลในระบบกระบวนการยุติธรรมโดยใช้เทคโนโลยีเฉพาะ

นอกจากการกำหนดให้มีการจัดสรรงบประมาณรายจ่ายประจำปีให้แล้วยังระบุให้หน่วยงานที่ทำหน้าที่ในการบังคับใช้กฎหมายด้านกระบวนการยุติธรรม เช่น ศาล อัยการ ราชทัณฑ์ ฯลฯ ได้มีการแลกเปลี่ยนข้อมูลและการสื่อสารในด้านข้อมูลให้มีประสิทธิภาพมากขึ้นบนหลักของการกำหนดเวลาที่แท้จริง (real – time basis) ด้วย รัฐบาลในมลรัฐต่างๆ สามารถขอทุนสนับสนุน (grants) ในการดำเนินการเข้าร่วมโครงการระดับชาติที่รัฐบาลกลางได้ดำเนินการ เช่น โครงการ The Integrated Automated Fingerprint Identification System โครงการ The National Crime Information Center 2000 หรือโครงการ National Incident – Based Reporting System project เป็นต้น[47] ทั้งนี้รัฐใดที่จะเข้าร่วมจะต้องมีการกำหนดยุทธศาสตร์ในการแลกเปลี่ยนข้อมูล มีแผนกลยุทธ์ และการใช้เทคโนโลยีสารสนเทศ

อย่างไรก็ตาม การบูรณาการข้อมูลนั้น อาจมีความหมายถึงการที่หน่วยงานใดหน่วยงานเดียว เป็นผู้บูรณาการข้อมูลด้านต่างๆ ในกระบวนการยุติธรรมก็ได้ หรือ อาจหมายถึง การบูรณาการข้อมูลด้านเดียว แต่หลายหน่วยงานก็ได้ แต่การดำเนินการจะต้องผ่านกระบวนการสร้างมาตรฐานข้อมูล (Data Standardization) ก่อน

---

[47] April Pattavina **Information Technology and Criminal justice System** p.198

กฎหมายฉบับนี้มีที่มาจากต้องการดำเนินมาตรการใดๆเพื่อสร้างความปลอดภัยแก่สาธารณะ (public safety) และถือเป็นส่วนหนึ่งของกฎหมายมหาชนแบบ Public Law 105 -251 จุดเด่นของตัว พระราชบัญญัติ The Crime Identification Technology Act of 1993 นี้มีเป้าหมาย ก็คือ เพิ่มการส่งเสริมการบูรณาการข้อมูลข่าวสารในระบบกระบวนการยุติธรรม และใช้เทคโนโลยีในการระบุเอกลักษณ์ ทั้งนี้กฎหมายฉบับนี้ อนุญาตให้หน่วยงานทุกหน่วยงานในกระบวนการยุติธรรม (หน่วยงานที่ทำหน้าที่ในการบังคับใช้กฎหมาย ศาลยุติธรรม อัยการ ราชทัณฑ์) มีการแลกเปลี่ยนข้อมูลให้มีประสิทธิภาพมากยิ่งขึ้นบนหลักการเรื่อง “real – time basis”

กฎหมายนี้ยังจัดสรรงบประมาณให้มลรัฐต่างๆได้ดำเนินการเข้าร่วมในโครงการระดับชาติเช่น ระบบ Integrated Automated Fingerprint Identification System หรือร่วมใน ศูนย์ขอ้มูลอาชญากรรมระดับชาติ (The National Crime Information Center) หรือโครงการ The National Incident – Based Reporing System Project” ทั้งนี้มลรัฐต่างๆต้องจัดทำ ระบบการแลกเปลี่ยนข้อมูล และพัฒนาแผนกลยุทธ์รวมทั้งการนำเอาเทคโนโลยีมาใช้ในการบูรณาการข้อมูล

2) The Brady Handgun Violence Prevention Act (Brady Act), Pub. L. No. 103-159, 107 Stat.1536 (1993), codified as amended at 18 U.S.C. Section 921 et seq.;

ในบรรดาคดีอุฉกรรจ์ (Violent Crime) ที่เกิดขึ้นในอเมริกานั้นพบข้อเท็จจริงว่า มีการใช้อาวุธปืนร่วมด้วยเกือบทุกครั้ง ดังนั้น กฎหมายฉบับนี้จึงมุ่งที่จะให้มีการขึ้นทะเบียนผู้ที่ค้าอาวุธปืน และผู้ที่มีอาวุธปืนไว้ในครอบครอง ตลอดจนมีการตรวจสอบการครอบครองอาวุธปืน รวมถึงมาตรการต่างๆ เช่น การต้องมาต่อทะเบียนอาวุธปืนที่ครอบครองทุก 2 ปี เป็นต้น การขึ้นทะเบียนอาวุธปืนจะสามารถจำแนกประเภทอาวุธปืนได้ว่า มีบุคคลใดครอบครองอาวุธปืนชนิดใด มีอานุภาพร้ายแรงมากน้อยเพียงใด แม้จะเป็นปืนพกก็ตาม

3) the National Child Protection Act of 1993 (NCPA), Pub. L. No. 103-209, 107 Stat. 2490 (1993), codified as amended at 42 U.S.C. Sections 3759, 5101 note, 5119, 5119a, 5119b, 5119c;

กฎหมายฉบับนี้มุ่งที่จะให้มลรัฐต่างๆได้ส่งข้อมูล “การประกอบอาชญากรรมที่มีการแสวงหาผลประโยชน์และล่วงละเมิดเด็ก” (Child abuse crime information) หรือ ดัชนีชี้วัดข้อมูลดังกล่าวในทะเบียนประวัติอาชญากรระดับชาติที่ FBI จัดเก็บ ดังนั้นถือเป็น

หน้าที่ของมลรัฐในการที่จะต้องจัดทำมาตรฐานด้านความปลอดภัยและการเข้าถึงข้อมูลดังกล่าวด้วย เช่น ใช้ระบบลายพิมพ์นิ้วมือของผู้ที่จะขอเข้าใช้ เป็นต้น และข้อมูลที่จัดเก็บแม้จะเริ่มที่เด็กและเยาวชนที่ตกเป็นเหยื่อก็ตาม แต่เมื่อครบถ้วนสมบูรณ์แล้วก็จะต้องเพิ่มเติมด้านผู้สูงอายุและผู้ทำการเข้าไปด้วย หน่วยงานนอกกระบวนการยุติธรรม ที่เป็นองค์กรกุศลสาธารณะที่ทำงานอาสาสมัครเพื่อช่วยเหลือเด็กสามารถเข้ามาขอใช้ข้อมูลนี้ได้

4) The Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act), Pub. L. No. 90 351, 82 Stat. 197 (1968), codified as amended at 42 U.S.C. Section 3711 et seq., as amended;

เดิมรัฐสภาอเมริกันได้ผ่านกฎหมาย เกี่ยวกับการดักฟังโทรศัพท์ (Wire tap Act) ซึ่งระบุให้การดักฟังโทรศัพท์จะต้องมีการขออนุญาตจากศาล และมีเหตุอันควร (probable cause) ที่จะเชื่อว่าบุคคลนั้นประกอบอาชญากรรม อย่างไรก็ตามกฎหมายฉบับดังกล่าวก็ยังไม่ครอบคลุมเทคโนโลยีใหม่ๆ จึงมีการออกกฎหมาย Electronic Communication Privacy Act (ECPA) 1986 ขึ้นมาแก้ไขกฎหมาย Wire Tap Act ให้ขยายครอบคลุมความก้าวหน้าทางเทคโนโลยี นอกจากนี้ยังมีการป้องกันการใช้ Pen Registers ซึ่งเป็นเทคโนโลยีใหม่ในการเก็บข้อมูล โดยเฉพาะอย่างยิ่งการเก็บรักษาข้อมูลด้านการสืบสวนสอบสวน ในปี 1994 มีการออกกฎหมายชื่อ The Communication Assistance for Law Enforcement Act (CALEA) ที่ผนวกเอากฎหมายทั้ง Wire Tap Act กับ ECPA เข้าด้วยกันตลอดรวมทั้งกฎหมาย Privacy Protection Act of 1980 และการพัฒนา The Omnibus Crime Control and Safe Streets Acts. ที่เกิดคำถามว่า ข้อมูลจากการดักฟังโทรศัพท์หรือการล่อซื้อจะใช้เพื่อการดำเนินคดีและควรมีการเก็บรักษาไว้ หรือไม่อย่างไร สามารถที่จะบูรณาการหรือเชื่อมโยงเข้ากับฐานข้อมูลอื่นได้หรือไม่ เป็นต้น

5) the Violent Crime Control and Law Enforcement Act of 1994 (Violent Crime Control Act), Pub. L. No.103 322, 108 Stat. 1796 (1994), codified as amended at 42 U.S.C. Section 13701 et seq., which pertain to the establishment,maintenance, analysis, or use of criminal history records and criminal record systems;

กฎหมายฉบับนี้เกิดจากการทำงานอย่างหนักตลอด 6 ปีของคณะกรรมาธิการยกร่าง กฎหมาย ด้านอาชญาวิทยาและงานยุติธรรม เป็นกฎหมายที่ระบุถึงการประกอบอาชญากรรมที่จะต้องเป็นภารกิจของรัฐ ซึ่งนอกจากจะให้รัฐจัดสรรงบประมาณในการรับเจ้าหน้าที่ตำรวจใหม่ ราว 1 แสนนาย แล้ว ยังจัดตั้งกองทุนเพื่อผู้ต้องขัง และจัดสรร

งบประมาณเพื่อดำเนินโครงการต่างๆในการป้องกันอาชญากรรม เนื้อหาของกฎหมายฉบับนี้ประกอบด้วย การห้ามการมีอาวุธร้ายแรง การเพิ่มการประหารชีวิต จำกัดการซื้อขายอาวุธและการออกใบอนุญาตมีอาวุธปืน การฉ้อโกง แก๊งค์อาชญากร การลักลอบเข้าเมืองมาประกอบอาชญากรรมการกระทำผิดของเด็กและเยาวชน การขึ้นทะเบียนอาชญากรทางเพศที่กระทำผิดร้ายแรง และกระทำผิดซ้ำ การห้ามการพักการลงโทษแก่อาชญากรที่กระทำผิดข้อหายาเสพติด และยังมีด้านเหยื่อหรือผู้เสียหาย ตลอดจนโครงการช่วยเหลือเหยื่อ และอาชญากรรมที่เกิดจากความเกลียดชัง (hate crime) รวมทั้งความรุนแรงในครอบครัว

สำหรับในส่วนของการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมกฎหมายฉบับนี้ ก็คือ กฎหมายฉบับนี้ให้รัฐต่างออกกฎหมายให้มีการลงทะเบียนข้อมูลประวัติอาชญากรทางเพศ ที่กระทำผิด และถูกคุมขัง หลังจากถูกปล่อยตัวไปแล้ว 10 ปี และที่สำคัญคือ ไม่เพียงแต่มลรัฐและหน่วยงานที่เกี่ยวข้องจะต้องมีการจัดทำทะเบียนข้อมูลผู้กระทำผิดดังกล่าวเท่านั้น แต่ยังมีการกำหนดโทษแก่หน่วยงาน หรือรัฐที่ไม่ได้มีการดำเนินการขึ้นทะเบียนข้อมูลดังกล่าวด้วย โดยการตัดงบประมาณการช่วยเหลือลง ในขณะเดียวกันก็จัดสรรงบประมาณ เพื่อช่วยให้มลรัฐต่างๆดำเนินการพัฒนาฐานข้อมูลด้วย เพื่อให้การดำเนินการมีความครบถ้วนในช่วงสิ้นปีจะมีคณะกรรมการที่ตั้งขึ้น (Task Force) มาตรวจสอบความถูกต้องของข้อมูล และให้คำแนะนำในการพัฒนาฐานข้อมูลตลอดจนการเชื่อมต่อข้อมูลกับหน่วยงานอื่นๆรวมทั้งการจัดทำรายงานเสนอเพื่ออนุมัติงบประมาณต่อไป

6) Relevant requirements of the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act, Pub. L. No. 103-322, 108 Stat. 2038,

กฎหมายฉบับนี้เป็นกฎหมายที่รัฐบาลกลางให้อำนาจแก่มลรัฐในการที่จัดเก็บข้อมูลที่เกี่ยวกับบุคคลที่มีการล่วงละเมิดทางเพศแก่เด็กและยังมีบทบัญญัติที่ให้สามารถเข้าถึงข้อมูลข่าวสารเกี่ยวกับผู้กระทำความผิด ในขณะเดียวกันยังให้อำนาจแก่เจ้าหน้าที่ในการสอบปากคำผู้ต้องหาว่าข้อมูลที่เป็นปัจจุบันที่สุด กฎหมายฉบับนี้เป็นกฎหมายที่มีบทบัญญัติยกเว้นการปกป้องข้อมูลส่วนตัวของจำเลยผู้กระทำผิดทางเพศแก่เด็ก ซึ่งโดยปกติแทบจะไม่มีกฎหมายฉบับใดเลยที่จะยกเว้นการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้กฎหมายฉบับนี้ยังให้อำนาจแก่อัยการสูงสุดของสหรัฐอเมริกาในการอนุญาตให้รัฐต่างๆที่มีความประสงค์จัดเก็บรวบรวมข้อมูลและนำกฎหมายฉบับนี้ไปใช้กับการประกอบอาชญากรรมที่กระทำต่อชนกลุ่มน้อย ซึ่งนั่นหมายความว่ารัฐต่างๆสามารถที่จะทำการลงทะเบียนอาชญากรที่เกิดขึ้นจากการกระทำผิดต่อชนกลุ่มน้อยซึ่งส่วนใหญ่เป็นอาชญากรรมที่เกิดจากความเกลียดชัง (Hate Crime) ในรอบ 10 ปีในขณะเดียวกันผู้ที่กระทำผิดซ้ำตั้งแต่ 2 ครั้งขึ้นไปในคดีที่เกี่ยวกับการประกอบ

อาชญากรรมทางเพศจะถูกส่งรายชื่อแจ้งที่อยู่และการเดินทางเข้าออกให้มลรัฐต่าง ๆทราบ กฎหมายฉบับนี้ยังกำหนดให้ผู้กระทำความผิดทางเพศในคดีอุกฉกรรจ์หรือใช้ความรุนแรงที่ได้รับความทุกข์ทรมานจากความผิดปกติทางจิต จะต้องถูกลงทะเบียนเป็นผู้รับการเฝ้าระวังเป็นกรณีพิเศษ

7) Megan's Law, Pub.L. No. 104-145, 110 Stat. 1345,

Megan's Law เป็นกฎหมายของมลรัฐเพนซิลวาเนีย จากฝ่าย Megan Law Section โดยระบุให้ตำรวจของมลรัฐต้องจัดทำและดูและข้อมูลการเปลี่ยนแปลงการลงทะเบียนของบุคคลที่เข้ามาอาศัยในพื้นที่ (ต่างจากทะเบียนราษฎร์ตรงที่ผู้ที่มีชื่อในทะเบียนบ้าน กับผู้เข้ามาอยู่อาศัยจริงในพื้นที่) ไม่ว่าเข้ามาทำงาน เรียน โดยเฉพาะวัยรุ่นที่เคยประกอบอาชญากรรมทางเพศ กฎหมายฉบับนี้จะมีส่วนในการส่งเสริม ให้มีการตรวจสอบและเทียบเคียงกับข้อมูลในหน่วยอื่น ๆที่มีการเก็บรวบรวมข้อมูล ซึ่งการดำเนินการดังกล่าว เมื่อมีการเชื่อมโยงข้อมูลกับข้อมูลในหน่วยงานอื่น ๆที่เก็บรักษาจะช่วยทำให้ข้อมูลที่ทันสมัยมากยิ่งขึ้น และการเชื่อมโยงข้อมูลจะช่วยทำให้สามารถป้องกันการก่ออาชญากรรมได้

8) The Pam Lychner Sexual Offender Tracking and Identification Act of 1996, Pub. L. No. 104-236, 110 Stat. 3093;

กฎหมายฉบับนี้ได้มอบหมายให้สำนักงานอัยการสูงสุดได้มีการดำเนินการจัดทำฐานข้อมูลระดับชาติโดยประสานงานกับ FBI ตามกฎหมาย Title 42 ของ United States Code Section 14072 ทั้งนี้มีศูนย์ข้อมูลหลักคือ The National Crime Information Center (NCIC) ดำเนินการลงทะเบียน อย่างไรก็ตาม การจัดเก็บและลงทะเบียนดังกล่าวเป็นการกระทำเฉพาะข้อมูลเกี่ยวกับผู้กระทำผิดในทางเพศเท่านั้น แต่จะมีรายละเอียดครบถ้วน ตั้งแต่สถานที่อยู่ ลายพิมพ์นิ้วมือ ภาพถ่าย และหากผู้กระทำผิดทางเพศ ได้กระทำผิดทางเพศซ้ำอีกก็จะถูกเชื่อมโยงส่งไปยังหน่วยงานต่าง ๆที่เกี่ยวข้อง เพื่อให้สาธารณชนช่วยสอดส่อง การจัดทำข้อมูลที่รู้จักกันในนาม “SOR” (Sex Offender Registry)

9) The Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386, 114 Stat. 1464 (2000) and related laws pertaining to the identification, collection, analysis and interstate exchange of records relating to domestic violence and stalking (including protection orders).

ในการต่อสู้กับอาชญากรรมประเภทเกี่ยวกับการค้าผู้หญิงและเด็กนั้น สหรัฐอเมริกาตระหนักในเรื่องนี้อย่างยิ่ง เนื่องจากพบว่า ผู้หญิงและเด็กถูกนำมาค้าเป็นทาส

และทางเพศในอเมริกา โดยการข้ามพรมแดนสูงถึงราว 7 แสนคน และราว 5 หมื่นคน ถูกนำมาค้าในอเมริกา ปัญหานี้เป็นปัญหาหนัก ในคดี United States V. Kozminskic 1988) ศาลสูงของอเมริการะบุว่า กฎหมายเดิมที่มีอยู่ คือ Section 1584 ของ title 18 United State Code มีบทบัญญัติที่ไม่เพียงพอต่อการนำมาใช้โดยเฉพาะการนำตัวผู้กระทำผิดมาขึ้นศาล และมีการตัดสินบนเจ้าหน้าที่ทำให้การปราบปรามยากจึงมีการออกกฎหมายนี้ขึ้นมา ซึ่งนอกจากจะมีมาตรการต่างๆขึ้นมาป้องกันและปราบปราม การช่วยเหลือเหยื่อ ก็จะมีการให้หน่วยงานที่เกี่ยวข้อง ทำการเก็บรวบรวมและประมาณข้อมูลที่เกี่ยวข้อง พร้อมทั้งจัดทำรายงานประจำปี (Annual Report) เสนอ หน่วยงานที่เกี่ยวข้องและยังมีการส่งข้อมูลให้ฝ่ายตรวจคนเข้าเมืองประสานการข้ามเดินทางเข้าประเทศแก่บุคคลที่ขึ้นบัญชีดำการค้าผู้หญิง และเด็กและให้ตรวจสอบผู้เสียหายที่เดินทางด้วย ตลอดจนรวบรวมพฤติกรรมและจัดทำพัฒนาฐานข้อมูล

1.3 ฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประเทศสหรัฐอเมริกาเป็นหนึ่งในประเทศแรกๆ ที่นำเอาหลักความเป็นอิสระของข้อมูลข่าวสารมาปรับใช้ต่อจากประเทศสวีเดน โดยได้ประกาศใช้เป็นกฎหมายที่รับรองสิทธิดังกล่าวในปี 1966 ในช่วงเวลานั้น อาจกล่าวได้ว่าวัฒนธรรมการเปิดเผยข้อมูลได้พัฒนาขึ้นภายในรัฐบาลแล้ว โดยจะเห็นชัดได้จากการประกาศใช้กฎหมายหลายฉบับ ได้แก่ พระราชบัญญัติความเป็นอิสระของข้อมูล (Freedom of Information Act) การเกิดขึ้นของกิจกรรมต่างๆ โดยนักเคลื่อนไหวทางการเมือง การประกาศใช้พระราชบัญญัติความเป็นส่วนตัว (The Privacy Act) ที่ให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่หน่วยงานราชการต่างๆ มีอยู่ พระราชบัญญัติรัฐบาลในแสงอาทิตย์ (The Government in the Sunshine Act) ซึ่งกำหนดให้มีการเปิดเผยข้อมูลของหน่วยงานราชการบางแห่ง โดยเฉพาะอย่างยิ่งหน่วยงานต่างๆ ที่มีคณะกรรมการบริหารดูแลและพระราชบัญญัติคณะกรรมการที่ปรึกษาแห่งรัฐ (The Federal Advisory Committee Act) ซึ่งกำหนดให้คณะกรรมการต่างๆ ที่เป็นที่ปรึกษาแก่หน่วยงานราชการต่างๆ จะต้องเปิดเผยข้อมูลนอกเหนือจากนี้ มลรัฐต่างๆ ทั้งหมดของประเทศสหรัฐอเมริกาได้มีพระราชบัญญัติความเป็นอิสระของข้อมูลเป็นของตนเองแล้วในขณะนี้

กระบวนการคุ้มครองเครือข่ายของการสื่อสารทั้งด้านกฎหมายและเทคนิคนั้นแยกระหว่างเนื้อหาของข้อความและการบันทึกข้อความ เช่น เครือข่ายของโทรศัพท์เนื้อหาของโทรศัพท์แทบจะไม่มีการเปิดเผยเมื่อมีการจัดทำข้อมูลที่เกิดขึ้นในการใช้โทรศัพท์ โดยศาลสูงในประเทศสหรัฐอเมริกาได้ระบุว่า การโทรศัพท์เป็นสิทธิส่วนบุคคล แต่หมายเลขที่ผู้ใช้โทรศัพท์หมุนไม่ได้รวมอยู่ในส่วนของการคุ้มครอง ตรงกันข้ามรัฐสภาได้พิจารณาว่าควรคุ้มครองจึงทำให้เกิดกฎหมายในปี ค.ศ. 1986 ชื่อ **Electronic Communications Privacy Act**

แนวทางในการคุ้มครองสิทธิส่วนบุคคลแบ่งออกเป็นทางด้านเทคนิคและทางด้านกฎหมาย ทางเทคนิคคือพยายามลดความเสี่ยงจากการถูกดักฟังการสื่อสาร การเรียกใช้โดยไม่รับอนุญาต รวมถึงการจัดทำหลักการและนโยบายทางด้านกฎหมาย แต่เกิดปัญหาทางปฏิบัติเสมอ คือ เมื่อข้อความผ่านจากประเทศหนึ่งยังอีกประเทศหนึ่งที่มีหลักกฎหมายแตกต่างกันทำให้เกิดการคุ้มครองสิทธิส่วนบุคคลที่ไม่เท่าเทียมกัน จึงต้องมีการพัฒนาในระดับเครือข่ายนานาชาติ

สหรัฐอเมริกามีกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ พระราชบัญญัติส่วนบุคคล (The Privacy Act 1974) ได้รับการลงมติเห็นชอบจากรัฐสภา และลงนามโดยประธานาธิบดีใน ค.ศ. 1974 พระราชบัญญัตินี้กำหนดให้มีการจัดตั้งคณะกรรมการที่ปรึกษาเรียกว่า คณะกรรมการศึกษาการคุ้มครองสิทธิในชีวิตส่วนบุคคล ประกอบด้วย กรรมการ 7 คน (3 คนแต่งตั้งโดยประธานาธิบดี, 2 คนโดยสภาพสูงสุด และอีก 2 คน โดยสภาผู้แทนราษฎร) ซึ่งทำห้าที่ในการจัดทำข้อเสนอต่อรัฐสภาและประธานาธิบดีโดยการจัดทำขึ้นเป็นรายงานภายใน 2 ปี รายงานดังกล่าวได้ทำขึ้นในเดือนมิถุนายน ค.ศ. 1977 รายงานฉบับนี้ได้ระบุถึงการขยายพระราชบัญญัติให้มีการบังคับให้ไปถึงการจัดเก็บข้อมูลในภาคเอกชน แนวทางหลักของกฎหมายว่าด้วยการคุ้มครองสิทธิส่วนบุคคลในสังคมมีดังนี้[48]

1) ข้อมูลข่าวสารนั้นต้องได้มากโดยตรงจากบุคคลที่เกี่ยวข้องกับข้อมูลข่าวสารนั้นๆ มากที่สุดเท่าที่จะทำได้

2) ต้องแจ้งให้บุคคลซึ่งถูกขอข้อมูลข่าวสารหรือถูกเก็บรวบรวมข้อมูลข่าวสาร ทราบว่าหน่วยงานใดเป็นผู้อนุมัติให้มีการรวบรวมข้อมูลดังกล่าว และจะต้องบอกให้รู้ถึงลักษณะเฉพาะของข้อมูลข่าวสารนั้น จะต้องบอกว่าข้อมูลข่าวสารดังกล่าวใช้ไปเพื่อวัตถุประสงค์ใด รวมทั้งผลใดๆ ที่จะเกิดขึ้นถ้าไม่ให้ข้อมูลตามที่ร้องขอ และแจ้งขอเงื่อนไขในการที่จะมีการสื่อข้อมูลนั้นไปยังหน่วยงานอื่นๆ

3) จะต้องพยายามปรับปรุงให้ข้อมูลข่าวสารดังกล่าวให้ทันสมัยอยู่เสมอ รวมทั้งต้องมีการตรวจสอบความถูกต้องของข้อมูลข่าวสารนั้นๆ อีกด้วย ถ้าหากจะมีการเผยแพร่หรือสื่อปังบุคคลภายนอก

4) ต้องมีการแจ้งให้ทราบตามสมควร เมื่อต้องมีการสื่อหรือเผยแพร่ข้อมูลข่าวสารนั้นๆ ไปยังบุคคลอื่นๆ ตามกระบวนการที่กฎหมายบังคับไว้ และกระบวนการนั้นเป็นเรื่องเกี่ยวกับเอกสารมหาชน

---

[48] ปทีป เมธาคุณาวุฒิ **เรื่องเดิม** หน้า29-38

5) ต้องจัดตั้งกฎระเบียบทางการบริหารด้านเทคนิคและทางกายภาพเพื่อคุ้มครองด้านความลับและการรักษาความปลอดภัยของข้อมูลหรือเอกสารนั้นๆ และเพื่อคุ้มครองป้องกันต่อการคุกคามหรืออันตรายใดๆ ต่อความมั่นคงปลอดภัยที่จะมีผลเป็นอันตราย หรือทำให้ได้รับความอับอายหรือไม่เหมาะสม หรือไม่ยุติธรรมต่อบุคคลผู้ถูกเก็บข้อมูล

การเก็บรวบรวมข้อมูลข่าวสารเกี่ยวกับบุคคลนั้นไว้ มีข้อยกเว้นในกรณีต่อไปนี้ที่ไม่ต้องมีการอนุมัติจากบุคคลผู้ถูกเก็บข้อมูลนั้น คือ

(1) กรณีการสื่อหรือเผยแพร่ข้อมูลข่าวสารที่รวบรวมไว้นั้นเป็นไปตามวัตถุประสงค์ดั้งเดิมในการเก็บรวบรวมหรือบันทึกข้อมูลข่าวสารนั้น

(2) การเผยแพร่ต่อเจ้าหน้าที่ของรัฐซึ่งมีอำนาจในการที่จะใช้ข้อมูลข่าวสารดังกล่าวและการใช้ข้อมูลดังกล่าวจำเป็นต่อการปฏิบัติหน้าที่ของเจ้าหน้าที่นั้นๆ

(3) การเผยแพร่ต่อสถาบันหรือองค์การซึ่งมีสิทธิที่จะใช้ข้อมูลข่าวสารได้โดยไม่ต้องอนุมัติ ได้แก่ รัฐสภา ศาล สำนักงานสถิติ สำนักงานสำรวจสำมะโนประชากร ฝ่ายเอกสารสิ่งพิมพ์แห่งชาติ รวมทั้งองค์กรทั้งหลายที่มีหน้าที่ในการบังคับใช้กฎหมายและในการดำเนินการในกรณีที่มีการฝ่าฝืนต่อกฎหมาย

(4) ข่าวสารซึ่งกฎหมาย FOIC (Freedom of Information Act) ระบุไว้ว่าสามารถสื่อหรือแพร่หลายได้ เว้นแต่จะมีข้อบัญญัติในทางนิติบัญญัติไว้เป็นอย่างอื่น ถ้าเป็นข้อมูลเกี่ยวกับเรื่องทางสุขภาพของบุคคล บุคคลทุกคนสามารถจะคัดค้านมิให้มีการสื่อสารหรือใช้ข้อมูลข่าวสารเกี่ยวกับลักษณะทางสุขภาพของตน

ตามกฎหมายว่าด้วยสิทธิในชีวิตส่วนบุคคลได้ให้การรับรองคุ้มครองสิทธิของบุคคลหนึ่งๆ ที่จะรู้ถึงสถานที่เก็บและลักษณะของเนื้อหาของข้อมูลข่าวสารเหล่านั้นไว้ ในระบบการจัดเก็บบันทึกข่าวสารของหน่วยงานนั้นๆ โดยกำหนดวิธีการให้บุคคลหนึ่งสามารถรู้ได้ว่าหน่วยงานของรัฐบาลกลางได้มีการจัดเก็บข้อมูลข่าวสารส่วนบุคคลหรือไม่ รวมทั้งกล่าวถึงลักษณะเนื้อหาไว้ 3 ประการ คือ

1) กำหนดให้มีการจัดพิมพ์แจ้งถึงความมีอยู่และลักษณะของระบบการจัดเก็บข้อมูลข่าวสารที่หน่วยงานต่างๆ จัดเก็บเหล่านี้ลงไป Federal Register ซึ่งเป็นวิธีการประกาศแจ้งให้ทราบเป็นทางการ หน่วยงานที่เก็บรักษาระบบบันทึกข้อมูลข่าวสารต้องทำดังต่อไปนี้

ภายใต้บทบัญญัติอนุมาตรของบัญญัตินี้ จัดพิมพ์แจ้งให้ทราบถึงความมีอยู่และลักษณะของระบบการจัดเก็บบันทึกข่าวสารที่มีการจัดเก็บหรือแก้ไขปรับปรุงขึ้นใหม่ลงใน Federal Register การแจ้งให้ทราบต้องรวมถึง

(1) ชื่อและสถานที่ตั้งของระบบการจัดเก็บบันทึกข่าวสาร

(2) บุคคลประเภทใดซึ่งบันทึกข่าวสารที่เกี่ยวกับตัวเองจะถูกเก็บรักษาไว้ในระบบการจัดเก็บ

(3) ประเภทของบันทึกข่าวสารที่จะเก็บรักษาในระบบ

(4) การใช้บันทึกข่าวสารที่เก็บไว้ในระบบตามระเบียบงาน รวมทั้งประเภทของผู้ใช้และวัตถุประสงค์ที่จะใช้

(5) นโยบายและข้อปฏิบัติของหน่วยงานเกี่ยวกับการเก็บสะสม การแก้ไข การควบคุมการเข้าถึง การรักษาและการจัดการเกี่ยวกับบันทึกข่าวสาร

(6) ตำแหน่งและที่ทำงานของเจ้าหน้าที่ของหน่วยงานซึ่งมีหน้าที่รับผิดชอบระบบบันทึกข้อมูลข่าวสาร

(7) ขั้นตอนของหน่วยงานที่บุคคลคนหนึ่งจะได้รับการแจ้งให้ทราบตามคำร้องขอของตนว่าจะสามารถเข้าถึงข้อมูลข่าวสารนั้นๆ ได้มีบันทึกข่าวสารอันเกี่ยวกับตนเอง

(8) ขั้นตอนของหน่วยงานที่บุคคลคนหนึ่งจะได้รับการแจ้งให้ทราบตามคำร้องขอของตนว่าจะสามารถเข้าถึงข้อมูลข่าวสารที่เกี่ยวกับตน รวมทั้งจะโต้แย้งเนื้อหาของข้อมูลข่าวสารดังกล่าวที่จัดเก็บไว้ในระบบจัดเก็บนั้นได้อย่างไร

(9) ประเภทของแหล่งที่มีของบันทึกในระบบนั้นๆ

ตามบทบัญญัติข้างต้น หากบุคคลคนหนึ่งๆ ต้องการทราบว่าหน่วยงานของรัฐบาลหน่วยงานหนึ่งอาจมีบันทึกข่าวสารประเภทใดบ้างก็สามารถพิจารณาได้จากการประกาศแจ้งให้ทราบตามที่กำหนดไว้ข้างต้นจาก Federal Register เมื่อคาดว่าหน่วยงานใดอาจมีข่าวสารอันเกี่ยวกับตนก็สามารถร้องขอ เพื่อให้หน่วยงานนั้นๆ แจ้งให้ทราบว่ามีบันทึกข่าวสารที่เกี่ยวกับตนหรือไม่

2) กำหนดให้มีการบอกกล่าวแก่บุคคลที่หน่วยงานนั้นๆ ขอให้บุคคลดังกล่าวให้ข้อมูลข่าวสารแก่หน่วยงานถึงรูปแบบที่หน่วยงานนั้นจะใช้ในการจัดเก็บข้อมูลข่าวสาร รวมทั้งวัตถุประสงค์ในการใช้ข้อมูลข่าวสารดังกล่าว (วิธีการแจ้งให้ทราบเป็นรายบุคคล)

3) บอกกล่าวแก่บุคคลผู้ที่หน่วยงานได้ขอข้อมูลข่าวสารในแบบสอบถามซึ่งใช้ในการเก็บข้อมูลข่าวสารหรือในเอกสารแยกต่างหากจากแบบสอบถามนั้น ทำให้บุคคลนั้นสามารถจะเก็บไว้โดยการบอกถึงรายละเอียดดังต่อไปนี้

(1) การร้องขอข้อมูลข่าวสารอาศัยอำนาจกฎหมายหรือกฎระเบียบใด และการเปิดเผยข้อมูลนั้นเป็นไปตามข้อกำหนดหรือเป็นไปโดยความสมัครใจหรือไม่

(2) วัตถุประสงค์หลักคาดว่าจะมีการใช้ข้อมูลข่าวสารนั้น

(3) การใช้ตามระเบียบที่อาจมีขึ้นต่อข้อมูลข่าวสารนั้นตามที่จัดพิมพ์ไว้

(4) จะมีผลใดๆ กับบุคคลนั้นหรือไม่ หากไม่ให้ข้อมูลอื่นๆ ทั้งหมดหรือให้ข้อมูลบางส่วนตามที่หน่วยงานดังกล่าวร้องขอ

จากบทบัญญัตินี้ทำให้บุคคลหนึ่งๆ ที่ถูกหน่วยงานของรัฐบาลขอข้อมูลข่าวสารเกี่ยวกับผู้นั้นเองได้ทราบว่า ข้อมูลข่าวสารนั้นมีการจัดเก็บและใช้ในรูปแบบใดตามบทบัญญัติของ Privacy Act นั้นได้ก่อให้เกิดพันธะหน้าที่แก่เจ้าหน้าที่หรือหน่วยงานของรัฐในการเอื้ออำนวยต่อการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลนั้น เมื่อมีคำร้องขอจากบุคคลคนหนึ่งเพื่อจะเข้าสู่ข่าวสารหรือข้อมูลของตนที่อยู่ในระบบ หน่วยงานดังกล่าวจะต้องอนุญาตตามคำร้องขอให้บุคคลนั้น หรือบุคคลที่ได้รับเลือกให้มาด้วยเพื่อตรวจดูบันทึกข่าวสารและได้รับสำเนาบันทึกข่าวสารนั้นๆ บางส่วนหรือทั้งหมด ในรูปแบบที่บุคคลนั้นสามารถเข้าใจได้ เว้นแต่หน่วยงานดังกล่าวอาจกำหนดให้บุคคลนั้นให้ข้อความอนุญาตเป็นหนังสือเกี่ยวกับการให้บุคคลที่มาด้วยพิจารณาเกี่ยวกับข้อมูลข่าวสารของบุคคลนั้น

บุคคลคนหนึ่งๆ ซึ่งเป็นประชาชนชาวอเมริกัน หรือมีภูมิลำเนาถาวรตามกฎหมายในประเทศอเมริกา จะสามารถเข้าสู่ข้อมูลข่าวสารที่เกี่ยวกับตนเองได้ โดยร้องขอต่อหน่วยงานที่ตนคาดว่าจัดเก็บข้อมูลข่าวสารของตน เพื่อขอเข้าสู่ข้อมูลข่าวสารนั้นๆ ดังนั้นหากข้อมูลข่าวสารนั้นเป็นรหัสทางเครื่องคอมพิวเตอร์หรือมีข้อสังเกตใดๆ ที่ไม่อาจเข้าใจได้ จะต้องมีการแปลให้เป็นภาษาที่เข้าใจได้

อย่างไรก็ตาม มีข้อยกเว้นกรณีนี้ใช้กับหน่วยงานของรับบาลกลางที่มีชื่อว่า Central Intelligence Agency (CIA) และหน่วยงานที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมายอาญา โดยหน่วยงานดังกล่าวจะได้รับการยกเว้นจากบทบัญญัติต่างๆ ของกฎหมายนี้หลายกรณีด้วยกัน รวมทั้งยกเว้นจากการใช้สิทธิในการเข้าสู่ข้อมูลสารสนเทศของบุคคล อย่างไรก็ตามหน่วยงานนี้ยังคงอยู่ภายใต้บทบัญญัติพื้นบานตามกฎหมายนี้ ข้อยกเว้นสำหรับข้อมูลข่าวสารที่จัดเก็บโดยอนุญาตให้หัวหน้าของ CIA ยกเว้นระบบจัดเก็บข้อมูลข่าวสารภายในหน่วยงานของตนจากข้อกำหนดต่างๆ ตามกฎหมาย บทบัญญัติที่ได้รับการยกเว้นเบื้องต้น คือ บทบัญญัติเกี่ยวกับการเขาสู่ข้อมูลข่าวสาร ข้อยกเว้นโดยหน่วยงานที่มีหน้าที่บังคับการให้เป็นไปตามกฎหมายอาญาของรัฐบาลกลางที่มีการจัดเก็บข้อมูลข่าวสารดังกล่าวถือเป็นการปฏิบัติหน้าที่ของหน่วยงานนั้นๆ เกี่ยวกับการบังคับการให้เป็นไปตามกฎหมายอาญา การ

ดำเนินการต่างๆ เพื่อป้องกัน ควบคุม หรือลดอาชญากรรม หรือเพื่อจับกุมอาชญากรรมและกิจกรรมด้านการฟ้องร้อง การศาล การตัดสันดาน การคุมประพฤติ อภัยโทษ หรือการให้ทัณฑ์บน ซึ่งประกอบไปด้วยบันทึกข้อมูลข่าวสาร 3 ประเภท คือ

1) ข้อมูลข่าวสารที่เก็บรวบรวมไว้เพื่อวัตถุประสงค์ในการเก็บรูปพรรณของผู้กระทำความผิดอาญา ผู้ถูกกล่าวหาว่ากระทำความผิดอันประกอบด้วยข้อมูลข่าวสารเกี่ยวกับรูปพรรณ บันทึกการจับกุมการกำหนดค่าปรับ คำพิพากษา กำหนดโทษ การคุมขัง การปล่อยตัวและการให้ทัณฑ์บนและสภาพการคุมประพฤติ

2) ข้อมูลข่าวสารที่จัดเก็บไว้เพื่อวัตถุประสงค์ในการสอบสวนสืบสวนอาชญากรรม รวมทั้งรายงานของผู้ให้ข่าวสาร นักสืบและการติดต่อกับบุคคลอันอาจระบุชื่อได้

3) รายงานที่อาจชี้ถึงตัวบุคคลผู้ดำเนินการในระดับต่างๆ ในกระบวนการด้านการบันทึกตามกฎหมายอาญาเกี่ยวกับการจับกุมหรือการพิพากษาลงโทษ ตลอดจนถึงการปล่อยจากการสอดส่องดูแล

นอกจากนี้ สำหรับข้อยกเว้นกรณีนี้ใช้กับหน่วยงานของรัฐบาลกลางทั่วไปภายใต้พฤติการณ์ที่ระบุไว้ ซึ่งมีอยู่ 7 ประการ หัวหน้าหน่วยงานสามารถยกเว้นระบบการจัดเก็บข้อมูลข่าวสารบางกรณี การเข้าสู่ข้อมูลข่าวสารและบทบัญญัติเกี่ยวกับการคัดค้านต่างๆ ตามกฎหมาย นอกจากบทบัญญัติพื้นฐานที่กล่าวถึงในข้อยกเว้นทั่วไปแล้ว ระบบข้อมูลข่าวสารที่อยู่ในข้อยกเว้นใดๆ ใน 7 ประการดังต่อไปนี้

1) กรณีที่ข้อมูลข่าวสารที่จัดเก็บไว้ในระบบจัดเก็บข้อมูลข่าวสารที่เกี่ยวกับการป้องกันประเทศและนโยบายต่างประเทศ

2) การจัดเก็บข้อมูลข่าวสารนั้นเป็นการจัดเก็บสิ่งที่รวบรวมไว้ในสืบสวนสอบสวน เพื่อวัตถุประสงค์ในการบังคับการให้เป็นไปตามกฎหมาย

3) ข้อมูลข่าวสารนั้นจัดเก็บไว้เพื่อใช้ในการให้ความคุ้มครองต่อประธานาธิบดีหรือบุคคลใดๆ ภายใต้การคุ้มครองของหน่วยงานที่มีชื่อว่า Secret Service

4) ข้อมูลข่าวสารนั้นถูกกำหนดไว้ในกฎหมายให้ใช้เพียงเพื่อวัตถุประสงค์ทางด้านสถิติ

5) ข้อมูลข่าวสารนั้นเป็นสิ่งที่เกี่ยวกับการสืบสวนสอบสวนที่เก็บรวบรวมไว้เพื่อใช้ในการวินิจฉัยเกี่ยวกับความเหมาะสม ได้รับเลือกหรือคุณสมบัติในการจ้างเข้าราชการพลเรือน การให้บริการเกี่ยวกับทางทหาร การทำสัญญากับรัฐบาล หรือการเข้าสู่บันทึกข้อมูลข่าวสารที่ระบุไว้เหล่านี้ในขอบเขตที่การเปิดเผยสิ่งที่จัดเก็บไว้นั้นจะเป็นการเปิดเผยถึงแหล่งที่ให้ข้อมูลข่าวสารซึ่งรัฐบาลได้สัญญาไว้ว่าจะปิดเป็นความลับ

6) ข้อมูลข่าวสารเกี่ยวกับสิ่งที่ใช้ในการตรวจสอบหรือทดสอบซึ่งใช้เพื่อวินิจฉัยคุณสมบัติของบุคคลที่จะได้รับเลือก หรือสนับสนุนในการให้บริการของรับ ถ้าการ

เปิดเผยสิ่งดังกล่าวจะเป็นการขัดต่อวัตถุประสงค์หรือความเป็นธรรมในกระบวนการในการตรวจสอบหรือทดสอบนั้น

7) ข้อมูลข่าวสารนั้นเป็นสิ่งที่ใช้ในการประเมิน วินิจฉัยถึงความน่าจะเป็นไปได้ในการสนับสนุนการดำเนินการทางการทหาร ในขอบเขตที่ว่าการเปิดเผยถึงสิ่งดังกล่าวจะเป็นการเปิดเผยแหล่งที่ให้ข้อมูลข่าวสารซึ่งรัฐบาลสัญญาว่าจะปิดเป็นความลับ

ถ้ามีการยกเว้นตามอนุมาตราเหล่านี้ หน่วยงานนั้นๆ จะต้องมีเหตุผลในการอ้างว่าเหตุใดจึงได้ยกเว้นระบบบันทึกข่าวสารนั้นๆ

เมื่อบุคคลหนึ่งได้ดำเนินการยื่นคำร้องขอตาม Privacy Act เพื่อจะเข้าสู่ข้อมูลข่าวสารของตน ซึ่งอยู่ในความครอบครองของหน่วยงานของรัฐบาลกลาง ถ้าปรากฏว่าหน่วยงานดังกล่าวปฏิเสธคำร้องขอที่จะเข้าสู่ข้อมูลข่าวสารของตนตากฎหมายแต่ละฉบับ บุคคลนั้นสามารถดำเนินการอุทธรณ์ได้

1.4 กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

ในสหรัฐอเมริกา กฎหมายลิขสิทธิ์ของสหรัฐอเมริกา คือ Copyright law of the United States of America หัวข้อ 104. ระบุถึง ลิขสิทธิ์ในงานที่มีการรวบรวม (copyrights in restored works) ว่า หากผลงานการดำเนินการดังกล่าวไม่เคยมีใครดำเนินการจัดทำมาก่อนในสหรัฐอเมริกา ผู้จัดทำก็อาจมีลิขสิทธิ์ในงานดังกล่าวได้ แต่ข้อมูลที่เก็บรวบรวม หากเดิมเป็นงานที่มีลิขสิทธิ์อยู่แล้ว ลิขสิทธิ์ในผลงานส่วนนั้นก็ถือเป็นส่วนที่ได้รับการคุ้มครองอยู่แล้ว ซึ่งในมาตรา 102 ของกฎหมายลิขสิทธิ์ได้ให้การรับรองว่า ผลงานที่เป็นการรวบรวม หรือผลงานที่เป็นในเชิงอนุพันธ์ (compilations and derivative works) นอกจากนี้ในมาตรา 106 ยังบ่งในเชิงขยายความว่า หากเป็นการเก็บรวบรวม และนำสำเนาโดยบรรณารักษ์ว่า หากเป็นการเก็บรวบรวม และนำสำเนาโดยบรรณารักษ์ หรือ ผู้ปฏิบัติงานที่เป็นหอจดหมาย หรือ เพียงศูนย์เอกสารก็จะไม่ได้รับการคุ้มครองในผลงานเชิงลิขสิทธิ์

อย่างไรก็ตาม สหรัฐอเมริกานั้นไม่มีกฎหมายว่าด้วยฐานข้อมูล (database law) เหมือนกลุ่มสหภาพยุโรป [49] จึงนำเอากฎหมายลิขสิทธิ์ในด้านของ “การรวบรวม (compilation)” มาใช้กับการรวบรวมและจัดทำฐานข้อมูลแทน (17 US Code 101) โดยให้การรับรองแก่ผู้จัดทำ แต่จะต้องเป็นการคัดสรรในเชิงการสร้างสรรค์ และสร้างงานใหม่(original/

[49] ยุโรปมี Council Directive 96/9/EC on The Legal Protection of Data Base

creative selection) [50]การเพียงรวบรวมธรรมดา เช่น สมุดหน้าเหลือง จะไม่ได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์

ดังนั้น ในการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลในกระบวนการยุติธรรมของสหรัฐอเมริกานั้น หากเป็นการดำเนินการรวบรวมและดำเนินการต่อโดยพัฒนาในเชิงสร้างสรรค์ก็ได้รับการคุ้มครองโดย ยึดถือตามหลัก sweat of the brow protection

1.5 กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ในสหรัฐอเมริกาได้มีการยอมรับกันว่าอาชญากรรมทางคอมพิวเตอร์เป็นหนึ่งในปัญหาต่างๆที่ท้าทายเจ้าหน้าที่ผู้บังคับใช้กฎหมายทั้งในระดับสหรัฐอเมริกา และระดับมลรัฐมากที่สุด

กฎหมายอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริการมี 2 ระดับ คือ กฎหมายอาชญากรรมทางคอมพิวเตอร์ของสหรัฐ (federal law) และกฎหมายของมลรัฐต่างๆ (state law) กฎหมายของสหรัฐ ใช้ในกรณีที่การกระทำความผิดนั้นเกี่ยวข้องกับผลประโยชน์ของสหรัฐอเมริกา (federal interests) หรือการค้าระหว่างรัฐ และกฎหมายของมลรัฐใช้ในกรณีที่การกระทำความผิดนั้น เกิดขึ้นภายในเขตของแต่ละมลรัฐ

กฎหมายสหรัฐอเมริกาที่ใช้ดำเนินคดีกับอาชญากรรมทางคอมพิวเตอร์มีมากกว่า 40 ฉบับ เช่น Copyright Act, National Stolen Property Act, Mail and Wire Fraud Statutes , Child Pornography Prevention Act of 1996 เป็นต้น ในกรณีที่เป็นการกระทำความผิดต่อคอมพิวเตอร์ กฎหมายที่เกี่ยวข้องโดยตรงกับเรื่องนี้ ได้แก่ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 นอกจากกฎหมายฉบับนี้แล้วก็ยังมีกฎหมายอื่นที่สามารถใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์ได้อีก คือ the Electronic Communications Privacy Act 1986 และ the Economic Espionage Act 1999

1.กฎหมายThe Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

แนวความคิดในการบัญญัติกฎหมายเพื่อใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่างๆคือ การที่สภาคองเกรสเห็นว่าการกระทำรูปแบบใหม่นี้มีลักษณะพิเศษที่แตกต่างไปจากความผิดรูปแบบเดิม เพราะเป็นการกระทำที่เกี่ยวข้องกับสิ่งที่ไม่

[50] Ius mentis Law and Technology P.1

มีรูปร่าง ทำให้การจะดำเนินคดีโดยอาศัยความผิดฐาน theft และ larceny ตามกฎหมายเดิมเป็นเรื่องที่ยากลำบาก เพื่อแก้ปัญหาเรื่องนี้ก็ควรที่จะบัญญัติกฎหมายใหม่ขึ้นมามากกว่าการพยายามจะนำกฎหมายเก่ามาใช้ดำเนินคดีกับความผิดรูปแบบใหม่ ด้วยเหตุนี้ สภาคองเกรสจึงบัญญัติ the Counterfeit Access Device and Computer Fraud and Abuse Act (ต่อไปจะเรียกว่า CFAA) ขึ้นในปี ค.ศ.1984 กฎหมายนี้เป็นส่วนหนึ่งของ The Comprehensive Crime Control Act และถือว่า CFAA เป็นกฎหมายฉบับแรกที่ถูกบัญญัติขึ้นเพื่อดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์โดยเฉพาะ

แต่เดิม CFAA มีเพียง 3 ฐานความผิดเท่านั้น ได้แก่

1.การเข้าถึงคอมพิวเตอร์ เพื่อให้ได้ไปซึ่งข้อมูลทางทหาร หรือข้อมูลเกี่ยวกับต่างประเทศ เพื่อที่จะทำให้เกิดอันตรายต่อสหรัฐอเมริกา หรือเพื่อให้เกิดประโยชน์ต่อรัฐอื่น

2.การเข้าถึงคอมพิวเตอร์ เพื่อให้ได้ไปซึ่งบันทึกทางการเงินจากสถาบันทางการเงิน หรือข้อมูลของผู้บริโภคจากตัวแทนของผู้บริโภค (consumer reporting agencies)

3.การแก้ไขเปลี่ยนแปลง การทำลาย การเปิดเผยข้อมูล ซึ่งทำให้เกิดผลกระทบต่อการใช้คอมพิวเตอร์ของรัฐบาล

ต่อมาเพื่อแก้ไขกฎหมายให้มีความสมบูร์และทันสมัยมากขึ้น CFAA จึงถูกแก้ไขในปี ค.ศ. 1986 โดยการแก้ไขปรับปรุงกฎหมายครั้งนี้ถือเป็นครั้งสำคัญ เพราะมีการแก้ไขปรับปรุงหลายเรื่อง คือ การบัญญัติเพิ่มเติมฐานความผิดเพิ่มขึ้นอีก 3 ฐานความผิด ได้แก่ การเข้าถึงคอมพิวเตอร์เพื่อฉ้อโกง การแก้ไขเปลี่ยนแปลง การทำให้เสียหาย หรือการทำลายข้อมูล หรือการขัดขวางการใช้คอมพิวเตอร์โดยชอบด้วยกฎหมาย และการค้าขายรหัสผ่านใดๆ นอกจากนี้ การใช้คำว่า “โดยเจตนา” (intentionally) แทนคำว่า “โดยรู้” (knowingly) การขยายขอบเขตคำว่า “Federal interest computer” ให้รวมถึงคอมพิวเตอร์ ซึ่งหนึ่งในสองของเครื่องคอมพิวเตอร์หรือมากกว่าใช้ในการกระทำความผิด โดยคอมพิวเตอร์ทั้งหมดไม่จำเป็นต้องอยู่ในรัฐเดียวกัน[51] เป็นต้น

---

[51] Edward M. Wise. Informtion Technology Crime p.29

2.กฎหมาย The Electronic Communications Privacy Act (ต่อไปจะเรียกว่า ECPA)

เนื่องจากกฎหมายที่ใช้ดำเนินคดีกับการดักข้อมูล คือ The Federal Wiretapping Statues 18 U.S.C. มาตรา 2510) ใช้ดำเนินคดีกับการดักข้อมูลจากการติดต่อสื่อสารทางสายและทางคำพูด (wire and oral communications) เท่านั้น มิได้รวมถึงการดักข้อมูลในรูปแบบอื่นๆด้วย และเพื่อให้ก้าวทันต่อความเจริญก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ และเพื่อคุ้มครองความเป็นส่วนตัวของผู้ใช้คอมพิวเตอร์ในการติดต่อสื่อสารในรูปแบบใหม่ๆด้วย สภาคองเกรสจึงบัญญัติ ECPA โดยให้ความคุ้มครองถึงความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบอื่นด้วย ได้แก่ เครื่องมือรับส่งข้อความทางคลื่นวิทยุ (radio paging devices) จดหมายอิเล็กทรอนิกส์ (e-mail) โทรศัพย์เคลื่อนที่ การติดต่อสื่อสารส่วนบุคคล (private communication carriers) และการรับส่งข้อมูลทางคอมพิวเตอร์

ECPA (18 U.S.C. มาตรา 2701) กำหนดให้การได้รับ การแก้ไขเปลี่ยนแปลง การขัดขวางการเข้าถึงที่ชอบด้วยกฎหมายในสิ่งที่เก็บไว้ในลักษณะที่เป็นอิเล็กทรอนิกส์เป็นความผิดอาญา

3.กฎหมายThe Economic Espionage Act (ต่อไปจะเรียกว่า EEA) 18 U.S.C. มาตรา 1831-1839

กฎหมายนี้ใช้ดำเนินคดีกับผู้กระทำการจารกรรมทางเศรษฐกิจ (economic espionage) และการขโมยความลับทางการค้า ซึ่งทั้งสองกรณีเป็นความผิดร้ายแรง (felony) EEA มีผลใช้บังคับเมื่อวันที่ 11 ตุลาคม ค.ศ. 1996 ในขั้นร่างกฎหมายฉบับนี้ the House Report of the Committee on the Judiciary ได้ให้เหตุผลประกอบการประกาศใช้กฎหมายฉบับนี้ โดยอ้างผลการสำรวจของ the American Society for Industrial Security international ซึ่งแสดงให้เห็นถึงการเพิ่มขึ้นกว่า 300 เปอร์เซนต์ของการจารกรรมทางเศรษฐกิจในช่วงเวลา 4 ปี ซึ่งทำให้เกิดความเสียหายต่ออุตสาหกรรมของสหรัฐอเมริกาเป็นเงินถึง 63,000 ล้านเหรียญสหรัฐต่อปี

นอกจากนี้ the House Report of the Committee on the Judiciary ยังได้อ้างผลการศึกษาที่แสดงให้เห็นว่าทรัพย์สินที่ไม่มีรูปร่างกำลังขยายตัวโดยเป็นส่วนหนึ่งของทรัพย์สินทั้งหมด ของธุรกิจของชาวอเมริกัน รวมทั้ง สภาคองเกรสได้ตั้งข้อสังเกตไว้ด้วยว่าข้อมูลอันเป็นความลับทางธุรกิจ อาจเป็นวัตถุของการกระทำความผิดได้ โดยการกระทำของรัฐบาลหรือบริษัทต่างประเทศ รวมทั้งบุคลากรภายในองค์กร เพื่อหวังที่จะหากำไรจากการขายข้อมูลอันเป็นความลับของบริษัทให้กับบริษัทคู่แข่ง

ความผิดในส่วนที่เกี่ยวกับการกระทำความผิดต่อคอมพิวเตอร์ คือการห้ามการดึงข้อมูลจากระบบคอมพิวเตอร์มาเก็บไว้ (download) การนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์ (upload) การส่ง หรือการติดต่อสื่อสารซึ่งความลับทางการค้าโดยปราศจากอำนาจ (มาตรา 1831 (a) (2))

ในระดับมลรัฐ การบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ ได้เริ่มขึ้นในปี ค.ศ. 1978 โดยเริ่มจากมลรัฐอาริโซนา (Arizona) และฟลอริดา (Florida) ก่อน หลังจากนั้น มลรัฐอื่น จึงประกาศใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ตามมา ในขณะนี้ทุกมลรัฐมีกฎหมายอาชญากรรมทางคอมพิวเตอร์ครบหมดแล้ว โดยมลรัฐเวอร์มอนท์ (Vermont) เป็นมลรัฐสุดท้ายที่เพิ่งประกาศใช้กฎหมายดังกล่าว

ในกรณีของการกระทำความผิดต่อคอมพิวเตอร์นั้น กฎหมายของมลรัฐต่างๆ ส่วนใหญ่กำหนดให้การเข้าถึงคอมพิวเตอร์เป็นความผิดอาญา โดยกำหนดให้การกระทำดังกล่าวเป็นความผิดพื้นฐาน (baseline offenses) และเมื่อมีการกระทำใดๆต่อไป ภายหลังจากการเข้าถึงระบบคอมพิวเตอร์แล้ว การกระทำนั้นถือว่าเป็นความผิดร้ายแรง (aggravated forms) โดยผู้กระทำต้องรับโทษหนักขึ้น โดยแต่ละมลรัฐจะบัญญัติความผิดร้ายแรงไม่เหมือนกัน แต่โดยส่วนใหญ่จะมีลักษณะคล้ายคลึงกัน เช่น การแก้ไขเปลี่ยนแปลง หรือทำลายข้อมูลคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์ การกรรโชกทรัพย์ เป็นต้น

2) ประเทศอังกฤษหรือสหราชอาณาจักร

เดิมอังกฤษมีการกำหนดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล เฉพาะในกรณีที่มีการดำเนินการที่มีเหตุหรือกรณีฉุกเฉินในการร่วมมือกันดำเนินการ โดยการดำเนินการดังกล่าวสามารถกระทำได้ทั้งหน่วยงานของรัฐ-รัฐ หรือ รัฐกับเอกชน และโดยการดำเนินการที่เป็นทางการและไม่เป็นทางการ แต่ต่อมาเมื่อมีการดำเนินการให้มีการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างองค์กรที่มีภารกิจการปฏิบัติการที่คล้ายๆกันได้ (community) โดยมีการแยกเป็นประเภท (Category) ทั้งนี้เนื่องจากการที่ EU ได้มีนโยบายหลักในการให้มีการแลกเปลี่ยนข้อมูลต่างๆที่เป็นประโยชน์ต่อการดำเนินภารกิจขององค์กร

สหราชอาณาจักรเองมีระบบข้อมูลที่มีการพัฒนาแต่ก็ยังมีข้อวิจารณ์ว่ายังไม่ทันสมัยเพียงพอหากเทียบกับของสก๊อตแลนด์ ระบบการบูรณาการข้อมูลด้านกระบวนการยุติธรรมของสก๊อตแลนด์ (Integration of Scottish Criminal Justice Information System)

ระบบการบูรณาการข้อมูลด้านกระบวนการยุติธรรมของสก๊อตแลนด์มีชื่อเรียกย่อๆ ว่า ISCJIS (Integration of Scottish Criminal Justice Information System) เป็นโครงการที่ให้หน่วยงานหลักในกระบวนการยุติธรรมมาร่วมในการบูรณาการข้อมูล และใช้ร่วมกัน ซึ่งยังรวมเอาหน่วยงานที่เกี่ยวข้องหลักๆ เข้าไปร่วมด้วย อันได้แก่

1. Scottish Executive
2. Crown Office and Procurator Fiscal Service (CO/PFS)
3. Scottish Court Service (SCS)
4. Scottish Police Force (and the British Transport Police)
5. Scottish Prison Service (SPS)
6. Scottish Criminal Record Office
7. Scottish Local Authorities (including District Courts)
8. Scottish Children's Reporter Administration
9. Scottish Legal Aid Board
10. Driver and Vehicle Licensing Agency (DALA)

การดำเนินการบูรณาการข้อมูลดังกล่าวไม่ใช่ใช้ระบบคอมพิวเตอร์ใหม่ แต่ใช้การเชื่อมโยงข้อมูล โดยมีการจัดตั้งศูนย์กลาง คือ SCRO เป็นศูนย์กลาง (hub) ของการส่ง – รับข้อมูล ศูนย์กลางดังกล่าวจะทำหน้าที่ประมวลข้อมูลในระบบ และการดำเนินการดังกล่าวได้ดำเนินการโดยหน่วยงานที่เกี่ยวข้องได้ทำความตกลงร่วมกัน (agreement) ให้มีการเชื่อมโยง

การดำเนินการดังกล่าวส่งผลต่อการปฏิบัติงานในกระบวนการยุติธรรมใน 4 ประการ คือ

1) การบริการด้านข้อมูลเป็นไปโดยรวดเร็ว (Faster Services)

เนื่องจากข้อมูลต่างๆ สามารถถ่ายโอนกันทางระบบอิเล็กทรอนิกส์ระหว่างองค์การต่างๆ ทำให้สามารถใช้ข้อมูลได้รวดเร็วประกอบการดำเนินการ เช่น ศาลสามารถใช้ข้อมูลจากฝ่ายราชทัณฑ์หรือคุมประพฤติประกอบการพิจารณาในการกำหนดโทษ หรือการพิจารณาคดี

2) การปรับปรุงในเรื่องความถูกต้องของข้อมูล (Improvement in Accuracy)

ระบบข้อมูลที่ผ่านระบบเทคโนโลยีสารสนเทศจะมีการจัดทำโปรแกรมตรวจสอบประเภทและลักษณะของข้อมูลให้ถูกต้องและตรงกัน ข้อมูลที่ได้รับจึงมีความถูกต้องในการดำเนินคดี

3) การปรับปรุงประสิทธิภาพในการใช้ของเจ้าหน้าที่ผู้ที่เกี่ยวข้อง (Improved efficiency in the use of staff)

ข้อมูลที่ป้อนจากหน่วยงานต่างๆ จะไปปรากฏยังศูนย์ข้อมูลและทำให้หน่วยงานที่รับเรื่องต่อสามารถเตรียมการและวางแผนในการปฏิบัติงานต่อเนื่อง ลดปริมาณการใช้กระดาษ เวลา บุคลากรที่จะต้องพิมพ์และทำสำนวนใหม่ ทำให้ประสิทธิภาพของงานดีขึ้นและกระบวนการดำเนินคดีลดเวลาลง

4) ปรับปรุงการเข้าถึงข้อมูล (Improve access to information)

การพัฒนาการบูรณาการข้อมูลดังกล่าว อาศัยหลักของการเป็นหุ้นส่วน (Partnership) ที่หน่วยงานต่างๆ ต้องดำเนินการร่วมกัน ไม่ใช่หน่วยงานใดจะเข้าถึงข้อมูลเฉพาะหน่วยงานอื่นๆ คดีต่างๆ จึงมีข้อมูลจากทุกหน่วยงานที่เกี่ยวข้องอย่างรวดเร็ว

อย่างไรก็ตาม จะมีการประเมินความเสี่ยงข้อมูล (Risk Management Evaluation) ทุกปี

(1)กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

กฎหมายที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของอังกฤษมีหลายฉบับ แต่ก็อาจจะระบุจำแนกตามประเภทของภารกิจงาน เช่น The Freedom of Information Act (FOIA) และ The Environmental Impact Regulations (EIR) ซึ่งให้สิทธิของบุคคลในการสอบถามและให้ข้อมูลทั้งทั่วไปและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูล กฎหมายที่มีผลโดยตรงต่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม ได้แก่ The Civil Contingencies Act (CCA) 2004 เป็นกฎหมายที่มีการจำแนก Category 1 และ Category 2 . โดยการแลกเปลี่ยนข้อมูลระหว่างองค์กรที่มีพันธะหน้าที่คล้ายกัน อย่างไรก็ตาม กฎหมายฉบับนี้ไม่ได้ขัดแย้งกับกฎหมาย Data Protection Act 1998

อย่างไรก็ตาม ข้อมูลที่มีการแลกเปลี่ยนและเชื่อมโยงก็มิได้ให้เป็นข้อมูลทุกประเภท มีข้อจำกัดว่าข้อมูลเหล่านี้เป็นข้อมูลที่มีผลกระทบอย่างรุนแรง จึงห้ามมิให้มีการแลกเปลี่ยนข้อมูล ถ้ามีลักษณะข้อมูลต่อไปนี้

1. ข้อมูลที่จะก่อให้เกิดผลกระทบต่ออคติด้านความมั่นคงของประเทศ (information prejudicial to national security)

2. ข้อมูลที่จะก่อให้เกิดผลกระทบต่ออคติด้านความปลอดภัยของชุมชน (information prejudicial to public safety)

3. ข้อมูลมีผลกระทบต่อการค้า (commercially sensitive information) และ

4. ข้อมูลส่วนบุคคล (personal information) แต่ต้องภายใต้ข้อกำหนดตามกฎหมาย Data Protection

นอกจากกฎหมายดังกล่าวแล้วยังมีระเบียบบางประการที่เกี่ยวข้องอาทิ Ministry of Justice-legal advice and jargon buster, Regulation of The Information Commissioners Office เป็นต้น

(2)กฎหมายคุ้มครองข้อมูลส่วนบุคคล

เมื่อยุโรปมีการเคลื่อนไหวจัดทำ Convention for the protection of Individuals เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลด้วยคอมพิวเตอร์ ซึ่ง European Commission ได้ขอให้สมาชิกของกลุ่มประชาคมยุโรปให้ลงนาม และให้สัตยาบันต่ออนุสัญญาฉบับนี้ก่อสิ้น ค.ศ. 1982 ประเทศอังกฤษได้ให้สัตยาบันต่ออนุสัญญาฉบับดังกล่าวใน ค.ศ. 1981 และเพื่อให้เป็นไปตามอนุสัญญาฉบับนี้ อังกฤษได้ตรากฎหมายเพื่อคุ้มครองสิทธิในชีวิตส่วนบุคคลมีชื่อว่า Data Protection Act 1984

ตามพระราชบัญญัตินี้ได้กำหนดให้มีเจ้าหน้าที่เรียกว่า Data Protection Registrar และคณะกรรมการพิเศษที่เรียกว่า Data Protection Tribune ขึ้น อำนาจหน้าที่ของ Data Protection Registrar คือ[52]

1) มีหน้าที่พิจารณาอนุญาตการขออนุญาตจัดเก็บข้อมูลเกี่ยวกับบุคคล

2) มีหน้าที่ควบคุม ดูแล ตรวจตราว่ามีการล่วงละเมิดหลักการคุ้มครองข้อมูลอันเกี่ยวกับบุคคลตามกฎหมายฉบับใหม่หรือไม่

3) มีอำนาจหน้าที่ในการส่งคำเตือน 3 ประเภท ในกรณีพบว่ามีการล่วงละเมิด คำเตือนฉบับแรกเป็นการแจ้งให้ปฏิบัติให้ถูกต้องในระยะเวลาที่กำหนด คำเตือนประเภทที่สองเป็นการเตือนซ้ำถ้ายังไม่ปฏิบัติตามคำเตือนหลังนี้จะดำเนินการเพิกถอนทางทะเบียน คำเตือนประเภทสุดท้ายเป็นคำเตือนเกี่ยวกับการห้ามสื่อข้อมูลข้ามแดนอันผิดไปจากที่กฎหมายฉบับนี้กำหนดไว้

4) หน้าที่ในการประกาศโฆษณาถึงการปฏิบัติตามหลักการคุ้มครองข้อมูลของผู้ใช้ข้อมูลและผู้ปฏิบัติงานในสำนักงานคอมพิวเตอร์

---

[52] ปทีป เมธาคุณวุฒิ **เรื่องเดิม** หน้า38-42

5) อำนาจในการพิจารณาคำร้องขอของผู้เสียหายว่ามีการล่วงละเมิดหลักการคุ้มครองข้อมูลหรือล่วงละเมิดกฎหมายนี้และดำเนินการโดยไม่ชักช้า รวมแจ้งให้บุคคลนั้นๆ ทราบถึงการพิจารณาและมาตรการที่จะใช้

6)หน้าที่จัดทำรายการทั่วไปเสนอต่อรัฐสภาเป็นรายปีเกี่ยวกับการปฏิบัติงานของตนในเรื่องที่เห็นสมควร

อำนาจหน้าที่ของคณะกรรมการพิเศษ Data Protection Tribune สรุปได้ดังนี้

1) รับพิจารณาอุทธรณ์เรื่องการปฏิเสธการจดทะเบียนของ Registrar รวมทั้งการปฏิเสธการเปลี่ยนแปลงการจดทะเบียน

2) รับพิจารณาอุทธรณ์เกี่ยวกับการออกคำเตือนของ Registrar

3) มีอำนาจในการพิจารณาทบทวนข้อเท็จจริงเกี่ยวกับเรื่องที่อุทธรณ์

4) มีอำนาจสั่งให้ Registrar ดำเนินการใหม่หรือยกอุทธรณ์นั้นๆ

ขอบเขตการใช้ Data Protection Act

1) กำหนดไม่ให้บุคคลผู้ปฏิบัติงานอยู่ในสำนักงานคอมพิวเตอร์ หรือตัวแทนของบุคคลดังกล่าวเปิดเผยข้อมูลอันเกี่ยวกับบุคคลโดยปราศจากอำนาจ ถ้าบุคคลใดฝ่าฝืนโดยเจตนาหรือไม่นำพาถึงผลที่เกิดขึ้นถือว่ากระทำผิดตามกฎหมายนี้

2) กำหนดสิทธิของบุคคลผู้ถูกระบุในข้อมูลนั้นเช่น สิทธิที่จะทราบว่าตนถูกระบุอยู่ในข้อมูลนั้นๆ หรือไม่ ระบุอย่างไร สิทธิเข้าสู่ข้อมูลของตน สิทธิในการแก้ไขหรือลบล้างข้อมูลดังกล่าวที่ผิดพลาด สิทธิอนุญาตหรือไม่อนุญาตให้มีการเปิดเผยข้อมูลนั้น สิทธิในการรับค่าเสียหาย กรณีได้รับความเสียหายจากข้อมูลที่เกี่ยวกับบุคคลที่ผิดพลาด

3) กำหนดหลักการคุ้มครองข้อมูลของบุคคลไว้ ดังนี้

(1) ข่าวสารที่ได้รับในรูปแบบและการดำเนินการของข้อมูลส่วนบุคคลต้องได้มาโดยถูกต้องชอบธรรมตามกฎหมาย

(2) ข้อมูลส่วนบุคคลจะเก็บสะสมเท่าที่ระบุในการจดทะเบียนและตามวัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น

(3) ข้อมูลส่วนบุคคลเก็บไว้เพื่อวัตถุประสงค์ใดก็สามารถใช้และเปิดเผยไม่เกินกว่าวัตถุประสงค์นั้น

(4) ข้อมูลส่วนบุคคลเก็บไว้เพื่อวัตถุประสงค์ใดต้องมีความสัมพันธ์เกี่ยวข้องไม่เกินกว่าความสัมพันธ์ต่อวัตถุประสงค์นั้น

(5) ข้อมูลส่วนบุคคลต้องได้รับการจัดทำให้ถูกต้องทันสมัยเท่าที่จำเป็น

(6) ข้อมูลส่วนบุคคลต้องไม่จัดเก็บไว้นานกว่าที่จำเป็นตามวัตถุประสงค์ในการจัดเก็บ

4) บุคคลหนึ่งๆ จะได้รับสิทธิดังนี้

(1) สิทธิที่จะได้รับการบอกกล่าวจากบุคคลผู้เก็บหรือถือข้อมูลว่าตนได้ถือหรือเก็บข้อมูลของบุคคลดังกล่าวนั้นๆ หรือไม่

(2) สิทธิที่จะเข้าสู่ข้อมูลส่วนบุคคลที่บุคคลอื่นจัดเก็บไว้ ซึ่งทั้งการบอกกล่าวและการเข้าถึงข้อมูลจะต้องเป็นไปในระยะเวลาอันสมควร โดยไม่ชักช้าหรือเสียค่าใช้จ่ายเกินควร

(3) สิทธิที่จะแก้ไขหรือลบข้อมูลดังกล่าวตามสมควร

(4) ข้อมูลเกี่ยวกับบุคคลที่จัดเก็บไว้โดยบุคคลผู้ถือหรือเก็บข้อมูลหรือเกี่ยวข้องกับบริการ ซึ่งจัดหาโดยดำเนินการในสำนักงานคอมพิวเตอร์ จะต้องได้รับการให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมต่อการเข้าถึงการจัดการ เปิดเผย หรือทำลายโดยไม่ได้รับอนุญาตและมีมาตรการการรักษาความปลอดภัยที่อาจเกิดขึ้นที่ทำให้เกิดการสูญหายหรือการทำลายโดยอุบัติเหตุ

อย่างไรก็ตาม มีข้อยกเว้นที่Data Protection Act ได้กำหนดข้อยกเว้นจากบัญญัติของกฎหมายฉบับนี้ไว้ในกรณีดังนี้

1) กรณีเกี่ยวกับความมั่นคงแห่งชาติ ข้อมูลส่วนบุคคลอาจได้รับการยกเว้นจากบทบัญญัติว่าด้วยการเข้าถึงข้อมูล บทบัญญัติว่าด้วยการชดใช้ค่าเสียหาย บทบัญญัติว่าด้วยการแก้ไข บทบัญญัติห้ามเปิดเผยและบทบัญญัติที่เกี่ยวข้องและเป็นไปเพื่อวัตถุประสงค์ในการรักษาความมั่นคงแห่งชาติ

2) กรณีเกี่ยวกับอาชญากรรมและภาษีอากร ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการป้องกันหรือสืบหาเกี่ยวกับอาชญากรรม การจัดหรือดำเนินคดีผู้กระทำผิดทางอาญาหรือประเมินหรือจัดเก็บภาษีเหล่านี้ได้รับการยกเว้นจากบทบัญญัติการเข้าถึง ถ้าการเข้าถึงก่อให้เกิดความเสียหายต่อวัตถุประสงค์ดังกล่าว นอกจากนี้หากมีการจัดเก็บเพื่อวัตถุประสงค์ในการปฏิบัติหน้าที่ตามกฎหมายและข้อมูลนั้นประกอบด้วยข้อมูลที่มาจากครอบครองของบุคคลอื่น เพื่อวัตถุประสงค์ที่กล่าวแล้วก็ได้รับการยกเว้นจากการเปิดเผยเช่นกัน และถ้าหากการเปิดเผยเป็นไปตามวัตถุประสงค์ข้างต้นหรือการใช้บทบัญญัติห้ามเปิดเผยตามกฎหมายนี้จะก่อให้เกิดความเสียหายต่อกรณีเหล่านี้ก็จะได้รับการยกเว้นจากบทบัญญัติห้ามเปิดเผย

3) กรณีเกี่ยวกับงานด้านสุขภาพและสังคม ในกรณีที่ข้อมูลนั้นประกอบด้วยข้อมูลที่เกี่ยวกับบุคคลในเรื่องสุขภาพและจิตใจของบุคคล Secretary of State อาจออกคำสั่งให้ได้รับการยกเว้นจากบทบัญญัติการเข้าถึงของบุคคลหรืออาจแก้ไขปรับปรุงบทบัญญัตินั้นๆ นอกจากนี้ถ้าเป็นข้อมูลที่จะต้องเก็บไว้หรือได้มาในระหว่างการดำเนินงานด้านสังคมที่เกี่ยวกับบุคคล ซึ่งจัดเก็บและรักษาไว้โดยรัฐบาลหรือเจ้าหน้าที่ส่วนท้องถิ่น Secretary of State อาจออกคำสั่งยกเว้นจากบทบัญญัติเรื่องการเข้าถึงของบุคคลหรืออาจแก้ไขปรับปรุงบทบัญญัติได้เช่นกัน อย่างไรก็ตาม ในกรณีหลังนี้จะยกเว้นหรือปรับปรุงแก้ไขได้เฉพาะเมื่อการใช้บัญญัติดังกล่าวก่อให้เกิดผลร้ายต่อการดำเนินงานด้านสังคมให้เรียบร้อย

4) กรณีเกี่ยวกับการออกกฎระเบียบด้านการบริหารทางการเงิน ข้อมูลเกี่ยวกับบุคคลเพื่อการปฏิบัติหน้าที่ตามกฎหมายอาจเป็นหน้าที่ที่ Secretary of State ได้กำหนดเพื่อให้เป็นไปตามวัตถุประสงค์ของมาตรานี้ หรือเป็นหน้าที่ที่กำหนดเพื่อคุ้มครองสมาชิกของสังคมต่อความสูญเสียทางการเงินเพราะความทุจริต ความไม่มีอำนาจหรือการปฏิบัติการในทางมิชอบของผู้ดำเนินกิจการด้านธนาคาร การประกันภัย การลงทุนหรือการบริการทางการเงินอื่นๆ หรือในการจัดการบริษัทข้อมูลดังกล่าวจะได้รับการยกเว้นจากการใช้บทบัญญัติว่าด้วยการเข้าถึงข่าวสารของบุคคล หากการใช้บทบัญญัติดังกล่าวอาจก่อให้เกิดความเสียหายต่อการปฏิบัติหน้าที่นั้นๆ

5) กรณีเกี่ยวกับสิทธิพิเศษทางอาชีพด้านกฎหมายและคำพิพากษาของศาล กรณีข้อมูลส่วนบุคคลที่หน่วยงานของรัฐบาลได้รับจากบุคคลที่สาม เป็นข้อมูลที่ถือว่าเกี่ยวกับคำพิพากษาของศาล จะได้รับการยกเว้นจากบทบัญญัติเรื่องการเข้าถึง และถือว่าได้รับสิทธิหรือความคุ้มครองพิเศษในทางวิชาชีพด้านกฎหมาย เป็นความลับระหว่างลูกความและผู้มีวิชาชีพให้คำปรึกษาทางด้านกฎหมาย ซึ่งสามารถรักษาไว้ได้ในการดำเนินกระบวนการตามกฎหมายก็จะได้รับการยกเว้นเช่นกัน

6) กรณีเกี่ยวกับบัญชีเงินเดือนและบัญชีรายรับรายจ่าย หากข้อมูลส่วนบุคคลใช้เพื่อวัตถุประสงค์ด้านการคำนวณจำนวนเงินใช้จ่ายเป็นค่าตอบแทนหรือเงินชดเชยเกี่ยวกับการทำงานในการจ้างงานหรือหน้าที่ใดหรือในการจ่ายหรือจำนวนที่หักออกจากเงินดังกล่า หรือเพื่อวัตถุประสงค์ในการเก็บรักษาบัญชีรายชีรายรับรายจ่ายที่เกี่ยวกับกิจการงานนั้นหรือเพื่อการคาดคะเนเกี่ยวกับการจัดการหรือเพื่อช่วยการประกอบกิจการงานหรือธุรกิจนั้นๆ เหล่านี้จะได้รับการยกเว้นจากบทบัญญัติการเข้าถึงข่าวสาร บทบัญญัติว่าด้วยการชดใช้ค่าเสียหาย การแก้ไข การห้ามเปิดเผย ภายใต้เงื่อนไขข้อมูลเหล่าสี้ต้องไม่ใช้เกินกว่าวัตถุประสงค์ที่ได้ระบุไว้ และต้องไม่เปิดเผยเว้นแต่เป็นไปตามข้อยกเว้นที่ระบุไว้ในมาตรานี้

7) กรณีเกี่ยวกับข้อมูลส่วนบุคคลที่จัดเก็บเพื่อใช้ภายในบ้านของตน หรือเพื่อวัตถุประสงค์อื่นๆอันจำกัด กรณีนี้ข้อมูลส่วนบุคคลที่จัดเก็บโดยบุคคลหนึ่งที่เกี่ยวกับเรื่องการจัดการเรื่องส่วนตัว ครอบครัวหรือกิจการเกี่ยวกับบุคคลที่อาศัยอยู่ในบ้านหรือเก็บไว้เพื่อใช้ในทางการบันเทิง เหล่านี้ได้รับการยกเว้นจากบทบัญญัติเรื่องการเข้าถึง การชดใช้ค่าเสียหาย การแก้ไข การห้ามเปิดเผย

8) กรณีข้อมูลเกี่ยวกับบุคคลได้รับการจัดเก็บโดยสมาชิกของสโมสรซึ่งไม่ได้จัดตั้งเป็นรูปบริษัทและเกี่ยวข้องกับสมาชิกของสโมสรเท่านั้น ยังรวมถึงข้อมูลที่เก็บรักษาไว้โดยผู้ใช้ข้อมูลเพื่อจุดประสงค์การจำหน่ายจ่ายแจกข่าวสารหรือบทความผู้ซึ่งถูกบันทึกข้อมูลที่เกี่ยวกับตนหรือเพื่อบันทึกการจำหน่ายจ่ายแจกข้อมูลหรือบทความนั้นๆ และข้อมูลดังกล่าวประกอบไปด้วยชื่อและที่อยู่ของบุคคลเหล่านั้น หรือสิ่งที่จำเป็นเพื่อแจกจ่ายข้อมูล ในสองกรณีหลังนี้จะได้รับการยกเว้นเช่นกันแต่มีเงื่อนไขว่าต้องมีการสอบถามได้รับความยินยอมจากบุคคลผู้ถูกบันทึกข้อมูลเสียก่อน

9) ข้อมูลเกี่ยวกับบุคคล ที่ใช้เพื่อวัตถุประสงค์ในการจัดเตรียมทางด้านสถิติหรือการค้นคว้า จะได้รับยกเว้นจากบทบัญญัติว่าด้วยการเข้าถึงของบุคคล แต่ต้องไม่ใช่หรือเปิดเผยข้อมูลนั้นเพื่อจุดประสงค์อื่น และทั้งผลของการค้นคว้าหรือสถิติจะต้องไม่อยู่ในรูปที่อาจบ่งชี้ถึงบุคคลที่ถูกบันทึกหรือสิ่งอื่นใดเกี่ยวกับบุคคลเหล่านั้น

10) กรณีเกี่ยวกับคะแนนในการทดสอบ ในกรณีที่ข้อมูลเกี่ยวกับบุคคลประกอบด้วยคะแนนหรือข้อมูลใดๆ ที่ผู้ใช้และเก็บข้อมูลไว้เพื่อการวินิจฉัยทางวิชาการ อาชีพหรือผลการทดสอบอื่นๆ หรือทำให้สามารถวินิจฉัยผลการสอบนั้นๆ ได้ หรือเป็นข้อมูลอันสืบเนื่องจากการวินิจฉัยผลดังกล่าวเหล่านี้ การบังคับใช้บทบัญญัติว่าด้วยสิทธิการเข้าสู่ข้อมูลส่วนบุคคลจะต้องเป็นไปตามที่กำหนดไว้ตามอนุมาตรา

ในการแจ้งการเก็บข้อมูล Data Protection Act ซึ่งบังคับใช้ทั้งภาครัฐและเอกชนนั้น ได้กำหนดวิธีการทำให้บุคคลหนึ่งๆ สามารถรู้ได้ว่าข้อมูลที่เกี่ยวกับตนในหน่วยงานของรัฐหรือหน่วยงานของเอกชนหรือไม่ รวมทั้งข้อมูลนั้นมีลักษณะเนื้อหาหรือถูกระบุไว้อย่างไร โดยประกาศแจ้งให้ทราบเป็นทางการและแจ้งให้ทราบเป็นรายบุคคล ดังนี้

1)กำหนดให้บุคคลหรือองค์กรใดๆ ผู้ต้องการจะถือหรือเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องดำเนินการขออนุญาตจดทะเบียนต่อ Data Protection Registrar และจะต้องระบุรายละเอียดที่สำคัญเพื่อให้ทราบถึงสถานที่เก็บข้อมูล แหล่งข้อมูล ลักษณะของข้อมูล

ข่าวสารที่จะถือหรือเก็บรวบรวมและกำหนดให้ Data Protection Registrar ดำเนินการเพื่อให้สาธารณะชนสามารถตรวจดูทะเบียนที่จดนั้นได้โดยสะดวก

2) ภายใต้บทบัญญัติมาตรานี้ การจดทะเบียนของผู้เก็บและใช้ข้อมูลจะต้องประกอบไปด้วยสิ่งเหล่านี้

(1) ชื่อและสถานที่อยู่ของผู้เก็บและใช้ข้อมูล

(2) แจ้งถึงข้อมูลอันเกี่ยวกับบุคคลนั้นจะถือไว้ และวัตถุประสงค์ในการเก็บและใช้ข้อมุลนั้น

(3) แจ้งถึงแหล่งต่างๆ ที่บุคคลนั้นมุ่งหมายหรือคาดว่าอาจจะได้มาซึ่งข้อมูลที่จะจัดเก็บไว้

(4) แจ้งถึงบุคคลใดๆ ที่มุ่งหมายหรือคาดว่าอาจจะมีการเปิดเผยข้อมูลนั้น

(5) แจ้งรายชื่อหรือประเทศนอกประเทศอังกฤษที่มุ่งหมายหรือคาดหวังว่าอาจจะมีการสื่อข้อมูลไปยังประเทศดังกล่าวทั้งทางตรงและโดยทางอ้อม

(6) สถานที่ใดๆ ที่จะรับคำร้องขอเข้าสู่ข้อมูลของตน ของบุคคลผู้ถูกระบุไว้ในข้อมูลข่าวสารนั้น

3) หากเป็นการจดทะเบียนในกรณีของผู้ปฏิบัติงานในสำนักงานคอมพิวเตอร์จะต้องระบุชื่อและที่อยู่ของบุคคลนั้นๆ ลงในทะเบียนด้วย กรณีที่เป็นบริษัทที่จดทะเบียนแล้วจะต้องระบุหมายเลขที่ทำการจดทะเบียนตั้งบริษัทไว้ในทะเบียนสถานที่อยู่คือสถานที่หลักในการประกอบธุรกิจ

4) Registrar จะต้องดำเนินการให้ความสะดวกโดยจัดให้ข้อมูลที่มีอยู่ในทะเบียนสามารถเข้าถึงได้เพื่อตรวจตราในรูปแบบที่เห็นได้และเข้าใจได้ง่ายโดยสาธารณชนในช่วงเวลาและอัตราค่าธรรมเนียมที่เหมาะสม

5) กำหนดให้ผู้เก็บและใช้ข้อมูลที่ได้รับคำร้องขอเป็นหนังสือจากบุคคลหนึ่งๆ จะต้องบอกกล่าวให้บุคคลนั้นทราบว่าตนมีข้อมูลซึ่งระบุถึงบุคคลผู้ร้องขอหรือไม่อย่างไร

ในการเข้าสู่ข้อมูล สิทธิที่จะได้รับสำเนาบันทึกข้อมูลเกี่ยวกับตนจากผู้เก็บและใช้ข้อมูลนั้นๆ ไว้ หากข้อมูลนั้นอยู่ในรูปแบบหรือถ้อยคำที่ไม่อาจเข้าใจได้ หากไม่มีการอธิบายจะต้องมีคำอธิบายประกอบข้อมูลข่าวสารนั้นๆ ให้มาด้วยพร้อมกับสำเนาข้อมูลนั้น การร้องขอดังกล่าวจะต้องเป็นไปตามเงื่อนไขที่กำหนดไว้ โดยสรุปได้ดังนี้

1) คำร้องขอต้องทำเป็นหนังสือและจ่ายค่าธรรมเนียมในการร้องขอ ซึ่งหากไม่ระบุไว้เป็นอย่างอื่น การร้องขอเพื่อที่จะได้รับการแจ้งให้ทราบว่ามีข้อมูลที่เกี่ยวกับตนหรือไม่ หากมีจะได้รับสำเนาข้อมูลนั้นๆ ด้วย และหากผู้เก็บและใช้ข้อมูลได้จดทะเบียนในการเก็บและใช้แยกเป็นกรณีๆ จะต้องทำคำร้องขอและจ่ายค่าธรรมเนียมแยกกัน

2) ผู้ร้องขอจะต้องแสดงหลักฐานประจำตัวและระบุรายละเอียดถึงข้อมูลที่ตนต้องการตามที่ผู้เก็บและใช้ข้อมูลได้กำหนดไว้ตามสมควร และถาเป็นข้อมูลที่เมื่อเปิดเผยแล้วจะต้องเปิดเผยถึงข้อมูลอันเกี่ยวกับบุคคลอื่นๆ จะต้องมีการอนุญาตจากบุคคลนั้นๆ

3) ระยะเวลาในการตอบคำถามจะต้องตอบสนองคำร้องนั้นภายใน 40 วัน หลังจากที่ได้รับคำร้องขอและหลักฐานต่างๆ ตามเงื่อนไขที่กำหนดไว้

4) นอกจากนี้ได้ให้อำนาจ Secretary of State ที่จะแก้ไขหรือยกเว้นบทบัญญัติที่เกี่ยวกับการเข้าสู่ข้อมูลของบุคคลหนึ่งๆ ได้ตามสมควร ในกรณีที่ข้อมูลนั้นเป็นเรื่องสุขภาพและจิตใจของบุคคล ดังนั้นในกรณีที่เป็นข้อมูลข่าวสารทางการแพทย์ที่การเข้าสู่ข้อมูลนั้นโดยตรง อาจจะเป็นผลร้ายต่อบุคคลผู้ร้องขอได้ Secretary of State ย่อมมีอำนาจออกกฎระเบียบให้การเข้าสู่ข้อมูลดังกล่าวเป็นไปโดยอ้อม หรือเข้าสู่ข้อมูลที่เกี่ยวกับบุคคลอื่นๆ

ด้านการแก้ไขเพิ่มเติมข้อมูล ตามกฎหมายฉบับนี้การรับรองคุ้มครองสิทธิที่จะแก้ไขเพิ่มเติมข้อมูลที่เกี่ยวกับบุคคล แยกพิจารณาได้ 2 กรณี คือ

1) การร้องขอแก้ไขเพิ่มเติมข้อมูลของตน โดยร้องขอกับผู้จัดเก็บและใช้ข้อมูลนั้นโดยตรง

2) การร้องขอแก้ไขเพิ่มเติมข้อมูลของตนโดยร้องขอต่อศาล

บุคคลหนึ่งๆ จะต้องได้รับสิทธิที่จะแก้ไขเพิ่มเติมหรือลบข้อมูลของตน ดังนั้น Data Protection Act นี้กำหนดให้ใช้บังคับกับผู้จัดเก็บและใช้ข้อมูลส่วนบุคคล และผู้ปฏิบัติงานในสำนักงานคอมพิวเตอร์ซึ่งเก็บและใช้ข้อมูลดังกล่าว บุคคลหนึ่งๆ จึงสามารถร้องขอแก้ไขเพิ่มเติมข้อมูลของตนที่ได้ใช้สิทธิในการเข้าสู่ข้อมูลนั้นเพื่อตรวจดูและได้รับสำเนาข้อมูลหากพบว่ามีความผิดพลาดหรือไม่เป็นไปตามกฎหมายกำหนดไว้ จากหน่วยงานหรือบุคคลผู้ที่จัดเก็บข้อมูลดังกล่าว และจากหลักการคุ้มครองข้างต้นนี้ หน่วยงานหรือบุคคลผู้จักเก็บข้อมูลที่เกี่ยวกับบุคคลจะต้องดำเนินการเพื่อให้เป็นไปตามหลักการคุ้มครองเช่นว่านี้ โดยจะต้องรับคำร้องขอดังกล่าว และดำเนินการต่างๆ หากพบว่าข้อมูลส่วนบุคคลที่ตนจัดเก็บไว้มีความผิดพลาดหรือบกพร่อง หรือไม่เป็นไปตามกฎหมายที่กำหนดไว้ก็ต้องดำเนินการแก้ไขเพิ่มเติมหรือลบข้อมูลเช่นว่านั้น

หากหน่วยงานหรือผู้จัดเก็บดังกล่าวไม่ดำเนินการตามหลักการที่ว่านี้ บุคคลผู้ร้องขออาจยื่นคำร้องแก่ Data Protection Registrar ว่ามีการล่วงละเมิดหลักการคุ้มครองข้อมูลข่าวสาร และเจ้าหน้าที่ดังกล่าวจะดำเนินการกับผู้ฝ่าฝืนตามที่กฎหมายฉบับนี้ได้กำหนดไว้ก็อาจยื่นคำร้องขอต่อศาลให้มีการดำเนินการนั้นๆ

3) การร้องขอแก้ไขเพิ่มเติมข้อมูลของตนโดยร้องขอต่อศาล

การที่สิทธิของบุคคลหนึ่งๆ ได้รับการคุ้มครองไว้ตามกฎหมายถูกล่วงละเมิด บุคคลผู้ได้รับความกระทบกระเทือนย่อมมีสิทธิที่จะร้องขอต่อศาล เพื่อให้มีการบังคับการตามสิทธิของตนได้ แต่ตม Data Protection Act นี้ได้กำหนดรับรองในการร้องขอแก้ไขเพิ่มเติมหรือลบข้อมูลที่เกี่ยวกับตน ตามที่บุคคลดังกล่าวมีสิทธิเช่นนั้นอีกชั้นหนึ่ง โดยกำหนดเงื่อนไขที่จะษมารถร้องขอต่อศาล รวมทั้งอำนาจของศาลในการออกคำสั่งเรื่องนี้

พระราชบัญญัติความเป็นอิสระของข้อมูลของสหราชอาณาจักรไม่เหมือนกฎหมายในลักษณะเดียวกันนี้ของประเทศอื่นๆ ตรงที่ไม่ได้ให้รายละเอียดของข้อมูลที่หน่วยงานราชการแต่ละแห่งจะต้องตีพิมพ์เผยแพร่ แม้ว่าจะไม่มีผู้ใดร้องขอก็ตาม มาตรา 19 กำหนดว่าหน่วยงานราชการทุกแห่งจะต้องสร้าง ผลิตและดำเนินการโครงการจัดพิมพ์ซึ่งระบุประเภทของข้อมูลที่หน่วยงานจัดตีพิมพ์ ลักษณะของเอกสารที่ตีพิมพ์ออกมาและกำหนดว่าจะจัดเก็บค่าธรรมเนียม สำหรับเอกสารที่ตีพิมพ์เป็นบางอย่างโดยเฉพาะเจาะจงหรือไม่ การดำเนินการโครงการจัดพิมพ์ดังกล่าว หน่วยงานราชการจะต้องพิจารณาถึงผลประโยชน์ของสาธารณชนต่อการเข้าถึงข้อมูลข่าวสารที่หน่วยงานมีอยู่และต่อเหตุผลของหน่วยงานในการตัดสินใจตีพิมพ์เช่นนั้น

