ปัญหาการจัดเก็บและการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เพื่อนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

Problems of Preservation and Accumulation of Traffic Data Used as Evidence in Case of Copyright Infringement on the Internet

ปัญหาการจัดเก็บ และการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ เพื่อนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

Problems of Preservation and Accumulation of Traffic Data Used as Evidence in Case of Copyright Infringement on the Internet

สุรเชษฐ ชาติชาคร

การค้นคว้าอิสระเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
มหาวิทยาลัยกรุงเทพ
ปีการศึกษา 2556

บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ
อนุมัติให้การค้นคว้าอิสระเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เรื่อง ปัญหาการจัดเก็บ และการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ เพื่อนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

ผู้วิจัย สุรเชษฐ ชาติชาคร

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษา _____
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

อาจารย์ที่ปรึกษาร่วม _____
(อาจารย์ไพบูลย์ อมรภิญโญเกียรติ)

ผู้เชี่ยวชาญ _____
(อาจารย์ปัจฉิมา ธนสันติ)

_____
(ผู้ช่วยศาสตราจารย์ ดร.ศิวพร หวังพิพัฒน์วงศ์)
คณบดีบัณฑิตวิทยาลัย
2 กันยายน 2557

สุรเชษฐ ชาติชาคร. ปริญญานิติศาสตรมหาบัณฑิต, กันยายน 2557, บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ.
ปัญหาการจัดเก็บและการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เพื่อนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต (120 หน้า)
อาจารย์ที่ปรึกษา: ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ

บทคัดย่อ

ปัจจุบันการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเกิดขึ้นอย่างแพร่หลาย แต่การได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานสำคัญแต่กลับพบว่ายังมีปัญหาอยู่ในหลายประการ การวิจัยนี้จึงมีความประสงค์ในการศึกษาปัญหาการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต โดยประเด็นการจัดเก็บข้อมูลจราทางคอมพิวเตอร์ ได้แก่ ผู้มีหน้าที่จัดเก็บ วิธีการจัดเก็บ ระยะเวลาการจัดเก็บ และการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ โดยการวิจัยทำโดยการทบทวนวรรณกรรม แบบศึกษาเปรียบเทียบกฎหมายอเมริกา และกฎหมายยุโรป

จากการวิจัยพบว่าปัญหาเกี่ยวกับการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เกิดขึ้นจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้เป็นอำนาจของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติดังกล่าวเป็นการเฉพาะ อีกทั้งข้อจำกัดที่ให้ใช้อำนาจเรียกข้อมูลจราจรทางคอมพิวเตอร์ได้เฉพาะความผิดตามพระราชบัญญัตินี้เท่านั้น ส่งผลให้เจ้าหน้าที่ตำรวจตามประมวลกฎหมายวิธีพิจารณาความอาญาผู้มีหน้าที่รับผิดชอบในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตไม่สามารถหมายเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้มีหน้าที่จัดเก็บได้ สำหรับส่วนของการจัดเก็บ พบว่ากฎหมายไทยยังไม่มีแบบแผนที่ชัดเจนดังเช่นมาตรฐานการจัดเก็บข้อมูลสารสนเทศแบบ ISO27001:2013 และการบริหารจัดการข้อมูลสารสนเทศแบบ COBIT 5 และพบว่าระยะเวลาการจัดเก็บไม่สามารถตอบสนองต่อการสืบสวนสอบสวนคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต งานวิจัยนี้มีข้อเสนอแนะ คือ (1) กำหนดให้ความผิดเกี่ยวกับลิขสิทธิ์บนอินเทอร์เน็ตเป็นฐานความผิดหนึ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (2) เพิ่มระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์อย่างน้อย 180 วันและให้มีการเยียวยาค่าใช้จ่ายเพิ่มเติมกรณีมีคำสั่งให้จัดเก็บเกินกว่าระยะเวลาที่กฎหมายกำหนด และ (3) ตั้งหน่วยงานกลางของรัฐบาลเพื่อรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้สำหรับคดีที่อาจกระทบต่อความมั่นคงของประเทศ

คำสำคัญ: ลิขสิทธิ์บนอินเทอร์เน็ต, ข้อมูลจราจรทางคอมพิวเตอร์, การจัดเก็บ, การได้มา

Chatchakorn, S. LL.M., September 2014, Graduate School, Bangkok University.
Problems of Preservation and Accumulation of Traffic Data Used as Evidence in Case of Copyright Infringement on the Internet (120 pp.)
Advisor: Asst.Prof.Aunya Singsangob, Ph.D.

ABSTRACT

Nowadays, Copyright infringement on the internet is becoming widespread. Still, there are many problems related to the accumulation traffic data, the most important evidence, still has many problems. Thus, this dissertation mainly focus on studying problems of preservation and accumulation of traffic data used as evidence in case of copyright infringement on the internet focusing on the issues of accumulation of traffic data includes the person who has duty to preservation traffic data, means and period of preservation traffic data and means of accumulation traffic data. The research process will be undertaken by studying literature review and comparative law among Thai, American and European.

This research shows that problems of accumulation traffic data were occur since Computer crime act B.E. 2550 which authorize an official under the act to call traffic data from service provider if there is any reasonable cause to believe that a violation of the act has occurred. Thus, the power to call data of the police officer, who in charge of copyright infringement on the internet case, is restrict to only general evidence. Besides, another problems of preservation of traffic data in Thailand is that there is no a clear standard system of preservation traffic data as ISO 27001/2013 standard and COBIT 5 : system of management of computer data, moreover, the period of traffic data storage is not conform with the copyright infringement on the internet. From the result, this research suggested as following:

(1) Enact a copyright infringement on the internet to be one of perpetration of an offence under computer crime act B.E. 2550.