ที่สำคัญยิ่งคือโครงการจัดพิมพ์ต้องได้รับการยินยอมโดยคณะกรรมการพิจารณาข้อมูลข่าวสาร คณะกรรมการสามารถกำหนดเวลาสิ้นสุดสำหรับการอนุญาตของตนดังกล่าวได้ หรือสามารถยกเลิกการอนุญาตโดยมีจดหมายแจ้งยกเลิกดังกล่าวมายังหน่วยงานเป็นระยะเวลาหกเดือนก่อนการยกเลิก นอกเหนือจากนี้พระราชบัญญัติดังกล่าวยังได้กำหนดให้คณะกรรมการพิจารณาข้อมูลข่าวสารจัดทำโครงการจัดพิมพ์ในรูปแบบต่างๆ สำหรับหน่วยงานราชการต่างประเภทกัน ตราบเท่าที่โครงการจัดพิมพ์ได้รับความเห็นชอบหน่วยงานราชการที่อยู่ในประเภทหน่วยงานนั้นๆ สามารถนำเอารูปแบบโครงการจัดพิมพ์มาปรับใช้ได้เลยโดยไม่ต้องจัดทำขึ้นมาใหม่

พระราชบัญญัติความเป็นอิสระของข้อมูลของสหราชอาณาจักรมีข้อยกเว้นที่กว้างขวางมากซึ่งปรากฏอยู่ในพระราชบัญญัติในฐานะข้อยกเว้น ซึ่งสะท้อนให้เห็น

ถึงความหมกมุ่นที่ราชการมีต่อความลับต่างๆ มีข้อยกเว้นทั่วไป 3 ข้อ และมีข้อยกเว้นโดยเฉพาะเจาะจง 20 ข้อ ข้อยกเว้นส่วนใหญ่นั้นจะชัดเจน ไม่จำกัดและในบางกรณีมีข้อยกเว้นในกฎหมายนี้ของสหราชอาณาจักรมากกว่าข้อยกเว้นในกฎหมายแบบเดียวกันนี้ของประเทศอื่นๆ

ข้อยกเว้นบางส่วนขึ้นอยู่กับผลจากแบบทดสอบความเป็นอันตราย ซึ่งจะทำให้ต้องอยู่ในประเภทข้อมูลที่ต้องยกเว้นไม่ให้เปิดเผย ข้อมูลที่อยู่ในข้อยกเว้นไม่ต้องเปิดเผยได้แก่ข้อมูลดังต่อไปนี้ ข้อมูลที่สามารถเข้าถึงได้โดยวิธีทางอื่นๆ นอกจากการร้องขอให้เปิดเผย (มาตรา 21) ข้อมูลที่หน่วยงานตั้งใจจะตีพิมพ์เผยแพร่อยู่แล้ว (มาตรา 22) ข้อมูลที่เกี่ยวกับหน่วยงานความมั่นคง (มาตรา 23) ข้อมูลลับที่ได้มาจากประเทศอื่นๆ หรือจากหน่วยงานระหว่างรัฐบาลของประเทศต่างๆ (มาตรา 27 (2)) การสืบสวนสอบสวนของหน่วยงานราชการ (มาตรา 30) บันทึกของศาล (มาตรา 32) อภิสิทธิ์ของรัฐสภา (มาตรา 34) กระบวนการก่อตัวของนโยบายรัฐบาล (มาตรา 35) การสื่อสารที่มีถึงพระราชินีอลิซาเบธ (มาตรา 37) ข้อมูลส่วนบุคคล (มาตรา 40) ข้อมูลลับ (มาตรา 41) ข้อมูลที่ได้รับความคุ้มครองตามกฎหมาย (มาตรา 42) ความลับทางการค้า (มาตรา 43(1)) และข้อมูลที่กฎหมายอื่นหรือข้อบังคับของประชาคมยุโรป (European Community) บัญญัติห้ามมิให้เปิดเผย (มาตรา 44)

ในพระราชบัญญัติฉบับนี้ยังได้ระบุถึงแบบทดสอบผลประโยชน์ของสาธารณชนซึ่งได้กำหนดว่าจะต้องไม่มีการเปิดเผยข้อมูลในกรณีที่ “ผลประโยชน์ของสาธารณชนในการรักษาให้เป็นความลับมีมากกว่าผลประโยชน์ของสาธารณชนในการเปิดเผยข้อมูลดังกล่าว” นี่เป็นแบบทดสอบที่ดีที่กำหนดให้เหตุผลในการยกเว้นการเปิดเผยมีน้ำหนักมากกว่าเหตุผลในการเปิดเผย อย่างไรก็ตาม ในมาตรา 2 (3) ได้ระบุถึงข้อยกเว้นจำนวนหนึ่งที่ไม่สามารถอ้างผลประโยชน์ของสาธารณชนมาขอให้เปิดเผยข้อมูลได้ ซึ่งได้แก่ข้อมูลต่อไปนี้ ข้อมูลที่สามารถเข้าถึงได้โดยวิธีทางอื่นๆ (มาตรา 21) ข้อมูลที่เกี่ยวกับหน่วยงานความมั่นคง (มาตรา 23) บันทึกของศาล (มาตรา 32) อภิสิทธิ์ของรัฐสภา (มาตรา 34) การดำเนินการกิจการสาธารณชนของสภาสูงและสภาล่าง (มาตรา 36) ข้อมูลส่วนบุคคล (มาตรา 40) ข้อมูลลับ (มาตรา 41) และข้อมูลที่กฎหมายอื่นหรือข้อบังคับของประชาคมยุโรปบัญญัติห้ามมิให้เปิดเผย (มาตรา 44)

ข้อยกเว้นที่เกี่ยวกับการมิให้เปิดเผยข้อมูลเพราะอ้างผลประโยชน์ของสาธารณชนมีอยู่หลายข้อแต่ข้อยกเว้นที่สำคัญยิ่งคืออำนาจของหัวหน้าส่วนราชการที่สามารถขัดคำตัดสินของคณะกรรมการพิจารณาข้อมูลข่าวสารได้ มาตรา 53 อนุญาตให้ผู้รับผิดชอบในหน่วยงานราชการต่างๆ ซึ่งอยู่ภายใต้มาตรานี้ ซึ่งก็คือรัฐมนตรีให้สามารถลงนามในคำรับรองภายในระยะเวลา 20 วัน หลังจากที่คณะกรรมการพิจารณาข้อมูลข่าวสารได้มีคำตัดสินออกมา

ให้เปิดเผยข้อมูลเพราะอ้างผลประโยชน์ของสาธารณชน ว่ามีเหตุผลความจำเป็นเพียงพอที่การไม่เปิดเผยข้อมูลนั้นจะไม่ขัดต่อกฎหมายที่มีอยู่

คำรับรองของหัวหน้าส่วนราชการดังกล่าวจะมีผลยกเลิกคำตัดสินของคณะกรรมการพิจารณาข้อมูลข่าวสาร หน่วยงานราชการที่หัวหน้าส่วนราชการสามารถใช้อำนาจดังกล่าวได้ ได้แก่กระทรวง ทบวง กรมทุกแห่ง รัฐสภาของเวลส์และหน่วยงานราชการอื่นๆ ที่กำหนดโดยรัฐมนตรี ในทางปฏิบัติ มาตรานี้ลดทอนอำนาจของคณะกรรมการพิจารณาข้อมูลข่าวสารที่สามารถอ้างเรื่องของผลประโยชน์สาธารณชน

นอกจากนี้ พระราชบัญญัตินี้ยังมีข้อยกเว้นมิให้เปิดเผยข้อมูลสำหรับข้อมูลที่จำเป็นต่อการรักษาความมั่นคงของชาติ หรือการเปิดเผยในสิ่งที่เป็นผลร้ายต่อกระทรวงกลาโหมอย่างไรก็ตาม เฉกเช่นเดียวกับหน่วยงานความมั่นคงคำรับรองจากรัฐมนตรีว่าข้อมูลนั้นสำคัญต่อความมั่นคงของชาติ เป็นหลักฐานสำคัญที่จะรับรองข้อเท็จจริงดังกล่าว

ข้อมูลจะถูกยกเว้นมิให้เปิดเผยหากว่าเป็นข้อมูลของกระทรวง ทบวง กรมหรือรัฐสภาของเวลส์และเกี่ยวข้องกับการก่อตัวหรือพัฒนาการของนโยบายรัฐบาล อย่างไรก็ตาม ข้อยกเว้นดังกล่าวจะไม่ใช้บังคับแก่ข้อมูลที่เป็นตัวเลขสถิติ ในภายหลังจากที่มีการนำเอานโยบายมาปรับใช้แล้ว ทว่าสำหรับข้อมูลอื่นๆ ที่เกี่ยวข้องกับการก่อตัวของนโยบายก็ยังคงได้รับการยกเว้นไม่ต้องเปิดเผยอยู่ต่อไป ข้อมูลนั้นจะได้รับการยกเว้นมิให้เปิดเผยหากว่าเกี่ยวข้องกับการสื่อสารระหว่างรัฐมนตรีหรือเกี่ยวกับงานของสำนักงานเลขาธิการรัฐมนตรี ข้อมูลจะถูกยกเว้นมิให้เปิดเผยเช่นกันหากว่าการเปิดเผยข้อมูลจะขัดขวางการให้คำแนะนำที่เป็นอิสระและยุติธรรม หรือมิฉะนั้นก็ก่อให้เกิดผลร้ายต่อการบริหารงานสาธารณอย่างมีประสิทธิภาพ

พระราชบัญญัติความเป็นอิสระของข้อมูลยังคงสงวนสิทธิสำหรับความลับที่กำหนดให้ปกปิดในกฎหมายอื่นๆ เช่นเดียวกับความลับที่ห้ามเปิดเผยโดยข้อบังคับของประชาคมยุโรปหรือโดยระเบียบข้อบังคับของศาล อย่างไรก็ตาม พระราชบัญญัติฉบับนี้ได้ให้อำนาจแก่รัฐมนตรีที่จะยกเลิกหรือแก้ไขพระราชบัญญัติฉบับนี้โดยออกกฎหมายที่จำกัดการเปิดเผยข้อมูลแทน

ในพระราชบัญญัตินี้มีหลายมาตราที่เกี่ยวกับบันทึกทางประวัติศาสตร์ที่กำหนดว่าเป็นบันทึกที่มีอายุมากกว่า 30 ปี ข้อยกเว้นมิให้เปิดเผยทั้งหมดไม่สามารถมาใช้บังคับกับบันทึกทางประวัติศาสตร์ได้ รวมถึงบันทึกทางประวัติศาสตร์เกี่ยวกับความสัมพันธ์

ภายในสหราชอาณาจักร (มาตรา 28) ข้อมูลของศาล (มาตรา 32) บันทึกทางประวัติศาสตร์ที่เกี่ยวกับกระบวนการภายในรัฐบาล (มาตรา 35 และมาตรา 36) และข้อมูลความลับเชิงพาณิชย์ (มาตรา 43)

ในพระราชบัญญัติความเป็นอิสระของข้อมูลได้กำหนดให้มีการอุทธรณ์ไว้ 3 ระดับ กล่าวคือ ระดับแรกคือ การอุทธรณ์ภายในหน่วยงานราชการที่มีข้อมูลดังกล่าว ระดับที่สองคือ การอุทธรณ์ต่อคณะกรรมการพิจารณาข้อมูลข่าวสาร และ ระดับที่สามคือ การอุทธรณ์ต่อศาลพิเศษทางด้านข้อมูลข่าวสาร (Special Infomation Tribunal)

คณะกรรมการพิจารณาข้อมูลข่าวสารและศาลพิเศษทางด้านข้อมูลข่าวสารเป็นหน่วยงานที่ตั้งขึ้นตามพระราชบัญญัติการปกป้องข้อมูลข่าวสาร ปี 1998 (The Data Protection Act 1998) คณะกรรมการพิจารณาข้อมูลข่าวสารแต่งตั้งโดยพระราชินีอลิซาเบธ ส่วนศาลพิเศษทางด้านข้อมูลข่าวสารนั้นประกอบด้วยผู้ว่าการและผู้ช่วยผู้ว่าการจำนวนหนึ่งซึ่งแต่งตั้งโดย Lord Chancellor (ซึ่งก็คือรัฐมนตรีกระทรวงยุติธรรม) เช่นเดียวกับคณะกรรมการของศาลซึ่งแต่งตั้งโดยรัฐมนตรี แม้ว่าจะเป็นหน่วยงานที่มีการแต่งตั้งโดยผู้ที่มีอำนาจเหนือกว่าแต่หน่วยงานทั้งสองก็ปฏิบัติงานเป็นหน่วยงานอิสระ

นอกจากนี้ อังกฤษมีกฎหมาย The Anti-Terrorism Crime and Security Act 2001 ใน Part 11 ระบุให้มีการเก็บรักษาข้อมูลที่ผ่านการให้บริการ โดยข้อมูลเหล่านี้จะระบุถึง ผู้โทร ผู้รับ และข้อมูลที่มีการติดต่อสื่อสาร เช่น หากมีการใช้โทรศัพท์มือถือ ก็จะมีการเก็บรักษาข้อมูลเกี่ยวกับเจ้าของโทรศัพท์ ผู้ติดต่อ แต่จะไม่รวมสิ่งที่เป็นการสนทนา กฎหมายฉบับนี้ให้ Secretary of State for Home Office จัดทำ “คู่มือการปฏิบัติ (Code of Practice) หรือ อาจออกเป็นกฎหมายลูกรองรับการดำเนินการได้

ในขณะที่ยังมีกฎหมายอื่นๆอีก คือ Data Protection Act 1998 และ The Privacy and Electronic Communication (EC Directive) Regulations 2003. รวมไปถึงมาตรา 8 ของ European Convention on Human Rights

(3) กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

ประเทศสหราชอาณาจักรอังกฤษนำหลักกฎหมายความคุ้มครองฐานข้อมูลสหภาพยุโรปบัญญัติกฎหมายความคุ้มครองแก่ฐานข้อมูลในสหราชอาณาจักรอังกฤษ (U.K. Copyright and Rights in Database Regulation 1997) หรือ เรียกอีกอย่างว่า (The Regulation) ซึ่งมีผลบังคับใช้เมื่อ 1 มกราคม 1998

ในอังกฤษและเวลล์นั้น ได้มีการรับรองทางกฎหมายแก่ฐานข้อมูลใน 2 ลักษณะ คือ

1. ลิขสิทธิ์ (Copyright)
2. สิทธิในฐานข้อมูล (database right)

ทั้งนี้เนื่องจาก กฎหมายลิขสิทธิ์ของอังกฤษนั้น สามารถปรับใช้ได้กับระบบฐานข้อมูลอยู่แล้ว แต่ไม่ทั้งหมด โดยมีเกณฑ์ในการกำหนดความเป็นไปได้ของการมีลิขสิทธิ์ในฐานข้อมูลอยู่ที่ว่า ฐานข้อมูลนั้นมีคุณสมบัติเป็นงานวรรณกรรม (literal works) หรือไม่ ในขณะที่สิทธิในฐานข้อมูลนั้น ได้มีการรับรองให้แก่ทุกฐานข้อมูล

กฎหมายลิขสิทธิ์ของอังกฤษและเวลล์นั้น ได้มี Copyright, Designs and Patents Act 1988 ได้ระบุในมาตรา 3 (1) ว่า งานวรรณกรรม หมายถึง งานใด ที่มากกว่างานทางดนตรี ละคร ซึ่งได้ถูกจัดทำขึ้นโดยการพูด เขียน หรือ การขับร้อง ลิขสิทธิ์จะมีอยู่ในฐานข้อมูล หากมีลักษณะของการสร้างสรรค์เป็นงานต้นแบบ (original) โดยการคัดสรร หรือดำเนินการเนื้อหาในเชิงฐานข้อมูล ทั้งนี้ โดยมีการจัดเก็บ (record) อย่างเป็นระบบด้วย และภายใต้มาตรา 11 (1) ของกฎหมายดังกล่าว ก็ได้ระบุให้ ผู้เขียน บรรณาธิการ หรือผู้เขียนร่วมฐานข้อมูลเป็นผู้มีลิขสิทธิ์ และภายใต้กฎหมายในฐานข้อมูล ถ้าผู้จัดทำฐานข้อมูลได้กระทำขึ้นในฐานะที่ตนเป็นลูกจ้าง แต่หากฐานข้อมูลถูกนำขึ้นในรูปของคณะทำงาน หรือคณะกรรมการ ลิขสิทธิ์จะตกแก่ผู้ลงมือกระทำ ผู้เขียน ไม่ใช่ขององค์กรหรือบริษัทเจ้าของ [53]

(4) กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ประเทศอังกฤษเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางเทคโนโลยีการติดต่อสื่อสารและคอมพิวเตอร์ และกฎหมายอาชญากรรมทางคอมพิวเตอร์ของอังกฤษได้เป็นแบบอย่างการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ให้แก่หลายๆ ประเทศ โดยเฉพาะอย่างยิ่งประเทศในเครือจักรภพของอังกฤษ เช่น กฎหมายสิงคโปร์ มาเลเซีย ออสเตรเลีย และนิวซีแลนด์ เป็นต้น ดังนั้น การศึกษาและทำความเข้าใจกฎหมายของประเทศอังกฤษ จึงเป็นประโยชน์ต่อการพัฒนากฎหมายของประเทศไทยที่เกี่ยวข้องกับเรื่องนี้ต่อไป

ในประเทศอังกฤษ ช่วงกลางปี ค.ศ. 1980 มีความเห็นกันว่า อาชญากรรมทางคอมพิวเตอร์เป็นเพียงการกระทำความผิดเดิมในรูปแบบใหม่เท่านั้น (they were merely

---

53 คดี Blair v. Alan S Tomkins&Anor (1971) และ คดี R. Griggs Group Ltd v. Evans (2003)

old offences appearing in a new guise) และกฎหมายที่ใช้บังคับอยู่สามารถดำเนินคดีกับอาชญากรรมทางคอมพิวเตอร์ได้ ดังนั้น เมื่อเกิดการกระทำความผิดทางคอมพิวเตอร์ จึงพยายามนำกฎหมายที่ใช้บังคับอยู่ไปปรับใช้กับความผิดที่เกิดขึ้น ทั้งๆ ที่กฎหมายนั้นไม่ครอบคลุมถึงความผิดรูปแบบใหม่ที่เกิดขึ้น ซึ่งในที่สุดทำให้เกิดข้อสงสัยเรื่องความชอบธรรมในการใช้กฎหมายของศาล เช่น ในคดี Cox v. Riley

ประเทศอังกฤษมีกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ คือ The Computer Misuse Act 1990 ที่กำหนดความผิดใหญ่ ๆ ไว้ 3 รูปแบบ ได้แก่ ความผิดของการปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence) ความผิดของการปราศจากอำนาจในการเข้าสู่ระบบ ซึ่งเป็นความผิดร้ายแรง หรือให้ความสะดวกแก่ผู้กระทำผิดในการก่อให้เกิดการกระทำความผิดร้ายแรง (Modification of Computer Material) ส่วนวิธีการและหลักเกณฑ์ในการจับกุมตรวจค้นนั้นต้องคำนึงถึง The Police and Criminal Evidence Act 1984 นอกจากนี้ยังมีกฎหมายที่เกี่ยวข้อง คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล The Data Protection Act 1998

การกำหนดฐานความผิดสำหรับการกระทำความผิดต่อคอมพิวเตอร์ใน CMAเป็นไปตามที่คณะกรรมการพัฒนากฎหมายอังกฤษเสนอคือ คณะกรรมการชุดนี้ เห็นว่ารูปแบบหรือลักษณะของกฎหมายที่ดีที่สุดนั้นจะต้องมีการจัดระดับของความผิดไว้เป็นลำดับชั้น (hieachically) คือ

1.ความผิดพื้นฐาน คือ การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (มาตรา 1)

2.ความผิดขั้นสูงหรือความผิดฉกรรจ์ คือ ความผิดที่ใช้สำหรับกรณีที่นักเจาะระบบคอมพิวเตอร์มีเจตนาที่จะกระทำความผิดอย่างอื่นต่อไป หลังจากที่สามารถเข้าถึงระบบคอมพิวเตอร์ได้แล้ว (มาตรา 2)

เมื่อพิจารณากฎหมาย CMA แล้วจะเห็นว่า ลักษณะการบัญญัติกฎหมายของอังกฤษที่กำหนดความผิดแบ่งเป็นความผิดพื้นฐานและความผิดร้ายแรงนี้มีลักษณะคล้ายกับกฎหมายของมลรัฐส่วนใหญ่ในสหรัฐอเมริกา

แนวความคิดในการบัญญัติกฎหมาย CMA ของประเทศอังกฤษแล้ว จะเห็นว่า กฎหมายนี้ถูกบัญญัติขึ้น เพื่อแก้ปัญหาเรื่องการที่กฎหมายที่ใช้บังคับอยู่เดิมไม่สามารถหรือไม่เหมาะสมที่จะนำมาใช้ดำเนินคดีกับความผิดรูปแบบใหม่ เช่น คดี R.v. Gold Shifeen และคดี Cox v. Riley

นอกจากนี้ การประกาศใช้กฎหมาย CMA ก็มีความมุ่งหมายเพื่อให้ความคุ้มครองแก่สิ่งที่ไม่มีรูปร่างโดยเฉพาะ เช่น ข้อมูลคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ เป็นต้น ซึ่งสิ่งต่างๆเหล่านี้ เป็นสิ่งที่เกิดขึ้นในยุคที่สังคมมีการใช้เทคโนโลยีทางการติดต่อสื่อสารและคอมพิวเตอร์ และอยู่นอกเหนือขอบเขตของการได้รับความคุ้มครองตามกฎหมายที่ใช้บังคับอยู่เดิม โดย CMA ได้ให้ความคุ้มครองแก่ความลับ ความครบถ้วน และความสามารถในการใช้ประโยชน์ได้ของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์อย่างครบถ้วน และคุ้มครองสิทธิในทรัพย์สินของเจ้าของทรัพย์สินจากการกระทำความผิดรูปแบบใหม่ด้วย

การทำประเทศอังกฤษมีกฎหมายที่ใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์ โดยเฉพาะนั้น ทำให้สังคมสามารถใช้ประโยชน์ต่างๆจากเทคโนโลยีสารสนเทศได้อย่างเต็มที่ และทำให้สังคมรู้สึกปลอดภัยจากการกระทำความผิดต่อคอมพิวเตอร์ เนื่องจากศาลสามารถลงโทษผู้กระทำความผิดได้อย่างมีประสิทธิภาพ เช่น ในคดี Christopher Pile โดยที่ไม่ต้องไปอาศัยกฎหมายที่ใช้บังคับอยู่เดิมมาปรับใช้กับความผิดรูปแบบใหม่ที่เกิดขึ้น ซึ่งอาจทำให้ไม่สามารถลงโทษผู้กระทำความผิดได้ ดังเช่น คดี R.v.Gold Shefreen หรืออาจทำให้เกิดปัญหาเรื่องความชอบธรรมในการบังคับใช้กฎหมาย ดังเช่นในคดี Cox v. Riley

ในเรื่องการพยายามแก้ปัญหาอาชญากรรมทางคอมพิวเตอร์นั้น การดำเนินการอย่างจริงจังเริ่มขึ้นตั้งแต่เดือนเมษายน ค.ศ. 1998 เป็นต้นมา เมื่อคณะกรรมการสหภาพยุโรป (The Commission of the European Communities) ได้เสนอผลการศึกษาเรื่องอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ที่เรียกกันว่า “COMCRIME” study ต่อ the Council of Europe

ในเดือน ตุลาคม ค.ศ. 1999 The Tampere Summit of the European Council ได้ สรุปผลการประชุมว่าอาชญากรรมทางคอมพิวเตอร์ จำเป็นที่จะต้องได้รับการแก้ไขโดยการพยายามทำให้มีฐานความผิดและสภาพบังคับทางกฎหมายที่เป็นสากล (common definition and sanctions)

ในเดือนมีนาคม ค.ศ. 2000 ในการประชุมที่เมืองลิสบอน ประเทศโปรตุเกส The European Council ได้กล่าวเน้นถึงความสำคัญของการเปลี่ยนแปลงให้ระบบเศรษฐกิจมีลักษณะที่สามารถแข่งขันกับผู้อื่นได้อย่างมีประสิทธิภาพ มีลักษณะเป็นพลวัตร (dynamic) และเป็นระบบเศรษฐกิจที่ตั้งอยู่บนพื้นฐานความรู้ (Knowledge based economy) และได้ชักชวนให้ The Council of Europe และ Commission of European จัดทำแผนดำเนินการ “e Europe” เพื่อให้สามารถใช้ประโยชน์ต่างๆจากข้อดีของสับคมสารสนเทศให้ได้มากที่สุด

แผนดำเนินการนี้จัดทำโดยThe Comission of European และThe Council of Europe ซึ่ง The Feira Summit of The Europe Council ยอมรับแผนดังกล่าวเมื่อเดือน มิถุนายน ค.ศ. 2000 โดยแผนดำเนินการนี้นอกจากกล่าวถึงเรื่องเศรษฐกิจแล้ว ก็ยังครอบคลุมถึงเรื่องการเพิ่มความปลอดภัยให้แก่เครือข่ายคอมพิวเตอร์ และการต่อต้านอาชญากรรมทางคอมพิวเตอร์โดยมีเป้าหมายขของการดำเนินงานให้เสร็จสิ้นก่อนสิ้นปี ค.ศ. 2002 ด้วย

อนุสัญญาฉบับนี้เปิดให้มีการลงนามเมื่อเดือนพฤศจิกายน ค.ศ. 2001 ที่เมืองบูดาเปส (Budapest) ประเทศฮังการี ขณะนี้ประเทศต่างๆที่เป็นสมาชิกของกลุ่มประเทศยุโรปได้ลงนามไปแล้วเป็นจำนวน 34 ประเทศ ส่วนประเทศที่มิได้เป็นสมาชิกของกลุ่มประเทศยุโรป ได้แก่ ประเทศสหรัฐอเมริกา แคนาดา ญี่ปุ่น และแอฟริกาใต้ ก็ได้ลงนามในอนุสัญญาฉบับนี้ด้วยแล้ว อนุสัญญาฉบับนี้ จะมีผลบังคับใช้ต่อเมื่อมีการให้สัตยาบันในอนุสัญญา 5 ประเทศ โดยต้องเป็นสมาชิกของกลุ่มประเทศยุโรปที่ให้สัตยาบันอย่างน้อย 3 ประเทศ ขณะนี้มีการให้สัตยาบันในอนุสัญญาแล้ว 2 ประเทศคือ ประเทศอัลบาเนีย และประเทศโครเอเชีย

ในเรื่องของความจำเป็นที่จะต้องมีอนุสัญญาฉบับนี้อาจพิจารณาได้จากส่วนอารัมภบท (Preamble) ของอนุสัญญานี้ซึ่งกล่าวโดยสรุปได้ว่า ในขณะนี้มีความจำเป็นอย่างยิ่งที่จะต้องมีนโยบายทางอาญาที่มุ่งคุ้มครองสังคมให้รอดพ้นจากปัญหาเรื่องอาชญากรรมทางคอมพิวเตอร์ โดยการใช้กฎหมายที่เหมาะสม และการสนับสนุนเรื่องความร่วมมือระหว่างประเทศ โดยจะต้องมีการยับยั้งการกระทำที่มุ่งกระทำต่อความลับ ความครบถ้วน และความสามารถในการใช้ประโยชน์ได้ของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ รวมทั้งการกำหนดให้การใช้ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ รวมทั้งการกำหนดให้การใช้ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ โดยมิชอบเป็นความผิดอาญาตามที่อนุสัญญากำหนดไว้

3) ประเทศสวีเดน

1. การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

สวีเดนเป็นประเทศหนึ่งที่มีบทบาทในฐานะตลาดการให้บริการด้านข้อมูลอิเลกโทรนิกส์ โดยบริการส่วนใหญ่นั้นจะให้แก่ภาครัฐเป็นหลัก ส่วนเอกชนมุ่งที่การค้า อย่างไรก็ตามสวีเดนนั้นได้มีการกำหนดให้ประเทศเป็น Information Society Policies และความร่วมมือ

ระหว่างหน่วยงานในการแลกเปลี่ยนข้อมูลส่วนใหญ่ระหว่างกระทรวงยุติธรรมจะเป็นการแลกเปลี่ยนกับกระทรวงการคลังและStateskontoret รวมไปถึงการตั้ง IT Commission ขึ้นมาดูแล ในส่วนของการแลกเปลี่ยนข้อมูลหรือการเชื่อมโยงข้อมูล มีการตั้งศูนย์ชื่อ Rixlex [54] ดูแลในด้านการใช้เทคโนโลยีสารสนเทศ ในขณะที่ในกระทรวงยุติธรรมเองก็มีการเชื่อมโยงและมีการแลกเปลี่ยนข้อมูลในการดำเนินการอยู่แล้ว

2.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

กฎหมายหลักที่เกี่ยวข้องกับการเชื่อมโยงการแลกเปลี่ยนและการบูรณาการของสวีเดน คือ the Electronic Communications Act 2000 ซึ่งเป็นกฎหมายที่เอื้อต่อการแลดเปลี่ยนข้อมูลทั่วไปแต่ก็สามารถใช้เป็นกกหมายหลักสำหรับการดำเนินการได้ดี

3. กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประเทศสวีเดนนับเป็นประเทศแรกที่มีการใช้พระราชบัญญัติการคุ้มครองข้อมูลในปี ค.ศ. 1974 และฉบับแก้ไข ค.ศ. 1992 มีเนื้อหาระบุว่า “ข้อมูลส่วนบุคคล” หมายถึง ข่าวสารซึ่งเกี่ยวกับเฉพาะบุคคล และ“แฟ้มส่วนบุคคล” หมายถึง แฟ้มชนิดใด รายการหรือบันทึกอื่นๆ ที่จัดเก็บรักษา โดยวิธีการเก็บข้อมูลอัตโนมัติ และบรรจุข้อมูลส่วนบุคคลซึ่งอ้างอิงเกี่ยวเฉพาะบุคคลแต่ละบุคคล การอนุญาตจัดทำขึ้นและจัดเก็บรักษาแฟ้มส่วนบุคคล มีหลักเกณฑ์ว่า[55]

1)แฟ้มส่วนบุคคลจะต้องจัดทำขึ้นและเก็บรักษาโดยบุคคลผู้ซึ่งคณะกรรมการตรวจสอบข้อมูลเห็นชอบ และได้รับใบอนุญาตจากคณะกรรมการให้ทำการดังกล่าว การอนุญาตของคณะกรรมการจะต้องเป็นไปเพื่อจัดทำขึ้นและจัดเก็บรักษาแฟ้มส่วนบุคคล ซึ่งบรรจุ

(1) ข่าวสารตามที่บัญญัติ

(2) ข่าวสารเกี่ยวกับบุคคลผู้ซึ่งเกี่ยวข้องในการเป็นสมาชิก ในการทำงาน ความสัมพันธ์กับลูกค้าหรือความสัมพันธ์อื่นๆ

(3) ข้อมูลส่วนบุคคลที่จัดหามาจากแฟ้มส่วนบุคคลอื่นๆ

---

54 Ministry of Justice, Sweden

55 ปทีป เมธาคุณวุฒิ **เรื่องเดิม** หน้า 22-28

2) การอนุญาตของคณะกรรมการตรวจสอบข้อมูลไม่จำเป็นต้องมีสำหรับแฟ้มส่วนบุคคลที่จัดทำขึ้นโดยข้อตกลงของรัฐบาล ความเห็นของคณะกรรมการตรวจสอบข้อมูลนำมาซึ่งการพิจารณาแฟ้ม ซึ่งบรรจุข่าวสารตามที่บัญญัติไว้ดังนี้

(1) ชมรม หรือกลุ่ม หรือสมาคมอาจจัดทำและเก็บแฟ้มข้อมูลซึ่งบรรจุข่าวสารเกี่ยวกับทัศนคติทางการเมืองของสมาชิกของบริษัท ความเชื่อทางศาสนา หือความเชื่อถือในสิ่งอื่นๆ ตามองค์ประกอบขั้นพื้นฐานสำหรับการเป็นสมาชิก

(2) สิทธิหรืออำนาจในส่วนที่เกี่ยวกับสุขภาพและการบริการทางการแพทย์ อาจจะเก็บโดยมีวัตถุประสงค์เพื่อการรักษาพยาบาล โดยจัดทำขึ้นและเก็บแฟ้มส่วนบุคคลที่บรรจุข่าวสารเกี่ยวกับความเจ็บป่วยของบุคคล

(3) สิทธิหรืออำนาจในการบริการทางสังคม อาจจะจัดทำขึ้นและเก็บรักษาแฟ้มส่วนบุคคลซึ่งบรรจุข่าวสารของบุคคลที่ได้รับความช่วยเหลือทางด้านการเงินหรือให้ความดูแลจากบริการทางด้านสังคม

(4) แพทย์หรือทันตแพทย์อาจจะจัดทำหรือจัดเก็บรักษาแฟ้มส่วนบุคคล ซึ่งมีข่าวสารเกี่ยวกับความเจ็บป่วยของบุคคล ซึ่งเกี่ยวข้องกับวิชาชีพ

(5) นายจ้างอาจจะจัดทำหรือเก็บรักษาแฟ้มส่วนบุคคลซึ่งบรรจุข้อมูลลูกจ้างเกี่ยวกับความเจ็บป่วยเพื่ออ้างถึงการลาหยุดงาน ถ้าโดยปกตินายจ้างจะต้องจ่ายค่าจ้างอยู่แล้ว หรือเพื่อให้นายจ้างได้ตัดสินใจตามที่ได้บัญญัติไว้ในพระราชบัญญัติประกันชีวิตแห่งชาติ

3) คณะกรรมการตรวจสอบข้อมูลจะรับรองการอนุญาต จัดทำขึ้นและเก็บรักษาแฟ้มส่วนบุคคล ถ้าไม่มีเหตุอันจะสันนิษฐานได้ว่า มีการปฏิบัติอย่างต่อเนื่องของข้อกำหนดดังที่ว่าไว้นี้ล่วงละเมิดสิทธิส่วนบุคคลของทะเบียนบุคคล

4) ในกรณีที่การล่วงละเมิดเกินการอาจเกิดจากเจตนาเฉพาะ จะต้องได้รับการพิจารณาตามที่เป็นจริงเกี่ยวกับข้อมูลส่วนบุคคลที่มีการบันทึกในแฟ้ม ในกรณีที่จะพิจารณาว่ามีการล่วงละเมิดหรือไม่ จะต้องให้ความสนใจต่อลักษณะและปริมาณของข้อมูลส่วนบุคคลที่เก็บไว้ในแฟ้มข้อมูลว่าเก็บรวบรวมอย่างไร เก็บรวบรวมจากใครและแฟ้มข้อมูลมีวัตถุประสงค์ในการเก็บอย่างไร ใครเป็นผู้จดทะเบียน ในการจัดเก็บจะต้องระบุอย่างชัดเจนว่าไม่มีการจัดเก็บข้อมูลของบุคคลนอกเหนือจากที่จดทะเบียนไว้ตามวัตถุประสงค์ที่ขอไว้

5) การอนุญาตจัดทำหรือเก็บรักษาแฟ้มส่วนบุคคลที่ไม่ใช่สมาชิก ลูกจ้างหรือลูกค้า ผู้ที่มีหน้าที่รับผิดชอบในแฟ้มหรือบุคคลที่มีความสัมพันธ์กับผู้ที่มีความรับผิดชอบเก็บรวบรวมข้อมูล อาจจะได้รับการอนุญาตในกรณีที่มีเหตุการณ์เฉพาะสำหรับที่จะทำดังนั้น

6) การขออนุญาตจัดทำขึ้นและเก็บรักษาแฟ้มส่วนบุคคลนั้น บุคคลหนึ่งบุคคลใดซึ่งถูกสงสัยหรือถูกลงโทษในความผิดทางอาญา หรือได้รับคำพิพากษาหรือถูกลงโทษ สำหรับความผิดทางอาญาหรืออยู่ในอำนาจการบังคับภายใต้กฎหมายอื่นอาจจะทำได้นอกจากมีเหตุผลที่ชัดเจนที่จะได้รับการลงโทษ

7) การอนุญาตจัดทำขึ้นและเก็บรักษาแฟ้มส่วนบุคคลในประการอื่นซึ่งได้บรรจุข่าวสารเกี่ยวกับความเจ็บป่วยของบุคคลใดบุคคลหนึ่ง บันทึกเกี่ยวกับสุขภาพ หรือชีวิตความสัมพันธ์ทางเพศ หรือข่าวสารซึ่งบุคคลใดบุคคลหนึ่งได้รับความช่วยเหลือทางการเงิน หรือได้รับการดูแลภายใต้บริการทางสังคมหรือได้รับการดูแลภายใต้พระราชบัญญัติคนเข้าเมืองอาจจะทำได้ถ้ามีเหตุผลที่ชัดเจนเพื่อที่จะเก็บรวบรวมข้อมูลเหล่านี้

8) การอนุญาตจัดทำขึ้นและเก็บรักษาแฟ้มส่วนบุคคลซึ่งบรรจุข่าวสารเกี่ยวกับเชื้อชาติของบุคคล ทัศนคติทางการเมือง ความเชื่อทางศาสนา การนับถือศาสนาหรือความเชื่อในด้านอื่นๆ อาจจะได้รับการพิจารณาถ้ามีเหตุการณ์พิเศษ สำหรับที่จะทำดังนั้น

9) ในการอนุญาตเพื่อจัดทำขึ้นและเก็บรักษาแฟ้มส่วนบุคคล คณะกรรมการตรวจสอบข้อมูล จะออกข้อบังคับเกี่ยวกับวัตถุประสงค์ของการจัดเก็บ การอนุญาตอาจจะถูกจำกัดระยะเวลาที่แน่นอน ถ้ามีเหตุการณ์พิเศษสำหรับที่จะทำดังนั้น

(1) จัดข้อมูลให้เป็นหมวดหมู่สำหรับแฟ้มส่วนบุคคล

(2) ข้อมูลส่วนบุคคลซึ่งอาจจะถูกบันทึกในแฟ้มส่วนบุคคล

(3) วิธีพิจารณากระบวนการประมวลผลข้อมูลอัตโนมัติ

(4) อุปกรณ์ทางด้านเทคนิคในการจัดเก็บ

(5) การปฏิบัติการเกี่ยวกับข้อมูลส่วนบุคคลในแฟ้มส่วนบุคคลนั้นซึ่งอาจจะใช้กระบวนการประมวลผลข้อมูลอัตโนมัติ

(6) การระบุเกี่ยวกับบุคคลที่เกี่ยวข้อง

(7) ข้อมูลส่วนบุคคลซึ่งอาจจะถูกละเมิด

(8) การเผยแพร่และการใช้ข้อมูลส่วนบุคคลวิธีอื่นๆ

(9) การรักษาและการแยกประเภทข้อมูลส่วนบุคคล

(10) การควบคุมและรักษาความปลอดภัย

(11) การตรวจ แก้ไข และกระทำการอื่นใดในกรณีที่ข่าวสารไม่ถูกต้อง หรือทำให้เกิดการเข้าใจผิด

10) ในกรณีที่กฎข้อบังคับมีข้อกำหนดอาจจะนำมาซึ่งการตัดสินใจพิเศษเกี่ยวกับแฟ้มส่วนบุคคล ซึ่งบรรจุข้อมูลส่วนบุคคลประกอบคำพิพากษาหรือประเมินค่าของทะเบียนบุคคล

11) การพิจารณาข้อบังคับสำหรับการเผยแพร่ข้อมูลส่วนบุคคลจะแยกออกจากอำนาจหน้าที่ของสาธารณะภายใต้พระราชบัญญัติเสรีภาพของสื่อมวลชน(Freedom of the Press Act)

หน้าที่และความรับผิดชอบของผู้ที่จัดเก็บรักษาแฟ้มส่วนบุคคล

1) แฟ้มส่วนบุคคลและถูกจัดทำให้มีขึ้นและถูกเก็บรักษาไว้ในทางใดทางหนึ่งที่จะไม่มีการล่วงละเมิดสิทธิส่วนบุคคลของทะเบียนบุคคล โดยมีประเด็นดังต่อไปนี้

(1) แฟ้มส่วนบุคคลถูกเก็บโดยมีวัตถุประสงค์เฉพาะเจาะจง

(2) ไม่มีสิ่งอื่นถูกบันทึกมากกว่าที่ระบุไว้ตามวัตถุประสงค์ในการจัดเก็บแฟ้ม

(3) สิ่งที่เก็บไว้ในแฟ้มส่วนบุคคลต้องไม่ถูกขาย โดยอำนาจสาธารณะโดยปราศจากความยินยอมของผู้ที่อยู่ในทะเบียนบุคคล เว้นแต่จะบัญญัติไว้โดยออกกฎหมายหรือมติพิเศษของรัฐบาล

(4) สิ่งที่จัดเก็บในแฟ้มส่วนบุคคลไม่ถูกจัดเป็นหมวดหมู่ เปิดเผยหรือถูกใช้ในทางอื่นๆ เกินกว่าข้อตกลงตามวัตถุประสงค์ที่ได้จดทะเบียนไว้ หรือบทบัญญัติของกฎหมายหรือที่ได้กำหนดไว้โดยพระราชบัญญัติหรือได้รับความยินยอมโดยบุคคลที่อยู่ในทะเบียนบุคคล

(5) สิ่งที่จัดเก็บในแฟ้มส่วนบุคคลได้รับการป้องกันจากการทำลายโดยไม่มีเจตนา หรือไม่ถูกกฎหมาย หรือจากการดัดแปลง แก้ไขหรือเผยแพร่โดยไม่ถูกต้องตามกฎหมาย

2) บุคคลผู้มีหน้าที่จัดเก็บรักษาแฟ้มส่วนบุคคลจะต้องจัดทำรายการในแฟ้มส่วนบุคคลซึ่งตนเองมีความรับผิดชอบอยู่ให้ทันสมัยโดยรายการจะบรรจุสิ่งต่างๆ เหล่านี้

(1) ชื่อของแฟ้ม

(2) วัตถุประสงค์ของแฟ้ม

(3) หลักการซึ่งกระบวนการประมวลข้อมูลอัตโนมัติสามารถทำงานให้สำเร็จได้มากที่สุด

(4) จำนวนของใบอนุญาตของผู้มีหน้าที่รับผิดชอบจัดเก็บรักาจากคณะกรรมการตรวจสอบข้อมูล

(5) ขอบเขตของข้อมูลส่วนบุคคลถูกนำไปเผยแพร่โดยคณะกรรมการประมวลผลข้อมูลอัตโนมัติในต่างประเทศ

(6) ขอบเขตซึ่งสำนักทะเบียนแห่งชาติได้จดทะเบียนไว้

3) หลักการของอำนาจสาธารณะให้สิทธิบุคคล ดังนั้นรายการจะรวมถึงบันทึกการยินยอมของผู้ที่อยู่ในทะเบียนบุคคล หรือมติพิเศษของรัฐบาลที่ให้อำนาจ

4) รายการจะถูกเก็บรักษาโดยที่สามารถเรียกดูได้โดยคณะกรรมกรที่มีชื่อเรียกว่า คณะกรรมกาตรวจสอบข้อมูล (Data Inspection Board) เมื่อผู้มีหน้าที่รับผิดชอบเก็บรักษาแฟ้มส่วนบุคคลส่งเอกสาร ซึ่งบรรจุข้อมูลส่วนบุคคลจากแฟ้มส่วนบุคคลถึงผู้อยู่ในทะเบียนบุคคล จะต้องแจ้งให้ทราบระดับของผู้มีหน้าที่รับผิดชอบจัดเก็บรักษาซึ่งออกโดยคณะกรรมการตรวจสอบข้อมูล

5) ข้อบัญญัติของมาตรานี้ ไม่นำมาใช้กับแฟ้มส่วนบุคคล ซึ่งถูกเก็บรักษาโดยแต่ละบุคคลสำหรับใช้ส่วนบุคคล หรือได้รับอนุญาตโดยอำนาจสาธารณะเพื่อการคุ้มครอง

6) ในกรณีที่มีเหตุอันควรสงสัยว่าข่าวสารส่วนบุคคลซึ่งเป็นส่วนหนึ่งของแฟ้มส่วนบุคคลไม่ถูกต้องหรือเป็นไปในทางที่ผิด ผู้มีหน้าที่เก็บรักษาแฟ้มจะจัดให้มีการไต่สวนทันที ข่าวสารที่ไม่ถูกต้อง หรือเป็นไปในทางที่ผิดจะต้องถูกแก้ไขดัดแปลง หรือลบออก นอกจากไม่มีเหตุที่จะสันนิษฐานได้ว่า มีการละเมิดเกินการต่อสิทธิส่วนบุคคลของผู้ที่อยู่ในทะเบียนบุคคล

7) ข่าวสารที่มีการจดทะเบียนซึ่งได้รับการแก้ไข เปลี่ยนแปลงหรือลบออกโดยบุคคลที่สาม ผู้ที่มีหน้าที่ดูแลจัดเก็บรักษาแฟ้มจะต้องแจ้งการแก้ไขดัดแปลงหรือลบออกของบุคคลที่สาม ถ้าบุคคลที่ถูกจดทะเบียนได้ร้องขอหรือถ้ามีความเสี่ยงสำหรับการล่วงละเมิดสิทธิส่วบุคคลมากเกินไป

8) บุคคลผู้ที่อยู่ในทะเบียนซึ่งได้รายงานข้อสงสัยว่า ข่าวสารส่วนบุคคลไม่ถูกต้องหรือเป็นไปในทางที่ผิด ต้องแจ้งการกระทำที่เป็นผลของรายงานต่อผู้ที่มีหน้าที่รับผิดชอบจัดเก็บแฟ้มส่วนบุคล ซึ่งจะแต่งตั้งบุคคลหนึ่งหรือมากกว่านั้นเพื่อช่วยเหลือบุคคลผู้ที่อยู่ในทะเบียนบุคคลนั้น เมื่อมีข้อสงสัยเกี่ยวข้องกับข่าวสารส่วนบุคคลที่ไม่ถูกต้องหรือเป็นไปในทางที่ผิด และรายงานการกระทำที่เกิดขึ้นดังกล่าว ชื่อของบุคคลที่ถูกแต่งตั้งจะเปิดเผยต่อสาธารณะ

9) ถ้าแฟ้มส่วนบุคคลบรรจุข้อมูลส่วนบุคคล ซึ่งเมื่อพิจารณาตามวัตถุประสงค์ของแฟ้มได้รับการตัดสินว่าไม่สมบูรณ์ หรือถ้าแฟ้มส่วนบุคคลซึ่งประกอบด้วยรายละเอียดของบุคคลละเลยบุคคลใดบุคคลหนึ่ง ซึ่งในมุมมองของวัตถุประสงค์ของแฟ้มมีการคาดหวังเพื่อให้บันทึกไว้ ผู้เก็บรักษาแฟ้มจะต้องรับผิดชอบให้เพิ่มเติม ถ้ามีการละเลยอาจจะสันนิษฐานไว้ก่อนถึงการนำไปสู่การล่วงล้ำความเป็นส่วนตัวของบุคคลเกินการหรือเสียหรือสูญหายของสิทธิ

10) ตามการร้องขอของผู้ที่อยู่ในทะเบียน ผู้รับผิดชอบเก็บรักษาแฟ้มส่วนบุคคลจะต้องแจ้งให้ผู้ที่อยู่ในทะเบียนทราบเร็วที่สุดเกี่ยวกับข้อมูลของตนเองที่มีการจัดเก็บในแฟ้มข้อมูล การร้องขอจะทำเป็นลายลักษณ์อักษรโดยผู้เป็นเจ้าของ และการแจ้งจะทำภายใน 12 เดือน ในช่วงนี้จะไม่มีการแจ้งอีกจนกระทั่งผ่านไป 12 เดือนแล้ว ในกรณีที่เจ้าหน้าที่รัฐบาลได้รับสิทธิเพื่อขายรายละเอียดจากทะเบียน การแจ้งจะรวมรายการที่บ่งชี้ว่าการขายนี้ได้รับการยินยอมจากผู้ที่อยู่ในทะเบียนบุคคลหรือรายการที่แจ้งว่าได้รับการอนุญาตตามกฎหมายหรือรัฐบาลลงมติให้ขาย

11) การประกาศจะไม่มีการเก็บค่าธรรมเนียมในการร้องขอจากผู้ที่อยู่ในทะเบียนบุคคล อย่างไรก็ตาม คณะกรรมการตรวตสอบอาจจะอนุญาตให้จัดเก็บค่าธรรมเนียมในบางชนิดของข้อมูลส่วนบุคคลหรือในการประกาศ ถ้ามีเหตุผลพิเศษที่จะทำดังนั้น

12) ข้อมูลส่วนบุคคลในแฟ้มส่วนบุคคลจะไม่ถูกเปิดเผย นอกจากถ้ามีเหตุพอสันนิษฐานได้ว่า ข้อมูลจะถูกใช้เพื่อกระบวนการประมวลผลข้อมูลอัตโนมัติตรงข้ามกับพระราชบัญญัตินี้ หรือถ้ามีเหตุที่สันนิษฐานได้ว่าข้อมูลจะถูกใช้สำหรับกระบวนการประมวลผลข้อมูลอัตโนมัติในต่างประเทศ ข้อมูลอาจจะถูกเปิดเผยภายหลังจากได้รับอนุญาตจากคณะกรรมการตรวจสอบข้อมูลแล้วเท่านั้น การอนุญาตแต่ละครั้งอาจทำได้แต่ถ้ามีเหตุอันสันนิษฐานได้ว่าการเปิดเผยข้อมูลจะไม่นำไปสู่การล่วงล้ำสิทธิความเป็นส่วนตัวของบุคคลจนเกินไป การอนุญาตไม่ต้องกำหนดไว้

13) ข้อมูลส่วนบุคคลที่อ้างถึงบุคคลซึ่งเกี่ยวข้องกับข้อมูล จะถูกเคลื่อนย้ายจากแฟ้มส่วนบุคคล เมื่อข้อมูลนั้นไม่เป็นที่ต้องการเป็นเวลายาวนาน เพื่อเป็นไปตามวัตถุประสงค์ของแฟ้ม นอกจากว่าข้อมูลจะได้ถูกรักษาไว้โดยเหตุผลของบทบัญญัติแห่งกฎหมาย หรือสถานภาพอื่นหรือโดยการตัดสินใจของเจ้าหน้าที่รัฐบาล และในทำนองเดียวกันเมื่อผู้รับผิดชอบเก็บรักษาแฟ้มส่วนบุคคลยุติการเก็บรักษา

ถ้าผู้รับผิดชอบเก็บรักษาแฟ้มส่วนบุคคลเลิกเก็บรักษาแฟ้มส่วนบุคคลซึ่งคณะกรรมกาตรวจสอบข้อมูลได้อนุญาตไว้จะต้องแจ้งคณะกรรมการตรวจสอบข้อมูล ในการการตรวจตราดูแลนั้นมีหลักเกณฑ์ ดังนี้

1) คณะกรรมการตรวจสอบข้อมูลจะตรวจตราว่า กระบวนการประมวลผลข้อมูลอัตโนมัติไม่ล่วงล้ำเกินการต่อความเป็นส่วนตัวของบุคคล

2) การดูแลตรวจตราที่ปฏิบัติจะต้องไม่มีเหตุให้ต้องเสียค่าใช้จ่ายหรือยุ่งยาก ไม่สะดวกมากเกินกว่าความจำเป็น

3) ตามวัตถุประสงค์ของการตรวจราดูแล คณะกรรมการตรวจสอบข้อมูลมีสิทธิในการยอมรับข้อสัญญาใดๆ ซึ่งกระบวนการประมวลผลข้อมูลอัตโนมัติทำบรรลุผลสำเร็จ คณะกรรมการมีสิทธิเข้าถึงเอกสารเกี่ยวข้องกับกระบวนการข้อมูลอัตโนมัติ

4) ผู้รับผิดชอบเก็บรักษาแฟ้มจะส่งมอบข่าวสารที่เกี่ยวกับกระบวนการประมวลผลข้อมูลอัตโนมัติแก่คณะกรรมการตรวจสอบข้อมูล

5) ถ้าการคุ้มครองต่างการล่วงล้ำหรือล่วงละเมิดต่อความเป็นส่วนตัวของบุคคลไม่สามารถทำสำเร็จวิธีการใดๆ คณะกรรมการตรวจสอบข้อมูลอาจห้ามการเก็บรักษาแฟ้ม หรือยกเลิกการรับรองการอนุญาต

บทลงโทษและความเสียหาย

1) บุคคลใดโดยจงใจหรือประมาทเลินเล่อ

(1) จัดทำหรือเก็บรักษาแฟ้มส่วนบุคคล โดยปราศจากใบอนุญาตหรือขออนุญาตภายใต้กฎหมายนี้ตามที่ได้กำหนด

(2) ผิดข้อตกลงหรือข้อห้ามที่ออกไว้

(3) เปิดเผยข้อมูลส่วนบุคคลในลักษณะฝ่าฝืน

(4) ส่งมอบข่าวสารไม่ถูกต้องในการปฏิบัติตามหน้าที่ จะถูกปรับหรือระวางโทษจำคุกไม่เกิน 1 ปี

2) บุคคลที่ทำผิดกฎหมายโดยดำเนินการบันทึกข้อมูลส่วนบุคคล เพื่อใช้ในกระบวนการประมวลผลข้อมูลอัตโนมัติ หรือผู้ซึ่งดัดแปลงหรือลบ หรือสดแทรกบันทึกในแฟ้ม

ส่วนบุคคลโดยผิดกฎหมาย จะถูกระวางโทษสำหรับการล่วงล้ำข้อมูล โดยปรับหรือจำคุกไม่เกินกว่า 2 ปี นอกจากการกระทำผิดถูกลงโทษตามประมวลกฎหมายอาญา หรือภายใต้พระราชบัญญัติการคุ้มครองความลับทางธุรกิจ (Protection of Business Secrets Act 1990) สำหรับวัตถุประสงค์เหล่านี้ข้อความ รายการ พาดพิงถึงข่าวสารในกระบวนการของการสื่อสารโดยอิเล็กทรอนิกส์ด้วย หรือในความหมายสำหรับการใช้กระบวนการประมวลผลข้อมูลอัตโนมัติ

3) บุคคลใดผู้ซึ่งพยายามหรือตระเตรียมการล่วงล้ำทางอาญากับข้อมูลจะต้องถูกระวางโทษตามบทที่ 23 ของประมวลกฎหมายอาญา แต่อย่างไรก็ดีการกระทำความผิด ถ้าทำไม่สำเร็จจะถูกพิจารณาโทษสถานเบาเท่านั้น ผู้กระทำความผิดไม่ถูกระวางโทษดังที่ได้กล่าวไว้

4) ถ้าผู้ที่อยู่ในทะเบียนบุคคลอาจจะได้รับความเสียหายโดยเหตุที่แฟ้มส่วนบุคคลซึ่งบรรจุข่าวสารที่ผิด โดยความรับผิดชอบของผู้เก็บรักษาจะต้องหาเงินค่าปรับไว้สำหรับความเสียหายดังกล่าวนี้

5) การตัดสินโดยคณะกรรมการตรวจสอบข้อมูลตามพระราชบัญญัตินี้อาจได้รับการโต้แย้งโดยการอุทธรณ์ต่อรัฐบาล การโต้แย้งการตัดสินกระทำเพื่อป้องกันรักษาอำนาจของสาธารณะ

เงื่อนไขหลาย ๆ เงื่อนไขของพระราชบัญญัติความลับอนุญาตให้รัฐบาลสามารถเปิดเผยเอกสารทางราชการบางอย่างได้เป็นกรณีพิเศษ

ผลประโยชน์ของรัฐ (Interest) ที่ได้รับการปกป้องมิให้มีการเปิดเผยข้อมูลข่าวสารได้แก่

- ความมั่นคงหรือความสัมพันธ์กับต่างประเทศหรือองค์กรระหว่างประเทศ
- นโยบายการคลังของส่วนกลาง นโยบายการเงินหรือนโยบายการแลกเปลี่ยนเงินตราต่างประเทศ
- การตรวจสอบ การควบคุมหรือหน้าที่สอดส่องดูแลอย่างอื่น
- ผลประโยชน์ทางด้านการป้องกันอาชญากรรมและการพิพากษา
- ผลประโยชน์ทางเศรษฐกิจสาธารณะ
- การป้องกันศีลธรรมส่วนตัวและความลับทางเศรษฐกิจ
- การสงวนรักษาสัตว์และพันธุ์พืช

เอกสารใด ๆ ที่เกี่ยวกับผลประโยชน์ข้างต้นนั้นจะไม่สามารถเปิดเผยได้ และในกรณีนี้จะต้องมีข้อความระบุเงื่อนไขที่ไม่อนุญาตให้เปิดเผยไว้ในเอกสารดังกล่าวด้วย (มาตรา 16)

4. กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

สวีเดนได้มีการนำเอาDirective Act of 6 November 1997 (Act 1997:79) ซึ่งประกาศใช้เมื่อวันที่ 1 มกราคม 1998 มาใช้โดยมีการแก้ไขใน มาตรา 49ของกฎหมาย Swedish Copyright Act 1997[56] ทั้งนี้เพื่อให้มีการคุ้มครองฐานข้อมูลต่างๆ รวมทั้งฐานข้อมูลที่เกี่ยวข้องกับงานยุติธรรมที่กระทรวงยุติธรรมได้ดำเนินการ ยังผลให้ฐานข้อมูลใดๆที่ได้มีการจัดทำขึ้นก็สามารถที่จะได้รับการคุ้มครอง

5. กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ในส่วนของกฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิดของสวีเดนนั้น อาจกล่าวได้ว่า เป็นการคัดลอกแนวทางมาจากกฎหมายของอังกฤษ คือ The Computer Misuse Act 1990 แต่ก็ได้มีการแก้ไขบทบัญญัติบางประการที่ทำให้ตำรวจสามารถที่จะจับกุมผู้ที่กระทำผิดได้สะดวกขึ้น ซึ่งก็ส่งผลทำให้อัตราการใช้คอมพิวเตอร์ของชาวสวีเดนลดลง เพราะเกิดความไม่แน่ใจว่าการใช้ของตนในการสืบค้นข้อมูลในเชิงลึกจะเข้าข่ายหรือไม่

4) ประเทศแคนาดา

1. การแลกเปลี่ยน เชื่อมโยง และบูรณาการข้อมูลในกระบวนการยุติธรรมของแคนาดา

การแลกเปลี่ยน เชื่อมโยง และบูรณาการข้อมูลในกระบวนการยุติธรรมของแคนาดา มีการดำเนินการที่เป็นไปด้วยความยุ่งยากพอสมควร เนื่องจากองค์กรใน

---

56 Swedish Copyright Act 1997 **Article 49.** A catalogue, a table or another similar production in which a large number of information items have been compiled may not be reproduced without the authorization of the producer until ten years have elapsed from the year in which the production was published.The provisions of Articles 6 - 9, 11, second paragraph, 12, first paragraph, 13, 16 - 18, 26 - 26 b and 26 e shall apply also to productions referred to in this Article. If a production of this kind, or a part thereof, is subject to copyright, also copyright protection may be claimed.

กระบวนการยุติธรรมของแคนาดามีลักษณะเฉพาะที่ดำเนินการเป็นเอกเทศและมีจำนวนหน่วยงานในกระบวนการยุติธรรมหลายหน่วยงาน มีความซับซ้อน และมีการให้บริการแตกต่างกันออกไป

รัฐบาลแคนาดาได้ตั้งคณะทำงานขึ้นมาดำเนินการเชื่อมโยงและบูรณาการข้อมูลในกระบวนการยุติธรรม และได้วางกรอบการดำเนินการไว้ 4 ส่วนคือ [57]

1. เทคโนโลยี (Technology) เทคโนโลยีเป็นองค์ประกอบที่มีความสำคัญอย่างยิ่งในการดำเนินการระบบเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม เนื่องจากหากมีความพร้อมในระบบเทคโนโลยีแล้วการเชื่อมโยงก็จะสามารถกระทำได้อย่างรวดเร็ว มีการตั้ง Canada Public Safety Information Net ให้เข้าร่วมเป็นหุ้นส่วนในฐานะองค์กรหนึ่ง ที่มีศักยภาพในการช่วยสร้างเสริมด้านการสร้างระบบข้อมูลยังหน่วยงานที่เข้าร่วม ได้แก่ ฝ่ายตำรวจคือ The Royal Canadian Mounted Police ราชทัณฑ์บริการ (Correctional Service Canada) หน่วยตรวจคนเข้าเมือง (Citizenship and Immigration Canada) ศุลกากรและสรรพากร (Canada Custom and Revenue Agency) คณะกรรมการด้านคุมประพฤติที่ชื่อว่า The National Parole Board และกระทรวงยุติธรรมของแคนาดาเป็นผู้มีบทบาทสนับสนุนหลักในการก่อตั้งเครือข่ายนี้ การดำเนินการมีการจัดโครงสร้างพื้นฐานเพื่อให้เหมาะสมสำหรับการดำเนินการทั้งในปัจจุบันและในอนาคต

ศูนย์ข้อมูลของตำรวจแคนาดา (The Canadian Police Information Centre) หรือที่รู้จักกันในนาม CPIC เป็นหน่วยงานที่มีความทันสมัยที่จะสามารถช่วยสนับสนุนงานตำรวจได้ทั่วประเทศ การทำงานมีกระบวนการพัฒนาไปตามดัชนีชี้วัดระดับชาติ ด้านการพัฒนาอิเลคโทรนิคส์ในกระบวนการยุติธรรม โดยเฉพาะตำรวจที่ราบสูง(The Royal Canadian Mounted Police) กับระบบการรายงานผลเหตุการณ์ของตำรวจ หรือThe Police Reporting and Occurrence System (PROS) ในขณะที่หน่วยงานด้านคุมประพฤติและราชทัณฑ์ก็มีการจัดทำระบบฐานการบริหารผู้กระทำผิด (Offender Management System) รวมทั้งการสร้างระบบการปล่อยที่มีเงื่อนไข ซึ่งเป็นสิ่งจำเป็นที่จะเพิ่มความปลอดภัยให้ชุมชน รวมทั้งเพิ่มคุณภาพข้อมูล รวมทั้งให้ข้อมูลที่ครบถ้วน ถูกต้อง รวดเร็ว สำหรับการตัดสินในระบบกระบวนการยุติธรรม

---

57 Canada Public Safety Information Network

2. นโยบาย (Policy) แม้ว่าจะยอมรับกันว่า เทคโนโลยีจะเป็นสิ่งที่ช่วยในการบูรณาการ แลกเปลี่ยนและเชื่อมโยงข้อมูล แต่สิ่งที่มีความสำคัญที่จะส่งเสริมและสนับสนุนการดำเนินการก็คือ กฎหมาย นโยบาย และการปฏิบัติการจะเป็นสิ่งที่ช่วยเสริมการดำเนินการให้หน่วยงานที่บังคับใช้กฎหมายได้ดำเนินการไปอย่างมีประสิทธิภาพและในขณะเดียวกัน สิทธิส่วนบุคคล และสิทธิพื้นฐานของประชาชน ก็ได้รับการปกป้องคุ้มครองด้วยในเวลาเดียวกัน

ภายใต้การดำเนินการดังกล่าวมีการตั้งนโยบายในด้านมาตรฐาน (Standard) และในด้านข้อแนะนำ (guideline) ในการบริหารจัดการข้อมูล ซึ่งก็จะรวมทั้งมาตรฐานการบริหารจัดการ ข้อมูลที่จัดเก็บ (record management standard) หลักการวางแผนด้านข้อมูลส่วนบุคคล (Privacy design principles) และมาตรฐานด้านความปลอดภัยในการปกป้องคุ้มครองข้อมูลอิเลกโทรนิกส์ (security standard for the protection of electronic information) ซึ่งสิ่งที่พัฒนาขึ้นเหล่านี้จะกลายเป็นรูปแบบพื้นฐานสำหรับทุกหน่วยงานในเครือข่ายที่จะต้องมีโทรแลกเปลี่ยนข้อมูล หรือ เชื่อมโยงข้อมูลในกระบวนการยุติธรรม

ดัชนีกระบวนการยุติธรรมแห่งชาติ หรือ The National Criminal Justice Index (NcJi) เป็นเครื่องมือระดับชาติที่รัฐบาลแคนาดากำหนดให้เป็นเครื่องมือสำหรับการแลกปลี่ยนข้อมูลทางอิเลคโทรนิคส์ เพื่อจะทำให้กระแสข้อมูลทั้งเกี่ยวกับตัวผู้กระทำผิด และข้อมูลที่เกี่ยวข้องกับการประกอบอาชญากรรมได้กระจายไปยังหน่วยงานเครือข่ายได้อย่างถูกต้องและเหมาะสม เมื่อมีการสร้างและพัฒนาแล้ว ก็จะถูกนำไปถ่ายทอดเพื่อสร้างความเข้าใจในการเก็บรวบรวมข้อมูล การใช้ การรักษา และการเปิดเผย ฯลฯ แก่หน่วยงานเครือข่าย นอกจากนี้ยังมีการประเมินโครงการและมีการรายงานความก้าวหน้าเป็นระยะ รวมทั้ง การจัดทำรายงานประจำปี (The annual Integrated Justice Inforation Progress Reports) ทั้งนี้ในการแลกเปลี่ยนข้อมูลและการให้การส่งเสริมสรับสนุนความรู้แก่ผู้ปฏิบัติงานด้วย

มีการจัดทำธรรมนูญ หรือ Charter ร่วมกัน และหุ้นส่วนในเครือข่ายได้ร่วมกันลงนามโดยหน่วยงานในกระบวนการยุติธรรมของรัฐทั้ง 9 หน่วยงาน

3. มาตรฐานและเครื่องมือทั่วไป(Standards and Common tools) ในการสร้างมาตรฐานข้อมูล (The Data Standard) ได้มีการกำหนดให้องค์กรในกระบวนการยุติธรรม และสำนักงานสถิติแห่งชาติ เข้าร่วมกำหนดและพัฒนามาตรฐาน ไม่ว่าจะเป็นภาพถ่าย ลายพิมพ์นิ้วมือ การกำหนดรหัสร่วมกัน การให้นิยามความหมายในการดำเนินการ เช่น คำว่า “สถานที่เกิดเหตุ (Crime scene description) เป็นต้น

4. การเป็นหุ้นส่วน (Partnership) การเป็นหุ้นส่วนถือเป็นกลไกสำคัญสำหรับการเชื่อมโยง หรือบูรณาการข้อมูลในกระบวนการยุติธรรมเข้าด้วยกัน เพราะจะเป็นสิ่งที่แสดงถึงเจตจำนงร่วมกัน (Common Will) ที่จะแลกเปลี่ยนข้อมูลข่าวสารให้มีประสิทธิภาพ มีความเชื่อมั่นและเกิดความรู้สึกมั่นใจ ด้วยการทำงานร่วมกันกับตัวแทนจากหน่วยงานทั้งระดับรัฐบาลกลาง จังหวัด เขตมลฑล และพื้นที่ต้องมีการปรับและสร้างการรับรู้ร่วมกันว่า กรณีใดดำเนินการได้หรือไม่ อย่างไร เป็นต้น นอกจากนี้ยังมีการสื่อสารระหว่างหุ้นส่วนเพื่อให้เกิดความชัดเจนในประเด็นต่างๆและเกิดความตระหนักในการดำเนินการและการใช้ข้อมูล อีกทั้งยังมีการพยายามแสวงหาเครือข่ายอื่นๆ ที่เกี่ยวข้องร่วมกัน เช่น สำนักงานประกันสังคม เป็นต้น

จะเห็นได้ว่า การบูรณาการ การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมของแคนาดานั้นมีการดำเนินการอย่างเป็นระบบชัดเจน โดยร่วมจากการพัฒนาและเตรียมความพร้อมด้านเทคโนโลยีกับหน่วยงานก่อน จากนั้นมีการพัฒนานโยบายและกฎหมาย (รวมทั้งระเบียบต่างๆ) มาสนับสนุน มีการสร้างมาตรฐานเพื่อให้เป็นระบบเพื่อใช้ในการดำเนินการ ต่อจากนั้นก็มีการสร้างความเข้าใจร่วมกันระหว่างหุ้นส่วนที่ร่วมดำเนินการ และเมื่อเข้มแข็งแล้ว ก็มีการขยายการดำเนินการโดยเพิ่มเครือข่ายต่อไป การดำเนินการของแคนาดาจึงน่าจะเป็นบทเรียน (lesson to be learnt) ประการหนึ่งในการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของกลุ่มประเทศ Common Law

2. กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

กฎหมายเกี่ยวกับการแลกเปลี่ยนเชื่อมโยงและบูรณาการข้อมูลในกระบวนการยุติธรรมมีหลากหลายซึ่งได้แก่ กฎหมายลิขสิทธิ์ กฎหมายสิทธิบัตร กฎหมายเครื่องหมายการค้า นิติกรรมสัญญา การบูรณาการข้อมูล (Topography)[58] ซึ่งกฎหมายเหล่านี้มีวัตถุประสงค์ในการใช้แตกต่างกันออกไป ขึ้นอยู่กับการแลกเปลี่ยนเชื่อมโยงข้อมูลว่าจะเป็นลักษณะใด อย่างไรก็ตาม แคนาดายังมีกฎหมายที่เกี่ยวข้องกับการทำธุรกรรมทางอิเลกโทรนิกส์ซึ่งสามารถนำมาปรับใช้ และสามารถที่จะประยุกต์กับการบูรณาการข้อมูลในกระบวนการยุติธรรมได้ ทั้งนี้ โครงการต่างๆ ของแคนาดาได้มีการพัฒนาและปรับปรุงตามนโยบายของกระทรวงยุติธรรมแคนาดา

---

58 Michael Geist **Internet Law in Canada** Cptus Press 2005 P.17

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประเทศแคนาดาซึ่งนำเอากฎหมายความเป็นอิสระของข้อมูลข่าวสารของรัฐมาใช้ในปี 1983 คือพระราชบัญญัติการเข้าถึงข้อมูล ปี 1983 (the Access to information ACT 1983) มีรัฐบาลแบบ Westminster-style จังหวัดทุกจังหวัดยกเว้นเกาะ Prince Edward ล้วนมีกฎหมายความเป็นอิสระของข้อมูลข่าวสารเป็นของตนเอง (ตัวอย่างเช่น Newfoundland มี Freedom of Information Act 1981, New Brunswick มี Right to Information Act 1978) กฎหมายความเป็นอิสระของข้อมูลข่าวสารได้ถูกนำเสนอในเกาะ Prince Edward ในช่วงพิจารณาของสภาระหว่างปี 2000- 2001

พระราชบัญญัติการเข้าถึงข้อมูล ปี 1983 หรือ AIA นี้ใช้บังคับกับกระทรวงทบวง กรมและหน่วยงานของรัฐทุกแห่ง ซึ่งรวมทั้งหน่วยงานตำรวจ และสำนักงานข่าวกรองด้วย ตั้งแต่ปี 1989 เป็นต้นมา ประชาชนหรือบริษัทเอกชนที่อยู่ในประเทศแคนาดาล้วนได้รับสิทธิในการเข้าถึงข้อมูลข่าวสาร รัฐบาลต้องให้คำตอบในทุกเรื่องที่ประชาชนสอบถามไม่ว่าเหตุผลในการร้องขอจะเป็นอย่างไร หน่วยงานราชการที่อยู่ภายใต้พระราชบัญญัติฉบับนี้จะต้องเผยแพร่ข้อมูลเกี่ยวกับบทบาทหน้าที่ของตน โครงสร้างและการดำเนินงานตามนโยบายของตน ต้องเผยแพร่ตารางคิดค่าธรรมเนียมในการขอข้อมูลข่าวสารด้วย ผู้ร้องขอจะต้องได้รับทราบผลการพิจารณาคำร้องขอภายใน 30 วัน

ข้อยกเว้นที่กำหนดในพระราชบัญญัติการเข้าถึงข้อมูลข่าวสารบางอย่างเป็นข้อยกเว้นที่กำหนดโดยกฎหมายส่วนบางอย่างเป็นข้อยกเว้นที่ขึ้นอยู่กับการพิจารณาของหน่วยงานข้อยกเว้นที่กำหนดโดยกฎหมายซึ่งหน่วยงานรัฐไม่สามารถเปิดเผยข้อมูลได้ครอบคลุมข้อมูลที่เป็นความลับที่ได้จากรัฐบาลต่างชาติ ข้อมูลส่วนบุคคล ข้อมูลเชิงการค้าของบุคคลที่สาม และข้อมูลที่เป็นความลับที่มีกฎหมายอื่นบัญญัติไว้ว่าห้ามเปิดเผย ส่วนการประชุมของคณะรัฐมนตรีนั้นได้รับยกเว้นไม่ต้องเปิดเผย ตามพระราชบัญญัติฉบับนี้เป็นเวลายี่สิบปี ยกเว้นเอกสารที่ใช้ประกอบการอภิปรายที่เกี่ยวข้องกับมติของคณะรัฐมนตรี ซึ่งจะต้องเผยแพร่ต่อประชาชนหรือที่ได้จัดทำขึ้นเป็นเวลา สี่ ปีก่อนหน้าที่จะมีการประชุมจะอยู่บังคับของพระราชบัญญัติฉบับนี้ ข้อยกเว้นที่มาจากการพิจารณาของหน่วยงานราชการนั้นครอบคลุมข้อมูลซึ่งสามารถคาดได้ว่าจะก่อให้เกิดอันตรายต่อ การบริหารราชการส่วนท้องถิ่น ความสัมพันธ์ระหว่างประเทศ ความมั่นคงภายในประเทศ ความมั่นคงภายนอกประเทศ ความปลอดภัยของบุคคล ผลประโยชน์ทางเศรษฐกิจของรัฐ การบังคับใช้กฎหมาย การตัดสินใดๆ ของรัฐบาล การปรึกษาระหว่างทนายความกับลูกความ ข้อยกเว้นที่มาจากการพิจารณาของหน่วยงานนั้นขึ้นกับแบบทดสอบความเป็นอันตราย ผู้ตรวจการแผ่นดินรัฐสภา และ

คณะกรรมการพิจารณาข้อมูลข่าวสารอาจทบทวนคำตัดสินของรัฐบาลที่ไม่ได้เปิดเผยข้อมูล เมื่อผู้ร้องขอนั้นได้อุทธรณ์ต่อศาล

ภายใต้บังคับของพระราชบัญญัติความเป็นส่วนตัว (the Privacy Act of . 1983) กำหนดให้บุคคลสามารถเข้าถึงข้อมูลส่วนบุคคลของตนเองได้ ถ้าหน่วยงานราชการมีข้อมูลดังกล่าว โดยต้องเป็นหน่วยงานที่อยู่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ด้วย ในระดับจังหวัด มาตรการเกี่ยวกับความเป็นส่วนตัวและความเป็นอิสระของข้อมูลข่าวสารมีแนวโน้มจะรวมกันเป็นกฎหมายเดียวกัน

การมีพระราชบัญญัติที่กำหนดให้ความเป็นอิสระของข้อมูลข่าวสารในประเทศแคนาดาได้ก่อให้เกิดผลดีอย่างใหญ่หลวง ข้อมูลที่ได้มาโดยบังคับตามข้อกำหนดในพระราชบัญญัติฉบับนี้ได้เปิดเผยให้เห็นการตรวจสอบที่บกพร่องของรัฐบาลที่ทำให้เกิดปัญหาเครื่องบินของสายการบิน AIR CANADA ตก ซึ่งมีผู้เสียชีวิต 24 คน ข้อมูลที่ได้จากเอกสารของทางราชการที่เปิดเผยภายใต้บังคับของพระราชบัญญัติฉบับนี้ได้แสดงให้เห็นว่าเงินอุดหนุนการเกษตรรัฐบาลให้แก่ชาวนาจำนวนหนึ่งพันล้านเหรียญดอลล่าร์แคนาดานั้นเป็นสิ่งที่ไม่จำเป็น เพราะชาวนาหลายคนจะต้องได้รับเงินช่วยจากโครงการ Western Grain Stabilization

อย่างไรก็ตามจากรายงานของคณะกรรมการยุติธรรมที่สืบสวนการบังคับใช้พระราชบัญญัติฉบับนี้ในปี 1986 พบว่า จำเป็นต้องมีการปฏิรูปกฎหมายนี้ และในเดือนสิงหาคม ปี 2000 ก็ได้มีการจัดตั้งคณะทำงานขึ้นมาคณะหนึ่งเพื่อทบทวนพระราชบัญญัติฉบับนี้ งานวิจัย เรื่อง Limited Access: Assessing the Health of Canada’s Freedom of Infoemation Laws School of Policy Studies ใน Queen’s Unievrsity ได้เปิดเผยว่าเกิดข้อบกพร่องในด้านประสิทธิภาพของพระราชบัญญัติความเป็นอิสระของข้อมูลข่าวสารอันเกิดจากการปรับเปลี่ยนโครงสร้างขององค์กรของรัฐใหม่ โดยเฉพาะอย่างยิ่งการตัดลดปริมาณการบริหารของรัฐซึ่งได้ส่งผลให้เกิดความล่าช้าในการดำเนินการปฏิบัติการเกี่ยวกับคำร้องขอ และเกิดผลกระทบต่อความพยายามของรัฐบาลต่อการหาแหล่งรายได้ใหม่ โดยการขยายข้อมูลข่าวสารหรือการเพิ่มค่าธรรมเนียมการร้องขอข้อมูล รายงานวิจัยเรื่องนี้ได้สรุปผลว่า การเพิ่มขึ้นของการไม่ปฏิบัติตามกฎหมายนั้นแสดงให้เห็นถึงความจำเป็นต้องมีรูปแบบใหม่ๆ ในการบังคับใช้กฎหมาย

คณะกรรมการพิจารณาข้อมูลข่าวสารได้วิพากษ์วิจารณ์พระราชบัญญัติฉบับนี้ ในรายงานประจำปี 1998-1999 ว่า

"...จนกระทั่งปัจจุบัน The Treasury Board (ประธานของคณะกรรมการดังกล่าวมีหน้าที่รับผิดชอบการปฏิบัติงานของพระราชบัญญัติฉบับนี้ ได้ปัดความรับผิดชอบของตนในการตรวจสอบคุณภาพของระบบการเข้าถึงข้อมูลข่าวสาร สนับสนุนและเอาใจใส่ผู้ประสานงานการเข้าถึงข้อมูล และปกปิดสถานะการจัดการเอกสารข้อมูลโดยรัฐบาลจากการตรวจสอบ (เอกสารข่าวแจก สำนักงานคณะกรรมการพิจารณาข้อมูลข่าวสารแห่งประเทศแคนาดา วันที่ 21 กรกฎาคม ปี 1999)..."

คณะกรรมการพิจารณาข่าวสารยังได้อ้างอยู่บ่อย ๆ ว่าวัสดุอุปกรณ์ไม่เพียงพอและมีอุปสรรคที่เกิดจากเจ้าหน้าที่ของรัฐเป็นเหตุผลสำคัญของความล่าช้าที่เกิดขึ้นในระบบความเป็นอิสระของข้อมูลข่าวสาร (คำกล่าวของคณะกรรมการพิจารณาข้อมูลข่าวสารต่อที่ประชุมเรื่องการปฏิรูปการเข้าถึงข้อมูลข่าวสาร วันที่ 1 พฤษภาคม ปี 2000[59] เจ้าหน้าที่คนนี้ยังได้เปิดเผยว่าปรารถนาที่จะเห็นทัศนคติแบบใหม่ต่อการเปิดเผยข้อมูลในประเทศแคนาดา โดยสิ่งที่สำคัญในการเปิดเผยของรัฐบาลก็คือการเปลี่ยนแปลงทัศนคติเก่าต่อการเปิดเผยข้อมูลของรัฐบาลที่มองว่าเป็นสิ่งคุกคามความปลอดภัยของตน โดยควรมองเสียใหม่ว่าเป็นโอกาสสำหรับรัฐบาลและประชาชน (คณะกรรมการพิจารณาข้อมูลข่าวสารแห่งประเทศแคนาดา รายงานประจำปี 1994-1995 ออตตาวา ปี 1995 หน้า 4) นอกเหนือจากนี้คำเรียกร้องให้มีการปฏิรูปการเข้าถึงข้อมูลข่าวสารได้แสดงให้ว่าจำเป็นต้องมีการยกเลิกข้อยกเว้นที่ว่าด้วยความลับของคณะรัฐมนต์ตรี โดยอาจจะแทนที่ข้อยกเว้นดังกล่าวด้วยข้อยกเว้นที่ว่าด้วยการยกเว้นไม่เปิดเผยเฉพาะเอกสารของทางราชการที่จะดึงความตั้งใจของคณะรัฐมนตรี และความจำเป็นต้องสร้างหลักเกณฑ์สำหรับข้อยกเว้นที่มาจากการพิจารณาของหน่วยงาน ซึ่งครอบคลุมคำแนะนำด้านนโยบายต่อรัฐมนตรี หรือหน่วยงานต่าง ๆ (คำกล่าวของคณะกรรมการพิจารณาข้อมูลข่าวสารต่อที่ประชุมเรื่อง การปฏิรูปการเข้าถึงข้อมูลข่าวสารวันที่ 1 พฤษภาคม ปี 2000[60]

อาจสรุปได้ว่าในกรณีของประเทศแคนาดานั้น เห็นได้ชัดว่าความตั้งใจของรัฐบาลที่จะปฏิบัติตามกฎหมายความเป็นอิสระของข้อมูลข่าวสาร และบทบัญญัติของกฎหมายความเป็นอิสระของข้อมูลข่าวสารได้เปลี่ยนแปลงการบริหารจัดการภาครัฐแบบมีการปกปิด เป็นการบริหารจัดการภาครัฐอย่างเปิดกว้าง

---

59 www.infoweb.magi.com/-accessca

60 www.infoweb.magi.com/-accessca

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

แคนาดา มีการคุ้มครองฐานข้อมูลที่แตกต่างออกไป โดย แคนาดาถือว่า ฐานข้อมูลนั้น เป็นสิ่งที่ได้รับการคุ้มครองในเชิงสิทธิบัตร (Patent Law) ซึ่งในขณะเดียวกัน ฐานข้อมูลทางอิเลคโทรนิคส์ก็ได้รับการคุ้มครองในเชิงสิทธิบัตรเช่นเดียวกัน ทั้งนี้ ตั้งแต่วันที่ 1 ตุลาคม 1989 โดยในระบบการจัดจำแนก สิทธิบัตรดังกล่าวนั้น ฐานข้อมูล หรือ data base ก็เป็นประเภทหนึ่งของสิทธิบัตรที่ได้รับการคุ้มครอง

อย่างไรก็ตาม ก่อนปี 1991 ฐานข้อมูลที่ได้มีการจัดทำขึ้น จะได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์ก่อน โดยกฎหมาย Copyright Act 1985 โดยมีคดีเกิดขึ้นที่นำไปสู่ปัญหาการเปลี่ยนแปลงคือ คดี CCH Canadian limited v. The Law Society of Upper Canada [61] โดยสมาคมกฎหมายชั้นสูงของแคนาดาได้รวบรวมตีพิมพ์รายงานทางกฎหมาย และอ้างว่า เป็นฐานข้อมูลที่ควรได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์ ซึ่งในคดีนี้ศาลแคนาดาได้พิจารณาถึง ความเป็นงานต้นแบบ (original work) ซึ่งเป็นมาตรฐานขั้นต่ำสุดในการพิจารณาเงื่อนไขของการสร้างสรรค์งาน ซึ่งศาลแคนาดาได้ยึดหลัก การคุ้มครองแบบ overprotection of work มาใช้ติดสิน โดยถือว่า ยังไม่มีหลักฐานเพียงพอที่จะตัดสินถึงการได้รับการคุ้มครองตามกฎหมายลิขสิทธิ์

คดีดังกล่าวส่งผลทำให้แคนาดาได้มีการพัฒนาและปรับปรุงกฎหมาย โดยยกเอาการคุ้มครองฐานข้อมูลไปบรรจุในกฎหมายสิทธิบัตรแทน ดังนั้น ในกรณีการจัดทำฐานข้อมูลด้านงานยุติธรรม และการเชื่อมโยง แลกเปลี่ยน ตลอดจนการบูรณาการข้อมูลในงานด้านยุติธรรมของแคนาดาถือว่าอาจได้รับการคุ้มครอง

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิดของแคนาดา เริ่มจากการที่แคนาดาแก้กฎหมายอาญา (Criminal Act 1985) ให้การเข้าถึงการบริการคอมพิวเตอร์โดยผิดกฎหมายเป็นความผิดอาญา โดยมาตรา 342.1 อย่างไรก็ตาม ต่อมาในมลฑลบริติส โคลัมเบีย ได้มีการออกกฎหมายเฉพาะทางมาใช้คือ The British Computer Misuse Act 1990 โดยมุ่งพิจารณาการกระทำโดยเจตนาที่จะเจาะเข้าแสวงหาประโยชน์จากข้อมูลหรือทำลายในคอมพิวเตอร์โดยไม่มีอำนาจ (รวมทั้งการโจรกรรม) แต่ก็ไม่ได้คุ้มครองการเข้าถึงข้อมูลส่วนบุคคล ปัจจุบันมีการอภิปรายกันอย่างกว้างขวางถึง บทบัญญัติตามกฎหมายอาญาดังกล่าวว่าอาจจะไม่ครอบคลุมการเจาะเข้าระบบข้อมูล (hacking)

---

61 Gervais D. “Feist Goes Global : A Comparative Analysis of the Notion of Original in Copyright law (2002) Journal of Copyright. P.949

5) ประเทศออสเตรเลีย

1. การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

แนวทางในการดำเนินการแลกเปลี่ยน เชื่อมโยงและบูรณาการข้อมูลในกระบวนการยุติธรรมของออสเตรเลียครั้งแรกเริ่มที่ มลฑลวิคตอเรียก่อน โดยเป็นโครงการ “Project Pathfinder” จากนั้น ได้มีการปรับเปลี่ยนและพัฒนากลายมาเป็น โครงการด้านงานยุติธรรม โดยมีหน่วยงานที่ต้องประสานการทำงานคือ ตำรวจ ศาล และราชทัณฑ์ มีการแลกเปลี่ยนข้อมูล ทั้งที่เริ่มจากในรูปเอกสารก่อน การดำเนินการในช่วงแรกเป็นไปอย่างช้า ส่งผลให้มีคดีค้างในศาล Magistrates’Courts มาก ปรากฏการณ์ดังกล่าวเกิดขึ้นทั้งออสเตรเลีย แต่เมื่อโครงการดังกล่าวมีการปรับปรุง แก้ไขจุดบกพร่อง มีการตั้งคณะทำงานร่วมมาดำเนินการ ส่งผลให้บรรลุผลสำเร็จในการดำเนินคดีที่รวดเร็ว มีการใช้การประสานงานแลกเปลี่ยนข้อมูลทางอิเลกโทรนิกส์มากขึ้น การประเมินผลและข้อเสนอแนะจากโครงการ Pathfinder Project นำไปสู่การเปิดโครงการที่เกี่ยวข้องอีกหลายโครงการ อาทิ Mercury Project และ Justice Information Exchange (JIX) เป็นต้น[62] ต่อมา มลฑลอื่นๆ อันได้แก่ Western Australia Queensland New South Wales, South Australia และ Northern ‘Territory ได้ดำเนินการต่อมา

2.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

ในออสเตรเลีย มีกฎหมายที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลที่เป็นปัญหาอุปสรรคอยู่บางฉบับ โดยเฉพาะอย่างยิ่ง กฎหมาย The Privacy Act 1988 ถูกหยิบยกมาอภิปรายว่า ข้อมูลเกี่ยวกับ DNA ที่มีการสืบสวนประกอบการดำเนินคดีจะได้รับการคุ้มครองจากกฎหมายฉบับดังกล่าวหรือไม่ อย่างไรก็ตาม เนื่องจากข้อมูลที่มีการประมวลผลและจัดเก็บได้ดำเนินการในรูป Crim Trac System จึงไม่เข้าข่ายเป็นข้อมูลส่วนตัวที่จะแลกเปลี่ยน เชื่อมโยงหรือส่งต่อไม่ได้ ต่อมารัฐบาลออสเตรเลียมีการออกระเบียบ Model Forensic Procedure Bill และมี The Model Criminal Code Officer’Committee มารองรับ รัฐบาล Commonwealth ได้มีการแก้ไข Crime Act 1914 ในปี 2001 เพื่อป้องกันการนำข้อมูล

---

62 G. Greenleaf and A. Mowbrays **Information Technology in Complex Criminal Trails** (AIJA 1993). P.97

มาใช้ในทางที่ผิด รวมทั้งมีกฎหมาย The Public Service Act 1999[63] ที่ช่วยให้รัฐและมลฑลต่างๆสามารถเชื่อมโยงข้อมูลระหว่างกันได้

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติข้อมูลข่าวสารส่วนบุคคลออสเตรเลีย คือ The Australian federal Freedom of Information Act (AuFOIA)) ประกาศเป็นกฎหมายในปี 1982 (New South Wales-Freedom of Information Act 1989, Queenland-Freedom of Information Act 1992, South Australia-Freedom of Information Act 1991, Victoria-Freedom of Information Act 1982, Western Australia-Freedom of Information Act 1992)

พระราชบัญญัติ AuFOIA ใช้บังคับกับรัฐบาลกลางและหน่วยงานหลายแห่ง ซึ่งรวมหน่วยงานตำรวจด้วย หน่วยงานของรัฐบางแห่งไม่ตกอยู่ภายใต้บังคับของพระราชบัญญัตินี้ อาทิ หน่วยงานด้านความมั่นคงและข่าวกรอง ASIS และ ASIO ซึ่งในพระราชบัญญัติความเป็นอิสระของข้อมูลข่าวสารในสหราชอาณาจักรก็ได้ยกเว้นไม่ใช้พระราชบัญญัตินี้บังคับกับหน่วยงานดังกล่าวข้างต้น

ภายใต้ข้อกำหนดของพระราชบัญญัติ AuFOIA บุคคลใดๆ สามารถเข้าถึงข้อมูลได้โดยต้องมีการเสียค่าธรรมเนียม และจะดำเนินการที่เหมาะสม เพื่อแจ้งผู้ร้องขอถึงผลการพิจารณาคำร้องขอภายใน 30 วัน ซึ่งอาจจะขยายระยะเวลาดังกล่าวออกไปอีก 30 วัน ได้ถ้ารัฐมนตรีหรือหน่วยงานราชการต้องมีการปรึกษากับบุคคลที่สามก่อนมีการเปิดเผยข้อมูล

ข้อยกเว้นที่กำหนดโดยพระราชบัญญัติ AuFOIA หมวดที่ 4 ได้แก่ ข้อมูลดังต่อไปนี้

(a) ข้อมูลที่จะมีผลต่อความมั่นคงของประเทศ การป้องกันประเทศและความสัมพันธ์ระหว่างประเทศ

(b) ข้อมูลที่จะมีผลต่อความสัมพันธ์กับมลรัฐต่างๆ ในประเทศออสเตรเลียซึ่งรวมถึง the Australian Ccpital Territory และ Northern Territory

(c) เอกสารของคณะรัฐมนตรี

(d) เอกสาร Executive Council

(e) เอกสารปฏิบัติงานภายในหน่วยงาน

---

63 Jonathan D. Mobbs **Working at the Edge of The Data Sharing Envelope** (Australian Institute of Criminology 2005) P.2.

(f) ข้อมูลที่จะมีผลต่อการบังคับใช้กฎหมาย และการรักษาความปลอดภัยของประชาชน

(g) เอกสารที่ตกอยู่ภายใต้ข้อบังคับของกฎหมายให้ปกปิดข้อมูล

(h) ข้อมูลที่จะมีผลต่อผลประโยชน์ทางการเงินหรือทรัพย์สินของประเทศ

(i) เอกสารที่เกี่ยวข้องกับการดำเนินงานบางอย่างของหน่วยงานราชการต่างๆ

(j) เอกสารที่เกี่ยวกับความเป็นส่วนตัวของบุคคล

(k) เอกสารที่ขึ้นอยู่กับว่ามีอภิสิทธ์ของวิชาชีพด้านกฎหมายหรือไม่

(l) ข้อมูลเกี่ยวกับการดำเนินธุรกิจ

(m) เอกสารที่เกี่ยวกับการวิจัย

(n) เอกสารที่เกี่ยวกับเศรษฐกิจของประเทศ

(o) เอกสารที่บรรจุวัสดุที่ได้รับมาโดยไม่เปิดเผย

(p) เอกสารที่หากมีการเปิดเผยแล้วจะขัดต่อคำสั่งของรัฐสภาหรือคำตัดสินของศาล

(q) เอกสารบางอย่างที่เกิดจากการพิจารณากฎหมายเกี่ยวกับความมั่นคง และบริษัทเอกชน

(r) Electoral Rolls และเอกสารที่เกี่ยวข้อง

ข้อยกเว้นทั้งหมดนี้ขึ้นอยู่กับการพิจารณาของหน่วยงาน บางอย่างเป็นแบ่งตามประเภทของข้อมูล และไม่มีการทดสอบความเป็นอันตราย ตัวอย่างเช่น ข้อยกเว้นที่เกี่ยวกับเอกสารของคณะรัฐมนตรีมีข้อยกเว้น 5 ข้อ การเปิดเผยจะขึ้นอยู่กับการที่ผลประโยชน์ของสาธารณชนมากกว่าผลประโยชน์จากการปกปิดข้อมูล ได้แก่ข้อยกเว้นในเรื่องเศรษฐกิจของประเทศ เอกสารที่การปฏิบัติงานภายในหน่วยงาน และการปฏิบัติราชการของกระทรวง ทบวง กรมต่างๆ ข้อยกเว้นบางข้อกว้างมากและไม่เจาะจง นอกจากนี้รัฐมนตรีสามารถออกใบรับรองให้ปกปิดข้อมูล ซึ่งพบว่ามักจะใช้บ่อยภายหลังปี 1982 เป็นต้นมา

เมื่อได้รับคำปฏิเสธไม่เปิดเผยข้อมูล ผู้ร้องขอสามารถอุทธรณ์ได้ภายใต้ข้อกำหนดของพระราชบัญญัติ AuFOIA ผู้ร้องขออาจขอให้มีการพิจารณาทบทวนภายในโดยหน่วยงานหรือรัฐมนตรีหรือมีการพิจารณาทบทวนภายนอกโดยคณะกรรมการพิจารณาคำอุทธรณ์ (Administrative Appeals Tribunal) ซึ่งไม่สามารถกลับคำปฏิเสธไม่ให้เปิดเผยข้อมูลได้หากว่าข้อมูลที่ร้องขอไม่ได้มีข้อมูลที่ยกเว้นไม่ให้เปิดเผย การอุทธรณ์ต่อ The Federal Court ในภายหลังจะต้องเป็นเรื่องของประเด็นของกฎหมายที่ใช้

พระราชบัญญัติความเป็นส่วนตัว ปี 1988 (The Privacy Act 1988) ได้ให้สิทธิในการปกป้องจากการใช้ข้อมูลส่วนบุคคลโดยหน่วยงานราชการในเขต Australian Capital Territories และหน่วยงานราชการอื่นๆ ในประเทศ หน่วยงานที่เกี่ยวกับสินเชื่อและหน่วยงานที่รายงานการใช้สินเชื่อ บุคคลที่มีข้อมูลหมายเลขผู้เสียภาษีของบุคคลในครอบครองและใช้ข้อมูลดังกล่าว และหน่วยงานซึ่งขอข้อมูลประวัติอาชญากรรมของบุคคล เมื่อใดก็ตามที่พบว่ามีการละเมิดสิทธิส่วนบุคคลซึ่งขัดต่อข้อกำหนดของพระราชบัญญัติความเป็นส่วนตัว คณะกรรมการพิจารณาความเป็นส่วนตัวจะต้องพิจารณาตัดสินยื่นข้อร้องเรียนต่อผู้ที่กระทำละเมิดดังกล่าว

ในพระราชบัญญัติ AuFOIA ไม่ได้ระบุถึงการตั้งคณะกรรมการพิจารณาข้อมูลข่าวสารโดยให้ภาระหน้าที่ในการสอดส่องดูแลการดำเนินการด้านนี้ตกอยู่กับผู้ตรวจการของรัฐสภา ในรายงานประจำปีของผู้ตรวจการรัฐสภาได้วิพากษ์วิจารณ์ถึงทัศนคติของรัฐบาลต่อพระราชบัญญัติ AuFOIA ในปี 1995 เขาได้รายงานว่า หน่วยราชการหลายแห่งไม่ได้ดำเนินการตามที่กฎหมายพระราชบัญญัติความเป็นอิสระของข้อมูลข่าวสารกำหนดไว้ (ผู้ตรวจการแผ่นดินของรัฐสภารายงานประจำปี 1994-1995,ASPS,1995 หน้า 35)

การจัดตั้งคณะกรรมการพิจารณาความเป็นอิสระของข้อมูลข่าวสารเป็นหนึ่งในคำแนะนำสำคัญที่ปรากฏอยู่ในรายงานประจำปี 1995 ของคณะกรรมการร่วมระหว่างสภาทบทวนการปฏิบัติราชการและคณะกรรมการปฏิรูปกฎหมายแห่งประเทศออสเตรเลีย ได้มีผู้กล่าวถึงประสบการณ์ในด้านความเป็นอิสระของข้อมูลข่าวสารในประเทศออสเตรเลียว่าเป็นการให้ข้อมูลอย่างชักช้า น่าหงุดหงิดมาก (R. Snell, IP Submission 31 to Australian Law Reform Commission and Administration Review Council อ้างถึงในรายงายเรื่อง Administrative Compliance and Freedom of Information in Three Jurisdictions: Australia, Canada, and New Zealand. ซึ่งเสนอต่อที่ประชุมเรื่อง หนึ่งปีภายหลังมีพระราชบัญญัติความเป็นอิสระของข้อมูลข่าวสาร ณ เมือง Dublin วันที่ 23 เมษายน ปี 1999)

ในรายงานของคณะกรรมการร่วมข้างต้น ได้ให้คำแนะนำให้มีการปฏิรูปโดยได้จัดทำแนวทางปฏิบัติที่มีประโยชน์ในการแก้ไขปัญหาที่ประสบในการเปิดเผยข้อมูลข่าวสาร หลังจากที่ได้มีพระราชบัญญัติประกาศใช้แล้วเป็นเวลากว่าหนึ่งทศวรรษ คำแนะนำเหล่านี้ถูกรวมอยู่ในพระราชบัญญัติแก้ไขความเป็นอิสระของข้อมูลข่าวสาร ปี 2000 (the Freedom of Information Amendment (Open Government) Bill 2000) คำแนะนำอื่นๆ ที่สำคัญได้แก่ ข้อเสนอให้มีการจัดตั้งสำนักงานตามกฎหมายของคณะกรรมการพิจารณาความเป็นอิสระของข้อมูลข่าวสารประเด็นเรื่องการทดสอบผลประโยชน์สาธารณชนต่อข้อมูลที่สื่อสารในทางลับ โดยองค์กรระหว่างประเทศ การยกเว้นไม่ต้องเปิดเผยเอกสารของคณะรัฐมนตรีเป็น

เวลายี่สิบปี และการขยายขอบเขตการบังคับใช้พระราชบัญญัติ AuFOIA ต่อหน่วยงานของรัฐประเภทอื่นๆ รายงานดังกล่าวมีความเห็นต่อพระราชบัญญัติ AuFOIA ว่าได้สร้างผลกระทบต่อวิธีการที่หน่วยงานราชการพิจารณาตัดสินและวิธีการที่บันทึกข้อมูล พระราชบัญญัติความเป็นอิสระของข้อมูลข่าวสารได้เน้นการพิจารณาตัดสินอยู่บนปัจจัยที่เกี่ยวข้อง และการบันทึกกระบวนการพิจารณาตัดสินดังกล่าว ความรู้ ความเข้าใจว่า การพิจารณาตัดสินและกระบวนการดังกล่าวจะต้องเปิดกว้างให้ตรวจสอบได้ภายใต้ข้อกำหนดของพระราชบัญญัติความเป็นอิสระของข้อมูลข่าวสารได้สร้างวินัยให้เกิดแก่ภาครัฐโดยทันที

สำหรับโทษทางอาญานั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศออสเตรเลีย มิได้ระบุโทษอาญาสำหรับอาญาสำหรับองค์การเอกชนที่มิได้ปฏิบัติตามคำชี้ขาดของนายทะเบียนหรือคณะกรรมการ อย่างไรก็ตาม ในกรณีที่องค์กรเอกชนมิได้ปฏิบัติตามคำชี้ขาด ผู้เสียหายก็ดี คณะกรรมการก็ดี หรือนายทะเบียนก็ดี สามารถฟ้องต่อ Federal Court Magistrates Court เพื่อสั่งให้องค์การเอกชนปฏิบัติตามคำชี้ขาด เมื่อมีการฟ้องร้องต่อศาลแล้ว ศาลต้องเริ่มพิจารณาคดีใหม่ (trail de novo)

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

ในกฎหมายลิขสิทธิ์ที่คุ้มครองฐานข้อมูลของออสเตรเลียนั้น เกิดจากการตัดสินของศาลในคดี Desk top Marketing Systems Pty Ltd v Telstra Corporation Limited ว่าจะขยายกฎหมายลิขสิทธิ์ไปคุ้มครองฐานข้อมูลในกฎหมายออสเตรเลียได้อย่างไร[64]

หลักเกณฑ์ที่สำคัญของกฎหมายลิขสิทธิ์ก็คือ ลิขสิทธิ์จะไม่คุ้มครองแนวคิดหรือ ข้อเท็จจริง (ideas or facts) แต่จะให้การคุ้มครองรูปแบบของแนวคิดหรือข้อเท็จจริงที่ปรากฏนั้น และหลักเกณฑ์การจะได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์นั้น ก็คือ ผลงานนั้นต้องมีลักษณะต้นแบบ (original) คดีดังกล่าวได้รับการอภิปรายกันมาว่า บันทึกระบบโทรศัพท์หน้าเหลือง และหน้าขาว (White and Yellow Pages telephone directories) ของบริษัท Telstra โดยมีการทำ CD ประกอบเพื่อให้บุคคลต่างๆสามารถค้นหา ชื่อ รหัสไปรษณีย์ ที่อยู่ หรือ หมายเลขโทรศัพท์ ซึ่ง Telstra อ้างว่า การดำเนินการดังกล่าวเป็นการพัฒนาและจัดทำฐานข้อมูลจำเป็นจะต้องได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์ คือ Copyright Act 1968 เพราะถือว่า เป็นงานที่มีลักษณะเป็นงานต้นแบบ ประเด็นปัญหากฎหมายก็คือ กฎหมายลิขสิทธิ์ออสเตรเลียให้การคุ้มครองการรวบรวมข้อมูล ตามหลัก Sweat of the brow หรือ industrious collection มิฉะนั้น อาจมีบุคคลใดทำการคัดลอกทำสำเนาออกจำหน่ายในเชิงพาณิชย์ได้

---

64 Brain Fitzrerald and Cheranne Bartlett Database Protection under Australian Copyright law. P. 308

ดังนั้น ในออสเตรเลีย การจัดทำฐานข้อมูล และการดำเนินการเชื่อมโยงแลกเปลี่ยนข้อมูลตลอดจนการบูรณาการข้อมูลก็จะได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์ด้วยเช่นกัน หากเข้าเงื่อนไขการดำเนินการ

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ในประเทศออสเตรลีย การป้องกันและควบคุมอาชญากรรมคอมพิวเตอร์มีการดำเนินงานมาอย่างต่อเนื่องในช่วงทศวรรษที่ผ่านมา ปี พ.ศ. 2532 ตำรวจรัฐวิคตอเรียจัดตั้งหน่วยสืบสวนคดีอาชญากรรมคอมพิวเตอร์ ต่อมาในปี พ.ศ. 2533 ตำรวจแห่งชาติออสเตรเลียตั้งแผนกอาชญากรรมคอมพิวเตอร์ พร้อมที่ทำการในส่วนภูมิภาค ณ กรุงเมล์เบิร์น ซิดนีย์ และเพิร์ท และชุดตรวจพิสูจน์คอมพิวเตอร์ (Computer Forensic Examination Team) ประจำอยู่ ณ กรุงแคนเบอร์ร่า การดำเนินงานในรัฐควีนแลนด์เริ่มต้นในปี พ.ศ. 2535 โดยคณะกรรมาธิการกระบวนการยุติธรรมแห่งรัฐควีนแลนด์ จัดให้มีโครงการบริการตรวจพิสูจน์คอมพิวเตอร์ (Computer Forensic Unit) ในปี พ.ศ. 2538 สำหรับตำรวจรัฐเวสท์เทิร์นออสเตรเลีย ตั้งหน่วยสืบสวนคดีอาชญากรรมคอมพิวเตอร์ เมื่อปี พ.ศ. 2539 หน่วยงานที่เกี่ยวข้องกับคดีอาชญากรรมคอมพิวเตอร์ ได้รับการสนับสนุนและการประสานงานความร่วมมือทางวิชาการและเทคนิค จากสถาบันวิจัยการตำรวจแห่งชาติ (National Police Research Unit) ภายใต้โครงการเทคนิคการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์(Computer Investigation Techniques Program) ซึ่งเริ่มตั้งแต่ปี พ.ศ. 2535 ในรัฐต่าง ๆ ของประเทศออสเตรเลียยกเว้นรัฐควีนแลนด์ กฎหมายอาชญากรรมคอมพิวเตอร์ (Computer specific laws) มีบังคับใช้เป็นการเฉพาะ โดยแยกจากกฎหมายอาชญากรรมธุรกิจ ซึ่งเริ่มออกเป็นกฎหมายระหว่างปี พ.ศ. 2526 ถึง 2534 เป็นต้นมา และในปี พ.ศ. 2539 มีการแก้ไขเพิ่มเติมเกี่ยวกับภาพเด็กลามกอนาจารและความรุนแรงของเกมคอมพิวเตอร์ การฝึกอบรมด้านการสืบสวนคดีอาชญากรรมคอมพิวเตอร์เริ่มต้นดำเนินการในช่วงต้นของทศวรรษ 1980 ส่งเจ้าหน้าที่ศึกษาดูงานหน่วยงานในต่างประเทศ และเข้าร่วมฝึกอบรมหลักสูตรการสืบสวนคดีอาชญากรรมคอมพิวเตอร์ในต่างประเทศ

เมื่อวันที่ 1 ตุลาคม 2001 กฎหมาย Cybercrime 2001 (Cth) Act ได้รับความเห็นชอบจากสภาผู้แทนของออสเตรเลีย และกฎหมายเพื่อต่อต้านและป้องกันการกระทำผิดอันเกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ต จะมีผลใช้บังคับคับ ในวันที่ 2 เมษายน 2002 นี้ กฎหมายฉบับนี้ได้เพิ่มเติมบทบัญญัติใหม่ในส่วนที่ 10.7 ของกฎหมายอาญา Crime Code Act 1995 (Cth) ซึ่งบทบัญญัติใหม่ดังกล่าวนี้ ได้ประกอบด้วยฐานความผิดซึ่งกระทำในรูปแบบต่าง ๆ ของอาชญากรรมไซเบอร์ ซึ่งทำให้เสียหายต่อความปลอดภัย ความสมบูรณ์ และความน่าเชื่อถือได้ของข้อมูลคอมพิวเตอร์ และการสื่อสารอิเล็กทรอนิกส์

กฎหมายนี้ได้กำหนดโทษร้ายแรงต่อการกระทำผิดอันเกี่ยวกับคอมพิวเตอร์ไว้ 3 ประการดังนี้

(1) การเข้าไปในระบบ ทำการเปลี่ยนแปลง หรือทำให้เสียหาย ด้วยเจตนากระทำการละเมิดอย่างร้ายแรง ซึ่งจะมีโทษสูงสุด เท่ากับโทษสูงสุดที่กำหนดไว้ในกรณีที่เป็นเหตุฉกรรจ์ ตัวอย่างที่ได้ให้ไว้ในระหว่างการร่าง กฎหมายฉบับนี้ เช่น ในกรณีที่ผู้ใดได้เจาะระบบ หรือแฮคส์ (hacking) คอมพิวเตอร์ของธนาคาร และเข้าถึง ข้อมูลหมายเลขเครดิตการ์ด ซึ่งผู้กระทำการดังกล่าวเจตนาที่จะใช้ข้อมูลเพื่อการได้มาซึ่งเงิน ถือได้ว่า เป็นความผิด และต้องได้รับโทษ ฐานฉ้อโกงหรือ Fraud

(2) การเปลี่ยนแปลงข้อมูลโดยมิได้รับอนุญาต ในกรณีที่ผู้ใดประมาทเลินเล่อ ไม่ว่าการเปลี่ยนแปลงข้อมูลจะทำให้ข้อมูล เสียหาย หรือไม่ก็ตาม มีโทษสูงสุดจำคุก 10 ปี บทบัญญัติดังกล่าวนี้ มีความมุ่งหมายที่จะให้ครอบคลุมถึงการกระทำผิด ในหลายรูปแบบ เช่น การที่นักเจาะระบบ หรือ แฮคเกอร์ได้เจาะเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และทำให้ข้อมูลเสียหาย

(3) การทำให้เสียหาย ซึ่งการสื่อสารทางอิเล็กทรอนิกส์ มีโทษจำคุกสูงสุด 10 ปี กรณีนี้ เช่น การใช้กลอุบาย โดยทำให้การสื่อสาร ที่อิเล็กทรอนิกส์ขัดข้อง โดยการโจมตีด้วยการส่งข้อความอิเล็กทรอนิกส์อันไม่ถึงประสงค์เป็นจำนวนมาก ไปยังเว็บไซต์ใดเว็บไซต์หนึ่ง อันก่อให้เซิร์ฟเวอร์ของระบบดังกล่าวล้มเหลวในการทำงาน หรือให้บริการ

นอกจากนี้ กฎหมายใหม่นี้ ยังได้เพิ่มอำนาจในการทำการสืบสวนสอบสวน ในกรณีที่ต้องมีการตรวจสอบค้นหรือยึดชั่วคราว ซึ่งข้อมูลที่รักษาไว้ในรูปแบบอิเล็กทรอนิกส์ ทั้งนี้โดยการทำการแก้ไข Crime Act 1914 และ Customs Act 1901 ทั้งนี้รวมถึง การแก้ไขกฎหมายอื่น เพื่อให้รับกับกฎหมายใหม่นี้ ได้แก้ไขกฎหมายต่อไปนี้ด้วย : Australian Security Intelligence Organization Act 1979,Education Services for Overseas Students Act 2000 และ Telecommunications (Interception) Act 1997

6) ประเทศนิวซีแลนด์

1. การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

นิวซีแลนด์ มีการสร้างยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ คือ The Justice Sector Information Strategy for 2006-2011 โดยมีการกำหนดเกณฑ์การวัดความก้าวหน้าในระยะต่างๆ (milestone) ในการแลกเปลี่ยนข้อมูลข่าวสารในกระบวนการยุติธรรม โดยมีการพัฒนาจากระบบ LES (Law Enforcement System) ไปสู่การกระจายข้อมูลให้หน่วยงานในท้องถิ่น

มีการดำเนินการในระยะเวลาที่ผ่านมาที่เอื้อต่อการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมคือ

1. มีการตั้งศูนย์ข้อมูลกลาง (Central Electronic database)
2. ปรับปรุงการเข้าถึงข้อมูลสารสนเทศในกระบวนการยุติธรรม
3. พัฒนามาตรฐานทั่วไปและ protocol ในการแลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรม และดำเนินการตามมาตรฐานด้าน E-Government
4. กำหนด / จัดตั้งห้องปฏิบัติการร่วม (justice Workspace) เพื่อให้คณะทำงานด้านเทคโนโลยีสารสนเทศจากหลายๆองค์กรในกระบวนการยุติธรรมมาทำงานร่วมกัน

โดยหน่วยงานที่มีการเริ่มต้นแลกเปลี่ยนข้อมูลประกอบด้วย กระทรวงยุติธรรมนิวซีแลนด์ ตำรวจราชทัณฑ์ กรมการขนส่งทางบก

2.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

นิวซีแลนด์ได้ทบทวนและมีการออกกฎหมายที่เกี่ยวข้องกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลที่เด่น คือ [65]Electorinic Transaction Bill ซึ่งผ่านออกมาบังคับใช้เมื่อพฤศจิกายน 2003 กฎหมายดังกล่าว มีวัตถุประสงค์ที่จะเอื้อต่อการใช้เทคโนโลยีสารสนเทศและส่งเสริมนวัตกรรมทางเศรษฐกิจ โดยให้รายละเอียดในด้านการเก็บรวบรวม ลายเซ็นข้อมูลทางอิเลกทรอนิกส์ การให้ความยินยอมในการใช้เทคโนโลยีทางอิเลกทรอนิกส์

---

65 New Zealand Ministry of Justice

ยังมีกฎหมายประกอบอื่นๆอีก ได้แก่ Electronic Commerce Part three The Telecommunication Act 2001 และ ยอมรับ Australian Electronic Transaction Bill 1999 การให้ข้อมูลเป็นลายลักษณ์อักษร ลายเซ็น และความรับผิด เอกสารในรูป electronic form และการรับรองเป็นพยาน เป็นต้น

นิวซีแลนด์มีพัฒนากฎหมายด้านอิเลกโทรนิกส์ค่อนข้างช้า ทั้งๆที่ชนชั้นกลางในนิวซีแลนพ์นั้นมีการใช้เทคโนโลยีสารสนเทศและคอมพิวเตอร์อย่างแพร่หลาย กฎหมาย The Electronic Transaction Bill ได้ผ่านสภา เมื่อ พฤศจิกายน 2000

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติข้อมูลข่าวสารของราชการในประเทศนิวซีแลนด์ (The Official Information Act OIA) ได้รับการประกาศใช้เป็นกฎหมายในปี ค.ศ. 1982 หลักการตีความมาตราต่างๆ ในพระราชบัญญัตินี้อยู่ในมาตรา 5 ซึ่งกำหนดว่าพระราชบัญญัติจะต้องถูกตีความอย่างสอดคล้องกับวัตถุประสงค์ของพระราชบัญญัติและหลักการที่ว่าข้อมูลจะต้องเผยแพร่แก่ประชาชนได้ เว้นเสียแต่ว่าจะมีเหตุผลที่ดีในการปกปิดข้อมูลนั้นๆ พระราชบัญญัติฉบับนี้ใช้บังคับรัฐบาลกลาง หน่วยงานราชการต่างๆ สำนักงานตำรวจ สำนักงานข่าวกรอง และรัฐวิสาหกิจส่วนใหญ่พระราชบัญญัติฉบับนี้ให้สิทธิในการเข้าถึงข้อมูลของรัฐบาลซึ่งอยู่ในรูปแบบเอกสารทางราชการและข้อมูลที่ยังไม่ได้รับการบันทึก (สำหรับตำแหน่งที่เกี่ยวข้องกับข้อมูลที่ยังไม่ได้รับการบันทึกภายใต้พระราชบัญญัติฉบับนี้)

สำหรับพระราชบัญญัติข้อมูลส่วนบุคคล ปี 1993 (The Privacy Act 1993) ได้กำหนดหลักการเกี่ยวกับข้อมูลส่วนบุคคล 12 หลักเกณฑ์เกี่ยวกับการรวบรวม การเก็บรักษาการใช้และการเปิดเผยข้อมูลข่าวสาร พระราชบัญญัติฉบับนี้ได้ให้สิทธิในการเข้าถึงข้อมูลและขอให้มีการแก้ไข ข้อมูลส่วนบุคคล ผู้บังคับใช้ให้เป็นไปตามพระราชบัญญัตินี้ได้แก่ คณะกรรมการข้อมูลส่วนบุคคล ซึ่งใช้บังคับกับหน่วยงานทั้งภาครัฐและเอกชน

ข้อยกเว้นทั้งหมดในพระราชบัญญัติข้อมูลข่าวสารของราชการ เป็นข้อยกเว้นที่ขึ้นอยู่กับการพิจารณาของหน่วยงาน และขึ้นอยู่กับแบบทดสอบความเป็นอันตรายข้อยกเว้นนี้ครอบคลุมข้อยกเว้นที่เมื่อเปิดเผยแล้วจะทำให้

(a) เกิดผลร้ายต่อความมั่นคง หรือการป้องกันประเทศนิวซีแลนด์ หรือความสัมพันธ์ระหว่างประเทศ

(b) เกิดผลร้ายต่อข้อมูลลับสุดยอดที่รัฐบาลต่างชาติ หรือองค์กรระหว่างประเทศให้แก่รัฐบาลประเทศนิวซีแลนด์

(c) เกิดผลร้ายต่อการรักษากฎหมายของประเทศ

(d) เกิดอันตรายต่อความปลอดภัยของบุคคล หรือ

(e) ทำลายเศรษฐกิจของประเทศนิวซีแลนด์อย่างร้างแรง โดยการเปิดเผยข้อมูลเกี่ยวกับการตัดสินใจเปลี่ยนแปลงหรือนโยบายทางการเงิน หรือนโยบายทางเศรษฐกิจของรัฐบาลต่อไป

มีข้อยกเว้น 11 ข้อ ดังต่อไปนี้ที่สามารถปกปิดข้อมูลได้โดยอาศัยการทดสอบผลประโยชน์สาธารณชน โดยข้อมูลที่จะได้รับยกเว้นเป็นข้อมูลเพื่อ

(a) ป้องกันการละเมิดความเป็นส่วนตัวของบุคคล

(b) ป้องกันความลับทางการค้า

(c) ป้องกันข้อมูลซึ่งจำเป็นต้องรักษาเป็นความลับ หรือเป็นข้อมูลที่บุคคลถูกหรือสามารถถูกบังคับต้องให้ข้อมูล ภายใต้ข้อกำหนดของกฎหมายต่างๆ ซึ่งการเผยแพร่ข้อมูลนั้นๆ จะเกิดผลเสียต่อการจัดหาข้อมูลในลักษณะเดียวกัน หรือข้อมูลที่มาจากแหล่งเดียวกัน และขึ้นอยู่กับผลของการทดสอบผลประโยชน์สาธารณชนว่า ข้อมูลนั้นๆ สมควรได้รับการเปิดเผยต่อไปหรือไม่

(d) หลีกเลี่ยงผลเสียที่จะเกิดขึ้นต่อมาตรการปกป้องสุขภาพหรือความปลอดภัยของประชาชน

(e) หลีกเลี่ยงผลเสียต่อผลประโยชน์ทางเศรษฐกิจของประเทศนิวซีแลนด์

(f) หลีกเลี่ยงผลเสียต่อมาตรการที่ช่วยป้องกันหรือลดความสูญเสียวัสดุอุปกรณ์ของประชาชน

(g)รักษาให้เป็นไปตามข้อบัญญัติของรัฐธรรมนูญในการคุ้มครองการสื่อสารของพระมหากษัตริย์ หรือการสื่อสารกับกษัตริย์ หรือผู้แทนของพระมหากษัตริย์ ความรับผิดชอบของรัฐมนตรีแต่ละคน ความเป็นกลางของเจ้าพนักงานของรัฐ และคำแนะนำของรัฐมนตรีสำนักพระราชวัง และเจ้าหน้าที่ที่มีต่อพระมหากษัตริย์

(h) รักษาการบริหารกิจการสาธารณะอย่างมีประสิทธิภาพ ผ่านการเสนอความเห็นที่เป็นกลางและเป็นอิสระของหรือระหว่างรัฐมนตรี หรือเจ้าหน้าที่และลูกจ้างของกระทรวง ทบวง กรมของรัฐใดๆ

(i) รักษาอภิสิทธิ์ของวิชาชีพทางกฎหมาย

(j) ทำให้รัฐมนตรีสำนักพระราชวัง หรือกระทรวงใดๆ หรือหน่วยงานใดที่มีข้อมูลข่าวสารนั้นสามารถดำเนินการปฏิบัติงานกิจกรรมทางพาณิชย์หรือการเจรจาของอุตสาหกรรมโดยไม่มีผลเสียหรือการเสียเปรียบ

(k) ป้องกันไม่ให้มีการเปิดเผยข้อมูลของราชการหรือการใช้ข้อมูลของราชการเพื่อผลประโยชน์ที่ไม่เหมาะสม

พระราชบัญญัติฉบับนี้นั้นจะมีผู้ตรวจราชการแผ่นดินของรัฐสภาเป็นผู้ดูแลสอดส่องให้มีการบังคับใช้กฎหมายดังกล่าว เพื่อความเป็นอิสระของข้อมูลข่าวสาร การอุทธรณ์การปฏิเสธคำร้องขอที่ขอให้เปิดเผยข้อมูลจะต้องกระทำต่อผู้ตรวจการแผ่นดินของรัฐสภาและศาล เมื่อผู้ตรวจการแผ่นดินของรัฐสภามีคำสั่งให้มีการเปิดเผยข้อมูลแล้ว คณะรัฐมนตรีจะร่วมกันใช้สิทธิวีโต้ (Veto) ไม่ได้

พระราชบัญญัติข้อมูลของราชการ ปี 1982 ได้รับการทบทวนแก้ไขในปี 1997 โดยคณะกรรมการพิจารณากฎหมายของประเทศนิวซีแลนด์ คณะกรรมการดังกล่าวพบว่าปัญหาสำคัญของพระราชบัญญัติฉบับนี้และการบังคับใช้กฎหมายคือ การที่มีผู้ร้องขอทราบข้อมูลจำนวนมาก และมีขอบข่ายกว้างขวาง ความล่าช้าในการดำเนินการตามคำร้องขอ การขัดขืนต่อด้านจากหน่วยงานที่อยู่ภายนอกภาครัฐ และการขาดการประสานงานในด้านการกำกับดูแลการปฏิบัติตาม การให้คำแนะนำในนโยบาย และการให้ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติฉบับนี้

อย่างไรก็ตาม รายงานของคณะกรรมการพิจารณากฎหมายของประเทศนิวซีแลนด์ พบว่า ไม่มีการนำเอาปัญหาต่างๆ หรือขอบเขตการอ้างอิงที่เกิดขึ้นมาตั้งคำถามต่อหลักการสำคัญของพระราชบัญญัติฉบับนี้ (New Zealand Law Commission Report 40, Review of the Official Information Act 1982, (1997), หน้า11) ในรายงานดังกล่าวยังได้มีข้อแนะนำเกี่ยวกับมาตรการส่งเสริมการติดต่อสื่อสารระหว่างหน่วยงานราชการกับผู้ร้องขอทราบข้อมูล และมาตรการในการลดจำนวนคำร้องขอที่ถูกปฏิเสธไม่ให้มีการเปิดเผยข้อมูลเพราะเหตุผลว่าการทำตามคำร้องขอดังกล่าวจะต้องมีการรวบรวมหรือวิจัยจำนวนมาก คำแนะนำในรายงานยังคงเห็นด้วยกับการมีอยู่ของสิทธิร่วมกันของคณะรัฐมนตรีในการคัดค้าน (Veto) และโครงสร้างการคิดค่าธรรมเนียม ทว่ารัฐมนตรีกระทรวงยุติธรรมจะต้องมีหน้าที่ความรับผิดชอบอย่างเป็นระบบในการดูแล การปฏิบัติการ การดำเนินการและการให้ความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติฉบับนี้ นอกจากนี้ยังมีคำแนะนำที่เกี่ยวกับการมีทรัพยากรที่มีเพียงพอเพื่อช่วยให้ผู้ตรวจการของรัฐสภา หรือองค์กรอื่นๆ สามารถปฏิบัติหน้าที่ของตนตามข้อกำหนดของพระราชบัญญัตินี้อย่างมีประสิทธิภาพ คณะกรรมการพิจารณากฎหมายมีความเห็นว่าระยะเวลาการดำเนินการคำร้องขอควรจะลดจากเดิม 20 วัน เป็น 10 วัน

ในรายงานประจำปีของผู้ตรวจการแผ่นดินของรัฐสภา ปี 1999 ได้กล่าวถึงการไม่ปฏิบัติตามข้อบังคับของพระราชบัญญัติฉบับนี้ว่า

มีหลายครั้งที่รัฐมนตรีและหน่วยงานราชการไม่ได้ทำตามระยะเวลาที่กำหนดไว้ในพระราชบัญญัติ แม้ว่าจะไม่มีการกำหนดถึงกลไกการลงโทษในการไม่ปฏิบัติภายในระยะเวลาที่กำหนดไว้ก็ตาม หน่วยงานราชการก็ควรพยายามปฏิบัติตามเจตนารมณ์ของพระราชบัญญัติโดยการดำเนินการคำร้องขอภายในระยะเวลาที่เหมาะสม การไม่ปฏิบัติตามเจตนารมณ์ของพระราชบัญญัติเป็นการทำลายคุณธรรมของการบริหารจัดการภาครัฐที่ดีและลดทอนความเชื่อถือที่ประชาชนมีต่อการดำเนินงานของภาครัฐดังกล่าว โดยรวมแล้ว การดำเนินงานที่ผ่านมาในเรื่องความเป็นอิสระของข้อมูลข่าวสารเป็นไปในทางบวก เห็นได้ชัดว่าคุณภาพของเอกสารทางราชการและข้อมูลที่เจ้าพนักงานของรัฐจัดทำขึ้นได้มีการพัฒนาดีขึ้นอย่างชัดเจนจากการเกิดขึ้นของพระราชบัญญัติข้อมูลของราชการนี้

ในรายงานของคณะกรรมการพิจารณากฎหมายของประเทศ นิวซีแลนด์ได้พบว่าการยอมรับหลักการเปิดเผยของรัฐบาลในประเทศนิวซีแลนด์เป็นผลมาจากพระราชบัญญัติข้อมูลของราชการนอกจากนี้รายงานฉบับนี้ยังพบว่าภายหลังปี 1982 เป็นต้นมาได้มีการเปลี่ยนแปลงขนานใหญ่ในทัศนคติต่อการเปิดเผย ข้อมูลข่าวสารของรัฐบาล รัฐมนตรีและเจ้าพนักงานของรัฐ เรียนรู้ที่จะมีการเปิดกว้างของข้อมูล สมมุติฐานที่ว่าคำแนะนำเกี่ยวกับนโยบายของรัฐบาลต้องได้มีการเผยแพร่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ ได้มีส่วนพัฒนาคุณภาพและความโปร่งใสของคำแนะนำเกี่ยวกับนโยบายของรัฐบาล ผู้ตรวจการแผ่นดินของรัฐสภาได้พูดถึงวิวัฒนาการของพระราชบัญญัติฉบับนี้และผลกระทบต่อการดำเนินงานของรัฐบาลจนกระทั่งเมื่อไม่นานมานี้ ในตอนแรกพระราชบัญญัติฉบับนี้ถูกใช้บังคับเพื่อวัตถุประสงค์ในการมีความรับผิดชอบ (Accountability) มากกว่าวัตถุประสงค์ในการมีส่วนร่วมของประชาชน (Participation) หลักฐานที่มีอยู่แสดงให้เห็นว่าวัตถุประสงค์แรกเริ่มนั้นได้ค่อยๆ เปลี่ยนแปลงไปเป็นการตระหนักถึงประโยชน์ซึ่งเป็นผลมาจากการออกพระราชบัญญัติและนโยบายต่างๆ ในทำนองเดียวกัน อาจกล่าวได้ว่าถ้ากฎหมายและนโยบายต่างๆ ถูกตราขึ้นหรือจัดทำขึ้นอย่างดีมาตั้งแต่เริ่มแรก ก็ไม่จำเป็นที่ผู้ที่ออกกฎหมาย หรือจัดทำนโยบายจะต้อง รับผิดชอบใดๆ

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

กฎหมายลิขสิทธิ์ของนิวซีแลนด์คือ The Copyright Act 1994 ซึ่งกฎหมายฉบับนี้ให้นิยามความหมายของงานที่มีลิขสิทธิ์ไว้ และมาตรการในการคุ้มครอง ซึ่งเมื่อไม่นานมานี้ (ธันวาคม 2006) รัฐบาลนิวซีแลนด์ได้มีการแก้ไขกฎหมาย โดยให้คุ้มครอง New Technology and performer's rights เพื่อปกป้องข้อมูลที่เป็นเทคโนโลยีสารสนเทศโดยมีการกำหนดการ

ทดสอบ 3 ขั้นตอน และกำหนดความรับผิดไว้ชัดเจนในด้านเกี่ยวกับการเก็บรวบรวมข้อมูลด้วยระบบดิจิตอล

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ในเดือน ธันวาคม 1998 คณะกรรมาธิการกฎหมายของนิวซีแลนด์ได้เสนอให้มีการแก้ไขกฎหมาย The Crime Act 1961 เพื่อให้เหมาะสมกับคดีที่เกิดขึ้น ในนิวซีแลนด์ คือ คดี R v Wilkinson (1999)[66] โดยในหมวด X อย่างไรก็ดี ต่อมากระทรวงยุติธรรมของนิวซีแลนด์ ได้เสนอร่างกฎหมาย The Computer Misuse Act เพราะเห็นว่า กฎหมายฉบับใหม่จะสามารถกำหนดบทบัญญัติให้ครอบคลุมได้มากกว่า โดยมีการกำหนดองค์ประกอบ

(1) การขัดขวางการจัดเก็บข้อมูลในคอมพิวเตอร์โดยไม่มีอำนาจ

(2) การเข้าถึงข้อมูลที่เก็บในคอมพิวเตอร์ โดยไม่มีอำนาจ

(3) การใช้ข้อมูลที่จัดเก็บในคอมพิวเตอร์ โดยไม่มีอำนาจ และ

(4) การทำลายข้อมูลที่มีการจัดเก็บในคอมพิวเตอร์โดยไม่มีอำนาจ

ข.กลุ่มประเทศ Civil Law

ประเทศในกลุ่ม Civil Law หลายประเทศเป็นประเทศที่มีระบบกฎหมายที่มีการพัฒนาและมีการปรับเปลี่ยนตามแนวทางของสหภาพยุโรป อันเป็นผลมาจากการรวมตัวกันของกลุ่มประเทศในสหภาพยุโรปนั่นเอง แม้ว่าบางประเทศ เช่น อังกฤษ จะเป็นประเทศที่มีระบบกฎหมายแบบCommon Law ก็ตาม ดังนั้นก่อนที่จะลงในรายละเอียดของประเทศต่างๆในระบบ Civil law ขอนำเอาแนวทางการดำเนินการที่เกี่ยวข้องกับการเชื่อมโยงและกฎหมายที่เกี่ยวข้องกับการแลกเปลี่ยน การบูรณาการข้อมูลในกระบวนการยุติธรรมบางแนวทางมาแสดงดังนี้

2.1กฎหมายคุ้มครองข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์ของสหภาพยุโรป

แม้ประเทศในกลุ่มสหภาพยุโรป จะมีศักยภาพในการพัฒนาเทคโนโลยีทางด้านข้อมูลข่าวสารไม่น้อยหน้าไปกว่าสหรัฐอเมริกา แต่ก็ต้องประสบกับอุปสรรคหลายประการในการที่จะพัฒนาระบบเทคโนโลยีสารสนเทศที่แข็งแกร่งและเป็นหนึ่งเดียวกัน อย่างเช่นปัญหาในเรื่องการใช้ภาษาที่แตกต่าง และกฎหมายแรงงานที่เป็นอุปสรรค ประเทศสมาชิกใช้ภาษาที่แตกต่างกัน และขนาดของเศรษฐกิจที่เล็กกว่าสหรัฐอเมริกามาก ความเป็นจริงที่อุตสาหกรรมทางด้านฐานข้อมูลของยุโรปกระจุกตัวอยู่ในประเทศเดียว คือ สหราชอาณาจักร ยังสะท้อนให้เห็นถึงความไม่เท่าเทียมกันในส่วนฐานข้อมูลระหว่างประเทศสมาชิกของสหภาพยุโรป และความ

---

66 New Zealand Info Tech Weekly 11 April 1999.

แตกต่างในนโยบายเรื่องการคุ้มครองทรัพย์สินทางปัญญาด้วยเช่นกัน สหภาพยุโรปไม่มีระบบการให้ความคุ้มครองฐานข้อมูลอิเล็กทรอนิกส์ที่เป็นอันหนึ่งอันเดียวกัน มีเพียงบางประเทศที่คุ้มครองเนื้อหาของฐานข้อมูล (the database contents)

ความพยายามในการพัฒนาอุตสาหกรรมฐานข้อมูลของยุโรป เริ่มที่จะเป็นรูปเป็นร่างตั้งแต่การศึกษาและประชาพิจารณ์ความคิดเห็นของอุตสาหกรรมฐานข้อมูลในยุโรป โดยคณะกรรมาธิการยุโรป (European Committee) ในปี 1988 เพื่อหาแนวทางและกำหนดเกณฑ์การให้ความคุ้มครองทางทรัพย์สินทางปัญญาจากการพัฒนาเทคโนโลยี จากนั้นจึงได้ทำรายงานสมุดปกเขียวเกี่ยวกับลิขสิทธิ์และความก้าวหน้าของเทคโนโลยี (Green Paper on Copyright and the Challenge of Technology: Copyright Issues Requiring Immediate Action) เพื่อให้สหภาพยุโรปสามารถนำไปใช้เพื่อเอาชนะอุปสรรคปัญหาในการเคลื่อนย้ายข้อมูลข่าวสารอิสระ (Obstacles to the free movement of information) ที่จะเอื้อประโยชน์ต่อการพัฒนาฐานข้อมูลอิเล็กทรอนิกส์ของกลุ่มประเทศสมาชิก หลังจากนั้นในปี 1992 กรรมาธิการยุโรปได้นำหลักกฎหมายคุ้มครองฐานข้อมูลที่ได้จากรายงานสมุดปกเขียวพิจารณาและเสนอให้ออกกฎหมายคุ้มครองฐานข้อมูล (Proposal for a Council Directive on the Legal Protection of Database) ซึ่งกำหนดรูปแบบ ขอบเขต และระยะเวลาความคุ้มครองทั้งภายในกฎหมายลิขสิทธิ์ และหลักกฎหมายลักษณะเฉพาะ (sui generic) จนสำเร็จออกมาเป็นกฎหมายออกมาให้ความคุ้มครองแก่ฐานข้อมูล (European Database Directive) ซึ่งมีผลบังคับใช้เมื่อ 1 มกราคม 1998 ที่ให้อำนาจผู้บริหารสหภาพยุโรปได้เลือกใช้กฎหมายที่มีอยู่ของรัฐต่างๆ ร่วมกับข้อกำหนดและข้อจำกัดทางการค้าที่จำเป็นต่อการคุ้มครองทรัพย์สินทางปัญญาของยุโรป

บทบัญญัติให้ความคุ้มครองข้อมูลของสหภาพยุโรป (The EU Copyright Directive)สหภาพยุโรปได้ตระหนักถึงปัญหาและอุปสรรคในการสร้างสังคมข้อมูลข่าวสาร (Information Society) ให้เป็นเอกภาพในหมู่ประเทศสมาชิก และได้แสวงหาทางออกมาอย่างต่อเนื่อง โดยหนึ่งในแนวทางนั้นได้แก่ การสร้างระบบกฎเกณฑ์ให้เป็นหนึ่งเดียว สร้างมาตรฐานการให้ความคุ้มครองฐานข้อมูลและฐานข้อมูลที่เข้มแข็งเท่าเทียมกันในประเทศสมาชิกสหภาพยุโรปทุกประเทศในด้านกำเนิดบทบัญญัติการให้ความคุ้มครองข้อมูล บทบัญญัติของสหภาพยุโรป (The EU Copyright Directive) เป็นการกำหนดมาตรฐานการให้ความคุ้มครอง “ข้อมูล” ที่บัญญัติขึ้นใช้ในประเทศสมาชิกด้วยวัตถุประสงค์ที่ต้องการสร้างตลาดภายใน (internal market) ของสหภาพยุโรปให้แข็งแรง มีการถ่ายทอดข้อมูลการค้า และการบริการระหว่างประเทศสมาชิกอย่างสะดวกไร้อุปสรรค มีการแข่งขันกันอย่างเสรี โดยใช้เทคโนโลยีสารสนเทศที่ทันสมัยสร้างสังคมข้อมูลข่าวสารอันมีประสิทธิภาพอย่างจริง จึงได้สร้างกรอบกำหนดของกฎหมาย (legal frame work) ลิขสิทธิ์ และกฎหมายอื่นๆ ที่เกี่ยวเนื่องกันให้เป็นมาตรฐานเดียวกัน

แรงผลักดันอีกประการหนึ่งของการสร้างบทบัญญัติลิขสิทธิ์ของสหภาพยุโรปขึ้นมาคือ ความเคลื่อนไหวขององค์การทรัพย์สินทางปัญญาโลก ที่ได้เสนอสนธิสัญญา 2 ฉบับต่อประเทศสมาชิก คือ สนธิสัญญาลิขสิทธิ์ (WIPO Copyright Treaty) และสนธิสัญญาเกี่ยวกับการแสดงและการบันทึกเสียง (WIPO Performances and Phonograms Treaty) ที่เป็นมาตรการปรับปรุงการคุ้มครองลิขสิทธิ์ และสิทธิข้างเคียงที่เกี่ยวเนื่องในระบบนานาชาติ โดยมีมาตรการจริงจังในการต่อต้านการใช้ข้อมูลอย่างผิดกฎหมาย (Piracy) ทั่วโลก โดยนำเอาเทคโนโลยีที่ทันสมัยเข้ามาช่วย ซึ่งได้รับการตอบรับเป็นอย่างดีจากประเทศสมาชิกองค์การทรัพย์สินทางปัญญาโลกทั่วโลก และประเทศสมาชิกสหภาพยุโรปหลายประเทศก็ได้ลงนามรับรอง สนธิสัญญาทั้งสองฉบับยังอยู่ในขั้นตอนรับสัตยาบัน เพื่อนำไปปฏิบัติในประเทศสมาชิกองค์การทรัพย์สินทางปัญญาโลก ดังนั้นหากสหภาพยุโรปบังคับใช้ (Copyright Directive) อย่างได้ผลก็จะเป็นการเสริมสร้างมาตรฐานในการคุ้มครองข้อมูลและฐานข้อมูล ในระดับนานาชาติได้อีกทางหนึ่ง

ขอบเขตความคุ้มครองข้อมูล บทบัญญัติลิขสิทธิ์ของสหภาพยุโรปให้ความคุ้มครองกับผู้สร้างสรรค์และงานสร้างสรรค์ 5 ประการคือ

1. ผู้สร้างสรรค์ผลงาน (Author of their works)
2. นักแสดงและผลงานการแสดง (Performers of fixation of their Performances)
3. ผู้ผลิตสื่อบันทึกเสียงและงานบันทึกเสียง (Phonograms Producer of their Phonograms)
4. ผลผลิตภาพยนตร์และภาพยนตร์ (The Producer of the first fixation of films)
5. องค์กรสื่อสารและกิจกรรมการสื่อสาร (Broadcasting Organization of fixation of their broadcasts)

อีกทั้งบทบัญญัติลิขสิทธิ์จะไม่มีผลต่อข้อบังคับที่มีอยู่แล้วอันเกี่ยวข้องกับสิทธิต่อไปนี้

1. กฎหมายคุ้มครองโปรแกรมคอมพิวเตอร์
2. สิทธิการเช่า ให้เช่า และสิทธิที่เกี่ยวเนื่องกับทรัพย์สินทางปัญญา
3. ลิขสิทธิ์และสิทธิข้างเคียงที่เกี่ยวกับองค์กรสื่อสารและกิจกรรมการสื่อสารผ่านเคเบิลและดาวเทียม
4. เงื่อนไขทางกฎหมายให้ความคุ้มครองแก่ลิขสิทธิ์และสิทธิข้างเคียง
5. กฎหมายคุ้มครองฐานข้อมูล

แต่เดิมนั้นในการกำหนดบทบัญญัติให้ความคุ้มครองฐานข้อมูลบางประเทศในสหภาพยุโรปอาทิเช่น สหราชอาณาจักร ไอร์แลนด์ เนเธอแลนด์ และกลุ่มประเทศสหภาพยุโรปมีมาตรการคุ้มครองฐานข้อมูลของตนเองเป็นอย่างดี แต่ในประเทศสมาชิกอื่นๆ นั้น มีการเอาใจใส่ในเรื่องนี้น้อยกว่ามาก ทำให้สหภาพยุโรปดำริที่จะยกระดับกฎหมายลิขสิทธิ์ของประเทศสมาชิกทั้งหมดให้เท่าเทียมกัน โดยเริ่มจากการศึกษาระบบการคุ้มครองฐานข้อมูลประเทศสมาชิก ในตอนปลายทศวรรษที่ 1980 และได้รับความร่วมมือจากประเทศเหล่านั้นอย่างแข็งขัน จนในที่สุดสภาแห่งสหภาพยุโรป (EU Council) ก็ได้ประเทศใช้ “The Directive on Legal Protection of Database” หรือบทบัญญัติการให้ความคุ้มครองฐานข้อมูลเมื่อเดือนมีนาคม 1996

ในด้านขอบเขตความคุ้มครองฐานข้อมูล (Directive on Legal Protection of Database)บทบัญญัติจะครอบคลุมฐานข้อมูลตามกฎหมายในทุกรูปแบบ ฐานข้อมูลในที่นี้หมายถึง การรวบรวมงานที่แยกกันอยู่เป็นชิ้นๆ (independent work) หรือข้อมูลอื่นๆ ให้เป็นระบบระเบียบและสามารถเข้าถึงได้เป็นรายบุคคลผ่านสื่ออิเล็กทรอนิกส์ หรือสื่อใดๆ ก็ตามซึ่งข้อมูลนับรวมถึง วรรณกรรม ศิลปกรรม ดนตรีกรรม หรืองานในแขนงอื่นๆ รวมทั้งตัวอักษร เสียง ภาพ ตัวเลข ข้อเท็จจริง และสถิติ โดยการรวบรวมนั้น จะต้องแสดงให้เห็นถึงการอุทิศแรงงานและทรัพยากรอย่างมาก เช่น ซีดีรอม (CD-ROM) ซีดีไอ (CD-I) ภายใต้ Sui generic rights

ทั้งนี้การเก็บรวบรวมข้อมูลอาจกระทำในลักษณะของสื่ออิเล็กทรอนิกส์ (Electronic Database) ไม่จำเป็นจะต้องเป็นตัวตนหรือจับต้องได้เสมอไป แต่ทว่าไม่รวมถึงโปรแกรมคอมพิวเตอร์ที่ใช้ในการผลิตฐานข้อมูลหรือการทำงาน (Operation) ของอุปกรณ์ที่เป็นสื่อให้เข้าถึงฐานข้อมูลนั้นๆ

ฐานข้อมูลที่ได้สร้างขึ้นมาจากสติปัญญาและสมองของผู้สร้างเท่านั้นที่จะได้รับการคุ้มครองตามกฎหมายลิขสิทธิ์ ไม่เกี่ยวข้องกับสุนทรียภาพหรือปริมาณของงานใดๆ ทั้งสิ้น โดยคุ้มครองรวมไปถึงโครงสร้างของฐานข้อมูลด้วย อย่างไรก็ดีไม่รวมถึงเนื้อหา (contents) และไม่เกี่ยวข้องกับสิทธิใดๆ ที่ครอบคลุมเนื้อหาของฐานข้อมูลนั้นๆ อยู่แล้ว ฐานข้อมูลใดที่ได้รับการคุ้มครองจากมาตรการทางกฎหมายอื่นๆ เช่น กฎหมายลิขสิทธิ์ ก็ยังได้รับความคุ้มครองอยู่เช่นเดิม รวมถึงสิทธิอันชอบธรรมอื่นๆ ที่มีอยู่ภายใต้กฎหมายของประเทศสมาชิกแต่ละประเทศและภายใต้อนุสัญญากรุงเบอร์น (Bern Convention for the protection of the Literary and Artistic Works)

7) ประเทศฝรั่งเศส

1. การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

การแลกเปลี่ยนข้อมูลในฝรั่งเศสนั้นเริ่มขึ้นจากปรากฏการณ์ 2 ส่วน คือ ประการแรก การกระตุ้นให้มีการแลกเปลี่ยนข้อมูลระหว่าง ตำรวจสากล (Interpol) กับหน่วยงานด้านตำรวจตรวจคนเข้าเมือง และกระบวนการยุติธรรม กับ ประการที่สอง การกระตุ้นให้มีการแลกเปลี่ยนข้อมูลในวงการธุรกิจ โดยมีการจำแนกข้อมูลเป็น Negative data และ Positive data (โดย negative data เช่น ประวัติการกระทำผิด การไม่จ่าย หรือชำระหนี้ ภาวะล้มละลาย เป็นต้น) ส่วนข้อมูลในทางที่ดี คือ ข้อมูลเกี่ยวกับการกู้ยืมเงินและการชำระ ต่อมามีการแลกเปลี่ยนข้อมูลที่มีบทบาท คือ การแลกเปลี่ยนข้อมูลด้านการก่อการร้ายที่เกิดขึ้นระหว่างประเทศกลุ่ม EU ผลจากการดำเนินการดังกล่าวทำให้ฝรั่งเศสได้กระตุ้นให้หน่วยงานต่างๆที่ดำเนินงานร่วมกัน แลกเปลี่ยนข้อมูลการปฏิบัติงาน เช่น ด้าน DNA Data Sharing หรือ ด้านศุลกากร เป็นต้น

2.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

ฝรั่งเศสออกกฎหมายที่เกี่ยวข้องกับการเชื่อมโยง และแลกเปลี่ยนข้อมูล คือ The Data Processing, Data Files and Individual Liberties 1978 ต่อมามีการปรับปรุงแก้ไขในปี 2004 กฎหมายฉบับนี้จะเป็นกฎหมายหลักที่ใช้ในการประมวลข้อมูล โดยมีการจำแนกประเภทข้อมูล การเข้าถึง การควบคุมข้อมูล และสิทธิส่วนบุคคล ข้อมูลทางการแพทย์ เป็นต้น

นอกจากนี้ในส่วนกฎหมายอื่นๆที่ฝรั่งเศสนำมาปรับใช้คือ กฎหมายอาญา (Penal Code) ที่มีการปรับปรุงแก้ไข เมื่อวันที่ 8 พฤษภาคม 2007 ให้ข้อมูลต่างๆได้รับการคุ้มครองจากบทบัญญัติของกฎหมายอาญา

3.กฎหมายการคุ้มครองข้อมูลข่าวสาร

ฝรั่งเศสได้ออกรัฐบัญญัติลงวันที่ 6 มกราคม ค.ศ. 1987 ว่าด้วยการเก็บรักษาข้อมูลข่าวสารโดยเครื่องคอมพิวเตอร์และเสรีภาพ ได้กำหนดให้มี “คณะกรรมการควบคุมการใช้คอมพิวเตอร์ในระบบข่าวสารและเสรีภาพของประชาชนแห่งประเทศฝรั่งเศส” โดยเป็นหน่วยงานปกครองอิสระมีอำนาจที่จะทำคำสั่งหรือนิติกรรมทางปกครองและออกกฎหมายลำดับ

รองได้ แต่ไม่มีอำนาจตุลาการ ประกอบด้วยสมาชิก 17 คน ซึ่งแต่งตั้งขึ้นมีกำหนด 5 ปี หรือตามระยะเวลาของตำแหน่งหน้าที่ที่ได้รับการแต่งตั้ง สมาชิกประกอบด้วย

1) สมาชิกสภาผู้แทนราษฎร 2 คน และสมาชิกวุฒิสภา 2 คน

2) สมาชิกสภาเศรษฐกิจและสังคม 2 คน

3) สมาชิกหรือผู้ที่เคยเป็นสมาชิกของสภาที่ปรึกษาแห่งรัฐ 2 คน ซึ่งหนึ่งในสองนี้จะต้องมีฐานะเทียบเท่าผู้พิพากษาของสภาที่ปรึกษาแห่งรัฐ

4) สมาชิกหรือผู้ที่เคยเป็นสมาชิกของศาลฎีกา 2 คน ซึ่งหนึ่งในสองนี้จะต้องมีฐานะเทียบเท่าผู้พิพากษาในศาลฎีกา

5) สมาชิกหรือผู้ที่เคยเป็นสมาชิกของศาลบัญชี (Cour des Comptes) 2 คน ซึ่งหนึ่งในสองนี้จะต้องมีฐานะเทียบเท่าผู้พิพากษาของศาลบัญชี

6) สมาชิก 2 คน ซึ่งมีคุณสมบัติเหมาะสมเพราะความรู้ความสามารถในการใช้คอมพิวเตอร์ และได้รับการแต่งตั้งโดยรัฐกฤษฎีกาตามคำแนะนำของสภาผู้แทนราษฎรและประธานวุฒิสภา

7) สมาชิก 3 คน ซึ่งแต่งตั้งโดยความรู้ความษมารถและความเชี่ยวชาญโดยรัฐกฤษฎีกาในคณะรัฐมนตรี

คณะกรรมการชุดนี้จะเลือกประธาน 1 คน และรองประธาน 2 คน จากบรรดาสมาชิกทั้งหลาย ประธานและรองประธานจะอยู่ในตำแหน่ง 5 ปี หากประธานหรือสมาชิกคนใดพ้นตำแหน่งไป บุคคลที่ได้รับการแต่งตั้งเข้ามาแทนจะดำรงตำแหน่งในวาระเท่ากับบุคคลที่พ้นตำแหน่งโดยมีหน้าที่ความรับผิดชอบ

1) อำนาจในการได้มาซึ่งข้อมูลและแจ้งข้อมูลให้ประชาชนทราบ หลักการของอาจก็คือต้องการให้ประชาชนเห็นความสำคัญของปัญหา เห็นอันตรายและเริ่มป้องกันสิทธิของตนเอง เพราะจะทำให้ประชาชนใช้สิทธิในการเข้าถึงข้อมูลข่าวสารของตนเองตามกฎหมายได้และทำให้อำนาจในกาควบคุมของคณะกรรมการเป็นไปอย่างมีประสิทธิภาพ อำนาจนี้แยกได้เป็น 3 หัวข้อย่อยดังนี้

(1) อำนาจได้มาซึ่งข้อมูลข่าวสารโดยได้รับแจ้งจากผู้เก็บข้อมูลข่าวสาร

(2) มีสิทธิได้รับคำร้องเรียน คำร้องทุกข์จากบุคคลผู้เก็บข้อมูลข่าวสารเพื่อทราบว่าข้อมูลที่ได้มาจากการแจ้งของผู้เก็บข้อมูลข่าวสารเป็นจริงหรือครบถ้วนตามความเป็นจริงเท่าใด

(3) มีอำนาจเข้าไปหาข้อมูลข่าวสารด้วยตนเอง สามารถทราบพัฒนาการของเทคนิคใหม่ๆ ที่เกิดขึ้นในวงการคอมพิวเตอร์ นอกจากที่ได้ทราบสถานการณ์ต่างๆ ที่เกิดขึ้นในวงกาคอมพิวเตอร์แล้ว ยังมีอำนาจที่จะหาข้อมูลเกี่ยวกับกิจกรรมทางอุตสาหกรรมและการให้บริการที่เกี่ยวกับการใช้คอมพิวเตอร์ได้ มีอำนาจรับฟังพยานหลักฐานเรียกบุคคลมาให้ถ้อยคำ เพื่อจะทำให้คณะกรรมการสามารถติดตามพัฒนาการใหม่ๆ ทางเทคนิคของคอมพิวเตอร์ได้โดยตลอด เพื่อที่จะได้ใช้อำนาจควบคุมได้ทันต่อความก้าวหน้าทางเทคโนโลยี

2) การเก็บข้อมูลข่าวสารประเภทระบุชื่อที่ไม่ได้กระทำเพื่อหน่วยงานของรัฐหรือเพื่อนิติบุคคลในกฎหมายเอกชนที่ดำเนินงานในการบริการสาธารณะ หมายถึง การเก็บข้อมูลของเอกชนเพื่อเอกชนเอง

รัฐบัญญัติฉบับนี้ไม่ได้กำหนดเรื่องอำนาจไว้ แต่กำหนดเพียงกระบวนการในการแจ้งให้คณะกรรมการทราบ อย่างไรก็ตามได้มีการควบคุมอำนาจในการใช้เครื่องคอมพิวเตอร์กับข้อมูลข่าวสารในเรื่องส่งข้อมูลข้ามประเทศ โดยกำหนดให้มีการอนุญาตหากจะมีการส่งข้อมูลข่าวสารประเภทระบุชื่อออกนอกประเทศ

ข้อยกเว้น หลักดังกล่าวไม่ใช้กับการส่งข่าวสารของหนังสือพิมพ์ข้ามประเทศ ไม่ว่าจะเป็นหนังสือพิมพ์ที่เป็นลายลักษณ์อักษรหรือทางวิทยุ โทรทัศน์

การแจ้งและการปรึกษาคณะกรรมการ

1) การปรึกษาคณะกรรมการ ในกรณีของรัฐหรือหน่วยงานของรัฐนั้น รัฐบัญญัติมิได้กำหนดไว้เพียงเรื่องอำนาจในการริเริ่มใช้คอมพิวเตอร์กับการเก็บข้อมูลข่าวสารประเภทระบุชื่อของรัฐหรือหน่วยงานเท่านั้น แต่ได้กำหนดกระบวนการในการปรึกษากับคณะกรรมการด้วย เมื่อมีคำปรึกษาคณะกรรมการจะต้องให้ความเห็นพร้อมเหตุผลก่อนที่จะมีการตรารัฐกฤษฎีกาให้อำนาจในการเริ่มใช้คอมพิวเตอร์ในการเก็บข้อมูลของรัฐหรือเพื่อรัฐ และคณะกรรมการจะต้องให้ความเห็นดังกล่าวภายในระยะเวลาสองเดือนนับแต่ได้รับการปรึกษา มิฉะนั้นกฎหมายให้ถือว่าให้ความเห็นชอบ ทั้งนี้ระยะเวลาดังกล่าอาจขยายไปได้อีกหนึ่งครั้ง ไม่เกินสองเดือน โดยคำสั่งของประธานคณะกรรมการ ถ้าคณะกรรมการไม่เห็นสมควรให้ใช้คอมพิวเตอร์กับการเก็บข้อมูลของรัฐหรือหน่วยงานของรัฐ การที่จะใช้คอมพิวเตอร์กับข้อมูลข่าวสารดังกล่าวต้องทำเป็นรัฐกฤษฎีกาที่ผ่านความเห็นชอบของสภาที่ปรึกษาแห่งรัฐ และถ้าการเก็บข้อมูลข่าวสารดังกล่าวเป็นองค์กรปกครองท้องถิ่น ถ้าคณะกรรมการไม่เห็นด้วย แต่

องค์กรนั้นๆ ยังประสงค์ให้จัดเก็บข้อมูลดังกล่าวด้วยคอมพิวเตอร์จะต้องให้สภาท้องถิ่นเห็นชอบและมีรัฐกฤษฎีกาที่ผ่านความเห็นชอบของสภาที่ปรึกษาแห่งรัฐ โดยอนุมัติตามความเห็นชอบของสภาท้องถิ่นด้วย

2) การแจ้งให้คณะกรรมการทราบก่อนที่จะมีการใช้คอมพิวเตอร์กับข้อมูลข่าวสาร การแจ้งให้ทราบนี้แยกเป็น 2 วิธีด้วยกัน วิธีแรกใช้เฉพาะภาคเอกชนเท่านั้น ส่วนวิธีการหลังใช้ทั้งกับภาครัฐและภาคเอกชน

(1) การแจ้งตามแบบธรรมดา ในกรณีที่เอกชนต้องการใช้คอมพิวเตอร์กับข้อมูลข่าวสารประเภทระบุชื่อต้องแจ้งให้คณะกรรมการทราบก่อนที่จะลงมือใช้คอมพิวเตอร์ในการเก็บข้อมูลข่าวสารนั้น ในใบแจ้งประเภทนี้จะต้องประกอบด้วยคำรับรองว่าจะปฏิบัติตามข้อกำหนดในกฎหมายทุกประการ เมื่อมีการแจ้งคณะกรรมการจะตรวจสอบว่าได้มีการปฏิบัติตามกฎหมายครบถ้วนหรือไม่ หากเงื่อนไขครบถ้วนตามกฎหมาย คณะกรรมกาจะต้องออกไปรับให้ผู้แจ้ง

(2) การแจ้งอย่างง่าย หากเป็นการใช้คอมพิวเตอร์กับข้อมูลข่าวสารประเภทที่เกี่ยวกับงานทั่วไป ไม่ว่าจะเป็นภาครัฐหรือเอกชน กำหนดให้หน่วยงานทั้งของรัฐและเอกชนที่ประสงค์จะเก็บข้อมูลข่าวสารประเภทนี้ด้วยคอมพิวเตอร์ แจ้งให้คณะกรรมการทราบตามวิธีการอย่างง่ายและรวบรัด และเมื่อไดรับใบรับจากคณะกรรมการผู้แจ้งก็สามารถใช้คอมพิวเตอร์กับข้อมูลข่าวสารได้

การบังคับและบทลงโทษ

ในภาครัฐนั้น บุคคลที่มีอำนาจในการตัดสินใจให้มีการใช้คอมพิวเตอร์กับข้อมูลข่าวสารนั้น แยกเป็น 2 ส่วน คือ

1) ระดับรัฐบาล รัฐมนตรีของแต่ละกระทรวงเป็นผู้มีอำนาจตัดสินว่าการเก็บข้อมูลจำเป็นสำหรับการดำเนินงานของหน่วยงานภายใต้อำนาจของตนอันเป็นเรื่องภายใน เช่น การเก็บข้อมูลเกี่ยวกับบุคลากรของกระทรวง

2) ระดับองค์กรปกครองส่วนท้องถิ่นหรือส่วนราชการที่เป็นนิติบุคคลอื่น หัวหน้าหน่วยงานนั้นอาจทำข้อบังคับให้เก็บข้อมูลข่าวสารที่เป็นการภายในของหน่วยงานนั้น

ข้อบังคับมีผลเป็นการทั่วไป ซึ่งกำหนดการใช้คอมพิวเตอร์กับข้อมูลข่าวสารจะต้องระบุถึงสิ่งต่อไปนี้

1) ชื่อเรียกของการเก็บข้อมูลและวัตถุประสงค์ของการใช้คอมพิวเตอร์กับข้อมูลนั้น

2) หน่วยงานที่บุคคลอาจจะใช้สิทธิในการเข้าถึงข้อมูลที่เก็บไว้ได้

ประเภทของข้อมูลที่บันทึกไว้พร้อมผู้ใช้ข้อมูลนี้หรือประเภทของผู้ที่จะใช้ข้อมูลซึ่งมีอำนาจที่จะได้รับการแจ้งข้อดังกล่าว

รัฐกฤษฎีกาในสภาที่ปรึกษาแห่งรัฐอาจจะบัญญัติให้ข้อบังคับที่มีลักษณะทั่วไปอันเป็นการจัดตั้งให้มีการใช้คอมพิวเตอร์กับข้อมูลข่าวสารดังกล่าวนั้น โดยเฉพาะในส่วนที่เกี่ยวกับความมั่นคงของรัฐ การป้องกันปะเทศและความปลอดภัยสาธารณะไม่ต้องประกาศก็ได้

ในภาคเอกชนเนื้อหาที่เอกชนจะต้องระบุในการแจ้งให้คณะกรรมการทราบ คือ

1) บุคคลที่ทำคำขอและบุคคลที่มีอำนาจในการตัดสินใจให้มีการเก็บข้อมูลหรือในกรณีที่บุคคลดังกล่าวอยู่ในต่างประเทศจะต้องระบุผู้แทนในประเทศฝรั่งเศส

2) ลักษณะพิเศษตลอดจนวัตถุประสงค์และต้องระบุชื่อการเก็บข้อมูลข่าวสาร

3) หน่วยงานที่มีหน้าที่ในการเก็บข้อมูล

4) หน่วยงานที่บุคคลอาจใช้สิทธิเข้าสู่ข้อมูลข่าวสารได้ และมาตรการที่หน่วยงานจะช่วยให้การเข้าถึงข้อมูลข่าวสารเป็นไปได้โดยสะดวก

5) ประเภทของบุคคลที่อาจเข้าถึงข้อมูลข่าวสารโดยตรง

6) การเชื่อมโยงข้อมูลที่เก็บบันทึกไว้ตลอดจนสิ่งอื่นที่มีลักษณะเป็นการนำข้อมูลไปเทียบเคียงหรือไปเชื่อมโยงกับข้อมูลที่ผู้อื่น และจะมีการให้ข้อมูลดังกล่าวกับบุคคลที่สามหรือไม่

7) กฎเกณฑ์ที่วางไว้สำหรับความปลอดภัยในการเก็บข้อมูลข่าวสารดังกล่าว และกาประกันความลับของบุคคลที่กฎหมายรับรอง

8) หากข้อมูลข่าวสารประเภทระบุชื่อดังกล่าวจะมีการแลกเปลี่ยนหรือส่งข้ามประเทศฝรั่งเศสหรือนอกประเทศฝรั่งเศสบางส่วน โดยเฉพาะในส่วนที่เก็บไว้นอกประเทศฝรั่งเศสก่อนที่จะมีการเข้ามาขออนุญาตใช้คอมพิวเตอร์กับข้อมูลข่าวสารดังกล่าวในประเทศฝรั่งเศส

การแก้ไขเปลี่ยนแปลงรายละเอียดเนื้อหาที่ระบุไว้หรือการยกเลิกการใช้คอมพิวเตอร์กับข้อมูลข่าวสารจะต้องแจ้งให้คณะกรรมการทราบ ในส่วนของรัฐ ถ้าหากเป็นคำขอความเห็นของคณะกรรมการที่กระทบถึงความมั่นคงแห่งรัฐการทหารหรือความปลอดภัยสาธารณะอาจไม่ต้องระบุไว้ในคำขอความเห็น

รัฐบัญญัติฉบับนี้ได้กำหนดสภาพบังคับทางอาญาไว้ ในกรณีที่ฝ่าฝืนไม่ปฏิบัติตามหลักเกณฑ์เกี่ยวกับอำนาจและกระบวนการที่กล่าวมาข้างต้น กรณีเป็นการลงโทษบุคคลไม่

ปฏิบัติตามกระบวนการที่กำหนดไว้ก่อนการลงเก็บข้อมูลข่าวสารด้วยคอมพิวเตอร์ กล่าวคือ การไม่แจ้งหือขอความเห็นตามที่กำหนดไว้จะต้องรับโทษจำคุกตั้งแต่ 6 เดือนถึง 3 ปี หรือปรับตั้งแต่ 2,000 – 200,000 ฟรังค์

กรณีเป็นความผิดที่เรียกว่า การบิดเบือน การใช้ข้อมูลโดยไม่ชอบ กล่าวคือ บุคคลใดก็ตามที่เป็นผู้เก็บข้อมูลบิดเบือนการใช้ข้อมูลให้ผิดไปจากที่ระบุไว้ในวัตถุประสงค์ การใช้ข้อมูลท่แจ้งไว้แต่ต้น จะต้องับโทษจำคุก 1 ปีถึง 5 ปี และปรับตั้งแต่ 20,000 – 200,000 ฟรังค์

การแจ้งการเก็บข้อมูลข่าวสาร

1) ข้อมูลข่าวสารจะต้องได้รับการเก็บรักษาโดยบุคคลที่เกี่ยวข้องโดยตรง นั่นคือ บุคคลจะใช้ข้อมูลประเภทใดภายหลังจากที่มีการแจ้งหรือทำคำขอความเห็นแล้วบุคคลนั้นจะต้องเก็บรักษาข้อมูลข่าวสารนั้นเอง จะให้บุคคลที่สามเก็บไม่ได้ เว้นแต่จะมีกฎหมายกำหนดไว้เป็นอย่างอื่น

นอกจากนี้ได้กำหนดหน้าที่ของบุคคลผู้ที่สั่งให้มีการเก็บข้อมูลประเภทระบุชื่อ ไม่ว่าจะเป็นการเก็บด้วยเครื่องคอมพิวเตอร์หรือมือก็ตามจะต้องรับรองต่อบุคคลที่เกี่ยวข้องกับข้อมูลข่าวสารนั้นว่าจะดำเนินการเท่าที่จำเป็นเพื่อป้องกันความปลอดภัยในส่วนที่เกี่ยวกับข้อมูล และต้องรับรองว่าข้อมูลนั้นจะไม่ถูกดัดแปลง ทำให้เสียหายหรือส่งไปให้บุคคลที่สามซึ่งไม่มีอำนาจ

การกำหนดให้คณะกรรมการให้ข้อมูลข่าวสารเกี่ยวกับการเก็บข้อมูลข่าวสารโดยเครื่องคอมพิวเตอร์แก่ประชาชน รัฐบัญญัติฉบับนี้กำหนดมาตรการต่างๆ เพื่อให้คณะกรรมการได้ข้อมูลข่าวสารที่เกี่ยวกับการเก็บข้อมูลข่าวสารโดยคอมพิวเตอร์ ไม่ว่าจะเป็นการกำหนดให้มีการแจ้งแก่คณะกรรมการก่อนที่จะมีการเก็บข้อมูลข่าวสารประเภทระบุชื่อ การให้อำนาจแก่คณะกรรมการในการรับคำร้องเรียน คำร้องทุกข์ การให้อำนาจแก่คณะกรรมการในการหาข้อมูลด้วยตนเอง เมื่อคณะกรรมการได้ข้อมูลในเรื่องดังกล่าวแล้ว รัฐบัญญัติได้กำหนดให้คณะกรรมการจะต้องให้บัญชีรายชื่อระบบการจัดเก็บข้อมูลข่าวสารนั้นๆ แก่ประชาชน การใช้บัญชีรายชื่อดังกล่าวรัฐบัญญัติไม่ได้กำหนดบังคับให้ลงในประกาศของราชการ ดังนั้นคณะกรรมการอาจลงตีพิมพ์เผยแพร่ในรูปแบบต่างๆ อันมีผลให้ประชาชนทราบรายละเอียดต่างๆ ได้อย่างเพียงพอโดยระบุ

(1) ชื่อของระบบข้อมูลนั้นและวัตถุประสงค์สุดท้ายในการใช้ข้อมูลนั้น

(2) หน่วยงานที่เอกชนมีสิทธิหรือใช้สิทธิเข้าถึงตามที่ระบุไว้

(3) ระบุประเภทของข้อมูลประเภทระบุชื่อที่บันทึกไว้ ตลอดจนผู้มีสิทธิใช้ และประเภทของผู้ที่มีสิทธิที่จะใช้ข้อมูลเหล่านี้

2) กำหนดให้สิทธิแก่ประชาชนในการสอบถามหน่วยงานที่เก็บข้อมูลข่าวสารโดยคอมพิวเตอร์ว่าตนถูกเก็บข้อมูลข่าวสารไว้โดยระบุชื่อหรอไม่

เมื่อประชาชนคนหนึ่งๆ ได้ทราบว่าหน่วยงานใดได้จัดเก็บข้อมูลข่าวสารประเภทใดไว้ด้วยคอมพิวเตอร์แล้ว รัฐบัญญัติฉบับนี้ได้ให้สิทธิแก่ประชาชนในการสอบถามกับหน่วยงานนั้นๆ ว่าตนถูกเก็บข้อมูลข่าวสารไว้โดยระบุชื่อหรือไม่

3) กำหนดให้แจ้งรายละเอียดบางประการแก่บุคคลผู้ซึ่งถูกเก็บข้อมูลข่าวสาร

นอกจากมาตรการในการที่รับรองคุ้มครองสิทธิดังกล่าวของประชาชนแล้ว รัฐบัญญัติได้กำหนดให้แจ้งรายละเอียดบางประการแก่บุคคลผู้ถูกเก็บข้อมูลข่าวสารในเวลาที่ขอเก็บข้อมูลเกี่ยวกับบุคคลนั้น ดังมีรายละเอียดต่อไปนี้

(1)จะต้องได้ทราบว่าข้อมูลที่ตนให้นั้นมีลักษณะเป็นการบังคับที่จะให้ตอบหรือไม่

(2)ผลอันเกิดจากการไม่ตอบ

(3)บุคคลซึ่งจะใช้ข้อมูลข่าวสารนั้นเป็นบุคคลธรรมดาหรือนิติบุคคล

(4)บอกให้ทราบว่ามีสิทธิในการแก้ไขและเข้าถึงข้อมูลข่าวสารนั้นหรือไม่ อย่างไร หากเป็นกรณีแบบสอบถาม จะต้องระบุหลักเกณฑ์ดังกล่าวไว้ในแบบสอบถามนั้น

บทบัญญัตินี้ไม่ใช้กับการเก็บข้อมูลข่าวสารที่จำเป็นสำหรับการสืบหาผู้กระทำความผิด

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

กฎหมายลิขสิทธิ์ของฝรั่งเศส พัฒนามาพร้อมกับกฎหมายลิขสิทธิ์ของอังกฤษ โดยยึดเอาสิทธิของผู้สร้างสรรค์งาน และยอมรับธรรมสิทธิ์ (moral rights) ในผลงาน อย่างไรก็ตาม ฝรั่งเศสก็ยังมีการปรับปรุง กฎหมายลิขสิทธิ์ให้สอดคล้องกับบทบัญญัติของ EU และถือว่า การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อนำไปใช้ ไม่ใช่การละเมิด

กฎหมายลิขสิทธิ์[67]แม้ว่าจะเป็นที่ยอมรับกันว่า ฝรั่งเศสนั้นมีกฎหมายลิขสิทธิ์ที่ครอบคลุมผลงานที่เกิดจากความคิดและการแสดงออกทางความคิดที่เรียกว่า the work of mind[68] มีขอบข่ายการคุ้มครองที่กว้างมากโดยเฉพาะที่เป็นผลงานทางด้านดิจิดอล และทางสื่อต่างๆ เมื่อวันที่ 8 ธันวาคม 2005 Tribunal de grande instance de Paris ได้สรุปว่าการแลกเปลี่ยนข้อมูลผ่านทางระบบแฟ้มข้อมูลระหว่างองค์กรไม่ใช่การกระทาผิดด้านอาชญากรรมเกี่ยวกับทรัพย์สินทางปัญญา ดังนั้น ผลงานการรวบรวมข้อมูลและการแลกเปลี่ยนข้อมูลทางด้านงานยุติธรรมเช่นกันในลักษณะที่เป็นฐานข้อมูลจะได้รับการคุ้มครองทางด้านทรัพย์สินทางปัญญา

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ในฝรั่งเศสนั้นอาจกล่าวได้ว่าไม่มีกฎหมายที่ปรับใช้ได้ทุกประเภทของการประกอบอาชญากรรม นอกจากนี้กฎหมายเฉพาะทางของการสื่อสารโทรคมนาคมก็ไม่มีการออกระเบียบใดๆมาโดยเฉพาะ แต่ฝรั่งเศสจะมีการปรับใช้กฎหมายอาญา[69] โดยเฉพาะการเข้าถึงการใช้คอมพิวเตอร์โดยไม่มีอำนาจ ได้แก่ มาตรา 323-(1)-(4)(7)ส่วนการละเมิดสิทธิส่วนบุคคลอันเป็นผลมาจากการใช้การใช้กรรมวิธีทางด้านคอมพิวเตอร์หรือการเข้าถึงแฟ้มข้อมูลผู้อื่นโดยไม่มีอำนาจก็มีความผิดตาม มาตรา 226(16)-(17)

8) ประเทศญี่ปุ่น

1.การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

เดิมญี่ปุ่นมีการพัฒนาทางด้านเทคโนโลยีสารสนเทศช้ามาก จนกระทั่งหลังการฟื้นฟูประเทสสมัยเมจิ จึงได้มีการพัฒนาเศรษฐกิจขนานใหญ่และก่อให้เกิดความเจริญทางเศรษฐกิจอย่างรวดเร็วและผลพวงดังกล่าวก่อให้เกิดการพัฒนาทางด้านเทคโนโลยีสารสนเทศเพื่อรองรับความเติบโตดังกล่าวด้วย โดยเฉพาะตั้งแต่ปี1985 เป็นต้นมาเมื่อการตลาดทางด้านการโทรคมนาคมของญี่ปุ่นขยายตัวรวดเร็วมาก ทำให้การติดต่อสื่อสารและการแลกเปลี่ยนข้อมูลทางอิเลกโทรนิกส์เกิดการขยายตัวทุกองค์กร

---

67 *Code de la propriété intellectuelle*,

68 MISE A JOUR LEGIFRANCE 15/09/03 *Dernier texte modificateur Loi 2003-706 du 01/08/03* (JO 02/08/03)

69 MOHAMED CHAWKI Cybercrime in France: An Overview Computer Crime Research Center December 07, 2005

ตั้งแต่วันที่ 22 มกราคม 2001 เป็นต้นมาญี่ปุ่นได้ออกนโยบาย e-Japan Strategy โดยเป็นนโยบายเชิงยุทธศาสตร์ชาติ [70]เพื่อให้ญี่ปุ่นเป็นประเทศที่ก้าวไปอยู่แนวหน้าทางด้านเทคโนโลยีสารสนเทศในกลุ่มประเทศที่พัฒนาแล้ว โดยการดำเนินการที่สำคัญมีดังต่อไปนี้

1.การตั้ง Ultra-hispeed network infrastructure and promotion of competition โดยการดำเนินการดังกล่าวนั้นมีความมุ่งหมายที่จะสร้างระบบโครงสร้างพื้นฐานที่สามารถให้ใช้งานได้กว้างขวางและมีระบบการป้องกันที่ดีและการสนับสนุนการดำเนินการด้าน Intelligent transport system(ITS)และระบบเทคโนโลยีสารสนเทศทางภูมิศาสตร์(GIS)

2.การสนับสนุนทางการค้าและอิเลกโทรนิกส์และการตั้ง EC Rule ทั้งนี้เนื่องมาจากตลาดทางการค้าในปัจจุบันนั้มีการขยายตัวอย่างรวดเร็วและไร้พรมแดนและในขระเดียวกันก็มีการปรับปรุงกฎหมายให้สอดคล้องกับการพัฒนาด้วย

3. การสร้างความตระหนักในการดำเนินการด้าน e-Government การดำเนินการดังกล่าวมุ่งหมายที่จะพัฒนาทางด้านการDigitalization of Administrationทั้งในการประสานการดำเนินการของรัฐทั้งในส่วนกลางและส่วนภูมิภาค

4.การพัฒนาทรัพยากรมนุษย์ด้านเทคโนโลยีสารสนเทศ การดำเนินการดังกล่าวนี้ไม่เพียงแต่เป็นการมุ่งการฝึกอบรมแก่บุคลากรเท่านั้น แต่ยังเป็นการพัฒนาเอกสารและตำราต่างๆด้วย เนื่องจากเห็นว่า แม้บุคคลากรจะมีความพร้อมแต่หากขาดเอกสารที่เกี่ยวข้องและเป็นประโยชน์ที่จะใช้ช่วยในการศึกษาด้วยตนเองแล้วการพัฒนาในด้านนี้จะไปช้า

2.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

กฎหมายที่เกี่ยวข้องกับการแลกเปลี่ยน เชื่อมโยงและบูรณาการข้อมูลในกระบวนการยุติธรรมของญี่ปุ่นมีหลายฉบับ ซึ่งแต่ละฉบับมีบทบัญญัติที่เกี่ยวข้องแตกต่างกันออกไปดังต่อไปนี้

---

[70] www.kantei.go.jp

1. The Act for Protection of Computer Processed Personal Date กฎหมายฉบับนี้เริ่มมีผลใช้บังคับตั้งแต่ วันที่ 1 ตุลาคม 1989 โดยมีวัตถุประสงค์ในการปกป้องผลประโยชน์และสิทธิของบุคคล จากการเก็บรวบรวมข้อมูลส่วนบุคคลโดยประมวลผลผ่านระบบคอมพิวเตอร์จากฝ่ายบริหาร โดยกำหนดให้มีการตรวจสอบความถูกต้อง รักษาความปลอดภัยของข้อมูล การเปิดเผยข้อมูล และการส่งมอบหรือเชื่อมต่อข้อมูลส่วนบุคคลระหว่างองค์กรของรัฐ

2. Law Concerning Electronic Signatures and Certification Serviecs กฎหมายฉบับนี้ประกาศใช้ เมื่อ 1 เมษายน 2001 โดยมีเป้าหมายส่งเสริมการใช้ข้อมูลทางอิเลกโทรนิกส์ โดยที่มีการใช้ลายมือชื่อทางอิเลกโทรนิกส์ มีการให้นิยามความหมายของลายเซ็นอิเล็กโทรนิกส์ การให้การรับรองทั้งในประเทศและต่างประเทศ การตรวจสอบและรับรอง โดยมีคณะกรรมการ The National Public Safety Commission เป็นผู้ดูแลและออกมาตรการต่าง ๆที่จำเป็น เพื่อให้การรับรองเอกสารเพื่อใช้ในทางการค้า การดำเนินคดี สัญญา รวมไปถึงการรับรองเอกสารที่จะมีการเชื่อมโยงและส่งต่อ

3. Basic Law on the Formation of an Advanced Information and Telecommunications Network Society กฎหมายฉบับนี้ มีเป้าหมายในการสร้างและส่งเสริมมาตราการต่าง ๆในการสร้างความก้าวหน้าทางเทคโนโลยีสารสนเทศ โทรคมนาคม และการสร้างเครือข่าย โดยที่สำคัญคือ ใน Article 7 ได้มีการกำหนดถึงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานรัฐกับรัฐบาลท้องถิ่น และหน่วยงานรัฐกับเอกชน รวมทั้งใน Article 10 ได้กำหนดมาตรการความรับผิดของหน่วยงานต่อการเก็บรวบรวมและแลกเปลี่ยนข้อมูลโดยทางอิเลกโทรนิกส์

ในรอบ 5 ปีที่ผ่านมา ตั้งแต่ปี 2000 จนถึง 2005 ญี่ปุ่นได้ออกกฎหมายที่เกี่ยวข้องกับ e-Government มาดังนี้

1. ปี 2000-2001 ได้แก่ IT Basic Law (2001) และ Electronic Signatures Law (2001)

2. ปี 2002-2003 ได้แก่ e-Voting law (2002) Personal Information Protection law (2003) Online Administrative Procedure Law (2003) และ Public Personal Authentication Services Law 2003.

3. ปี 2004-2005 มี e-Document Law (2005).

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล (The Privacy Protection Act)

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่น คือThe Privacy Protection Act การคุ้มครองสารสนเทศส่วนบุคคลที่ประมวลผลด้วยคอมพิวเตอร์ในหน่วยงานของรัฐบาลกลางของประเทศญี่ปุ่น มีวัตถุประสงค์เพื่อการคุ้มครองสิทธิของแต่ละบุคคล และเพื่อสนับสนุนส่งเสริมบทบาทของหน่วยงานให้มีความเข้าใจหลักการพื้นฐานในการประมวลผลสารสนเทศส่วนบุคคล

ในพระราชบัญญัตินี้ได้ระบุคำจำกัดความไว้ดังนี้

สารสนเทศส่วนบุคคล หมายถึง สารสนเทศที่ได้จัดเก็บไว้ซึ่งเกี่ยวกับแต่ละบุคคล สามารถเรียกดูชื่อ วันเดือนปีเกิดหรือข้อมูลอื่นๆ ทั้งที่เป็นความและตัวเลขหรือสัญลักษณ์ รวมทั้งสารสนเทศอื่นๆ ที่สามารถเชื่อมโยงกันได้

การประมวลผลทางคอมพิวเตอร์ หมายถึง ตัวป้อน การบันทึก การตรวจสอบการประมวลผล การแก้ไข เปลี่ยนแปลง การสอบถาม การลบ รวมทั้งรายงานหรือสิ่งอื่นๆ ที่ทำด้วยคอมพิวเตอร์ โดยยกเว้นการประมวลผลที่จัดทำตามกฎหมายของรัฐบาล

ธนาคารสารสนเทศส่วนบุคคล หมายถึง การเก็บรวบรวมสารสนเทศส่วนบุคคลที่มีการจัดการทำอย่างเป็นระบบเพื่อใช้ในหน่วยงานและใช้สื่อต่างๆ

สารสนเทศที่ผ่านการประมวล (Processed Information) หมายถึง สารสนเทศที่ได้จัดเก็บไว้ในแฟ้มข้อมูลของสารสนเทศส่วนบุคคล

ในพระราชบัญญัติได้ระบุข้อยกเว้นไว้สำหรับสารสนเทศส่วนบุคคลที่มีการรวบรวมเพื่อจัดทำสถิติเฉพาะเรื่องที่กำหนดไว้ใน พ.ร.บ. สถิติ และรวมทั้งสารสนเทศส่วนบุคคลที่จัดเก็บเพื่อสถิติงานวิจัย

การประมวลผลสารสนเทศส่วนบุคคลนั้นหน่วยงานจะต้องปฏิบัติตามหน้าที่กำหนดไว้ตามกฎหมายและขอบข่ายของรายการที่บันทึกในแฟ้มข้อมูลสารสนเทศส่วนบุคคลจะต้องไม่นอกเหนือจากที่กำหนดไว้ในวัตถุประสงค์

การรักษาความปลอดภัยของสารสนเทศส่วนบุคคล

1) หัวหน้าหน่วยงานของรัฐบาลจะต้องใช้ความพยายามทุกด้านเพื่อดำเนินการป้องกันการลักลอบหรือทำลาย และจัดการสารสนเทศส่วนบุคคลในทางที่ควรในการประมวลผลด้วยคอมพิวเตอร์ ทั้งในด้านการเตรียมข้อมูลและการจัดเก็บรักษาเทปแม่เหล็ก

2) หัวหน้าหน่วยงานของรัฐบาลที่รักษาสารสนเทศส่วนบุคคลจะต้องพยายามทุกวิธีเพื่อวัตถุประสงค์ในการคงไว้ของแฟ้ม เพื่อให้แน่ใจว่าสามารถมีสารสนเทศทั้งในอดีตและปัจจุบัน

การแจ้งในการสร้างสารสนเทศส่วนบุคคล

1) หัวหน้าหน่วยงานจะต้องแจ้งการสร้างแฟ้มสารสนเทศส่วนบุคคล ให้ผู้อำนวยการของ MCA (Management and Coordination Agency) ก่อนที่จะสร้างแฟ้มสารสนเทศส่วนบุคคล การแจ้งประกอบด้วย

(1) ชื่อของแฟ้มสารสนเทศส่วนบุคคล

(2) ชื่อหน่วยงานที่เก็บแฟ้มและชื่อองค์กรที่จัดการและใช้สารสนเทศส่วนบุคคล

(3) วัตถุประสงค์ในการเก็บแฟ้มสารสนเทศส่วนบุคคล

(4) รายการที่จะเก็บ รวมถึงขอบข่ายของสิ่งที่จะเก็บ

(5) วิธีการในการประมวลผลสารสนเทศที่เก็บ

(6) ชื่อหน่วยงานหรือองค์กรอื่น นอกเหนือจากผู้ที่เก็บแฟ้มซึ่งจะเป็นผู้ใช้สารสนเทศนี้

2) สิ่งที่กล่าวมานี้ไม่รวมกรณีแฟ้มสารสนเทศส่วนบุคคลที่มีลักษณะ

(1) แฟ้มสารสนเทศส่วนบุคคลที่เกี่ยวกับความปลอดภัยของประเทศ ความมั่นคงด้านต่างประเทศ หรือประเด็นอื่นๆ ที่สำคัญต่อประเทศ

(2) แฟ้มสารสนเทศส่วนบุคคลเพื่อสืบสวนคดีต่างๆ หรือการสืบสวนการละเมิดกฎหมายระเบียบเกี่ยวกับทางด้านภาษี

(3) แฟ้มสารสนเทศส่วนบุคคลของข้าราชการและสิ่งที่เก็บนั้นเกี่ยวกับเงินเดือน สวัสดิการ และสิ่งอื่นๆ ที่เป็นการตรวจสอบโดยหน่วยงานของรัฐบาล

(4) แฟ้มสารสนเทศส่วนบุคคลเพื่อการทดลองเพื่อประมวลผลด้วยคอมพิวเตอร์

(5) แฟ้มสารสนเทศส่วนบุคคลที่กำหนดไว้ว่าจะลบทิ้งภายใน 1 ปี

(6) แฟ้มสารสนเทศเพื่อส่งเอกสาร จดหมาย เงินหรือสิ่งอื่นๆ ที่จำเป็นในการบริการจัดส่ง โดยมีรายการเพียงที่อยู่ ชื่อ และอื่นๆ เท่าที่จำเป็น

(7) แฟ้มสารสนเทศส่วนบุคคลที่เก็บโดยหน่วยงานของรัฐบาลและใช้ตามหน้าที่ความรับผิดชอบของหน่วยงานนั้น

(8) แฟ้มสารสนเทศส่วนบุคคลสำหรับวัตถุประสงค์ทางด้านวิชาการ

(9) แฟ้มสารสนเทศส่วนบุคคลซึ่งมีการประมวลผลตามที่รัฐบาลกำหนดและไม่มีการส่งต่อให้กับหน่วยงานอื่น นอกจากหน่วยงานที่รวบรวมสารสนเทศ

การแจ้งแฟ้มสารสนเทศส่วนบุคคลให้สาธารณะทราบ

1) ผู้อำนวยการของ MCA ต้องแจ้งในราชกิจจานุเบกษาอย่างเป็นทางการอย่างน้อยปีละครั้งเกี่ยวกับสิ่งที่เก็บรวบรวม

2) ผู้อำนวยการของ MCA ไม่ต้องแจ้งแก่สาธารณะเกี่ยวกับรายการในแฟ้มสารสนเทศ ในกรณีแฟ้มไม่ได้ลงทะเบียนตามการขออนุญาตที่ระบุไว้

การกำหนดการใช้และการประมวลผลสารสนเทศ

1) สารสนเทศที่ประมวลผลแล้วต้องไม่ใช้นอกเหนือจากวัตถุประสงค์ที่กำหนดไว้เมื่อขออนุญาตเก็บรวบรวมแฟ้มสารสนเทศส่วนบุคคล นอกจากในกรณีที่มีการใช้ภายในหน่วยงานนั้นๆ หรือนำไปใช้ในหน่วยงานอื่นตามที่ขออนุญาตไว้ตามกรณีต่อไปนี้

(1) บุคคลที่เกี่ยวข้อตกลงให้นำไปใช้ได้

(2) หน่วยงานที่เก็บแฟ้มจะใช้สารสนเทศที่ประมวลผลแล้วภายในหน่วยงานตามจำเป็นเท่าที่กฎหมายอนุญาตไว้และสมเหตุผล

(3) สารสนเทศที่ประมวลผลแล้วได้รับการยินยอมให้หน่วยงานใช้ได้ไม่ว่าจะเป็นหน่วยงานรับภูมิภาค สาธารณะ รัฐวิสาหกิจ และใช้ความที่สมควร และจำเป็นต่อการดำเนินงานหรือธุรกิจตามที่กฎหมายระบุไว้

(4) ในกรณีที่ใช้สารสนเทศที่ประมวลผลแล้วเพื่อทำเป็นสถิติ หรือใช้เพื่อวัตถุประสงค์ทางการศึกษาหรือในกรณีที่เป็นการให้แก่บุคคลที่สามแล้วจะเกิดประโยชน์แก่ผู้ที่เป็นเจ้าของหรือในกรณีที่มีเหตุผลพิเศษ ในการให้ใช้สารสนเทศที่ประมวลแล้ว

ทั้งหมดนี้จะต้องไม่นำไปใช้กับกรณีใดๆ ที่สิทธิของผู้ที่เป็นเจ้าของหรือบุคคลที่สามจะได้รับผลกระทบอย่างร้ายแรงจากการใช้หรือการให้ใช้สารสนเทศที่ประมวลผลแล้ว

2) หัวหน้าหน่วยงานที่เก็บรักษาแฟ้มข้อมูลจะต้องเข้มงวดกับการใช้ภายในของสารสนเทศที่ประมวลแล้ว ไม่ให้นำไปใช้นอกเหนือจากวัตถุประสงค์ที่ระบุไว้

หน้าที่ความรับผิดชอบของผู้รับผิดชอบการประมวลสารสนเทศ ผู้ที่รับผิดชอบในหน้าที่นี้จะต้องไม่ทำนอกเหนือไปจากที่ได้กำหนดวัตถุประสงค์ไว้ การเปิดเผยสารสนเทศที่มีการประมวลผลแล้ว จะต้องดำเนินการดังนี้

1) บุคคลสามารถเขียนคำร้องเพื่อขอเปิดเผยสารสนเทศที่มีการประมวลผลแล้ว ในกรณีที่ตนเองมีส่วนเกี่ยวกับสารสนเทศนั้น นอกจากสารสนเทศนั้นอยู่ในกรณีที่เกี่ยวกับผลการเรียนในโรงเรียน การสอบเข้าในโรงเรียนที่เกี่ยวกับพระราชบัญญัติ School Education Act หรือแม้สารสนเทศที่มีรายการของบุคคลเกี่ยวกับการตรวจทางการแพทย์ในโรงพยาบาล คลินิกหรือคลินิกสำหรับการคลอดบุตร หรือแฟ้มสารสนเทศส่วนบุคคลซึ่งมีรายการเกี่ยวกับการทำความผิด การกำหนดโดยทนาย หรือเจ้าหน้าที่ตำรวจ หรือรายการที่เกี่ยวกับการบังคับลงโทษ

2) หัวหน้าหน่วยงานที่เก็บรวบรวมแฟ้มข้อมูลจะเปิดเผยสารสนเทศที่ประมวลผลแล้วได้โดยการทำบันทึกถึงผู้ที่เป็นเจ้าของข้อมูล

กรณีที่ไม่อนุญาตให้เปิดเผยสารสนเทศ

1) หัวหน้าหน่วยงานรวบรวมแฟ้มสารสนเทศส่วนบุคคลได้รับอนุญาตที่จะไม่เปิดเผยสารสนเทศที่ประมวลผลแล้วทั้งหมดหรือบางส่วน ถ้าหัวหน้าหน่วยงานพบว่าการเปิดเผยนั้นจะทำให้เกิดสิ่งต่อไปนี้

(1) เกี่ยวกับหน้าที่รับผิดชอบและการทำงาน การสอบสวนผู้กระทำความผิด การสอบสวนกรณีล่วงละเมิดต่อกฎระเบียบตามที่กำหนดไว้ในพระราชบัญญัติภาษี (Tax Act) หรือกรณีที่เกี่ยวกับการสอบสวนเฉพาะเรื่องภายใต้กฎหมาย

(2) กรณีที่เป็นการตรวจสอบความรู้หรือเทคนิคที่เป็นความเชี่ยวชาญเฉพาะเรื่อง การทบทวนคุณสมบัติ

(3) กรณีใดๆ ที่จัดทำโดยคณะกฤษฎีกาที่เกี่ยวกับกฎหมายของรัฐบาล

(4) ในกรณีที่การเปิดเผยสารสนเทศที่ประมวลแล้ว จะมีผลให้ต่อความสัมพันธ์ที่มีความไว้วางใจกัน หรือความร่วมมือระห่างหน่วยงานหรือกลุ่มที่สามใดๆ

(5) ในกรณีที่การเปิดเผยทำให้มีผลร้ายต่อชีวิต ร่างกาย ทรัพย์สิน หรือความสนใจอื่นๆ ของบุคคลใดบุคคลหนึ่ง

2) หัวหน้าหน่วยงานที่เก็บรวบรวมข้อมูลต้องเปิดเผยโดยไม่ชักช้าจากเวลาที่ได้มีการอนุญาตของกฎหมายโดยการทำบันทึก และโดยการเสนอเหตุผลสำหรับการตัดสินใจ

ระยะเวลาในการเปิดเผย

1) การตัดสินใจว่าจะเปิดเผยหรือไม่เปิดเผยภายใต้ จะต้องทำเป็นบันทึกภายใน 30 วัน นับตั้งแต่การรับเรื่องร้องขอให้เปิดเผย

2) หัวหน้าหน่วยงานที่เก็บรวบรวมข้อมูลจะต้องเปิดเผยโดยไม่ชักข้าจากเวลาที่ได้มีการอนุญาตในกรณีที่ไม่สามารถทำได้ หรือมีเหตุผลอื่นใดที่ทำให้ไม่สามารถเปิดเผยได้ในระยะเวลาที่ระบุ หัวหน้าหน่วยงานที่เก็บรวบรวมจะต้องแจ้งให้ผู้ร้องนั้นทราบเหตุผลที่ไม่สามารถเปิดเผยได้ในระยะเวลาที่ระบุไว้

3) ผู้ร้องขอให้เปิดเผยอาจจะพิจารณาว่าถ้าสารสนเทศนั้นไม่สามารถเปิดเผยได้ในระยะเวลาที่ระบุอาจไม่มีการเปิดเผยสารสนเทศนั้น

การเก็บค่าธรรมเนียม

1) ผู้ร้องขอจะต้องจ่ายค่าธรรมเนียมที่กำหนดไว้

2) ในกรณีที่มีการจัดส่งสารสนเทศที่เปิดเผยนั้น ผู้ร้องขอจะต้องเสียค่าใช้จ่ายที่เกิดขึ้น นอกจากในกรณีที่เป็นไปตามกฎหมาย

การร้องขอเพื่อเสนอเอกสารและคำอธิบาย

1) ผู้อำนวยการของ MCA สามารถร้องขอ หัวหน้าฝ่ายงานสำหรับการจัดส่งเอกสารและคำอธิบาย ถ้าผู้อำนวยการงานเห็นว่ามีความจำเป็นในส่วนที่เกี่ยวกับการประมวลผลทางคอมพิวเตอร์ของสารสนเทศส่วนบุคคลที่หน่วยงานนั้น

2) ผู้อำนวยการของ MCA อาจจะให้ความคิดเห็นล่วงหน้าแก่นายกรัฐมนตรี หรือหัวหน้าหน่วยงานเกี่ยวกับการจัดการสนเทศส่วนบุคคลทีประมวลผลด้วยคอมพิวเตอร์ที่เก็บไว้ที่หน่วยงานถ้าจำเป็น

การลงโทษบุคคลที่เปิดเผยสารสนเทศส่วนบุคคลจะต้องถูกปรับไม่เกิน 100,000 เยน

กฎหมายที่เกี่ยวข้องกับการเข้าถึงข้อมูลข่าวสารที่หน่วยงานราชการญี่ปุ่นนั้นผ่านการพิจารณาของสภานิติบัญญัติเป็นครั้งแรกในเดือนพฤษภาคม ปี ค.ศ. 1999 ภายหลังการต่อสู้เรียกร้องของประชาสังคมญี่ปุ่นเพื่อนำมาใช้เป็นกฎหมายของประเทศ การเข้าถึงข้อมูลข่าวสารของหน่วยงานราชการนับว่าเป็นสิ่งที่สำคัญมากต่อการเปิดโปงความล้มเหลวของรัฐบาลญี่ปุ่น ซึ่งทำให้ประชาชนตระหนักถึงความจำเป็นภายหลังจากที่ความเติบโตทางเศรษฐกิจของญี่ปุ่นเริ่มล่มสลายไปและการที่รัฐบาลปกปิดความลับของประชาชน ซึ่งประเด็นนี้ได้สะท้อนอยู่ในมาตรา 1 ของพระราชบัญญัติซึ่งระบุถึงวัตถุประสงค์ในการเปิดเผยของข้อมูลว่าเพื่อให้แน่ใจว่ารัฐบาลญี่ปุ่นรับผิดชอบต่อประชาชนในการดำเนินการของตนและมีส่วนช่วยส่งเสริมการบริหารงานที่ยุติธรรมและเป็นประชาธิปไตยโดยขึ้นอยู่กับความเข้าใจที่ถูกต้องและการวิพากษ์วิจารณ์ของประชาชน ในช่วงเวลาที่พระราชบัญญัติดังกล่าวได้ประกาศใช้เป็นกฎหมายในปี ค.ศ. 1999 ปรากฏว่าองค์กรปกครองส่วนท้องถิ่นมากกว่า 900 แห่งได้นำเอากฎหมายความเป็นอิสระของข้อมูลข่าวสารมาใช้แล้วในเวลานั้น กฎหมายนี้ในระดับชาติเริ่มมีผลบังคับใช้ในเดือนเมษายน ปี ค.ศ. 2001

บุคคลใดบุคคลหนึ่งรวมทั้งผู้ที่ไม่ถือสัญชาติญี่ปุ่นสามารถยื่นคำร้องต่อหัวหน้าส่วนราชการเพื่อให้เปิดเผยข้อมูลข่าวสารของทางราชการ เมื่อได้รับคำร้องขอดังกล่าว หัวหน้าส่วนราชการจะต้องเปิดเผยข้อมูลซึ่งขึ้นอยู่ว่าเข้าข่ายข้อยกเว้นห้ามมิให้เปิดเผยข้อมูลที่กฎหมายบัญญัติหรือไม่ สิทธิในการเข้าถึงข้อมูลอาจถูกจำกัดได้โดยคำนิยามของเอกสารทางราชการและหน่วยงานราชการ

พระราชบัญญัติฉบับนี้ระบุว่าเอกสารของทางราชการ หมายถึง เอกสารใด ๆ ก็ตามไม่ว่าจะเป็นบันทึกทางแผ่นบันทึกข้อมูลหรือบันทึกที่วาดขึ้น ตระเตรียมโดยเจ้าพนักงานตามหน้าที่ของตนหรือที่ได้มาหากว่าเอกสารเหล่านั้นเป็นไปเพื่อการใช้ในหน่วยงานราชการโดยเจ้าพนักงาน คำนิยามตามนี้มีข้อจำกัดในความครอบคลุมของคำนิยามเพราะว่าข้อมูลอาจถูกจัดเก็บอยู่ในรูปแบบอื่น ๆ และตามนิยามนี้ครอบคลุมเฉพาะบันทึกที่มีอยู่เพื่อวัตถุประสงค์ของทางราชการเท่านั้น อย่างไรก็ตาม มีเอกสารที่ได้รับการยกเว้นอยู่ 2 ประเภท คือ บันทึกของทางราชการที่ได้นำมาตีพิมพ์เผยแพร่เพื่อขาย และจดหมายเหตุของทางราชการที่มีคำสั่งคณะรัฐมนตรีให้เก็บรักษาไว้ในฐานะเอกสารทางประวัติศาสตร์หรือทางวัฒนธรรม หรือเอกสารเพื่อการศึกษาวิจัย การที่เอกสารทั้งสองประเภทข้างต้นอยู่ในข้อยกเว้นนั้นเป็นสิ่งที่ไม่ค่อยพบเห็นในกฎหมายลักษณะเดียวกันนี้ของประเทศอื่น ๆ

หน่วยงานต่าง ๆ ที่นิยามเป็น “หน่วยงานราชการ” ในพระราชบัญญัตินี้ได้แก่

1) สำนักงานของคณะรัฐมนตรี หรือสำนักงานต่าง ๆ ภายใต้กำกับดูแลของคณะรัฐมนตรีที่จัดตั้งขึ้นตามกฎหมาย

2) หน่วยงานราชการต่าง ๆ ที่กำหนดโดยกฎหมายต่าง ๆ และ

3) คณะกรรมการการตรวจสอบ

รัฐวิสาหกิจที่ให้บริการสาธารณูปโภคขั้นพื้นฐานซึ่งมีอยู่เป็นจำนวนมากในประเทศญี่ปุ่นนั้น ไม่ตกอยู่ในบังคับของพระราชบัญญัติฉบับนี้ อย่างไรก็ตาม พระราชบัญญัติฉบับนี้กำหนดให้มีการตรากฎหมายที่กำหนดให้รัฐวิสาหกิจเหล่านี้ต้องเปิดเผยข้อมูลภายในเวลาสองปีที่กฎหมายนั้น ๆ ได้ออกมาบังคับใช้ ในทางปฏิบัตินั้น กฎหมายที่กำหนดให้มีการกระทำดังกล่าวได้ออกมาบังคับใช้ในวันที่ 2 เดือนพฤศจิกายน ปี ค.ศ. 2001

คำร้องขอต้องระบุชื่อผู้ร้องขอ (หรือชื่อตัวแทนของบริษัทที่ร้องขอ) ที่อยู่และรายละเอียดของเอกสารทางราชการที่ต้องการเพื่อให้สามารถค้นหาได้ เมื่อใดก็ตามที่คำร้องขอนั้นขาดรายละเอียดและไม่สมบูรณ์ หน่วยงานราชการจะแจ้งผู้ร้องขอให้ทราบและให้เวลาที่เหมาะสมเพื่อการแก้ไข ขณะเดียวกันหน่วยงานต้องใช้ความพยายามที่จะให้ความช่วยเหลือด้วย (มาตรา 4) คำร้องขออาจจะถูกส่งต่อไปยังหน่วยงานราชการอื่น ๆ เมื่อมีเหตุผลที่เหมาะสมโดยต้องมีจดหมายแจ้งไปยังผู้ร้องขอด้วย

ในพระราชบัญญัติฉบับนี้มีเงื่อนไขหลายอย่างที่เกี่ยวข้องกับการปรึกษาบุคคลที่สามที่ข้อมูลที่ร้องขอนั้นเกี่ยวพันถึง บุคคลที่สามนั้นจะได้รับโอกาสให้ชี้แจงอย่างเป็นทางการและได้รับจดหมายแจ้งเป็นเวลาสองอาทิตย์ก่อนที่ข้อมูลจะถูกเปิดเผยเพื่อให้สามารถอุทธรณ์คำตัดสินให้มีการเปิดเผยข้อมูลได้ (มาตรา 13)

โดยปกติแล้ว คำตัดสินให้เปิดเผยข้อมูลต้องกระทำขึ้นภายในระยะเวลาสามสิบวัน และผู้ร้องขอต้องได้รับการแจ้งเป็นลายลักษณ์อักษรถึงคำตัดสินดังกล่าว เมื่อใดก็ตามที่คำร้องขอถูกส่งกลับไปยังผู้ร้องขอเพื่อให้แก่ไขหรือทำให้ชัดเจนขึ้น เวลาที่ใช้ในการแก้ไขคำร้องขอดังกล่าวจะไม่นับรวมอยู่ในเวลาสามสิบวันข้างต้น “เมื่อมีเหตุผลที่เหมาะสม เช่น ปัญหาที่เกิดขึ้นจากการดำเนินธุรกิจ” อาจมีการขยายระยะเวลาออกไปอีกสามสิบวัน โดยผู้ร้องขอจะต้องได้รับจดหมายแจ้งถึงการขยายระยะเวลาเป็นลายลักษณ์อักษรพร้อมระบุเหตุผล (มาตรา 9 และมาตรา 10)

หากคำร้องขอนั้นครอบคลุมถึงเอกสารทางราชการจำนวนมาก และมีความเป็นไปได้ว่าประสิทธิภาพของหน่วยงานราชการในการให้ข้อมูลต่าง ๆ ภายในระยะเวลาหกสิบวันจะ “ถูกมองว่ามีอุปสรรค” หัวหน้าส่วนราชการอาจจะเปิดเผยข้อมูล “บางส่วนที่เหมาะสม” ภายในระยะเวลาที่กำหนด แล้วอาจให้ข้อมูลทั้งหมดที่เหลือภายใน “ระยะเวลาที่เหมาะสม” ในกรณีนี้ผู้ร้องขอจะต้องได้รับจดหมายแจ้งถึงการปฏิบัติดังกล่าวข้างต้น และเวลาสิ้นสุดของระยะเวลาที่ขยายออกไปสำหรับเอกสารที่เหลือ (มาตรา 11)

ผู้ร้องขออาจขอตรวจดูเอกสารทางราชการ ขอสำเนาซ้ำ หรือรูปแบบต่างๆ ในการเข้าถึงบันทึกที่อยู่ในแผ่นบันทึกข้อมูลตามที่กำหนดโดยคำสั่งของคณะรัฐมนตรี โดยปกติแล้ว คำร้องจะถูกดำเนินการให้หากว่าไม่ได้ทำให้เกิดอันตรายต่อเอกสารทางราชการ (มาตรา 14)

อาจมีการเรียกเก็บค่าธรรมเนียมในการดำเนินการตามคำร้องขอและการให้ข้อมูลที่ต้องการตามคำสั่งของคณะรัฐมนตรี บนเงื่อนไขว่าค่าธรรมเนียมจะต้องไม่เกินค่าใช้จ่ายที่เกิดขึ้นจริงในการจัดหาข้อมูลที่ต้องการ โครงสร้างของค่าธรรมเนียมจะต้องพิจารณาถึงค่าธรรมเนียมที่เป็น “จำนวนที่สามารถจ่ายได้จริง” และตามคำสั่งของคณะรัฐมนตรี หัวหน้าส่วนราชการสามารถลดหรือยกเว้นค่าธรรมเนียมในกรณีมีวิกฤติทางเศรษฐกิจหรือเหตุผลสำคัญอื่น ๆ ทั้งนี้พระราชบัญญัติของประเทศญี่ปุ่นไม่ได้กำหนดให้มีการตีพิมพ์เผยแพร่ข้อมูลข่าวสารบางชนิด

ข้อยกเว้นจากภาระหน้าที่ในการเปิดเผยถูกกำหนดไว้ในมาตรา 5 ซึ่งได้ระบุถึงข้อยกเว้นจำนวน 6 ข้อที่แตกต่างกัน ข้อยกเว้นส่วนมากขึ้นอยู่กับแบบทดสอบความเป็นอันตราย พระราช บัญญัติฉบับนี้ยังกำหนดว่า “เมื่อใดก็ตามที่มีความจำเป็นในผลประโยชน์สาธารณะเฉพาะอย่าง” ให้ผลประโยชน์สาธารณะมีความสำคัญมากกว่าข้อยกเว้น โดยหัวหน้าส่วนราชการสามารถเปิดเผยเอกสารทางราชการได้ (มาตรา 7)

ข้อยกเว้นข้อแรกเกี่ยวกับข้อมูลของบุคคลซึ่งมีความเป็นไปได้ที่จะระบุตัวบุคคลหรือซึ่งไม่มีความเป็นไปได้ที่จะระบุตัวบุคคลใด ๆ อันทำให้ “มีความเสี่ยงที่สิทธิและผลประโยชน์ของบุคคลอาจได้รับการกระทบกระเทือน” ข้อยกเว้นนี้ระบุไว้อย่างกว้าง ๆ ซึ่งครอบคลุมข้อมูลทั้งหมดที่ระบุตัวบุคคลมากกว่าข้อมูลที่อาจทำลายผลประโยชน์ส่วนบุคคลที่ถูกกฎหมาย หรือซึ่งเกี่ยวกับผลประโยชน์ส่วนบุคคลนอกเหนือจากนี้ ข้อยกเว้นนี้ไม่ขึ้นอยู่กับแบบทดสอบความอันตราย ข้อยกเว้นนี้มีข้อจำกัดตรงที่ข้อมูลอาจถูกเปิดเผยได้หากการเปิดเผยนั้นเป็นไปตามกฎหมายหรือ ธรรมเนียมปฏิบัติ หรือการเปิดเผยเป็นสิ่งที่จำเป็นต่อการปกป้องชีวิต สุขภาพ การดำรงชีพ หรือทรัพย์สมบัติของบุคคล อย่างไรก็ตามข้อยกเว้นนี้ไม่ใช้กับข้อมูลเกี่ยวกับการปฏิบัติราชการของเจ้าพนักงานซึ่งเป็นข้อจำกัดที่สำคัญอย่างหนึ่งของข้อยกเว้นนี้

ข้อยกเว้นข้อที่สองเกี่ยวข้องกับข้อมูลของบริษัทซึ่งมีความเสี่ยงที่มีจุดแข็งในการแข่งขันหรือผลประโยชน์ต่าง ๆ ที่ถูกกฎหมายของบริษัทจะได้รับการกระทบกระเทือน หรือข้อมูลที่เป็นความลับ หรือข้อมูลที่การรักษาความลับเป็นเงื่อนไขที่สมเหตุสมผล ข้อยกเว้นข้อนี้มีข้อจำกัดที่ข้อมูลอาจนำมาเปิดเผยได้หากว่าจำเป็นต่อการปกป้องชีวิต สุขภาพ การดำรงชีพหรือทรัพย์สินของบุคคล

ข้อยกเว้นข้อที่สามครอบคลุมข้อมูลซึ่งมีเหตุผลที่เพียงพอที่หัวหน้าส่วนราชการหากเปิดเผยไปแล้ว จะทำให้เกิดความเสี่ยงต่อความมั่นคงของรัฐ หรือต่อความสัมพันธ์กับประเทศอื่นๆ หรือองค์กรระหว่างประเทศ หรือทำให้เกิดความเสียเปรียบในการเจรจากับประเทศอื่น ๆ หรือองค์กรระหว่างประเทศ

ข้อยกเว้นข้อที่สี่ครอบคลุมข้อมูลซึ่งมีเหตุผลที่เพียงพอที่การเปิดเผยทำให้เกิดอันตรายต่อ “การป้องกัน การปกปิดความลับหรือการสืบสวนคดีอาชญากรรม การรักษากระบวนการพิสูจน์ความผิด การดำเนินการพิพากษา และความมั่นคงทางสังคมอื่น ๆ และเรื่องต่าง ๆ ที่เกี่ยวกับการรักษากฎระเบียบของสังคม”

ข้อยกเว้นข้อที่ห้าใช้กับความตั้งใจภายในรัฐบาลหรือการปรึกษาหารือซึ่งการเปิดเผยข้อมูลจะเสี่ยงต่อการกระทบกระเทือนการแลกเปลี่ยนทัศนะที่ยุติธรรมหรือความเป็นกลางในการตัดสินใจ เสี่ยงต่อทำให้เกิดความสับสนหรือเสี่ยงต่อการเกิดข้อได้เปรียบหรือข้อเสียเปรียบที่ไม่ยุติธรรมต่อบุคคลใด ๆ ข้อยกเว้นนี้สอดคล้องกับมาตรฐานนานาชาติ

ข้อยกเว้นข้อที่หกมีจุดมุ่งหมายในการปกป้องอันตรายที่เกิดต่อการดำเนินงานธุรกิจโดยหน่วยงานราชการต่าง ๆ ซึ่งข้อยกเว้นนี้รายชื่อแบบฟอร์มความเป็นอันตรายพิเศษรายชื่อดังกล่าวรวมอุปสรรคต่อการวิจัย อันตรายต่อผลประโยชน์ที่ถูกกฎหมาย ต่อการจัดการของบุคคลอันตรายต่อผลประโยชน์ของรัฐในสัญญาหรือการเจรจาต่อรอง และการเอื้อประโยชน์ต่อการกระทำผิดกฎหมายหรือการกระทำที่ไม่ยุติธรรม

พระราชบัญญัติฉบับนี้ กำหนดให้มีการจัดตั้งคณะกรรมการทบทวนการเปิดเผยข้อมูลภายใต้สำนักงานเลขาธิการนายกรัฐมนตรีเพื่อพิจารณาคำอุทธรณ์ แม้ว่าคณะกรรมการดังกล่าวจะอยู่ภายใต้สำนักงานเลขาธิการนายกรัฐมนตรี แต่ก็ได้มีความพยายามที่จะทำให้คณะกรรมการดังกล่าวมีความเป็นอิสระ คณะกรรมการทบทวนการเปิดเผยข้อมูลข่าวสารประกอบด้วยสมาชิกจำนวนเก้าคน ซึ่งสามคนในเก้าคนเป็นกรรมการเต็มเวลา นายกรัฐมนตรีแต่งตั้งสมาชิกของคณะกรรมการดังกล่าวจากบุคคลที่ “มีความสามารถเป็นเลิศในการพิจารณาตัดสิน” ซึ่งได้รับการเสนอชื่อจากสภาผู้แทนราษฎรและวุฒิสภา ซึ่งอย่างน้อยก็รับประกันการเปิดกว้างและมีส่วนร่วมทางการเมืองของประชาชน คณะกรรมการทบทวนการเปิดเผยข้อมูลนั้นมีวาระการดำรงตำแหน่งสามปี และสมาชิกของคณะกรรมการดังกล่าวอาจได้รับการแต่งตั้งอีกวาระหนึ่งได้ สมาชิกอาจถูกเพิกถอนตำแหน่งโดยนายกรัฐมนตรีเมื่อได้รับการอนุญาตจากสภาผู้แทนราษฎรและวุฒิสภา

เหตุผลในการเพิกถอนตำแหน่งมาจากการไร้ความสามารถ การกระทำผิดหรือได้กระทำในสิ่งที่ขัดต่อหน้าที่ของตน ในขณะที่ดำรงตำแหน่งเป็นสมาชิกของคณะกรรมการทบทวนการเปิดเผยข้อมูล สมาชิกจะต้องไม่เป็นเจ้าหน้าที่ของพรรคการเมืองใด ๆ หรือสมาคมใด ๆ ท้ายที่สุดนี้ พระราชบัญญัติกำหนดว่าเงินเดือนของสมาชิกของคณะกรรมการดังกล่าวนั้นกำหนดโดยกฎหมายอื่น พระราชบัญญัติกำหนดให้มีการจัดตั้งสำนักงานที่ทำหน้าที่เลขานุการให้แก่คณะกรรมการดังกล่าวด้วย

การอุทธรณ์นั้นอาจอุทธรณ์ต่อหัวหน้าส่วนราชการซึ่งจะต้องส่งคำอุทธรณ์นี้ต่อไปยังคณะกรรมการทบทวนการเปิดเผยข้อมูล ถ้าคำอุทธรณ์นั้นไม่ขัดต่อกฎหมายหรือได้มีคำตัดสินให้เปิดเผยข้อมูลไปแล้ว ผู้ร้องขอซึ่งได้แก่บุคคลต้องการให้มีการอุทธรณ์ และบุคคลที่สามซึ่งได้เป็นตัวแทนต้องได้รับการบอกกล่าวถึงคำอุทธรณ์ใด ๆ (มาตรา 18 และมาตรา 19)

เมื่อมีการพิจารณาคำอุทธรณ์ คณะกรรมการทบทวนการเปิดเผยข้อมูลอาจกำหนดให้หน่วยงานราชการส่งบันทึกของทางราชการที่เป็นต้นเรื่องมาพร้อมกับคำอุทธรณ์หรือขอข้อมูลต่าง ๆ จากผู้ร้องขอ (มาตรา 27) พระราชบัญญัติฉบับนี้ยังให้รายละเอียดในการกระบวนการพิจารณาคำอุทธรณ์ ซึ่งรวมถึงการเป็นตัวแทนหรือการสืบสวน คำอุทธรณ์อาจถูกพิจารณาโดยศาลประจำเขต (มาตรา 36)

พระราชบัญญัติกำหนดให้หัวหน้าส่วนราชการต่าง ๆ ตั้งกฎระเบียบที่กำหนดให้มีการจัดการเอกสารที่ถูกต้องสอดคล้องกับคำสั่งของคณะรัฐมนตรี และเผยแพร่กฎระเบียบดังกล่าวต่อประชาชน คำสั่งของคณะรัฐมนตรีกำหนดมาตรฐานทั่วไปเกี่ยวกับ “การแยกประเภท การตระเตรียม การรักษา และการทำลายเอกสารทางราชการต่าง ๆ” (มาตรา 37)

หัวหน้าส่วนราชการต่าง ๆ จำต้องเอื้อให้มีการเปิดเผยข้อมูลโดยให้ข้อมูลเกี่ยวกับเอกสารทางราชการที่หน่วยงานมีอยู่ เช่นเดียวกับปฏิบัติตาม “ขั้นตอนที่เหมาะสม” อื่น ๆ ผู้อำนวยการทั่วไปของสำนักงานประสานงานและจัดการ (The Director-General of the Management and Coordination Agency) ต้องจัดตั้งสำนักงานเพื่อรับคำร้องขอข้อมูลทั่วไป สำนักงานดังกล่าวต้องกำหนดให้หน่วยงานราชการต่าง ๆ ส่งรายงานการปฏิบัติงานของตนและนำรวบรวมและตีพิมพ์เอกสารสรุปของรายงานต่าง ๆ ปีละหนึ่งครั้ง (มาตรา 38 และมาตรา 39)

พระราชบัญญัติฉบับนี้ยังกำหนดถึงมาตรการทั่วไปต่าง ๆ ในการส่งเสริมการเปิดกว้างของข้อมูล โดยทั่วไปนั้น รัฐบาลญี่ปุ่นต้อง “พยายามส่งเสริมมาตรการต่าง ๆ ที่เกี่ยวกับการจัดหาข้อมูลที่หน่วยงานราชการต่าง ๆ มีอยู่” หน่วยงานราชการส่วนท้องถิ่นต่าง ๆ ต้องสร้างและพยายามปฏิบัติตามมาตรการเปิดเผยข้อมูล

ท้ายที่สุดนี้ภายหลังที่พระราชบัญญัติฉบับนี้ได้มีผลบังคับใช้ครบสี่ปีแล้ว รัฐบาลจะต้องตรวจสอบประสิทธิภาพในการเปิดเผยข้อมูล และนำมาตรการต่าง ๆ ที่จำเป็นมาใช้ เพื่อปรับปรุงการเปิดเผยข้อมูลทั้งนี้ขึ้นอยู่กับผลการตรวจสอบประสิทธิภาพในการเปิดเผยข้อมูลดังกล่าว (มาตรา 40 มาตรา 41 และมาตรา 44)

ญี่ปุ่นเป็นประเทศตัวอย่างของปัญหาเรื่องสิทธิส่วนบุคคลนี้ที่ชัดเจนที่สุด ซึ่งโดยวัฒนธรรมและความนิยมของญี่ปุ่นจะไม่เน้นเรื่องสิทธิส่วนบุคคล เพราะมีชีวิตการอยู่ร่วมกันแบบช่วยเหลือซึ่งกันและกัน ดังนั้นกฎหมายญี่ปุ่นจึงมีบทลงโทษไม่หนัก เช่น ผู้ทำความผิด พ.ร.บ. สารสนเทศส่วนบุคคลจะถูกปรับไม่เกิน 100,000 เยน สิทธิส่วนบุคคลมีการป้องกันโดยกฎหมายเฉพาะเรื่อง ซึ่งขึ้นอยู่กับกฎหมายรัฐธรรมนูญในสายงานของการสื่อสารในส่วนที่เกี่ยวกับกฎหมายที่เป็นการป้องกันสิทธิส่วนบุคคลที่กำหนดไว้ในกฎหมายรัฐธรรมนูญเป็นเพียงพื้นฐานของการป้องกันสิทธิส่วนบุคคล เพราะว่ากฎหมายนี้ใช้บังคับเพียงหน่วยงานของรัฐบาลและไม่สามารถใช้กับหน่วยงานที่เกี่ยวกับการโทรศัพท์หรือสื่อสาร เช่น NTI (Nippon Telegraph and Telephone Company) KDD (Dokusai Denshin Denwa Company) หรือ NCC (New Common Carrier Company) ได้ แต่ญี่ปุ่นก็ยังมีกฎหมายอื่นๆ ที่ให้ความคุ้มครองสิทธิส่วนบุคคลไว้ดังนี้

บทที่ 21 ของกฎหมายรัฐธรรมนูญระบุว่า เสรีภาพในการแสดงออกจะไม่มีการตรวจสอบ การใช้จะต้องไม่มีการรุกล้ำความลับของราชการ กฎหมายที่เรียกว่า Telecommunications Business Act กำหนดให้บริษัททางการสื่อสารไม่รุกล้ำสิทธิส่วนบุคคลที่เกี่ยวกับการสื่อสารที่บริษัทรับผิดชอบอยู่ ถ้ามีการกระทำผิดโดยพนักงานของบริษัท บทลงโทษคือจำคุกสูงสุดไม่เกิน 2 ปี โดยต้องทำงานหนักในเรือนจำ หรือปรับมากกว่า 500,000 เยน ถ้าทำความผิด (เปิดเผยความลับ) โดยผู้อื่นที่ไม่ใช่พนักงานของบริษัท บทลงโทษจำคุกสูงสุด 1 ปี โดยต้องทำงานหนัก หรือปรับ 300,000 เยน และ บทที่ 9 ของ Wire Telecommunication Act ระบุว่าความลับทางการสื่อสารจะต้องได้รับความคุ้มครอง ส่วนบทที่ 59 ของ Radio Law ระบุว่าห้ามไม่ให้มีการดักฟังข้อความที่ส่งผ่านทางวิทยุ เมื่อมีการสื่อสารดำเนินการโดยบริษัทเอกชน เช่น NTT และ KDD ได้มีการถกเถียงกันว่ารัฐธรรมนูญนี้ควรจะใช้กับพนักงานของบริษัท เช่น ข้อมูลที่เป็นความลับที่เก็บทางการสื่อสาร

อย่างไรก็ตามหากสรุปกฎหมายคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลของญี่ปุ่นอาจสรุปได้ดังตารางต่อไปนี้

ลักษณะ	กฎหมายคุ้มครองข้อมูลส่วนบุคคล (The Law on the Protection of Personal Information)	กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ดำเนินการโดยฝ่ายบริหาร (The Law Concerning the Protection of Personal Information held by Administrative Organs)
วัตถุประสงค์	ปกป้อง สิทธิและผลประโยชน์ส่วนบุคคลในการนำเอาข้อมูลส่วนบุคคลไปใช้	การบริหารรัฐกิจให้การปกป้องสิทธิและผลประโยชน์ของบุคคลดำเนินไปด้วยความเรียบร้อย
รูปแบบ	เป็นกฎหมายพื้นฐาน (Fundamental law) : เป็นกฎหมายที่วางกรอบการปกป้องคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเฉพาะบุคคล (Individual law) เป็นระเบียบว่าด้วยการบริหารจัดการข้อมูลส่วนบุคคลที่หน่วยงานของรัฐต้องยึดเป็นหลักเกณฑ์
หลักการ	เคารพต่อความเป็นอิสระของบุคคล ออกระเบียบเท่าที่จำเป็นในฐานของการปกป้องข้อมูลส่วนบุคคล	การบริหารจัดการข้อมูลส่วนบุคคลของหน่วยงานรัฐต้องเคร่งครัด และดำเนินการภายใต้หลักธรรมรัฐในการบริหารรัฐกิจ
ระเบียบด้านข้อมูล	ข้อมูลข่าวสารส่วนบุคคลต้องมีการจัดเก็บอย่างเป็นระบบ มีมาตรฐานในลักษณะเป็นฐานข้อมูล	ข้อมูลส่วนบุคคลที่หน่วยงานรัฐจัดเก็บต้องเป็นมาตรฐานเดียวกัน รวมทั้งข้อมูลที่เป็นเอกสารหรือรูปแบบอื่นๆ
ข้อยกเว้น	ต้องกระทำโดยไม่มีความมุ่งหมายสร้างความแตกแยกทางศาสนา ผลทางการเมือง การวิจัยทางวิทยาศาสตร์และงานเขียนตลอดจนสื่อมวลชน	หน่วยงานบริหารจัดการเป็นหน่วยรัฐบาลกลาง รัฐบาลท้องถิ่นต้องมีการตราระเบียบรองรับ
สิทธิของเจ้าของข้อมูล	แก้ไข อ้างและตรวจสอบ ได้รับการแจ้งถูกใช้ข้อมูล	แจ้ง ดำเนินการแก้ไขให้ถูกต้อง
ผลบังคับ	30 May 2003	2 ปี นับแต่วันที่ 30 May 2003

4. กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

กฎหมายลิขสิทธ์ของญี่ปุ่นไม่ได้ให้การรับรองคอมพิวเตอร์ซอฟแวร์หรือโปรแกรมคอมพิวเตอร์ต่างๆ ทั้งนี้เป็นไปตามมาตรา 10-3 โดยยึดถือว่าการดำเนินการดังกล่าวนั้นเป็นเรื่องของIdea หรือ Expression Ditchotomy(Computer program) ทั้งนี้จากคำพิพากษาของศาลในคดี Computer association,Int Inc,vAltai Inc,982 (1992) ซึ่งในคดีดังกล่าวศาลยึดหลักFilter Test อย่างไรก็ตามหากมีการดำเนินการรวบรวมข้อมูลและจัดทำเป็นฐานข้อมูลที่มีลักษณะของการสร้างสรร(Creative Compilation) ศาลได้เคยตัดสินในคดีFeist Publication Inc v Rural Tel.Serv.Co(1991)และในคดีAsban v Higashinihon Tel.(2000) [71] หากพิจารณาถึงต้นแบบและการสร้างสรรในระดับล่างสุด ก็อาจได้รับการคุ้มครอง ซึ่งอาจจำเป็นต้องมีการพิสูจน์เป็นรายๆไป เพราะอาจเข้าข้อจำกัดตามมาตรา 39 ได้

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ญี่ปุ่นมีกฎหมายที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ในทางที่ผิดอยู่หลายฉบับ ได้แก่**กฎหมายอาญา(Penal Code)**ที่ให้การคุ้มครองในระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์ **กฎหมายการเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจ(Unauthorized Computer Access Law)**ที่ให้การป้องกันการควบคุมการเข้าถึง และ**กฎหมายอื่นๆ** เช่น กฎหมายลิขสิทธิ์ กฎหมายโทรคมนาคม กฎหมายว่าด้วยสิ่งลามกอนาจารเด็ก เป็นต้น

สำหรับญี่ปุ่นแล้วมีกฎหมาย Unauthorized Computer Access Law No.128,1990 เป็นกฎหมายแม่บทของการกระทำความผิดที่เกี่ยวกับการคอมพิวเตอร์กับการกระทำผิด กฎหมายดังกล่าวมีผลใช้บังคับเมื่อ 3 กุมภาพันธ์ 2000ซึ่งได้วางกรอบการป้องกันการใช้คอมพิวเตอร์โดยผ่านระบบโทรคมนาคมและส่งเสริมให้มีการจัดระเบียบการเข้าถึงข้อมูลเพื่อให้เป็นไปตามนโยบายแห่งชาติ การเข้าถึงการใช้คอมพิวเตอร์ในรูปแบบต่างๆที่ไม่มีอำนาจถือเป็นความผิดทางอาญาที่อาจถูกจำคุก 1 ปี และปรับ 50000 เยน นอกจากนี้ ภายใต้กฎหมาย Computer Crime Act of the Japanese Penal code[72] หากมีการใช้คอมพิวเตอร์ร่วมในการกระทำผิดลักษณะฉ้อโกง(ตามมาตรา 6)และความผิดในลักษณะComputer fraud ตามมาตรา 246 อาจต้องถูกจำคุกที่มีโทษหนักถึง 5 ปี

---

[71] www.cric.or.jp

[72] Takato Natsui **Cybercrimes in Japan :Recent Case ,Legislation,Problems and Perspectives** Meiji Journal vol.10 March 2003 p.5

9) ประเทศเนเธอร์แลนด์

1.การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

ในเนเธอร์แลนด์ ความริเริ่มในการส่งเสริมการแลกเปลี่ยนข้อมูลข่าวสารในกระบวนการยุติธรรมเกิดขึ้นในองค์กรด้านกระบวนการยุติธรรม โดยมีการใช้ระบบคุณภาพที่เรียกว่า ISO 11179[73] มาใช้ทั้งเพื่อการพัฒนาคุณภาพข้อมูลที่จะแลกเปลี่ยนและในขณะเดียวกันก็เพื่อที่จะลดการใช้เวลากับงานเอกสารตามหลักการ e-Business และ e-Government และเน้นที่ XML Business Process กับ Core Components และ UBL NDR มีองค์กรเข้าร่วมเริ่มแรก 6 องค์กร และมีการออกกฎหมายระดับชาติ คือ Electronic Traffic Law

ในอดีตหน่วยงานด้านกระบวนการยุติธรรมทั้งหลายไม่ว่าจะเป็นตำรวจ อัยการ ศาล ราชทัณฑ์หรือองค์กรอื่นๆ มักมีการใช้ข้อมูลเทคโนโลยีสารสนเทศ สำหรับการดำเนินการภายในองค์กรเท่านั้น (the internal) ไม่ค่อยได้ให้ความสำคัญหรือการใส่ใจในการพัฒนาปรับปรุงความร่วมมือกับหุ้นส่วนอื่นๆในกระบวนการยุติธรรมอีกทั้งการสื่อสารข้อมูลก็ยังใช้การดำเนินการแนบเอกสาร (paper document) เป็นหลักเช่นกัน

ในปี ค.ศ.2001 หน่วยงานในกระบวนการยุติธรรมที่ได้มีการริเริ่มการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรม ได้แก่ ตำรวจกับอัยการ โดยอาศัยกฎหมาย คือ มาตรา 8 ของ The National Road and traffic law) โดยมีการใช้โครงสร้างแบบ XML ส่งให้อัยการ และใช้ระบบ SOAP over SMTP เชื่อมโครงการนำร่องดังกล่าวประสบความสำเร็จในการเชื่อมโยงและแลกเปลี่ยนข้อมูล แต่ก็ยังไม่ได้มีการขยายออกไปทั่วประเทศ เนื่องจากยังขาดการพัฒนามาตรฐานในการประสานแลกเปลี่ยนข้อมูลและการกำหนดลักษณะเฉพาะที่ต้องการข้อตกลงก็เป็นลักษณะทวิภาคี (bilateral agreement) ระหว่างตำรวจกับอัยการโดยอัยการแขวง 19 แห่ง กับสถานีตำรวจ Police district 26 แห่ง

ในปี 2002 เนเธอร์แลนด์ ได้มีการกำหนดยุทธศาสตร์การดำเนินการชื่อ “Electronische Berichtenuitwisseling in de Strafrechts Keten (ePV)” โดยมีเป้าหมายในการดำเนินการ คือ

---

[73] Pim van der Eijk **Electronic Information Exchang in Criminal Justice System in Netherland** p.55

1.ส่งเสริมให้เกิดความตระหนักและสนับสนุนการแลกเปลี่ยนข้อมูลข่าวสารทางอิเลกโทรนิกส์และการบูรณาการประสานสัมพันธ์เพื่อให้เกิดสายใยที่มีคุณค่า (Value Chain)

2.เพื่อขอบข่ายและระดับกระบวนการและเปลี่ยนข้อมูล โดยเทคโนโลยีสารสนเทศ

3.เพิ่มจำนวนองค์กรที่มีการเชื่อมโยงข้อมูลทางด้านเทคโนโลยีสารสนเทศในบริบทของการบูรณาการแบบ Value Chain integration และ การสร้างความร่วมมือ (Collaboration initiatives)

นอกจากนี้ ยังมีการจัดทำ Collaboration Protocal Profiles and Agreement (CPPA) ขึ้นมา อย่างไรก็ตาม ในเนเธอร์แลนด์ ก็ยังมีการผสมผสานในระบบ BPSS ร่วมกับการใช้โทรสาร และโทรศัพท์ เอกสารต่างๆก็ยังมีการใช้และมีความจำเป็น เนื่องจากในเนเธอร์แลนด์ ยังไม่มีการออกกฎหมายลายเซ็นดิจิตอล (digital signatures) นอกจากนี้ กฎหมายที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลตลอดจนการบูรณาการข้อมูลในกระบวนการยุติธรรมโดยตรงอยู่ระหว่างการดำเนินการ

2.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

เนเธอร์แลนด์ได้มีการพัฒนาและเร่งปรับปรุงในด้านกฎหมายด้านโทรคมนาคม และเทคโนโลยีสารสนเทศอย่างรวดเร็ว ในรอบทศวรรษที่ผ่านมาทั้งนี้ เนื่องจากเหตุผลและความจำเป็นจากความเจริญเติบโตทางด้านการค้าขายผ่านระบบเทคโนโลยีสารสนเทศ หรือ ระบบ e-commerce ประกอบกับการที่กลุ่ม EU ได้พัฒนาและสร้างต้นแบบทางกฎหมายซึ่งในรูปของอนุสัญญา และกฎระเบียบการดำเนินการที่เป็นต้นแบบ (model law) ที่เรียกว่า Directive

รูปแบบทางการค้าที่เนเธอร์แลนด์ได้ใช้และมีการปรับปรุงในการแลกเปลี่ยนข้อมูล คือ ระบบ EDI (ซึ่งแม้ว่าจะเริ่มจากการใช้เพื่อมุ่งหมายทางการค้า แต่ต่อมาก็ได้มีการนำมาใบ้ในการแลกเปลี่ยนข้อมูลระหว่างองค์กรต่างๆของรัฐ เช่นกัน) ทำให้เมื่อเดือนมีนาคม 2002 เนเธอร์แลนด์ได้ผ่านกฎหมาย Electronic Signature Act 2002 เพื่อช่วยในการรับรองการส่งข้อมูลและยืนยันข้อมูลตามเอกสารอิเลกทรอนิกส์ ทำให้เอื้อต่อทั้งระบบ e-Commerce และ e-Government ของรัฐ โดยก่อนหน้านี้ เนเธอร์แลนด์ มีกฎหมาย Electronic

Decree of 1998 หรือ รู้จักกันในนาม Dutch Telecom Law ออกมาใช้ก่อนแล้ว และยังมีกฎหมายอีกฉบับที่เอื้อต่อการทำธุรกรรมทางการค้า แต่กฎหมายฉบับนี้เอื้อต่อการทำธุรกรรมทางการค้า แต่กฎหมายฉบับนี้เป็นการอนุวัติการตาม Directive ของ EU ก็คือ The Distance Contract Act 2001 (EU ออก EU Distance Contract Directive มาเป็นต้นแบบ)

จากการที่เนเธอร์แลนด์เป็นประเทศที่ไม่ใหญ่มากนักและนโยบายการดำเนินการก็มุ่งที่การค้า ดังนั้น การดำเนินการด้านต่างๆ แม้กระทั่งการเชื่อมโยงและแลกเปลี่ยนข้อมูลก็จะมุ่งดำเนินการเพื่อสนับสนุนด้านการค้าเป็นหลักก่อน ในขณะที่การดำเนินการดังกล่าวก็จะส่งผลให้การเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างหน่วยงานอื่นๆสามารถกระทำได้สะดวกรวดเร็วมากยิ่งขึ้น เพราะรูปแบบการดำเนินการมาตรการต่างๆ (รวมทั้งมาตรการทางกฎหมาย) ก็สามารถนำมาปรับใช้ได้ในทำนองเดียวกัน

อย่างไรก็ตาม รัฐธรรมนูญของเนเธอร์แลนด์ มาตรา 7, 10 และ 13 ได้มีบทบัญญัติในการคุ้มครองความเป็นส่วนตัว และเสรีภาพในการแสดงความคิดเห็น กฎหมายป้องกันข้อมูลส่วนบุคคลจึงมีการตราออกมาใช้ เมื่อวันที่ 1 กันยายน 2001 เพื่อเสริมการรวบรวมข้อมูลทางอิเลกทรอนิกส์ (Electronic information gathering)

ในขณะที่กฎหมาย Telecommunication Act ได้มีผลออกมาบังคับใช้เมื่อ 19 พฤษภาคม 2004 อันเป็นการอนุวัติตาม EU directive on electronic communication และมีการนำเอาหลักการตาม Electronic Commerce Platform Netherland (E CP.NL) มาปรับใช้เช่นกัน

จากที่กล่าวมาจะเห็นข้อเท็จจริงว่า แม้จะเห็นว่า เนเธอร์แลนด์ จะมีการออกกฎหมายมาส่งเสริมการแลกเปลี่ยน เชื่อมโยงข้อมูลทางการค้า แต่บทบัญญัติเหล่านั้น ก็สามารถนำมาปรับใช้กับการแลกเปลี่ยนเชื่อมโยงและการบูรณาการข้อมูลในกระบวนการยุติธรรมได้ ซึ่ง เนเธอร์แลนด์กำลังอยู่ในระหว่าง การกระตือรือล้นที่จะดำเนินการ

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายการคุ้มครองข้อมูลส่วนบุคคลของเนเธอร์แลนด์ เกิดขึ้นจากอิทธิพลของ EU Directive เช่นกัน โดยเนเธอร์แลนด์ นำ Directive ดังกล่าว มาอนุวัติเป็นกฎหมาย Data Protection Act 1995[74] ซึ่งเป็นกฎหมายที่เกิดปัญหาการปรับใช้พอสมควร

[74] J.M.A. Berkvens and J.E.J. Prins “De bescherming van persoonsgegevens: van WPR naar WBP, Recht en computer Deventer 1997 pp. 315-369

เนื่องจาก แนวคิดเรื่อง ข้อมูลส่วนบุคคลกับข้อมูลที่เป็นกลุ่มบุคคลระหว่างที่หน่วยงานต่างๆ จัดเก็บเพื่อเปรียบเทียบในฐานข้อมูล (databank) ที่เจ้าหน้าที่ต้องตรวจสอบเปรียบเทียบโดยการเรียกข้อมูลที่เก็บอยู่จาก file อื่นๆ กลับถูกปกปิด เช่น สำนักงานอัยการต้องการทราบประวัติในการกระทำผิดซ้ำ และพฤติกรรมการกระทำผิดของนาย ก. แต่ไม่สามารถเรียกตรวจสอบจากฐานข้อมูลของตำรวจ หรือราชทัณฑ์ได้ เพราะเมื่อเข้าไปจะถูก block เนื่องจากเป็นข้อมูลส่วนบุคคล ทำให้ต้องมีหนังสือติดต่อไปยังหน่วยงาน ซึ่งทำให้ล่าช้า หรืออาจต้องมีการขออนุมัติจากรมต.ว่าการกระทรวงยุติธรรมก่อน ปัญหาเหล่าสี้ได้มีการยกขึ้นมาอภิปรายกันว่า แม้ว่าเนเธอร์แลนด์จะพัฒนาเทคโนโลยีสารสนเทศก้าวหน้าแต่ก็จะประสบปัญหาจากด้านการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

ในปี 1980 จนถึงต้นปี 1990 ได้เกิดข้อสงสัยอย่างยิ่งว่ากฎหมายลิขสิทธิ์ของเนเธอร์แลนด์ที่มีอยู่จะสามารถปรับใช้ได้กับโปรแกรมคอมพิวเตอร์ (Computer Software) ได้หรือไม่ รวมถึงฐานข้อมูล (Database) ด้วย ในการตรากฎหมายของเนเธอร์แลนด์ได้มีการนำเอา European Software Directive มาปรับใช้ตั้งแต่ยังเป็นร่างเพื่อคุ้มครองฐานข้อมูล อย่างไรก็ตาม ประเด็นหลักของคำถาม ยังอยู่ที่ว่า แนวคิดเรื่องลิขสิทธิ์ในกฎหมายเดิมจะสามารถนำมาปรับใช้กับฐานข้อมูล และการส่งข้อมูลทางอิเลคโทรนิคส์ได้หรือไม่ ซึ่งในทางปฏิบัติการนำเอาหลักของสิทธิในการทำซ้ำ (reproduction rights) มาใช้ได้หรือไม่ โดยเฉพาะกับการดำเนินการในระบบดิจิตอล ต่อมาในปี 1996 มีการศึกษาและมีการเสนอให้ยกเลิกสิทธิในการทำซ้ำว่าเป็นการใช้สิทธิในการแสวงหาประโยชน์[75]

นอกจากประเด็นดังกล่าวแล้วก็ยังมีการหยิบยกในเรื่อง domain names ขึ้นมาอภิปราย พร้อมกับประเด็นในเรื่องของปัญหาด้านเครื่องหมายการค้า

ในที่สุดก็ได้ข้อสรุปว่า ประเด็นปัญหาเกิดจากการที่จะจำแนกงานต่างๆว่าเข้าข่ายการคุ้มครองในระบบลิขสิทธิ์หรือไม่ การนำเอาแนวทาง European Council Directive มาปรับใช้ทำให้กฎหมายลิขสิทธิ์ของเนเธอร์แลนด์มีความยืดหยุ่นและครอบคลุมการดำเนินการเชื่อมโยง แลกเปลี่ยนและบูรณาการฐานข้อมูล ดังนั้น กฎหมายลิขสิทธิ์ของเนเธอร์แลนด์ จึงถือได้ว่ามีบทบัญญัติที่สามารถนำมาปรับใช้ได้กับการแลกเปลี่ยน และบูรณาการข้อมูลในกระบวนการยุติธรรมของเนเธอร์แลนด์ได้ โดยถือว่า ฐานข้อมูลด้านงานยุติธรรมที่เกิดจากการบูรณาการมีลิขสิทธิ์ในส่วนที่มีการดำเนินการขึ้นมาใหม่

---

[75] D.J.G. Visser Auteurstech op toegang's – gravenhage 1997

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิดของเนเธอร์แลนด์เกิดขึ้นจากการที่เดิมในเดือนพฤศจิกายน 1985 กระทรวงยุตะรรมเนเธอร์แลนด์ได้มีการตั้งคณะกรรมการขึ้นมาตรวจสอบประมวลกฎหมายอาญาและประมวลกฎหมายวิธีพิจารณาความอาญาว่ามีบทบัญญัติที่จะสามารถนำมาปรับใช้กับการใช้เทคโนโลยีทางคอมพิวเตอร์หรือไม่ ซึ่งคณะกรรมการได้มีการรายงานผลว่าไม่สามารถปรับใช้ได้โดยเฉพาะอย่างยิ่ง ในกรณีของการประกอบอาชญากรรมคอมพิวเตอร์ ดังนั้นในปี 1991 ได้มีการตรากฎหมาย Computer Crime Act 1991 ออกมาใช้[76] โดยในกฎหมายดังกล่าวมีการกำหนดลักษณะและประเภทของการประกอบอาชญากรรม การใช้อินเตอร์เน็ตโดยองค์กรอาชญากรรมและการโฆษณาภาพลามกอนาจารทางอินเตอร์เน็ต

10) ประเทศสิงคโปร์

1.การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

รัฐบาลสิงคโปร์ให้ความสำคัญกับการใช้เทคโนโลยีสารสนเทศสูงมากทั้งสำหรับการทำงานภายในหน่วยงานภาครัฐและงานบริการประชาชน การใช้ประโยชน์ของเทคโนโลยีสารสนเทศที่มีประสิทธิภาพสามารถทำให้การทำงานหลายอย่างเป็นไปได้โดยอัตโนมัติ ทำให้เกิดการใช้ทรัพยากรร่วมกันในหน่วยงาน และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทำได้ง่ายขึ้น รัฐบาลสิงคโปร์ได้กำหนดโปรแกรมประยุกต์มาตรฐาน (Government – Wide applications) สำหรับการทำงานของหน่วยงานในภาครัฐขึ้นหลายโปรแกรมด้วยกัน อาทิ เช่น SGEMS E-mail และ Lotus Notes สำหรับการสื่อสารทางอิเล็กทรอนิกส์เมลม PAC@gov ซึ่งเป็นโปรแกรมสำหรับการทำเรื่องเบิกจ่ายเงินค่าเดินทางของบุคลากร รัฐบาลสิงคโปร์มีการใช้บริการระบบเครือข่ายกลางด้วยเช่นเดียวกัน (Government Intranet) ระบบดังกล่าวจะถูกแยกออกจากระบบเครือข่ายสาธารณะ (Internet) เพื่อให้สามารถให้การบริการได้อย่างมีประสิทธิภาพและปลอดภัย นอกจากนี้แต่ละกระทรวงภายในประเทศยังมีการวางมาตรฐาน (Ministry-wide applications) สำหรับการเลือกใช้โปรแกรมประยุกต์เช่นเดียวกัน

---

[76] Corien Prins **Information and Communication Technology : An Overview of Key Regulations and Strategies in The Netherland.**

หน่วยงานหลักที่ทำหน้าที่ควบคุมดูแลและให้คำปรึกษาเกี่ยวกับเทคโนโลยีต่างๆมีชื่อว่า Infocomm Development Authority of Singapore หรือ IDA หน่วยงานดังกล่าวมีความรับผิดชอบในการให้บริการทางด้านสารสนเทศแก่หน่วยงานอื่นๆในภาครัฐ รวมถึงการวางมาตรฐานและแนวทางต่างๆ เช่น ระบบงานในการพัฒนาโปรแกรมที่เหมาะสม มาตรฐานการแลกเปลี่ยนข้อมูล โปรแกรมประยุกต์ ระบบเครือข่ายรวมไปถึงเทคโนโลยีของเซิร์ฟเวอร์ ซึ่งมาตรฐานต่างๆเหล่านี้จะส่งผลให้การบูรณาการข้อมูลทำได้ง่ายขึ้น

การทำงานของเกือบทุกหน่วยงานในกระบวนการยุติธรรมอาศัยเทคโนโลยีสารสนเทศอย่างกว้างขวาง รวมถึงการติดตามความก้าวหน้าของงานผู้ใต้บังคับบัญชา การอ่านเอกสารเวียนในหน่วยงาน หรือการอ่านทบทวนเอกสารคดีต่างๆไปจนถึงการอ่านบันทึกการประชุมของผู้มีสิทธ์

การเชื่อมโยงระบบข้ามหน่วยงาน เช่น การเชื่อมโยงฐานข้อมูลหรือการเข้าถึงระบบจากทางไกลที่ไม่ปรากฏในหน่วยงานกระบวนการยุติธรรม การแลกเปลี่ยนข้อมูลข้ามหน่วยงานเกิดขึ้นได้ 2 วิธี คือ การส่งข้อมูลเป็นตัวอักษร (Text) ผ่านระบบเครือข่ายของรัฐโดยอาศัยเทคโนโลยี FTP (File Transfer Protocol) และ การอนุญาตให้บุคลากรบางคนเข้าถึงระบบโดยตรงในแบบจำกัดสิทธิการปรับปรุงข้อมูล (Update) ข้ามหน่วยงานให้ทันสมัยนั้นสามารถทำได้ในช่วงเวลาตามที่หน่วยงานกำหนด เช่น ทุกเย็นหรือทุก 2 วัน เป็นต้น การตรวจสอบบุคคลทำได้โดยใช้ข้อมูลเลขประจำตัวประชาชนข้อมูลรหัสผ่าน และข้อมูลลายนิ้วมือ

2.ฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

ในปี 1998 รัฐสภาสิงคโปร์ได้ออกมาตรการชัดเจนที่เกี่ยวข้องกับระบบ ISP เพื่อให้มีความรับผิดทั้งทางแพ่งและทางอาญาภายใต้มาตรา 10 ของกฎหมาย Electronic Transactions Act 1998 ซึ่งมีข้อความระบุว่า

10. ---(1)--- ผู้ที่ให้บริการเครือข่ายจะได้รับการยกว้นความรับผิดทั้งทางแพ่งและทางอาญาภายใต้หลักนิติธรรม หาก ข้อมูลที่ถูกเก็บไว้ในรูปข้อมูลอิเลคโทรนิกส์ ได้มีการให้บริการเพียงแต่

(1) การจัดทำ การตีพิมพ์เผยแพร่ การแจกจ่าย กระจาย

(2) ไม่กระทบหรือรอนสิทธิจากการใช้

ข้อความในกฎหมายตามบทบัญญัติมาตรานี้จะไม่มีผลใช้บังคับหาก

(ก) มีการกำหนดหน้าที่ไว้แล้วตามสัญญา

(ข) หน้าที่ในการให้บริการแก่เครือข่าย ภายใต้การอนุญาต หรือภายใต้กฎระเบียบที่มีการตราไว้ เป็นลายลักษณ์อักษร

(ค) หน้าที่ที่ได้มีการระบุไว้ตามกฎหมายอย่างชัดแจ้ง หรือ โดยคำสั่งศาลให้มีการถอน ป้องกัน หรือการปฏิเสธการเข้าถึงข้อมูล

บทบัญญัติดังกล่าว เป็นบทบัญญัติที่ส่งเสริมต่อการแลกเปลี่ยน เชื่อมโยง และบูรณาการข้อมูลจากฐานข้อมุลใดๆ เพราะหากการเชื่อมโยงนั้นมีการจัดทำและส่งต่อแลกเปลี่ยนข้อมูล ระหว่างหน่วยงานตามปกติ โดยมิได้มีการบิดเบือน หรือ เปลี่ยนแปลงใดๆ จากข้อมุลที่จัดเก็บ หรือ แลกเปลี่ยน หรือ หากการแลกเปลี่ยน เชื่อมโยงข้อมูลที่เกิดขึ้นไม่ไปกระทบกระเทือน หรือรอนสิทธิของผู้อื่นๆ

ดังนั้น จากกฎหมายฉบับดังกล่าว หากมีการเชื่อมโยง แลกเปลี่ยน หรือบูรณาการข้อมูลในกระบวนการยุติธรรม โดยมีการแลกเปลี่ยนเหล่านั้น ไม่ได้กระทบกระเทือนรอนสิทธิ หรือ ก่อความเสียหายแก่ผู้ใด ก็ไม่ต้องรับผิดชอบทั้งทางแพ่งและทางอาญา

3.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

รัฐธรรมนูญของสิงคโปร์นั้นมีรากฐานที่มาจากกฎหมายของอังกฤษที่ไม่มีบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลและสิทธิส่วนบุคคล ศาลสูงของสิงคโปร์ได้เคยตีความว่าข้อมูลส่วนบุคคลจะได้รับการคุ้มครองตามหลัก Duty of Confidence ดังนั้นการปกป้องและคุ้มครองข้อมูลส่วนบุคคลในสิงคโปรจึงไม่ได้มีการบัญญัติกฎหมายไว้เพื่อการนี้โดยตรง ทั้งๆที่เรื่องการคุ้มครองข้อมูลส่วนบุคคลนี้ได้เคยถูกหยิบยกมาเป็นประเด็นในการอภิปรายมาแล้วเป็นเวลานานถึง 12 ปี แต่อย่างไรก็ตาม คณะกรรมการ The National Internet Advisory Committee ได้มีการเสนอทางออกให้ดดยการเสนอให้มีการออก Model Data Protection Code for the Private Sector ในเดือนกุมภาพันธ์ 2002 ซึ่งต่อมาจากความจำเป็นดังกล่าวจึงมีการออกกฎหมายมาใช้ก่อนคือE-Commerce Code for the Protection of Personal Information and Communication of Consumers of Internet Commerce อย่างไรก็ตามกฎหมายดังกล่าวก็มีเป้าหมายในการสนับสนุนการดำเนินการในเชิงธุรกิจเท่านั้น แม้ว่าจะสามารถนำมาปรับใช้ได้กับการดำเนินการในการเชื่อมโยงข้อมูลที่ต้องมีการรักษาข้อมูลส่วนบุคคลก็ตาม

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

กฎหมายลิขสิทธิ์ของสิงคโปรคือ The Copyright Act 1987 ได้ออกมาโดยยึดแนวทางคล้ายกับประเทศอื่นๆโดยทั่วไป ต่อมาจากการพัฒนาทางด้านเทคโนโลยีสารสนเทศ ได้มีการปรับปรุงแก้ไขใหม่ถึง 3 ครั้ง คือ ในปี1994 1998 และ1999 โดยมีการแก้ไขให้ครอบคลุมการคุ้มครองการสร้างและการออกแบบhardward โดยที่หากมีการทำLayout Design ตามกฎหมายแล้ว(15 กุมภาพันธ์ 1999) ก็จะได้รับการคุ้มครองตั้งแต่ 5-15 ปี หลังจากการสร้างสรรงานและอาจได้รับการตีความตามหลักe-patent อันเป็นแบบสำหรับการให้ความคุ้มครองสิทธิบัตรในฐานข้อมูลได้

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

สิงคโปร์ได้ตรากฎหมายต่อต้านการใช้คอมพิวเตอร์ในทางที่ผิดขึ้นมาใช้ในปี ค.ศ.1993 เนื่องจากนโยบายเดิมของรัฐบาลสิงคโปร์ที่ต้องการให้ประเทศสิงคโปร์เป็น “intelligent island” ที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศ ในเอเชียและยังทำเครือข่ายกับสหรัฐอเมริกา เพื่อให้มีการพัฒนาเทคโนโลยีในระดับแนวหน้า สิงคโปร์ยังได้พัฒนากฎหมายขึ้นมารองรับการค้าทางเทคโนโลยีสารสนเทศ ต่อมาในปี 1998 ก็ได้มีการปรับปรุงแก้ไขกฎหมาย Computer Misuse Act 1993[77] โดยมีการขยายขอบข่ายความรับผิดมากยิ่งขึ้น เดิมกฎหมายฉบับนี้มุ่งดำเนินการในการเอาผิดกับพวกที่มุ่งเจาะระบบข้อมูลคอมพิวเตอร์ (hacking) แต่การแก้ไข ในมาตรา 7 ให้ครอบคลุมการ Spamming และการ mail bombing โดยมาตรา 7 ระบุว่า

7 (1) ผู้ใดรู้ ควรจะรู้ และปราศจากอำนาจหรือกระทำโดยผิดกฎหมายในลักษณะต่อไปนี้

(ก) แทรกแซง ขัดขวาง หรือ กระทำการใดๆอันเป็นการใช้ในทางที่ผิดกฎหมายต่อคอมพิวเตอร์

(ข) ขจัด หรือ ขัดขวางการเข้าถึง หรือการใช้ประโยชน์ หรือ การทำให้เกิดผลแก่ข้อมูลหรือโปรแกรมใดๆในคอมพิวเตอร์

กฎหมายป้องกันการกระทำผิดในการใช้คอมพิวเตอร์ในทางที่ผิดของสิงคโปร์นี้ เป็นกฎหมายที่มีลักษณะกึ่งทางแพ่งและทางอาญา คือ มีบทบัญญัติการลงโทษทั้งทางแพ่งและอาญา บางครั้งจะเรียกกฎหมายฉบับนี้ว่า “Cyber-Trepass” ปัญหาสำคัญอยู่ที่การตีความอย่างชัดเจน ถึงว่า การบุกรุก (trepass), มีได้ทั้งการบุกรุกทางกายภาพ และการบุกรุกทางอิเลคโทรนิกส์ และสิงคโปร์ก็มุ่งที่จะออกกฎหมายเกี่ยวกับความรับผิดด้าน ISP.

---

77 Dan Mc Donald “Internet computer network law and legislation **Singapore Law** Vol.9 No.1 (March 2002) P.9

11) ประเทศไทย

1. การเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

ปัจจุบัน หน่วยงานในกระบวนการยุติธรรมที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานมีทั้งสิ้น 14 หน่วยงาน ได้แก่ ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติ กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน กรมบังคับคดี สถาบันนิติวิทยาศาสตร์และกรมคุ้มครองสิทธิและเสรีภาพ แต่หน่วยงานเหล่านั้นก็ยังมีการเชื่อมโยงข้อมูลและการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องในการปฏิบัติงานน้อยมาก ทั้งทั้งที่มีความต้องการในการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

ปัญหาและอุปสรรคของการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลสารสนเทศในกระบวนการยุติรรมที่พบได้แก่ การขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม ขาดการดำเนินการอย่างจริงจังและต่อเนื่อง ประกอบกับการเปลี่ยนแปลงรัฐบาลที่ทำให้การพัฒนากระบวนการยุติธรรมของประเทศดำเนินไปอย่างล่าช้า ซึ่งก็ส่งผลกระทบต่อการใช้เทคโนโลยีสารสนเทศด้วย ในการดำเนินการยังขาดหน่วยงานที่เป็นเจ้าภาพหลักในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการประมวลผล ผู้บริหารระดับสูงยังไม่ให้ความสำคัญเท่าที่ควร ปัญหาด้านงบประมาณก็มีส่วนสำคัญ การมองว่างานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน ขาดความพร้อมทางด้านอุปกรณ์ต่างๆ ขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน

ด้านปัญหาการเก็บรวบรวมข้อมูลที่มีความซับซ้อนนั้น ปัญหานี้มีสาเหตุจากการที่แต่ละหน่วยงานจะจัดเก็บกันเอง โดยมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ต่างฝ่ายต่างจัดเก็บ ก็ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก เพราะยังขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ส่งผลตามมาทำให้ข้อมูลมีความน่าเชื่อถือน้อย เพราะมีข้อมูลจำนวนมากที่ขาดการปรับปรุง เปลี่ยนแปลง ข้อมูลให้เป็นปัจจุบัน จัดเก็บแล้วก็ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน

ส่วนปัญหาหลักอื่นๆก็คือ การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ ซึ่งก็ส่งผลให้หลายๆหน่วยงานจึงขาดความพร้อม เพื่อการบูรณาการ

กระทรวงยุติธรรมได้จัดทำแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติขึ้นซึ่งจากแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551) ที่ได้มีการกำหนดยุทธศาสตร์การดำเนินงานด้านเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม 6 ยุทธศาสตร์ คือ

ยุทธศาสตร์ที่ 1 : การพัฒนาและบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 3 : การพัฒนาเครือข่ายเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 4 : การพัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 5 : การพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 6 : การพัฒนากฎหมาย ระเบียบ ข้อบังคับให้สอดคล้องต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

โดยที่ในแต่ละยุทธศาสตร์ได้มีแผนการดำเนินการและโครงการต่างๆรองรับและอยู่ระหว่างการดำเนินการซึ่งหากเป็นไปตามกำหนดการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรมจะปรากฏผลที่เป็นรูปธรรมชัดเจนและเอื้อประโยชน์แก่หน่วยงานในกระบวนการยุติธรรมในการดำเนินการตามภารกิจและเป้าหมายอื่นๆให้สัมฤทธิ์ผลต่อไป

2. กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรมมีทั้งกฎหมายที่เป็นอุปสรรคและกฎหมายที่เอื้อต่อการเชื่อมต่อและการแลกเปลี่ยนข้อมูล แต่โดยภาพรวมมีกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศดังนี้

กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศนั้น อาจกล่าวได้ว่า กฎหมายทุกฉบับเกี่ยวข้องหมดแต่การจะปรับใช้กฎหมายฉบับใดนั้น ขึ้นอยู่กับว่าธุรกรรมที่เกิดขึ้นอยู่ภายใต้การควบคุมของกฎหมายฉบับใด อย่างไรก็ตาม ในส่วนที่เกี่ยวกับเทคโนโลยีสารสนเทศ อาจมีประเด็นข้อกฎหมายอื่นที่นำมาพิจารณา ดังนี้

1. กฎหมายระหว่างประเทศในส่วนที่เกี่ยวกับกฎหมายขัดกัน (Conflicts of Law) และขอบเขตอำนาจพิจารณาคดีของศาล (Jurisdiction) เนื่องจากในโลกของเทคโนโลยีสารสนเทศนั้นไม่มีพรมแดน การทำธุรกิจบนอินเทอร์เน็ต จึงเหมือนเป็นการทำธุรกิจกับคนทั้งโลก ดังนั้น เมื่อเกิดข้อพิพาท ปัญหาโดยจะนำกฎหมายของประเทศใดมาบังคับใช้ และศาลประเทศใดมีเขตอำนาจพิจารณาคดี ศาลประเทศที่เครื่องคอมพิวเตอร์เซิร์ฟเวอร์ตั้งอยู่ หรือศาลในประเทศที่คู่สัญญามีภูมิลำเนา ศาลในประเทศที่มีประเทศที่มีการชำระหนี้ตามสัญญาล้วนแล้วแต่เป็นปัญหา ข้อกำหนดและเงื่อนไข (Terms & Condition) ในเว็บไซต์ จึงมีความสำคัญมากและควรระบุไว้ในเว็บไซต์

2. กฎหมายว่าด้วยการเกิดของสัญญา ลายมือชื่ออิเล็กทรอนิกส์ ที่ระบุว่าสัญญาเกิดขึ้นเมื่อใด ความรับผิดทางกฎหมายเป็นอย่างไร เช่น ประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยนิติกรรมสัญญา พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ หรือกฎหมายที่เกี่ยวข้องกับสัญญาแต่ละประเภท

3. กฎหมายที่เกี่ยวกับการคุ้มครองผู้บริโภค เช่น พ.ร.บ.คุ้มครองผู้บริโภค พ.ร.บ.ว่าด้วยข้อสัญญาที่ไม่เป็นธรรม เป็นต้น กฎหมายในส่วนนี้เกี่ยวข้องกับสัญญาและข้อกำหนดเงื่อนไขประเภท Click wrap Agreement โดยกำหนดข้อสัญญาดังกลาวมีผลบังคับใช้เพียงใด

4. กฎหมายทรัพย์สินทางปัญญา เช่น พ.ร.บ.ลิขสิทธิ์ พ.ร.บ.เครื่องหมายการค้า พ.ร.บ.แบบวงจรรวม (ร่าง) พ.ร.บ.ความลับทางการค้า กฎหมายส่วนนี้มีความสำคัญอย่างมาก เพราะมุ่งคุ้มครองข้อมูล รูปภาพต่าง ๆ บนอินเทอร์เน็ต การทำลิงค์ประเภทต่าง ๆ ชื่อโดเมนแนวคิดทางธุรกิจ (Business Method) ฯลฯ

5. กฎหมายอาญาที่เกี่ยวกับความรับผิดของบุคคลที่เป็นสื่อกลางในการให้บริการอินเทอร์เน็ต (Intermediaries) เช่น ความผิดฐานหมิ่นประมาท การพนัน สื่อลามก อนาจาร ฯลฯ

6. กฎหมายภาษีอากร เช่น ปัญหาการจัดเก็บภาษีผ่านสื่ออิเล็กทรอนิกส์ การออกใบกำกับภาษี ปัญหาเรื่องสินค้าไม่มีรูปร่างที่ดาวน์โหลดผ่านอินเทอร์เน็ต อนุสัญญาภาษีซ้อนระหว่างประเทศไทยกับประเทศต่าง ๆ

7. กฎหมายว่าด้วยการโอนเงินผ่านสื่ออิเล็กทรอนิกส์ เช่น พ.ร.บ. ธนาคารพาณิชย์ พ.ร.บ.ธนาคารแห่งประเทศไทยพร้อมหลักเกณฑ์ในเรื่องต่าง ๆ ร่าง พ.ร.บ. การโอนเงินอิเล็กทรอนิกส์ ฯลฯ

8. กฎหมายว่าด้วยการเงิน เช่น พ.ร.บ.หลักทรัพย์และตลาดหลักทรัพย์ ประกาศของ ก.ล.ต. หรือประกาศของตลาดหลักทรัพย์ ฯลฯ

9. กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และพยานหลักฐาน เช่น ร่าง พ.ร.บ.อาชญากรรมทางคอมพิวเตอร์ ประมวลกฎหมายอาญา ประมวลกฎหมายวิธีพิจารณาความอาญา

10. กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อคุ้มครองข้อมูลลูกค้าหรือข้อมูลส่วนบุคคลและการใช้โปรแกรมคุ้กกี้ เช่น ร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล กฎหมายรัฐธรรมนูญ ประมวลกฎหมายแพ่งและพาณิชย์

11. กฎหมายว่าด้วยการแข่งขันทางการค้า เช่น กรณีของบริษัทไมโครซอฟท์ ที่ผูกขาดการใช้โปรแกรมเบราเซอร์ (Internet Explorer)

การพัฒนากฎหมายเทคโนโลยีสารสนเทศ (Information Technology Law) หรือ กฎหมายไอที (IT Law) ในประเทศไทย เริ่มตั้งแต่ช่วงที่รัฐบาลผลักดันนโยบายไอที 2000 และหน่วยงานที่ได้รับมอบหมายให้ทำหน้าที่เป็นเลขานุการในการพัฒนา คือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติหรือเนคเทค

สำหรับกฎหมายไอทีชุดแรกที่มีการพัฒนา ได้แก่ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับลายมือชื่อทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายลำดับรองของรัฐธรรมนูญ มาตรา 78 ว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน

กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์รวมเข้ากับกฎหมายลายมือชื่ออิเล็กทรอนิกส์ใช้บังคับเมื่อปี 2544 สำหรับกฎหมายฉบับอื่น ๆ ยังอยู่ในขั้นตอนของการเสนอกฎหมายหรือยกร่าง ความมุ่งหมายของการออกกฎหมายเหล่านั้น มีดังนี้

1.กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law)

กฎหมายนี้มีเป้าหมายคือเพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

2.กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures Law)

กฎหมายนี้มีเป้าหมายเพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้บริการอื่นที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

3.กฎหมายที่เกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน(National Information Infrastructure Law)

กฎหมายฉบับนี้เป็นกฎหมายลำดับรองของรัฐธรรมนูญมาตรา 78 เพื่อก่อให้เกิดการส่งเสริม สนับสนุน และพัฒนาโครงสร้างพื้นฐานสารสนเทศ อันได้แก่ โครงข่ายโทรคมนาคมเทคโนโลยีสารสนเทศ สารสนเทศ ทรัพยากรมนุษย์ และโครงสร้างพื้นฐานของรัฐ ซึ่งรองรับเจตนารมณ์สำคัญประการหนึ่งของแนวนโยบาย พื้นฐานแห่งรัฐตามรัฐธรรมนูญมาตรา 78 ในการกระจายสารสนเทศให้ทั่วถึงและเท่าเทียมกัน และนับเป็นกลไกสำคัญในการช่วยลดความเหลื่อมล้ำของสังคมอย่างค่อยเป็นค่อยไป เพื่อสนับสนุนให้ท้องถิ่นมีศักยภาพในการปกครองตนเอง พัฒนาเศรษฐกิจภายในชุมชน และนำไปสู่สังคมแห่งปัญญาและการเรียนรู้

4.กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)

เพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผลเปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็ว โดย

อาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

5.กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law)

กฎหมายฉบับนี้ออกมาเพื่อกำหนดมาตรการทางอาญาในการลงโทษผู้กระทำผิดต่อระบบการทำงานคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ซึ่งในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายฉบับใด กำหนดว่าเป็นความผิด ทั้งนี้ เพื่อเป็นหลักประกันสิทธิเสรีภาพและการคุ้มครองการอยู่ร่วมกันของสังคม

อย่างไรก็ตาม เพื่อให้เกิดความชัดเจนในประเด็นที่เกี่ยวข้องกับการศึกษา จึงจำแนกกฎหมาย ระเบียบและข้อกำหนดต่างๆที่เกี่ยวข้องออกเป็นกลุ่มดังต่อไปนี้ต่อไปนี้

ก.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม:กฎหมายที่เป็นอุปสรรคต่อการเชื่อมต่อและการแลกเปลี่ยนข้อมูล มีดังนี้

1.ระเบียบการตำรวจเกี่ยวกับคดี

ในระเบียบการตำรวจเกี่ยวกับคดีลักษณะ 12 รายงานประจำวัน ข้อ 377 ห้ามบุคคลภายนอกอ่าน หรือคัดลอกข้อความใดๆ จากรายงานประจำวัน เว้นไว้แต่ผู้แจ้งความต้องการจะขอดู หรือสำเนาข้อความที่แจ้งไว้จากรายงานประจำวันไว้เป็นหลักฐาน ก็ให้ผู้มีตำแหน่งตั้งแต่หัวหน้ากิ่งสถานีตำรวจ หรือหัวหน้าสถานี หรือผู้รักษาการแทนในตำแหน่งนั้นๆ ซึ่งเป็นนายตำรวจชั้นสัญญาบัตรแล้วแต่กรณีเป็นผู้พิจารณาอนุญาต

ระเบียบการตำรวจเกี่ยวกับคดี รายงานประจำวันโดยหลักแล้วจะถือว่าเป็นความลับของราชการจะไม่เปิดเผยแก่บุคคลภายนอก เว้นแต่ผู้แจ้งความต้องการจะขอตรวจดู ซึ่งในที่นี้หมายความถึงการตรวจสอบว่าคำให้การของตนถูกต้องตรงกับที่ได้แจ้งไว้และพนักงานสอบสวนหรือผู้รับแจ้งรายงานประจำวันจัดถูกต้องหรือไม่เท่านั้น ชั้นพนักงานสอบสวนผู้เสียหายมีสิทธิที่จะตรวจคำให้การของตน ซึ่งสิทธิดังกล่าวพนักงานสอบสวนจะไม่แจ้งให้ผู้เสียหายทราบถึงสิทธิในส่วนนี้ ซึ่งทำให้ผู้เสียหายที่ไม่มีความรู้ หรือไม่ทราบถึงระเบียบนี้ก็จะไม่ได้ตรวจสอบคำให้การของตนว่าถูกต้องตรงกับที่แจ้งไว้หรือไม่

แม้ว่าการเปิดเผยอาจจะทำให้การทำงานของพนักงานสอบสวนเป็นไปด้วยความยากลำบาก เนื่องจากพยานหลักฐานบางส่วนอาจถูกทำลาย ดังนั้น การเปิดเผยข้อมูลในสำนวนคดีจึงต้องกระทำด้วยความระมัดระวังเพื่อความสงบเรียบร้อยของสังคมและเป็นการคุ้มครองความปลอดภัยของพยานบุคคลด้วยเพื่อให้พยานไม่มีความรู้สึกว่าเข้ามามีส่วนร่วมในคดีจะก่อให้เกิดอันตรายต่อชีวิตหรือครอบครัว

2.ระเบียบสำนักงานอัยการสูงสุด

ในคดีอาญาเมื่อพนักงานอัยการมีคำสั่งเด็ดขาดไม่ฟ้องคดีแล้ว ผู้เสียหายมีสิทธิขอทราบสรุปพยานหลักฐาน พร้อมความเห็นของพนักงานสอบสวนและพนักงานอัยการในการสั่งคดี เพื่อให้ผู้เสียหายได้ตรวจสอบว่าการสั่งไม่ฟ้องคดีของพนักงานอัยการให้เหตุผลว่าอย่างไร ซึ่งถ้าตนเองเห็นว่าคดีของตนมีพยานหลักฐานเพียงพอในการที่จะนำตัวผู้กระทำความผิดมาลงโทษก็สามารถที่จะนำคดีนั้นมาฟ้องต่อศาลได้

แม้จะมีระเบียบของสำนักงานอัยการว่าด้วยการดำเนินคดีว่าให้ผู้เสียหายขอตรวจสำนวนคดีได้ก็ตาม แต่ในทางปฏิบัติหัวหน้าพนักงานอัยการก็จะไม่อนุญาตให้เปิดเผยสำนวนคดีให้ทราบ เพราะถือว่าเป็นความลับของทางราชการ โดยอ้างว่าเปิดเผยจะทำให้การใช้กฎหมายเสื่อมประสิทธิภาพตามข้อยกเว้นของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ข้อยกเว้นตามพระราชบัญญัติข้อมูลข่าวสารของราชการ มาตรา 15 (2) จะมีการยกขึ้นกล่าวอ้างกันอยู่บ่อยครั้ง โดยมิได้อธิบายถึงการไม่เปิดเผยข้อมูลดังกล่าว ทำให้ผู้ขอเปิดเผยข้อมูลหรือสำนวนคดีไม่เข้าใจว่าเมื่อมีการเปิดเผยสำนวนคดีดังกล่าวแล้วจะทำให้การใช้กฎหมายเสื่อมประสิทธิภาพอย่างไร

นอกจากนี้เรายังพบปัญหาอีกประการ คือ ประมวลกฎหมายวิธีพิจาณาความแพ่งและวิธีพิจารณาความอาญา ไม่มีบทบัญญัติรองรับเรื่องการรับฟังพยานหลักฐานคอมพิวเตอร์ ซึ่งเป็นหลักฐานชิ้นสำคัญในการพิสูจน์การกระทำผิดต่อข้อมูลส่วนบุคคลโทษฐานละเมิดได้ จะมีก็เพียงพระราชบัญญัติจัดตั้งศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ (ข้อ 33 – 36) และข้อกำหนดคดีล้มละลาย พ.ศ. 2542 (ข้อ 18 – 22) ระบุให้รับฟังพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งจะกล่าวต่อไปในส่วนกฎหมายทีเอื้ออำนวยต่อการเชื่อมต่อและการแลกเปลี่ยนข้อมูลต่อไป

ข.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม:กฎหมายทีเอื้ออำนวยต่อการเชื่อมต่อและการแลกเปลี่ยนข้อมูล มีดังนี้

1.ระเบียบสำนักงานอัยการสูงสุด

สำนักงานอัยการสูงสุด ในฐานะผู้ที่ทำหน้าที่ดำเนินคดีอาญาให้กับรัฐจึงได้ออกระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ (ฉบับที่ 7) พ.ศ. 2545 ซึ่งก่อนมีการแก้ไขระเบียบมาจนถึงปัจจุบันก็ได้มีการบัญญัติไว้ในข้อ 19 และข้อ 20 ซึ่งมีรายละเอียดดังนี้

ข้อ 19 (การยืมหรือคัดสำเนา)

การยืม หรือคัดสำเนาการสอบสวนให้ดำเนินการได้ดังต่อไปนี้

1) สำนวนการสอบสวนคดีที่เสร็จเด็ดขาดแล้ว หากพนักงานสอบสวนหรือส่วนราชการที่เกี่ยวข้อง ประสงค์จะขอยืมหรือขอคัดค้านสำเนาสำนวนทั้งหมดหรือบางส่วนไปเพื่อใช้ประโยชน์ในราชการแล้ว ให้หัวหน้าพนักงานอัยการอนุญาตให้ยืมหรือให้คัดสำเนาไปได้

2) สำนวนการสอบสวนคดีที่ยังไม่เสร็จเด็ดขาด หากผู้เกี่ยวข้องประสงค์จะขอยืมหรือคัดสำเนาสำนวนทั้งหมดหรือบางส่วนเพื่อใช้ประโยชน์ในราชการแล้ว ให้หัวหน้าพนักงานอัยการพิจารณา หากเห็นว่าไม่เป็นการขัดข้องหรือเสียหายแก่การดำเนินคดี ให้อนุญาตให้ยืมหรือคัดสำเนาไปได้

3) สำนวนการสอบสวนที่อยู่ในระหว่างการพิจารณาของพนักงานอัยการ หากปรากฏแก่พนักงานสอบสวนว่าได้จับกุมผู้ต้องหาผิดตัว และพนักงานสอบสวนได้ติดต่อขอให้พนักงานอัยการสั่งสอบสวนเพิ่มเติมหรือส่งพยานมาให้ซักถาม เมื่อพนักงานสอบสวนได้ขอยืมสำนวนไปเพื่อประโยชน์ในการดำเนินการดังกล่าว ให้หัวหน้าพนักงานอัยการพิจารณา ถ้าเห็นว่าไม่เป็นการเสื่อมเสียความยุติธรรม ก็ให้อนุญาตให้ยืมหรือคัดสำเนาไปได้

4) การติดต่อขอรับสำนวนการสอบสวน ให้หัวหน้าพนักงานสอบสวนหรือหัวหน้าส่วนราชการที่เกี่ยวข้องติดต่อโดยตรงกับหัวหน้าพนักงานอัยการ สำหรับรับส่วนกลาง กระทรวง ทบวง กรมต่างๆ จะติดต่อขอจากอธิบดีกรมอัยการโดยตรงก็ได้

5) ในกรณีที่สำนวนการสอบสวนอยู่ที่พนักงานอัยการอุทธรณ์ หรือพนักงานอัยการฎีกา ให้พนักงานอัยการอุทธรณ์หรือพนักงานอัยการฎีกา เป็นผู้พิจารณาอนุญาตให้ยืมหรือคัดสำนวนการสอบสวนแล้วแต่กรณี

ต่อมาเมื่อมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 สำนักงานอัยการสูงสุด จึงได้มีการแก้ไขระเบียบในข้อ 19 และ 20 ตรี เพื่อได้สอดคล้องกับพระราชบัญญัติดังกล่าวซึ่งมีใจความดังนี้

“ข้อ 19 (การขอตรวจหรือคัดสำเนาคำให้การในชั้นสอบสวน)

เมื่อพนักงานอัยการได้ยื่นฟ้องคดีต่อศาลแล้ว หากผู้เสียหายหรือจำเลยขอตรวจหรือคัดสำเนาคำให้การของตน หรือเอกสารประกอบคำให้การของตนในชั้นสอบสวนซึ่งผู้ขอเป็นผู้นำมามอบให้พนักงานสอบสวนหรือพนักงานอัยการ หรือเอกสารที่ผู้ขอลงลายมือชื่อไว้ ให้หัวหน้าพนักงานอัยการเป็นผู้พิจารณาอนุญาต

กรณีที่ผู้เสียหายหรือจำเลยขอตรวจหรือคัดสำเนาเอกสารอื่นๆ ในสำนวนการสอบสวน ให้หัวหน้าพนักงานอัยการพิจารณาตามความเหมาะสมและไม่ให้เกิดความเสียหายแก่ราชการและแก่ผู้อื่น โดยให้นำพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 14, 15 และมาตรา 17 มาพิจารณาประกอบด้วย

ในคดีที่ศาลได้มีคำพิพากษาเสร็จเด็ดขาดแล้ว หากผู้เสียหายหรือจำเลยหรือผู้มีส่วนได้เสียขอตรวจหรือคัดสำเนาเอกสารในสำนวนการสอบสวนคดีนั้น ให้หัวหน้าพนักงานอัยการเป็นผู้พิจารณาอนุญาต”

ดังได้กล่าวมาแล้วว่า ประมวลกฎหมายวิธีพิจาณาความแพ่งและวิธีพิจารณาความอาญา ไม่มีบทบัญญัติรองรับเรื่องการรับฟังพยานหลักฐานคอมพิวเตอร์ ซึ่งเป็นหลักฐานชิ้นสำคัญในการพิสูจน์การกระทำผิดต่อข้อมูลส่วนบุคคลโทษฐานละเมิดได้จะมีก็เพียงพระราชบัญญัติจัดตั้งศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ (ข้อ 33 – 36) และข้อกำหนดคดีล้มละลาย พ.ศ. 2542 (ข้อ 18 – 22) ระบุให้รับฟังพยานหลักฐานอิเล็กทรอนิกส์ดังนี้

1. ข้อกำหนดศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ

“ข้อ 33 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้หาก

1) การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์หรือการประมวลผลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์

2) การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิเสธงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และแม้หากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม 1) และความถูกต้องของการบันทึกและการประมวลผลตาม 2) ต้องมีคำรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

มาตรา 34 คู่ความที่ประสงค์จะเสนอข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์จะต้องระบุข้อมูลที่อ้างไว้ในบัญชีระบุพยานตามมาตรา 88 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง พร้อมยื่นคำแถลงแสดงความจำนงเช่นว่านั้น และคำรับรองตามข้อ 33 วรรคสองของสำเนาสื่อที่บันทึกข้อมูลนั้นในจำนวนที่เพียงพอเพื่อให้คู่ความอีกฝ่ายหนึ่งมารับไปจากเจ้าพนักงานศาล เว้นแต่

1) สื่อที่บันทึกข้อมูลนั้นอยู่ในความครอบครองของคู่ความฝ่ายอื่นหรือของบุคคลภายนอก ให้คู่ความที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาล ขออนุญาตงดส่งคำรับรองตามข้อ 33 วรรคสอง และสำเนาสื่อที่บันทึกข้อมูล และขอให้ศาลมีคำสั่งเรียกสื่อที่บันทึกข้อมูลนั้นมาจากผู้ครอบครองโดยให้คู่ความฝ่ายที่อ้างอิงนั้นมีหน้าที่ติดตามเพื่อให้ได้สื่อที่เห็นสมควรกำหนด

2) ถ้าการทำสำเนาสื่อที่บันทึกข้อมูลนั้น จะทำให้กระบวนการพิจารณาล่าช้าหรือเป็นที่เสื่อมเสียแก่คู่ความซึ่งอ้างอิงข้อมูลนั้น หรือมีเหตุผลแสดงว่าไม่อาจส่งสำเนาที่บันทึกข้อมูลนั้นให้แล้วเสร็จภายในเวลาตามที่กำหนดให้ ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งสำเนาสื่อที่บันทึกข้อมูลและขอนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลวันสืบพยานหรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

ถ้าคู่ความฝ่ายที่อ้างอิงไม่สามารถนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลได้ภายในเวลาตามวรรคหนึ่ง ศาลจะกำหนดให้ทำการตรวจข้อมูลดังกล่าว ณ สถานที่ เวลา และภายในเงื่อนไขตามที่ศาลเห็นสมควรแล้วแต่สภาพแห่งข้อมูลนั้นก็ได้

ถ้าคู่ความที่ประสงค์จะอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มิได้ปฏิบัติให้ถูกต้องตามความในวรรคหนึ่งหรือวรรคสอง ห้ามมิให้ศาลรับฟังข้อมูลนั้นเป็นพยานหลักฐาน แต่ถ้าศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมจะรับฟังข้อมูลเช่นว่านั้นเป็นพยานหลักฐานประกอบหลักฐานอื่นด้วยก็ได้

ข้อ 35. คู่ความฝ่ายที่ถูกอีกฝ่ายหนึ่งอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มาเป็นพยานหลักฐานยันตนอาจยื่นคำแถลงต่อศาลก่อนการสืบข้อมูลนั้นเสร็จคัดค้านการอ้างข้อมูลนั้น โดยเหตุว่าข้อมูลดังกล่าวไม่เข้าเงื่อนไขของการรับฟังตามข้อ 33 หรือสื่อที่บันทึกข้อมูลนั้นปลอมหรือสำเนาสื่อที่บันทึกข้อมูลนั้นไม่ถูกต้องทั้งหมดหรือบางส่วน เว้นแต่จะแสดงให้เป็นที่พอใจแก่ศาลว่ามีเหตุอันสมควรที่ไม่อาจทราบเหตุผลแห่งการคัดค้านได้ก่อนเวลาดังกล่าว คู่ความฝ่ายนั้นอาจยื่นคำร้องขออนุญาตคัดค้านการอ้างอิงข้อมูลหรือสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้นต่อศาลไม่ว่าเวลาใด ๆ ก่อนพิพากษาคดี และถ้าศาลเห็นว่าคู่ความว่ายนั้นไม่อาจยกข้อคัดค้านดังว่ามานี้ ให้นำมาตรา 126 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่งมาบังคับใช้โดยอนุโลม

ถ้าคู่ความซึ่งประสงค์จะคัดค้านการอ้างข้อมูลดังกล่าวเสียก่อนการสืบข้อมูลนั้นเสร็จหรือศาลไม่อนุญาตให้คัดค้านภายหลัง ห้ามมิให้คู่ความฝ่ายนั้นคัดค้านการอ้างอิงข้อมูลนั้นเป็นพยานหลักฐาน แต่ทั้งนี้ไม่ตัดอำนาจของศาลในการที่จะไต่สวนและชี้ขาดในเรื่องเงื่อนไขของการรับฟังข้อมูลนั้นตามข้อ 33 หรือในเรื่องความแท้จริงหรือถูกต้องของสื่อหรือสำเนาที่บันทึกข้อมูลเช่นว่านั้นในเมื่อศาลเห็นสมควรเพื่อประโยชน์แห่งความยุติธรรม

ข้อ 36. ให้นำข้อกำหนดข้อ 33 ถึงข้อ 35 มาใช้บังคับแก่การรับฟังข้อมูลที่บันทึกไว้ในหรือได้มาจากไมโครฟิล์ม สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศประเภทอื่นโดยอนุโลม”[78]

2. การคุ้มครองตามข้อกำหนดศาลล้มละลาย

“ข้อ 18 ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้ หาก

1) การบันทึกข้อมูลโดยเครื่องคอมพิวเตอร์หรือการประมวลโดยเครื่องคอมพิวเตอร์เป็นการกระทำตามปกติในการประกอบกิจการของผู้ใช้เครื่องคอมพิวเตอร์ และ

---

[78] ชวลิต อัตถศาสตร์ **อ้างแล้ว** หน้า31 – 32

2) การบันทึกและการประมวลผลข้อมูลเกิดจากการใช้เครื่องคอมพิวเตอร์ปฏิบัติงานตามขั้นตอนการทำงานของเครื่องคอมพิวเตอร์อย่างถูกต้อง และแม้หากมีกรณีการทำงานของเครื่องคอมพิวเตอร์ขัดข้องก็ไม่กระทบถึงความถูกต้องของข้อมูลนั้น

การกระทำตามปกติของผู้ใช้ตาม 1) และความถูกต้องของการบันทึกและการประมวลผลข้อมูลตาม 2) ต้องมีคำรับรองของบุคคลที่เกี่ยวข้องหรือดำเนินการนั้น

ข้อ 19 คู่ความที่ประสงค์จะเสนอข้อมูลที่บันทึกโดยคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์จะต้องระบุข้อมูลที่อ้างไว้ในบัญชีระบุพยานตามมาตรา 88 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง พร้อมยื่นคำแถลงแสดงความจำนงเช่นว่านั้น และคำรับรองตามข้อ 18 วรรคสอง กับสำเนาสื่อที่บันทึกข้อมูลนั้นในจำนวนที่เพียงพอให้คู่ความอีกฝ่ายมารับไปจากเจ้าพนักงานศาล เว้นแต่

1) สื่อที่บันทึกข้อมูลนั้นอยู่ในความครอบครองของคู่ความฝ่ายอื่นหรือของบุคคลภายนอก ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาลขออนุญาตงดส่งคำรับรองตามข้อ 18 วรรคสอง และสำเนาสื่อที่บันทึกข้อมูล และขอให้ศาลมีคำสั่งเรียกสื่อที่บันทึกข้อมูลนั้นมาจากผู้ครอบครองโดยให้คู่ความฝ่ายที่อ้างอิงนั้นมีหน้าที่ติดตามเพื่อให้ได้สื่อที่บันทึกข้อมูลนั้นมาแสดงต่อหน้าศาลในวันสืบพยาน หรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

2) ถ้ากำหนดทำสำเนาสื่อที่บันทึกข้อมูลนั้น จะทำให้กระบวนการพิจารณาล่าช้าหรือเป็นที่เสื่อมเสียแก่คู่ความซึ่งอ้างอิงข้อมูลนั้น หรือมีเหตุผลแสดงว่าไม่อาจส่งสำเนาสื่อที่บันทึกข้อมูลนั้นให้แล้วเสร็จภายในเวลาตามที่กำหนดได้ ให้คู่ความฝ่ายที่อ้างอิงข้อมูลยื่นคำขอโดยทำเป็นคำร้องต่อศาล ขออนุญาตงดส่งสำเนาสื่อที่บันทึกข้อมูลและขอนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลในวันสืบพยานหรือในวันอื่นตามที่ศาลเห็นสมควรกำหนด

ถ้าคู่ความฝ่ายที่อ้างอิงไม่สามารถนำสื่อที่บันทึกข้อมูลนั้นมาแสดงต่อศาลได้ภายในเวลาตามวรรคหนึ่ง ศาลจะกำหนดให้ทำการตรวจข้อมูลดังกล่าว ณ สถานที่ เวลาและภายในเงื่อนไขตามที่ศาลเห็นสมควรแล้วแต่สภาพแห่งข้อมูลนั้นๆ ก็ได้

ถ้าคู่ความที่ประสงค์จะอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มิได้ปฏิบัติให้ถูกต้องตามความในวรรคหนึ่งหรือวรรคสอง ห้ามมิให้ศาลรับฟังข้อมูลนั้นเป็นพยานหลักฐาน แต่ถ้าศาลเห็นว่าเพื่อประโยชน์แห่งความยุติธรรมจะรับฟังข้อมูลเช่นว่านั้นเป็นพยานหลักฐานประกอบพยานหลักฐานอื่นด้วยก็ได้

ข้อ 20 คู่ความฝ่ายถูกอีกฝ่ายหนึ่งอ้างอิงข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์มาเป็นพยานหลักฐานยันตนอาจยื่นคำแถลงต่อศาลก่อนการสืบข้อมูลนั้นเสร็จ คัดค้านการอ้างข้อมูลนั้น โดยเหตุที่ว่าข้อมูลดังกล่าวไม่เข้าเงื่อนไขของการรับฟังตามข้อ 18 หรือสื่อที่บันทึกข้อมูลนั้นปลอมหรือสำเนาสื่อที่บันทึกข้อมูลนั้นไม่ถูกต้องทั้งหมดหรือบางส่วน เว้นแต่จะแสดงให้เป็นที่พอใจแก่ศาลว่ามีเหตุอันสมควรที่ไม่อาจทราบเหตุแห่งการคัดค้านได้ก่อนเวลาดังกล่าว คู่ความฝ่ายนั้นอาจยื่นคำร้องขออนุญาตคัดค้างการอ้างข้อมูลหรือสื่อสำเนาที่บันทึกข้อมูลเช่นว่านั้นต่อศาลไม่ว่าเวลาใดๆ ก่อนพิพากษาคดี และถ้าศาลเห็นว่าคู่ความฝ่ายนั้นไม่อาจยกข้อคัดค้านได้ก่อนนั้นและคำร้องนั้นมีเหตุผลฟังได้ก็ให้ศาลอนุญาตตามคำร้อง ในกรณีที่มีการคัดค้านดังว่ามานี้ให้นำมาตรา 126 แห่งประมวลกฎหมายวิธีพิจารณาความแพ่งมาใช้บังคับโดยอนุโลม

ถ้าคู่ความซึ่งประสงค์คัดค้างการอ้างข้อมูลดังกล่าวเสียก่อนการสืบข้อมูลนั้นเสร็จ หรือศาลไม่อนุญาตให้คัดค้านภายหลัง ห้ามมิให้คู่ความฝ่ายนั้นคัดค้านการอ้างอิงข้อมูลนั้นเป็นพยานหลักฐาน แต่ทั้งนี้ไม่ตัดอำนาจของศาลในการที่จะไต่สวนหรือชี้ขาดในเรื่องเงื่อนไขของการรับฟังข้อมูลส่วนบุคคลตามข้อ 18 หรือในเรื่องจริงหรือถูกต้องของสื่อหรือสำเนาสื่อที่บันทึกข้อมูลเช่นว่านั้น ในเมื่อศาลเห็นสมควรเพื่อประโยชน์แห่งความยุติธรรม

ข้อ 21. ให้นำข้อกำหนดข้อ 18 ถึง 20 มาใช้บังคับแก่การรับฟังข้อมูลที่บันทึกไว้ในหรือได้มาจากไมโครฟิล์ม สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศประเภทอื่นโดยอนุโลม”

3. กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูล

ในปัจจุบันนี้ประเทศไทยยังไม่มีกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลโดยตรงที่มีอยู่เป็นกฎหมายที่มีความเกี่ยวข้องซึ่งสามารถจำแนกตามศักดิ์ของกฎหมายได้ดังนี้

1) กฎหมายรัฐธรรมนูญ

ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 ได้ระบุที่เกี่ยวข้องกับการคุ้มครองข้อมูลในกระบวนการยุติธรรม โดยเริ่มตั้งแต่ในชั้นพนักงานสอบสวน ต้องรับคำร้องทุกข์หรือคำกล่าวโทษจากผู้เสียหายหรือบุคคลอื่นว่ามีการกระทำความผิดเกิดขึ้น พนักงานสอบสวนซึ่งทำการสอบสวนและรวบรวมพยานหลักฐานทั้งหลายเพื่อพิสูจน์ความผิดของผู้ต้องหาว่าเป็นผู้กระทำความผิดหรือไม่ เมื่อพนักงานสอบสวนทำการสอบสวนและทำสำนวนคดี ผู้เสียหายจึงต้องการทราบสำนวนคดีของตนเพื่อความโปร่งใสในการดำเนินคดีอาญา เพื่อให้สอดคล้องกับรัฐธรรมนูญฉบับปัจจุบัน

การเปิดเผยข้อมูลหรือสำนวนคดีในชั้นพนักงานสอบสวน รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 241 วรรคสาม ได้บัญญัติว่า ผู้เสียหายหรือจำเลยในคดีอาญาย่อมมีสิทธิตรวจ หรือคัดสำเนาคำให้การของตนในชั้นสอบสวน หรือเอกสารประกอบย่อมมีสิทธิตรวจหรือคัดสำเนาคำให้การของตนในชั้นสอบสวน หรือเอกสารประกอบคำให้การของตน เมื่อพนักงานอัยการได้ยื่นฟ้องคดีต่อศาลแล้ว ทั้งนี้ตามที่กฎหมายบัญญัติ

ในชั้นพนักงานสอบสวนนี้เมื่อผู้เสียหายขอตรวจดูสำนวนคดีเมื่อพนักงานสอบสวนปฏิเสธไม่ให้ผู้เสียหายได้ตรวจดูสำนวนคดีของตน พนักงานสอบสวนก็จะอ้างว่าถ้ามีการเปิดเผยข้อมูลหรือสำนวนคดีในส่วนของผู้ต้องหาแล้วจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ[79] ซึ่งการที่พนักงานจะให้ตรวจดูสำนวนได้หรือไม่นั้นเป็นการใช้ดุลพินิจของหัวหน้าพนักงานสอบสวน ซึ่งต้องมีการผ่านขั้นตอนโดยยื่นคำร้องต่อพนักงานสอบสวนที่กระทำการสอบสวนคดีของตน คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขอย่างใดก็ได้ แต่ต้องระบุไว้ด้วยว่าที่เปิดเผยไม่ได้เพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใดและให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการเป็นดุลพินิจ โดยเฉพาะของเจ้าหน้าที่ของรัฐตามลำดับสายการบังคับบัญชา แต่ผู้ขออาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้ตามที่กำหนดในพระราชบัญญัตินี้

นอกจากรัฐธรรมนูญฉบับปัจจุบันจะให้การคุ้มครองข้อมูลแล้วประเทศไทยยังมีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลอีก คือ

2) ประมวลกฎหมายอาญา

สำหรับกฎหมายอาญาได้ระบุไว้บางประการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งจะต้องนำมาตีความ ในหมวดที่ 2 กล่าวคือ ความผิดฐานเปิดเผยความลับ[80] ระบุไว้ในมาตรา 322 เกี่ยวกับการเปิดผนึกเอกสารใดๆ ซึ่งเปิดผนึกของผู้อื่นไปเพื่อล่วงรู้ข้อความนำข้อความในเอกสารนั้นออกเปิดเผยในลักษณะที่จะก่อให้เกิดความเสียหายแก่ผู้หนึ่งผู้ใด[81]

---

[79] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 15 (2) ที่บัญญัติไว้ว่า “การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ”

[80] ประมวลกฎหมายอาญา มาตรา 322 323 และ 324

[81] “**มาตรา 322** ผู้ใดเปิดผนึกหรือเอาจดหมาย โทรเลขหรือเอกสารใดๆ ซึ่งเปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมาย โทรเลข หรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใดต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

หรือการล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น แล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ตามมาตรา 323 [82]และ มาตรา 324 [83]โดยเหตุที่ตนมีตำแหน่งหน้าที่ วิชาชีพ หรืออาชีพอันเป็นที่ไว้วางใจล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น เปิดเผยหรือใช้ความลับนั้นเพื่อประโยชน์ตนเองหรือผู้อื่น นอกจากนี้ยังมีมาตรา 358 [84]ว่าด้วยความผิดฐานทำให้เสียทรัพย์ โดยทำให้เสียหาย ทำลาย ทำให้เสื่อมค่าหรือทำให้ไร้ประโยชน์ ซึ่งทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วย

จากมาตราข้างต้นโดยเฉพาะมาตรา 323 และมาตรา 324 เกิดปัญหาว่ากฎหมายอาญาไม่ได้ให้การคุ้มครองครอบคลุมไปถึงผู้กระทำผิดอยู่นอกสาขาวิชาชีพที่บัญญัติไว้ และอีกปัญหาก็คือถ้าสิ่งที่ล่วงรู้มาไม่ใช่ความลับแต่มีความสำคัญมากเมื่อนำไปใช้ข้อมูลอื่นๆ หรือจะเป็นความลับที่ไม่ก่อให้เกิดความเสียหายแก่เจ้าของความลับ เราจะสามารถถือว่าเป็นความผิดฐานเปิดเผยความลับหรือไม่

---

82 “**มาตรา 323** ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมดความ ทนายความ หรือผู้สอบบัญชี หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น แล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งพันบาทหรือทั้งจำทั้งปรับ

ผู้รับการศึกษาอบรมในอาชีพดังกล่าวในวรรคแรก เปิดเผยความลับของผู้อื่นอันตนได้ล่วงรู้หรือได้มาในการศึกษาอบรมนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษเช่นเดียวกัน”

83 **“มาตรา 324** ผู้ใดโดยเหตุที่ตนมีตำแหน่งหน้าที่ วิชาชีพ หรืออาชีพอันเป็นที่ไว้วางใจล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น เกี่ยวกับอุตสาหกรรม การค้นพบหรือการนิมิตในวิทยาศาสตร์ เปิดเผยหรือใช้ความลับนั้นเพื่อประโยชน์ตนเองหรือผู้อื่นต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

84 **“มาตรา 358** ผู้ใดทำให้เสียหาย ทำลาย ทำให้เสื่อมค่าหรือทำให้ไร้ประโยชน์ ซึ่งทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วย ผู้นั้นกระทำความผิดฐานทำให้เสียทรัพย์ ต้องระวางโทษจุกไม่เกินสามปี หรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ”

3) ประมวลกฎหมายแพ่งและพาณิชย์

เป็นกฎหมายเพื่อฟ้องร้องดำเนินคดีกับผู้กระทำความผิดในฐานะที่ละเมิดและก่อให้เกิดความเสียหายต่อทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล เช่น ข้อมูลส่วนบุคคลเสียหาย หรือระบบคอมพิวเตอร์ใช้การไม่ได้ เช่น ตามมาตรา 420[85] เป็นต้น

จากมาตรา 420 และมาตรา 438 จะมีปัญหาว่าประเทศไทยยังไม่มีกฎหมายใดที่รับรองว่า ข้อมูลส่วนบุคคลในเครื่องสื่อสารอิเล็กทรอนิกส์ (ข้อมูลอิเล็กทรอนิกส์) เป็นทรัพย์หรือไม่ เพราะกฎหมายฉบับนี้ให้ความหมายเกี่ยวกับทรัพย์ว่า เป็นวัตถุที่มีรูปร่าง ทำให้เราไม่สามารถฟ้องร้องต่อผู้กระทำผิดได้เพราะสิ่งที่เขาละเมิดนั้นไม่ใช่ทรัพย์ และการละเมิดต่อข้อมูลส่วนบุคคลที่เก็บไว้ในเครื่องคอมพิวเตอร์ดังกล่าวก็จะเป็นรูปแบบของการคัดลอกข้อมูลมา จึงเป็นอีกประเด็นที่ว่าผู้กระทำผิดจะไม่ต้องรับผิดฐานละเมิด เนื่องจากเขาไม่ได้ทำให้ข้อมูลอิเล็กทรอนิกส์ (ซึ่งไม่ใช่ทรัพย์) เกิดความเสียหายแต่อย่างใด

ยังมีอีกมาตราที่เกี่ยวข้องกับการทำสัญญาซึ่งมีปัญหาเรื่องลายมือชื่อที่ใช้ในการยืนยันความเป็นบุคคล (Identification) ในการสั่งซื้อผ่านทางสื่ออิเล็กทรอนิกส์ ได้แก่ มาตรา 9 [86] จากมาตราดังกล่าวเมื่อพิจารณาวินิจฉัยประกอบคำพิพากษาฎีกาที่ 3046/2537 เกี่ยวกับเรื่องการซื้อขายข้าวผ่านโทรศัพท์ ซึ่งศาลฎีกาวินิจฉัยว่าโทรพิมพ์ไม่มีลายมือชื่อของจำเลยจึงฟ้องร้องไม่ได้ จะเห็นได้ว่าการซื้อขายโดยใช้สื่อสารอิเล็กทรอนิกส์ในปัจจุบัน เช่น โทรศัพท์จะใช้รหัส PIN code หรือ password แทนการแสดงเจนตาของเจ้าของโทรศัพท์มือถือ อาจจะเกิดปัญหาข้อกฎหมายได้เช่นเดียวกับโทรพิมพ์ ดังนั้นในทางปฏิบัติผู้ขายและผู้ซื้อมักจะทำสัญญาหลักเพื่อให้ผู้ซื้อยอมรับว่า รหัส PIN code หรือ password ดังกล่าวเป็นลายมือชื่อของผู้ซื้อและให้ผู้ซื้อยืนยันคำสั่งซื้อเป็นลายลักษณ์อักษรแก่ผู้ขายอีกครั้งหนึ่ง หรือชำระเงินบางส่วนเพื่อใช้เป็นหลักฐานในการซื้อขาย

การดำเนินการในส่วนนี้คงต้องรอกฎหมายที่เกี่ยวข้องกับลายมือชื่ออิเลกโทรนิกส์ที่จะออกมาใช้บังคับต่อไป

---

85 "มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น"

86 "มาตรา 9 เมื่อมีกิจการอันใดซึ่งกฎหมายบังคับให้ทำเป็นหนังสือบุคคลผู้จะต้องทำหนังสือไม่จำเป็นต้องเขียนเอง แต่หนังสือนั้นต้องลงลายมือชื่อของบุคคลนั้น

ลายพิมพ์นิ้วมือ แกงได ตราประทับ หรือเครื่องหมายอื่นเช่นว่านั้นที่ทำลงในเอกสารแทนการลงลายมือชื่อ หากมีพยานลงลายมือชื่อรับรองไว้ด้วยสองคนแล้วถือเสมอกับลงลายมือชื่อ"

4.ประมวลกฎหมายวิธีพิจารณาความอาญา

บทบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญา เมื่อมีคำสั่งไม่ฟ้องคดีแล้ว กฎหมายให้สิทธิแก่ผู้เสียหายในการที่จะฟ้องคดีได้ด้วยตนเอง แต่ประมวลกฎหมายวิธีพิจารณาความอาญาก็มิได้รับรองสิทธิของผู้เสียหาย ในการที่จะได้รับทราบความเห็นของพนักงานสอบสวน หรือพนักงานอัยการ

แม้ว่ารัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 241 วรรคสามจะบัญญัติว่า ผู้เสียหายหรือจำเลยในคดีอาญาย่อมมีสิทธิตรวจ หรือคัดสำเนาคำให้การของตนในชั้นสอบสวน หรือเอกสารประกอบคำให้การของตน เมื่อพนักงานอัยการได้ยื่นฟ้องคดีต่อศาลแล้ว ทั้งนี้ตามที่กฎหมายบัญญัติ

มาตรา 241 วรรคท้าย บัญญัติว่า ในคดีอาญา ที่พนักงานอัยการมีคำสั่งเด็ดขาดไม่ฟ้องแล้ว ผู้เสียหาย ผู้ต้องหา หรือผู้มีส่วนได้เสียย่อมมีสิทธิขอทราบสรุปพยานหลักฐานพร้อมความเห็นของพนักงานสอบสวนและพนักงานอัยการในการสั่งคดี ทั้งนี้ตามที่กฎหมายบัญญัติ

จากรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 241 วรรคสามและวรรคท้ายก็มิได้มีการกำหนดรายละเอียดในการปฏิบัติไว้ โดยรัฐธรรมนูญได้กล่าวในประโยคท้ายว่าทั้งนี้ตามที่กฎหมายบัญญัติ จึงต้องมาพิจารณากฎหมายลำดับรอง ซึ่งต้องกำหนดรายละเอียดขั้นตอนปฏิบัติ มิฉะนั้นแล้วจะไม่เกิดผลเป็นรูปธรรม ซึ่งกฎหมายลำดับรองก็คือประมวลกฎหมายวิธีพิจารณาความอาญามิได้แก้ไขให้มีความสอดคล้องกับรัฐธรรมนูญแห่งราชอาณาจักรไทย ตามมาตราดังกล่าวข้างต้น

ผู้เสียหาย พยาน หรือบุคคลภายนอกคดี ผู้มีส่วนได้เสียโดยชอบ ประมวลกฎหมายวิธีพิจารณาความอาญามิได้บัญญัติโดยตรงถึงสิทธิในการตรวจดูข้อมูลข่าวสาร ดังเช่นจำเลยตามมาตรา 8 กรณีนี้ต้องนำมาตรา 15 ประกอบด้วยประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 54 มาปรับใช้โดยยังต้องนำพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 15 มาปรับใช้ด้วย

5.ประมวลกฎหมายวิธีพิจารณาความแพ่ง

ในชั้นศาลการที่จะได้รับการเปิดเผยข้อมูล ต้องอยู่ภายใต้บังคับของประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 52 ความว่า เมื่อคำพิพากษาหรือคำสั่งอันเป็นเด็ดขาดถึงที่สุดแล้ว เรื่องใดได้มีการปฏิบัติตาม หรือบังคับไปแล้ว หรือระยะเวลาที่กำหนดไว้

เพื่อการบังคับนั้นได้ล่วงพ้นไปแล้ว ให้ศาลที่เก็บสำนวนนั้นไว้ จัดส่งสำนวนนั้นไปยังกระทรวงยุติธรรม เพื่อเก็บรักษาไว้ หรือจัดการตามกฎกระทรวงว่าด้วยการนั้นและมาตรา 54 ความว่า คู่ความก็ดี หรือพยานในส่วนที่เกี่ยวกับคำให้การของตนในคดีนั้นก็ดี หรือบุคคลภายนอกผู้มีส่วนได้เสียโดยชอบหรือมีเหตุผลอันสมควรก็ดี อาจร้องขออนุญาตต่อศาลไม่ว่าเวลาใดในระหว่างหรือภายหลังการพิจารณา เพื่อตรวจเอกสารทั้งหมดหรือแต่บางฉบับในสำนวนเรื่องนั้น หรือขอคัดสำเนาหรือขอให้จ่าศาลคัดสำเนาและรับรองแต่ทั้งนี้

1)ห้ามมิให้อนุญาตเช่นว่านั้นแก่บุคคลอื่นนอกจากคู่ความหรือพยานในคดีที่พิจารณาโดยไม่เปิดเผย หรือในคดีที่ศาลได้มีคำสั่งห้ามการตรวจหรือคัดสำเนาเอกสารในสำนวนทั้งหมดหรือบางฉบับ เพื่อรักษาความสงบเรียบร้อยหรือผลประโยชน์ทั่วไปของประชาชน ถึงแม้ผู้ขอจะเป็นคู่ความหรือพยานก็ห้ามมิให้อนุญาตดุจกัน แต่ทั้งนี้ไม่ตัดสิทธิของคู่ความในการที่จะตรวจหรือคัดสำเนาคำพิพากษาหรือคำสั่งในคดีนั้น หรือในการที่จะขอสำเนาอันรับรองถูกต้อง

2) ห้ามมิให้อนุญาตให้คู่ความคัดคำพยานฝ่ายตนจนกว่าจะได้สืบพยานฝ่ายตนเสร็จสิ้นแล้ว เว้นแต่จะมีพฤติการณ์พิเศษที่จะให้อนุญาต

เมื่อได้ให้อนุญาตแล้ว การตรวจ หรือการคัดสำเนานั้น ให้ผู้ขอหรือบุคคลซึ่งได้รับการแต่งตั้งจากผู้ขอโดยชอบเป็นผู้คัดค้านตามเวลาและเงื่อนไข ซึ่งจ่าศาลจะได้กำหนดให้เพื่อความสะดวกของศาล หรือเพื่อความปลอดภัยของเอกสารนั้น

ห้ามมิให้คัดสำเนาคำพิพากษาหรือคำสั่ง ก่อนที่ได้อ่านคำพิพากษาหรือคำสั่งนั้นและก่อนที่ได้ลงทะเบียนในสารบบคำพิพากษา

ในกรณีที่ศาลได้ทำคำอธิบายเพิ่มเติมกลัดไว้กับรายงานแห่งคำสั่งหรือคำพิพากษาซึ่งกระทำด้วยวาจาตามบทบัญญัติ มาตรา 141 คำอธิบายเพิ่มเติมเช่นว่านั้นคู่ความจะขอตรวจหรือขอคัดสำเนา หรือขอสำนวนเสมือนเป็นส่วนหนึ่งแห่งคำสั่งหรือคำพิพากษาก็ได้

สำเนาที่รับรองนั้น ให้จ่าศาลเป็นผู้รับรองโดยเรียกค่าธรรมเนียมตามที่กำหนดไว้ในอัตราท้ายประมวลกฎหมายนี้ ในกรณีที่ผู้ขอตรวจเอกสารหรือขอคัดสำเนาด้วยตนเอง ไม่ต้องเรียกค่าธรรมเนียม

การตรวจและคัดสำเนาความในศาลนั้น ตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 54 บุคคลเหล่านี้อาจขอคัดได้ คือ

(1) คู่ความ

(2) พยานในส่วนที่เกี่ยวกับคำให้การของตนในคดีนั้น คือ พยานคนหนึ่งไม่มีสิทธิจะขอคัดคำให้การของพยานคนอื่นได้

(3) บุคคลภายนอก ผู้มีส่วนได้เสียโดยชอบ หรือมีเหตุผลอันสมควร

บุคคลภายนอกผู้มีส่วนได้เสียโดยชอบนั้น เช่น บุคคลผู้มีสิทธิจะร้องสอดเข้ามาเป็นคู่ความ ส่วนบุคคลภายนอกเมื่อมีเหตุผลอันสมควรนั้นกินความกว้างมากอาจรวมถึงผู้สื่อข่าวหนังสือพิมพ์ด้วยก็ได้

ส่วนบุคคลอื่นซึ่งไม่มีความเกี่ยวข้องกับคดีเรื่องใดที่กล่าวมานี้ ไม่มีสิทธิจะขอตรวจหรือคัดสำเนาความเรื่องนั้นได้

3) กรณีขอคัดหรือขอถ่ายไม่ได้

ก. คดีที่พิจารณาโดยไม่เปิดเผยตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 177 มาตรา 178 คดีที่พิจารณาโดยไม่เปิดเผยนั้น บุคคลที่ไม่ใช่คู่ความหรือไม่ใช่เป็นพยานในคดีนั้นจะขอคัดหรือขอถ่ายไม่ได้

ข. คดีที่ศาลเห็นสมควรสั่งห้ามคัดหรือถ่ายถ้อยคำสำนวนทั้งหมดหรือบางส่วนเพื่อรักษาความสงบเรียบร้อยหรือผลประโยชน์ทั่วไปของประชาชน ในข้อนี้ก็ถือหลักที่ว่าประโยชน์ของสารธารณะย่อมเหนือประโยชน์ทั่วไปของบุคคล ศาลอาจไม่อนุญาตแม้กระทั่งคู่ความในคดีนั้นหรือพยานที่เบิกความในเรื่องนั้นก็ขอคัดถ่ายไม่ได้

ค. คู่ความจะขอคัดถ้อยคำพยานฝ่ายตนก่อนที่จะสืบพยานเสร็จไม่ได้ ห้ามในข้อนี้ก็เพื่อมิให้คู่ความเอาเปรียบกันในทางคดีที่จะนำคำเบิกความของพยานฝ่ายตนที่เบิกความไว้ก่อนแล้วไปปรุงแต่งเพื่อให้สอดคล้องกับคำพยานของตนที่จะนำเข้ามาเบิกความภายหลัง ทำให้อีกฝ่ายหนึ่งเสียเปรียบในทางคดี แต่ก็มีข้อยกเว้นไว้ว่าถ้ามีพฤติการณ์พิเศษก็สามารถที่จะขอคัดหรือขอถ่ายได้ พฤติการณ์พิเศษนี้จะต้องระบุในคำร้องขอคัดหรือขอถ่ายในคดี กรณีนี้ว่าจะนำไปใช้เพื่อการใด

ง. คำพิพากษาหรือคำสั่งก่อนอ่านจะขอคัดไม่ได้ โดยหลักแล้วถ้าเป็นคำพิพากษาของศาลชั้นต้น ศาลชั้นต้นก็จะอ่านตามร่างที่ร่างขึ้นมา และก่อนอ่านนั้นจะขอคัดไม่ได้ส่วนร่างที่อ่านแล้วจะขอคัดได้หรือไม่ได้นั้น แล้วแต่เรื่องของผู้พิพากษาบางท่าน

1. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นกฎหมายเดียวที่กล่าวถึงการคุ้มครองข้อมูลข่าวสารส่วนบุคคลมากที่สุดในขณะนี้ โดยได้ให้ความหมายของ “ข้อมูลข่าวสารส่วนบุคคล” ไว้ดังนี้

> *“ข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัสหรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่ายและให้หมายความถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย*
> (พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540)

จากกฎหมายฉบับนี้ ข้อมูลข่าวสารของราชการมีหลักสำคัญ 2 ประการ[87] ได้แก่ “หลักที่ว่าบุคคลไม่จำต้องเป็นผู้มีส่วนได้เสียกับข้อมูลข่าวสารที่ขอ” และ “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น” แต่ในส่วนของข้อมูลข่าวสารส่วนบุคคลนั้น กฎหมายต้องการคุ้มครองความเป็นส่วนตัวของบุคคล จึงจำเป็นต้องกำหนดหลักการแตกต่างไปจากข้อมูลข่าวสารของราชการ โดยกำหนดว่า “ผู้ที่เข้าถึงข้อมูลข่าวสารส่วนบุคคลได้ คือ เจ้าของข้อมูลข่าวสารนั้นเองหรือบุคคลที่เจ้าของข้อมูลข่าวสารยินยอมและบุคคลที่มีสิทธิตามกฎหมาย” ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ มาตรา 24 ในหลักการที่ว่าข้อมูลข่าวสารส่วนบุคคลจะเปิดเผยต่อบุคคลอื่นโดยปราศจากความยินยอมของเจ้าของข้อมูลไม่ได้ เว้นแต่จะเข้าข้อยกเว้น

อย่างไรก็ตาม แนวความคิดของข้อมูลข่าวสารส่วนบุคคลได้มีกฎหมายบางฉบับได้ให้ความคุ้มครองไว้บ้างแล้ว ได้แก่ **พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534** ได้คุ้มครองข้อมูลข่าวสารส่วนบุคคลบางประการ เช่น ข้อมูลทะเบียนประวัติราษฎร เป็นข้อมูลบุคคลเกี่ยวกับวันเดือนปีเกิดและตาย สัญชาติ ศาสนา ภูมิลำเนา สถานการณ์สมรส เป็นต้น ซึ่งถือเป็นความลับ มิให้เปิดเผยแก่ผู้อื่นเว้นแต่ผู้มีส่วนได้เสีย เช่น กรณีคู่หมั่นขอทราบสถานภาพทางครอบครัวของผู้ดีตนจะมีนิสิตสัมพันธ์ด้วยว่าบุคคลนั้นยังเป็นโสดหรือไม่ เป็นต้น หรือจะเพื่อประโยชน์ในการเก็บหรือจัดทำสถิติเพื่อประโยชน์ด้านความมั่นคงของรัฐ การดำเนินคดี การพิพากษาและการปฏิบัติหน้าที่ตามกฎหมาย (พระราชบัญญัติการทะเบียนราษฎร, 2534: 17)

---

[87] ฤทัย หงส์สิริและมานิตย์ จุมปา **อ้างแล้ว** หน้า. 86

แต่พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534 จะแตกต่างกับกฎหมายข้อมูลข่าวสารของราชการตรงที่ พ.ร.บ. การทะเบียนราษฎรเป็นเพียงกฎหมายเฉพาะฉบับหนึ่งเท่านั้น ส่วนกฎหมายข้อมูลข่าวสารของราชการได้วางหลักเกณฑ์ในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลเป็นการทั่วไป

ความสำคัญของข้อมูลข่าวสารส่วนบุคคล ข้อมูลข่าวสารส่วนบุคคลมีความสำคัญ 3 ประเด็นหลัก ได้แก่

1.ข้อมูลข่าวสารส่วนบุคคลนั้นมีผลกระทบต่อบุคคลในหลายด้าน เช่น มีผลเกี่ยวกับชีวิตและความปลอดภัยของบุคคล เพราะจะรู้ว่าบุคคลนั้นอาศัยอยู่ที่ใด มีฐานะทางเศรษฐกิจดีเพียงใด อันจะนำไปสู่การปองร้ายอย่างง่ายดาย

2.ข้อมูลข่าวสารส่วนบุคคลเป็นข้อมูลที่ใช้ประโยชน์ในเชิงธุรกิจได้ เช่น ระดับราคาสินค้าหรือบริการ ลักษณะและกลุ่มเป้าหมาย ลักษณะรสนิยมของบุคคล เพื่ออาศัยข้อมูลดังกล่าวเป็นข้อได้เปรียบทางการพาณิชย์ได้

3.ข้อมูลข่าวสารส่วนบุคคลเป็นสิ่งที่ใช้ในกาตรวจสอบการปฏิบัติหน้าที่ของเจ้าหน้าที่และใช้เป็นฐานในการเรียกร้องสิทธิทางกฎหมาย เช่น บันทึกการตรวจโรคย่อมเป็นหลักฐานในการตรวจสอบความถูกต้องและมาตรฐานการรักษาของแพทย์ผู้นั้นได้อย่างชัดเจน

จากความสำคัญของข้อมูลข่าวสารส่วนบุคคลดังกล่าว กฎหมายจึงคุ้มครองข้อมูลข่าวสารส่วนบุคคลให้ครอบคลุมโดยมีองค์ประกอบของการคุ้มครองข้อมูลข่าวสารส่วนบุคคลต่อไปนี้

1.บุคคลผู้ได้รับความคุ้มครองเกี่ยวกับข้อมูลข่าวสารส่วนบุคคล

บุคคลที่มีสัญชาติไทยย่อมได้รับความคุ้มครองเกี่ยวกับข้อมุลข่าวสารส่วนบุคคลอยู่แล้ว และยังขยายสิทธินี้ไปยังบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทยด้วย ได้แก่ คนต่างด้าวที่เข้ามาทำงานในประเทศไทยและมีถิ่นที่อยู่ในประเทศไทย แรงงานต่างด้าวเหล่านั้นย่อมได้รับการคุ้มครองเช่นเดียวกับผู้มีสัญชาติไทย แต่ประเด็นสำคัญของข้อมูลข่าวสารส่วนบุคคล คือจะให้ความคุ้มครองข้อมูลข่าวสารของบุคคลธรรมดาเท่านั้น ไม่กล่าวรวมถึงนิติบุคคล สังเกตได้จากมาตรา 21 ของกฎหมายข้อมูลข่าวสารของราชการ ได้บัญญัติไว้ว่า

“เพื่อประโยชน์แห่งหมวดนี้ “บุคคล” หมายความว่า บุคคลธรรมดาที่มีสัญชาติไทยและบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย”

2.การจัดเก็บข้อมูลข่าวสารส่วนบุคคล พระราชบัญญัติข้อมูลข่าวสารของราชการได้บัญญัติไว้ในมาตรา 23 ว่า หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคล ดังต่อไปนี้

(1)ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(2)พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

(3)จัดให้มีการพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก)ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข)ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค)ลักษณะการใช้ข้อมูลตามปกติ

(ง)วิธีการขอตรวจดูข้อมูลข่าวสารส่วนบุคคลของเจ้าของข้อมูล

(จ)วิธีการขอให้แก่ไขเปลี่ยนแปลงชุดข้อมูล

(ฉ)แหล่งที่มาของข้อมูล

(4)ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(5)จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และการที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใด ซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ”

(1)ต้องมีระบบข้อมูลข่าวสารส่วนบุคคลเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงาน โดยหลักคือ ต้องมีแต่เจ้าของข้อมูลข่าวสารส่วนบุคคลเท่านั้นที่ควรรู้ หน่วยงานของรัฐไม่ควรจัดเก็บข้อมูลข่าวสารส่วนบุคคล เนื่องจากรัฐมีหน้าที่ดำเนินงานในส่วนที่เป็นประโยชน์ส่วนรวมมากกว่าประโยชน์บุคคลใดบุคคลหนึ่งโดยเฉพาะ หน่วยงานของรัฐจึงมีอำนาจจัดเก็บข้อมูลข่าวสารส่วนบุคคลเท่าที่เกี่ยวข้องและจำเป็นต้องการดำเนินงาน และเมื่อหมดความจำเป็นก็ต้องเลิกใช้ระบบดังกล่าวเพื่อรักษาสิทธิของบุคคลนั้น

(2) ทำการเก็บข้อมูลโดยตรงจากเจ้าของข้อมูล ประเด็นที่น่าสังเกตได้แก่ พ.ร.บ. ข้อมูลข่าวสารของราชการได้ใช้คำว่า “พยายาม” เพราะบางกรณีการจัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรงอาจจะไม่ได้รับความถูกต้องตามความเป็นจริง สาเหตุมาจากเจ้าของข้อมูลอาจจะมีผลประโยชน์ได้เสียในการให้ข้อมูลหรือไม่ต้องการให้ข้อมูลที่เป็นจริงแก่หน่วยงานของรัฐ เช่น กรณีที่ศาลมีคำสั่งให้สืบประวัติและความประพฤติของจำเลยเพื่อใช้ประกอบการพิจารณาของศาล จำเลยจะมีแนวโน้มที่จะให้ข้อมูลหรือไม่ให้ข้อมูลเพ่อเป็นประโยชน์ต่อตนเอง เจ้าหน้าที่ของรัฐจึงจำเป็นต้องหาข้อมูลทั้งตัวจำเลยเอง หรือบุคคลที่เกี่ยวข้องหรือบุคคลอื่นด้วย เพื่อให้ได้ข้อมูลข่าวสารที่ตรงกับความจริงมากที่สุด

(3) ให้จัดพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องเสมอเกี่ยวกับสิ่งต่อไปนี้

1. ประเภทของบุคคลที่มีการเก็บข้อมูลไว้ เช่น หน่วยงานบางหน่วยงานได้เก็บข้อมูลข่าวสารที่เกี่ยวกับข้าราชการ พนักงาน ลูกจ้าง กรรมการของรัฐวิสาหกิจ อนุกรรมการต่างๆ ผู้รับทุนการศึกษา หรือบุคคลประเภทอื่นๆ แต่กฎหมายให้ใช้ข้อมูลที่เกี่ยวข้องกับประเภทของบุคคลเท่านั้น ไม่ต้องนำข้อมูลของทุกคนไปลงพิมพ์ในราชกิจจานุเบกษา

2. ประเภทของข้อมูลข่าวสารสวนบุคคล เช่น ข้อมูลข่าวสารที่เป็นประวัติบุคคลหรือประวัติการทำงาน เป็นต้น

3. ลักษณะการใช้ข้อมูลตามปกติ เช่น กรณีข้าราชการเก็บข้อมูลเพื่อใช้ประโยชน์ในการบริหารงานบุคคล การเลื่อนขั้นตำแหน่งหรือเพื่อพัฒนาตนเอง เป็นต้น

4. วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล คือ เมื่อบุคคลใดพบว่าข้อมูลข่าวสารของตนไม่ถูกต้อง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นแก้ไข เปลี่ยนแปลงหรือลบข้อมูลส่วนนั้นได้ โดยหน่วยงานของรัฐจะพิจารณาคำขอนั้น และแจ้งบุคคลนั้นทันทีว่าจะแก้ไขหรือไม่ เป็นต้น

5. แหล่งที่มาของข้อมูล เช่น ได้ข้อมูลจากที่ใด จากเจ้าของข้อมูล เป็นต้น

ทั้งนี้ในส่วนที่เป็นข้อมูลข่าวสารของราชการ หน่วยงานของรัฐจะพิมพ์ลงราชกิจจานุเบกษาตามมาตรา 7 ขณะเดียวกันยังต้องนำข้อมูลข่าวสารส่วนบุคคลพิมพ์ลงในราชกิจจานุเบกษาตามาตรา 23 ด้วย

อย่างไรก็ตาม ก็ยังมีข้อยกเว้นสำหรับหน่วยงานบางแห่งที่ไม่ต้องปฏิบัติตามก็ได้ ด้วยเหตุผลในการเก็บข้อมูลข่าวสารเป็นความลับ เพื่อประโยชน์ต่อความมั่นคงและความปลอดภัยแห่งชาติ โดยที่หน่วยงานดังกล่าว ได้แก่ สำนักงานข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานของรัฐที่กำหนดในกฎกระทรวง ตามความเห็นชอบของคณะกรรมการข้อมูลข่าวสารของราชการ กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขที่ไม่ต้องนำข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลตามมาตรา 23 วรรคแรก (3) ลงพิมพ์ในราชกิจจานุเบกษาก็ได้

(4) การตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลให้ถูกต้องอยู่เสมอ หน่วยงานของรัฐจะทำการแก้ไขข้อมูลข่าวสารที่บันทึกผิดพลาดทั้งที่เป็นของเอกชนขอให้แก้และข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบอยู่เสมอ เพราะหากข้อมูลไม่ถูกต้องอาจก่อความเสียหายหรือเป็นการตัดสิทธิของบุคคลนั้นไป

(5) การจัดระบบรักษาความปลอดภัย โดยหลักการแล้วข้อมูลส่วนบุคคลจะไม่เปิดเผยต่อบุคคลทั่วไป ดังนั้นหน่วยงานของรัฐต้องมีกฎระเบียบและมาตรการในการเก็บรักษาและการเข้าถึงข้อมูลข่าวสารส่วนบุคคล เพื่อรักษาความปลอดภัยของข้อมูลข่าสารส่วนบุคคลดังกล่าว

3) การเปิดเผยข้อมูลข่าวสารส่วนบุคคล โดยทั่วไปแล้ว หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นไม่ได้ เว้นแต่เป็นการเปิดเผยตามมาตรา 24 โดยสรุปแล้วผู้ที่สามารถเข้าถึงข้อมูลส่วนบุคคล คือ

“ก .เจ้าของข้อมูล

ข. ผู้ที่ข้าวของข้อมูลให้ความยินยอมเป็นหนังสือไว้ล่วงหน้าหรือในขณะนั้น

ค. ผู้ที่อาจรับรู้ข้อมูลข่าวสารส่วนบุคคลตามมาตรา 24 ซึ่งกรณีที่หน่วยงานของรัฐอาจเปิดเผยข้อมูลข่าวสารส่วนบุคคลให้แก่ผู้อื่นหรือหน่วยงานอื่นได้ พร้อมทั้งต้องทำบัญชีแสดงการเปิดเผยข้อมูลข่าวสารไว้ด้วย”

(1) กรณีที่หน่วยงานของรัฐอาจเปิดเผยข้อมูลข่าวสารบุคคลให้แก่ผู้อื่นหรือหน่วยงานอื่น ซึ่งกรณีดังกล่าวจะกระทำได้ดังนี้

ก.การเปิดเผยต่อเจ้าหน้าที่ของรับในหน่วยงานเพื่อนำไปใช้ตามอำนาจหน้าที่ หน่วยงานของรัฐซึ่งเป็นนิติบุคคลไม่สามารถดำเนินการใดๆ ได้ด้วยตนเอง จำเป็นต้องกระทำโดยผ่านทางจะเจ้าหน้าที่ของรัฐผู้ที่จะจัดเก็บและใช้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามอำนาจหน้าที่ของตน ดังนั้นผู้ที่จัดเก็บข้อมูลข่าวสารส่วนบุคคลจึงไม่ใช่ผู้ที่จะใช้ข้อมูลเหล่านั้นเพียงคนเดียว เช่น เจ้าหน้าที่กองการเจ้าหน้าที่เป็นผู้เก็บประวัติข้าราชการ แต่ข้อมูลข่าวสารส่วนบุคคลนั้น ยังมีเจ้าหน้าที่อื่นที่มีความจำเป็นในการใช้ข้อมูลข่าวสารนั้น เช่น ผู้บังคับบัญชาต้องใช้ข้อมูลข่าวสารส่วนบุคคลเพื่อแสดงการประเมินผลงานเพื่อเลื่อนขั้นและตำแหน่ง หรือเพื่อประกอบการพิจารณาลงโทษทางวินัยแก่ข้าราชการในหน่วยงานนั้น ดังนั้นเจ้าหน้าที่ที่เก็บรักษาข้อมูลข่าวสารส่วนบุคคลจึงมีอำนาจเปิดเผยข้อมูลนั้นต่อเจ้าหน้าที่อื่นในหน่วยงานท่มีความจำเป็นต้องใช้ข้อมูลข่าวสารเพื่อการปฏิบัติงานตามอำนาจหน้าที่ โดยไม่ต้องได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ข.การเปิดเผยโดยการใช้ข้อมูลตามปกติ หน่วยงานของรัฐต้องแจ้งวัตถุประสงค์ที่นำข้อมูลข่าวสารไปใช้แก่เจ้าของข้อมูล และต้องประกาศลักษณะการใช้ข้อมูลตามปกติลงในราชกิจจานุเบกษาด้วย กล่าวคือ การใช้ข้อมูลข่าวสารส่วนบุคคลตามวัตถุประสงค์ของการจัดระบบข้อมูลข่าวสารส่วนบุคคลจึงเป็นเรื่องที่หน่วยงานของรัฐมีอำนาจทำได้และเจ้าของข้อมูลข่าวสารย่อมรู้อยู่แล้ว

ค.การเปิดเผยต่อหน่วยงานของรัฐด้านการวางแผนสถิติและสำมะโน กฎหมายกำหนดให้สามารถเปิดเผยข้อมูลข่าวสารส่วนบุคคลแก่หน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติหรือสำมะโนต่างๆ ซึ่งต้องเก็บรักษาข้อมูลข่าวสารส่วนบุคคลไม่ให้เปิดเผยไปยังบุคลอื่นที่ไม่มีอำนาจหน้าที่ เช่น การให้ข้อมูลข่าวสารแก่สำนักงานสถิติแห่งชาติ ได้แก่ การเก็บรวบรวมข้อมูลเกี่ยวกับประชากร เคหะ การเกษตร อุตสาหกรรม ธุรกิจ และการอื่นเพื่อใช้ประโยชน์ในทางสถิติ เช่น พระราชกฤษฎีกาการทำสำมะโนประชากรและเคหะ พ.ศ. 2532 [88] กำหนดให้สำนักงานสถิติแห่งชาติ จัดทำสำมะโนประชากรและเคหะเพื่อทราบสถิติเกี่ยวกับจำนวนประชากรและเคหะ รวมทั้งรายละเอียดเกี่ยวกับประชากรในเรื่อง เพศ อายุ สัญชาติ สถานที่เกิด การศึกษา สถานภาพการสมรส จำนวนบุตร จำนวนที่อยู่อาศัย ฐานะทางเศรษฐกิจ เพื่อประโยชน์ในการวางแผนพัฒนาท้องถิ่นและกำหนดนโยบายในการพัฒนาเศรษฐกิจและสังคมของประเทศ และเพื่อใช้ประกอบการวางแผนงานบริหารของหน่วยงานต่างๆ

---

[88] ฤทัย หงส์สิริและมานิตย์ จุมปา, 2542: 94

ทั้งของรัฐและของเอกชน เป็นต้น โดยพระราชบัญญัติสถิติ พ.ศ. 2508 ได้กำหนดให้ข้อมูลความหรือตัวเลขที่ได้มานั้นเป็นความลับ ห้ามผู้ที่มีหน้าที่ปฏิบัติการตามกฎหมายนี้เปิดเผยข้อความหรือตัวเลขดังกล่าว เว้นแต่เพื่อประโยชน์ในการสอบสวนหรือการพิจารณาคดีที่บุคคลนั้นต้องหาว่าการกระทำความผิดต่อพระราชบัญญัตินี้

ง.การเปิดเผยเป็นการใช้ประโยชน์ในการศึกษาวิจัย การเปิดเผยข้อมูลข่าวสารส่วนบุคคลเพื่อการศึกษาวิจัยย่อมกระทบต่อสิทธิส่วนบุคคล กฎหมายจึงให้สิทธิเปิดเผยเพียงข้อมูลที่ไม่ระบุชื่อหรือสิ่งที่ทำให้รู้ว่าเป็นบุคคลใด

จ.การเปิดเผยต่อหอจดหมายเหตุแห่งชาติ กฎหมายให้หน่วยงานของรัฐที่ไม่ประสงค์จะเก็บข้อมูลข่าวสารส่วนบุคคลอีกต่อไป ต้องส่งข้อมูลข่าวสารส่วนบุคคลไปยังหอจดหมายเหตุแห่งชาติหรือหน่วยงานอื่นตามที่กำหนดภายหลัง เพื่อตรวจสอบคัดเลือกเก็บไว้เพื่อการศึกษาค้นคว้าของประชาชน

ฉ.การเปิดเผยต่อเจ้าหน้าที่ของรัฐเพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย หน่วยงานของรัฐสามารถเปิดเผยข้อมูลข่าวสารส่วนบุคคลต่อเจ้าหน้าที่ของรัฐเพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวนการสอบสวน หรือการฟ้องคดี เพื่อประโยชน์ในการบังคับใช้กฎหมาย

ช.การเปิดเผยซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล ประเด็นระหว่างการคุ้มครองข้อมูลข่าวสารส่วนบุคคลกับการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคลแล้ว กฎหมายจะให้ความสำคัญต่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคลมากกว่าทำให้สามารถเปิดเผยข้อมูลข่าวสารส่วนบุคคลได้

ซ.การเปิดเผยต่อศาลและเจ้าหน้าที่ของรัฐหรือบุคคลที่มีอำนาจตามกฎหมาย

ฌ.กรณีอื่นตามที่กำหนดโดยพระราชกฤษฎีกา

(2)หน้าที่ของหน่วยงานของรัฐในการจัดทำบัญชีแสดงการเปิดเผยข้อมูลข่าวสาร

ในการเปิดเผยข้อมูลข่าวสารใน (3) – (9) ข้างต้น หน่วยงานของรัฐต้องจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวนั้น เพื่อให้เจ้าของข้อมูลสามารถรู้ได้ว่า มีผู้ใดหรือหน่วยงานใดมาขอให้เปิดเผยข้อมูลข่าวสารส่วนบุคคลของตน การที่กฎหมายให้ทำบัญชีและ

เฉพาะข้อ (3) – (9) เท่านั้น โดย (1) และ (2) ไม่ได้กำหนดทำ ทั้งนี้เพราะทั้งสอง (1) และ 2) เป็นกรณีที่เจ้าของข้อมูลทราบอยู่แล้วว่าหน่วยงานของรัฐจะใช้ข้อมูลข่าวสารส่วนบุคคลในลักษณะใดหรือจะเปิดเผยกับเจ้าหน้าที่หรือหน่วยงานใด โดยการประกาศข้อความเกี่ยวกับลักษณะการใช้ข้อมูลตามปกติลงในราชกิจจานุเบกษา หรือแจ้งให้เจ้าของข้อมูลทราบในกรณีที่ขอข้อมูลจากเจ้าของข้อมูลโดยตรง

ในการจัดทำบัญชีแสดงการเปิดเผยนั้น ได้มีหลักเกณฑ์และวิธีการกำหนดไว้ตามกฎกระทรวง ดังนี้

ก.ให้จัดทำบัญชีแสดงการเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามมาตรา 24 (3) ถึง (9) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พร้อมสำเนาชุดหนึ่ง โดยอย่างน้อยต้องมีรายการตามบัญชีแสดงการเปิดเผยข้อมูลข่าวสารส่วนบุคคล และเก็บรักษาไว้กับเจ้าหน้าที่ผู้ควบคุมดูแลข้อมูลข่าวสารดังกล่าว

ข.ให้หน่วยงานของรับจัดเก็บรวบรวมบัญชีหรือสำเนาบัญชีแสดงการเปิดเผยข้อมูลข่าวสารส่วนบุคคลให้เป็นระบบกำกับไว้กับข้อมูลข่าวสารนั้น เพื่อความสะดวกในการเก็บรักษาของหน่วยงานของรัฐและตรวจของบุคคลที่ขอตรวจข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวข้องกับตนตามมาตรา 25

กรณีที่บัญชีแสดงการเปิดเผยข้อมูลข่าวสารส่วนบุคคลมีส่วนที่ไม่ควรเปิดเผยแก่ผู้ขอตรวจดูหรือยืมอยู่ด้วย หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐจะต้องตัดรายการใดออกจากรายการในบัญชีที่เปิดเผยก็ได้ แต่อย่างน้อยก็ต้องคงรายการที่แสดงลำดับที่ วัน เดือน ปี ที่ขอตรวจหรือขอยืมไว้ พร้อมทั้งเหตุผลที่ไม่เปิดเผยไว้ด้วย

(3)การตรวจดูข้อมูลข่าวสารส่วนบุคคลโดยเจ้าของข้อมูล

กฎหมายได้ให้สิทธิแก่เจ้าของข้อมูลในการตรวจดู เพื่อป้องกันการผิดพลาดในกระบวนการจัดเก็บ ตามมาตรา 25 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่ระบุว่าบุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา 9 วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม

การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้

ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน ส่วนใดไม่ถูกต้องตามที่เป็นจริงให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอ ให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวันนับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ต่อคณะกรรมการ และไม่ว่ากรณีใดๆ ให้เจ้าของมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนที่เกี่ยวข้องได้

ให้บุคคลตามที่กำหนดในกฎกระทรวงมีสิทธิดำเนินการตามมาตรา 23 มาตรา 24 และมาตรานี้แทนผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ หรือเจ้าของข้อมูลที่ถึงแก่กรรม”

จากมาตราดังกล่าวจะเห็นว่ามีหลักการในการตรวจดูข้อมูลข่าวสารส่วนบุคคลโดยเจ้าของข้อมูล มีดังนี้

(1) ข้อมูลข่าวสารส่วนบุคคลที่ขอตรวจดูต้องไม่ใช่ข้อมูลข่าวสารราชการที่เปิดเผยไม่ได้ ข้อมูลข่าวสารส่วนบุคคลที่จะตรวจดูนี้ต้องไม่เป็นข้อมูลข่าวสารที่เปิดเผยไม่ได้ตามมาตรา 14 หรือมาตรา 15 กล่าวคือ ข้อมูลข่าวสารส่วนบุคคลแม้เป็นเรื่องส่วนตัวของบุคคลหากเข้ากรณีที่กฎหมายห้ามเปิดเผย บุคคลแม้จะเป็นเจ้าของข้อมูลข่าวสารนั้นก็ขอตรวจดูไม่ได้ ถึงกระนั้น หากข้อมูลข่าวสารที่ขอตรวจดูนั้นมีบางส่วนที่ต้องห้ามไม่ให้เปิดเผยตามมาตร 14 หรือ 15 อยู่ ก็สามารถตรวจดูได้ แต่หน่วยงานของรัฐต้องลบหรือตัดทอนหรือทำอย่างอื่นเพื่อไม่เปิดเผยข้อมูลข่าวสารนั้น หรือจะเป็นกรณีที่เอกสารใดมีข้อมูลข่าวสารส่วนบุคคลของบุคคลอื่นรวมอยู่ด้วย ก็ต้องลบหรือตัดทอนข้อความดังกล่าวออก

(2) ผู้มีสิทธิตรวจดู ผู้มีสิทธิโดยปกติ ได้แก่ เจ้าของข้อมูลข่าวสารโดยการตรวจดูนี้หน่วยงานของรัฐอาจวางหลักเกณฑ์เรียกค่าธรรมเนียมก็ได้

ตัวอย่างกรณีของผู้ป่วย เมื่อวันที่ 16 เมษายน 2541 แพทยสภา สภาการพยาบาล สภาพเภสัชกรรม ทันตแพทยสภา และคณะกรรมการควบคุมการประกอบโรคศิลป์ ได้ร่วมกันออกประกาศรับรองสิทธิของผู้ป่วยไว้หลายประการ ซึ่งสอดคล้องกับสิทธิของเจ้าของข้อมูลข่าวสารส่วนบุคคลตามกฎหมาย เช่น ผู้ป่วยมีสิทธิรับทราบข้อมูลอย่างเพียงพอและ

ชัดเจน เพื่อเลือกตัดสินใจในการยินยอมหรือไม่ยินยอมให้ผู้ประกอบการวิชาชีพด้านสุขภาพปฏิบัติต่อตน ผู้ป่วยมีสิทธิให้ปกปิดข้อมูลเกี่ยวกับตนเองโดยเคร่งครัด ผู้ป่วยมีสิทธิรับทราบข้อมูลเกี่ยวกับการรักษาพยาบาลเฉพาะของตนที่ปรากฏในเวชระเบียนเมื่อร้องขอ (ฤทัย หงส์สิริ และมานิตย์ จุมปา, 2542: 100)

กรณีที่เจ้าของข้อมูลข่าวสารส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ หรือเจ้าของข้อมูลถึงแก่กรรม (มาตรา 25 วรรคท้าย) ก็ได้มีกฎกระทรวงฉบับที่ 2 (พ.ศ. 2541) กำหนดให้บุคคลต่อไปนี้เป็นผู้มีสิทธิดำเนินการให้ความยินยอมในการเปิดเผยข้อมูลข่าวสารส่วนบุคคล (มาตรา 24) รับแจ้งการเปิดเผยข้อมูลข่าวสารส่วนบุคคล (มาตรา 23) และตรวจสอบข้อมูลข่าวสาร (มาตรา 25) คือ

“ข้อ 1 ในกรณีเจ้าของข้อมูลเป็นผู้เยาว์ ให้ผู้ใช้อำนาจปกครองมีสิทธิดำเนินการแทนตามมาตรา 25 วรรคห้า

การดำเนินการตามวรรคหนึ่ง ถ้าผู้เยาว์มีอายุไม่ต่ำกว่า 15 ปี ต้องได้รับความยินยอมจากผู้เยาว์ด้วย

ข้อ 2 ในกรณีเจ้าของข้อมูลเป็นคนไร้ความสามารถ ให้ผู้อนุบาลมีสิทธิดำเนินการแทนตามมาตรา 25 วรรคห้า

ข้อ 3 ในกรณีเจ้าของเป็นคนเสมือนไร้ความสามารถ ไม่สามารถทำตามมาตรา 23 หรือ มาตรา 24 และมาตรา 25 ด้วยตนเอง เพราะเหตุมีกายพิการหรือจิตฟั่นเฟือนไม่สมประกอบ หรือมีเหตุอื่นทำนองเดียวกัน ให้ผู้พิทักษ์มีสิทธิดำเนินการแทนตามมาตรา 24 ได้ตามลำดับก่อนหลัง ดังต่อไปนี้

(1) บุตรชอบด้วยกฎหมายหรือบุตรบุญธรรม”
(2) คู่สมรส
(3) บิดามารดา
(4) ผู้สืบสันดาน
(5) พี่น้องร่วมบิดามารดา
(6) คณะกรรมการข้อมูลข่าวสารของราชการ

ในกรณีตามมาตรา 23 และมาตรา 25 ห้ามบุคคลตามข้อ 4 (1) (2) (3) (4) และ (5) มีสิทธิดำเนินการแทนได้ ไม่ว่าบุคคลหนึ่งบุคคลใดจะมีความเห็นเช่นใดก็ตาม

เห็นได้ว่า การกำหนดตัวบุคลที่จะให้ความยินยอมในการเปิดเผย รับแจ้งการเปิดเผย และตรวจดูข้อมูลข่าวสารส่วนบุคคลนั้นจะยึดหลักของผู้มีอำนาจการแทนตามกฎหมาย เช่น ผู้ใช้อำนาจปกครอง เช่น บิดามารดาทำการแทนบุตรผู้เยาว์ ผู้อนุบาลทำการแทนคนไร้

ความสามารถ ผู้พิทักษ์ทำการแทนคนเสมือนไร้ความสามารถ และผู้ที่เป็นทายาทโดยธรรมดาตามประมวลกฎหมายแพ่งและพาณิชย์ เช่น บุตร คู่สมรส บิดามารดา เป็นต้น

(3) วิธีการขอตรวจดู

ในการขอตรวจดู เจ้าของข้อมูลข่าวสารส่วนบุคคลจะต้องมีคำขอเป็นหนังสือต่อหน่วยงานของรัฐที่ควบคุมดูแลข้อมูลอยู่นั้น และหน่วยงานของรัฐนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารที่เกี่ยวกับบุคคลนั้น

(4) การขอให้แก้ไขข้อมูลข่าวสารส่วนบุคคล

ถ้าบุคคลใดเห็นว่า ข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริงย่อมมีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ โดยหน่วยงานของรัฐที่ได้รับคำขอนั้นจะต้องพิจารณาคำขอดังกล่าวและมีคำสั่งว่าแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลที่เจ้าของข้อมูลอ้างว่าไม่ถูกต้องหรือไม่และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

ในกรณีที่หน่วยงานของรัฐไม่แก้ไขให้ตรงตามที่ผู้ขอ ผู้ยื่นคำขอมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายใน 30 วัน นับวันที่ได้รับคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารจะพิจารณาวินิจฉัยว่า จะให้แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารนั้นหรือไม่ ในกรณีที่คณะกรรมการวินิจฉัยเปิดเผยข้อมูลข่าวสารวินิจฉัยว่า หน่วยงานของรัฐไม่ต้องแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารนั้น หือไม่ว่ากรณีใด เจ้าของข้อมูลก็ยังมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารที่เกี่ยวข้องได้

(4) การคุ้มครองโดยพระราชบัญญัติสถิติ พ.ศ. 2508

เป็นการคุ้มครองต่อบุคคลหรือประชาชนทั่วไปเกี่ยวกับข้อมูลที่เกี่ยวข้องกับบุคคลนั้นว่าต้องเก็บไว้เป็นความลับ[89] การคุ้มครองต่อบุคคลหรือประชาชนทั่วไปเกี่ยวกับข้อมูลที่เกี่ยวข้องกับบุคคลนั้นๆ ว่าต้องจัดเก็บไว้เป็นความลับ ซึ่งจะครอบคลุมและกว้างขวางมากเกินไป เพราะในความเป็นจริงบรรดาข้อความหรือตัวเลขเฉพาะบุคคลหรือเฉพาะรายที่ได้กรอก

89 “มาตรา 21 บรรดาข้อความหรือตัวเลขเฉพาะบุคคลหรือเฉพาะรายที่ได้กรอกในใบแบบหรือใบกำหนดข้อถามนั้นต้องถือเป็นความลับโดยเคร่งครัด ห้ามมิให้ผู้ซึ่งมีหน้าที่ปฏิบัติงานตามพระราชบัญญัตินี้เปิดเผยข้อความหรือตัวเลขนั้นแก่บุคคลใดซึ่งไม่มีหน้าที่ปฏิบัติการตามพระราชบัญญัตินี้ เว้นแต่เพื่อประโยชน์แก่การสอบสวนหรือการพิจารณาคดีที่บุคคลนั้นต้องหาว่ากระทำความผิดต่อพระราชบัญญัติ”

ในใบแบบหรือใบกำหนดข้อถาม ได้พัฒนาไปเป็นฐานข้อมูลในระบบคอมพิวเตอร์แล้ว ซึ่งอาจจะอยู่ในรูปของภาพ เสียง หรือภาพยนตร์ เมื่อมาพิจารณาแล้ว “ข้อความหรือตัวเลข” จะเป็นเพียงตัวอักษรและตัวเลขเท่านั้น บทบัญญัตินี้จึงไม่ได้ให้การคุ้มครองข้อมูลรูปแบบที่เป็นภาพ เสียง หรือภาพยนตร์แต่อย่างใด

4.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

กฎหมายลิขสิทธิ์ไทยได้พยายามอธิบายถึง นิยามของคำต่างๆ ที่เกี่ยวข้องกับลิขสิทธิ์ไว้ในมาตรา 4 และได้แบ่งประเภทของลิขสิทธิ์ไว้เป็น 9 ประเภท พร้อมคำนิยามซึ่งแสดงให้เห็นถึงความพยายามของรัฐที่ตระหนักถึงการให้ความคุ้มครองลิขสิทธิ์เป็นไปอย่างชัดเจน

คำว่า “ลิขสิทธิ์” ตามพระราชบัญญัติลิขสิทธิ์ 2537 มาตรา 4 ให้นิยามว่า “ลิขสิทธิ์” หมายความว่า สิทธิแต่ผู้เดียวที่จะกระทำการใดๆ ตามพระราชบัญญัติลิขสิทธิ์เกี่ยวกับงานที่ผู้สร้าง สรรค์ได้ทำขึ้น (“copyright as the exclusive right to do any act under this Act in relation to work made by the author.) โดยมีวัตถุประสงค์ของการให้ความคุ้มครองมุ่งที่จะคุ้มครองสิทธิของผู้สร้างสรรค์ในงานที่ได้กระทำขึ้นด้วยสติปัญญา ความวิริยะอุตสาหะและแรงกาย และเพื่อให้เกิดประ โยชน์แก่มนุษยชาติ สิทธิที่ผู้สร้างสรรค์จะได้รับการคุ้มครองเป็นสิทธิแต่ผู้เดียวที่เปิดโอกาสให้สามารถกระทำการใดๆ ก็ได้เกี่ยวกับงานอันมีลิขสิทธิ์ของตน ดังนั้น เนื้อหาหรือถ้อยคำของคำนิยามของลิขสิทธิ์และวัตถุประสงค์จึงมีลักษณะสอดคล้องกับข้อความในคำปรารภของสนธิสัญญาที่ว่า “มุ่งให้เกิดการพัฒนาและรักษาการคุ้มครองสิทธิของผู้สร้างสรรค์ (Rights of Authors) ที่มีผลใช้บังคับอย่างแท้จริงและในรูปแบบที่เสมอกันและคล้ายกันมากที่สุด”

ส่วนคำว่า ”งานอันมีลิขสิทธิ์ คือ งานที่เกิดขึ้นจากการใช้สติปัญญา” ซึ่งภายใต้มาตรา 6 ได้มีการระบุประเภทของงานลิขสิทธิ์ไว้ชัดเจนว่า มีงานประเภทใดที่จะได้รับความคุ้มครองและงานแต่ละประเภทได้มีการนิยามไว้ในมาตรา 4 ได้แก่ งานวรรณกรรม นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ ซึ่งงานศิลปกรรมนั้นแบ่งออกได้เป็นงานจิตรกรรม งานประติมากรรม งานภาพพิมพ์ งานสถาปัตยกรรม งานภาพถ่าย งานภาพประกอบ งานศิลป-ประยุกต์ ทั้งนี้ ไม่ว่างานนั้นจะมีคุณค่าทางศิลปะหรือไม่ อย่างไรก็ตามมาตรา 6 ได้ระบุไว้อย่างชัดเจนว่า “การคุ้มครองลิขสิทธิ์ไม่คลุมถึงความคิดหรือขั้นตอน กรรมวิธี หรือระบบ หรือวิธีใช้ทำงาน หรือแนวความคิด หลักการ การค้นพบ หรือทฤษฎีทางวิทยาศาสตร์หรือคณิตศาสตร์” ซึ่งสอดคล้องและมีลักกษณะเดียวกับการคุ้ม ครองลิขสิทธิ์ตามสนธิสัญญา

WIPO ในข้อ 2 ดังนี้ “Copyright Protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.” **และเมื่อเปรียบเทียบกับคำนิยามของกฎหมายประเทศอื่น ๆ ย่อมมีลักษณะใกล้เคียงกัน ดังเช่น** คำนิยามตามกฎหมายลิขสิทธิ์ของสหรัฐใน title 17 กล่าวว่า”การคุ้มครองลิขสิทธิ์เป็นการคุ้มครองรูปแบบหนึ่งที่ให้แก่ผู้สร้างสรรค์งานดั้งเดิม (original works of authorship) รวมถึง งานวรรณกรรม การแสดง งานดนตรีกรรม ศิลปกรรมและงานทรัพย์สินทางปัญญา”

มาตรา 12 บัญญัติให้การนำงานอันมีลิขสิทธิ์มารวบรวมหรือประกอบเข้ากันโดยได้รับอนุญาตจากเจ้าของลิขสิทธิ์หรือการนำเอาข้อมูลหรือสิ่งอื่นใดซึ่งสามารถอ่านหรือถ่ายทอดได้โดยอาศัยเครื่องกลหรืออุปกรณ์อื่นใด ซึ่งงานส่วนนี้อาจจะไม่มีลิขสิทธิ์ หากการรวบรวมหรือประกอบเข้ากันได้กระทำในลักษณะที่เป็นการสร้างสรรค์งานโดยการคัดเลือกหรือจัดลำดับ โดยมิได้ลอกเลียนงานของบุคคลอื่น ให้ผู้รวบรวมมีลิขสิทธิ์ที่รวบรวม หรือประกอบเข้ากัน แต่ไม่กระทบกระเทือนถึงสิทธิของเจ้าของลิขสิทธิ์ที่มีอยู่ในงานหรือข้อมูลหรือสิ่งใดของผู้สร้างสรรค์เดิมที่ถูกนำมารวบรวม

สำหรับ ”งานอันมีลิขสิทธิ์” ให้หมายรวมถึง งานสร้างสรรค์ใดๆ ทางทรัพย์ สินทางปัญญาเกี่ยงกับงานวรรณกรรม ศิลปกรรม หรือวิทยาศาสตร์ และหมายรวมถึงงานด้านอื่นๆ ด้วยซึ่งสร้างสรรค์ขึ้นในรูปแบบต่างๆ เช่น งานที่มีลักษณะเป็นวาจกรรม (Oral Works) เป็นงานที่สร้างสรรค์โดยการพูดและไม่ได้บันทึกลงในวัตถุใดๆ เช่น ปาฐกถาสด บรรยาย การพิจารณาคดีในศาล ซึ่งในเรื่องของการพิจารณาคดีในศาลเมื่อเทียบกับกฎหมายจะพบว่า คำพิพากษาไม่ได้รับความคุ้มครองว่า เป็นงานอันมีลิขสิทธิ์ตามมาตรา 7 ของพระราชบัญญัติลิขสิทธิ์ 2537 ได้กำหนดสิ่งซึ่งไม่ถือว่าเป็นงานอันมีลิขสิทธิ์ ดังนี้ ข่าวประจำวันและข้อเท็จจริงต่างๆ ที่มีลักษณะเป็นเพียงข่าสาร รัฐธรรมนูญและกฎหมาย ระเบียบ ข้อบังคับ ประกาศ คำสั่ง คำชี้แจง และหนังสือโต้ตอบของกระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐหรือของท้องถิ่น คำพิพากษา คำสั่ง คำวินิจฉัยและรายงานทางราชการ คำแปลและการรวบรวมสิ่งต่างๆ ตาม 1 ถึง 4 ที่กระทรวง ทบวง กรม หรือหน่วยงานอื่นใดของรัฐ หรือของท้องถิ่นจัดทำขึ้น ซึ่งประเด็นในเรื่องข่าวประจำวันใดมีลักษณะเป็นข่าวสาร มิใช่งานในแผนกวรรณคดี แผนกวิทยาศาสตร์และแผนกศิลปะย่อมอาจก่อปัญหาในเรื่องการตีความได้

การคุ้มครองฐานข้อมูลมีมาตั้งแต่อนุสัญญาเบอร์น ข้อตกลง TRIPS และสนธิสัญญาลิขสิทธิ์ของ WIPO โดยหลักการ “ฐานข้อมูลได้รับความคุ้มครองเนื่องมาจากการคัดเลือก และหรือการเรียบเรียงซึ่งถือว่า เป็นการใช้สติปัญญาสร้างสรรค์ ซึ่งทั้งข้อตกลง TRIPS และสนธิสัญญาลิขสิทธิ์ได้รับการปรับปรุงจากถ้อยคำของอนุสัญญาเบอร์น เพื่อรับมือกับ

เทคโนโลยียุคดิจิตอลเพราะข้อตกลง TRIPS และสนธิสัญญานี้ใช้ถ้อยคำว่า ”การรวบรมข้อมูลหรือวัสดุอื่น”

สำหรับประเทศไทยแต่เดิมการรวบรวมข้อมูลมิใช่งานอันมีลิขสิทธิ์หากเป็นการคัดเลือก หรือจัดลำดับใหม่จะไม่ได้รับการคุ้มครอง แต่กฎหมายลิขสิทธิ์ฉบับใหม่นี้ยอมรับสิทธิประเภทนี้ทั้งนี้โดยไม่กระทบกระเทือนสิทธิของเจ้าของลิขสิทธิ์ที่มีอยู่ในงานหรือข้อมูลเดิมที่ถูกนำมารวบรวมเข้ากัน ซึ่งการวางกรอบของกฎหมายลิขสิทธิ์นี้เป็นไปตามอนุสัญญาเบอร์นและข้อตกลง TRIPS โดยบัญญัติไว้ในมาตรา 12 ดังนี้”งานใดมีการนำเอาลักษณะงานอันมีลิขสิทธิ์ตามพระราชบัญญัตินี้มารวบรวมหรือประกอบเข้ากัน โดยได้รับอนุญาตจากเจ้าของลิขสิทธิ์หรือเป็นการนำเอาข้อมูลหรือสิ่งอื่นใดซึ่งสามารถอ่านหรือถ่ายทอดได้ โดยอาศัยเครื่องกลหรืออุปกรณ์อื่นใดมารวบรวมหรือประกอบเข้ากัน หากผู้ที่ได้รวบรวมหรือประกอบเข้ากัน ได้รวบรวมหรือประกอบเข้ากันซึ่งงานดังกล่าวขึ้นโดยการคัดเลือกหรือจัดลำดับในลักษณะซึ่งไม่ได้ลอกเลียนงานของบุคคลอื่นให้ผู้ได้รวบรวมหรือประกอบเข้ากันนั้นมีลิขสิทธิ์ในงานที่ได้รวบรวมหรือประกอบเข้ากันตามพระราชบัญญัตินี้ แต่ทั้งนี้ไม่กระทบกระ เทือนสิทธิของเจ้าของลิขสิทธิ์ที่มีอยู่ในงานหรือข้อมูล หรือสิ่งอื่นใดของผู้สร้างสรรค์เดิมที่ถูกนำมารวบรวมหรือประกอบเข้ากัน” จากข้อความนี้พบว่า การให้ความคุ้มครองฐานข้อมูลภายใต้พระราช บัญญัติลิขสิทธิ์ 2537 มีลักษณะยืดหยุ่นและสอดคล้องกับสนธิสัญญาฉบับนี้เนื่องจากถ้อยคำที่ใช้”สิ่งอื่นใด” เป็นการคลุมถึงงานในรูปแบบใหม่ที่อาจมีขึ้นได้ในอนาคต เช่น คณะนี้ยุคดิจิตอลเป็นยุคที่มีอิทธิพลต่อชีวิตประจำวันของมนุษย์ทั่วโลก

5.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

ปัจจุบันยังไม่มีกฎหมายเฉพาะที่นำมาลงโทษผู้กระทำผิดได้เกี่ยวกับข้อมูลในคอมพิวเตอร์ได้ อย่างไรก็ตามหน่วยงานที่บังคับใช้กฎหมายพยายามที่จะปรับการกระทำผิดดังกล่าวให้เข้ากับฐานความผิดตามประมวลกฎหมายอาญา หรือความผิดตามพระราชบัญญัติที่มีลักษณะใกล้เคียงกัน แต่ก็ส่งผลให้เกิดปัญหาการตีความ เช่น กรณีความว่าข้อมูลมิใช่ทรัพย์จึงไม่อาจลงโทษผู้กระทำความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา มาตรา 334 หรือฐานทำให้เสียทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 358 หรือฐานบุกรุก ตามประมวลกฎหมายอาญา มาตรา 362 อย่างไรก็ตาม กฎหมายอาณาของไทยก็เป็นที่ยอมรับกันแล้วว่าไม่สามารถนำมาปรับใช้กับการกระทำผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ได้ครอบคลุม[90]

---

[90] องอาจ เทียนหิรัญ. “**อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์.”**

นอกจากนี้ มีผลการศึกษาที่เกี่ยวข้องกับปัญหากฎหมายการกระทำผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ได้แก่ [91]

จากการศึกษาของเลิศชาย สุธรรมพร (2541) ซึ่งศึกษาเกี่ยวกับความปลอดภัยของข้อมูล พบว่า ปัจจุบันยังไม่มีกฎหมายเฉพาะที่จะนำมาปรับใช้เพื่อลงโทษผู้กระทำผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ได้ อย่างไรก็ตาม เมื่อมีการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์เกิดขึ้น หน่วยงานที่บังคับใช้กฎหมายพยายามที่จะปรับการกระทำผิดดังกล่าวให้เข้ากับฐานความผิด ตามประมวลกฎหมายอาญาหรือความผิดตามพระราชบัญญัติที่มีลักษณะใกล้เคียงกัน แต่ก็ส่งผลให้เกิดปัญหาการตีความ เช่น กรณีตีความว่าข้อมูลมิใช่ทรัพย์ จึงไม่อาจลงโทษผู้กระทำความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 334 หรือฐานทำให้เสียทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 358 ได้

องอาจ เทียนหิรัญ (2546) ซึ่งศึกษาเกี่ยวกับการกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์ พบว่า การกระทำผิดต่อคอมพิวเตอร์เป็นอาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่ง ซึ่งทำให้เกิดผลกระทบต่อกฎหมายอาญาของประเทศต่าง ๆ ทั่วโลก กล่าวคือ การกระทำดังกล่าวอยู่นอกขอบเขตกฎหมายที่บังคับใช้อยู่ทำให้ไม่เป็นความผิดทางอาญา เนื่องจากกฎหมายอาญาของประเทศต่าง ๆ ล้วนแต่เน้นให้ความคุ้มครองแก่วัตถุที่มีรูปร่าง เช่น ทรัพย์ เป็นต้น เมื่อการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่าง ๆ เป็นการกระทำต่อวัตถุที่ไม่มีรูปร่าง ได้แก่ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ดังนั้น การกระทำความผิดต่อคอมพิวเตอร์จึงไม่เป็นความผิดทางอาญา

รัชฎาวรรณ ชัชวาล (2544) ซึ่งศึกษาเกี่ยวกับอาชญากรรมคอมพิวเตอร์บนอินเตอร์เน็ต พบว่า การประกอบกิจกรรมบนอินเตอร์เน็ตมีความแตกต่างกับการประกอบกิจกรรมที่เกิดขึ้นโดยทั่วไป จึงส่งผลให้เกิดความแตกต่างในการพิจารณาการกระทำผิดของอาชญากรรมคอมพิวเตอร์และอาชญากรรมทั่วไป คือ วัตถุแห่งการกระทำความผิดที่เปลี่ยนไปเป็นสิ่งที่ไม่สามารถจับต้องได้ หรือไม่มีลักษณะทางกายภาพ วิธีการกระทำความผิดรูปแบบใหม่ที่อาจไม่ต้องมีการกระทำทางกายภาพ ระยะเวลาในการกระทำความผิดที่เปลี่ยนไป ความรวดเร็วในการกระทำผิด และการไม่มีอาณาเขตของการกระทำผิดที่ชัดเจน

---

[91] ดูรายละเอียดได้จากวิทยานิพนธ์ดังกล่าว

นอกจากนี้ ยังพบว่าความรุนแรงและความเสียหายที่ต่างประเทศได้รับจากกรณีที่เกิดขึ้นนั้นมากกว่าในประเทศไทย อย่างไรก็ตาม กรณีการเกิดอาชญากรรมคอมพิวเตอร์บนอินเตอร์เน็ตในประเทศไทยมีแนวโน้มที่จะเพิ่มมากขึ้น เนื่องจากปัจจุบันกฎหมายอาชญากรรมคอมพิวเตอร์บนอินเตอร์เน็ตในประเทศไทยยังไม่สามารถนำมาบังคับใช้ได้ เพราะอยู่ในกระบวนการบัญญัติกฎหมาย ซึ่งธรรมชาติของผู้กระทำผิด หากประเทศใดที่ไม่มีมาตรการที่สามารถลงโทษกับผู้กระทำผิดได้อย่างมีประสิทธิภาพและประสิทธิผล ผู้กระทำผิดจะมุ่งก่ออาชญากรรมในประเทศนั้น

จักริน พันธ์ทอง (2543) ซึ่งศึกษาเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พบว่า มีปัญหาและอุปสรรคหลายด้าน ด้านนโยบายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของไทย ภาครัฐไม่มีนโยบายที่เฉพาะเจาะจงเกี่ยวกับปัญหาอาชญากรรมคอมพิวเตอร์ ด้านกฎหมายอาญาที่ใช้อยู่ในปัจจุบันไม่สามารถใช้ดำเนินคดีกับผู้กระทำผิดฐานอาชญากรรมคอมพิวเตอร์ได้ครอบคลุมในทุกกรณี การบังคับใช้กฎหมายของเจ้าพนักงานทำได้โดยการปรับตัวบทกฎหมายให้เข้ากับข้อเท็จจริงที่เกิดขึ้นเท่านั้น ปัญหาด้านการบริหารการจัดองค์กร ปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ต้องมีการจัดตั้งหน่วยงานที่มีอำนาจหน้าที่โดยเฉพาะสำหรับดำเนินการ โดยมีบุคลากรหรือคณะทำงานที่มีความรู้เชี่ยวชาญพิเศษ ทั้งในด้านคอมพิวเตอร์และการสืบสวนคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์เป็นผู้ปฏิบัติ และด้านการปฏิบัติงานของเจ้าพนักงาน ทั้งตำรวจ อัยการ และศาล ยังขาดความรู้ความเข้าใจเกี่ยวกับปัญหาอาชญากรรมคอมพิวเตอร์ เจ้าหน้าที่ตำรวจซึ่งเป็นเจ้าพนักงานผู้ปฏิบัติงานในปัจจุบันประสบปัญหาด้านต่าง ๆ ในการสืบสวน สอบสวน รวบรวมพยานหลักฐานทางคดี

สุรพันธ์ มั่นคงดี (2541) ซึ่งศึกษาเกี่ยวกับพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ พบว่า ในการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ต้องประสบปัญหาสำคัญ คือ ความสามารถทางเทคนิคของผู้สืบสวน ความจำเป็นในการเพิ่มทักษะการเรียนรู้ของเจ้าหน้าที่ตำรวจ ความยากลำบากในการแกะรอยผู้บุกรุกเข้าสู่ระบบ ปัญหาในการชี้และการรวบรวมพยานหลักฐาน การขาดสถิติและความรู้เกี่ยวกับรูปแบบ และลักษณะของอาชญากรรมคอมพิวเตอร์ ความยากลำบากในการติดตามวิวัฒนาการคอมพิวเตอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว ข้อจำกัดในการปรับใช้กฎหมายลักษณะพยานกับอาชญากรรมคอมพิวเตอร์

รติรส อัจฉริยะเสถียร (2544) ซึ่งศึกษาเกี่ยวกับการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ในประเทศไทย พบว่า ผลตอบแทนทางด้านวัตถุไม่มีผลต่อการลักลอบเข้าถึง

ข้อมูลทางคอมพิวเตอร์ ในขณะที่ผลตอบแทนทางด้านจิตใจมีผลต่อการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ และการที่ผู้กระทำผิดคิดว่าการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ของบุคคลอื่นไม่เป็นความผิด มีผลต่อการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ รวมทั้งแนวโน้มของอาชญากรรมคอมพิวเตอร์ในอนาคตเกี่ยวกับการลักลอบเข้าถึงข้อมูลทางคอมพิวเตอร์ จะมีความซับซ้อนและก่อให้เกิดความเสียหายมากยิ่งขึ้น

เชิดพันธุ์ อุปนิสากร (2542) ซึ่งศึกษาเกี่ยวกับความรับผิดทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต พบว่า นโยบายทางอาญาสำหรับผู้เจาะระบบคอมพิวเตอร์นั้นสามารถแยกพิจารณาได้เป็น 4 ประการ คือ ประการแรก มาตรการทางอาญาควรกำหนดขึ้นเพื่อลดหรือจำกัดแรงจูงใจในการกระทำของผู้เจาะระบบคอมพิวเตอร์ ประการที่สอง ควรบัญญัติกฎหมายเป็นพิเศษ เนื่องจากพบว่ากฎหมายที่มีอยู่ในปัจจุบันไม่สามารถรองรับกับผู้กระทำผิดได้ ประการที่สาม ควรกำหนดวิธีการลงโทษและระดับของโทษตามลักษณะของแรงจูงใจ ประการที่สี่ ควรสร้างความร่วมมือและเพิ่มประสิทธิภาพของหน่วยงานต่าง ๆ ในกระบวนการยุติธรรม

สำหรับประเทศไทย เนื่องจากการกระทำความผิดต่อคอมพิวเตอร์ทั้ง 6 รูปแบบดังกล่าวไม่เป็นความผิดตามประมวลกฎหมายอาญา ซึ่งเป็นกฎหมายอาญาหลักของประเทศไทย อีกทั้งในปัจจุบันประเทศไทยยังไม่มีกฎหมายในการคุ้มครองข้อมูลหรือการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse act) มาใช้ทำให้เกิดปัญหาในการปราบปรามอาชญากรรมทางคอมพิวเตอร์

จากสรุปผลการสัมมนาเกี่ยวกับปัญหาในการปราบปรามอาชญากรรมคอมพิวเตอร์ของสถาบันกฎหมายอาญา[92] มีดังนี้

1. ปัญหาอันเกิดจากสภาพไร้พรมแดนของอาชญากรรม

1.1 ปัญหาเขตอำนาจศาล อาชญากรรมคอมพิวเตอร์มีลักษณะไร้พรมแดน เกี่ยวกันกับได้หลายประเทศผู้กระทำความผิด ผู้เสียหาย สถานที่เกิดการกระทำความผิด และสถานที่เกิดผลแห่งการกระทำไม่จำเป็นต้องอยู่ในประเทศเดียวกัน ทำให้เกิดปัญหาว่าความผิดเกิดขึ้นในประเทศใด ศาลของประเทศใดควรมีอำนาจในการพิจารณาคดี

---

[92]สถาบันกฎหมายอาญา 2542, น. 160-161

1.2 ปัญหาความร่วมมือระหว่างประเทศในการดำเนินคดี สืบเนื่องจากปัญหาเขตอำนาจศาล หากต้องสืบสวน สอบสวน และดำเนินคดีในประเทศหนึ่ง จะขอความร่วมมือในทางคดีกับประเทศที่เกี่ยวข้องได้หรือไม่ และในขอบเขตมากน้อยเพียงใด

1.3 ปัญหาความต่างกันของกฎหมาย มาตรฐานทางวัฒนธรรม ศีลธรรมของแต่ละประเทศแตกต่างกัน อันทำให้กฎหมายทางอาญาของแต่ละประเทศแตกต่างกันได้ เช่น ประเทศหนึ่งกำหนดความผิดเรื่องการเผยแพร่ภาพลามากและการพนัน แต่อีกประเทศหนึ่งไม่มีกำหนดความผิดดังกล่าว ดังนี้ หากประเทศที่กำหนดความผิดต้องการดำเนินคดีความผิดนั้นกับบุคคลที่อยู่ในประเทศที่มิได้กำหนดความผิด ย่อมเกิดปัญหาการขอความร่วมมือระหว่างประเทศทางอาญา หรือการขอส่งผู้ร้ายข้ามแดนจากประเทศที่มิได้กำหนดความผิด

2. ปัญหากฎหมายสารบัญญัติ

2.1 ความล้าสมัยของกฎหมาย กฎหมายอาญาบัญญัติมานานแล้ว ซึ่งอาจไม่สามารถเอาความผิดกับการกระทำความผิดโดยใช้เทคโนโลยีสมัยใหม่ได้ เช่น กรณีการจูนมือถือ มีคำพิพากษาฎีกาว่าเป็นการแย่งคลื่นสัญญาณโทรศัพท์ ไม่ใช่เป็นการเอาทรัพย์ผู้อื่นไป ไม่เป็นความผิดฐานหลักทรัพย์ แต่เป็นความผิดฐาน ทำ มี และใช้เครื่องวิทยุคมนาคมโดยไม่ได้รับอนุญาต ตามพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498 ซึ่งเป็นกฎหมายเก่าและมีโทษต่ำ

2.2 การตีความโดยเคร่งครัดของกฎหมายอาญา

ความผิดเกี่ยวกับทรัพย์ อาชญากรรมคอมพิวเตอร์ในหลายกรณีเกี่ยวข้องกับการทำซ้ำ คัดลอก แก้ไข เปลี่ยนแปลง ลบ ทำลาย ซึ่งข้อมูล (Information) ที่เก็บในระบบคอมพิวเตอร์ มีปัญหาว่าข้อมูลเป็นทรัพย์ตามกฎหมายอาญาหรือไม่ เพราะทรัพย์ต้องมีรูปร่าง แต่ข้อมูลดังกล่าวไม่มีรูปร่างจะตีความขยายความให้ทรัพย์รวมถึงข้อมูลได้หรือไม่ ซึ่งจะเกี่ยวพันไปในประเด็นความผิดว่าจะเป็นความผิดฐานลักทรัพย์ ทำให้เสียทรัพย์ ฉ้อโกง บุกรุกหรือไม่

ความผิดเกี่ยวกับเอกสาร เอกสาร หมายถึง กระดาษ หรือวัตถุอื่นใดที่ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะสามารถตีความเอกสารให้ความหมายรวมถึงข้อมูลที่เก็บอยู่ในระบบคอมพิวเตอร์ได้หรือไม่

3. ปัญหากฎหมายวิธีบัญญัติ

3.1 การค้นและยึด

- การออกหมายค้นจะต้องสามารถระบุได้ว่าจะค้นสิ่งใดซึ่งอยู่ที่ใด แต่ข้อมูลคอมพิวเตอร์นั้นบางกรณีไม่อาจระบุได้ว่าอยู่ในรูปแบบใด เก็บไว้ที่ใด ประกอบด้วยสิ่งใดบ้าง

- หากในการค้นตามหมายค้น พบการกระทำความผิดฐานอื่น ซึ่งไม่เกี่ยวกับความผิดที่มีการออกหมายค้น จะสามารถดำเนินการกับสิ่งที่พบเห็นในขณะนั้นได้หรือไม่ เพราะเป็นการดำเนินการเกินกว่าที่กำหนดในหมายค้น

- การค้นข้อมูลในระบบเครือข่ายมีขอบเขตเพียงใด กล่าวคือ สามารถค้นเข้าไปในข้อมูลที่อยู่ต่างประเทศได้หรือไม่ จะสามารถทำสำเนาข้อมูลได้หรือไม่ ต้องขอความช่วยเหลือตามทางการกับประเทศนั้นหรือไม่

- การยึดพยานหลักฐานที่เป็นข้อมูลในคอมพิวเตอร์ ซึ่งเป็นสิ่งไม่มีรูปร่างจะทำโดยวิธีการใด

- หากข้อมูลที่จะยึดมาจากระบบเครือข่ายคอมพิวเตอร์ของผู้อื่น และมีอยู่มากมายหลายแห่ง จะสามารถยึดทั้งระบบได้หรือไม่

3.2 พยานหลักฐาน

ข้อมูลคอมพิวเตอร์เป็นพยานหลักฐานอิเล็กทรอนิกส์ จะจัดเป็นพยานเอกสารหรือพยานวัตถุตามกฎหมายเรื่องพยานหลักฐาน และศาลจะรับฟังพยานอิเล็กทรอนิกส์หรือไม่ หากทำสำเนาข้อมูลคอมพิวเตอร์เพื่อเป็นพยานหลักฐาน จะเกิดปัญหาว่าศาลจะรับฟังสำเนาพยานหลักฐานหรือไม่

รัฐบาลได้ตั้งคณะกรรมการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติ มีองค์กร คือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ เป็นเลขานุการ แต่คณะกรรมการและองค์กรดังกล่าวยังไม่ได้พิจารณาครอบคลุมถึงเรื่องการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ที่กำลังเกิดขึ้นในปัจจุบัน องค์กรบังคับใช้กฎหมายได้แก่เจ้าหน้าที่ในกระบวนการยุติธรรม คือ ตำรวจ อัยการ ศาล ราชทัณฑ์ โดยเฉพาะอย่างยิ่งตำรวจยังไม่มีความพร้อมในการรับมือกับปัญหาดังกล่าว แม้ว่าจะมีองค์กร คือ กองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ กองปราบปรามศูนย์ข้อมูลข้อสนเทศ แต่ยังมีปัญหาและอุปสรรคข้อขัดข้องในการดำเนินงาน ได้แก่

(1) ในเรื่องด้านกำลังพลยังขาดบุคคลที่มีคุณสมบัติพิเศษ มีความชำนาญเฉพาะอย่าง เฉพาะประเภทในการสืบสวนสอบสวน

(2) ปัญหาด้านประชาชนไม่ว่าจะผู้ใช้ส่วนบุคคลหรือองค์กร ยังขาดความสนใจต่อคดีอาชญากรรมบนอินเทอร์เน็ต จึงมีโอกาสตกเป็นเหยื่อของอาชญากรรมประเภทนี้อยู่ตลอดเวลา เนื่องจากมีความรู้สึกว่าเป็นอาชญากรรมที่ไม่รุนแรงหรือสะเทือนขวัญเช่นคดีอาญาทั่วไป

(3) ปัญหาด้านกฎหมาย ซึ่งถือเป็นเครื่องมือที่ใช้ในการควบคุมสังคมค่อนข้างล้าสมัย ไม่ทันต่อความเปลี่ยนแปลงกับสภาพความเป็นจริงที่เป็นอยู่ในปัจจุบัน

(4)ปัญหาด้านวิธีปฏิบัติ ไม่มีหน่วยงานที่รับผิดชอบโดยตรงในการสืบสวนและดำเนินคดีอาชญากรรมคอมพิวเตอร์บนอินเทอร์เน็ต ซึ่งควรมีหน่วยงานรับผิดชอบดำเนินการก่อนที่ความเสียหายจะเกิดขึ้นทำให้มักไม่ทันการณ์

(5)ปัญหาด้านการประสานงาน การร่วมมือกับองค์กรอื่นทั้งภาครัฐและเอกชนทั้งภายในและภายนอกประเทศ จะต้องมีการเพิ่มบทบาทให้มากขึ้น

จากการที่พัฒนาการทางเทคโนโลยีสารสนเทศแม้ได้มีการนำมาประยุกต์ใช้และก่อให้เกิดประโยชน์มากมายแก่มนุษย์ก็ตาม แต่หากนำไปใช้ในทางมิชอบก็อาจก่อให้เกิดความเสียหายทางเศรษฐกิจอย่างรุนแรงหรือส่งผลกระทบที่ร้ายแรงแก่สังคมได้ และเกิดรูปแบบใหม่ของอาชญากรรมที่เกิดจากการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดจึงจำเป็นต้องมีการพัฒนา “กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law)” หรือที่บางประเทศเรียกว่า “กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางมิชอบ (Computer Misuse Law)” ขึ้นหรือต้องปรับแก้ประมวลกฎหมายอาญาที่ใช้บังคับอยู่ในปัจจุบันให้ทันการด้วยการกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์หรือการใช้คอมพิวเตอร์ในทางมิชอบขึ้นให้เหมาะสมและมีประสิทธิภาพ

ประเทศต่าง ๆ ที่พัฒนาและออกกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้นใช้บังคับแล้ว อาทิ สหรัฐอเมริกา แคนาดา อังกฤษ ฝรั่งเศส เยอรมัน อิตาลี ญี่ปุ่น สิงค์โปร มาเลเซี และ Council of Europe ได้ออก Convention on Cyber-Crime เพื่อเป็นแนวทางให้ประเทศภาคีอนุสัญญาตรากฎหมายภายในขึ้นบังคับใช้ในทิศทางเดียวกัน เป็นต้น และอีกหลาย ๆ ประเทศที่อยู่ระหว่างการพัฒนากฎหมายขึ้นเพื่อใช้บังคับ แม้รูปแบบของการพัฒนากฎหมายในแต่ละประเทศอาจจะหลายหลายแตกต่างกันไปบ้าง แต่การกำหนดฐานความผิดหลักมักจะคล้ายคลึงกัน ทั้งนี้ โดยคำนึงถึงลักษณะของการใช้คอมพิวเตอร์ในการกระทำความผิดเป็นสำคัญ

สำหรับประเทศไทยมีการจัดทำร่างกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้นโดยมีสาระสำคัญคือ

ก.ลักษณะของการกระทำความผิด

การกระทำความผิดหรือการก่อให้เกิดภยันตรายหรือความเสียหายอันเนื่องมาจากการก่ออาชญากรรมทางคอมพิวเตอร์ อาจแบ่งออกได้เป็น 2 ลักษณะ ตามวัตถุหรือระบบที่ถูกกระทำ คือ

- การกระทำต่อระบบคอมพิวเตอร์ (Computer System)
- การกระทำต่อข้อมูลคอมพิวเตอร์

ข.การกำหนดฐานความผิดและบทกำหนดโทษ

การพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์ในเบื้องต้นนั้นพัฒนาขึ้นโดยคำนึงถึงแต่เพียงลักษณะการกระทำความผิดต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ซึ่งอาจสรุปความผิดสำคัญได้ 3 ฐานความผิด คือ

- การเข้าถึงโดยไม่มีอำนาจ (unauthorized access)
- การใช้คอมพิวเตอร์โดยไม่ชอบ (computer misuse)
- ความผิดเกี่ยวข้องกับคอมพิวเตอร์ (Computer related crime)

ทั้งนี้ตามร่างพระราชบัญญัติฉบับนี้ได้แบ่งการกระทำความผิดออกเป็นสองหมวดด้วยกัน คือ หมวดว่าด้วยความผิดเกี่ยวกับการรักษาความลับ ความครบถ้วน และการทำงานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ และหมวดว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์

การกำหนดบทลงโทษของการทำผิดภายใต้ พ.ร.บ.ฉบับนี้ มีโทษต่ำสุดตั้งแต่จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ ขณะที่โทษสูงสุดปรับไม่เกิน 140,000 บาท จำคุกไม่เกิน 7 ปี หรือทั้งจำทั้งปรับ เช่น กรณีที่มีการนำรูปภาพดารามาปรับแต่งให้เป็นภาพเปลือยหรือภาพอนาจารแล้วนำออกเผยแพร่ ทางอินเทอร์เน็ตจะมีโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ และถ้าสิ่งลามกอนาจารเกี่ยวข้องกับบุคคลอายุไม่เกิน 18 ปี ไม่ว่าผู้กระทำจะรู้หรือไม่ก็ตาม ต้องระวางโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

ขณะที่ผู้ทำการเปลี่ยนแปลงหรือลบข้อมูลทางคอมพิวเตอร์ เพื่อให้ได้มาซึ่งทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ นอกจากนี้ ข้อบัญญัติดังกล่าวยังให้อำนาจเจ้าพนักงานในการเข้าตรวจค้นโดยไม่ต้องมีหมายค้น หากมีเหตุเชื่อว่าได้กระทำผิดตามที่บัญญัติไว้ตามร่าง พ.ร.บ.นี้ เป็นต้น

2.6 กฎหมายคุ้มครองข้อมูลของประเทศไทย

ประเทศไทยยังไม่มีกฎหมายด้านนี้โดยเฉพาะ อีกทั้งกฎหมายที่ใช้ในการควบคุมสื่อในปัจจุบันก็ยังไม่มีประเด็นการคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมเข้าไป ซึ่งกฎหมายที่เกี่ยวข้องการใช้สื่อของไทยปัจจุบันมี 4 ฉบับคือ[93]

1) พระราชบัญญัติโทรเลขและโทรศัพท์ พ.ศ.2477
2) พระราชบัญญัติวิทยุคมนาคสม พ.ศ.2498
3) พระราชบัญญัติองค์การโทรศัพท์แห่งประเทศไทย พ.ศ.2497
4) พระราชบัญญัติการสื่อสารแห่งประเทศไทย พ.ศ.2519

พ.ร.บ.โทรเลขและโทรศัพท์ พ.ศ.2497 กำหนดว่าให้การบริการโทรเลขและโทรศัพท์เป็นอำนาจสิทธิขาดของรัฐแต่เพียงผู้เดียว โดยไม่ได้กำหนดความหมายของเครื่องโทรเลขหรือเครื่องโทรศัพท์ว่าอย่างไร มีเพียงแต่คำจำกัดความคำว่า เครื่องโทรเลขหรือเครื่องโทรศัพท์ หมายถึง เครื่องชนิดที่ใช้กำลังไฟฟ้า และรวมทั้งเครื่องใช้และเครื่องสำหรับส่งหรือทำการโทรเลขโทรศัพท์ หรือการคมนาคมอย่างอื่นโดยใช้ไฟฟ้า

จากคำวินิจฉัยของคณะกรรมการกฤษฎีกาในการให้ความเห็นทางกฎหมาย พ.ศ. 2524 ว่า การให้บริการโทรคมนาคมอันนอกเหนือจากบริการโทรเลขและโทรศัพท์ อันได้แก่ โทรพิมพ์ เทเล็กซ์ โทรภาพ โทรสาร ข้อมูลที่นำมาใช้กับระบบคอมพิวเตอร์อยู่ในความหมายของเครื่องโทรเลขและโทรศัพท์

แต่ในปัจจุบันด้วยสัญญาแบบ BTO (Build Transfer Operate) (เลอสรร ธนสุกาญจน์, สุธรรม อยู่ในธรรมและคณะ, 2539 : หน้า 63.) จะให้เอกชนผู้ให้บริการโทรคมนาคมรับผิดชอบติดตั้งบำรุงเครือข่ายและอุปกรณ์ในนามของรัฐ โดยต้องโอนทรัพย์สินทั้งหมดเกี่ยวกับการติดตั้ง และให้บริการโทรคมนาคมทั้งหมดให้แก่รัฐนับแต่วันแรกที่เสร็จสมบูรณ์ และพร้อมที่จะนำมาให้บริการ โดยเอกชนผู้โอนทรัพย์สินให้รัฐจะได้รับสิทธิที่จะใช้เครือข่ายเหล่านั้นในการให้บริการแก่ประชาชนโดยทั่วไปในนามของรัฐ และจะให้ค่าตอบแทนแก่รัฐเป็นรายปีตลอดอายุสัมปทาน เช่น สัญญาโครงการโทรศัพท์ 2 ล้านเลขหมายที่องค์การโทรศัพท์แห่งประเทศไทยให้สัมปทานกับบริษัทเทเลคอมเอเชียเพื่อให้บริการโทรคมนาคมขั้นพื้นฐานในเขต จะเห็นได้ว่าการที่เอกชนสามารถเข้าร่วมธุรกิจกับรัฐบาลได้นั้นก็จะสามารถนำพระราชบัญญัติ

---

93 เลอสรร ธนสุกาญจน์, สุธรรม อยู่ในธรรมและคณะ, **อ้างแล้ว** 2539 : หน้า 62.

ข้อมูลข่าวสารของราชการ พ.ศ.2540 มาบังคับใช้ได้ทันที อย่างไรก็ตามจากจุดอ่อนของพระราชบัญญัตินี้ ประกอบกับการพัฒนาทางเทคโนโลยีทางสื่ออิเล็กทรอนิกส์ได้เปลี่ยนแปลงอยู่ตลอดเวลาทำให้รูปแบบของข้อมูลข่าวสารเป็นจากเอกสารตัวจริง (ต้นฉบับเอกสาร) เป็นข้อมูลข่าวสารอิเล็กทรอนิกส์ ซึ่งก็มีปัญหาว่าข้อมูลที่ส่งผ่านกันด้วยสื่ออิเล็กทรอนิกส์นั้นยังใช้ในการอ้างอิงหรือเป็นหลักฐานทางกฎหมายใดๆ ไม่ได้ ดังนั้นเมื่อเกิดการละเมิดในข้อมูลข่าวสารอิเล็กทรอนิกส์ กฎหมายที่มีอยู่ก็ไม่ทันสมัยพอที่จะยอมรับการใช้ข้อมูลข่าวสารอิเล็กทรอนิกส์เพื่อนำมาใช้เป็นพยานหลักฐานในการดำเนินคดีต่อผู้กระทำความผิด

โดยสรุป พระราชบัญญัติหรือกฎหมายเกี่ยวกับสิทธิในข้อมูลข่าวสารส่วนบุคคลจากการใช้สื่ออิเล็กทรอนิกส์จะเอื้อผลประโยชน์ต่อประเทศไทยอย่างทั่วถึงมากกว่าจะส่งผลเสียของการมีกฎหมายดังกล่าวขอแบ่งลักษณะของประโยชน์ดังนี้[94]

ในส่วนของสภาพแวดล้อมภายในประเทศ องค์ประกอบสำคัญไม่ว่าจะเป็นภาคประชาชน ภาคธุรกิจเอกชนและภาครัฐ ต่างจะได้รับประโยชน์จากการคุ้มครองในข้อมูลข่าวสารส่วนบุคคลทั้งที่สามารถเปิดเผยได้และที่เป็นความลับ อยู่ 4 ประการ

ประการแรก ได้แก่ ทำให้เกิด “ความปลอดภัย” ในข้อมูลข่าวสารส่วนบุคคลว่าจะไม่ถูกภาคใดภาคหนึ่งนำไปใช้โดยไม่มีอำนาจหน้าที่ หรือนำไปใช้หาผลประโยชน์ส่วนตัวหรือจะเป็นการนำไปใช้ในทางที่ผิดกฎหมาย เพราะกฎหมายคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลจากการใช้สื่ออิเล็กทรอนิกส์ จะต้องระบุถึงลักษณะของข้อมูลข่าวสารส่วนบุคคล รูปแบบของสื่ออิเล็กทรอนิกส์ ผู้ที่มีอำนาจหน้าที่ในการใช้ข้อมูล ขอบเขตของการใช้ข้อมูล ตลอดจนการเก็บรักษาข้อมูล

ประการที่สอง ได้แก่ ทำให้เกิด “การป้องกันและปราบปราม” ต่อข้อมูลข่าวสารส่วนบุคคลโดยใช้มาตรการทางกฎหมาย ไม่ว่าจะเป็นการจัดตั้งองค์กรคุ้มครองข้อมูลข่าวสารส่วนบุคคลขึ้น โดยเฉพาะอย่างยิ่งเพื่อป้องกันการล่วงละเมิดในข้อมูลข่าวสารส่วนบุคคลจากนักเจาะระบบต่างๆ การพัฒนาเจ้าหน้าที่ให้มีความรู้ความสามารถในการติดตามการใช้ข้อมูลข่าวสารส่วนบุคคลในทางมิชอบ และกระบวนการในการพิสูจน์หลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ให้สามารถใช้เป็นหลักฐานยืนยันในทางคดี และสามารถใช้บังคับคดีได้ ตลอดจนการพัฒนาอุปกรณ์อิเล็กทรอนิกส์หรือระบบการป้องกันข้อมูลให้ทันสมัยอยู่ตลอดเวลา

---

[94] ปทีป เมธาคุณวุฒิ, **อ้างแล้ว** 2539 : หน้า 187-206

ประการที่สาม ได้แก่ ทำให้เกิด “การพัฒนากฎหมาย” คุ้มครองข้อมูลข่าวสารส่วนบุคคลและกฎหมายอื่นๆ ที่เกี่ยวข้อง เพื่อป้องกันช่องว่างทางกฎหมายในการกระทำความผิดได้ เห็นได้จากหัวใจของกฎหมายที่ว่า “ไม่มีโทษโดยไม่มีกฎหมาย” (Nulla poena sine lege) กล่าวคือ ถ้าไม่มีกฎหมายระบุการกระทำใดการกระทำหนึ่งว่าเป็นความผิดทางอาญา การกระทำนั้นก็ไม่ถือเป็นความผิดทางอาญา ดังนั้นจึงต้องตราและแก้ไขกฎหมายให้ครอบคลุมมากที่สุดกับลักษณะการใช้สื่ออิเล็กทรอนิกส์ที่ใช้อยู่ในปัจจุบันและในอนาคต

ประการที่สี่ ได้แก่ ทำให้เกิด “การมีส่วนร่วม” ของบุคคลทั้งที่อยู่ในภาคประชาชน ภาคธุรกิจเอกชนและภาครัฐ เพราะทุกคนต่างตื่นตัวที่จะรักษาสิทธิส่วนบุคคลในข้อมูลข่าวสารของตนเอง

ในส่วนของสภาพแวดล้อมระหว่างประเทศ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศจากที่ได้กล่าวมาแล้ว โดยเฉพาะกลุ่มประเทศยุโรปจะใช้หลักการประการหนึ่ง คือ ข้อบัญญัติว่าด้วยการจำกัดการถ่ายโอนข้อมูลไปยังประเทศนอกกลุ่มประชาคมยุโรป อนุญาตให้มีการถ่ายโอนข้อมูลไปยังประเทศที่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่น้อยกว่าที่กำหนดไว้ในกฎระเบียบ หากประเทศไทยสามารถพัฒนากฎหมายฉบับนี้ให้มีระดับมาตรฐานเท่าเทียมกับต่างประเทศเหล่านี้ได้จะเกิดประโยชน์ต่อประเทศไทยดังนี้

ประการแรก ได้แก่ สามารถขจัดกระบวน “การกีดกันในการติดต่อสื่อสาร” ได้โดยเฉพาะอย่างยิ่งทางด้านเศรษฐกิจการค้า ซึ่งจำเป็นต้องใช้ข้อมูลข่าวสารในประเทศต่างๆ ที่ทันสถานการณ์อยู่เสมอ

ประการที่สอง ได้แก่ สามารถสร้าง “ความเชื่อมั่น” ในการติดต่อสื่อสารกับประเทศไทย โดยจะมีประโยชน์ต่อการลงทุนทางเศรษฐกิจของต่างประเทศเข้าสู่ประเทศไทยอย่างยิ่ง

ประการที่สาม ได้แก่ สามารถสร้าง “ความร่วมมือ” ในการคุ้มครองข้อมูลข่าวสารจากการสื่อสารด้วยอิเล็กทรอนิกส์ชนิดต่างๆ ตลอดจนการดำเนินคดีต่อผู้กระทำความผิดหรืออาชญากรทางคอมพิวเตอร์ระหว่างประเทศได้ เมื่อพิจารณาถึงผลประโยชน์ดังกล่าวที่จะเกิดขึ้นกับประเทศไทยเราแล้ว แนวโน้มในอนาคตของระบบการสื่อสารทั่วโลกย่อมพัฒนาก้าวหน้าขึ้นเรื่อย สื่ออิเล็กทรอนิกส์จะพัฒนาเปลี่ยนแปลงเป็นเทคโนโลยีสารสนเทศรูปแบบใหม่ๆ เพิ่มขึ้น ประกอบกับประเทศไทยยังไม่มีกฎหมายใดที่คุ้มครองข้อมูลข่าวสารส่วนบุคคลได้ครอบคลุมเพียงพอ มีเฉพาะร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

บทที่ 4
การวิเคราะห์ข้อมูล

4.1การวิเคราะห์ปัญหาและอุปสรรคในการเชื่อมต่อข้อมูลของหน่วยงานในกระบวนการยุติธรรมในประเทศไทย

4.1.1ปัญหาและอุปสรรคของการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลสารสนเทศในกระบวนการยุติรรมของไทย

ปัญหาและอุปสรรคของการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลสารสนเทศในกระบวนการยุติรรมของไทย ได้แก่ การขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม ขาดการดำเนินการอย่างจริงจังและต่อเนื่องการดำเนินการยังขาดหน่วยงานที่เป็นเจ้าภาพหลักในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการประมวลผล ผู้บริหารระดับสูงยังไม่ให้ความสำคัญเท่าที่ควร ปัญหาด้านงบประมาณ งานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน ขาดความพร้อมทางด้านอุปกรณ์ต่าง ๆของทุกหน่วยงานในกระบวนการยุติธรรม ปัญหาการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน

ส่วนด้านปัญหาการเก็บรวบรวมข้อมูลที่มีความซับซ้อนนั้น ปัญหานี้มีสาเหตุจากการที่แต่ละหน่วยงานจะจัดเก็บกันเอง โดยมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ต่างฝ่ายต่างจัดเก็บ ก็ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก เพราะยังขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ส่งผลตามมาทำให้ข้อมูลมีความน่าเชื่อถือน้อย เพราะมีข้อมูลจำนวนมากที่ขาดการปรับปรุง เปลี่ยนแปลง ข้อมูลให้เป็นปัจจุบัน จัดเก็บแล้วก็ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน ด้านการคุ้มครองข้อมูลก็เป็นสิ่งที่จำเป็นเพราะถือว่าข้อมูลของบุคคลที่เป็นความลับส่วนบุคคล เป็นสิ่งที่เป็นผลเสียได้สำหรับบุคคลนั้น การเคารพสิทธิ์ในข้อมูลส่วนบุคคลจึงต้องมีอยู่และให้การคุ้มครอง

ปัญหาหลักอื่น ๆก็คือ การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ ซึ่งก็ส่งผลให้หลาย ๆหน่วยงานจึงขาดความพร้อม เพื่อการบูรณาการ

4.1.2 ปัญหาและอุปสรรคในกลุ่มประเทศ Common Law

ส่วนปัญหาและอุปสรรคในกลุ่มประเทศ Common Law จากการศึกษาเกี่ยวกับการประมวลผลข้อมูลเกี่ยวกับกระบวนการยุติธรรมและการนำเอาระบบข้อมูลเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมนั้น พบว่า[95] ประสบปัญหาและอุปสรรคดังต่อไปนี้

1.หน่วยงานในกระบวนการยุติธรรมมีหลากหลายมากเกินไปและความต้องการของหน่วยงานก็แตกต่างกัน ทำให้การกำหนดมาตรฐานและการประมวลผลข้อมูล แตกต่างกันออกไป เช่น องค์กรตำรวจมีความต้องการและใช้ข้อมูลเกี่ยวกับการสืบสวนและจับกุม แต่ในองค์กรศาลไม่ต้องการข้อมูลที่เกี่ยวกับการสืบสวน เป็นต้น ดังนั้น ทำให้การประมวลผลมีความยุ่งยาก และล่าช้า เพราะอาจจะต้องมีการจำแนกเป็นข้อมูลประเภท primary, secondary เป็นต้น

2.บางองค์กรในกระบวนการยุติธรรมยังไม่ให้ความสำคัญและจัดสรรงบประมาณให้น้อย ทำให้การดำเนินการเป็นไปอย่างล่าช้าและเชื่อมโยงข้อมูลได้ยาก เนื่องจากหลายๆองค์กรในกระบวนการยุติธรรม มองว่า หน่วยงานด้านเทคโนโลยีสารสนเทศเป็นหน่วยงานสนับสนุนการทำงานไม่ใช่หน่วยงานหลัก และหน่วยงานตนเองก็อาจไม่จำเป็นต้องใช้ข้อมูลที่ได้จากการเก็บและประมวลผล ดังนั้นจึงไปมุ่งให้ความสำคัญกับการปฏิบัติงานหลัก

3.หน่วยงานบางหน่วยงานยังมีขนาดเล็กเกินไปที่จะมีการจ้างบุคลากรที่มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศมาประมวลผลข้อมูลในกระบวนการยุติธรรม และการเป็นหน่วยงานเล็ก ข้อมูลน้อย การจ้างบุคลากรมาประจำเป็นการไม่คุ้มค่าใช้จ่ายในการดำเนินการองค์กร

4.การขาดการวางแผนระยะยาวในการดำเนินการ การจัดสรรงบประมาณอาจพิจารณาให้ไม่ต่อเนื่องให้เฉพาะบางปี ทำให้การประมวลผลก็ขาดความต่อเนื่องตามไปด้วย

5.การมีข้อจำกัดในด้านบุคลากรและการออกแบบเพื่อนำมาใช้งานหรือใช้ประโยชน์อย่างจริงจัง เนื่องจากการเก็บรวบรวมและแลกเปลี่ยนข้อมูลตลอดจนการบูรณาการข้อมูลในองค์กรจำเป็นจะต้องอาศัยบุคลากรที่มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะ

---

95 Dawes et al 2003; **SEARCH,** 2001 b

ด้านมาเป็นผู้ช่วยวางแผนและออกแบบระบบให้เหมาะสมกับองค์กรและการใช้งาน ซึ่งองค์กรหลายองค์กรในกระบวนการยุติธรรมก็ขาดบุคลากรด้านนี้โดยตรง การจัดหาจึงเป็นเพียงอุปกรณ์มาประจำ

6.การประสบปัญหาในด้านความเสี่ยงต่างๆ ปัญหาความเสี่ยงต่างๆที่เกิดขึ้นมีหลายประการ โดยเฉพาะอย่างยิ่ง จากด้าน ข้อมูลส่วนบุคคล (privacy) และ เรื่องความปลอดภัยของข้อมูล (security) นอกจากนี้ยังมีปัญหาความเสี่ยงอื่นๆตามมา อาทิ เช่น ความถูกต้องของข้อมูล การสร้างข้อจำกัดในการใช้ การเข้าไปใช้ข้อมูลโดยไม่ได้รับอนุญาต หรือไม่มีอำนาจอาชญากรรมคอมพิวเตอร์ เป็นต้น

7.ความหวาดกลัวในปัญหาเกี่ยวกับความรับผิด (liability) หากมีความผิดพลาดเกิดขึ้นกับข้อมูล โดยเฉพาะหากตนเองต้องรับผิดชอบโดยตรง ซึ่งความรับผิดจะเกิดขึ้นกับตน ซึ่งจะสร้างความยุ่งยากในการปฏิบัติงานในองค์กร ดังนั้น การดำเนินการประมวลผลและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม จึงดูเหมือนจะสร้างความยุ่งยากลำบากใจมากกว่า จึงไม่ให้ความสนใจในการดำเนินการ

ปัญหาต่างๆเหล่านี้ บางปัญหาก็ได้รับการแก้ไข เช่น ในปัญหาที่เกี่ยวพันกับงบประมาณ หากองค์กรใดสนใจสมัครเข้าร่วมในการดำเนินการ ก็จะมีการจัดสรรงบประมาณให้จำนวนหนึ่ง(โดยมีการประเมินผล) และให้ผู้เชี่ยวชาญในการวางแผนระบบเข้าไปช่วยวางแผนในหน่วยงาน เป็นต้น

4.1.3 ปัญหาและอุปสรรคในการเชื่อมโยงและแลกเปลี่ยนข้อมูลกลุ่มประเทศ Civil Law

ปัญหาและอุปสรรคในการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมในกลุ่มประเทศ Civil Law นั้น เป็นปัญหาที่เกิดขึ้น โดยทั่วไป และมีลักษณะคล้ายๆกัน ซึ่ง Wen (1999) [96] ได้ประมวลสรุปว่าเกิดขึ้นในลักษณะต่อไปนี้

1.การขาดมาตรฐานในการจัดเก็บข้อมูล การขาดมาตรฐานในการจัดเก็บข้อมูลนั้น หมายถึง การที่แต่ละหน่วยงานต่างจัดเก็บข้อมูลที่เกิดจากการปฏิบัติงานหรือแนวทางของตนเอง โดยที่ต่างคนต่างเก็บ ขาดการกำหนดรูปแบบหรือหลักเกณฑ์ในการจัดเก็บ ซึ่งการจัดเก็บข้อมูลไม่เพียงแต่มีปัจจัยด้านองค์กรที่ต่างฝ่ายต่างจัดเก็บเท่านั้น แต่ยังขึ้นอยู่กับ

96 Wen **Ibid** p.12

ผู้ปฏิบัติงานแต่ละคนที่จัดเก็บ และดุลยพินิจในการจัดเก็บอีกด้วย ซึ่งการดำเนินการดังกล่าวส่งผลให้ระบบฐานข้อมูลยังขาดมาตรฐาน หรือ การจัดเก็บยังไม่เป็นระบบ ขาดข้อมูลบางประการ ซึ่งก็จะส่งผลต่อการเชื่อมโยงและการบูรณาการข้อมูลกับหน่วยงานอื่นๆต่อไปในอนาคต

2.ปัญหาด้านบุคลากรในกระบวนการยุติธรรม ยังขาดความรู้ความเข้าใจในด้านเทคโนโลยีสารสนเทศ ปัญหาและอุปสรรคด้านนี้เกิดจากการที่บุคลากรที่ปฏิบัติงานยังไม่สนใจและใส่ใจในการแสวงหาความรู้และการใช้งานจากคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศอย่างจริงจังและต่อเนื่อง ในขณะเดียวกันก็ไม่ได้มีการพัฒนาทักษะทางด้านการใช้งานเทคโนโลยีสารสนเทศ

3.ปัญหาความไม่เชื่อมันในการอนุญาตให้ใช้ข้อมูล ความไม่เชื่อมั่นในการอนุญาตให้ใช้ข้อมูลนั้นเกิดจากความวิตกกังวลเกี่ยวกับข้อมูลในความรับผิดชอบดูแลของตน ซึ่งตนเองเป็นผู้ครอบครองและรักษาข้อมูลดังกล่าว ซึ่งหากถูกนำออกไปเผยแพร่หรือนำไปใช้และเกิดผลเสีย ตนเองจะต้องร่วมรับผิดชอบด้วย และยังเกิดความไม่เชื่อมั่นในการอนุญาตให้ใช้ข้อมูลว่า ข้อมูลจะถูกนำไปใช้ได้ตรงตามวัตถุประสงค์หรือไม่ด้วยเช่นกัน

4.ปัญหาการขาดการประเมินผลและการพัฒนาองค์กรให้รองรับการใช้เทคโนโลยีสารสนเทศ ซึ่งปัญหานี้เป็นปัญหาที่เกิดขึ้นกับแทบทุกองค์กร

5.ปัญหาวัตถุประสงค์ของการมีเทคโนโลยีสารสนเทศในองค์กรยังไม่ชัดเจน ปัญหานี้เกิดจากการจัดหาหรือจัดให้มีเทคโนโลยีสารสนเทศในองค์กรนั้น เป็นการจัดหาเพื่อให้ดูเหมือนเป็นการพัฒนาและการปรับปรุงองค์กรให้มีความทันสมัยและเป็นการจัดให้มีเพื่อดูเหมือนว่า การดำเนินการนั้นได้มีการนำเอาเทคโนโลยีสารสนเทศมาช่วยในการปฏิบัติงาน แต่ยังไม่มีแผนงาน โครงการหรือเป้าหมายที่จะใช้ข้อมูลที่เกี่ยวข้องไปปฏิบัติงาน

6.ปัญหาการขาดความเข้าใจในประโยชน์และข้อจำกัดของเทคโนโลยี ปัญหานี้เกี่ยวข้องกับความคุ้นเคยกับวิธีการปฏิบัติงานแบบเดิมๆ ซึ่งเห็นว่าก็สามารถปรับเปลี่ยนได้ แต่บางองค์กรก็ยังคุ้นเคยแบบเดิม

7.ปัญหาการขาดการวางแผนในด้านของผู้ใช้ประโยชน์และการพัฒนา ปัญหานี้เกิดขึ้นเนื่องจากไม่ได้มีการสำรวจเกี่ยวกับผู้ที่ใช้ประโยชน์จากเทคโนโลยีสารสนเทศว่า มีปริมาณการใช้และความต้องการในการใช้ตลอดจนทิศทางในการดำเนินการอย่างไรบ้าง ดังนั้นองค์กรจึงไม่ได้ให้ความใส่ใจในการวางแผนในด้านนี้อย่างจริงจัง

หากนำเอาปัญหาต่างๆของแต่ละกลุ่มมาจำแนกเพื่อเปรียบเทียบสามารถแสดงได้ดังตารางต่อไปนี้

ปัญหาของ กลุ่ม Civil Law	ปัญหาของ กลุ่ม Common Law	ปัญหาของประเทศไทย
1. การยังขาดมาตรฐานในการจัดเก็บข้อมูล	1.การมีหน่วยงานหลากหลายมากเกินไป และความต้องการใช้ข้อมูลไม่เหมือนกัน ทำให้การประมวลผลข้อมูลล่าช้าไม่ครบถ้วน	1. ปัญหาการขาดนโยบายที่ชัดเจนว่าควรจะเก็บข้อมูลอะไรบ้าง
2.ปัญหาด้านบุคลากรในกระบวนการยุติธรรม ที่ยังไม่มีความรู้ในด้านนี้มีอยู่มาก	2.บางองค์กรในกระบวนการยุติธรรม ยังไม่ให้ความสำคัญมากนัก จึงมีการจัดสรรงบประมาณให้น้อย	2.ปัญหาการจัดส่งงบประมาณให้น้อย
3. ความไม่เชื่อมั่นในการอนุญาตให้ใช้ข้อมูลต้องให้ศาลมาควบคุม	3. หน่วยงานบางหน่วย ยังเล็กเกินไป ที่จะมีการจ้างบุคลากรที่มีความรู้ทาง IT มาประจำ	3.ปัญหาการขาดงานเจ้าภาพหลัก
4. ขาดการประเมินผลและพัฒนาองค์กรให้รองรับการใช้ IT	4. ขาดการวางแผน ระยะยาว ตัดงบให้เฉพาะบางปี	4.การขาดการเอาใจใส่ทุ่มเทอย่างจริงจังในการดำเนินการ
5. วัตถุประสงค์ของการมี IT ในองค์กรไม่ชัดเจน	5. มีข้อจำกัดในด้านบุคลากรและการออกแบบเพื่อนำมาใช้งานหรือใช้ประโยชน์อย่างจริงจัง	5. ขาดบุคลากรผู้เชี่ยวชาญ
6. ขาดความเข้าใจในประโยชน์และข้อจำกัดของเทคโนโลยี	6. ประสบกับปัญหาด้านความเสี่ยงต่างๆในกระบวนการดำเนินการ	6.ผู้บริหารยังไม่ให้ความสนใจในการพัฒนาเทคโนโลยีสารสนเทศเท่าที่ควรและไม่สนใจในเรื่องการบูรณาการ
7. ขาดการวางแผนในด้านของผู้ใช้ประโยชน์และการพัฒนา	7. กลัวปัญหาเรื่องความรับผิดหากเกิดความผิดพลาด	7. ปัญหาด้านนักการเมืองและการแทรกแซงข้อมูล

4.2 การวิเคราะห์ปัญหาทางด้านกฎหมาย

ในแง่ของการพัฒนากฎหมายที่เกี่ยวข้องนั้น ตัวอย่างของการดำเนินการที่มีกฎหมายมารองรับการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมเป็นของสหรัฐอเมริกานั้น ไม่ว่าจะเป็นระดับรัฐบาลกลาง มลรัฐ หรือท้องถิ่น ก็จะมีการออกกฎหมายมารองรับในการแลกเปลี่ยนข้อมูลและการบูรณาการข้อมูลทั้งสิ้น กฎ ระเบียบ และ/หรือ กฎหมายของรัฐบาลกลาง อาจจะถูกมลรัฐ หรือ ท้องถิ่น นำไปใช้เป็นแนวทาง หรือ อาจถูกยกเว้นบางหลักเกณฑ์ หากขาดความเหมาะสมกับท้องถิ่นใดๆ เว้นแต่กฎ ระเบียบ หรือ กฎหมายนั้นจะถูกจำกัดว่า ห้ามออกข้อยกเว้น หรือ ระบุไว้โดยเฉพาะว่า จะต้องมีองค์ประกอบ แม้ว่ากฎหมายของรัฐบาลกลางส่วนใหญ่จะมีข้อจำกัดในการเข้าถึงข้อมูลอิเลกโทรนิกส์ แต่ก็มีกฎหมายที่ได้ตราไว้ในอำนาจอย่างเป็นกลาง และเขียนไว้อย่างกว้างๆ

กฎหมายหลักของอเมริกาที่ตราไว้อย่างกว้างๆ และให้อำนาจในการบูรณาการและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรมได้แก่ The Code of Federal Regulations (CFR) โดยอยู่ในหมวด 28 CFR Part 23 : Criminal Justice History Information กระทรวงยุติธรรมของสหรัฐอเมริกา โดย Office of Justice Programs ได้นำมาประยุกต์ออกระเบียบควบคุมการดำเนินการเกี่ยวกับระบบข่าวกรองทางอาชญากรรม หรือ Criminal Intelligence System โดยดำเนินการร่วมภายใต้กฎหมาย The Omnibus Crime Control and Safe Streets Act of 1968 กฎหมายดังกล่าวได้มีการตราให้มีการดำเนินการออกแบบในการรับข้อมูล การเก็บรวบรวมและประมวลผลข้อมูลทั้งข้อมูลส่วนบุคคล และข้อมูลจากองค์กรต่างๆ บนฐานของหลักการที่เชื่อได้ว่าเป็นกิจกรรมการดำเนินการที่เกี่ยวข้องกับการประกอบอาชญากรรม (28 CFR S23.3 (b)) ระเบียบเหล่านั้น มีข้อสังเกตว่า ข้อมูลที่มีหลักฐานหรือเชื่อได้ว่า เป็นเครือข่าย (network) กับการประกอบอาชญากรรมก็สามารถที่จะดำเนินการเก็บรวบรวมข้อมูลได้ อย่างไรก็ตาม การเก็บรวบรวมข้อมูลก็จะต้องเป็นไปตามหลักการเรื่อง “intelligence Project” ที่ระบุว่า องค์กรใดๆหรือหลายๆองค์กรอาจรวบรวมและเก็บรักษาข้อมูลของบุคคลใด (individual) เฉพาะเมื่อมีเหตุผลอันควรสงสัยว่า บุคคลนั้น เกี่ยวข้องกับการประกอบอาชญากรรม หรือกิจกรรมที่เกี่ยวข้องกับอาชญากรรม และข้อมูลนั้นต้องเกี่ยวข้องกับศาสนา การเมือง สมาคม หรือทัศนคติทางสังคม หรือ การดำเนินการใดๆ หากไม่มีความเกี่ยวข้องโดยตรงกับการประกอบอาชญากรรมจะไม่อนุญาตให้มีการรวบรวม โดยในการรวบรวมข้อมูลดังกล่าวต้องมีหลักฐานและข้อเท็จจริงเพียงพอที่จะเชื่อว่า บุคคลดังกล่าวเกี่ยวพันกับการประกอบอาชญากรรมหรือ มีส่วนรู้เห็น (28 CFR S23.20 (a)-(c))

อย่างไรก็ตามสามรถที่จะสรุปมาตรการทางกฎหมายที่ประเทศต่างๆใช้เสริมการดำเนินการดังนี้

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สหรัฐอเมริกา	**1.The Code of Federal Regulations (CFR) โดยอยู่ในหมวด 28 CFR Part 23 : Criminal Justice History Information** มีบทบัญญัติกว้างๆ และให้อำนาจในการบูรณาการและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม **2. The Omnibus Crime Control and Safe Streets Act of 1968** กฎหมายดังกล่าวได้มีการตราให้มีการดำเนินการออกแบบในการรับข้อมูล การเก็บรวบรวม และประมวลผลข้อมูลทั้งข้อมูลส่วนบุคคล และข้อมูลจากองค์กรต่างๆ บนฐานของหลักการที่เชื่อได้ว่าเป็นกิจกรรมการดำเนินการที่เกี่ยวข้องกับการประกอบอาชญากรรม	**-Freedom of Information Act 1966** **-The Privacy Act 1974** ให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลที่หน่วยงานราชการต่างๆ มีอยู่ **-The Government in the Sunshine Act** **-Electronic Communications Privacy Act** 1986	Copyright law ลิขสิทธิ์ในงานที่มีการรวบรวม หากผลงานการดำเนินการดังกล่าวไม่เคยมีใครดำเนินการจัดทำมาก่อนมาตรา 102 ผลงานที่เป็นการรวบรวม หรือผลงานที่เป็นในเชิงอนุพันธ์	มีมากกว่า 40 ฉบับ เช่น Copyright Act, National Stolen Property Act, Mail and Wire Fraud Statutes Child Pornography Prevention Act of 1996 เป็นต้น ในกรณีที่เป็นการกระทำความผิดต่อคอมพิวเตอร์ กฎหมายที่เกี่ยวข้องโดยตรงกับเรื่องนี้ ได้แก่ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 นอกจากกฎหมายฉบับนี้แล้วก็ยังมีกฎหมายอื่นที่สามารถใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์ได้อีก คือ the Electronic Communications Privacy Act 1986 และ the Economic Espionage Act 1999

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สหรัฐอเมริกา	3. ***The Crime Identification Technology Act 1998*** ให้รัฐสภาตัดงบประมาณรายจ่ายจำนวน 250 ล้านเหรียญอเมริกันต่อปี ติดต่อกัน 5 ปี ให้มลรัฐต่างๆ ได้บูรณาการข้อมูลในระบบกระบวนการยุติธรรมโดยใช้เทคโนโลยี 4.**The Brady Handgun Violence Prevention Act (Brady Act (1993),** ให้มีการขึ้นทะเบียนผู้ที่ค้าอาวุธปืน และผู้ที่มีอาวุธปืนไว้ในครอบครอง ตลอดจนมีการตรวจสอบการครอบครองอาวุธปืน รวมถึงมาตรการต่างๆ เช่น การต่อทะเบียนอาวุธปืนทุก 2 ปี			

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สหรัฐอเมริกา	**5.the National Child Protection Act of 1993 (NCPA) (1993)** กฎหมายฉบับนี้มุ่งที่จะให้มลรัฐต่างๆได้ส่งข้อมูล “การประกอบอาชญากรรมที่มีการแสวงหาผลประโยชน์และล่วงละเมิดเด็ก” (Child abuse crime information) **6. the Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act1968** มีการเก็บรักษาข้อมูลจากการดักฟังโทรศัพท์หรือการล่อซื้อเพื่อใช้ดำเนินคดี และบูรณาการหรือเชื่อมโยงเข้ากับฐานข้อมูลอื่น			

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สหรัฐอเมริกา	**7. the Violent Crime Control and Law Enforcement Act of 1994 (Violent Crime Control Act), (1994)**ให้รัฐต่างออกกฎหมายให้มีการลงทะเบียนข้อมูลประวัติอาชญากรทางเพศ ที่กระทำผิด และถูกคุมขัง หลังจากถูกปล่อยตัวไปแล้ว 10 ปี และมีการกำหนดโทษแก่หน่วยงานหรือรัฐที่ไม่ได้มีการดำเนินการขึ้นทะเบียนข้อมูลดังกล่าวด้วย 8**. relevant requirements of the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act,** รัฐบาลกลางให้อำนาจแก่มลรัฐในการที่จัดเก็บข้อมูลที่เกี่ยวกับบุคคลที่มีการล่วงละเมิดทางเพศแก่เด็กและยกเว้นการปกป้องข้อมูลส่วนตัวของจำเลยผู้กระทำผิดทางเพศแก่			

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สหรัฐอเมริกา	**9. Megan's Law,** ตำรวจของมลรัฐต้องจัดทำและดูและข้อมูลการเปลี่ยนแปลงการลงทะเบียนของบุคคลที่เข้ามาอาศัย มีการตรวจสอบและเทียบเคียงกับข้อมูลในหน่วยอื่นๆที่มีการเก็บรวบรวมข้อมูล **10.the Pam Lychner Sexual Offender Tracking and Identification Act of 1996**ให้สำนักงานอัยการสูงสุดได้มีประสานงานกับ FBI ลงทะเบียนเฉพาะข้อมูลเกี่ยวกับผู้กระทำผิดในทางเพศ			

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สหรัฐอเมริกา	**11. the Victims of Trafficking and Violence Protection Act of 2000** ให้หน่วยงานที่เกี่ยวข้อง ทำการเก็บรวบรวมและประมาณข้อมูลที่เกี่ยวข้อง พร้อมทั้งจัดทำรายงานประจำปี (Annual Report) มีการส่งข้อมูลให้ฝ่ายตรวจคนเข้าเมืองประสานการข้ามเดินทางเข้าประเทศแก่บุคคลที่ขึ้นบัญชีดำการค้าผู้หญิง และเด็กและให้ตรวจสอบผู้เสียหายที่เดินทางด้วย ตลอดจนรวบรวมพฤติกรรมและจัดทำพัฒนาฐานข้อมูล			

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สวีเดน	**1.Electronic Communications Act 2000** ซึ่งเป็นกฎหมายที่เอื้อต่อการแลกเปลี่ยนข้อมูลทั่วไป	1.พระราชบัญญัติการคุ้มครองข้อมูลในปี ค.ศ. 1974 และฉบับแก้ไข ค.ศ. 1992	**1.Directive Act of 6 November 1997 (Act 1997:79)** ซึ่งประกาศใช้เมื่อวันที่ 1 มกราคม 1998 มาใช้โดยมีการแก้ไขใน มาตรา 49ของกฎหมาย **Swedish Copyright Act 1997**	1.**The Computer Misuse Act 1990** คัดลอกแนวทางมาจากกฎหมายของอังกฤษ

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
ออสเตรเลีย	-กฎหมาย The Privacy Act 1988 ออกระเบียบ Model Forensic Procedure Bill และมี The Model Criminal Code Officer' Committee มารองรับ -Commonwealth ได้มีการแก้ไข Crime Act 1914 ในปี 2001 เพื่อป้องกันการนำข้อมูลมาใช้ในทางที่ผิด รวมทั้งมีกฎหมาย The Public Service Act 1999 ที่ช่วยให้รัฐและมณฑลต่างๆ สามารถเชื่อมโยงข้อมูลระหว่างกันได้	-พระราชบัญญัติข้อมูลข่าวสารส่วนบุคคลออสเตรเลีย คือ The Australian federal Freedom of Information Act (AuFOIA)) ประกาศเป็นกฎหมายในปี 1982 (New South Wales-Freedom of Information Act 1989, Queensland-Freedom of Information Act 1992, South Australia-Freedom of Information Act 1991, Victoria-Freedom of Information Act 1982, Western Australia-Freedom of Information Act 1992) พระราชบัญญัติความเป็นส่วนตัว ปี 1988 (The Privacy Act 1988)	-Copyright Act 1968 เพราะถือว่า เป็นงานที่มีลักษณะเป็นงานต้นแบบ ประเด็นปัญหากฎหมายก็คือ กฎหมายลิขสิทธิ์ออสเตรเลียให้การคุ้มครองการรวบรวมข้อมูล ตามหลัก Sweat of the brow หรือ industrious collection	-Computer specific laws พ.ศ. 2539แก้ไขเพิ่มเติมเกี่ยวกับภาพเด็กลามกอนาจารและความรุนแรงของเกมคอมพิวเตอร์ -Cyber crime 2001 (Cth) Act เพิ่มเติมบทบัญญัติใหม่ในส่วนที่ 10.7 ของกฎหมายอาญา Crime Code Act 1995 (Cth) และ Customs Act 1901 แก้ไขกฎหมายต่อไปนี้ด้วย : Australian Security Intelligence Organization Act 979,Education Services for Overseas Students Act 2000/ Telecommunications (Interception) Act 1997

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
ฝรั่งเศส	-The Data Processing, Data Files and Individual Liberties 1978 ปรับปรุงแก้ไขปี 2004 เป็นกฎหมายหลักที่ใช้ในการประมวลข้อมูล โดยมีการจำแนกประเภทข้อมูล การเข้าถึง การควบคุมข้อมูล และสิทธิส่วนบุคคล ข้อมูลทางการแพทย์ เป็นต้น -นอกจากนี้ในส่วนกฎหมายอื่นๆที่ฝรั่งเศสนำมาปรับใช้คือ กฎหมายอาญา (Penal Code) ที่มีการปรับปรุงแก้ไข เมื่อวันที่ 8 พค. 2007 ให้ข้อมูลต่างๆได้รับการคุ้มครองจากบทบัญญัติของกฎหมายอาญา	-ฝรั่งเศสได้ออกรัฐบัญญัติลงวันที่ 6 มกราคม ค.ศ. 1987 ว่าด้วยการเก็บรักษาข้อมูลข่าวสารโดยเครื่องคอมพิวเตอร์และเสรีภาพ	-ฝรั่งเศสนั้นมีกฎหมายลิขสิทธิ์ที่ครอบคลุมผลงานที่เกิดจากความคิดและการแสดงออกทางความคิดที่เรียกว่า the work of mind	-ฝรั่งเศสจะมีการปรับใช้กฎหมายอาญา มาตรา 323-(1)-(4)(7)ส่วนการละเมิดสิทธิส่วนบุคคลอันเป็นผลมาจากการใช้การใช้กรรมวิธีทางด้านคอมพิวเตอร์หรือการเข้าถึงแฟ้มข้อมูลผู้อื่นโดยไม่มีอำนาจก็มีความผิดตาม มาตรา 226(16)-(17)

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
ญี่ปุ่น	**-The Act for Protection of Computer Processed Personal Date 1989** ใช้ปกป้องผลประโยชน์และสิทธิของบุคคลจากการเก็บรวบรวมข้อมูลส่วนบุคคลโดยประมวลผลผ่านระบบคอมพิวเตอร์ **-Law Concerning Electronic Signatures and Certification Services 2001** ใช้ส่งเสริมการใช้ลายมือชื่อทางอิเลกโทรนิกส์ **- Basic Law on the Formation of an Advanced Information and Telecommunications Network Society** ส่งเสริมมาตรการต่างๆในการ	**-1.The Law on the Protection of Personal Information** **-2.The Law Concerning the Protection of Personal Information held by Administrative Organs**	**-The copyright Act**ไม่ได้ให้การรับรองคอมพิวเตอร์ซอฟแวร์หรือโปรแกรมคอมพิวเตอร์ต่างๆ ทั้งนี้เป็นไปตามมาตรา 10-3 ถือว่าการดำเนินการดังกล่าวนั้นเป็นเรื่องของIdea หรือ Expression Dichotomy(Computer program)	-ญี่ปุ่นมีกฎหมายที่เกี่ยวข้องหลายฉบับ ได้แก่**กฎหมายอาญา (Penal Code)**ที่ให้การคุ้มครองในระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์ **กฎหมายการเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจ(Unauthorized Computer Access Law) กฎหมายอื่นๆ** เช่น กฎหมายลิขสิทธิ์ กฎหมายโทรคมนาคม กฎหมายว่าด้วยสิ่งลามกอนาจารเด็ก เป็นต้น

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
เนเธอร์แลนด์	-ใช้ระบบคุณภาพที่เรียกว่า ISO 11179 พัฒนาคุณภาพข้อมูลที่จะแลกเปลี่ยนและในลดการใช้เวลากับงานเอกสารตามหลักการ e-Business และ e-Government และเน้นที่ XML -ออกกฎหมายระดับชาติ คือ Electronic Traffic Law -มาตรา 8 ของ The National Road and traffic law) โดยมีการใช้โครงสร้างแบบ XML	-Electronic Signature Act 2002 รับรองการส่งข้อมูลและยืนยันเอกสารอิเลกทรอนิกส์ เอื้อ e-Commerce และ e-Government -Electronic Decree of 1998 หรือ Dutch Telecom Law อนุวัติตาม Directive ของ EU ก็คือ The Distance Contract Act 2001 (EU ออก EU Distance Contract Directive มาเป็นต้นแบบ) -รัฐธรรมนูญของเนเธอร์แลนด์ มาตรา 7, 10 และ 13 คุ้มครองความเป็นส่วนตัว และเสรีภาพในการแสดงความคิดเห็น -Telecommunication Act 2004 อนุวัติตาม EU directive on electronic communication และ มีการนำหลักการ Electronic Commerce Platform Netherlands (E CP.NL) มาปรับใช้	-Data Protection Act 1995 นำ Directive ดังกล่าว มาอนุวัติเป็นกฎหมาย -นำเอา European Software Directive มาปรับใช้ -นำเอาแนวทาง European Council Directive มาปรับใช้ทำให้กฎหมายลิขสิทธิ์ของเนเธอร์แลนด์ ฐานข้อมูลด้านงานยุติธรรมที่เกิดจากการบูรณาการมีลิขสิทธิ์ในส่วนที่มีการดำเนินการขึ้นมาใหม่	-Computer Crime Act 1991 กำหนดลักษณะและประเภทของการประกอบอาชญากรรม การใช้อินเตอร์เน็ตโดยองค์กรอาชญากรรม และการโฆษณาภาพลามกอนาจารทางอินเตอร์เน็ต

ตารางที่ 4.1 สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม (ต่อ)

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
สิงคโปร์	-Electronic Transactions Act 1998 มีความรับผิดทั้งทางแพ่งและทางอาญาภายใต้ มาตรา 10 ของกฎหมาย	ไม่ได้มีการบัญญัติกฎหมายไว้เพื่อการนี้โดยตรง เสนอให้มีการออก Model Data Protection Code for the Private Sector ในเดือนกุมภาพันธ์ 2002 ซึ่งต่อมาจากความจำเป็นดังกล่าวจึงมีการออกกฎหมายมาใช้ก่อนคือE-Commerce Code for the Protection of Personal Information and Communication of Consumers of Internet Commerce	-The Copyright Act 1987 ปรับปรุงแก้ไข1994 1998 และ1999 ให้ครอบคลุมการคุ้มครองการสร้างและการออกแบบhardware คุ้มครองตั้งแต่ 5-15 ปี หลังจากการสร้างสรรค์งาน หลักe-patent อันเป็นแบบสำหรับการให้ความคุ้มครองสิทธิบัตรในฐานข้อมูลได้	-Computer Misuse Act 1993 เอาผิดกับพวกที่มุ่งเจาะระบบข้อมูลคอมพิวเตอร์ (hacking) กฎหมายที่มีลักษณะกึ่งทางแพ่งและทางอาญา คือ มีบทบัญญัติการลงโทษทั้งทางแพ่งและอาญา บางครั้งจะเรียกกฎหมายฉบับนี้ว่า “Cyber-Trespass” ปัญหาสำคัญอยู่ที่การตีความอย่างชัดเจน ถึงว่า การบุกรุก (trespass) , มีได้ทั้งการบุกรุกทางกายภาพ และการบุกรุกทางอิเลกโทรนิกส์

ตารางที่ 4.2 : สรุปกฎหมายของไทยที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม

ประเทศ	กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อการแลกเปลี่ยนและการบูรณาการข้อมูล	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา	กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด
ประเทศไทย	-มีทั้งกฎหมายที่เป็นอุปสรรคและเอื้อต่อการเชื่อมโยงข้อมูลแต่กระจัดกระจายออกไปตามแต่ละฉบับ -กฎหมายที่เป็นอุปสรรค ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย ประมวลกฎหมายอาญา ประมวลกฎหมายแพ่งและพาณิชย์ ประมวลกฎหมายวิธีพิจารณาความแพ่ง ประมวลกฎหมายวิธีพิจารณาความอาญา พรบ. ข้อมูลข่าวสารฯ พ.ศ. 2540 พรบ. ปปช. พรบ. ปปง พรบ. จัดตั้งศาลเยาวชนและครอบครัว พ.ศ. 2534 ระเบียบตำรวจเกี่ยวกับคดี เป็นต้น -กฎหมายที่เอื้อต่อการเชื่อมโยงฯ ได้แก่ พรบ. ข้อมูลข่าวสาร ฯ 2540 พรบ. ธุรกิจอิเลกทรอนิกส์ พรบ.การสอบสวนคดีพิเศษ พ.ศ. 2547 เป็นต้น	-ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยตรง จะมีที่เกี่ยวข้อง คือ 1. พรบ. ข้อมูลข่าวสารทางราชการ พ.ศ. 2540 2. พรบ. ทะเบียนราษฎร์ พ.ศ. 2534 3. พรบ.สถิติ พ.ศ. 2508	พรบ.ลิขสิทธิ์ พ.ศ. 2537	มีร่างกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การกระทำความผิดหรือการก่อให้เกิดภยันตรายหรือความเสียหายอันเนื่องมาจากการก่ออาชญากรรมทางคอมพิวเตอร์อาจแบ่งออกได้เป็น 2 ลักษณะตามวัตถุหรือระบบที่ถูกกระทำ คือการกระทำต่อระบบคอมพิวเตอร์การกระทำต่อข้อมูลคอมพิวเตอร์

4.3การวิเคราะห์การประยุกต์กับแผนแม่บท

มีการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551) โดยในแผนแม่บทดังกล่าว ได้มีการกำหนดยุทธศาสตร์การดำเนินงานด้านเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม 6 ยุทธศาสตร์ คือ

ยุทธศาสตร์ที่ 1 : การพัฒนาและบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรม

ยุทธศาสตร์นี้ประกอบด้วยแผนและโครงการ ได้แก่ แผนพัฒนากระบวนการทำงานแบบอิเลกโทรนิกส์สำหรับหน่วยงานในกระบวนการยุติธรรม โครงการจัดทำมาตรฐานและข้อตกลงสำหรับการบูรณาการข้อมูลจำเป็นกระบวนการยุติธรรมและ โครงการสำรวจและประมวลผลข้อมูลกระบวรการยุติธรรม

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

ยุทธศาสตร์นี้ประกอบด้วยแผนและโครงการ ได้แก่ แผนงานวิเคราะห์และสนับสนุนระบบเทคโนโลยีสารสนเทศของหน่วยงานในกระบวนการยุติธรรม แผนงานการใช้เทคโนโลยีด้านวีดีทัศน์ ในกระบวนการยุติธรรม แผนงานระบบสารสนเทศเพื่อพิสูจน์ทราบข้อมูลบุคคล โครงการจัดตั้งหน่วยงานเฉพาะและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมแห่งชาติ (DXC) โครงการนำร่องระบบเทคโนโลยีสารสนเทศกระบวนการยุติธรรมต้นแบบ โครงการตรวจสอบสถานะหมายจับออนไลน์ โครงการส่งสำเนาคำพิพากษาทางอิเลกโทรนิกส์

ยุทธศาสตร์ที่ 3 : การพัฒนาเครือข่ายเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์นี้ประกอบด้วยโครงการ ได้แก่ โครงการพัฒนาเครือข่ายกระทรวงยุติธรรม

ยุทธศาสตร์ที่ 4 : การพัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์นี้ประกอบด้วยโครงการ ได้แก่ โครงการกำหนดมาตรฐานการวางแผนการกู้ข้อมูล และระบบเทคโนโลยี โครงการกำหนดมาตรฐานเทคโนโลยีความมั่นคงปลอดภัยในกระบวนการยุติธรรม โครงการกำหนดมาตรฐานการใช้เทคโนโลยีในการรักษาความปลอดภัยของศูนย์ข้อมูลในกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 5 : การพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์นี้ประกอบด้วยโครงการ ได้แก่ โครงการฝึกอบรมผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศในกระบวนการยุติธรรมและ โครงการปรับปรุงสายงานวิชาชีพบุคลากรด้านเทคโนโลยี สารสนเทศกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 6 : การพัฒนากฎหมาย ระเบียบ ข้อบังคับให้สอดคล้องต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

ยุทธศาสตร์นี้ประกอบด้วยโครงการ ได้แก่ โครงการปรับปรุง ระเบียบ ข้อบังคับและกฎหมายที่เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

สำนักงานยุติธรรมจังหวัด OFFICE OF JUSTICE AFFAIRS

ยุทธศาสตร์ที่ 1 : การพัฒนาและบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
1.แผนพัฒนากระบวนการทำงานแบบอิเลกโทรนิกส์สำหรับหน่วยงานในกระบวนการยุติธรรม	**หลักการ :** หน่วยงานในกระบวนการยุติธรรมยังไม่สามารถรวบรวมข้อมูลนำไปวิเคราะห์และพัฒนา ควรมีการปรับเปลี่ยนกระบวนการทำงานให้เอื้อต่อการเก็บรวบรวมข้อมูลในระบบอิเลกโทรนิกส์ **วัตถุประสงค์ :** ให้มีระบบงานรองรับการจัดเก็บ ตรวจสอบแหล่งที่มาของข้อมูล แลกเปลี่ยนข้อมูลทางอิเลกโทรนิกส์และลดการเก็บข้อมูลซ้ำซ้อน **แนวทาง :** วิเคราะห์ขั้นตอนและปรับกระบวนการทำงาน จัดทำมาตรฐานรูปแบบเอกสารอิเลกโทรนิกส์ และพัฒนาระบบสารสนเทศให้มีประสิทธิภาพ	-ปัจจุบันหน่วยงานต่างๆในกระบวนการยุติธรรมยังไม่มีระเบียบที่ชัดเจนในการจัดเก็บข้อมูลและประมวลผลทางอิเล็กทรอนิกส์ตลอดจนจัดทำฐานข้อมูล -กระทรวงยุติธรรมจึงควรออกระเบียบกระทรวงยุติธรรมให้หน่วยงานในสังกัดทุกหน่วยงาน รวมทั้งหน่วยงานขึ้นตรงต่อ รมต.กระทรวงยุติธรรม ในการจัดเก็บ ประมวลผลและจัดทำฐานข้อมูลของแต่ละหน่วยงานให้เป็นมาตรฐานเดียวกันและเป็นการเตรียมความพร้อมสำหรับการเชื่อมโยงข้อมูล

ยุทธศาสตร์ที่ 1 : การพัฒนาและบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรม (ต่อ)

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
2. โครงการจัดทำมาตรฐานและข้อตกลงสำหรับการบูรณาการข้อมูลจำเป็นกระบวนการยุติธรรม	**หลักการ :** ข้อมูลในกระบวนการยุติธรรมยังขาดมาตรฐานชัดเจน ควรมีการประชุมจัดทำมาตรฐานข้อมูล และข้อตกลง **วัตถุประสงค์ :** เพื่อให้มีมาตรฐานและข้อตกลงสำหรับการบูรณาการข้อมูลเป็นแนวทางการปฏิบัติงาน **แนวทาง** 1. จัดประชุมร่วมเพื่อกำหนดมาตรฐานข้อมูล 2. กำหนดแนวทางและวางกลไกการดำเนินการอย่างต่อเนื่อง	-เป็นประเด็นด้านเทคนิคและการบริหารจัดการ

ยุทธศาสตร์ที่ 1 : การพัฒนาและบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรม (ต่อ)

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
3. โครงการสำรวจและประมวลผลข้อมูลกระบวรการยุติธรรม	**หลักการ :** สถิติและข้อมูลของหน่วยงานในกระบวนการยุติธรรมยังไม่ครบถ้วน ไม่สอดคล้องกับสถานการณ์ในสังคม ขาดความต่อเนื่อง ควรสำรวจจากประชาชน **วัตถุประสงค์ :** เก็บข้อมูลจากประชาชนเพื่อมาเปรียบเทียบ และปรับปรุงนโยบายและแผน **แนวทาง :** สำรวจข้อมูลจากหน่วยงานรัฐ เอกชน ประชาชน มาประมวลวิเคราะห์นำเสนอเชิงกลยุทธ์	-เป็นประเด็นด้านเทคนิคและการบริหารจัดการ

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
1.แผนงานวิเคราะห์และสนับสนุน ระบบเทคโนโลยีสารสนเทศของหน่วยงานในกระบวนการยุติธรรม	**หลักการ :** หน่วยงานในกระบวนการยุติธรรมขาดแคลนวัสดุอุปกรณ์ด้านเทคโนโลยีสารสนเทศ ควรมีการวิเคราะห์ โครงสร้างและภารกิจหน่วยงาน **วัตถุประสงค์ :** ให้หน่วยงานในกระบวนการยุติธรรมมีศักยภาพในการบูรณาการข้อมูล **แนวทาง :** ประเมินศักยภาพและกำหนดความต้องการหน่วยงานและนำเสนอเป็นรายงาน	เป็นประเด็นทางด้านเทคนิคและการบริหารจัดการ

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
2. แผนงานการใช้เทคโนโลยี ด้านวีดีทัศน์ในกระบวนการยุติธรรม	**หลักการ :** หน่วยงานในกระบวนการยุติธรรมมีการนำเทคโนโลยีด้านวีดิทัศน์มาใช้ในหน่วยงานและขยายผลในด้านงานคดี ซึ่งเกิดผลดี ควรส่งเสริม **วัตถุประสงค์ :** ลดขั้นตอน เวลา และค่าใช้จ่ายในการปฏิบัติงาน **แนวทาง :** กำหนดกิจกรรม มาตรฐาน และข้อตกลง รวมทั้งเตรียมบุคลากร – อุปกรณ์ และประสานการใช้ระเบียบข้อตกลง	ประสานงานสำนักงานศาลยุติธรรม ให้มีการออกระเบียบปฏิบัติในการพิจารณาคดี (การผัดฟ้อง ฝากขัง และสืบพยาน) และประสานงานกับกรมราชทัณฑ์ กรมพินิจฯ เพื่อออกระเบียบรองรับให้สอดคล้องกันกับแนวทางการดำเนินการและการประสานเชื่อมโยงข้อมูล

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
3. แผนงานระบบสารสนเทศเพื่อพิสูจน์ทราบข้อมูลบุคคล	**หลักการ :** การตรวจสอบและยืนยันตัวบุคคลทะเบียนราษฎร์ ต้องส่งข้อมูลหลายหน่วย ควรมีการดำเนินการพิสูจน์ทราบบุคคลแบบ One Stop Sevices และมีผู้เชี่ยวชาญ **แนวทาง :** สำรวจ ออกแบบและพัฒนา การเชื่อมโยงข้อมูลเพื่อยืนยันบุคคล และวางหลักเกณฑ์ ระเบียบปฏิบัติในการใช้ข้อมูลบุคคล	- ประสานงานสำนักงานทะเบียนราษฎร เพื่อทำความตกลงร่วม (Mou) และออกระเบียบรองรับ - สำนักงานนิติวิทยาศาสตร์ ออกระเบียบดำเนินการฯ

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
4. โครงการจัดตั้งหน่วยงานเฉพาะและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรมแห่งชาติ (DXC)	**หลักการ :** ต้องมีศูนย์กลางในการบูรณาการข้อมูลและกำหนดมาตรฐานสำหรับการเชื่อมโยงข้อมูล **วัตถุประสงค์ :** มีศูนย์กลางในการบูรณาการข้อมูลในกระบวนการยุติธรรม และบริการข้อมูลแบบ One-Stop Services. **แนวทาง :** เลือกสรรหน่วยงานและคณะทำงานพัฒนาระบบ DXC ตามแผนแม่บทและมาตรฐาน และวางแนวทางการบริหารจัดการ	- ออกเป็นกฎหมายเฉพาะ เพื่อรองรับการดำเนินการของศูนย์ เมื่อมีพระราชกฤษฎีกาจัดแบ่งส่วนราชการ โดยเป็นกฎหมายระดับพระราชบัญญัติ “พระราชบัญญัติ เชื่อมโยงแลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรม”

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
5.โครงการนำร่องระบบเทคโนโลยีสารสนเทศกระบวนการยุติธรรมต้นแบบ	**หลักการ :** หน่วยงานในกระบวนการยุติธรรมประสบปัญหาการปรับเปลี่ยนแนวทางการดำเนินการ ควร ทดสอบสร้างต้นแบบมาใช้ **วัตถุประสงค์ :** ศึกษา วิเคราะห์ ปรับปรุงการดำเนินการให้ เชื่อมโยงและเป็นระบบ **แนวทาง :** ประสานความร่วมมือระหว่างหน่วยงาน ตั้งคณะทำงานประสาน ติดตามประเมินผล และรายงานผล ตลอดจนประชาสัมพันธ์การดำเนินการ	- ประเด็นด้านเทคนิคและการบริหารจัดการ

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
6.โครงการตรวจสอบสถานะหมายจับออนไลน์	**หลักการ :** หมายจับปัจจุบันกระจัดกระจาย ตรวจสอบลำบาก ควรบูรณาการ **วัตถุประสงค์ :** หน่วยงานที่เกี่ยวข้อง สามารถตรวจสอบสถานภาพหมายจับได้ทันที **แนวทาง :** ประสานงานระหว่างหน่วยงาน จัดทำข้อตกลง และออกแบบพัฒนาระบบฯ	- หน่วยงานหลักที่เกี่ยวข้อง ได้แก่ สำนักงานตำรวจแห่งชาติ และสำนักงานศาลยุติธรรม

ยุทธศาสตร์ที่ 2 : การพัฒนาเทคโนโลยีสารสนเทศของกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
7. โครงการส่งสำเนาคำพิพากษาทางอิเลกโทรนิกส์	**หลักการ :** หลายหน่วยงานที่เกี่ยวข้องต้องการสำเนาคำพิพากษาฯ แต่ต้องคัดลอก เสียเวลา ค่าใช้จ่าย การดำเนินการโดยระบบอิเลกโทรนิกส์แทนจะช่วยให้มีประสิทธิภาพมากขึ้น **วัตถุประสงค์ :** ลด เวลา และค่าใช้จ่ายในการคัดลอก/ เอกสาร **แนวทาง :** ประสานงานกับหน่วยงานเพื่อจัดทำข้อตกลง ออกแบบพัฒนา เพื่อให้เป็นมาตรฐานและสามารถใช้งานได้	- ประสานงานกับสำนักงานตำรวจแห่งชาติและสำนักงานศาลยุติธรรม เพื่อจัดเก็บและประมวลผลข้อมูลให้ทันสมัยโดยสามารถใช้ฐานข้อมูลของกระทรวงยุติธรรมได้เช่นกัน - ประมวลกฎหมายวิธีพิจารณาความแพ่ง - มาตรา 92 93 ระบุให้เฉพาะคู่ความหรือผู้แทนที่จะสามารถคัดลอกสำเนาคำพิพากษา เฉพาะคดี - ประสานงาน สำนักงานศาลยุติธรรม ให้มีการออกระเบียบ โดยกำหนดให้หน่วยงานนกระบวนการยุติธรรม ถือเป็นผู้ที่มีส่วนได้เสียในคดีที่สามารถคัดลอกสำเนาได้

ยุทธศาสตร์ที่ 3 : การพัฒนาเครือข่ายเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
1. โครงการพัฒนาเครือข่ายกระทรวงยุติธรรม	**หลักการ :** ในการบูรณาการระบบเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม ต้องมีการสรรหาเครือข่ายเฉพาะที่สามารถเชื่อมโยงได้ **วัตถุประสงค์ :** เพื่อให้มีเครือข่ายเฉพาะของกระบวนการยุติธรรมที่หน่วยงานสามารถใช้และสามารถเชื่อมโยงกับหน่วยงานรัฐภายนอกกระบวนการยุติธรรม องค์กรอิสระและหน่วยงานต่างประเทศ **แนวทาง:** วิเคราะห์ความต้องการเครือข่าย ออกแบบ วางแผน และกระจาย ตลอดจนคัดสรรผู้ดำเนินการและติดตามประเมินผล	

ยุทธศาสตร์ที่ 4 : การพัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
1.โครงการกำหนดมาตรฐานการวางแผนการกู้ข้อมูล และระบบเทคโนโลยี	**หลักการ :** ศูนย์เทคโนโลยี สารสนเทศและการสื่อสารต้องมีการเตรียมความเสียหายจากภัยธรรมชาติหรือภัยพิบัติอื่นๆ เพื่อให้สามารถทำงานได้อย่างต่อเนื่อง **วัตถุประสงค์ :** ให้มีศูนย์เทคโนโลยีสำรองและมาตรการดำเนินการด้าน disaster discovery **แนวทาง :** สำรวจ วิเคราะห์ หาโครงสร้างร่วมและประสานงานกับหน่วยงานเพื่อทำข้อตกลงจัดตั้งศูนย์เทคโนโลยีสำรอง	- เป็นประเด็นด้านเทคนิค และ การบริหารจัดการ - อาจกำหนดเป็นแนวทางไว้ในระเบียบหรือกฎหมายเฉพาะในการดำเนินการได้

ยุทธศาสตร์ที่ 4 : การพัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม (ต่อ)

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
2. โครงการกำหนดมาตรฐานเทคโนโลยีความมั่นคงปลอดภัยในกระบวนการยุติธรรม	**หลักการ :** หน่วยงานในกระบวนการยุติธรรมมีการรักษาความปลอดภัยของข้อมูล และการเข้าถึงที่แตกต่างกัน ยังไม่มีการกำหนดมาตรฐาน ควรมีการกำหนดและแนวทางการตรวจสอบ **วัตถุประสงค์ :** มีมาตรฐานด้านสิทธิการเข้าถึงข้อมูล มีกฎ ระเบียบ และวิธีการปฏิบัติในการใช้การโอนย้ายสิทธิและความรับผิด **แนวทาง :** จัดประชุมสัมมนาเพื่อกำหนดข้อตกลง ระเบียบปฏิบัติ และมาตรฐานวางแนวทางปฏิบัติ และเสริมสร้างความรู้ ความเข้าใจ	- กำหนดเป็นมาตรฐานการทางกฎหมายในระเบียบหรือกฎหมายเฉพาะในการดำเนินการ ทั้งนี้ หากเป็นกฎหมายในเชิงการบริหารจัดการ อาจระบุให้เป็นอำนาจหน้าที่ของคณะกรรมการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลในกระบวนการยุติธรรม

ยุทธศาสตร์ที่ 4 : การพัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม (ต่อ)

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
3. โครงการกำหนดมาตรฐานการใช้เทคโนโลยีในการรักษาความปลอดภัยของศูนย์ข้อมูลในกระบวนการยุติธรรม	**หลักการ :** หน่วยงานในกระบวนการยุติธรรมต้องมีการกำหนดสิทธิการเข้าถึงพื้นที่ศูนย์ข้อมูล ป้องกันการก่อวินาศกรรม รวมทั้งการตรวจสอบ **วัตถุประสงค์ :** มีศูนย์ มีระเบียบและความปลอดภัย **แนวทาง :** จัดการประชุมสัมมนาเพื่อกำหนดระเบียบปฏิบัติ ทดลองศูนย์นำร่องและเสริมสร้างความรู้ ความเข้าใจ	- ผลักดัน กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ให้มีผลบังคับใช้ - ออกระเบียบการรักษาความปลอดภัยของศูนย์เพื่อรองรับ

ยุทธศาสตร์ที่ 5 : การพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
1. โครงการฝึกอบรมผู้บริหารและบุคลากรด้านเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม	**หลักการ :** ผู้บริหารระดับสูงมีทัศนคติและองค์ความรู้ต่างกัน ในขณะเดียวกันบุคลากรยังขาดความรู้ ทักษะ และวินัยในการทำงาน **วัตถุประสงค์ :** เตรียมบุคลากรรองรับ e-work และการเชื่อมโยงงานในกระบวนการยุติธรรมตลอดจนการเพิ่มศักยภาพหน่วยงาน **แนวทาง :** จัดหลักสูตรฝึกอบรมแก่ผู้บริหารและบุคลากรระดับต่างๆ โดยดำเนินการประเมินผล และฝึกอบรมอย่างต่อเนื่อง	- เป็นประเด็นด้านเทคนิคและการบริหารจัดการ

ยุทธศาสตร์ที่ 5 : การพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
2. โครงการปรับปรุงสายงานวิชาชีพบุคลากรด้านเทคโนโลยี สารสนเทศกระบวนการยุติธรรม	**หลักการ :** หน่วยงานต่างๆในกระบวนการยุติธรรม ยังไม่ได้กำหนดตำแหน่งและความก้าวหน้าในสายวิชาชีพอย่างชัดเจน **วัตถุประสงค์ :** มีบุคลากรด้านเทคโนโลยีสารสนเทศเพียงพอ และบุคลากรเกิดความพึงพอใจและรู้สึกมั่นคงในสายวิชาชีพ **แนวทาง :** ตั้งคณะกรรมการ/ คณะทำงานกำหนดมาตรฐานสายวิชาชีพด้านเทคโนโลยีสารสนเทศในกระบวนการยุติธรรม	- เป็นประเด็นด้านเทคนิคและ กฎ ระเบียบเกี่ยวกับการบริหารงานบุคคล

ยุทธศาสตร์ที่ 6 : การพัฒนากฎหมาย ระเบียบ ข้อบังคับให้สอดคล้องต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

แผนงาน / โครงการ	หลักการ / วัตถุประสงค์ / แนวทางดำเนินการ	ระเบียบ / กฎหมายที่เกี่ยวข้อง
1.โครงการปรับปรุง ระเบียบ ข้อบังคับ และกฎหมายที่เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม	**หลักการ :** มีกฎ ระเบียบ ข้อบังคับ และกฎหมายเป็นอุปสรรค หรือ ข้อจำกัดในการดำเนินการ ต้องมีการปรับปรุง กฎ ระเบียบ และกฎหมายเหล่านั้นให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม **วัตถุประสงค์ :** เพื่อให้หน่วยงานในกระบวนการยุติธรรมเกิดความสะดวกในการปฏิบัติงาน **แนวทาง :** ตั้งคณะกรรมการ / คณะทำงานวิเคราะห์ปรับปรุงระเบียบ ข้อบังคับ และกฎหมายที่เอื้อต่อการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรม และนำเสนอผลให้องค์กรเกี่ยวข้องทราบและขอความเห็นชอบดำเนินการ	มีระเบียบและกฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม ในขณะเดียวกันก็มีกฎ ระเบียบและกฎหมายที่เป็นอุปสรรคต่อการเชื่อมต่อข้อมูลที่ต้องมีการตรวจสอบและปรับใช้หรือการเสนอขอปรับแก้ไขเพื่อให้สอดคล้องกับการดำเนินการ -ในระยะยาวควรมีการเสนอออกกฎหมายเฉพาะทางเพื่อเป็นกฎหมายที่เอื้อต่อการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมโดยตรง

ตารางที่ 4.3 : สรุปปัญหาและอุปสรรคการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของไทย

ปัญหาและอุปสรรคฯ	สาเหตุ	ปัจจัย	แนวทางแก้ไข	หมายเหตุ
1.การขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม	1.การบูรณาการข้อมูลด้าน IT เป็นเรื่องใหม่ 2. ผู้กำหนดนโยบายไม่ได้ให้ความสำคัญ	1. มาตรฐานการจัดเก็บข้อมูล 2. ผู้บริหารองค์กร 3.การให้ความสำคัญและกำหนดเป็นนโยบายองค์กร	1. กำหนดเป็นนโยบายองค์กร ในการดำเนินงานต่อไป 2. ทำความตกลงร่วมมือ (MOU) เพื่อแลกเปลี่ยนข้อมูล	
2.ขาดการดำเนินการอย่างจริงจังและต่อเนื่อง	1. IT ไม่ใช่ภารกิจหลักองค์กร 2.ยังไม่เห็นประโยชน์ที่จะได้รับ 3.ขาดผู้รับผิดชอบหลักโดยตรง	1. ผู้บริหารองค์กร 2.การประสานงานระหว่างองค์กร 3. ผู้รับผิดชอบโดยตรง	1. กำหนดเป็นภารกิจหลักองค์กร 2.ผู้บริหารติดตามสอบถามความก้าวหน้า 3.กำหนดแผนการดำเนินการชัดเจนต่อเนื่อง	
3.ขาดหน่วยงานที่เป็นเจ้าภาพหลักในหน่วยงานที่จะทำหน้าที่รับและส่งต่อ	1.ยังไม่มีหน่วยงานริเริ่ม 2.หน่วยงานต่างๆมีภาระงานมาก 3.ขาดการประสานงานระหว่างหน่วยงานในการใช้ข้อมูลร่วม	1.นโยบายและแผน 2.งบประมาณและผู้บริหาร 3.ความร่วมมือจากองค์กรต่างๆ	1.มีการจัดตั้งหน่วยงานเฉพาะขึ้นมาดูแลรับผิดชอบ 2.มีการของบประมาณเพื่อดำเนินการ 3.มีการทำความตกลงร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง	

ตารางที่ 4.3 : สรุปปัญหาและอุปสรรคการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของไทย (ต่อ)

ปัญหาและอุปสรรคฯ	สาเหตุ	ปัจจัย	แนวทางแก้ไข	หมายเหตุ
4.ผู้บริหารระดับสูงยังไม่ให้ความสำคัญเท่าที่ควร	1. ผู้บริหารมุ่งภารกิจหลักขององค์กร 2. ผู้บริหารยังขาดความรู้ความเข้าใจการดำเนินการ	1. วิสัยทัศน์องค์กร 2. นโยบายและแผนชาติ	1.กำหนดเป็นวิสัยทัศน์แต่ละองค์กร 2.บรรจุเป็น National Agenda และสัมมนาผู้บริหารถึงแนวทาง	
5.ปัญหาด้านงบประมาณ (งานด้านเทคโนโลยีสารสนเทศต้องใช้งบประมาณสูง)	1. งบประมาณไม่เพียงพอ 2. ขาดการประสานงานขอความร่วมมือจากแหล่งทุนภายนอก	1. นโยบายและแผนไม่มีชัดเจนโดยเฉพาะ 2. ความร่วมมือจากภายนอก	1. แสวงหางบจากแหล่งภายนอก 2. ประสานงานกระทรวง IT ช่วยดำเนินการบางประการเกี่ยวกับวัสดุอุปกรณ์	
6.งานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน	1.ภารกิจหลักขององค์กรยังไม่ได้ประโยชน์จาก IT 2.ไม่มีการแทรกงานitในงานอื่น	1.จำนวนhardware และpeople ware ที่พอเพียง 2.การสอดแทรก IT ลงในภารกิจหลัก	1.กำหนดเป็นภารกิจหลักองค์กร 2.สอดแทรก IT เข้าไปในงานหลักขององค์กร	
7.ปัญหาการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน	1.หน่วยงานขาดการตั้งอัตรารองรับ 2. อัตราค่าจ้างบุคลากรสูง	1.การตั้งอัตราบุคลากร 2.บุคลากรที่มีความรู้เชี่ยวชาญเฉพาะด้าน	1.จ้างพนักงานชั่วคราวและประสานสำนักงบประมาณ 2.ตัดโอนบางงานให้Out sources	

ตารางที่ 4.3 : สรุปปัญหาและอุปสรรคการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของไทย (ต่อ)

ปัญหาและอุปสรรคฯ	สาเหตุ	ปัจจัย	แนวทางแก้ไข	หมายเหตุ
8.ปัญหาการมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน(ต่างฝ่ายต่างจัดเก็บ)	1. การขาดการประสานงาน 2.ขาดมาตรฐานในการจัดเก็บที่เป็นรูปแบบ	1. นโยบายองค์กร 2. ผู้บริหาร 3. ความร่วมมือระหว่างองค์กร	1.ประชุมร่วมกันเพื่อกำหนดรูปแบบมาตรฐาน 2.ประสานความร่วมมืออย่างต่อเนื่อง	
9.ขาดมาตรฐานในการจัดเก็บและขาดการการปรับปรุงข้อมูลให้เป็นปัจจุบัน ขาดการเรียกมาตรวจสอบความถูกต้องในปัจจุบัน	1.ยังไม่มีการกำหนดมาตรฐานจัดเก็บร่วมกัน 2.ขาดบุคลากรที่จะมาประเมินตรวจสอบ	1. มาตรฐานการจัดเก็บร่วมกัน 2. บุคลากรเพื่อตรวจสอบ	1.สร้างมาตรฐานการจัดเก็บและประมวลข้อมูลร่วมกัน 2.ตั้งคณะกรรมการตรวจสอบและปรับปรุงทุกข์และรายงานผล	
10.ขาดกฎหมายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล (โดยเฉพาะภาคเอกชน) พรบ.ข้อมูลข่าวสารทางราชการฯยังไม่สามารถคุ้มครองได้ครอบคลุม	1.กฎหมายคุ้มครองข้อมูลส่วนบุคคล ยังไม่ผ่านรัฐสภา 2. มีบทบัญญัติทางกฎหมายบางประการเป็นอุปสรรค	1.การมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล 2.การประสานงานหน่วยงานรัฐกับเอกชน	1.ผลักดันให้กฎหมายดังกล่าวผ่านสภาออกมาบังคับใช้ 2.ปรับปรุงแก้ไขกฎหมาย ระเบียบที่เป็นปัญหาอุปสรรคหรือจัดทำข้อตกลงร่วม	

ตารางที่ 4.3 : สรุปปัญหาและอุปสรรคการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของไทย (ต่อ)

ปัญหาและอุปสรรคฯ	สาเหตุ	ปัจจัย	แนวทางแก้ไข	หมายเหตุ
11.ขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ	1.บุคลากรขาดความรู้ความเชี่ยวชาญในการประมวลผลข้อมูล 2.ภาระงานประจำมีมาก	1.กฎหมายและระเบียบที่กำหนดให้มีการประมวลผลข้อมูลโดยการใช้เทคโนโลยี 2.		
12.ขาดการบูรณาการในระบบงานแม้ในองค์กรเดียวกันก็ตาม	1.บางหน่วยงานยังไม่ได้ประสานการทำงานโดยตรง 2.การยังไม่ทราบวิธีการและแนวทางการบูรณาการ			

ตารางที่ 4.4 : การเปรียบเทียบปัญหาและอุปสรรคของการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของไทยและต่างประเทศ

ปัญหาและอุปสรรคฯกลุ่ม Civil Law	ปัญหาและอุปสรรคฯกลุ่มCommon Law	ปัญหาและอุปสรรคฯกลุ่มประเทศไทย
1.การยังขาดมาตรฐานในการจัดเก็บข้อมูล	1.การมีหน่วยงานหลากหลายมากเกินไป และความต้องการใช้ข้อมูลไม่เหมือนกัน ทำให้การประมวลผลข้อมูลล่าช้า ไม่ครบถ้วน	1.การขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม
2.ปัญหาด้านบุคลากรในกระบวนการยุติธรรม ที่ยังไม่มีความรู้ในด้านนี้มีอยู่มาก	2.บางองค์กรในกระบวนการยุติธรรม ยังไม่ให้ความสำคัญมากนัก จึงมีการจัดสรรงบประมาณให้น้อย	2.ขาดการดำเนินการอย่างจริงจังและต่อเนื่อง
3.ความไม่เชื่อมั่นในการอนุญาตให้ใช้ข้อมูลต้องให้ศาลมาควบคุม	3.หน่วยงานบางหน่วย ยังเล็กเกินไป ที่จะมีการจ้างบุคลากรที่มีความรู้ทาง IT มาประจำ	3.ขาดหน่วยงานที่เป็นเจ้าภาพหลักในหน่วยงานที่จะทำหน้าที่รับและส่งต่อ
4.ขาดการประเมินผลและพัฒนาองค์กรให้รองรับการใช้ IT	4.ขาดการวางแผน ระยะยาวตัดงบให้เฉพาะบางปี	4.ผู้บริหารระดับสูงยังไม่ให้ความสำคัญเท่าที่ควร
5.วัตถุประสงค์ของการมี IT ในองค์กรไม่ชัดเจน	5.มีข้อจำกัดในด้านบุคลากรและการออกแบบเพื่อนำมาใช้งานหรือใช้ประโยชน์อย่างจริงจัง	5.ปัญหาด้านงบประมาณ(งานด้านเทคโนโลยีสารสนเทศต้องใช้งบประมาณสูง)
6.ขาดความเข้าใจในประโยชน์และข้อจำกัดของเทคโนโลยี	6.ประสบกับปัญหาด้านความเสี่ยงต่าง ๆในกระบวนการดำเนินการ	6.งานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน
7.ขาดการวางแผนในด้านของผู้ใช้ประโยชน์และการพัฒนา	7.กลัวปัญหาเรื่องความรับผิด หากเกิดความผิดพลาด	7.ปัญหาการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน

ตารางที่ 4.4 : การเปรียบเทียบปัญหาและอุปสรรคของการเชื่อมโยง แลกเปลี่ยนและบูรณาการข้อมูลในกระบวนการยุติธรรมของไทยและต่างประเทศ (ต่อ)

ปัญหาและอุปสรรคฯกลุ่ม Civil Law	ปัญหาและอุปสรรคฯกลุ่มCommon Law	ปัญหาและอุปสรรคฯกลุ่มประเทศไทย
		8.ปัญหาการมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน(ต่างฝ่ายต่างจัดเก็บ)
		9.ขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บและขาดการการปรับปรุงข้อมูลให้เป็นปัจจุบัน ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน
		10.ขาดกฎหมายและมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคล(โดยเฉพาะภาคเอกชน)พรบ.ข้อมูลข่าวสารทางราชการฯยังไม่สามารถคุ้มครองได้ครอบคลุม
		11.ขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ
		12.ขาดการบูรณาการในระบบงานแม้ในองค์กรเดียวกันก็ตาม

ตารางที่ 4.5 : ลักษณะบทบัญญัติกฎหมายที่เกี่ยวข้องกับการเชื่อมโยง แลกเปลี่ยนข้อมูล ในกระบวนการยุติธรรม

ประเภทกฎหมาย	ลักษณะบทบัญญัติกฎหมาย	หมายเหตุ
1.กฎหมายที่เอื้อต่อการเชื่อมโยงแลกเปลี่ยนข้อมูล ในกระบวนการยุติธรรม	ระบบCommon Lawออกกฎหมายรับรองการดำเนินการขององค์กร โดยจะออกกฎหมายของรัฐบาลกลางและเชิงประสานบังคับให้หน่วยงานในระดับท้องถิ่นประสานให้ความร่วมมือในการประสานการปฏิบัติการ Civil Law จึงมักจะใช้การออกกฎหมายเฉพาะในเชิงการบริหารจัดการในรูปของพระราชบัญญัติ (act) ออกมาใช้ โดยมีการตั้งคณะกรรมการเฉพาะกิจ (ad hoc Committee) หรือ อาจจะมีการตั้งเป็นคณะทำงาน (task force) ที่ประกอบด้วยตัวแทนจากหน่วยงานบังคับกฎหมายที่เกี่ยวข้องมาดำเนินการร่วมกัน	มีความจำเป็นที่ต้องมีมาตรการทางกฎหมายเป็นบทบัญญัติที่จะต้องออกมารองรับเพื่อให้หน่วยงานต่างๆสามารถที่จะเชื่อมโยงข้อมูลที่ตนเองมีอยู่และเก็บรักษามาปฏิบัติงานร่วมกับองค์กรหรือหน่วยงานอื่นๆ นอกจากนี้ข้อมูลข่าวสารในปัจจุบันได้ถูกเก็บรักษาไว้ในฐานข้อมูลและเป็นข้อมูลในทางอิเล็กทรอนิกส์ซึ่งจำเป็นต้องมีกฎหมายมารองรับและระบุความถูกต้องทั้งในการเข้าถึงข้อมูลและการใช้ข้อมูลตลอดจนการเก็บรักษาความลับ การเข้าถึงข้อมูล การรักษาความปลอดภัย ประเภทของข้อมูล และระยะเวลาในการจัดเก็บ

ตารางที่ 4.5 : ลักษณะบทบัญญัติกฎหมายที่เกี่ยวข้องกับการเชื่อมโยง แลกเปลี่ยนข้อมูล ในกระบวนการยุติธรรม (ต่อ)

ประเภทกฎหมาย	ลักษณะบทบัญญัติกฎหมาย	หมายเหตุ
2.กฎหมายการคุ้มครองข้อมูลส่วนบุคคล	ออกกฎหมายไว้เพื่อคุ้มครองข้อมูลและสิทธิส่วนบุคคล เรียกว่า Data Protection Act และ Privacy Act คุ้มครองตั้งแต่ข้อมูลทั่วไปของบุคคลนั้น ได้แก่ ชื่อ นามสกุล ที่อยู่ ระดับการศึกษา อาชีพ เป็นต้น จนถึงข้อมูลที่เป็นความลับ เช่น ประวัติทางการแพทย์ ประวัติทางวินัย ประวัติทางอาชญากรรม เป็นต้น	
3.กฎหมายทรัพย์สินทางปัญญา	ฐานข้อมูลที่จัดทำขึ้นใหม่ควรเป็นสิ่งที่มีกฎหมายให้การรองรับและถือเป็นการสร้างสรรค์ จึงควรได้รับการคุ้มครองจากกฎหมายทรัพย์สินทางปัญญา ดังนั้นในกรณีที่มีการจัดทำฐานข้อมูลขึ้นมาเฉพาะเพื่อการแลกเปลี่ยนเชื่อมโยงหรือบูรณาการข้อมูลในกระบวนการยุติธรรม ฐานข้อมูลเหล่านั้นจึงถือเป็นทรัพย์สินทางปัญญาของหน่วยงานหรือองค์กรที่ดำเนินการและควรมีมาตรการทางกฎหมายโดยเฉพาะกฎหมายลิขสิทธิ์มาให้การรับรองและคุ้มครอง	ประเทศส่วนใหญ่ในยุโรป จะได้รับอิทธิพลจาก EU Directive ทำให้ยอมรับฐานข้อมูล (database) ว่าได้รับการคุ้มครองจากกฎหมายลิขสิทธิ์ และ/หรือสิทธิบัตร โดยยอมรับลิขสิทธิ์ของผู้ที่ได้จัดทำข้อมูลก่อนและลิขสิทธิ์ของเจ้าของฐานข้อมูล

ตารางที่ 4.5 : ลักษณะบทบัญญัติกฎหมายที่เกี่ยวข้องกับการเชื่อมโยง แลกเปลี่ยนข้อมูล ในกระบวนการยุติธรรม (ต่อ)

ประเภทกฎหมาย	ลักษณะบทบัญญัติกฎหมาย	หมายเหตุ
4.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด	มีมาตรการทางกฎหมายป้องกันและเอาผิดกับผู้ที่สามารถนำข้อมูลเหล่านั้นไปใช้ประโยชน์โดยมิชอบจากการลักลอบเข้าถึงข้อมูลโดยไม่ถูกต้อง (Hacking) เนื่องจากกฎหมายอาญาของประเทศต่างๆล้วนแล้วแต่เน้นให้ความคุ้มครองแก่วัตถุที่มีรูปร่าง (tangible or corporeal objects) เช่น ทรัพย์ เป็นต้น เมื่อการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่างๆเป็นการกระทำต่อวัตถุที่ไม่มีรูปร่าง (intangible or incorporeal objects) ได้แก่ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ ดังนั้น การกระทำความผิดต่อคอมพิวเตอร์จึงไม่เป็นความผิดอาญา จึงต้องมีการออกกฎหมายพิเศษมาใช้บังคับ	ฐานข้อมูลที่เกี่ยวกับกระบวนการยุติธรรมเป็นฐานข้อมูลที่มีบทบาทและความสำคัญอย่างยิ่งทั้งต่อการดำเนินคดี การสร้างความยุติธรรม และผลกระทบต่อชีวิต ร่างกาย ทรัพย์สิน ของบุคคลที่เกี่ยวข้องไม่ว่าจะเป็นโจทก์ จำเลย พยาน และผู้เกี่ยวข้องอื่นๆ ซึ่งหากมีผู้ที่สามารถนำข้อมูลเหล่านั้นไปใช้ประโยชน์โดยมิชอบจากการลักลอบเข้าถึงข้อมูลโดยไม่ถูกต้อง (Hacking) จึงควรมีมาตรการทางกฎหมาย มาตรการคุ้มครองโดยเฉพาะต่อการกระทำความผิดต่อคอมพิวเตอร์ให้เป็นอาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่ง

บทที่ 5
บทสรุปและเสนอแนะ

5.1 บทสรุป

ในยุคปัจจุบันนี้ ความก้าวหน้าทางด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศรวมไปถึงการใช้สื่ออิเล็กทรอนิกส์ในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่งในรูปแบบของเครือข่ายอินเตอร์เน็ตได้รับการพัฒนามากขึ้นอย่างต่อเนื่องและรวดเร็ว ประเทศต่างๆจำเป็นต้องมีการพัฒนาปรับปรุงตลอดจนนำมาปรับใช้ในการปฏิบัติงานในองค์กรต่างๆโดยเฉพาะของรัฐให้ดำเนินไปอย่างมีประสิทธิภาพซึ่งก็รวมถึงการบูรณาการและการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรมด้วย ตามแผนแม่บทกระบวนการยุติธรรมแห่งชาติ พ.ศ. 2547-2549 กำหนดให้มีการพัฒนาและอำนวยความยุติธรรมอย่างเป็นระบบ มีประสิทธิภาพ รวดเร็ว โปร่งใสตรวจสอบได้โดยหน่วยงานในกระบวนการยุติธรรมจะต้องบูรณาการเป้าหมายและกระบวนการทำงานให้สอดคล้องและเป็นไปในทิศทางเดียวกัน รวมทั้งพัฒนาประสิทธิภาพการบริหารจัดการของหน่วยงานยุติธรรมด้วยการลดขั้นตอนการปฏิบัติให้สะดวก รวดเร็ว มีประสิทธิภาพ และใช้ทรัพยากรร่วมกัน

การนำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในกระบวนการยุติธรรมเพื่อช่วยให้มีการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้องรวมถึงการมีและใช้ข้อมูลดังกล่าวร่วมกันระหว่างหน่วยงาน จะส่งผลให้การทำงานของหน่วยงานในกระบวนการยุติธรรมเป็นอย่างสะดวก รวดเร็ว ถูกต้อง และมีประสิทธิภาพยิ่งขึ้น นอกจากนี้การสามารถเข้าถึงและใช้ข้อมูลที่มีอยู่แล้วของหน่วยงานใดหน่วยงานหนึ่งโดยหน่วยงานที่ต้องการใช้ข้อมูลไม่ต้องดำเนินการกรอกข้อมูลใหม่ ทำให้หน่วยงานนั้นๆได้รับและได้ใช้ข้อมูลที่มีความคลาดเคลื่อนน้อยที่สุด อันจะนำไปสู่หนทางที่จะอำนวยความยุติธรรมให้แก่ประชาชนอีกหนทางหนึ่งและการที่หน่วยงานต่างๆจะได้รับหรือได้ใช้ข้อมูลเหล่านั้นจากการเชื่อมโยงข้อมูลระหว่างหน่วยงานยุติธรรมได้ก็จักต้องมีการส่งต่อข้อมูลที่หน่วยงานนั้นๆมีอยู่ให้แก่กันและกัน ทั้งนี้เพื่อให้เกิดการบูรณาการข้อมูลสารสนเทศในกระบวนการยุติธรรมอย่างแท้จริง แต่ในทางปฏิบัติการส่งต่อข้อมูลระหว่างหน่วยงานในกระบวนยุติธรรมอาจมีปัญหาและอุปสรรคเกิดขึ้นได้ นอกจากนี้การดำเนินงานในกระบวนการยุติธรรมในปัจจุบันยังต้องเป็นไปตามขั้นตอนและวิธีการที่กฎ ระเบียบ ข้อบังคับ หรือกฎหมายที่แต่ละหน่วยงานได้กำหนดขึ้น ซึ่งอาจเป็นอีกสาเหตุหนึ่งที่ก่อให้เกิดความล่าช้าและเป็นอุปสรรคต่อการส่งต่อข้อมูลและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรม

นอกจากนี้ แผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551) ยังได้กำหนดยุทธศาสตร์ที่สำคัญหลายประการ โดยมุ่งหมายให้หน่วยงานในกระบวนการยุติธรรม จัดทำฐานข้อมูลสารสนเทศที่เกี่ยวข้องกับอำนาจหน้าที่ของแต่ละหน่วยงานในรูปแบบของข้อมูลอิเล็กทรอนิกส์โดยใช้มาตรฐานทางเทคโนโลยีสารสนเทศขั้นต่ำร่วมกันเพื่อประโยชน์ในการบูรณาการข้อมูลและใช้ข้อมูลร่วมกัน

วัตถุประสงค์ในการศึกษาในครั้งนี้คือ เพื่อสำรวจว่าการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมตามแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ ฉบับที่ 1 (พ.ศ. 2548-2551)เพื่อศึกษาวิเคราะห์สภาพปัญหาและอุปสรรค และกฎระเบียบ ข้อบังคับ และกฎหมายของหน่วยงานในกระบวนการยุติธรรมก่อให้เกิดปัญหาและอุปสรรคต่อการเชื่อมโยงข้อมูลและการนำเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรม และเพื่อนำเสนอแนวทางในการปรับปรุง แก้ไขกฎ ระเบียบ ข้อบังคับ หรือกฎหมายต่างๆที่เป็นอุปสรรคต่อการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมและการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานของหน่วยงานในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้อง

ผลการศึกษา พบว่า แนวคิดในการทำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กรเป็นแนวคิดที่มีความสำคัญอย่างยิ่ง เพราะจะเป็นการใช้ความก้าวหน้าทางเทคโนโลยีมาใช้ในการจัดเก็บ และประมวลข้อมูล ตลอดจนจัดทำระบบเพื่อการค้นคว้าอ้างอิงและการประสานการดำเนินการต่างๆ โดยเฉพาะอย่างยิ่งองค์กรในกระบวนการยุติธรรมนั้นเป็นหน่วยงานที่ต้องมีใครจัดเก็บ และประมวลข้อมูลที่เกี่ยวกับผู้กระทำผิด พฤติกรรมการกระทำผิด ผู้เสียหาย การดำเนินคดีและการบังคับใช้กฎหมายต่างๆให้มีประสิทธิภาพ และที่สำคัญอย่างยิ่ง เทคโนโลยีสารสนเทศที่นำมาใช้ในองค์กรในกระบวนการยุติธรรมจะเอื้อต่อการจัดการความรู้ในกระบวนการยุติธรรม (Criminal Justice Knowledge Management) ต่อไปในอนาคต

สำหรับข้อมูลสารสนเทศในกระบวนการยุติธรรมนั้น ในอดีตข้อมูลสารสนเทศในกระบวนการยุติธรรมมีการจัดแบ่งโดยมีการแบ่งระดับอาชญากรรมโดยใช้เกณฑ์ความร้ายแรง Crime Seriousness Scales เป็นการกำหนดระดับความรุนแรงของอาชญากรรมโดยการให้น้ำหนักของอาชญากรรมในแง่ของความสัมพันธ์ความรุนแรงที่เกิดขึ้น

อย่างไรก็ตามในปัจจุบัน ระบบข้อมูลด้านงานยุติธรรม (Criminal Justice Information System) อาจจะจำแนกโดยทั่วไปได้ 2 ประเภท คือ ข้อมูลที่มีการรายงานต่อสาธารณะ (Public record information) ข้อมูลเหล่านี้ได้แก่ รายงานการโจรกรรมทรัพย์สิน

รายงานการจับกุม รายชื่อผู้กระทำผิดทางเพศ เป็นต้นและข้อมูลการสืบสวนสอบสวน (investigative system) โดยปกติข้อมูลการสืบสวนสอบสวนมักจะเป็นข้อมูลที่ยังไม่สามารถเปิดเผยได้ เนื่องจากยังอยู่ในระหว่างการดำเนินการสืบสวนสอบสวน เช่น รายชื่อผู้ต้องสงสัย ผู้ให้ข้อมูล ผู้เสียหาย พยาน เป็นต้น

ในสหรัฐอเมริกานั้นหากจำแนกหน่วยงานในกระบวนการยุติธรรมในระดับประเทศ ระดับมลรัฐ และระดับท้องถิ่น รวมกันทุกเขตมีหน่วยงานถึง 19,000 หน่วย ในขณะที่หน่วยงานของตำรวจมีเกือบ 200 หน่วย ซึ่งหน่วยงานต่างๆเหล่านี้ ทั้งตำรวจ อัยการ ศาล ราชทัณฑ์ คุมประพฤติ หน่วยสืบสวนสอบสวนพิเศษ เช่น FBI ต้องการข้อมูลที่จัดเก็บในระบบฐานข้อมูล การเชื่อมต่อและการบูรณาการข้อมูลเพื่อใช้ในระดับชาติทั้งสิ้น สิ่งที่ต้องกระทำให้เกิดขึ้นก็คือ ความถูกต้องของข้อมูล (accuracy) การตรวจสอบและดำเนินการให้ถูกต้อง บุคคลผู้ที่มีสิทธิเข้ามาใช้วัตถุประสงค์ของการเก็บและใช้ข้อมูล ระยะเวลาในการเก็บ ระบบการป้องกันการนำเอาข้อมูลเหล่านี้ไปใช้ในทางที่ผิด การดำเนินการเหล่านี้ยังรวมถึงข้อคำถามที่ว่า ข้อมูลชนิดหรือประเภทใดที่ควรจะเปิดเผยต่อสาธารณะได้ ไม่ว่า โดยทั่วไป หรือผ่านระบบ Internet และการเชื่อมโยงและบูรณาการข้อมูลอย่างไรในอนาคต เพื่อให้การพัฒนามีประสิทธิภาพยิ่งขึ้น

ในส่วนของระบบข้อมูลที่มีการบูรณาการและจัดทำเครือข่ายที่ดำเนินการในสหรัฐอเมริกาในปัจจุบัน ได้แก่ **NLETS (The National Law Enforcement Telecommunications Systems)**ซึ่งเป็นเครือข่ายระดับชาติที่เชื่อมข้อมูลกับรัฐต่างๆ และหน่วยงานของรัฐบาลกลางเข้าด้วยกัน เพื่อการแลกเปลี่ยนข้อมูลด้านกระบวนการยุติธรรมทั้งหมดในแต่ละมลรัฐ ในแต่ละวัน มีผู้เข้าใช้สูงถึง 327,000 ราย **ศูนย์ข้อมูลเครือข่ายอาชญากรรมระดับชาติ FBI**(The FBI.s National Crime Information Center (NCIC) Network)ศูนย์ข้อมูลนี้ เริ่มดำเนินการมานานแล้ว โดยเริ่มตั้งแต่ปี 1967 และมาปรับปรุงใหม่จนเป็นมาตรฐานในปี 2000 โดยเป็นชุด NCIC Version 2000 เป็นศูนย์ที่สร้างตัวชี้วัดระดับชาติเกี่ยวกับข้อมูลด้านการโจรกรรม การประกันและข้อมูลด้านกระบวนการยุติธรรมทั้งหมดที่หน่วยบังคับใช้กฎหมายทุกหน่วยจากทั่วประเทศต้องส่งข้อมูลให้ นอกจากนี้ก็ยังมี**ศูนย์ข้อมูลเครือข่ายงานยุติธรรมของ FBI** (The FBI.s Criminal Justice Information Services Wide Area Network (CJIS WAN) เพื่อเชื่อมโยงกับรัฐต่างๆ ในการบูรณาการข้อมูลด้านลายพิมพ์นิ้วมือของ FBI’s Integrated Automated Fingerprint Identification Systems. (IAFIS) ระบบ WAN นี้ ได้เชื่อมต่อกันในแต่ละมลรัฐ ส่วนระบบเครือข่ายอื่นๆนี้ สามารถจำแนกออกได้เป็น 2 กลุ่ม คือ**ระบบระดับชาติ (National – *System)*** ที่สนับสนุนหน่วยงานรัฐในระดับท้องถิ่น

และรัฐบาลกลางจะประกอบด้วยระบบฐานข้อมูลและเครือข่ายและ**ระบบรัฐบาลกลาง (Federal – System)**เป็นระบบที่ให้การสนับสนุนกิจกรรมด้านงานยุติธรรมแก่หน่วยงานรัฐบาลกลางในหน่วยต่างๆ แต่ระบบนี้จะเอื้อเฉพาะระดับรัฐบาลกลางเท่านั้น

ด้านการแลกเปลี่ยนข้อมูลด้านกระบวนการยุติธรรมนั้น มีการใช้เทคโนโลยีเพื่อการป้องกัน (Information Sharing and Prevention Technology)เร่วมด้วย แม้ว่ากระแสการดำเนินการเกี่ยวกับการก่อการร้ายจะมีบทบาทต่อการเร่งเร้าให้มีการแลกเปลี่ยนข้อมูลในหน่วยงานด้านกระบวนการยุติธรรม หน่วยบังคับกฎหมายและด้านความมั่นคง แต่การพัฒนาการแลกเปลี่ยนข้อมูลด้านกระบวนการยุติธรรม และการบูรณาการข้อมูลด้านกระบวนการยุติธรรมก็เกิดขึ้นมาก่อนหน้านี้แล้ว โดยมีการทุ่มเททรัพยากรในด้านกระบวนการยุติธรรมเพื่อพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยี (technological infrastructures) เพื่อเอื้อต่อการแลกเปลี่ยนข้อมูลที่สำคัญๆ นอกจากนี้ระบบการบูรณาการข้อมูลด้านงานยุติธรรมหรือ The integrated justice information system ได้ถูกกำหนดขึ้นเพื่อให้การแลกเปลี่ยนข้อมูลเป็นไปในกรอบของความถูกต้อง ชัดเจนรวดเร็ว ในวงการกระบวนการยุติธรรม และยังส่งเสริมในด้านการลดค่าใช้จ่าย แต่มีประสิทธิภาพ การบูรณาการจึงมีทั้งแนวดิ่ง (Vertical) และแนวราบ (horizontal Approach)ในการดำเนินการที่เกี่ยวกับการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม ด้านการป้องกันอาชญากรรม รัฐบาลได้จัดทำเครือข่ายระดับชาติ (a national criminal intelligence network) ที่ชื่อ “RISS.NET” หรือ “The Regional Information Sharing Systems Network” โดยความร่วมมือกับ FBI (Federal Bureau of Investigations Database) และกระทรวงกลาโหม (Department of Defense) รวมทั้งกระทรวงความมั่นคงแห่งมาตภูมิ (Department of Homeland Security) แม้การสร้างเครือข่ายดังกล่าวจะยังไม่ใช่ต้นแบบในการบูรณาการข้อมูลด้านงานยุติธรรมทั้งหมดในอนาคต แต่ก็เป็นก้าวแรกของการสร้างเครือข่ายในการแลกเปลี่ยนและการบูรณาการข้อมูลด้านอาชญากรรม

การจัดเก็บ ประมวลผลข้อมูลและการจัดทำข้อมูลเทคโนโลยีสารสนเทศ เป็นสิ่งที่ดำเนินการไม่ยากในระหว่างหน่วยงานและองค์กร แต่การจำแนกและให้ความคุ้มครองข้อมูลจากการนำไปแสวงหาผลประโยชน์และการก่อให้เกิดการเสียหายกับบุคคลที่เกี่ยวข้องโดยเฉพาะข้อมูลส่วนบุคคล จำเป็นจะต้องมีกระบวนการและมาตรการทางกฎหมายในการคุ้มครองซึ่งในต่างประเทศ นอกจากจะมีมาตรการทางกฎหมายในการคุ้มครองการเข้าใช้ข้อมูลโดยไม่ถูกต้องแล้วยังมีการให้ความคุ้มครองข้อมูลในฐานะที่ระบบฐานข้อมูลที่จัดทำขึ้นก็ถือเป็นทรัพย์สินทางปัญญาประเภทหนึ่งที่จะต้องได้รับการดูแลที่สรุปได้อย่างกว้างๆว่าเป็นการรวบรวมข้อมูลหรือสารสนเทศอย่างเป็นระบบระเบียบ (Organized collection of information)

หรือชุดข้อมูลที่ได้รับการจัดเรียงเป็นหมวดหมู่อย่างดีจะเห็นได้ว่ามีคุณสมบัติคาบเกี่ยวและสามารถนับได้ว่าเป็นทรัพย์สินทางปัญญา ซึ่งในแง่ของกฎหมายแล้ว หมายถึง สิทธิอันเกิดขึ้นจากผลงานทางความคิด ดังนั้น ระบบฐานข้อมูลด้านกระบวนการยุติธรรมที่จัดทำขึ้นในต่างประเทศนอกจากรัฐจะต้องมีกลไกในการดำเนินการเพื่อปกป้องข้อมูลมิให้ถูกนำไปใช้เพื่อแสวงหาผลประโยชน์และก่อให้เกิดความเสียหายแล้วยังจะต้องให้การคุ้มครองถึงลักษณะด้านทรัพย์สินทางปัญญาอันเกี่ยวข้องกับกฎหมายลิขสิทธิ์ของข้อมูลข่าวสารในกระบวนการยุติธรรมนั้นด้วย

สำหรับการบูรณาการข้อมูลด้านการบริหารงานยุติธรรม (Integration of Criminal Justice Information System)นั้น ประเภทข้อมูลพื้นฐานที่ต้องจัดเก็บในรูปแบบอิเล็กทรอนิกส์เพื่อประโยชน์ในการบูรณาการข้อมูลและการบริหารจัดการกระบวนการยุติธรรม ประกอบด้วยข้อมูลที่เกี่ยวข้องกับงานด้านการป้องกันและปราบปรามอาชญากรรม ข้อมูลด้านการพิจารณาคดี ข้อมูลด้านการดำเนินงานตามคำพิพากษา และข้อมูลด้านการคุ้มครองสิทธิเสรีภาพของประชาชนรวมทั้งข้อมูลเพื่อการวางแผน กำหนดนโยบาย ศึกษาวิจัยและพัฒนาระบบงานยุติธรรมที่จะช่วยทำให้การบริหารงานกระบวนการยุติธรรมเป็นไปอย่างมีประสิทธิภาพทันสถานการณ์ และเกิดประสิทธิผลต่อการแก้ไขปัญหาต่างๆในสังคม

ส่วนหลักการบูรณาการข้อมูลสารสนเทศกระบวนการยุติธรรมที่เหมาะสมคือ สร้างศูนย์เชื่อมโยงข้อมูลครอบคลุมระบบฐานข้อมูลที่มีอยู่เดิม โดยใช้สถาปัตยกรรมระบบเทคโนโลยีสารสนเทศแบบกระจาย (Distributed Databases Architecture) ซึ่งฐานข้อมูลของทุกหน่วยงานจะยังคงอยู่ที่เดิม เฉพาะข้อมูลที่แลกเปลี่ยนจะถูกเก็บในรูปแบบมาตรฐานเดียวกันและมีหน่วยงานกลางหรือศูนย์แลกเปลี่ยนข้อมูล (DATA EXCHANGE CENTER) หรือ DXC ทำหน้าที่บริหารจัดการข้อมูล โดยจัดเก็บข้อมูลในลักษณะ METADATA ซึ่งจะระบุหน่วยงานเจ้าของข้อมูล ประเภทและรูปแบบข้อมูล สิทธิการเข้าถึง และวิธีขอข้อมูล รวมทั้งตรวจสอบสิทธิผู้ขอใช้และให้บริการตามขั้นตอนที่กำหนดไว้ ทั้งนี้ผู้มีสิทธิเข้าถึงข้อมูลสามารถใช้บริการจากทุกสถานที่ที่แบบ ONE-STOP SERVICE โดยเรียกใช้ผ่านโปรแกรมประยุกต์แบบ WEB-BASED ทั่วไป เพื่อเข้าสู่ระบบ DXC ซึ่งเป็นเครือข่ายเฉพาะที่มีความปลอดภัยสูง

ในการบูรณาการของต่างประเทศนั้น ระบบการบูรณาการข้อมูลด้านกระบวนการยุติธรรมของที่ได้รับการยอมรับ ได้แก่ ระบบการบูรณาการข้อมูลด้านกระบวนการยุติธรรมของสก๊อตแลนด์ มีชื่อเรียกย่อๆ ว่า ISCJIS (Integration of Scottish Criminal Justice Information System) เป็นโครงการที่ให้หน่วยงานหลักในกระบวนการยุติธรรมมาร่วมในการบูรณาการข้อมูลและใช้ร่วมกัน การดำเนินการบูรณาการข้อมูลดังกล่าวไม่ใช่ใช้ระบบคอมพิวเตอร์ใหม่ แต่ใช้

การเชื่อมโยงข้อมูล โดยมีการจัดตั้งศูนย์กลาง คือ SCRO เป็นศูนย์กลาง (hub) ของการส่ง – รับข้อมูล ศูนย์กลางดังกล่าวจะทำหน้าที่ประมวลข้อมูลในระบบ และการดำเนินการดังกล่าวได้ดำเนินการโดยหน่วยงานที่เกี่ยวข้องได้ทำความตกลงร่วมกัน (agreement) ให้มีการเชื่อมโยง

การดำเนินการดังกล่าวส่งผลต่อการปฏิบัติงานในกระบวนการยุติธรรมใน 4 ประการ คือ 1)การบริการด้านข้อมูลเป็นไปโดยรวดเร็ว (Faster Services)2)การปรับปรุงในเรื่องความถูกต้องของข้อมูล (Improvement in Accuracy) 3)การปรับปรุงประสิทธิภาพในการใช้ของเจ้าหน้าที่ผู้ที่เกี่ยวข้อง (Improved efficiency in the use of staff) 4) ปรับปรุงการเข้าถึงข้อมูล (Improve access to information)การพัฒนาการบูรณาการข้อมูลดังกล่าว อาศัยหลักของการเป็นหุ้นส่วน (Partnership) ที่หน่วยงานต่างๆ ต้องดำเนินการร่วมกัน ไม่ใช่หน่วยงานใดจะเข้าถึงข้อมูลเฉพาะหน่วยงานอื่นๆ คดีต่างๆ จึงมีข้อมูลจากทุกหน่วยงานที่เกี่ยวข้องอย่างรวดเร็วอย่างไรก็ตาม จะมีการประเมินความเสี่ยงข้อมูล (Risk Management Evaluation) ทุกปี ส่วนระบบการบูรณาการข้อมูลด้านกระบวนการยุติธรรมของสหรัฐอเมริกา กระทรวงยุติธรรมได้ดำเนินการจัดตั้งศูนย์ข้อมูลวิสาหกิจบริหารจัดการโดยส่วนกลาง อาทิเช่น ระบบอาชญายุติธรรม (CJIS) ศูนย์ข้อมูลอาชญากรรมแห่งชาติ (NCIC) และระบบข้อมูลที่รวบรวมลายพิมพ์นิ้วมือ (IAFIS) ศูนย์ข้อมูลดังกล่าวมีคณะทำงานดูแลตลอด 24 ชั่วโมง และให้บริการผ่านระบบเครือข่าย ทั้งแบบที่มีชั้นความลับสูง (classified) และแบบทั่วไป (SBU) ซึ่งหน่วยงานระดับท้องถิ่น รัฐและสหพันธรัฐสามารถขอใช้บริการได้กระทรวงยุติธรรมยังได้จัดทำโครงสร้างข้อมูลมาตรฐานสำหรับกระบวนการยุติธรรม ที่เรียกว่า (Global Justice XML) ซึ่งนำเอาเทคโนโลยี XML มาใช้เป็นมาตรฐานในการแลกเปลี่ยนข้อมูล สำหรับหน่วยงานทั้งภาครัฐและเอกชนในการใช้ข้อมูลร่วมกันในระดับมลรัฐทั่วประเทศ มาตรฐาน Global Justice XML

เพื่อส่งเสริมการใช้มาตรฐานข้อมูล global Justice XML สมาคมข้อมูลสารสนเทศและสถิติแห่งชาติ หรือ SEARCH ได้สนับสนุนโครงการสร้างแบบจำลองการแลกเปลี่ยนข้อมูลยุติธรรม ซึ่งมุ่งเน้นการพัฒนาระบบบูรณาการข้อมูล และการนำไปสู่อนุวัติการ (implement) ทั่วประเทศ โดยผ่านระบบรักษาความปลอดภัยที่ต้องอาศัยการระบุตำแหน่งในการเข้าถึงข้อมูล คณะทำงานในโครงการได้พัฒนาเครือข่ายจำลองและวิธีการดึงข้อมูลรายละเอียดทั้งในแง่ของกระบวนการ เหตุการณ์ หน่วยงาน ข้อมูล และลักษณะการแลกเปลี่ยนที่สัมพันธ์กับการบูรณาการข้อมูลยุติธรรม ผลงานจากโครงการดังกล่าวได้เริ่มทดลองใช้งานแล้วใน 5 รัฐ คือ โคโลราโด แคนซัส มินเนโซต้า นิวเม็กซิโก และเพนซิลเวเนีย พร้อมทั้งได้เผยแพร่ไปยังศาลปกครองอีกกว่า 20 เขต

ภารกิจอีกประการของกระทรวงยุติธรรม คือ การรวบรวมข้อมูลสถิติที่เกี่ยวข้องกับอาชญากรรม อาชญากร เหยื่อผู้เคราะห์ร้าย และการทำงานของกระบวนการยุติธรรมในหลายๆระดับของรัฐบาล และนำเอาข้อมูลสถิติที่รวบรวมได้มาทำการวิเคราะห์ในด้านต่างๆ ตีพิมพ์ผลการวิเคราะห์และแสดงผลต่อหน่วยงานราชการและประชาชน

ยังมีแนวทางในการเก็บข้อมูลในกระบวนการยุติธรรมอีกประเภทหนึ่ง คือ “Biometrics”โดยแนวการดำเนินการแบบไบโอเมตทริคส์เป็นการเก็บรวบรวมข้อมูลด้านรูปพรรณสัณฐาน ที่จะระบุตัวบุคคลหรือระบุเอกลักษณะของบุคคล เนื่องจากในอดีตเราใช้ลายพิมพ์นิ้วมือ (finger printing) เป็นการระบุเอกลักษณ์ของบุคคล (personel identification) และใช้มาเป็นนับศตวรรษ อย่างไรก็ตาม การใช้แนวทางแบบไบโอเมติคส์นี้จะให้ความชัดเจนและความรวดเร็วในการระบุตัวได้ชัดเจนมากกว่า โดยการใช้เทคนิคที่ ได้แก่ Facial recognition, iris scanning, retinal scanning และ voice recognitionการประยุกต์เทคนิคด้านการ biometric technology ที่นำมาใช้เร็วๆนี้ ในอเมริกาก็คือ การจัดระบบความปลอดภัยแก่โรงเรียน หรือ school นอกจาก Biometric technology ยังมีการใช้ Bioagent detection ซึ่งในส่วนนี้ได้รับการสนับสนุนจากกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of homeland security) เพื่อใช้ในกลยุทธ์เพื่อการป้องกันอาชญากรรม เดิมแนวทางนี้ใช้ในการตรวจสอบโรคแอนแทรกซ์ (anthrax) แต่ได้นำมาประยุกต์ใช้เพื่อเก็บข้อมูลในการระบุยาเสพติด เมื่อเร็วๆนี้ The National Institute of Justice ได้วางนโยบายในการเก็บข้อมูลด้านงานยุติธรรมโดยใช้เทคโนโลยีดำเนินการด้วย การตระหนักและเฝ้าระวังถึงการก่อการร้ายได้ส่งผลดีต่อเนื่องมาถึงการใช้เทคโนโลยีในการแลกเปลี่ยนข้อมูล ในกระบวนการยุติธรรม และการวางแผนการบูรณาการข้อมูลเพื่อป้องกันอาชญากรรม ทั้งการทบทวนแนวทางและข้อมูลเดิม การใช้วิธีการและเทคโนโลยีใหม่ๆ รวมไปถึงการมีหุ้นส่วนกับชุมชนในการร่วมดำเนินการ ทุกองค์กรยอมรับในหลักการร่วมกันว่า การแลกเปลี่ยนข้อมูลในระบบกระบวนการยุติธรรมนั้นจะทำให้เกิดความปลอดภัยแก่สังคมโดยส่วนรวม อย่างไรก็ตาม แนวคิดเรื่อง การบูรณาการระบบข้อมูลด้านงานยุติธรรมหรือ JISI นั้นก็ยังแตกต่างกันออกไป ขอบเขตของข้อมูลให้เป็นเอกภาพ การให้นิยามความหมายและประเภทข้อมูลก็ยังหลากหลายแตกต่างกันออกไป (SEARCH 2001)

ในการศึกษาปัญหาและอุปสรรคที่เกิดขึ้นนั้น จากการศึกษาเกี่ยวกับการประมวลผลข้อมูลเกี่ยวกับ กระบวนการยุติธรรม และการนำเอาระบบข้อมูลเทคโนโลยีสารสนเทศมาใช้ในกระบวนการยุติธรรมนั้น พบว่าในต่างประเทศประสบปัญหาและอุปสรรคในด้าน หน่วยงานในกระบวนการยุติธรรมมีหลากหลายมากเกินไปและความต้องการของหน่วยงานก็แตกต่างกันทำให้การกำหนดมาตรฐานและการประมวลผลข้อมูล แตกต่างกันออกไป เช่น องค์กรตำรวจมีความต้องการและใช้ข้อมูลเกี่ยวกับการสืบสวนและจับกุม แต่ใน

องค์กรศาลไม่ต้องการข้อมูลที่เกี่ยวกับการสืบสวน เป็นต้น ดังนั้น ทำให้การประมวลผลมีความยุ่งยาก และล่าช้า เพราะอาจจะต้องมีการจำแนกเป็นข้อมูลประเภท primary, secondary เป็นต้น บางองค์กรในกระบวนการยุติธรรมยังไม่ให้ความสำคัญและจัดสรรงบประมาณให้น้อย ทำให้การดำเนินการเป็นไปอย่างล่าช้าและเชื่อมโยงข้อมูลได้ยาก เนื่องจากหลายๆองค์กรในกระบวนการยุติธรรม มองว่า หน่วยงานด้านเทคโนโลยีสารสนเทศ เป็นหน่วยงานสนับสนุนการทำงานไม่ใช่หน่วยงานหลัก และหน่วยงานตนเองก็อาจไม่จำเป็นต้องใช้ข้อมูลที่ได้จากการเก็บและประมวลผล ดังนั้นจึงไปมุ่งให้ความสำคัญกับการปฏิบัติงานหลัก หน่วยงานบางหน่วยงานยังมีขนาดเล็กเกินไปที่จะมีการจ้างบุคลากรที่มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศมาประมวลผลข้อมูลในกระบวนการยุติธรรม และการเป็นหน่วยงานเล็ก ข้อมูลน้อย การจ้างบุคลากรมาประจำเป็นการไม่คุ้มค่าใช้จ่ายในการดำเนินการองค์กร การขาดการวางแผนระยะยาวในการดำเนินการ การจัดสรรงบประมาณอาจพิจารณาให้ไม่ต่อเนื่องให้เฉพาะบางปี ทำให้การประมวลผลก็ขาดความต่อเนื่องตามไปด้วย

การมีข้อจำกัดในด้านบุคลากรและการออกแบบเพื่อนำมาใช้งานหรือใช้ประโยชน์อย่างจริงจัง เนื่องจากการเก็บรวบรวมและแลกเปลี่ยนข้อมูลตลอดจนการบูรณาการข้อมูลในองค์กรจำเป็นจะต้องอาศัยบุคลากรที่มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้านมาเป็นผู้ช่วยวางแผนและออกแบบระบบให้เหมาะสมกับองค์กรและการใช้งาน ซึ่งองค์กรหลายองค์กรในกระบวนการยุติธรรมก็ขาดบุคลากรด้านนี้โดยตรง การจัดหาจึงเป็นเพียงอุปกรณ์มาประจำ การประสบปัญหาในด้านความเสี่ยงต่างๆ ปัญหาความเสี่ยงต่างๆที่เกิดขึ้นมีหลายประการ โดยเฉพาะอย่างยิ่ง จากด้าน ข้อมูลส่วนบุคคล (privacy) และ เรื่องความปลอดภัยของข้อมูล (security) (Peter Csonka 2001) นอกจากนี้ยังมีปัญหาความเสี่ยงอื่นๆตามมา อาทิ เช่น ความถูกต้องของข้อมูล การสร้างข้อจำกัดในการใช้ การเข้าไปใช้ข้อมูลโดยไม่ได้รับอนุญาต หรือไม่มีอำนาจอาชญากรรมคอมพิวเตอร์ เป็นต้น ความหวาดกลัวในปัญหาเกี่ยวกับความรับผิด (liability) หากมีความผิดพลาดเกิดขึ้นกับข้อมูล โดยเฉพาะหากตนเองต้องรับผิดชอบโดยตรง ซึ่งความรับผิดจะเกิดขึ้นกับตน ซึ่งจะสร้างความยุ่งยากในการปฏิบัติงานในองค์กร ดังนั้น การดำเนินการประมวลผลและแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม จึงดูเหมือนจะสร้างความยุ่งยากลำบากใจมากกว่า จึงไม่ให้ความสนใจในการดำเนินการ

ปัญหาต่างๆเหล่านี้ บางปัญหาก็ได้รับการแก้ไข เช่น ในปัญหาที่เกี่ยวพันกับงบประมาณ หากองค์กรใดสนใจสมัครเข้าร่วมในการดำเนินการ ก็จะมีการจัดสรรงบประมาณให้จำนวนหนึ่ง(โดยมีการประเมินผล) และให้ผู้เชี่ยวชาญในการวางแผนระบบเข้าไปช่วยวางแผนในหน่วยงาน เป็นต้น

สำหรับประเทศไทย การบูรณาการข้อมูลด้านงานยุติธรรมของไทย ปัจจุบันหน่วยงานในกระบวนการยุติธรรมที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานมีทั้งสิ้น 14 หน่วยงาน ได้แก่ ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติ กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน กรมบังคับคดี สถาบันนิติวิทยาศาสตร์ กรมคุ้มครองสิทธิและเสรีภาพ

นอกจากนี้ ผลการศึกษาพบยังพบว่า การเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมของไทยยังมีน้อยมาก เช่น กองทะเบียนประวัติอาชญากร ได้มีการเชื่อมโยงข้อมูลกับหน่วยงานแค่บางหน่วยงาน คือ สำนักงานป้องกันและปราบปรามยาเสพติด (ปปส.) กรมราชทัณฑ์ กรมคุมประพฤติ เป็นต้น ส่วนหน่วยงานอื่นๆในกระบวนการยุติธรรมยังไม่ได้มีการดำเนินการเชื่อมโยงข้อมูลแต่อย่างใด หน่วยงานต่างๆ ยังมีความต้องการเชื่อมโยงหรือบูรณาการข้อมูลอย่างยิ่งกับหน่วยงานอื่นๆในกระบวนการยุติธรรมโดยมุ่งที่จะเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรมในลักษณะที่เป็นทั้งผู้ให้และเป็นทั้งผู้ใช้ แต่ก็อยากที่จะเริ่มการเชื่อมโยงข้อมูลกับหน่วยงานที่จำเป็น และมีระบบข้อมูลคล้ายคลึงกันก่อน จากนั้น หากมีการดำเนินการที่ได้ผลจึงจะค่อยๆขยายออกไปกับหน่วยงานอื่นๆ เพราะข้อมูลเหล่านั้นจะเป็นประโยชน์สำหรับการปฏิบัติงานและสามารถนำไปใช้ในการจัดทำนโยบายและแผนของหน่วยงานได้

สำหรับปัญหาและอุปสรรคในการดำเนินการ ได้แก่ การขาดนโยบายที่ชัดเจนว่าควรจะจัดเก็บข้อมูลอะไรบ้าง และขาดความต่อเนื่องในการดำเนินการ (บางหน่วยงาน เช่น กรมราชทัณฑ์) ไม่ได้ขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม แต่ขาดการดำเนินการอย่างจริงจังและต่อเนื่องประกอบกับการเปลี่ยนแปลงรัฐบาลที่ทำให้การพัฒนากระบวนการยุติธรรมของประเทศดำเนินไปอย่างล่าช้า ซึ่งก็ส่งผลกระทบต่อการใช้เทคโนโลยีสารสนเทศด้วย และ ในการดำเนินการยังขาดหน่วยงานที่เป็นเจ้าภาพหลัก ในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการประมวลผล หากมีหน่วยงานที่เป็นเจ้าภาพหลักในการบูรณาการข้อมูลจะช่วยประสานงานให้หน่วยงานของแต่ละหน่วยงานมีข้อมูลที่ถูกต้อง เหมาะสม และทันเวลา การดำเนินการบูรณาการข้อมูลในกระบวนการยุติธรรมนั้น จำเป็นอย่างยิ่งที่ผู้บริหารระดับสูงต้องให้ความสำคัญอย่างยิ่ง ในขณะที่ปัญหาด้านงบประมาณก็มีส่วนสำคัญทั้งๆที่รู้และเข้าใจในบทบาทงานด้านเทคโนโลยีสารสนเทศแต่การต้องใช้งบประมาณที่สูง และงานด้านเทคโนโลยีสารสนเทศ

ยังไม่ใช่งานหลักของหน่วยงาน เป็นภาระงานที่ยังรอได้ อันส่งผลกระทบต่อเนื่องที่ทำให้ขาดความพร้อมทางด้านอุปกรณ์ต่าง ๆของทุกหน่วยงานในกระบวนการยุติธรรมมากน้อยแตกต่างกันไป ประกอบกันปัญหาการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน เนื่องจากการเปลี่ยนแปลงเทคโนโลยีที่รวดเร็วและบุคลากรที่เก่งจริงก็ไปอยู่ในภาคเอกชน

ส่วนด้านปัญหาการเก็บรวบรวมข้อมูลที่มีความซับซ้อนนั้น ปัญหานี้มีสาเหตุจากการที่แต่ละหน่วยงานจะจัดเก็บกันเอง โดยมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ต่างฝ่ายต่างจัดเก็บ ก็ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก เพราะยังขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ส่งผลตามมาทำให้ข้อมูลมีความน่าเชื่อถือน้อย เพราะมีข้อมูลจำนวนมากที่ขาดการปรับปรุง เปลี่ยนแปลง ข้อมูลให้เป็นปัจจุบัน จัดเก็บแล้วก็ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน ด้านการคุ้มครองข้อมูลก็เป็นสิ่งที่จำเป็นเพราะถือว่าข้อมูลของบุคคลที่เป็นความลับส่วนบุคคล เป็นสิ่งที่เป็นผลเสียได้สำหรับบุคคลนั้น การเคารพสิทธิ์ในข้อมูลส่วนบุคคลจึงต้องมีอยู่และให้การคุ้มครอง ปัญหาหลักอื่น ๆก็คือ การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ ซึ่งก็ส่งผลให้หลาย ๆหน่วยงานจึงขาดความพร้อมสำหรับการบูรณาการ

ส่วนปัญหาทางกฎหมายที่เกี่ยวข้องก็คือ มีข้อมูลจำนวนมากที่กองทะเบียนประวัติอาชญากรจัดเก็บ และมีการดำเนินการเตรียมในระบบฐานข้อมูลเทคโนโลยีสารสนเทศแล้ว แต่ข้อมูลเหล่านั้น ยังต้องถือเป็นความลับส่วนบุคคลที่ไม่สามารถจัดส่งให้หน่วยงานอื่น ๆได้ เนื่องจาก ข้อมูลของบุคคลเหล่านี้ (ยัง) เป็นข้อมูลเกี่ยวกับ “ผู้ต้องหา” ไม่ใช่จำเลย ซึ่งในกฎหมายแม่บท เช่น กฎหมายรัฐธรรมนูญกำหนดว่า ผู้ต้องหาหรือแม้จำเลยนั้น ต้องสันนิษฐานว่าเป็นผู้บริสุทธิ์อยู่ การเปิดเผยข้อมูลส่วนบุคคลอาจจะนำไปสู่การถูกฟ้องร้อง ตามประมวลกฎหมายอาญา มาตรา 157 และตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420, 423 เรื่องละเมิด และ หมิ่นประมาทได้

หากมีข้อตกลงระหว่างหน่วยงานในกระบวนการยุติธรรมชัดเจน ให้ถือเป็นการดำเนินการที่ชัดเจน ก็อาจเป็นข้อยกเว้นได้ และทางกองทะเบียนประวัติอาชญากรก็ได้มีการเตรียมดำเนินการปรับปรุงระเบียบการใช้ข้อมูลดังกล่าว แต่อยู่ในระหว่างการดำเนินการอยู่ อย่างไรก็ตามในส่วนของบุคลากรผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูล ยังมีความกังวลในเรื่องของการเชื่อมโยงข้อมูล เพราะนั่นหมายความว่า ข้อมูลที่อยู่ในครอบครองและถูกเก็บไว้ จะถูกใช้โดยหน่วยงานอื่น ๆซึ่งหากไม่มีกฎหมายมารองรับให้เกิดความชัดเจน เกรงว่าจะถูกฟ้องร้องดำเนินคดีได้ เพราะการจัดเก็บข้อมูล เป็นการจัดเก็บตามที่กฎหมายให้อำนาจ แต่การใช้ข้อมูลยังมีความไม่ชัดเจนหากมีบุคคลหรือหน่วยงานอื่น ๆเอาไปใช้

จากการศึกษากฎหมาย และระเบียบต่างๆที่เกี่ยวข้องกับการเชื่อมโยง การแลกเปลี่ยนและการบูรณาการข้อมูลด้านกระบวนการยุติธรรมทั้งจากของไทยและของต่างประเทศ สามารถจำแนกกฎหมาย และระเบียบต่างเหล่านั้น ออกได้เป็น 4 กลุ่มใหญ่ คือ

1.กฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรม

2.กฎหมายคุ้มครองข้อมูลส่วนบุคคล

3.กฎหมายเกี่ยวกับทรัพย์สินทางปัญญา

4.กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิด

โดยกฎหมายที่เกี่ยวข้องกับการเชื่อมต่อ การแลกเปลี่ยนและการบูรณาการข้อมูลในกระบวนการยุติธรรมประเทศที่มีระบบกฎหมายแบบ Common law ที่มีการพัฒนาและออกกฎหมายมารองรับการจัดทำฐานข้อมูลและการเชื่อมต่อบูรณาการข้อมูลในกระบวนการยุติธรรม โดยมีการกำหนดมาตรการต่างๆพบกฎหมายที่จำเป็นและวางแนวทางการดำเนินการอย่างเป็นระบบ ซึ่งกฎหมายเหล่านี้ได้แก่ เช่น กฎหมายของสหรัฐอเมริกา**The Crime Identification Technology Act of 1998 (CITA)**(กฎหมายฉบับนี้เป็นที่มีบทบัญญัติที่ครอบคลุมเกี่ยวกับการเชื่อมต่อและการบูรณาการข้อมูลและรวมทั้งการแลกเปลี่ยนข้อมูลในหน่วยงานในกระบวนการยุติธรรมมากที่สุด ฉบับหนึ่ง โดยเน้นการแลกเปลี่ยนและการบูรณาการข้อมูลในหน่วยงานในกระบวนการยุติธรรม โดยกฎหมายฉบับนี้ได้ให้รัฐสภาตัดงบประมาณรายจ่ายจำนวน 250 ล้านเหรียญอเมริกันต่อปี ติดต่อกันเป็นเวลา 5 ปี (รวมราว 1.25 พันล้านเหรียญอเมริกัน) เพื่อให้มลรัฐต่างๆ ได้ส่งเสริมการบูรณาการข้อมูลในระบบกระบวนการยุติธรรมโดยใช้เทคโนโลยีเฉพาะ นอกจากการกำหนดให้มีการจัดสรรงบประมาณรายจ่ายประจำปีให้แล้วยังระบุให้หน่วยงานที่ทำหน้าที่ในการบังคับใช้กฎหมายด้านกระบวนการยุติธรรม เช่น ศาล อัยการ ราชทัณฑ์ ฯลฯ ได้มีการแลกเปลี่ยนข้อมูลและการสื่อสารในด้านข้อมูลให้มีประสิทธิภาพมากขึ้นบนหลักของการกำหนดเวลาที่แท้จริง (real – time basis) ด้วย **(The Brady Handgun Violence Prevention Act (Brady Act),** ในบรรดาคดีอุฉกรรจ์ (Violent Crime) ที่เกิดขึ้นในอเมริกานั้น พบข้อเท็จจริงว่า มีการใช้อาวุธปืนร่วมด้วยเกือบทุกครั้ง ดังนั้น กฎหมายฉบับนี้จึงมุ่งที่จะให้มีการขึ้นทะเบียนผู้ที่ค้าอาวุธปืน และผู้ที่มีอาวุธปืนไว้ในครอบครอง ตลอดจนมีการตรวจสอบการครอบครองอาวุธปืน รวมถึงมาตรการต่างๆ เช่น การต้องมาต่อทะเบียนอาวุธปืน

ที่ครอบคาองทุก 2 ปี เป็นต้น การขึ้นทะเบียนอาวุธปืนจะสามารถจำแนกประเภทอาวุธปืนได้ว่ามีบุคคลใดครอบครองอาวุธปืนชนิดใด มีอานุภาพร้ายแรงมากน้อยเพียงใด แม้จะเป็นปืนพกก็ตาม **the National Child Protection Act of 1993 (NCPA)** กฎหมายฉบับนี้มุ่งที่จะให้มลรัฐต่าง ๆได้ส่งข้อมูล “การประกอบอาชญากรรมที่มีการแสวงหาผลประโยชน์และล่วงละเมิดเด็ก” (Child abuse crime information) หรือ ดัชนีชี้วัดข้อมูลดังกล่าวในทะเบียนประวัติอาชญากรระดับชาติที่ FBI จัดเก็บ ดังนั้น ถือเป็นหน้าที่ของมลรัฐในการที่จะต้องจัดทำมาตรฐานด้านความปลอดภัยและการเข้าถึงข้อมูลดังกล่าว **the Omnibus Crime Control and Safe Streets Act of 1968 (Omnibus Act) the Violent Crime Control and Law Enforcement Act of 1994 (Violent Crime Control Act)**, (กฎหมายฉบับนี้ให้รัฐต่างออกกฎหมายให้มีการลงทะเบียนข้อมูลประวัติอาชญากรทางเพศ ที่กระทำผิด และถูกคุมขังหลังจากถูกปล่อยตัวไปแล้ว 10 ปี) **Relevant requirements of the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act, Megan's Law,**(เป็นกฎหมายของมลรัฐเพนซิลวาเนีย จากฝ่าย Megan Law Section โดยระบุให้ตำรวจของมลรัฐต้องจัดทำและดูและข้อมูลการเปลี่ยนแปลงการลงทะเบียนของบุคคลที่เข้ามาอาศัยในพื้นที่) **the Pam Lychner Sexual Offender Tracking and Identification Act of 1996,** (การจัดเก็บและลงทะเบียนดังกล่าวเป็นการกระทำเฉพาะข้อมูลเกี่ยวกับผู้กระทำผิดในทางเพศเท่านั้น) **the Victims of Trafficking and Violence Protection Act of 2000**(มีมาตรการต่าง ๆขึ้นมาป้องกันและปราบปราม การช่วยเหลือเหยื่อ ก็จะมีการให้หน่วยงานที่เกี่ยวข้องทำการเก็บรวบรวมและประมาณข้อมูลที่เกี่ยวข้อง พร้อมทั้งจัดทำรายงานประจำปี (Annual Report) เสนอ หน่วยงานที่เกี่ยวข้องและยังมีการส่งข้อมูลให้ฝ่ายตรวจคนเข้าเมืองประสานการข้ามเดินทางเข้าประเทศแก่บุคคลที่ขึ้นบัญชีดำการค้าผู้หญิง และเด็กและให้ตรวจสอบผู้เสียหายที่เดินทางด้วย ตลอดจนรวบรวมพฤติกรรมและจัดทำพัฒนาฐานข้อมูล)

5.2 ข้อเสนอแนะ

จากการศึกษาวิจัย ผู้วิจัยมีข้อเสนอแนะดังต่อไปนี้

5.2.1 ข้อเสนอแนะด้านการดำเนินการ (การแก้ไขปัญหาและอุปสรรค)

1. จากการศึกษาพบว่า หน่วยงานในกระบวนการยุติธรรมส่วนใหญ่ ยังไม่ได้มีการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลในกระบวนการยุติธรรม จะมีก็เพียงส่วนน้อย

ไม่กี่หน่วยงาน และแม้บางหน่วยงานจะทำความตกลงร่วมมือกัน แต่ก็ยังขาดความชัดเจนว่าข้อมูลที่ต้องการเชื่อมโยงมีและจะดำเนินการเชื่อมโยงกันอย่างไร เนื่องจากขาดเจ้าภาพหลักในการดำเนินการ ดังนั้น กระทรวงยุติธรรม ควรจะเป็นเจ้าภาพหลักในการดำเนินการ โดยการมอบหมายให้มีหน่วยงานหลักที่รับผิดชอบดูแลโดยเฉพาะ และดำเนินการในกระทรวงยุติธรรมก่อน

2.กระทรวงยุติธรรมควรกำหนดเป็นนโยบายที่ให้ทุกหน่วยงานในสังกัดจัดทำแผน โครงการ จัดเก็บ ประมวลผลข้อมูล และดำเนินการเชื่อมต่อ แลกเปลี่ยน และบูรณาการข้อมูลระหว่างหน่วยงานในกระทรวงยุติธรรมเป็นหลักก่อน จากนั้นค่อยขยายความร่วมมือไปยังหน่วยงานเชื่อมโยง เช่น สำนักงานอัยการสูงสุด สำนักงาน ปปส. เป็นต้น และขยายความร่วมมือไปยังหน่วยงานภายนอก เช่น กรมศุลกากร เป็นต้น

3.ควรมีการจัดทำคู่มือการดำเนินการ (Code of Practice) ขึ้นมา เพื่อเป็นแนวทางให้หน่วยงานต่างๆ ได้ใช้เป็นแนวทางและมาตรฐานในการจัดเก็บข้อมูล ประมวลผลข้อมูล และการเชื่อมต่อ ตลอดจนหน่วยงานบุคลากรที่ติดต่อได้โดยตรงสำหรับหน่วยงาน และกฎหมายที่เกี่ยวข้อง

4.กระทรวงยุติธรรม ควรมีการจัดคณะทำงานกลาง (Liasison Staffs) เพื่อทำหน้าที่ประสานงาน และให้คำแนะนำเกี่ยวกับการจัดทำฐานข้อมูล และการแลกเปลี่ยนและเชื่อมต่อ ตลอดจนการบูรณาการข้อมูลระหว่างหน่วยงานในกระทรวงยุติธรรมก่อน

5. ควรมีการสำรวจความต้องการใช้ข้อมูลในการปฏิบัติงานของหน่วยงานต่างๆ เพื่อเป็นข้อมูลในการจัดทำแบบในการจัดเก็บให้เป็นมาตรฐานในการจัดเก็บ การประมวลข้อมูล และการวางแผนการเชื่อมต่อและการแลกเปลี่ยนข้อมูลสำหรับหน่วยงานในกระบวนการยุติธรรมต่อไป

5.2.2 ข้อเสนอแนะในด้านการปรับปรุงกฎหมาย

1. เนื่องจากจากการสำรวจโดยทั่วไปพบว่า ประเทศไทยยังไม่มีกฎหมายกลางโดยเฉพาะ ที่จะเอื้ออำนวยต่อการเชื่อมต่อและการแลกเปลี่ยนข้อมูล หรือ การบูรณาการข้อมูลในกระบวนการยุติธรรมโดยเฉพาะโดยตรง กฎหมายที่มีอยู่ก็กระจัดกระจายและไม่ได้มีวัตถุประสงค์โดยตรงสำหรับการเชื่อมโยง การแลกเปลี่ยน หรือการบูรณาการข้อมูลในกระบวนการยุติธรรม ซึ่งการปรับใช้และการนำมาประยุกต์ใช้อาจจะไม่ตรงกับเจตนารมณ์และ

วัตถุประสงค์ของการดำเนินการ ดังนั้นในระยะแรก ควรจะมีการออกเป็นระเบียบของกระทรวงยุติธรรมออกมาใช้ก่อน เพื่อให้มีการดำเนินการ เนื่องจากกระทรวงยุติธรรม มีหน่วยงานในด้านงานยุติธรรมที่เกี่ยวข้องหลายหน่วยงาน และยังมีหน่วยงานที่เชื่อมโยงหลายหน่วยงานจึงควรมีการ ออกกฎหมายในฝ่ายบริหาร มาดำเนินการในระยะแรก

2. การยกร่างกฎหมายที่เกี่ยวข้องกับการบริหารจัดการเกี่ยวกับการเชื่อมโยงแลกเปลี่ยน และบูรณาการข้อมูลในกระบวนการยุติธรรมซึ่งกฎหมายดังกล่าวควรให้มีการจัดตั้งคณะกรรมการขึ้นมาควบคุมกำกับดูแลการดำเนินการจะเหมาะสมกว่า เนื่องจากเทคโนโลยีมีการปรับเปลี่ยนอยู่เสมอ การดำเนินการในรูปคณะกรรมการที่มีอำนาจหน้าที่จะมีความเหมาะสมกว่า

3. ในการจัดทำร่างกฎ ระเบียบ หรือ กฎหมายที่เกี่ยวข้องนั้น ควรคำนึงถึงแนวคิด หลักการ และแนวทางการดำเนินการที่เป็นสากล เนื่องจากต่อไปในอนาคตอาจจะมีการเชื่อมต่อข้อมูลด้านกระบวนการยุติธรรมกับประเทศต่างๆที่มีมาตรฐานเดียวกัน

4. เนื่องจากหน่วยงานต่างๆในกระบวนการยุติธรรม มีการเก็บข้อมูลในฐานข้อมูลของตน และในบางหน่วยงาน เช่น สำนักงานคณะกรรมการ ปปช. สำนักงานคณะกรรมการ ปปง. มีกฎหมายเฉพาะที่ห้ามเปิดเผยข้อมูลเฉพาะ จึงมีควรมีการประชุมและกำหนดประเภทของข้อมูลที่เปิดเผยได้ เปิดเผยไม่ได้ ซึ่งในการออกระเบียบ กฎหมายที่เกี่ยวข้อง จำเป็นต้องมีมาตรการที่ระบุถึงประเภทข้อมูลเหล่านี้ด้วย เพราะให้สามารถเชื่อมโยงแลกเปลี่ยนและบูรณาการข้อมูลในบางระดับที่เหมาะสมต่อไป

5. ในการออกมาตรการทางกฎหมายที่เกี่ยวข้องนั้น ข้อที่ควรจะต้องพิจารณาอย่างยิ่งสำหรับกฎหมายเกี่ยวกับการเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลในกระบวนการยุติธรรมก็คือการต้องมีมาตรการที่ป้องกันมิให้นักการเมืองเข้ามาแสวงหาและใช้ประโยชน์จากฐานข้อมูลและการเชื่อมโยงข้อมูลและการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม

บรรณานุกรม

แก้วสรร อติโพธิ. **ความรู้เกี่ยวกับกฎหมายลิขสิทธิ์.** กรุงเทพมหานคร:โรงพิมพ์เจริญศิลป์, 2527.

จักรกฤษณ์ ควรพจน์. **กฎหมายระหว่างประเทศว่าด้วยลิขสิทธิ์ สิทธิบัตรและเครื่องหมายการค้า.** กรุงเทพมหานคร:นิติธรรม, 2538.

จรัญ ภักดีธนากุล. **กฎหมายทรัพย์สินทางปัญญา.** กรุงเทพมหานคร:บริการส่งเสริมงานตุลาการ, 2532.

ไชยยศ เหมะรัชตะ. **กฎหมายทรัพย์สินทางปัญญา**. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร:นิติธรรม, 2540.

ชวลิต อัตถศาสตร์. **Cyber Law กฎหมายกับอินเตอร์เน็ต.** กรุงเทพฯ: โปรวิชั่น, 2444.

ไชยวัฒน์ บุนนาค และ ไพบูลย์ อมรภิญโญเกียรติ. *"ความรู้เบื้องต้นและปัญหาข้อกฎหมายเกี่ยวกับการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์."* ใน **เอกสารประกอบการสัมมนาเรื่อง ปัญหาข้อกฎหมายที่เกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์ในสังคมยุคเทคโนโลยีสารสนเทศ.** หน้า 1 – 7. กรุงเทพฯ: สำนักพิมพ์ธรรมศาสตร์, 2541.

เลอสรร ธนสุกาญจน์, จิตรภัทร เครือวรรณ์ และ สุธรรม อยู่ในธรรม. **กฎหมายสำหรับบริกาอินเตอร์เน็ตในประเทศไทย**. กรุงเทพฯ: สำนักพิมพ์นิติธรรม, 2541.

ธัชชัย ศุภผลศิริ. **คำอธิบายกฎหมายลิขสิทธิ์.** กรุงเทพมหานคร:นิติธรรม, 2539.

สุธรรม อยู่ในธรรม, เลอสรร ธนสุกาญจน์, พรเพชร วิชิตชลชัย, บัณฑิต หลิมสกุล และ อรพรรณ พนัสพัฒนา. **แนวทางการพัฒนากฎหมายแลกเปลี่ยนข้อมูลด้วยสื่ออิเล็กทรอนิกส์ในประเทศไทย.** กรุงเทพฯ: สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ กระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม, 2539.

บริษัท คอมมิวนิเคชั่นคอนเซปต์ จำกัด. **เจาะลึกกฎหมายลิขสิทธิ์ 2537.** กรุงเทพมหานคร: เอช.เอ็น.กรุ๊ป, 2538.

ประสิทธิ์ เอกบุตร. **กฎหมายระหว่างประเทศ : สนธิสัญญา เล่ม 1.** กรุงเทพมหานคร: นิติธรรม, 2538.

ศิลปากร, กรม. **ความผูกพันระหว่างประเทศไทยกับอนุสัญญาเบอร์นเพื่อการคุ้มครองวรรณกรรมและศิลปกรรม.** กรุงเทพมหานคร:สหประชาพาณิชย์, 2529.

บทความ

กิติศักดิ์ ปรกติ. *"การคุ้มครองลิขสิทธิ์ในกฎหมายไทย".* **วารสารนิติศาสตร์,** ปีที่ 13 ฉบับที่ 3 (ธันวาคม, 2526) : หน้า 1-15.

จักรกฤษณ์ ควรพจน์. *"บทวิเคราะห์ร่างแก้ไขกฎหมายสิทธิบัตรศึกษาจากหลักการภายใต้ข้อตกลง TRIPS และอนุสัญญาปารีส".* **วารสารนิติศาสตร์.** ปีที่ 26 ฉบับที่ 3 (กันยายน 2539) : หน้า 450-467.

ประสิทธิ์ เอกบุตร. *"ข้อเสนอทางกฎหมายบางประการต่อการกำหนดนโยบายทางการค้าระหว่างประเทศของไทยใน GATT".* **วารสารนิติศาสตร์ มธ.** ปีที่ 15 ฉบับที่ 4 (ธันวาคม 2528) : หน้า 21-39.

ยรรยง พวงราช. *"ทรัพย์สินทางปัญญา : ความหมาย ขอบเขต ความเป็นมาและความสำคัญ".* **บทบัณฑิตย์.** เล่ม 54 (มีนาคม 2541) : หน้า 15-21.

วีรวิทย์ วีรวรวิทย์. "*Copyright in the Digital Age".* **บทบัณฑิตย์.** เล่ม 54 (มีนาคม 2541) : หน้า 35-59.

อรุณ ภาณุพงศ์. *"มิติใหม่ของกฎหมายระหว่างประเทศ".* **หนังสือวิชาการทางกฎหมายในโอกาสครบรอบ 50 ปี.** จัดพิมพ์โดยคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ (กรุงเทพมหานคร:โรงพิมพ์ธรรมศาสตร์, 2538) : หน้า 162-174.

อรุณ ภาณุพงศ์. “*จาก GATT สู่ WTO”.* **วารสารนิติศาสตร์.** ปีที่ 25 เล่มที่ 3 (กันยายน 2538) : หน้า 433-444.

อำนาจ เนตยสุภา. “*กฎหมายกับอินเตอร์เน็ต”.* **บทบัณฑิตย์.** เล่ม 54 (มีนาคม 2541) : หน้า 152-183.

วิทยานิพนธ์

วิชาญ ธรรมสุจริต. “**ปัญหาการดำเนินคดีละเมิดลิขสิทธิ์ระหว่างประเทศ”.** วิทยานิพนธ์บัณฑิตวิทยาลัย. คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2537.

สุกัญญา ศีลนำกิจ. “**การให้ความคุ้มครองงานอันมีลิขสิทธิ์ตามกฎหมายฮ่องกงในประเทศไทย”.** วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2530.

องอาจ เทียนหิรัญ. “**อาชญากรรมทางคอมพิวเตอร์: การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์.”** วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์: 2546

นัยนรัตน์ งามแสง. **“อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเทอร์เน็ต.”** วิทยานิพนธ์มหาบัณฑิต คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547.

เชิดพันธ์ อุปนิสากร. **“ความรับผิดทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต.”**วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2542.

พรชัย เหลียวพัฒนพงศ์. “**ความผิดเกี่ยวกับไวรัสคอมพิวเตอร์.”** วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย,2537.

ปารเมศ บุญญานันต์ 2543 **กฎหมายคุ้มครองข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์** วิทยานิพนธ์มหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย

ไตรภพ วงศ์ไตรรัตน์ 2544. **กฎหมายว่าด้วยการคุ้มครองสิทธิในข้อมูลข่าวสารส่วนบุคคลจากการใช้สื่ออิเลกโทรนิกส์** วิทยานิพนธ์มหาบัณฑิต มหาวิทยาลัยรามคำแหง

ภานุ รังสิสหัส. "**การกระทำผิดทางอาญาเกี่ยวกับคอมพิวเตอร์.**" วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย,2533.

เลิศชาย สุธรรมพร. **"อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล"** วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2541.

กิตติพงศ์ กมลธรามวงศ์. **มาตรการทางกฎหมายเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์.** กรุงเทพฯ : วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549

ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์

ภาษาอังกฤษ

Textbooks

A.A.L. Beers, Informatica Publica: publieke toegankelijkheid van electronischeoverheids-informatie, Den Haag: Rathenau Institute 1996, Study 34; A.A.L. Beers,"Overheidsinformatie op Internet", **Nederlands Juristenblad** 1996/41, pp. 1708-1716.

Actieprogramma Elektronische Snelwegen, **Parliamentary Papers,** 24 565, no. 1ff. Amersfoort 1996; R. Overdijk, De mythe van de elektronische snelweg: van karrenpad tot

Adam, Eric J. *"Second Coming for Electronic Data Interchange."* **World Trade** 15 (November, 1997): 36.

Alfred Blumstein, Jacqueline Cohen, and Richard Rosenfeld “Trend and Deviance in Crime Rates: A Comparison of UCR and NCUS data for Burglary and Robbery” **Criminology 29** (1991) : 237-248

Caffrey, L. (1998). I**nformation sharing between & within governments. A study group report of the Commonwealth Secretariat**. London: The International Council for Technology in Government Administration.

Chance, Clifford**. Data Protection.** Chicago: CCH. Edition, 1994.

Cole Durham. “The Emerging Strutting of Criminal information Law : Tracing the Contours of a New Paradigm, “information Technology Crime Vol 6. Berlin : Carl Heymanns Verlag KG,1994.

Commonwealth of Pennsylvania Governor’s Office. (2003,July 1). **Executive order: Pennsylvania Justice Network Governance Structure number 1999-4.** Last retrieved June 2, 2004,

Cresswell, A.M. and Connelly D. (1999). **Reconnaissance study. Developing a business case for the integration of criminal justice information.** Albany, NY: Center for Technology in Government.

David O. Arnold .**Computers and Society Impact.** San Francisco : McGraw-Hil,1991.

Dawes, S. (1996*). Interagency Information Sharing: Expected Benefits, Manageable Risks*. **Journal of Policy Analysis and Management,** 15, 377-394.

Donald K. Piragoff. “Computer Crimes and Other Crimes against Information Technology In Canada, “in **Information Technology Crime** Vol 6. Berlin : Carl Heymanns Verlag KG,1994.

Donn B.Parker,S.Nycum and S.Aura.**Computer Abuse.** California : Stanford Research Cited by Marith Wasik .**Crime and the Computer.** Oxford : CLARENDON press 1991.

Dunworth Terrance *"Criminal Justice and the it Revolution"* **Federal Probation**. Sep. 2001 Vol. 65. piv PAG.

Edward M. Wise. "Computer Crimes and Other Crimes against information Technology In the United States, " in **Informtion Technology Crime.** Vol 6.Berlin : Carl Heymanns Verlag KG,1994.

E.J. Dommering, "Het auteursrecht spoelt weg door het electronisch vergiet. De naderende crisis van het auteursrecht.", Computerrecht 1994/3, pp.109 ff. fax en email vogelvrij", **Nederlands Juristenblad** nr. 33, 1997, pp. 1554-1555.) "Inventory and evaluation of the penalization of crimes committed on the electronic superhighway (with the exception of the offences committed through expression)", ITeR studied, project leader Prof. M.S. Groenhuijsen, 1997.

Harris Kelly J. *"Justice System Integration: On the Threshold of a New Era"* **Correction Today.** July 99, Vol. 61 p. 72.

Hennepin County **Criminal Justice System Information Integration Project**. Last retrieved June 2, 2004,

Holmes, A. (Fall 1999/Winter 2000**) Delaware Criminal Justice Information System: The evolution of integration. Case study series. A report of the National Task Force on Court Automation and Integration.** Last retrieved June 2, 2004,

Hugenholtz(ed.), The Future of Copyright in a Digital Environment, The Hague/London/Boston 1996;snelweg, de ontwikkeling van het elektronisch wegennet, Amsterdam 1997.Staatsuitgeverij, Ministerie van Justitie 1987.

Gerald L.Jenkins, Terry F.Moritz, and Charles J.Muhl. **Business.law and the internet.** Chicago:Goldberg,Kohn,Bell Black,Rosenblooom & Moritz,Ltd0.,2002.

G.P.V.Vanderberghe. **Advanced Topics of Law and information Technology.** Boston : Kluwer Law and Taxation Publishers,1996.

James A.O.'Brien.**Management Information System : Managing information Technology in the Networked Enterprise**.3 rd. California: McGraw,1996.

James X. Eempsey 2004 **Overview of Current Criminal Justice Information System** NY Prentices-Hall

J.M.A. Berkvens and J.E.J. Prins, "De bescherming van persoonsgegevens: van WPR naar WBP", **Recht en computer, Deventer** 1997, pp. 315-369.

Larry J. Siegel 1998 **Criminology' Theories, Patterns and Typologies** Washington : West/Wadsworth Publishing Company.

Martin Wasik. " Computer Crimes and Other Crimes against information Technology in United Kingdom, "in **Information Technology Crime** Vol 6. Berlin : Carl Heymanns Verlag KG,1994.

Maritn Wasik. "Computer Crimes and Other Crimes against Information Technology in United Kingdom, "in **Information Technology Crimes** Vol 6. Berlin : Carl Heymanns Verlag KG,1994.

Maritn Wasik. **Crimes and the Computer.** Oxford : Clarendon Press ,1991.

Michael A. Sussmann. “The Critical Challenges from International High - Tech and Computer - Related Crime at the Millenium, “in **SELECTED MATEREAL ON COMBATING HIGH-TECH AND COMPUTER RELATER CRIME** Beijing China, 2000.

Manfred Mohrenschlager. “Computer Crimes and Other Crimes against Information Technology in Germany, “in **Information Technology Crimes** Vol 6. Berlin : Carl Heymanns Verlag KG,1994.

M.M Reuland **1997 Information Management and Crime Analysis : Practioner’s Recipe for Success**. Washington D.C. : Police Executive Research Forum

McCormack Robert J. and Savona Emesto U. *“Crime and Technology: New Frontier For Regulation, Law Enforcement and Research”* **International Journal of Police Science & Management.** Summer 2005, Vol. 7. pp. 137 – 142.

Miller, J. (2002, February 4). *Pennsylvania, FBI Shares Crime Data.* **Government Computing News**, 21, No. 3. Last retrieved June 3, 2004,

N.A.N.M. van Eijk, “(G)een recht op vertrouwelijke communicatie: P.B. Hugenholtz, “Het auteursrecht, het internet en de informatiesnelweg”,**Nederlands Juristenblad 1995/14**, pp. 513-519.

Rapport van de commissie computercriminaliteit, Informatietechniek en strafrecht, S.J.H. Gijrath, R. van den Hoven van Genderen, H. Wefers Bettink, **Intellectueel eigendom in digitaal perspectief,** Alphen aan den Rijn/Diegem 1996; P.B.

Reed, C. **Electronic Finance Law.** London: Woodhead-Faulkner, 1991.

Rodota, S. *"The Social Challenge o Information Technology: 1984 and Beyond." Colloque Ocde, Berlin, 1984 quoted in Stefano Rodota. "Protecting Information Privacy: Trend and Problems,"* In **Information Law Towards the 21th Century**, p. 37. Berlin: Colloque Ocde, 1992.

Rose Lance. **NetLaw : your rights in the online world**. California : Osborne McGraw - Hill c,1995.

Shri L. C. Amarnathan. "Crimes Related to Computer Network : Scope and underlying Issues : From New Economic Order to New Information Order, " in Crimes Related to the Computer Network. Tokyo : Japan , 2000.

Thomas J. Smedinghoff. **Online law : the SPA' s legal guide to doing business on the Internet** California : Addison - Westley Publishing Company , Inc,1996

T.Sohiano. **Cyber Law :Text and Cases.** Ohio : South Western College Publishing,2000

Ulrich Sieber. **Legal Aspects of Computer - Related Crime in the Information Society COMCRIME-STUDY-** Vol 1. version 1,1998.

UNAFEI . **Crimes Related to the Computer Network Challenges of the Twenty- First Century .**Tokyo : Japan ,2000.

U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. 2002**. Mission possible: Strong governance for the integration of justice information systems.** Washington, D.C.: U.S. Government Printing Office.

William Stallings. **Data and Computer Communications.** 5th New Jersy :Prentice - Hall,inc,1997.

Wright, Benjamin, and Jane L, Winn., **The Law of Electronic Commerce.** New York: Aspen Law & Business, 1957.

W.E. Scherpenhuijsen, Visie op versnellen, M&I Partners, Amersfoort 1995**and Diensten en infrastructuren voor elektronische snelwegen in Nederland,** M&I Partners,

Articles

Adams, Jo - Ann M. *CONTROLLING CYBERSPACE : APPLYING THE COMPUTER FRAUD AND ABUSE ACT TO THE INTERNET.* **Santa Clara Computer and High Technology Law Journal**.404 (1996).

Andra J. *Computer Crime an emerging Challenge for Law Enforcement.*65 **FBI Law Enforcement Bulletin** (1996)

Carl Benson, Andrew V. Jablon, Paul J. Kaplan and Mara Rosenthal. *Computer Crime*.34 **American Criminal Law Review.** 409 (1997)

Carter, David L and Kantz, Andra J. *Computer Crime an emerging challenge for Law Enforcement.*65 **FBI Law Enforcement Bulletin** (1996)

Charney, Scott and Alexander, Kent. *Computer Crime.*45 **Emory Law Journal** 931(1996)

Conley,John M. and Bryan, Robert M. **A Survey of computer Crime Legislation in the United States**. 8 **Information & Communications Technology Law** 35 (1999)

Bakewell,Eric J.,Koldaro Michelle and Tjia, Jennifer M.. *Computer Crime.* **American Criminal Law Review** 38 (2000)

Goodman,Marc. *Making Computer Crime Count*. 70 **FBI Law Enforcement Bulletin** 10 (2001)

Goodman,Marc. *Why The Police Don't Care About Computer Related Crimes Be The Subject Of Specific legislative Attention?* 12 **Albany Law Journal of Science and Technology** 97

Hancock, Douglas H. *To What Extent Should Computer Related Crimes Be The Subject Of Specific legislative Attention?*12 **Albany Law Journal of Science and Technology** 97 (2001).

Heymann, Stephen P. *Legislative Computer Crime.* 34 **Harvard Journal on Legislation** 373 (1997).

Kelly J. Harris. *"Justice System Integration : On the Threshold of a New Era"* **Correction Today** July 1999. pp. 72-76.

Katz, R**. Billion on net by 2005**. 5 The Australian by Australian Centre for Policing Research. " E- crime : A Global Challenge for Law *Offenses and Computer Crime.*41 **Boston Journal** 8 (1997)

Lawyer, Nevada. *10 HIGH TECH CRIMES TASK FORCE.* 5 **Nevada Lawyer** 10 (1997)

Litt, Robert S.*CRIME IN THE COMPUTER AGE : THE LAW ENFORCEMENT PERSPECTIVE.* 4 **Texas Review of Law and Politics** 59 (1999)

Loundy, David J. *E-Law : Legal Issues Affecting Computer Information Systems And Systems Operator Liabillity 3* **Albanny Law Journal of Science and Technology** 79 (1993).

Mascarino, George J. and Shumaker, Michael R. *CHANGING TIMES CHANGING CRIMES: THE CRIMINAL'S NEWEST WEAPON AND THE U.S.'S RESPONSE*. 16 **Dickinson Journal of intentional Law** 597 (1998).

Nemerofsky, Jeff. *The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of it ?* 6 **Richmond Journal of Law & Technology** 23 (2000)

R.Heffernan, *Securing Proprietary Information Committee of the American Society of Industrial Security* , **Committee presentation at the ASIS Annual Meeting**, New Orleens, LA September 12,

1995 cited by Carter, Daid Land Kantz, Andra J. *Computer Crime an emerging challenge for Law Enforcement*.65 **FBI Law Enforcement Bulletin** 1 (1996).

Banham Russ.Hacking. CFO Mag. (2000) cited by Katyal, Neal Kumar. *Criminal law in Cyberspace.* 149 **University of Pennsylvania Law Review** 1003 (2001)

Tower,Julie A.*Note : Hacking Vermont's Computer Crimes Status* 25 **Vermont Law Review** 945 (2001).

เว็ปไซต์

http://www.co.hennepin.mn.us/vhn/portal/internet/hcdetailmaster/0,2300,1273_82696_10037700.html

http://www.gcn.com/21_3/statelocal/17867-1.html

http://www.search.org/courts/pdf_files/DE%20case%20 study.pdf

ภาคผนวก

ภาคผนวก 1
สรุปผลการประชุมเชิงปฏิบัติการ ครั้งที่ 1
เพื่อรับฟังความคิดเห็นเกี่ยวกับ
การเชื่อมต่อข้อมูล ปัญหาและอุปสรรคที่เกี่ยวข้อง

ผลสรุปการประชุมเชิงปฏิบัติการเพื่อรับฟังข้อเท็จจริง “การปรับปรุงระเบียบกฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม”

วันพุธที่ 27 ธันวาคม 2549 เวลา 9.00 น. – 14.00 น.

ณ ห้องยูงทอง โรงแรม ที เค พาเลซ กรุงเทพมหานคร

---

1. การบรรยายสรุปโดยที่ปรึกษาโครงการ

หัวหน้าโครงการได้บรรยายสรุปถึงการดำเนินการในด้านต่าง ๆ 2 ส่วน ดังนี้

ส่วนที่ 1 บทนำ ได้กล่าวถึง ที่มาและแนวทางการดำเนินการตามลำดับ ดังนี้

1. หลักการและเหตุผล
2. วัตถุประสงค์
3. เป้าหมาย
4. วิธีดำเนินการศึกษา
5. ผลที่คาดว่าจะได้รับ

ส่วนที่ 2 แนวคิดการบูรณาการและการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม เป็นการบรรยายให้รายละเอียด ตามลำดับดังนี้

1. การนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กร
2. ข้อมูลสารสนเทศในกระบวนการยุติธรรม
3. การคุ้มครองข้อมูล (Data Protection)
4. การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์
5. การบูรณาการข้อมูลด้านการบริหารงานยุติธรรม
6. เทคโนโลยีสารสนเทศและการบูรณาการข้อมูลด้านงานยุติธรรมของไทย

2. กำหนดการ

กำหนดการ
การประชุมเชิงปฏิบัติการ เรื่อง
“การปรับปรุงระเบียบกฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม”
วันพุธที่ 27 ธันวาคม 2549 เวลา 9.00 น. – 14.00 น.
ณ ห้องยูงทอง โรงแรม ที เค พาเลซ กรุงเทพมหานคร

8.30 – 9.00 น. : ลงทะเบียนและรับเอกสาร

9.00 – 9.20 น. : พิธีเปิดการประชุมฯ

9.20 – 10.15 น.: การบรรยายเรื่อง **“การปรับปรุงระเบียบกฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม”**

โดย นายฐนันดรศักดิ์ บวรนันทกุล หัวหน้าโครงการฯ

10.15 – 10.30 น.: รับประทานอาหารว่าง

10.30 – 12.00 น.: ประชุมสัมมนา อภิปราย และแลกเปลี่ยนความคิดเห็น

12.00 น. : ปิดการประชุม รับประทานอาหารกลางวันร่วมกัน

3. ผลสรุปการประชุมเชิงปฏิบัติการ

การประชุมเชิงปฏิบัติการ ครั้งที่ 1 มีผลสรุป ดังนี้

1. ปัจจุบัน หน่วยงานในกระบวนการยุติธรรมที่ใช้เทคโนโลยีสารสนเทศในการปฏิบัติงานมีทั้งสิ้น 14 หน่วยงาน ได้แก่ ศูนย์ข้อมูลข้อสนเทศ สำนักงานตำรวจแห่งชาติ กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติสำนักงานป้องกันและปราบปรามการฟอกเงินสำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด กรมสอบสวนคดีพิเศษสำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรมกรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน กรมบังคับคดี สถาบันนิติวิทยาศาสตร์ กรมคุ้มครองสิทธิและเสรีภาพ

2. การเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมของไทย การเชื่อมโยง ข้อมูลระหว่างหน่วยงานในกระบวนยุติธรรมและการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการดำเนินการ ซึ่งจากการศึกษาและการประมวลข้อมูลจากการสัมภาษณ์ จากการประชุมเชิงปฏิบัติการเพื่อรับฟังข้อมูล ข้อเท็จจริง ข้อมูลต่างๆ ที่เกี่ยวข้อง สามารถวิเคราะห์ได้ดังนี้

1. ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาติ

ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาติ ปัจจุบันเปลี่ยนชื่อเป็น“ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ ทำหน้าที่เป็นศูนย์กลางในการดำเนินการเกี่ยวกับการจัดเก็บข้อมูลต่างๆที่เกี่ยวข้องกับการปฏิบัติงานของตำรวจ เป็นหน่วยงานระดับกองบังคับการที่ทำหน้าที่เป็นหน่วย ด้านระบบเทคโนโลยีสารสนเทศของสำนักงานตำรวจแห่งชาติ ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาตินั้น ปัจจุบันมีฐานข้อมูลบางส่วนของกองทะเบียนประวัติอาชญากร (ทว.)บางส่วน ที่เก็บรักษาไว้ที่ศูนย์เทคโนโลยีกลาง สำนักงานตำรวจแห่งชาติ และมีข้อมูลด้านยาเสพติด รวมทั้งบุคคลที่ขึ้นทะเบียนเป็นบุคคลต้องห้าม (Block lists) เท่านั้น

ส่วนการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมอื่นๆยังไม่มี ไม่ว่าจะเป็นสำนักงานป้องกันและปราบปรามการทุจริตแห่งชาติ (ปปช.) สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)กรมสอบสวนคดีพิเศษ (DSI) สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม กรมราชทัณฑ์ กรมคุมประพฤติ กรมพินิจและคุ้มครองเด็กและเยาวชน กรมบังคับคดี สถาบันนิติวิทยาศาสตร์ กรมคุ้มครองสิทธิและเสรีภาพ เป็นต้น ซึ่ง

ศูนย์ข้อมูลสารสนเทศ สำนักงานตำรวจแห่งชาตินั้น ยังมีความต้องการเชื่อมโยงหรือบูรณาการข้อมูลอย่างยิ่ง กับหน่วยงานอื่นๆ ในกระบวนการยุติธรรม เพราะข้อมูลเหล่านั้นจะเป็นประโยชน์สำหรับการปฏิบัติงานของเจ้าหน้าที่ตำรวจทั้งในด้านการป้องกัน และปราบปรามอาชญากรรม ทั้งประเทศและสามารถนำไปใช้ในการจัดทำนโยบายและแผนของสำนักงานตำรวจแห่งชาติได้ ตามความมุ่งหมายของการจัดตั้งศูนย์ฯต่อไป

ปัญหาในการดำเนินการ คือ ขาดนโยบายที่ชัดเจนว่า ควรจะจัดเก็บข้อมูลอะไรบ้าง และขาดความต่อเนื่องในการดำเนินการ หน่วยงานนี้เป็นหน่วยงานทางด้านเทคนิค ซึ่งบทบาทความสำคัญทั้งในด้านบุคลากร งบประมาณและการดำเนินการ ยังอยู่ในขั้นเตรียมความพร้อมสำหรับความร่วมมือในการเชื่อมโยง หรือบูรณาการข้อมูลเทคโนโลยีสารสนเทศด้านงานยุติธรรมกับหน่วยงานอื่นๆ

2. กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ

กองทะเบียนประวัติอาชญากร หรือรู้จักกันในนาม “ทว.” เป็นหน่วยงานที่มีบทบาทสำคัญที่จะเก็บรวบรวมข้อมูลบุคคลที่ก่ออาชญากรรมที่เกี่ยวข้อง โดยเป็นข้อมูลจากการพิมพ์ลายนิ้วมือและลักษณะพฤติกรรมการประกอบอาชญากรรม ซึ่งข้อมูลที่จัดเก็บเป็นข้อมูลสำคัญที่หน่วยงานต่างๆในกระบวนการยุติธรรมจำเป็นจะต้องอาศัยประกอบการจัดทำสำนวนและการดำเนินคดี ซึ่งในการดำเนินการเก็บรวบรวมและประมวลข้อมูลนั้นอาศัยข้อมูลจากสถานีตำรวจต่างๆได้ดำเนินการจัดส่งมาเก็บไว้ มีการประมวลและจัดเก็บเป็นหมวดหมู่รวมทั้งจัดเก็บในฐานข้อมูลทางอิเลกโทรนิกส์

กองทะเบียนประวัติอาชญากร ได้มีการเชื่อมโยงข้อมูลกับหน่วยงานหลายหน่วยงาน คือ สำนักงานป้องกันและปราบปรามยาเสพติด (ปปส.) กรมราชทัณฑ์ กรมคุมประพฤติ เป็นหลัก ส่วนหน่วยงานอื่นๆในกระบวนการยุติธรรมยังไม่ได้มีการดำเนินการเชื่อมโยงข้อมูลแต่อย่างใด

สำหรับหน่วยงานที่กองทะเบียนประวัติอาชญากรต้องการที่จะเชื่อมโยงข้อมูลด้วยมากที่สุด คือ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม เนื่องจากต้องการทราบผลของการดำเนินคดี ซึ่งผลดังกล่าวจะเป็นประโยชน์ต่อกองทะเบียนประวัติอาชญากร ในแง่ของการปรับปรุงข้อมูลให้มีความทันสมัยและถูกต้อง

ปัญหาที่กองทะเบียนประวัติอาชญากร ประสบในด้านของการเชื่อมโยงข้อมูลก็คือความต้องการข้อมูลที่เป็นประโยชน์ในคดี แต่มีการจัดส่งทางโทรสาร (Fax) หรือ ทาง E-Mail

ซึ่งข้อมูลเหล่านี้ ศาลจะรับฟังเป็นพยานหลักฐาน (พยานเอกสาร) ได้หรือไม่อย่างไร ในทางคดีอาญา

ส่วนปัญหาทางกฎหมายที่เกี่ยวข้องก็คือ มีข้อมูลจำนวนมากที่กองทะเบียนประวัติอาชญากรจัดเก็บ และมีการดำเนินการเตรียมในระบบฐานข้อมูลเทคโนโลยีสารสนเทศแล้ว แต่ข้อมูลเหล่านั้น ยังต้องถือเป็นความลับส่วนบุคคลที่ไม่สามารถจัดส่งให้หน่วยงานอื่นๆได้ เนื่องจาก ข้อมูลของบุคคลเหล่านี้ (ยัง) เป็นข้อมูลเกี่ยวกับ “ผู้ต้องหา” ไม่ใช่จำเลย ซึ่งในกฎหมายแม่บท เช่น กฎหมายรัฐธรรมนูญกำหนดว่า ผู้ต้องหาหรือแม้จำเลยนั้น ต้องสันนิษฐานว่าเป็นผู้บริสุทธิ์อยู่ การเปิดเผยข้อมูลส่วนบุคคลอาจจะนำไปสู่การถูกฟ้องร้อง ตามประมวลกฎหมายอาญา มาตรา 157 และตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420, 423 เรื่องละเมิด และ หมิ่นประมาทได้

หากมีข้อตกลงระหว่างหน่วยงานในกระบวนการยุติธรรมชัดเจน ให้ถือเป็นการดำเนินการที่ชัดเจน ก็อาจเป็นข้อยกเว้นได้ และทางกองทะเบียนประวัติอาชญากรก็ได้มีการเตรียมดำเนินการปรับปรุงระเบียบการใช้ข้อมูลดังกล่าว แต่อยู่ในระหว่างการดำเนินการอยู่ อย่างไรก็ตามในส่วนของบุคลากรผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูล ยังมีความกังวลในเรื่องของการเชื่อมโยงข้อมูล เพราะนั่นหมายความว่า ข้อมูลที่อยู่ในครอบครองและถูกเก็บไว้ จะถูกใช้โดยหน่วยงานอื่นๆซึ่งหากไม่มีกฎหมายมารองรับให้เกิดความชัดเจน เกรงว่าจะถูกฟ้องร้องดำเนินคดีได้ เพราะการจัดเก็บข้อมูล เป็นการจัดเก็บตามที่กฎหมายให้อำนาจ แต่การใช้ข้อมูลยังมีความไม่ชัดเจนหากมีบุคคลหรือหน่วยงานอื่นๆเอาไปใช้

กองทะเบียนประวัติอาชญากรมุ่งที่จะเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรมในลักษณะที่เป็นทั้งผู้ให้และเป็นทั้งผู้ใช้ แต่ก็อยากที่จะเริ่มการเชื่อมโยงข้อมูลกับหน่วยงานที่จำเป็น และมีระบบข้อมูลคล้ายคลึงกันก่อน จากนั้น หากมีการดำเนินการที่ได้ผลจึงจะค่อยๆขยายออกไปกับหน่วยงานอื่นๆสร้างระบบโดยเฉพาะกับกรมราชทัณฑ์ หรือสถาบันนิติวิทยาศาสตร์ เป็นต้น ข้อมูลเกี่ยวกับการกระทำผิดซ้ำ เป็นข้อมูลสำคัญ เพราะหากมีการพัฒนาและเชื่อมโยงฐานข้อมูลจากการกระทำผิดซ้ำแล้ว หน่วยงานอื่นๆจะสามารถนำไปใช้ประโยชน์ได้อย่างมากมาย และหน่วยงานที่เคยติดต่อประสานกันในสำนักงานตำรวจแห่งชาติ คือ สำนักงานตรวจคนเข้าเมือง (ตม.) ซึ่งตม.เองก็เชื่อมโยงข้อมูลกับสำนักงาน ปปส.อยู่แล้ว หากร่วมมือกันก็จะขยายเครือข่ายไปได้ หรือ หน่วยงานนอกกระบวนการยุติธรรม เช่น กระทรวงต่างประเทศ ก็เป็นหน่วยงานที่หากมีการเชื่อมโยงข้อมูลด้วยกันแล้วจะเป็นประโยชน์อย่างยิ่งในการปฏิบัติงาน

3. กรมพินิจและคุ้มครองเด็กและเยาวชน

กรมพินิจและคุ้มครองเด็กและเยาวชน เป็นหน่วยงานระดับกรมสังกัดกระทรวงยุติธรรม มีบทบาทมีอำนาจหน้าที่พิทักษ์และคุ้มครองสิทธิเด็กและเยาวชนที่กระทำความผิด ส่งเสริมความมั่นคงของสถาบันครอบครัวและชุมชนโดยใช้กระบวนการยุติธรรมทางเลือก กระบวนการยุติธรรมเชิงสมานฉันท์ การหันเหคดีออกจากกระบวนการยุติธรรม และมาตรการอื่นๆ ดำเนินการด้าน คดีอาญา คดีครอบครัว กำกับการปกครองและการบำบัดแก้ไข ฟื้นฟู ป้องกัน พัฒนาและสงเคราะห์ ตลอดจนการติดตามประเมินผลเด็กและเยาวชน ประสานความร่วมมือและสร้างเครือข่ายกับชุมชน องค์กรภาครัฐและเอกชนทั้งภายในและต่างประเทศ เพื่อการมีส่วนร่วมและสนับสนุนกระบวนการยุติธรรมสำหรับเด็กและเยาวชน ศึกษา วิเคราะห์ วิจัย และพัฒนากฎหมาย การพิทักษ์คุ้มครองสิทธิเด็กและเยาวชน รวมทั้งระบบ รูปแบบ และวิธีการปฏิบัติเกี่ยวกับงานคดีและการปฏิบัติต่อเด็กและเยาวชนและพัฒนาบุคลากรและระบบการบริหารจัดการให้เข้าสู่มาตรฐานการบริหารจัดการภาครัฐ

ในด้านการเชื่อมโยงข้อมูลระหว่างงานในกระบวนการยุติธรรม และการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการดำเนินการนั้น มีการเชื่อมโยงเพียง 4 หน่วยงาน คือ

1. กองทะเบียนประวัติอาชญากร (ทว.) สำนักงานตำรวจแห่งชาติ ในด้านการตรวจสอบประวัติและการดำเนินการ เรื่อง การลบทะเบียนประวัติอาชญากรของเด็กและเยาวชนที่กระทำผิดหรือถูกดำเนินการในกระบวนการยุติธรรมออกจากฐานข้อมูลประวัติอาชญากร

2. สำนักงานยุติธรรม การดำเนินการเป็นการใช้ฐานข้อมูลด้านการดำเนินคดี ผลคำพิพากษาของสำนักงานศาลยุติธรรม เพื่อดำเนินการในส่วนของกรมพินิจและคุ้มครองเด็กและเยาวชน อย่างไรก็ตาม ในปัจจุบัน ยังเป็นเพียงแค่ด้านการตรวจสอบเฉพาะราย ไม่สามารถดำเนินการตรวจสอบ โดยใช้ฐานข้อมูลด้านสารสนเทศ

3. กรมราชทัณฑ์ กรมพินิจและคุ้มครองเด็กและเยาวชน ใช้ฐานข้อมูลด้านผลการดำเนินการหลังคำพิพากษา ในกรณีที่เกี่ยวข้องกับเด็กและเยาวชนที่ศาลมีคำพิพากษาให้ไปอยู่ในความดูแลของกรมราชทัณฑ์

4. กรมคุมประพฤติ ในส่วนที่เกี่ยวข้องเป็นการที่กรมพินิจและคุ้มครองเด็กและเยาวชน ใช้ฐานข้อมูลด้านผลการคุมประพฤติ ในกรณีที่ผู้กระทำความผิดเป็นเด็ก หรือเยาวชนเพื่อนำผลไปประกอบการดำเนินงานด้านการสืบเสาะ ข้อเท็จจริง ของเด็กและเยาวชนที่ถูกจับกุมดำเนินคดีในชั้นสถานพินิจ

4. กรมราชทัณฑ์

กรมราชทัณฑ์มีอำนาจหน้าที่ปฏิบัติต่อผู้กระทำผิดให้เป็นไปตามคำพิพากษาหรือคำสั่งตามกฎหมายโดยดำเนินการตามกฎหมายว่าด้วยการราชทัณฑ์และกฎหมายอื่นที่เกี่ยวข้อง กำหนดแนวทางปฏิบัติต่อผู้ต้องขังให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ นโยบายของกระทรวง หลักอาชญาวิทยา และหลักทัณฑวิทยา ตลอดจนข้อกำหนดมาตรฐานขั้นต่ำสำหรับปฏิบัติต่อผู้ต้องขังและข้อเสนอแนะในเรื่องที่เกี่ยวข้องขององค์การสหประชาชาติ ดำเนินการเกี่ยวกับการสวัสดิการและการสงเคราะห์แก่ผู้ต้องขัง จัดทำและประสานแผนงานของกรมให้เป็นไปตามนโยบายและแผนแม่บทของกระทรวง รวมทั้งกำกับ เร่งรัด ติดตาม และประเมินผลการปฏิบัติงานตามแผนงานของหน่วยงานในสังกัดกรม

กรมราชทัณฑ์ได้มีการเชื่อมโยงระบบเพื่อการสืบค้นข้อมูล 13 หลัก กับศูนย์ทะเบียนราษฎรฯนอกจากนี้ยังมีการเชื่อมโยงและดำเนินการตามแผนแม่บทเทคโนโลยีสารสนเทศ กระทรวงยุติธรรม

ในส่วนของการใช้เทคโนโลยีสารสนเทศของหน่วยงานนั้น กรมราชทัณฑ์ ไม่ได้ขาดนโยบายที่ชัดเจนในการแลกเปลี่ยนข้อมูลของหน่วยงานในกระบวนการยุติธรรม กรมราชทัณฑ์มีการจัดทำและมีนโยบายในด้านการใช้เทคโนโลยีสารสนเทศที่ชัดเจน แต่ขาดการดำเนินการอย่างจริงจังและต่อเนื่องประกอบกับการเปลี่ยนแปลงรัฐบาลที่ทำให้การพัฒนากระบวนการยุติธรรมของประเทศดำเนินไปอย่างล่าช้า ซึ่งก็ส่งผลกระทบต่อการใช้เทคโนโลยีสารสนเทศด้วย และเห็นด้วยว่า ในการดำเนินการยังขาดหน่วยงานที่เป็นเจ้าภาพหลัก ในหน่วยงานที่จะทำหน้าที่รับและส่งต่อเพื่อให้หน่วยงานด้านเทคโนโลยีสารสนเทศทำการประมวลผล หากมีหน่วยงานที่เป็นเจ้าภาพหลักในการบูรณาการข้อมูลจะช่วยประสานงานให้หน่วยงานของแต่ละหน่วยงานมีข้อมูลที่ถูกต้อง เหมาะสม และทันเวลา

การดำเนินการบูรณาการข้อมูลในกระบวนการยุติธรรมนั้น จำเป็นอย่างยิ่งที่ผู้บริหารระดับสูงต้องให้ความสำคัญอย่างยิ่ง ในขณะที่ ปัญหาด้านงบประมาณก็มีส่วนสำคัญทั้ง ๆที่รู้และเข้าใจในบทบาทงานด้านเทคโนโลยีสารสนเทศแต่การต้องใช้งบประมาณที่สูง และงานด้านเทคโนโลยีสารสนเทศยังไม่ใช่งานหลักของหน่วยงาน เป็นภาระงานที่ยังรองได้ อันส่งผลกระทบต่อเนื่องที่ทำให้ขาดความพร้อมทางด้านอุปกรณ์ต่าง ๆของทุกหน่วยงานในกระบวนการยุติธรรม มากน้อยแตกต่างกันไป ประกอบกันปัญหาการขาดแคลนบุคลากรที่มีความรู้เฉพาะด้าน เนื่องจาก การเปลี่ยนแปลงเทคโนโลยีที่รวดเร็ว และบุคลากรที่เก่งจริง ก็ไปอยู่ในภาคเอกชน

ส่วนด้านปัญหาการเก็บรวบรวมข้อมูลที่มีความซับซ้อนนั้น ปัญหานี้มีสาเหตุจากการที่แต่ละหน่วยงานจะจัดเก็บกันเอง โดยมิได้มีการประสานการจัดเก็บข้อมูลร่วมกัน ต่างฝ่ายต่างจัดเก็บ ก็ส่งผลให้ข้อมูลบางส่วนขาดความสมบูรณ์และรวบรวมยาก เพราะยังขาดรูปแบบที่เป็นมาตรฐานในการจัดเก็บ ส่งผลตามมาทำให้ข้อมูลมีความน่าเชื่อถือน้อย เพราะมีข้อมูลจำนวนมากที่ขาดการปรับปรุง เปลี่ยนแปลง ข้อมูลให้เป็นปัจจุบัน จัดเก็บแล้วก็ขาดการเรียกมาตรวจสอบดูความถูกต้องในปัจจุบัน

ด้านการคุ้มครองข้อมูลก็เป็นสิ่งที่จำเป็นเพราะถือว่าข้อมูลของบุคคลที่เป็นความลับส่วนบุคคล เป็นสิ่งที่เป็นผลเสียได้สำหรับบุคคลนั้น การเคารพสิทธิ์ในข้อมูลส่วนบุคคลจึงต้องมีอยู่และให้การคุ้มครอง

ปัญหาหลักอื่นๆก็คือ การขาดความตั้งใจและขาดความมุ่งมั่นในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลโดยการใช้เทคโนโลยีสารสนเทศ ซึ่งก็ส่งผลให้หลายๆหน่วยงานจึงขาดความพร้อม เพื่อการบูรณาการ

กรมราชทัณฑ์มีความคาดหวังว่า สำหรับฐานข้อมูลของกรมราชทัณฑ์นั้นอย่างน้อยก็จะต้องมีข้อมูล หรือ ประวัติผู้ต้องขัง ในปีพ.ศ. 2545 กรมราชทัณฑ์ได้มอบหมายให้จุฬาลงกรณ์มหาวิทยาลัย และสถาบันเทคโนโลยีพระจอมเกล้าฯ ทำการวิเคราะห์ระบบงานเพื่อสามารถที่จะเชื่อมโยงข้อมูลเข้าออกได้ ซึ่งกรมราชทัณฑ์เตรียมความพร้อมในด้านการบูรณาการไว้ว่าจะต้องมีข้อมูล โดยเฉพาะเรื่องลายนิ้วมือ เนื่องจากในข้อมูลบางอย่าง เช่น หมายศาลไม่มีเลข 13 หลัก การมีการทำ Finger Print ที่เก็บรวบรวมข้อมูลได้ถึง 2 แสนคน และสามารถเรียกใช้ข้อมูลได้โดยระบบ real time

ในการเชื่อมโยงข้อมูลนั้นกรมราชทัณฑ์ ได้ลงนามความร่วมมือ (MOU) กับหน่วยงานด้านกระบวนการยุติธรรมในจังหวัดนนทบุรี เป็นโครงการนำร่อง และถือเป็นขั้นแรก (Phase I) ในขณะเดียวกันก็มีการจัดทำ DXC โดยมาตั้ง Brokerที่กรมราชทัณฑ์

ด้านกฎหมายและระเบียบที่เกี่ยวข้องนั้น ในตัวกฎหมาย คือ พระราชบัญญัติราชทัณฑ์ พ.ศ.2479 เอง ไม่ได้มีการระบุถึงการเชื่อมโยงข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมแต่เน้นที่การบริหารจัดการ และสิทธิของผู้ต้องขัง กฎหมายที่ใช้ก็จะเป็นพระราชบัญญัติข้อมูลข่าวสาร พ.ศ. 2540

ปัญหาอื่นๆก็คือ ปัญหาด้านงบประมาณ ซึ่งรัฐบาลไม่จัดให้ กรมราชทัณฑ์ต้องจัดเจียดมาดำเนินการเอง ซึ่งในส่วนนี้ก็ต้องขึ้นกับผู้บริหารกรมราชทัณฑ์ว่าจะมีการดำเนินการและนโยบายอย่างไร

5. กรมบังคับคดี

มีอำนาจหน้าที่ดำเนินการยึดทรัพย์สิน อายัดทรัพย์สิน จำหน่ายทรัพย์สิน บังคับคดีล้มละลายบุคคลธรรมดาตามคำสั่งศาล บังคับคดีล้มละลายนิติบุคคล บังคับคดีล้มละลายกิจการพิเศษ บังคับคดีฟื้นฟูกิจการของลูกหนี้ ชำระบัญชีห้างหุ้นส่วนบริษัทหรือนิติบุคคลในฐานะผู้ชำระบัญชี ตาม คำสั่งศาล รับวางทรัพย์จากลูกหนี้หรือผู้มีสิทธิวางทรัพย์ ดำเนินการประเมินราคาทรัพย์ ดำเนินการตรวจสอบสิทธิทางบัญชีของผู้มีส่วนได้เสียเพื่อรับส่วนแบ่งจากคดี ตรวจสอบค่าใช้จ่ายและเรียกเก็บค่าธรรมเนียมการบังคับคดี

6. กรมคุ้มครองสิทธิและเสรีภาพ

มีอำนาจหน้าที่จัดระบบการบริหารจัดการด้านคุ้มครองสิทธิและเสรีภาพของประชาชน ดำเนินการและส่งเสริมการคุ้มครองสิทธิและเสรีภาพของประชาชน การระงับข้อพิพาทในสังคม ส่งเสริม พัฒนา และประสานงานกับภาครัฐและภาคเอกชนทั้งในและต่างประเทศ จัดทำระบบมาตรการและดำเนินการช่วยเหลือประชาชนที่ตกเป็นเหยื่ออาชญากรรม รวมทั้งจำเลยที่ถูกดำเนินคดีอาญาโดยมิได้เป็นผู้กระทำความผิดตามกฎหมายว่าด้วยค่าตอบแทนผู้เสียหายและค่าทดแทนและค่าใช้จ่ายแก่จำเลยในคดีอาญา ส่งเสริมและศึกษาวิจัยเพื่อการพัฒนาในด้านการคุ้มครองสิทธิและเสรีภาพ ติดตามและประเมินผลการดำเนินการด้านการคุ้มครองสิทธิและเสรีภาพ ปรับปรุงและแก้ไขกฎหมาย กฎ หรือข้อบังคับในด้านการคุ้มครองสิทธิและเสรีภาพ ส่งเสริม ดำเนินการและปฏิบัติการตามแผนปฏิบัติการด้านสิทธิมนุษยชน และดำเนินการคุ้มครองพยานตามกฎหมายว่าด้วยการคุ้มครองพยานในคดีอาญา

ในการเชื่อมโยงข้อมูลในส่วนของกรมคุ้มครองสิทธิและเสรีภาพนั้น เนื่องจากเป็นหน่วยงานใหม่ การเชื่อมโยงข้อมูลในหน่วยงานด้านกระบวนการยุติธรรม ยังไม่ได้เกิดขึ้นชัดเจน แต่ก็มีการเตรียมการเพื่อรองรับตามแผนแม่บทเทคโนโลยี กระทรวงยุติธรรม ส่วนที่มีการเชื่อมโยงก็จะเป็นสำนักงานทะเบียนราษฎร์ เพื่อดำเนินการตรวจสอบและค้นหาข้อมูลในการดำเนินการด้านการจ่ายค่าทดแทน และการคุ้มครองพยาน ซึ่งหน่วยงานในกระบวนการยุติธรรมที่อยากจะเชื่อมโยงเร็วที่สุดก็คือ สำนักงานศาลยุติธรรม เพราะจะสะดวกต่อการปฏิบัติงาน ในความต้องการแล้ว ประสงค์อยากจะเชื่อมกับทุกหน่วยงานในกระบวนการยุติธรรม และนอกหน่วยงานในกระทรวงยุติธรรม เช่น สำนักงานผู้ตรวจการแผ่นดินรัฐสภา

เพราะภาระงานของกรมเชื่อมโยงกัน และภาระงานก็หลากหลายมากในการที่จะต้องประสานข้อมูลกับหน่วยงานอื่นๆให้มากที่สุดเท่าที่จะทำได้ โดยเฉพาะด้านสิทธิมนุษยชน และด้านของผู้เสียหายซึ่งเป็นข้อมูลที่สำนักงานตำรวจแห่งชาติ มีการจัดทำทะเบียนประวัติอาชญากร แต่ทะเบียนประวัติผู้เสียหาย ยังไม่ได้มีการดำเนินการอย่างเป็นระบบแต่อย่างใด กรมคุ้มครองสิทธิและเสรีภาพ เนื่องจากเป็นหน่วยงานใหม่ในกระทรวงยุติธรรม ดังนั้น การเชื่อมโยงข้อมูลในด้านงานยุติธรรมจะดำเนินการตามแผนแม่บทกระทรวงยุติธรรม และจะพยายามพัฒนาฐานข้อมูลของตนเอง ปัจจุบันมีข้อมูลบางส่วนที่เกิดจากการปฏิบัติงานแต่ยังไม่ได้จัดทำฐานเพื่อเชื่อมโยงข้อมูล

7. สถาบันนิติวิทยาศาสตร์

มีอำนาจหน้าที่รับผิดชอบงานธุรการของคณะกรรมการมาตรฐานงานด้านนิติวิทยาศาสตร์ และคณะกรรมการบริหารกิจการด้านนิติวิทยาศาสตร์ รวมทั้งศึกษา รวบรวม และวิเคราะห์ข้อมูลต่าง ๆ ที่เกี่ยวกับงานของคณะกรรมการทั้งสองคณะ แต่งตั้งและเพิกถอนการแต่งตั้งรวมทั้งกำกับดูแลการปฏิบัติหน้าที่ของผู้ช่วยผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์ให้เป็นไปตามหลักเกณฑ์ มาตรฐาน และจรรยาบรรณ รับเรื่องราวร้องทุกข์จากบุคคลซึ่งได้รับความเสียหายจากการประพฤติผิดหลักเกณฑ์ มาตรฐาน หรือจรรยาบรรณของผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์ ดำเนินการขอรับการสนับสนุนด้านงบประมาณเพื่อเป็นค่าตอบแทนการปฏิบัติงานของผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์ที่ได้รับการแต่งตั้ง รวมทั้งเพื่อเป็นเงินสนับสนุนสถานพยาบาลหรือสถานที่ที่คณะกรรมการมาตรฐานงานด้านนิติวิทยาศาสตร์กำหนดให้เป็นสถานปฏิบัติการ ปฏิบัติงานและให้บริการด้านนิติวิทยาศาสตร์โดยดำเนินการเองหรือร่วมมือกับส่วนราชการหรือหน่วยงานของรัฐ เพื่อขอรับการสนับสนุนด้าน สถานที่ เครื่องมือ หรือบุคลากรด้านนิติวิทยาศาสตร์

ช่วยเหลือและให้คำแนะนำเกี่ยวกับการปฏิบัติงานด้านนิติวิทยาศาสตร์ของส่วนราชการหรือหน่วยงานอื่นของรัฐ เผยแพร่ความรู้ ฝึกอบรม และพัฒนาบุคลากรด้านนิติวิทยาศาสตร์ สนับสนุนการศึกษาวิจัยหรือทำการศึกษาวิจัยเกี่ยวกับนิติวิทยาศาสตร์ร่วมกับส่วนราชการ หน่วยงานของรัฐ หรือองค์กรอื่น ประสานงานและกำกับดูแลให้ส่วนราชการหรือหน่วยงานของรัฐที่ดำเนินงานด้านนิติวิทยาศาสตร์ปฏิบัติให้เป็นไปตามระเบียบ หลักเกณฑ์ และมาตรฐานการปฏิบัติงานด้านนิติวิทยาศาสตร์ และปฏิบัติงานด้านการพิสูจน์บุคคลสูญหาย

ในส่วนของการเชื่อมโยงข้อมูลของสถาบันนิติวิทยาศาสตร์กับหน่วยงานอื่นๆในกระบวนการยุติธรรมนั้น สถาบันนิติวิทยาศาสตร์ มีการจัดทำโครงการพัฒนาด้านเทคโนโลยีสารสนเทศ เพื่อรองรับการปฏิบัติงาน และการดำเนินการตามแผนแม่บทเทคโนโลยีสารสนเทศใน

กระบวนการยุติธรรม โดยเฉพาะอย่างยิ่ง เพื่อให้สอดรับกับการดำเนินการจัดตั้งและพัฒนาศูนย์บุคคลสูญหาย เนื่องจากสถาบันนิติวิทยาศาสตร์นั้น เป็นหน่วยงานที่มีบทบาทในด้านข้อมูลเกี่ยวกับวัตถุพยาน ซึ่งผลการตรวจห้องปฏิบัติการจะส่งผลต่อคดี หน่วยงานของสถาบันติวิทยาศาสตร์จึงประสงค์จะให้ระบบฐานข้อมูลเป็นระบบปิด ซึ่งการจะเชื่อมโยงข้อมูลได้มากน้อยเพียงใด ก็ขึ้นอยู่กับผู้บริหารเป็นหลัก

ด้านกฎหมายและกฎระเบียบที่เกี่ยวข้องนั้น สถาบันนิติวิทยาศาสตร์ไม่ได้มีการจัดทำขึ้นโดยเฉพาะ กฎหมายที่ใช้ก็จะมีกฎหมายแม่ คือ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ.2540 เป็นหลัก ควบคู่กับการใช้ดุลพินิจของผู้บริหารของสถาบันในการให้ข้อมูล

8. กรมสอบสวนคดีพิเศษ

มีอำนาจหน้าที่รับผิดชอบในงานธุรการของคณะกรรมการคดีพิเศษ คณะอนุกรรมการที่แต่งตั้งโดยคณะกรรมการคดีพิเศษ และคณะกรรมการที่ปรึกษาการบริหารงานบุคคลพนักงานสอบสวนคดีพิเศษ ป้องกัน ปราบปราม สืบสวน และสอบสวนคดีพิเศษตามกฎหมายและตามหลักเกณฑ์ที่คณะกรรมการคดีพิเศษประกาศ กำหนด หรือตามมติของคณะกรรมการคดีพิเศษ ศึกษารวบรวมและวิเคราะห์ข้อมูลเพื่อประโยชน์แก่การปฏิบัติหน้าที่ของคณะกรรมการ คดีพิเศษ จัดให้มีการศึกษาอบรมเพื่อพัฒนาระบบงานการสืบสวนและสอบสวน พัฒนาความรู้และประเมินสมรรถภาพการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษ เจ้าหน้าที่คดีพิเศษ และข้าราชการกรมสอบสวนคดีพิเศษ ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและตามกฎหมายอื่นอันเกี่ยวกับความผิดทางอาญาที่เป็นคดีพิเศษ และดำเนินการเกี่ยวกับงานกฎหมายและระเบียบในความรับผิดชอบของกรมและกฎหมายอื่นที่เกี่ยวข้อง

9. กรมคุมประพฤติ

มีอำนาจหน้าที่ดำเนินการสืบเสาะและพินิจ ควบคุมและสอดส่อง แก้ไขฟื้นฟูและสงเคราะห์ผู้กระทำผิดในชั้นก่อนฟ้อง ชั้นพิจารณาคดีของศาล และภายหลังที่ศาลมีคำพิพากษาตามที่กฎหมายกำหนด ดำเนินการฟื้นฟูสมรรถภาพผู้ติดยาเสพติดในระบบบังคับรักษาตามกฎหมายว่าด้วยการฟื้นฟูสมรรถภาพผู้ติดยาเสพติด ส่งเสริมสนับสนุนเกี่ยวกับการดำเนินการแก้ไขฟื้นฟูและสงเคราะห์ผู้กระทำผิดในชุมชน พัฒนาระบบ รูปแบบ และวิธีการปฏิบัติต่อผู้กระทำผิดในชุมชน จัดทำและประสานแผนงานของกรมให้สอดคล้องกับนโยบายและแผนแม่บทของกระทรวง เร่งรัด ติดตามและประเมินผลการปฏิบัติงานของหน่วยงานในสังกัด เสริมสร้างสนับสนุนและประสานงานให้ภาคประชาสังคมเข้ามามีส่วนร่วมในการปฏิบัติต่อผู้กระทำผิด และป้องกันสังคมจากอาชญากรรม รวมทั้งให้สามารถรวมเป็นเครือข่ายเพื่อดำเนินภารกิจดังกล่าว

10. สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด

เป็นส่วนราชการที่อยู่ในบังคับบัญชาขึ้นตรงต่อรัฐมนตรี มีอำนาจหน้าที่ดำเนินการตามกฎหมายว่าด้วยการป้องกันและปราบปรามยาเสพติดกฎหมายว่าด้วยมาตรการในการปราบปรามผู้กระทำความผิดเกี่ยวกับยาเสพติด และกฎหมายอื่น ๆ ที่เกี่ยวเนื่องกับการป้องกันและปราบปรามยาเสพติด หรือการแก้ไขปัญหาเกี่ยวกับยาเสพติด ดำเนินการเกี่ยวกับงานเลขานุการของคณะกรรมการป้องกันและปราบปรามยาเสพติดและคณะกรรมการตรวจสอบทรัพย์สิน รวมทั้งงานเลขานุการของคณะกรรมการที่ปรึกษา และคณะอนุกรรมการที่คณะกรรมการป้องกันและปราบปรามยาเสพติดแต่งตั้ง หรือคณะอนุกรรมการที่คณะกรรมการตรวจสอบทรัพย์สินแต่งตั้ง ประเมินสถานการณ์การดำเนินงานและให้ข้อเสนอแนะด้านนโยบายยุทธศาสตร์ แผนและงบประมาณในการดำเนินงานด้านป้องกันและแก้ไขปัญหายาเสพติด อำนวยการ เร่งรัด กำกับ ติดตามการดำเนินงานด้านป้องกันและแก้ไขปัญหายาเสพติดให้เป็นตามนโยบาย แผนและงบประมาณ ให้ข้อเสนอแนะด้านยุทธศาสตร์และประสานความร่วมมือกับต่างประเทศด้านยาเสพติด พัฒนาและสนับสนุนวิชาการด้านการป้องกันและแก้ไขปัญหายาเสพติดแก่หน่วยงานทั้งภาครัฐและเอกชน ส่งเสริมและสนับสนุนด้านพัฒนาองค์กร ทรัพยากร บุคลากร ข้อมูลสารสนเทศ กฎหมาย และระเบียบที่เกี่ยวข้องกับการป้องกันและแก้ไขปัญหายาเสพติด ปฏิบัติงานด้านการรณรงค์และประชาสัมพันธ์ต่อต้านยาเสพติด

ในทางปฏิบัติสำนักงาน ปปส. เป็นทั้งผู้ให้ข้อมูลและผู้รับข้อมูล โดยหน่วยงานในกระบวนการยุติธรรมที่ได้มีการเชื่อมโยงข้อมูลแล้ว ได้แก่ สำนักงานคณะกรรมการป้องกันการฟอกเงิน (ปปง.) กรมสอบสวนคดีพิเศษ (DSI) ในขณะที่บางหน่วยงานยังไม่มีการเชื่อมต่ออีกหลายหน่วยงาน

สำนักงาน ปปส. มีการจัดทำฐานข้อมูลด้านยาเสพติดมาตั้งแต่ปี พ.ศ. 2506 แต่เป็นระบบปิดมีการกำหนดระบบรักษาความปลอดภัย ต่อมาก็มีการปรับเปลี่ยนเป็นระบบเปิดแต่ก็ยังมีระบบการรักษาความปลอดภัยของข้อมูลที่เข้มข้น มีการสอบถามหน่วยงานที่ใช้ข้อมูลทุก ๆ 6 เดือน เพื่อตรวจสอบผู้ที่ใช้ ในการดำเนินการโดยเฉพาะด้านทะเบียนยาเสพติด มีการนำเข้าข้อมูลเข้าฐานเอง หน่วยงานที่ประสานงานใกล้ชิด ได้แก่ สำนักงานตรวจคนเข้าเมือง สำนักงานตำรวจแห่งชาติ และกองทะเบียนประวัติอาชญากร ในการพัฒนาระบบใหม่ ๆ ควรต้องมีการสำรวจและดูความต้องการของหน่วยงานและข้อมูลเพื่อสามารถดำเนินการเชื่อมโยงได้อย่างเหมาะสม ตลอดรวมทั้งกรมคุมประพฤติ

11. สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน

เป็นส่วนราชการที่ไม่สังกัดสำนักนายกรัฐมนตรี กระทรวง หรือทบวง อยู่ในบังคับบัญชาของรัฐมนตรีว่าการกระทรวงยุติธรรม มีอำนาจหน้าที่ดำเนินการให้เป็นไปตามมติของคณะกรรมการป้องกันและปราบปรามการฟอกเงินและคณะกรรมการธุรกรรมตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และปฏิบัติงานธุรการอื่น ดำเนินการรับรายงานการทำธุรกรรมและแจ้งการตอบรับรายงานตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน เก็บรวบรวม ติดตาม ตรวจสอบ ศึกษา และวิเคราะห์รายงานและข้อมูลต่าง ๆ เกี่ยวกับการทำธุรกรรม เก็บรวบรวมพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิดตามกฎหมายว่าด้วยการ ป้องกันและปราบปรามการฟอกเงิน ดำเนินการจัดให้มีโครงการที่เกี่ยวกับการเผยแพร่ความรู้ การให้การศึกษาและฝึกอบรมในด้านต่าง ๆ ที่เกี่ยวกับการดำเนินการตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน หรือช่วยเหลือหรือสนับสนุนทั้งภาครัฐและภาคเอกชนให้มีการจัดโครงการดังกล่าวขึ้น ดำเนินการเกี่ยวกับงานเลขานุการของคณะกรรมการป้องกันและปราบปรามการฟอกเงินและคณะกรรมการธุรกรรม รวมทั้งงานเลขานุการของคณะอนุกรรมการที่คณะกรรมการป้องกันและปราบปรามการฟอกเงินแต่งตั้ง

สำนักงานคณะกรรมการ ปปง.ได้ประสานความร่วมมือกับกระทรวงเทคโนโลยีและสารสนเทศ ในการช่วยดำเนินการบูรณาการซอฟแวร์ HMC ในการแปลงฐานข้อมูล ซึ่งหากมีการออกระเบียบมารองรับก็สามารถเชื่อมโยงข้อมูล ได้โยอาจจะมีกฎหมาย 2 ฉบับที่สามารถใช้ได้คือ ร่าง พรบ. ธุรกรรมอิเลคโทรนิคส์ และร่างพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ ดังนั้น หากมีการเชื่อมโยงข้อมูลกับหน่วยงานในกระบวนการยุติธรรม ก็จะต้องมีกฎหมายหรือระเบียบฯ โดยเฉพาะมารองรับ เพราะที่มีการดำเนินการอยู่ในปัจจุบัน มีเพียงเลขาธิการ ปปง. และผู้ที่ได้รับมอบหมายเท่านั้นที่มีอำนาจในการอนุญาตให้บุคคลอื่นเข้าถึงข้อมูลของ ปปง.

12. สำนักงานอัยการสูงสุด

เป็นส่วนราชการที่ไม่สังกัดสำนักนายกรัฐมนตรี กระทรวง หรือทบวง อยู่ในบังคับบัญชาของรัฐมนตรีว่าการกระทรวงยุติธรรม มีอำนาจหน้าที่เกี่ยวกับการดำเนินคดีอาญาทั้งปวง ดำเนินคดีแพ่ง และให้คำปรึกษาด้านกฎหมายแก่รัฐบาลและหน่วยงานของรัฐ และอำนาจหน้าที่ตามที่กำหนดไว้ในกฎหมาย

สำนักงานอัยการสูงสุดได้จัดทำสารบบคดีด้านอิเลกโทรนิกส์ โดยมีการจัดเก็บฐานข้อมูลเป็นของตนเอง และมีการเชื่อมโยงข้อมูลกับสำนักงานศาลยุติธรรม สำนักงานป้องกันและปราบปรามยาเสพติด สำนักงานตำรวจแห่งชาติ (เฉพาะกรณีการฟ้องด้วยวาจา) และ

สำนักงานผู้ตรวจการแผ่นดินรัฐสภา สำนักงานอัยการสูงสุด มีขอบเขตการจำกัดการเก็บข้อมูล แต่ก็จะเก็บข้อมูลครบถ้วนในกลุ่มที่ดำเนินการในขณะนี้ก็อยู่ในระหว่างการดำเนินการเกี่ยวกับข้อมูลทางคดี

ในด้านกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องนั้นก็ใช้ระเบียบของอัยการสูงสุด (พ.ศ. 2542) เป็นกรอบส่วนการจะให้ข้อมูลหรือไม่แก่ฝ่ายใดนั้นก็จะให้เป็นดุลพินิจของผู้บริหารฯ (อธิบดีอัยการฯ)

13. สำนักงานศาลยุติธรรม

สำนักงานศาลยุติธรรมนั้น โดยทั่วไปในการปฏิบัตินั้น อาศัยประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 92 93 มาเป็นแนวทางการปฏิบัติ กล่าวคือ ถ้าเป็นในส่วนของการประสานงานขอข้อมูลระหว่างการดำเนินการของส่วนราชการก็ไม่มีปัญหา ศาลสามารถอนุญาตได้ แต่สำหรับบุคคลภายนอกแล้วก็จะอนุยาติเฉพาะคู่ความเท่านั้น ไม่ได้มีการออกกฎ หรือระเบียบภายในของสำนักงานศาลยุติธรรมเป็นการเฉพาะ การดำเนินการโดยทั่วไปก็จะอาศัยพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ประกอบเป็นหลักด้วย เช่นกัน อย่างไรก็ตาม ในการขอหรือเชื่อมโยงข้อมูลก็อาจจะประสบปัญหาเช่นกัน เพราะต้องยึดตามหลักกฎหมายที่ว่า การขอข้อมูลงานคดี ก็ต้องถือว่า เป็นคู่ความในคดี ดังนั้น หากไม่ใช่ เป็นคู่ความในคดี ก็อาจจะไม่สามารถกระทำได้ ในส่วนนี้จึงอาจจะกระทบต่อการเชื่อมต่อข้อมูล

ภาคผนวก 2
สรุปผลการประชุมเชิงปฏิบัติการ ครั้งที่ 2
เพื่อรับฟังความคิดเห็นเกี่ยวกับประเด็นทางกฎหมายที่เกี่ยวข้อง

ผลสรุปการประชุมเชิงปฏิบัติการ
“การปรับปรุงระเบียบกฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม”
เพื่อรับฟังข้อเท็จจริงประเด็นทางกฎหมาย
วันพฤหัสบดีที่ 8 กุมภาพันธ์ 2550 เวลา: 8.30-12.00 น.
ณ ห้องประชุม ชั้น 28 อาคารซอฟแวร์ปาร์ค กระทรวงยุติธรรม
ถนนแจ้งวัฒนะ กรุงเทพมหานคร

---

1. พิธีเปิดการประชุมฯ

โดย ผู้อำนวยการสถาบันวิจัยและพัฒนา สำนักงานกิจการยุติธรรม
นายวัลลภ นาคบัว

สำนักงานกิจการยุติธรรม OFFICE OF JUSTICE AFFAIRS

2.การบรรยายสรุปโดยที่ปรึกษาโครงการ

ที่ปรึกษาโครงการได้บรรยายสรุปถึงการดำเนินการในด้านต่าง ๆ 3 ส่วน ดังนี้

ส่วนที่ 1 บทนำ

ได้กล่าวถึง ที่มา และแนวทางการดำเนินการตามหลักการและเหตุผล วัตถุประสงค์ เป้าหมาย วิธีดำเนินการศึกษา และผลที่คาดว่าจะได้รับ

ส่วนที่ 2 แนวคิดการบูรณาการและการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม

เป็นการบรรยายให้รายละเอียด ในประเด็นการนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในองค์กร ข้อมูลสารสนเทศในกระบวนการยุติธรรม การคุ้มครองข้อมูล (Data Protection) แนวทางการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ การบูรณาการข้อมูลด้านการบริหารงานยุติธรรม และเทคโนโลยีสารสนเทศและการบูรณาการข้อมูล ด้านงานยุติธรรมของไทย

ส่วนที่ 3 ประเด็นต่าง ๆ ในทางกฎหมาย อันได้แก่

ประเด็นกฎหมายที่เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม ประเด็นกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล ประเด็นกฎหมายทรัพย์สินทางปัญญา ประเด็นด้านอาชญากรรมคอมพิวเตอร์ และ Computer Misuse ด้านช่องว่างทางกฎหมาย และแนวทางแก้ไข มาตรการทางกฎหมายในการบริหารจัดการ บทกำหนดด้านโทษ และประเด็นอื่น ๆ

3. กำหนดการ

กำหนดการ
การประชุมเชิงปฏิบัติการ เรื่อง
“การปรับปรุงระเบียบกฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม”
เพื่อรับฟังข้อเท็จจริงประเด็นทางกฎหมาย
วันพฤหัสบดีที่ 8 กุมภาพันธ์ 2550 เวลา 8.30 น. – 12.00 น.
ณ ห้องประชุมชั้น 28 อาคารซอฟแวร์ปาร์ค กระทรวงยุติธรรม
ถนนแจ้งวัฒนะ กรุงเทพมหานคร

8.30 – 9.00 น. : ลงทะเบียนและรับเอกสาร

9.00 – 9.20 น. : พิธีเปิดการประชุมฯ
โดย ผู้อำนวยการสถาบันวิจัยและพัฒนา
สำนักงานกิจการยุติธรรม
นายวัลลภ นาคบัว

9.20 – 10.15 น.: การบรรยายเรื่อง **“กฎหมาย และระเบียบ ที่เอื้ออำนวย และเป็นอุปสรรคต่อการเชื่อมต่อและการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม”**
โดย นายฐนันดรศักดิ์ บวรนันทกุล หัวหน้าโครงการฯ

10.15 – 10.30 น.: รับประทานอาหารว่าง

10.30 – 12.00 น.: ประชุมสัมมนา อภิปราย และแลกเปลี่ยนความคิดเห็น

12.00 น. : ปิดการประชุม รับประทานอาหารกลางวันร่วมกัน

ประเด็นทางกฎหมาย ประชุมเชิงปฏิบัติการ ครั้งที่ 2
การปรับปรุงระเบียบ กฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม

สารบัญ

1. ประเด็นกฎหมายที่เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม
2. ประเด็นกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล
3. ประเด็นกฎหมายทรัพย์สินทางปัญญา
4. ประเด็นด้านอาชญากรรมคอมพิวเตอร์ และ Computer Misuse
5. ช่องว่างทางกฎหมาย และแนวทางแก้ไข
6. มาตรการทางกฎหมายในการบริหารจัดการ
7. บทกำหนดด้านโทษ
8. ประเด็นอื่น ๆ

4. ผลสรุปการประชุมเชิงปฏิบัติการ

สรุปการอภิปราย แลกเปลี่ยนแนวคิดในการประชุมเชิงปฏิบัติการครั้งที่ 2

4.1 กองทะเบียนประวัติอาชญากร หรือ ทว. สำนักงานตำรวจแห่งชาติ ทำหน้าที่รักษาฐานข้อมูลกลางที่สำนักงานตำรวจแห่งชาติ จะดำเนินการจัดเก็บเกี่ยวกับประวัติผู้กระทำผิด กองทะเบียนประวัติอาชญากร ได้ทำความตกลงเชื่อมข้อมูลกับสำนักทะเบียนราษฎร์ กระทรวงมหาดไทย มีข้อสังเกต 2 ประการ คือ

ประการแรก การเคลื่อนไหวเปลี่ยนข้อมูล ซึ่งเป็นเรื่องจำเป็นเพราะจะต้องประสานกับสถานีตำรวจในการตรวจสอบประวัติการกระทำผิด ความทันสมัย และการเคลื่อนไหวเปลี่ยนแปลงข้อมูลจะช่วยในการสอบประวัติได้ชัดเจน

ประการที่สอง ประวัติการกระทำผิดของเด็ก และเยาวชน ซึ่งมีข้อมูลที่เก็บไว้ที่กองทะเบียนประวัติอาชญากร จะต้องมีการพิจารณาร่วมกันกับหน่วยงานต่างๆว่า มีความจำเป็นมากน้อยเพียงใดในการจัดเก็บ เพราะหากมีการเชื่อมโยงกันแล้วก็จะปรากฏประวัติการกระทำผิดของเด็กและเยาวชน ซึ่งอาจจะเป็นสิ่งกระทบต่ออนาคต และเป็นเรื่องที่ละเอียดอ่อน

4.2 สำนักงานศาลยุติธรรมนั้น ไม่ได้มีการออกกฎ หรือ ระเบียบภายในของสำนักงานศาลยุติธรรมเป็นการเฉพาะ การดำเนินการโดยทั่วไปก็จะอาศัยพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 เป็นหลักด้วย เช่นกัน อย่างไรก็ตาม ในการขอหรือเชื่อมโยงข้อมูลก็อาจจะประสบปัญหาเช่นกัน เพราะต้องยึดตามหลักกฎหมายที่ว่า การขอข้อมูลงานคดี ก็ต้องถือว่า เป็นคู่ความในคดี ดังนั้น หากไม่ใช่ เป็นคู่ความในคดี ก็อาจจะไม่สามารถกระทำได้ ในส่วนนี้จึงอาจจะกระทบต่อการเชื่อมต่อข้อมูล

4.3 ในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรมนั้น อาจต้องมีการกำหนดระดับ Security ระหว่างข้าราชการด้วยกัน นอกเหนือจากการที่ให้ระดับผู้บริหารในแต่ละองค์กรได้ลงนามความร่วมมือ หรือ MOU และให้เป็นชุดข้อมูล

4.4 ในส่วนของสำนักงาน ปปส.นั้น มีการเชื่อมโยงข้อมูลกับหน่วยงานต่างๆอยู่แล้ว แต่ระเบียบภายในโดยตรงไม่มีเป็นการเฉพาะ ที่จะมีใช้ก็จะเป็นกฎหมายของปปส.เองซึ่ง

เป็นกฎหมายพิเศษ ดูน่าจะเป็นอุปสรรคต่อการเชื่อมโยง เพราะข้อมูลอาจจะเปิดเผยไม่ได้ และนอกจากนั้นก็เป็นการใช้ปรับตามพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 เป็นหลัก และก็ใช้ประกอบในการปฏิบัติงาน

4.5 กรมพินิจและคุ้มครองเด็กนั้น มีกฎหมายที่เกี่ยวข้องคือ พระราชบัญญัติจัดตั้งศาลเยาวชนและครอบครัว พ.ศ. 2534 ที่ห้ามการเผยแพร่ข้อมูลเกี่ยวกับเด็กและเยาวชนที่กระทำผิด และการพิจารณาเยาวชนฯก็จะพิจารณาเป็นการลับ การเก็บข้อมูลของสถานพินิจฯ นอกจากเด็ก เยาวชนและญาติแล้ว ก็จะไม่ให้บุคคลอื่นได้รับรู้ ข้อมูลที่มีการเก็บรักษาจะมีการส่งต่อข้อมูลเพื่อให้ศาลได้พิจารณาประกอบ เมื่อศาลตัดสินและสั่งอบรม ก็จะดำเนินการเก็บข้อมูลหรือ หากมีการเปลี่ยนแปลงก็จะส่งต่อให้กรมคุมประพฤติ โดยหลักการแล้ว ข้อมูลที่เกี่ยวกับเด็กกระทำผิดก็เป็นข้อมูลที่ไม่ควรเปิดเผย เพราะจะเกิดความเสียหายได้ โดยเฉพาะหากเจ้าหน้าที่ไม่ตระหนักเปิดเผยออกไป อย่างไรก็ตาม ในทางปฏิบัติทางกรมพินิจฯก็ได้มีการตั้งคณะทำงานขึ้นมาร่างเป็นระเบียบภายในซึ่งก็จะใช้ต่อไป โดยจะมีการจำแนกข้อมูลออกและข้อมูลบางประเภท การเชื่อมโยงจะเป็นประโยชน์แก่เด็กเองและเป็นข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินคดี เช่น การฝึกอบรม เป็นต้น ซึ่งข้อมูลประวัติการกระทำผิดก็ได้มีการพูดคุยกับหน่วยงานที่เกี่ยวข้องว่าอาจจะต้องมีการย้ายไปเก็บในฐานพิเศษเฉพาะแยกออกไป เพื่อไม่ให้ปรากฏ

4.6 สำนักงานปปช.นั้น มีกฎหมายที่ให้อำนาจชัดเจน คือ พระราชบัญญัติประกอบรัฐธรรมนูญ ซึ่งในการทำงาน ปปช.สามารถอ้างพระราชบัญญัติประกอบรัฐธรรมนูญดังกล่าว ขอข้อมูลได้ทุกหน่วยงานและทุกประเภทของเอกสาร ซึ่งแม้บางหน่วยงาน เช่น สำนักงานประกันสังคม

ในการเชื่อมโยงข้อมูลจะไม่มีการเชื่อมโยงข้อมูลรายเรื่อง แต่จะเชื่อมโยงตามความจำเป็นเท่านั้น ใช้ระบบการเชื่อมโยงคล้ายกับของกรมสรรพากร มีการจัดทำฐานเก็บติดตั้งระบบอิเลคโทรนิคส์ เพื่อสร้าง Security ผู้ที่ใช้เกี่ยวข้องก็จะมี Card อิเลคโทรนิคส์ เพื่อสร้าง Security ผู้ที่ใช้เกี่ยวข้องก็จะมี Card จึงจะเข้าไปได้ อย่างไรก็ดี การจะขอข้อมูลก็อาจทำได้เป็นรายเรื่อง ปปช.เองก็อยากจะเชื่อมโยงข้อมูลกับหลายๆหน่วยงาน เช่น สำนักทะเบียนราษฎร กรมการขนส่งทางบก เป็นต้น เพราะการเชื่อมโยงก็ช่วยในการปฏิบัติงานของปปช.ให้รวดเร็วได้เช่นกัน เช่น กรณี การต้องเดินทางไปสอบสวนหรือตรวจสอบต่างจังหวัด ถ้ามีการเชื่อมโยง สามารถเข้าไปค้นหาได้เร็วยิ่งขึ้น ในหลักการเป็นสิ่งที่ดีเพียงแต่ต้องระมัดระวังเรื่องความปลอดภัยเท่านั้น การทำความตกลงหรือ MOU กับหน่วยงานต่างๆก็จะเป็นจุดเริ่มต้นได้ค่อยขยายต่อไป

4.7 สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม ยังไม่ได้มีการเชื่อมโยง และ/หรือ แลกเปลี่ยนข้อมูลกับหน่วยงานใด ๆในการเปิดเผยข้อมูลก็จะใช้หลักเกณฑ์ตามพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 เป็นหลัก ส่วนทิศทางหรือการดำเนินการเชื่อมโยง แลกเปลี่ยนหรือบูรณาการข้อมูลกับหน่วยงานอื่นๆในกระบวนการยุติธรรมก็คงขึ้นอยู่กับนโยบายของผู้บริหารเป็นหลัก

4.8 ด้านกรมการขนส่งทางบกนั้น มีหลายหน่วยงานที่เชื่อมต่อและต้องใช้ข้อมูล เช่น สำนักงานตำรวจแห่งชาติ ซึ่งก็มีการลงนามบันทึกความร่วมมือแล้ว และกำลังมีการจัดทำระบบการเช่าซื้อรถยนต์ ซึ่งก็จะเป็นประโยชน์ในการเชื่อมโยงข้อมูลต่อไปในการดำเนินการต่าง ๆ หรือในส่วนที่จะตรวจสอบการโจรกรรมรถยนต์

หน่วยงานต่าง ๆที่มีการจัดเก็บข้อมูลควรที่จะมีการ Update ข้อมูลอยู่เสมอและควรมีการแจ้งให้หน่วยงานอื่น ๆทราบว่ามีการจัดเก็บข้อมูลประเภทใด ซึ่งเมื่อหน่วยงานอื่นต้องการข้อมูลก็อาจจะทำหนังสือขอเชื่อมโยง และทำ MOU กันต่อไป อย่างน้อยแต่ละหน่วยงานก็จะมีฐานข้อมูลเบื้องต้น

4.9 ข้อที่กังวลใจมากที่สุด ก็คือ เกรงจะถูกนักการเมืองเข้ามาดูแลหน่วยงานนำเอาข้อมูลเหล่านี้ไปใช้แสวงหาประโยชน์หรือทำลายคู่ต่อสู้ ซึ่งข้าราชการประจำป้องกันยากในส่วนนี้ เพราะฉะนั้น ยิ่งมีการจัดเก็บเป็นระบบและเชื่อมโยงชัดเจน ยิ่งอาจจะเป็นช่องทางที่ทำให้นักการเมืองสามารถให้ข้าราชการไปเอาข้อมูลจากหน่วยงานอื่น ๆมาใช้ด้วย จึงควรมีมาตรการที่ชัดเจนในการปกป้องคุ้มครอง การเข้าถึงข้อมูลส่วนนี้อย่างเข้มงวด นอกจากนี้เวลาเกิดความรับผิดขึ้นมา ข้าราชการประจำเองจะต้องเป็นผู้รับผิด นักการเมืองมักจะรอดพ้นเพราะใช้ข้าราชการเป็นคนทำ

4.10 กรมคุ้มครองสิทธิก็มีการเก็บรวบรวมข้อมูลผู้เสียหายในคดีอาญาที่มาขอรับเงินค่าชดเชย แต่ก็ยังไม่ได้มีการเชื่อมโยงข้อมูลกับหน่วยงานอื่น ๆ จะใช้ข้อมูลฐานทะเบียนราษฎร์ ช่วยในการทำงาน ในส่วนของการดำเนินการตามพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 นั้น ได้มีการเตรียมออกระเบียบว่าด้วยการให้ข้อมูลฯ มารองรับการดำเนินงานตามพรบ.ข้อมูลข่าวสารฯ ดังกล่าว สำหรับบุคคลภายนอกที่จะมาขอข้อมูล

4.11 กรมบังคับคดี มีการจัดทำพัฒนาและปรับปรุงฐานข้อมูลให้มีความทันสมัย โดยเฉพาะในทางแพ่งมีข้อมูลเกี่ยวกับทรัพย์และการขายทอดตลาด ในทางล้มละลายก็มีข้อมูล

เกี่ยวกับบุคคล และก็ได้มีการประสานงานติดต่อในกรณีที่บุคคลนั้นขอเดินทางไปต่างประเทศ โดยประสานกับทางสำนักงานตรวจคนเข้าเมือง (ตม.) สำนักงานตำรวจแห่งชาติและกระทรวงต่างประเทศ กรมบังคับคดีก็ไม่ได้มีการออกระเบียบใดๆเป็นพิเศษเฉพาะมารองรับ แต่ก็จะปรับใช้จากตัวพระราชบัญญัติข้อมูลข่าวสารทางราชการพ.ศ. 2540

4.12 ในส่วนของสำนักงานศาลยุติธรรม มีการเก็บรวบรวมข้อมูลเป็นระบบส่วนการเชื่อมโยงและขอให้ข้อมูลก็คงต้องเป็นไปตามประมวลกฎหมายวิธีพิจารณาความแพ่ง ซึ่งผู้ที่จะไปขอได้ก็ต้องเป็นคู่ความ ทางสำนักงานก็ได้มีการออกระเบียบการขอ ซึ่งก็ต้องสอดคล้องกับหลักตามประมวลกฎหมายวิธีพิจารณาความแพ่งด้วยกัน

4.13 มีข้อควรระวัง เช่นกันเกี่ยวกับความถูกต้องของข้อมูล เพราะเคยขอข้อมูลที่สำนักงานเขต กับข้อมูลที่สำนักทะเบียนราษฎร์ ปรากฏว่า ไม่ตรงกัน และในการปฏิบัติงานก็เคยพบว่า บุคคลคนเดียวมีบัตรประชาชน 2 ใบ มีเลขที่บ้าน แตกต่างกันออกไป ดังนั้น จึงต้องมีการตรวจสอบยืนยัน และเกิดความชัดเจนว่าไม่ได้มีในด้านการเลือกตั้งหรือการเมืองเข้ามาเกี่ยว

4.14 อาจมีการนำเอาข้อมูลไปใช้ในทางที่ผิด เช่น ในการทวงหนี้บุคคล จึงต้องมีการจัดทำเป็นระบบป้องกัน และมีการตรวจสอบ รวมทั้ง การลงโทษการนำเอาข้อมูลเหล่านั้นไปใช้ในทางที่ผิด

4.15 ในการเชื่อมโยงข้อมูล เพื่อไม่ให้เกิดปัญหาจึงควรมีการจัดทำ MOU ระหว่างหน่วยงานย่อยๆก่อนแล้วค่อยๆขยายออกไป เป็นการดำเนินการในเชิงเทคนิค และการบริหารจัดการก่อน ส่วนกฎหมายควรดำเนินการภายหลัง และควรมีการออกกฎหมายพิเศษเฉพาะที่ตรงมาปรับใช้ดีกว่าไปปรับใช้จากกฎหมายทั่วไป ซึ่งไม่มีเป้าหมายหรือวัตถุประสงค์โดยตรง

ภาคผนวก 3
สรุปผลการประชุมสัมมนา ครั้งที่ 3
เพื่อเผยแพร่และรับฟังความคิดเห็น
เกี่ยวกับร่างรายงานฉบับสมบูรณ์

ภาคผนวก 3: สรุปผลการประชุมสัมมนา ครั้งที่ 3 เพื่อเผยแพร่และรับฟังความคิดเห็นเกี่ยวกับร่างรายงานฉบับสมบูรณ์

ภาคผนวก 3

ผลสรุปการประชุมเชิงปฏิบัติการเพื่อรับฟังข้อเท็จจริง

"การปรับปรุงระเบียบกฎหมายให้เอื้ออำนวยต่อการใช้เทคโนโลยีสารสนเทศในกระบวนการยุติธรรม"

เพื่อรับฟังการวิพากษ์ผลการวิจัย

วันพฤหัสบดีที่ 19 เมษายน 2550 เวลา 9.00-14.00 น.

ณ ห้องแคทลียา โรงแรมรามาการ์เด้นส์ ถนนวิภาวดีรังสิต กรุงเทพมหานคร

หัวหน้าโครงการได้บรรยายสรุปผลการศึกษาวิจัยและนำเสนอข้อเสนอแนะดังต่อไปนี้

1. ข้อเสนอแนะด้านการแก้ไขปัญหาและอุปสรรค ได้แก่ กระทรวงยุติธรรมควรจะเป็นเจ้าภาพหลักในการดำเนินการ โดยการมอบหมายให้มีหน่วยงานหลักที่รับผิดชอบดูแลโดยเฉพาะและดำเนินการในกระทรวงยุติธรรมก่อน และกำหนดเป็นนโยบายที่ให้ทุกหน่วยงานในสังกัดจัดทำแผน โครงการ จัดเก็บ ประมวลผลข้อมูล และดำเนินการเชื่อมต่อข้อมูลระหว่างหน่วยงานในกระทรวงยุติธรรมเป็นหลักก่อน จากนั้นค่อยขยายความร่วมมือไปยังหน่วยงานเชื่อมโยง มีการจัดทำคู่มือการดำเนินการ (Code of Practice) เพื่อเป็นแนวทางให้หน่วยงานต่าง ๆ ได้ใช้เป็นแนวทางและมาตรฐานในการจัดเก็บข้อมูล ประมวลผลข้อมูล และมีการจัดคณะทำงานกลาง (Liaison Staffs) เพื่อทำหน้าที่ประสานงานและให้คำแนะนำเกี่ยวกับการจัดทำฐานข้อมูล และควรมีการสำรวจความต้องการใช้ข้อมูลในการปฏิบัติงานของหน่วยงานต่างๆ เพื่อเป็นข้อมูลในการจัดทำแบบในการจัดเก็บให้เป็นมาตรฐานในการจัดเก็บ การประมวลข้อมูลต่อไป

2. ข้อเสนอแนะในด้านการปรับปรุงกฎหมาย ได้แก่ ควรจะมีการออกเป็นระเบียบของกระทรวงยุติธรรมออกมาใช้ก่อน เป็นกฎหมายในฝ่ายบริหาร มาดำเนินการในระยะแรกการยกร่างกฎหมายที่เกี่ยวข้องกับการบริหารจัดการเกี่ยวกับการเชื่อมโยง แลกเปลี่ยน

และบูรณาการข้อมูลในกระบวนการยุติธรรมโดยตรง ในการจัดทำร่างกฎ ระเบียบ หรือกฎหมายที่เกี่ยวข้องนั้นควรคำนึงถึงแนวทางที่เป็นสากล เนื่องจากในอนาคตอาจจะมีการเชื่อมต่อข้อมูลกับประเทศต่างๆที่มีมาตรฐานเดียวกัน เนื่องจากหน่วยงานต่างๆ ในกระบวนการยุติธรรม มีการเก็บข้อมูลในฐานข้อมูลของตน และในบางหน่วยงานควรมีการประชุมและกำหนดประเภทของข้อมูลที่เปิดเผยได้ เปิดเผยไม่ได้ มีมาตรการที่ระบุถึงประเภทข้อมูล ในการออกมาตรการทางกฎหมายต้องมีมาตรการที่ป้องกันมิให้นักการเมืองเข้ามาแสวงหาและใช้ประโยชน์จากฐานข้อมูลและการเชื่อมโยงข้อมูล และการแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรม

1. สรุปการอภิปราย แลกเปลี่ยนความคิดเห็น การสอบถามในการประชุมสัมมนาสรุปผลการวิจัยฯ

1.1 ความไม่ชัดเจนของแนวทางตามกฎหมายที่มีอยู่จะสามารถปรับใช้ได้หรือไม่ หากมีการเชื่อมโยง แลกเปลี่ยน หรือบูรณาการข้อมูลในกระบวนการยุติธรรมโดยเฉพาะตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 157 ที่ระบุว่า “ฟ้องต้องทำเป็นหนังสือ...” ดังนั้น หากสำนวนคดีที่อยู่ในรูปอิเลกโทรนิกส์ หากมีการนำไปฟ้องศาลจะรับฟ้องหรือไม่ และข้อมูลอิเลกโทรนิกส์ หากพิมพ์ออกมาและนำไปฟ้องจะถือว่าเป็น การฟ้องด้วยหนังสือหรือไม่ (ซึ่งแม้ประมวลกฎหมายวิธีพิจารณาความอาญาจะเปิดช่องให้การบันทึกคำให้การจะกระทำได้ในรูปอิเลกโทรนิกส์) ในส่วนนี้ ศาลก็ยังไม่ได้มีการออกระเบียบมารองรับโดยตรงและเท่าที่รู้ก็มีศาลจังหวัด นนทบุรี ที่มีการทดลองใช้แต่ก็ยังไม่ได้มีการออกแนวทางชัดเจน

1.2 การดำเนินการเชื่อมต่อ แลกเปลี่ยน หรือการบูรณาข้อมูลนั้น หลักการคือ การไม่มีฐานข้อมูล (data base) ที่ซ้ำซ้อน เมื่อมีการดำเนินการตั้งแต่ชั้นตำรวจฐานข้อมูลก็ควรจะสามารถใช้การได้ตลอดสายการดำเนินคดี

1.3 ประเด็นของกรณีที่ข้อมูลเป็นลักษณะดิจิตอลนั้น ประเด็นปัญหาที่ควรจะต้องพิจารณาก็คือ

ก. การมี E-work flow นั้น จะมีกฎหมายใดๆที่จะห้ามหรือไม่?

ข. ในการแลกเปลี่ยนข้อมูล (Share data) นั้น จะมีกฎหมายใดๆห้ามหรือไม่? ในการแลกเปลี่ยนข้อมูลเพราะบางประเทศ เช่น ออสเตรเลีย จะมีกฎหมายห้ามการแลกเปลี่ยนข้อมูลไว้โดยเฉพาะ

ค. ควรมีการสำรวจความต้องการ (Need assessment) เพื่อหารูปแบบ (formal) ที่ชัดเจนต่อไป เพราะการมี Format ที่ชัดเจนแล้วก็จะรู้กระบวนการทั้งระบบได้เลย

ซึ่งจะช่วยให้การเชื่อมโยงและการแลกเปลี่ยนข้อมูลสามารถกระทำได้ง่าย ในต่างประเทศนั้นจะมีการวางกรอบหรือ format ไว้ชัดเจนก่อน เป็นเสมือนการสร้างผลลัพธ์ (outcome) ให้เห็น ซึ่งในที่สุดก็จะทำให้มองเห็นว่า จะมีจุดเริ่มต้นจากตรงไหนแล้วจะพัฒนาไปสู่รูปแบบตรงไหน การเปลี่ยนแปลงจากเอกสาร (paper) ไปอยู่ในรูปข้อมูลอิเลกโทรนิกส์ หรือ ลงในคอมพิวเตอร์ธรรมดาไม่เกิดประโยชน์อะไร

1.4 ในการร่างระเบียบของหน่วยงานต่าง ๆที่จะประสานการเชื่อมโยงหรือแลกเปลี่ยนข้อมูล รวมถึงการบูรณาการข้อมูลในกระบวนการยุติธรรม ควรมีการนำเอาหลักการ 8 ประการ ซึ่งมีในเอกสารประการประชุม อันได้แก่ ขอบเขตในการรวบรวมคุณภาพของข้อมูล การกำหนดจุดมุ่งหมาย ขอบเขตการใช้งาน การป้องกันความปลอดภัย การเปิดเผย การใช้ร่วมกัน และการรับผิดชอบ มาบรรจุในระเบียบด้วย

1.5 ในการแลกเปลี่ยนข้อมูลนั้นคงจะต้องไปพิจารณาดูว่า จะจัดสมดุลการแลกเปลี่ยนข้อมูล (Balancing data sharing) ว่า ข้อมูลประเภทใด แลกเปลี่ยนได้ ข้อมูลประเภทใดแลกเปลี่ยนไม่ได้ มีกฎหมายใดห้ามการแลกเปลี่ยนหรือไม่ เพราะบางประเทศ เช่น ออสเตรเลีย ก็จะมีกฎหมายห้ามการแลกเปลี่ยนข้อมูล ส่วนของประเทศไทยคงมีข้อจำกัด เช่น ข้อมูลของ สำนักงานปปช. หรือ สำนักงาน ปปง. ก็คงจะมีข้อจำกัด และการเสนอขอแก้กฎหมายก็อาจจะกระทำไม่ได้ทั้งหมดเช่นกัน

1.6 ในปัจจุบัน กฎหมายที่เกี่ยวข้องโดยตรงกับการแลกเปลี่ยน เชื่อมโยง และบูรณาการข้อมูลในกระบวนการยุติธรรม ก็ยังไม่มีกฎหมายออกมาเฉพาะชัดเจน เห็นด้วยกับข้อเสนองานวิจัยว่า ในระยะยาวควรมีการเสนอร่างกฎหมายนี้ เพื่อให้สามารถดำเนินการได้ เพราะ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 ก็ไม่ได้ออกมาเพื่อรองรับการเชื่อมโยง หรือแลกเปลี่ยนข้อมูลโดยตรง และความมุ่งหมายก็ไปเน้นที่ให้เอกชน สามารถเข้าถึงข้อมูลของรัฐบางประการ หรือการป้องกันการทุจริต ซึ่งตัวพระราชบัญญัตินั้นก็ยังมีปัญหามากมาย เช่น ขอบเขตหรือความหมายของข้อมูลส่วนบุคคลหรือไม่ หรือ การออกกฎหมายลูก การวินิจฉัยในบางประเด็น เช่น กรณีที่ยกมาพูดกันเกี่ยวกับ กรณีว่า “การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ” ตามที่พูดกันก็ยังไม่ชัดเจน การจะแก้ไขตัวพระราชบัญญัติข้อมูลข่าวสารฯ ก็ยังไม่รู้ว่าจะทำได้มากน้อยแค่ไหน หากจะนำมาปรับใช้กับการเชื่อมโยงและแลกเปลี่ยนข้อมูล

1.7 พระราชบัญญัติธุรกรรมอิเลกโทรนิกส์ ก็มีบทบัญญัติที่มาปรับใช้ได้ในระดับหนึ่ง เช่น ตามมาตรา 15 แต่สิ่งที่ต้องพิจารณาและระวังก็คือ การเชื่อมโยง และ

แลกเปลี่ยน มิควรเป็นในรูปของการ duplicate หรือ copy ข้อมูลไปให้ เช่น เคยมีกรณีกรมบัญชีกลาง copy ข้อมูลผู้ที่สามารถเบิกจ่ายค่ารักษาพยาบาล ซึ่งก็จะมีปัญหา เพราะมีข้อมูลส่วนบุคคลปนไปอยู่ด้วยในฐานข้อมูล แต่การ copy หรือ duplicate ข้อมูลหรือต้องไปรับผิดตามกฎหมายลิขสิทธิ์ อย่างกฎหมายของสหภาพยุโรปด้วยหรือไม่นั้น สำหรับของไทยน่าจะยังไม่ไปไกลถึงขนาดนั้น เพราะผู้เก็บรวบรวมข้อมูลเก็บโดยอาศัยอำนาจของตนที่มีอยู่และข้อมูลที่เข้ามาสู่ในหน่วยงาน อาจจะยังไม่ถึงขั้นเป็นการรังสรรค์ข้อมูลหรือผลิตผลงานขึ้นมาใหม่

1.8 หลายหน่วยงานก็พยายามทำความตกลงเชื่อมโยงข้อมูลกัน ได้มากพอสมควร เช่น ทะเบียนประวัติอาชญากร (ทว.) กับกรมคุมประพฤติ หรือ กรมศุลกากรก็เชื่อมโยงข้อมูลกับกรมการขนส่งทางบก หรือ กระทรวงมหาดไทย เป็นต้น

1.9 ในส่วนของสถานีตำรวจนั้น พนักงานสอบสวนต้องมีการจัดทำประวัติการต้องโทษด้วย ในสถานีไม่มีข้อมูลที่จะเชื่อมโยงหรือตรวจสอบได้ ต้องอาศัยตรวจสอบไปที่กองทะเบียนประวัติอาชญากร โดยข้อเท็จจริง แล้วก็เป็นปัญหา เช่นกันว่า การพิสูจน์บุคคลเพื่อเพิ่มโทษ การตรวจเอกลักษณ์ จากการดูลายพิมพ์นิ้วมือ ประเด็นคือ ตามข้อกฎหมายประมวลกฎหมายวิธีพิจารณาความอาญา พนักงานสอบสวนมีอำนาจในการพิมพ์ลายนิ้วมือผู้ต้องหาได้หรือไม่ หากผู้ต้องหาไม่ยินยอม

1.10 ข้อเสนอพิจารณาจากผู้แทน กทช. เป็นข้อสังเกตว่า การนำเอากรอบทางกฎหมายกับด้านไอทีมาปรับใช้หรือ Implement ต้องมีกรอบหลัก แม้การใช้ e-government หรือการดำเนินการของกรมบัญชีกลาง ก็ยังต้องใช้กรอบของ World Bank ซึ่งก็จะประกอบด้วยองค์ประกอบด้าน 1) กฎหมาย 2) สังคม 3) เทคโนโลยี 4) การเชื่อมต่อ 5) ส่วน segments ต่างๆซึ่งการดำเนินการก็ต้องคำนึงถึงด้วย

1.11 ในการวางแผนดำเนินการเชื่อมต่อและแลกเปลี่ยนข้อมูลการบูรณาการข้อมูลในกระบวนการยุติธรรมของกระทรวงยุติธรรมนั้น เป็นการพิจารณาการปรับใช้กฎหมายกับยุทธศาสตร์ด้านอื่นๆ และกรอบแผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรมแห่งชาติ และที่ดำเนินการเป็น DXC หรือ Data eXchange Center ทำหน้าที่เป็นเสมือน broker กรอบของแผนแม่บทจะพัฒนางาน paper work ให้เป็น digital ซึ่งก็จำเป็นจะต้องมีข้อมูลพื้นฐาน เช่น ถิ่นที่อยู่ เอกลักษณ์ของบุคคล ข้อมูลที่ได้มาก็ต้องมีการ Identify ให้ชัดเจนว่า ข้อมูลอะไรที่ต้องการใช้ ข้อมูลอะไรที่ใช้ในการดำเนินคดีเหล่านี้เป็นต้น ซึ่งหน่วยงานที่เกี่ยวข้องก็จะสามารถดึงข้อมูลมาใช้โดยไม่ซ้ำซ้อน

สำหรับแนวคิดในการจัดรูปเป็น broker เพื่อเป็นตัวกลางวิ่งไปหาข้อมูล แล้วส่งต่อจะช่วยลดปัญหาลงได้มาก ในตอนนี้ มุ่งให้หน่วยงานเตรียมความพร้อมในการพัฒนาจาก paper เป็น digital system ส่วนการดำเนินการอื่นๆ ก็ต้องดำเนินการตามยุทธศาสตร์ และต้องมีการสร้าง protocol ออกมาร่วมเป็นตัวกำกับด้วย ส่วนด้านกฎหมายก็คือ ต้องพิจารณาในการทำงานนั้น มีกฎหมายบางตัวที่เป็นอุปสรรค ที่ทำให้การเชื่อมโยง และแลกเปลี่ยนข้อมูลทำไม่ได้ อาจจะต้องปรับแก้เป็นระยะไป และมีการกำหนดเงื่อนไขประกอบด้วย กระทรวงยุติธรรมมุ่งที่จะเป็น facilitators ที่ให้หน่วยงานอื่นมาใช้ประโยชน์ได้

1.12 ในด้านกฎหมายที่เป็นอุปสรรคต่อการปฏิบัติงานเชื่อมต่อข้อมูลของหน่วยงานต่างๆ พบว่าโดยทั่วๆไป ได้แก่ พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 ทำให้ขอข้อมูลจากหน่วยงานได้ลำบาก ส่วนกฎหมายเฉพาะที่เป็นปัญหาอุปสรรค เช่น กฎหมายของ ปปช. ม.25 ที่ระบุการขอข้อมูลจากหน่วยงานอื่นๆ สามารถกระทำได้ง่าย แต่มาตรา 120 จะระบุห้ามการเปิดเผยข้อมูลที่ได้มาจากการไต่สวน เสมือนประมวลรัษฎากรที่ห้ามการเปิดเผยข้อมูลจะมีข้อยกเว้นก็เพียงแต่ กรณีการได้รับอนุมัติจากคณะกรรมการปปช. เท่านั้น ซึ่งกรณีนี้ก็จะเป็นปัญหาอุปสรรคในการเชื่อมต่อ หรือ แลกเปลี่ยนข้อมูล

1.13 ในส่วนของกระบวนการยุติธรรมของทหารนั้น โดยข้อเท็จจริงแล้วถือเป็นส่วนหนึ่งในกระบวนการยุติธรรมที่สำคัญ เพราะหลายๆกรณีเป็นกรณีที่ทหารไปกระทำผิดต่อพลเรือน (ทหารกระทำผิดต่อทหารด้วยกันมีน้อยมาก) แต่เมื่อมีการบัญญัติกฎหมายออกมาใช้มักมองข้ามกระบวนการยุติธรรมของทหาร และพิจารณาถึงพลเรือน ทั้งๆที่กระบวนการยุติธรรม ฝ่ายทหารก็ไม่ได้มีกฎหมายโดยตรง การขอเป็นไปตามระเบียบข้อบังคับทหาร คือ ให้ผู้บังคับบัญชา เป็นผู้ใช้ดุลพินิจในการดำเนินการโดยความคิดเห็น อยากจะให้มีระเบียบข้อบังคับทหาร คือ ให้ผู้บังคับบัญชา เป็นผู้ใช้ดุลพินิจในการดำเนินการ โดยความคิดเห็น อยากจะให้มีระเบียบหรือกฎหมายกลางเฉพาะตามที่งานวิจัยเสนอโดยรวมฝ่ายทหารเข้าไปด้วย ซึ่งจะเป็นผลดีทั้งต่อการดำเนินคดี ที่ทหารกระทำผิดต่อพลเรือนและส่วนหนึ่ง การออกกฎหมายกลางก็สามารถที่จะทำให้สามารถตั้งงบประมาณในการดำเนินการจัดทำฐานข้อมูล เตรียมบุคลากร วัสดุอุปกรณ์ ตลอดจนการเตรียมความพร้อมสำหรับการเชื่อมโยงแลกเปลี่ยนและบูรณาการข้อมูล ซึ่งข้อมูลทหารส่วนใหญ่ก็เป็นเอกสาร

1.14 ด้านคณะกรรมการการเลือกตั้ง หรือ กกต. นั้น กกต.ไม่ได้มีการออกระเบียบ หรือ กฎหมายใดๆเฉพาะขึ้นมาใช้ จึงไม่ได้มีกฎหมายห้ามหรือเป็นอุปสรรค การดำเนินการก็จะปรับใช้ของพระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540 มาใช้โดยอนุโลม มีข้อสังเกตก็เพียงกรณี ข้อมูลที่มีผลกระทบ คือ ข้อมูลที่อยู่ในสำนวนการสอบสวน

เช่น ชื่อพยาน ซึ่งหากมีการเปิดเผยออกไป จะไม่มีใครกล้าให้ปากคำเป็นพยาน ก็จะมีการใช้มติคณะกรรมการการเลือกตั้ง ปกปิดชื่อบุคคล เป็นต้น อย่างไรก็ตาม ในส่วนของการปรับใช้กฎหมายเพื่อให้เกิดความชัดเจน กกต. ได้มีการตั้งกรรมการข้อมูลข่าวสาร ภายใน กกต. เพื่อมาช่วยพิจารณากลั่นกรอง สำหรับส่วนกกต. หากจะมีการขอเชื่อมโยงข้อมูลหรือแลกเปลี่ยนข้อมูลในกระบวนการยุติธรรมก็สามารถดำเนินการได้ โดยอาจจะต้องมีการมาจำแนกหรือ Classify ประเภทข้อมูลก่อนและกำหนดผู้ขอใช้ แล้วทำความตกลงให้ชัดเจน ซึ่งในระดับผู้บังคับบัญชาระดับสูงก็สามารถทำความตกลงแลกเปลี่ยนข้อมูลกันได้ โดยที่น่าสนใจ คือ การใช้ฐานข้อมูลทะเบียนราษฎรมาผสมผสานกับระบบพรรคการเมือง เพื่อดูการเคยต้องคดี เป็นต้น

1.15 ข้อมูลในเอกสารการศึกษามีอยู่แล้ว แต่เนื่องจากเป็นเอกสารต่อเนื่อง จึงอยากให้ทำสรุปเพื่อเติมเป็นตารางมี 4 คอลัมน์ ได้แก่ หน่วยงานต่างๆ กฎหมายที่เกี่ยวข้อง ปัญหาอุปสรรค และแนวทางแก้ไข ซึ่งก็จะสะดวกในการอ่านและทำความเข้าใจมากยิ่งขึ้น

สำนักงานยุติธรรม OFFICE OF JUSTICE AFFAIRS

ภาคผนวก 4
รายชื่อผู้เข้าร่วมการประชุมเชิงปฏิบัติการ ครั้งที่ 1, 2 และการประชุมสัมมนา ครั้งที่ 3

รายชื่อผู้เข้าร่วมประชุมเชิงปฏิบัติการ ครั้งที่ 1
“การปรับปรุงระเบียบกฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศ
ในกระบวนการยุติธรรม”
วันพุธที่ 27 ธันวาคม 2549 เวลา 9.00 น. – 14.00 น.
ณ ห้องยูงทอง โรงแรม ที เค พาเลซ กรุงเทพมหานคร

ชื่อ - สกุล	หน่วยงาน
1. พ.ต.ต.พรชัย โฆษิตสุรังคกุล	สารวัตรกลุ่มงานเทคโนโลยีสารสนเทศ / ศูนย์ข้อมูลข้อสนเทศกลาง สำนักงานตำรวจแห่งชาติ
2.พ.ต.อ.สรรพฤทธิ์ สมบัติ	รองผบก./กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ
3.พ.ต.ท.อัศนีย์ อินทรครรชิต	รองผกก.ฝ่ายฯ 2/ กองทะเบียนประวัติอาชญากร ทว .สำนักงานตำรวจแห่งชาติ
4.นายสุกันท์ บุญญานนท์	สำนักงานป้องกันและปราบปรามการฟอกเงิน
5.นางรัชดาวรรณ ศิริไพบูลย์	นักวิชาการคอมพิวเตอร์/ กรมพินิจและคุ้มครองเด็กและเยาวชน กระทรวงยุติธรรม
6.น.ส.ธันวลัตน์ เชิงดี	พนักงานคุมประพฤติ/กรมพินิจและคุ้มครองเด็กและเยาวชน กระทรวงยุติธรรม
7.น.ส.ขนิษฐา คะนึงทอง	นักวิชาการคอมพิวเตอร์/ กรมคุมประพฤติ กระทรวงยุติธรรม
8.นางอรนุช ภักตร์กระจ่าง	นักวิชาการคอมพิวเตอร์/ กรมคุมประพฤติ กระทรวงยุติธรรม
9.น.ส.ขนิษฐา หลิมวาณิชย์	นักวิชาการคอมพิวเตอร์/สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด(สำนักงานปปส.)
10.นส.จิตติมา อุดมกุศลศรี	นิติกร /สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (สำนักงานปปส.)
11.นายเรืองณรงค์ แสนสุทธิ์	นักวิชาการคอมพิวเตอร์/ กลุ่มงานสารสนเทศ สำนักงานวางทรัพย์กลาง กรมบังคับคดี กระทรวงยุติธรรม

ชื่อ - สกุล	หน่วยงาน
12.นายธัญธิญะ คงชม	นักวิชาการคอมพิวเตอร์/ กลุ่มงานสารสนเทศ สำนักงานวางทรัพย์กลาง กรมบังคับคดี กระทรวงยุติธรรม
13.นายเขมชาติ ศุภนรากุล	สำนักงานคณะกรรมการป้องกันและปราบปราม การทุจริตแห่งชาติ
14.นางสมพร ครุฑสาคร	สำนักงานคณะกรรมการป้องกันและปราบปราม การทุจริตแห่งชาติ
15.นายชาญ วชิรเดช	หัวหน้าศูนย์ทะเบียนประวัติผู้ต้องขัง กองแผนงาน กรมราชทัณฑ์ กระทรวงยุติธรรม
16.ดร.สวัสดิ์ จิรัฏฐิติกาล	ศูนย์ทะเบียนประวัติผู้ต้องขังกองแผนงาน กรมราชทัณฑ์ กระทรวงยุติธรรม
17.นายนพดล พิเศษพงษา	นักวิชาการคอมพิวเตอร์/ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานอัยการสูงสุด
18.นางสาวภูธิดา จันต๊ะพรหมา	นักวิชาการคอมพิวเตอร์/ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานอัยการสูงสุด

รายชื่อผู้เข้าร่วมประชุมเชิงปฏิบัติการ ครั้งที่ 2
“การปรับปรุงระเบียบกฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศ
ในกระบวนการยุติธรรม”เพื่อรับฟังข้อเท็จจริงประเด็นทางกฎหมาย
วันพฤหัสบดีที่ 8 กุมภาพันธ์ 2550 เวลา: 8.30-12.00 น.
ณ ห้องประชุม ชั้น 28 อาคารซอฟ์แวร์ปาร์ค กระทรวงยุติธรรม
ถนนแจ้งวัฒนะ กรุงเทพมหานคร

รายชื่อ	ตำแหน่ง	สังกัด
1.นายวัลลภ นาคบัว	ผู้อำนวยการ สถาบันวิจัยและพัฒนา กระบวนการยุติธรรม	สำนักงานกิจการยุติธรรม
2.นายฐนันดร์ศักดิ์ บวรนันทกุล	หัวหน้าโครงการ	มหาวิทยาลัยมหิดล
3. นางสาวกัญจนพร แสงกาศ	นิติกร 5	สำนักวิชาการศาลยุติธรรม สำนักงานศาลยุติธรรม
4.นายขนิษฐ์ ขาวสำอางค์	นักวิชาการคอมพิวเตอร์ 3	กลุ่มงานเทคโนโลยีสารสนเทศและการสื่อสาร สถาบันนิติวิทยาศาสตร์
5.นางสาวขนิษฐา อวยพร	นักวิชาการคอมพิวเตอร์ 7 วช.	สำนักเทคโนโลยีและการสื่อสาร สำนักงานศาลยุติธรรม
6. นายเขมชาติ ศุภนรากุล	เจ้าพนักงานปป.ช.	ศูนย์เทคโนโลยีสารสนเทศ สำนักงานปป.ช.
7.พ.ต.อ.โฆษิต ปิยเจริญ	ผกก.กลุ่มงานเทคโนโลยีสารสนเทศ	สำนักงานตำรวจแห่งชาติ
8.นางสาวจิติมา อุดมกุศลศรี	นิติกร 6 ว.	กองนิติการ สำนักงานป้องกันและปราบปรามการฟอกเงิน
9.นายเฉลิมชนม์ แน่นหนา	หัวหน้ากลุ่มงานนิติการ	กรมคุ้มครองสิทธิและเสรีภาพ

รายชื่อ	ตำแหน่ง	สังกัด
10.นางสาวณัฐนรีภัทร์ นาวีเสถียร	นิติกร 4	กลุ่มกฎหมายและระเบียบ กรมการขนส่งทางบก
11. นางสาวน้ำฝน เกตุสิงห์สร้อย	เจ้าพนักงานธุรการ 3	สำนักงานกิจการยุติธรรม
12.นายปรีชา โสวรรณี	หัวหน้าส่วนพัฒนาระบบงาน	กรมพินิจและคุ้มครองเด็กและเยาวชน
13.นายพิเชฐ มงคลวณิชา	เจ้าพนักงานปป.ช. 8	สำนักนโยบายและแผน สำนักงานปป.ช.
14.นางรัชดาวรรณ ศิริไพบูลย์	หัวหน้ากลุ่มงานข้อมูลและสารสนเทศ	กรมพินิจและคุ้มครองเด็กและเยาวชน
15.นางสาวรุ่งฤดี อารยะสันติภาพ	นิติกร 4 กลุ่มงานนิติกร	สถาบันนิติวิทยาศาสตร์
16.นายเลิศพันธ์ เทียนทอง	นิติกร 8 ว.	กรมบังคับคดีล้มละลาย 1 กรมบังคับคดี
17.พล.ต.ต.วรินทร์ บุณยเกียรติ	ผบก.ศทก.	สำนักงานตำรวจแห่งชาติ
18.นางสาววันเต็มดวง สุรินทรางกูร	นิติกร 5	กลุ่มกฎหมาย และระเบียบ 2 กรมการขนส่งทางบก
19.นายสมศักดิ์ หรรษคุณาชัย	นิติกร 8	กรมบังคับคดีล้มละลาย 2 กรมบังคับคดี
20.นายสรรเพชร แสงสว่างเนตร	เจ้าหน้าที่วิเคราะห์ฯโยบายและแผน 6 ว.	สำนักงานป้องกันและปราบปรามการฟอกเงิน
21.นายสุภัทท์ บุญญานนท์	นักวิชาการคอมพิวเตอร์ วช.	สำนักงานป้องกันและปราบปรามการฟอกเงิน
22. นางสางอรณิช สุขบาล	เจ้าหน้าที่วิเคราะห์ฯโยบายและแผน 6 ว.	กองแผนงานและสารสนเทศ กรมคุมประพฤติ
23.นางอรนุช ภักตร์กระจ่าง	นักวิชาการคอมพิวเตอร์ 3	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมคุมประพฤติ

รายชื่อ	ตำแหน่ง	สังกัด
24.พ.ต.ท.อัศนีย์ อินทรครรชิต	รองผกก.ฝ่ายฯ2ทว.	กองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ
25.นางอุไรวรรณ สถานานนท์	นักวิชาการคอมพิวเตอร์ 8 วช.	ศูนย์เทคโนโลยีสารสนเทศ สำนักงานป้องกันและปราบปรามการฟอกเงิน
26.นางสาวอุษณิภา ชูจันทร์	นักวิชาการคอมพิวเตอร์ 3	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
27.นางสาวเอมอร เสียงใหญ่	หัวหน้ากลุ่มพัฒนาระบบบริหาร	กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม
28.นายชาญ วชิรเดช	หัวหน้าศูนย์ทะเบียนประวัติผู้ต้องขัง	กรมราชทัณฑ์ กระทรวงยุติธรรม
29.นายอิสรพงศ์ สาพงษ์เอี่ยม	เจ้าหน้าที่วิเคราะห์ฯโยบายและแผน 5	กรมราชทัณฑ์ กระทรวงยุติธรรม
30.นายนพดล	นักวิชาการคอมพิวเตอร์	สถาบันนิติวิทยาศาสตร์
31.นางสาวอัฐภิญญา จงเจริญ	นักศึกษาปริญญาโท	มหาวิทยาลัยมหิดล
32.นางสาวสุวรรณี รัฐวร	นักศึกษาปริญญาโท	มหาวิทยาลัยมหิดล

รายชื่อผู้เข้าร่วมประชุมสัมมนาเพื่อรายงานผลการศึกษาวิจัย
ครั้งที่ 3
“การปรับปรุงระเบียบกฎหมายให้เอื้อต่อการใช้เทคโนโลยีสารสนเทศ
ในกระบวนการยุติธรรม”
วันพฤหัสบดีที่ 19 เมษายน 2550 เวลา 9.00 น. – 14.00 น.
ณ ห้องแคทลียา โรงแรมรามาการ์เด้นส์ ถนนวิภาวดี กรุงเทพมหานคร

สำนักงานตำรวจแห่งชาติ

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.พ.ต.ท.นิติพันธ์ กนกเวชยันต์	รองผกก.ศูนย์ข้อมูลตรวจคนเข้าเมือง สตม.
2. ร.ต.อ.สุกิจ กัลยากาญจน์	รองสารวัตรฝ่ายอำนวยการ 4 กองบังคับการอำนวยการ
3.พ.ต.ท.ศราวุธ จิตระเบียบ	รองผกก.ผอ.บก.น4 บก. น4
4.พ.ต.อ. โฆษิต ปิมเจริญ	ผู้กำกับการศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ
5.ร.ต.อ.พงศ์ศักดิ์ วัฒนหฤทัย	นายเวร ผู้บังคับการ ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ
6. พ.ต.อ.สาธิต ชมภพ	รองผบก.ปศท. มก.ปศท.
7. พ.ต.ต.กฤษณะ พัฒนเจริญ	สว.กก.1 มก.ปศท. บก.1 บก.ปศท.
8. พ.ต.ท.ธเนศ ประทุมวัลย์	สว. ศว.มท.ปศท
9. พ.ต.อ. ปาน ตันตระกูล	นักวิทยาศาสตร์(สบ.5) กองพิสูจน์หลักฐาน
10. พ.ต.อ.บุญชัย ฤาชัยสา	นักวิทยาศาสตร์ (สบ 4) กองพิสูจน์หลักฐาน
11. พ.ต.อ.อภินันท์ เกตุษเฐียร	ผกก.กพป. กพป.
12. พ.ต.ท.วินัย ทับทอง	รอง ผกก.กพป. กพป.
13. พ.ต.อ. ประสิทธิ์ แจ่มดวง	ผู้กำกับฝ่ายอำนวยการ
14. พ.ต.ท.พจน์ ฟอร์ดี้	สว.กลุ่มงานผู้เชี่ยวชาญ ทว. สังกัดกลุ่มผู้เชี่ยวชาญทว.
15.พ.ต.ท.สังวาลย์ กฤษ์ศรีลักษณ์	รองผู้กำกับสอบสวน สน.สมเด็จเจ้าพระยา สถานีตำรวจสมเด็จเจ้าพระยา

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
16.พ.ต.ท.พิพัฒน์ บุญเพ็ชร์	รองผู้กำกับการสอบสวน สน.บุคคโล สถานีตำรวจบุคคโล
17.ร.ต.ท.วิโรจน์ ลี้กุล	พงส.ฯ ช่วยราชการงานคดี บก.น.3 กองบัญชาการตำรวจนครบาล
18.พ.ต.ท.วรลภษ์ สุวรรณเกษการ	รอง ผกก.(สส.)สน.บางขุนเทียน บก.น.9
19.พ.ต.ท.ทรงยศ ทองแท้	พงส.(สบ 3) สน.หนองแขม บก.น.9
20.พ.ต.ท.อภิชน เจริญผล	พนักงานสอบสวน (สบ2) กลุ่มงานสอบสวน บก.ป. กองบังคับการปราบปราม
21.พ.ต.ท.สมยศ ร่มสน	พนักงานสอบสวน (สบ3) กลุ่มงานสอบสวน บก.ป. กองบังคับการปราบปราม
22.พ.ต.อ.ชวลิต เลิศศักดิ์วิมาน	ผกก.ฝ.1 สท. กองสารนิเทศ สำนักงานตำรวจแห่งชาติ
23.ร้อยตรีสุทธิ พรรณรายณ์	พสพ. 8ว กลุ่มงานคดีความเห็นแย้ง กรมสอบสวนคดีพิเศษ กท.ยธ

สำนักงานอัยการสูงสุด

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.น.ส. จารุรัตน์ ศิริวงศ์วิบูลย์	อัยการประจำกอง สำนักงานอัยการพิเศษฝ่ายคดีภาษีอากร 1
1.น.ส. จารุรัตน์ ศิริวงศ์วิบูลย์	อัยการประจำกอง สำนักงานอัยการพิเศษฝ่ายคดีภาษีอากร 1
2.นายวิรัช ตรรกวาทการ	อัยการผู้เชี่ยวชาญ สำนักงานอัยการพิเศษฝ่ายคดีภาษีอากร 4
3.นายสุทธิสาร ภัทรรังษี	อัยการประจำกรม สนง.อัยการพิเศษฝ่ายอำนวยความยุติธรรมขั้นสอบสวน
4.นางอุไรวรรณ สถานานนท์	นักวิชาการคอมพิวเตอร์ 7 วช. ศูนย์เทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ส.
5.นายสืบพงศ์ โอภาพงพันธ์	อัยการประจำกรม สำนักงานอัยการพิเศษฝ่าย สถาบันกฎหมายอาญา

สำนักงานอัยการสูงสุด

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
6.นายเชิดศักดิ์ หิรัญศิริสมบัติ	อัยการพิเศษฝ่ายสารสนเทศ สำนักงานอัยการสูงสุด
7.นายชัยพร เกริกกุลธร	อัยการผู้เชี่ยวชาญ สำนักงานอัยการพิเศษฝ่าย แผนช่วยเหลือทางกฎหมาย สำนักงานคุ้มครอง สิทธิและช่วยเหลือทางกฎหมาย
8.นายนพดล พิเศษพงษา	นักวิชาการคอมพิวเตอร์ 5 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อส.
9.นางสาวอุษณิกา ชูจันทร์	นักวิชาการคอมพิวเตอร์ 3 ศูนย์เทคโนโลยีสารสนเทศและการสื่อ อส.
10.นายวิชิต คำภักดี	อัยการพิเศษฝ่ายคดียาเสพติด 3 สำนักงานคดียาเสพติด สำนักงานอัยการสูงสุด
11.นายนิวาส นิวาสวุฒิกิจ	อัยการพิเศษฝ่ายคดียาเสพติด 4 สำนักงานคดียาเสพติด สำนักงานอัยการสูงสุด
12.นางสาวแววรวี สังขพงษ์	อัยการผู้เชี่ยวชาญ สำนักงานอัยการพิเศษฝ่ายคดี ทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ 1
13.นายโอภาษ วโรภาษ	อัยการจังหวัดประจำกรม สำนักงานอัยการพิเศษ ฝ่ายคดีทรัพย์สินทางปัญญาและ การค้าระหว่างประเทศ 1

กระทรวงยุติธรรม

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.นายเฉลิมชนม์ แน่นหนา	หัวหน้ากลุ่มงานนิติกร กรมคุ้มครองสิทธิและเสรีภาพ
2.นายภตภัทร อสุธาวุฒิจารณ์	นักวิชาการยุติธรรม 6 กลุ่มพัฒนาระบบบริหาร กรมคุ้มครองสิทธิและเสรีภาพ
3.จ.ส.อ.ไวทย์ศญากรณ์ เจริญยิ่ง	นักวิชาการคอมพิวเตอร์ 3 กลุ่มงานเทคโนโลยีสารสนเทศและการสื่อสาร สถาบันนิติวิทยาศาสตร์

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
4.นายปรีชา โสวรรณี	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 8 ว. กรมพินิจฯ
5.นางรัชดาวรรณ ศิริไพบูลย์	นักวิชาการคอมพิวเตอร์ 8 ว. กรมพินิจฯ
6. นางสาววีณา คชาธาร	นิติกร 4 สำนักกฎหมาย สำนักงานปลัดกระทรวงยุติธรรม
7.นายปรีชา โสวรรณี	จ.วิเคราะห์นโยบายและแผน ส่วนพัฒนาระบบงาน สำนักพัฒนาระบบงานยุติธรรมเด็กฯ
8.พ.ต.ท.วิชิต อุปะละ	พนักงานสอบสวนคดีพิเศษ 8 ว.
9.นางสาวจิตติมา อุดมกุศลศรี	นิติกร 6ว. สำนักงาน ป.ป.ส.
10..พ.ต.ท.โพธิวัฒน์ ทิมอุดม	พสพ. ส ว. กลุ่มงานคดีความเห็นแย้ง กรมสอบสวนคดีพิเศษ กก บธ.

กระทรวงการคลัง

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.นายเฉลิมศักดิ์ เลิศวงศ์เสถียร	นักวิชาการคอมพิวเตอร์ 7 ว ศทส. กระทรวงการคลัง
2.นายปริญญา ปรีดีจารณท์	นักวิชาการคอมพิวเตอร์ 6 ศทส.กระทรวงการคลัง
3.นางสาวอัมพวัน ฉันทาภิรมย์สุข	ผู้อำนวยการกลุ่มงานกฎหมาย กลุ่มงานกฎหมาย สำนักปลัดกระทรวงการคลัง
4.นางสาวพรทิพย์ บุญทวีสุข	นิติกร 4 กลุ่มงานกฎหมาย สำนักปลัดกระทรวงการคลัง
5.นายวิษณุ ช้างทอง	นิติกร กลุ่มงานกฎหมาย สำนักปลัดกระทรวงการคลัง
6. นายบุญเลิศ วงษ์ญาติ	นักวิชาการคอมพิวเตอร์ 7 วช.กรมสรรพากร
7.นางสุกัญญา พานิชนก	นักวิชาการคอมพิวเตอร์ 7 วช. กรมสรรพากร
8.นางนิตยาภรณ์ ชมจุรัย	นักวิชาการคอมพิวเตอร์ 7 วช. กรมสรรพากร

สำนักงบประมาณ

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1. นางวรภัทรา รารศิริ	นิติกร 6ว. สำนักงบประมาณ
2.นายภุชพงศ์ ทัดปิยมะรมย์	ผอ.สำนักเทคโนโลยีสารสนเทศ สำนักงบประมาณ
3.นายจีระศักดิ์ เสมาทอง	นักวิชาการคอมพิวเตอร์ 4 สำนักงบประมาณ

กรมสรรพสามิต

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.นางสาวสิริลักษณ์ จริงจิตร	นักวิชาการคอมพิวเตอร์ 6 ว. ศูนย์สารสนเทศ กรมสรรพสามิต
2.นายวีระชัย วงศ์นันทนานนท์	นักวิชาการคอมพิวเตอร์ 6 ว. ศูนย์สารสนเทศ กรมสรรพสามิต

กรมธนารักษ์

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.นายอรุณชัย ภัรานนท์	นิติกร 7 ว. กลุ่มกฎหมายและระเบียบ 1 กลุ่มงานกฎหมาย กรมธนารักษ์
2.นายชรินทร เข็มราช	นิติกร 7 ว.กลุ่มกฎหมายและระเบียบ 1 กลุ่มงานกฎหมาย กรมธนารักษ์

กรมศุลกากร

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.นายพรวิทย์ อุทัยรัฐนิธิกุล	นักวิชาการคอมพิวเตอร์ 7 ว. กรมศุลกากร สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
2.นายจเร บุตรณิกลม	นักวิชาการคอมพิวเตอร์ 6 ว. กรมศุลการกร สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

กรมศุลกากร

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
3.นายธีรภัทร อ่อนจิตต์	นักวิชาการคอมพิวเตอร์ 6 ว. กรมศุลกากร สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
4.นายอนันต์ สิทธิ์ฤทธิ์	นิติกร 7 ว. สำนักกฎหมาย
5.นายศิริศักดิ์ ตั้วสุภากิจ	นิติกร 7 ว. สำนักกฎหมาย

ศาลรัฐธรรมนูญ/สนง.ศาล/ศาลปกครอง

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1. นายธนะชัย ผดุงธิติ	ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา สำนักงานยุติธรรม
2.นางจริยา อัศวรักษ์	ผู้อำนวยการศูนย์เทคโนโลยีและข้อมูลสารสนเทศ สำนักงานศาลรัฐธรรมนูญ
3.นายภาณุมาศ พฤกษ์อุดม	เจ้าหน้าที่ศาลรัฐธรรมนูญ 4 สถาบันรัฐธรรมนูญศึกษา สำนักงานศาลรัฐธรรมนูญ
4.นางสาวขนิษฐา อวยพร	นักวิชาการคอมพิวเตอร์ 7 วช. สำนักงานเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม
5.นางสาวสมฤดี ธัญญสิริ	ผู้อำนวยการสำนักพัฒนาระบบงานคดีปกครอง สำนักงานศาลปกครอง
6.นางปิยดา จิตต์จำนงค์	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ สำนักงานศาลปกครอง

กระทรวงต่าง ๆ

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
1.นางสาววรพรรณ อติชัย	นักวิชาการศึกษา 8 ว. สำนักนิติกร สำนักงานคณะกรรมการกรมอุดมศึกษา
2.นายอาจิน วิรชีพพัฒนา	ผู้อำนวยการสำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
3.นายกฤษฎิ์พงษ์ วารีมเจริญภาค	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 7 ว. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
4.นายสมิต วิโรจน์วรรณ	นักวิชาการคอมพิวเตอร์ 8 ลช. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.ศธ.
5.นายประวิทย์ เสียงผล	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงแรงงาน
6.นายเถกิง พีรนรวิชฐ์	ผู้อำนวยการกลุ่มงานกฎหมาย สำนักงานปลัดกระทรวงแรงงาน
7. นางสาวจุฑารัตน์ หนูผ่อง	นักวิชาการคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงแรงงาน
8. นางศศิธร หวังวรวุฒิ	นักวิชาการคอมพิวเตอร์ 8 วช. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการพัฒนาและความมั่นคงของมนุษย์
9. นางสาวจินดามณี นพรัตน์	นักวิชาการคอมพิวเตอร์ 6 ว. สำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี
10. นายหฤษฎ์ ปะสาทะ	เจ้าหน้าที่ประสานงานเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงวิทยาศาสตร์และเทคโนโลยี

กระทรวงต่าง ๆ

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
11.นางเมธินี เทพมณี	ผู้อำนวยการสำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
12.นางสมใจ ประเสริฐจีรังกุล	นักวิชาการคอมพิวเตอร์ 8 วช. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
13. นางสาวณิชาพร สุขเจริญ	นักวิชาการคอมพิวเตอร์ 5 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
14. นายณณฐ พันธ์ชาติ	นิติกร 7 ว. สำนักกฎหมาย สน. สำนักงานปลัดกระทรวงมหาดไทย
15.นายสุรพล มณีพงษ์	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวง กระทรวงการต่างประเทศ
16.นางสาวพรรณี อมรพิทักษ์กุล	นักวิชาการคอมพิวเตอร์ 7 วช. สำนักงานปลัดกระทรวงการต่างประเทศ
17. นายสายลม วุฒิสมบูรณ์	นักพัฒนาทรัพยากรบุคคล 7 ว. สำนักงานปลัดกระทรวงการต่างประเทศ
18. นางสาวมลฑา พราหมเภทย์	นิติกร 7 ว. กองนิติการ กรมการประกันภัย กระทรวงพาณิชย์
19. นายอัมพล มงคลอินทร์	นิติกร 6 ว. กองนิติการ กรมการประกันภัย กระทรวงพาณิชย์
20. นายเทอดไท ศรีอุประ	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 8 ว. สำนักงานสภาความมั่นคงแห่งชาติ
21. นายธนิน เกตุทอง	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 6ว. สำนักงานสภาความมั่นคงแห่งชาติ
22. นายสรรเพชญ แสงเนตรสว่าง	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 6 ว. ศต.
23.นายวิทเยนทร์ แสงห้าว	ผู้ช่วยผู้อำนวยการ ฝ่ายกฎหมายธุรกิจ บริษัท อสมท จำกัด (มหาชน)

กระทรวงต่าง ๆ

ชื่อ - สกุล	ตำแหน่ง/หน่วยงาน
24. นางสาวปณิศา เหลืองวรเมท	นักวิชาการคอมพิวเตอร์ 8 วช. สำนักงานสำนักปลัดสำนักนายกรัฐมนตรี
25. นายชำนัญ ชูโต	เจ้าหน้าที่วิเคราะห์นโยบายและแผน 8ว. สำนักงานสำนักปลัดสำนักนายกรัฐมนตรี

หน่วยงานอื่น ๆ

1.นางอุบล ชุมวิสูตร	นิติกร 7 ว. กองนิติการ สำนักงาน ก.พ.
2.นายทนงศักดิ์ สุขชนินทร์	ผู้บริหารระดับต้น สำนักเทคโนโลยีสารสนเทศ สำนักงาน กทช.
3.นายเขมชาติ ศุภนรำกุล	เจ้าพนักงาน ป.ป.ช.9 สำนักงานป.ป.ช.
4.นางสมพร ครุฑสาคร	เจ้าพนักงาน ป.ป.ช.8 สำนักงานป.ป.ช.
5.นางสาวอ้อย โชติธีรชัย	นักพัฒนาระบบราชการ 4 สำนักงานก.พ.ร.
6. นางสาวสุพรรณี สะมาแก้ว	นิติกร 5 สำนักงานการตรวจเงินแผ่นดิน
7. นางสาวกิติมา พันธุ์คำ	นิติกร 4 สำนักงานการตรวจเงินแผ่นดิน
8. นายธนันชัย โกมลเสน	นักการข่าว 7 ว.
9. นายอนันต์ ตระกูลอุดมสุข	นักการข่าว 7 ว.
10. พลตรี จักรินทร์ นาคชาติ	ตุลาการพระธรรมนูญ ประจำสำนักตุลาการทหาร กรมพระธรรมนูญ
11.พันโท นุรัช กองแก้ว	ประจำฝ่ายวิชาการ สำนักตุลาการทหาร กรมพระธรรมนูญ
12.นายยงเกียรติ อดิเศรษฐกุล	ผู้อำนวยการสำนักกฎหมายและคดี สำนักกฎหมายและคดี สนง.กกต.
13.นายอภิรัตน์ จันทนฤกษ์	ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ สำนักนโยบายและแผน สนง.กกต
14.น.อ.หญิงพงศ์พรพร ศรีสุวรรณ ธ.น.	นักวิชาการคอมพิวเตอร์ 8 วช. สำนักงานก.พ.
15.นายธชาคภิต สนธิ	จ.วิเคราะห์งานบุคคล 4 สำนักงานก.พ.

คณะทำงาน

ฐนันดร์ศักดิ์ บวรนันทกุล	หัวหน้าโครงการ
เฉลียว นครจันทร์	นักวิจัย
ณัฐพัชร จันทรสูตร	นักวิจัย
พนัญญา บวรนันทกุล	นักวิจัย
วีระสิทธิ์ บูรณะประภานนท์	นักวิจัย
ปิติพงษ์ เต็มเจริญ	นักวิจัย
ณัฐวิทย์ บูรณประภานนท์	นักวิจัย

คณะทำงาน

ฐนันดร์ศักดิ์ บวรนันทกุล สำเร็จปริญญาตรีทางภาษาอังกฤษ จากมหาวิทยาลัยศรีนครินทรวิโรฒและปริญญาตรีทางกฎหมายจากมหาวิทยาลัยรามคำแหง ปริญญาโททางปรัชญาและศาสนาเปรียบเทียบ โดยทุนจากมหาวิทยาลัยมหิดล ปริญญาโททางมานุษยวิทยา (Anthropology) จากมหาวิทยาลัยศิลปากร และปริญญาโททางกฎหมายธุรกิจจากมหาวิทยาลัยธรรมศาสตร์ ประกาศนียบัตรด้านกฎหมายสิ่งแวดล้อม จาก IUCN/UNEP ปริญญาเอก (Cand.) ด้านอาชญาวิทยา การบริหารงานยุติธรรมและสังคม มหาวิทยาลัยมหิดล เคยเป็นนักวิจัย รองผู้อำนวยการศูนย์ทรัพยากรมนุษย์ ปัจจุบันเป็นอาจารย์ประจำและกรรมการบริหารหลักสูตร อาชญาวิทยาและงานยุติธรรม คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล

เฉลียว นครจันทร์ สำเร็จปริญญาตรีทางกฎหมาย จากมหาวิทยาลัยธรรมศาสตร์ ปริญญาโททางกฎหมายธุรกิจระหว่างประเทศ จากจุฬาลงกรณ์มหาวิทยาลัย เคยเป็นนิติกร สำนักงานเร่งรัดพัฒนาชนบท กระทรวงมหาดไทย ทนายความ รองคณบดีคณะนิติศาสตร์ มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ คณะอนุกรรมการ คณะกรรมการผู้ทรงคุณวุฒิ ด้านกฎหมายและกรรมาธิการ ปัจจุบันดำรงตำแหน่งคณบดีคณะนิติศาสตร์ มหาวิทยาลัยณิวัฒนา

ณัฐพัชร จันทรสูตร สำเร็จปริญญาตรีทางกฎหมายจากมหาวิทยาลัยธรรมศาสตร์ ปริญญาโททางด้านกฎหมายธุรกิจระหว่างประเทศ จากจุฬาลงกรณ์มหาวิทยาลัย ปริญญาเอกทางด้านบริหารการศึกษา จากจุฬาลงกรณ์มหาวิทยาลัย ประกาศนียบัตรทางด้านทรัพย์สินทางปัญญาจากสหรัฐอเมริกา เคยเป็นนิติกร กระทรวงสาธารณสุข ทนายความ คณบดีคณะนิติศาสตร์ มหาวิทยาลัยเทคโนโลยีอุบลราชธานี คณบดีคณะนิติศาสตร์ มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ นักกฎหมายผู้เชี่ยวชาญทางด้านกฎหมายเทคโนโลยีสารสนเทศ ประจำศูนย์เทคโนโลยีและสารสนเทศแห่งชาติ (NETECH) ปัจจุบันเป็นผู้เชี่ยวชาญทางกฎหมายสำนักงานวิสาหกิจขนาดย่อม (SME)

พนัญญา บวรนันทกุล สำเร็จปริญาตรีทางด้านภาษาอังกฤษเพื่อการสื่อสาร จากมหาวิทยาลัยหอการค้าไทย ปริญญาโททางด้านรัฐประศาสนศาสตร์จากมหาวิทยาลัยมหิดล เคยทำงานด้านการบริหารในองค์กรเอกชน เป็นอาจารย์ผู้บรรยายพิเศษในมหาวิทยาลัยรัฐและเอกชนหลายแห่ง เป็นนักวิจัยอิสระ ปัจจุบันเป็นผู้จัดการภาค Mister Donut บริษัทเซ็นทรัลเรสตอรองส์กรุ๊ป จำกัด

วีระสิทธิ์ บูรณะประภานนท์ สำเร็จปริญญาตรีทางกฎหมาย จากมหาวิทยาลัยรามคำแหง ปริญญาโททางกฎหมายมหาชน จากมหาวิทยาลัยรามคำแหง ปริญญาเอกทางด้านกฎหมายมหาชน (Cand.) จากฝรั่งเศส เคยเป็นทนายความสำนักงาน Michael Law Office นักวิจัยอิสระ ปัจจุบัน เป็นเจ้าพนักงานคดี สำนักงานศาลปกครองกลาง กรุงเทพมหานคร

ปิติพงษ์ เต็มเจริญ สำเร็จปริญญาตรีทางกฎหมายจากมหาวิทยาลัยธรรมศาสตร์และปริญญาโททางด้านกฎหมายระหว่างประเทศ จาก American University สหรัฐอเมริกา ปริญญาโทด้านวิทยาศาสตร์สิ่งแวดล้อม จากสถาบันเทคโนโลยีแห่งเอเชีย(AIT) เคยเป็นสมาชิกสภาผู้แทนราษฎร หลายสมัย เป็นประธานกรรมาธิการและกรรมาธิการชุดต่างๆในสภาผู้แทนราษฎรและคณะทำงานด้านงานยุติธรรมและยาเสพติด และยังเป็นนักวิชาการอิสระ

ณัฐวิทย์ บูรณประภานนท์ สำเร็จปริญญาตรีทางวิศวกรรมคอมพิวเตอร์ และปริญญาโททางวิศวกรรมคอมพิวเตอร์ จากคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ เคยทำงานด้านการวางระบบเทคโนโลยีสารสนเทศในบริษัทยักษ์ใหญ่ด้านโทรคมนาคมและการสื่อสารหลายแห่ง ปัจจุบัน เป็นผู้จัดการฝ่ายวิศวกรรมระบบ บริษัท DTAC จำกัด มหาชน

OFFICE OF JUSTICE AFFAIRS