(2) Extend the period of traffic data storage for at least 180 days from the date on which the data is input into a computer system and restrict a compensation

to service provider for any loss or damages incurred if an official order to store data longer than 180 days.

(3) Establish a new government organization to preservation traffic data in order to use in national security case.

Keywords: Copyright on the Internet, Traffic Data, Preservation, Accumulation

กิตติกรรมประกาศ

การวิจัยเฉพาะบุคคลฉบับนี้สำเร็จลุล่วงไปได้ด้วยดีด้วยความกรุณาของท่านคณาจารย์ ผู้เขียนจึงขอกราบขอบพระคุณท่าน ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ ท่านอาจารย์ไพบูลย์ อมรภิญโญเกียรติ และท่านอาจารย์ปัจฉิมา ธนสันติ ที่ได้ให้ความกรุณาสละเวลาโดยรับเป็นอาจารย์ที่ปรึกษา และคอยเอาใจใส่ให้คำแนะนำในส่วนต่าง ๆ ของการวิจัยเฉพาะบุคคลฉบับนี้ตลอดระยะเวลาหลายปี

และผู้เขียนขอขอบคุณบิดา มารดา สำหรับกำลังใจ รวมถึงบรรดาเพื่อนร่วมรุ่นและเพื่อนต่างมหาวิทยาลัยที่คอยให้ความช่วยเหลือในด้านข้อมูลเพิ่มเติมรวมถึงกำลังใจ ตลอดระยะเวลาการจัดทำการวิจัยเฉพาะบุคคล

หากในอนาคตประโยชน์ของการวิจัยเฉพาะบุคคลฉบับนี้จะพึงมีอย่างใด ๆ ผู้เขียนขอมอบบูชาพระคุณบิดา มารดาตลอดจนครูบาอาจารย์ที่ได้ประสิทธิประสาทวิชาการให้ รวมตลอดถึงผู้มีพระคุณทั้งหมดที่ได้เอ่ยนามไปแล้วและที่ไม่สามารถเอ่ยนามได้ ณ ที่นี้ ส่วนข้อผิดพลาดหรือข้อบกพร่องที่อาจเกิดขึ้นจากการวิจัยเฉพาะบุคคลในครั้งนี้ผู้เขียนใคร่ขอน้อมรับไว้แต่เพียงผู้เดียว

สุรเชษฐ ชาติชาคร

สารบัญ

สารบัญ (ต่อ)

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

ในปัจจุบันเทคโนโลยีมีการพัฒนาอย่างรวดเร็ว การพัฒนาทางเศรษฐกิจและเทคโนโลยี ส่งผลกระทบต่อการพิสูจน์ความผิดของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ตเป็นสื่อในการกระทำความผิด ระบบอินเทอร์เน็ตมีการพัฒนาจนแพร่หลายและสามารถเข้าถึงได้ง่าย ด้วยลักษณะที่สำคัญคือ เป็นสื่อในการติดต่อสื่อสารที่มนุษย์สามารถใช้ติดต่อหรือเข้าสู่ข้อมูลเดียวกันได้แม้อยู่คนละซีกโลก ทำให้เกิดสังคมใหม่ที่เรียกว่าสังคมออนไลน์หรือสังคมบนโลกอินเทอร์เน็ต กิจกรรมของสังคมบนอินเทอร์เน็ตจะเป็นการนำเสนอข้อมูล ใหม่ ๆ แลกเปลี่ยนข้อมูลความคิดเห็นต่าง ๆ ผ่านช่องทางการแลกเปลี่ยนข้อมูลและนำเสนอข้อมูลที่มีความรวดเร็วในการเข้าถึงและมีการแพร่กระจายข้อมูลทั่วโลก ทำให้เกิดช่องทางของการละเมิดทรัพย์สินทางปัญญาในรูปแบบใหม่ขึ้น คือการละเมิดลิขสิทธิ์อินเทอร์เน็ต โดยจากผลการรวบรวมข้อมูลของบริษัท Motion Picture of America[1] พบว่าหนึ่งในสี่ของการใช้งานอินเตอร์เน็ตเป็นการละเมิดทรัพย์สินทางปัญญาบนอินเทอร์เน็ต ซึ่งส่งผลกระทบต่อเจ้าของลิขสิทธิ์ต่าง ๆ อย่างมาก สำหรับประเทศไทยการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตปรากฏให้เห็นอยู่อย่างแพร่หลายไม่ว่าจะเป็นการเปิดเว็บไซต์ให้ดาวโหลดงานอันละเมิดลิขสิทธิ์ เช่น 4 Shared หรือ การนำผลงานมาเผยแพร่โดยไม่ได้รับอนุญาติผ่านทางเว็บไซต์เป็นต้น

ปัจจุบันประเทศไทยถูกสำนักผู้แทนการค้าสหรัฐ (USTR) ใช้มาตราการตามมาตรา 301 พิเศษ แห่งกฎหมาย Omnibus Trade and Competitiveness Act of 1988 [2] จัดสถานะทางการค้าของไทยอยู่ในบัญชีประเทศที่ต้องจับตามองเป็นพิเศษ (PWL) เรื่องทรัพย์สินทางปัญญามาแล้ว 5 ปี ทำให้ไทยต้องถูกตัดสิทธิพิเศษทางการค้าจากสหรัฐฯ[3] และในปี พ.ศ. 2558 ที่จะมีการเริ่มต้นระบบประชาคมเศรษฐกิจอาเซียน จะมีการลงทุนจากต่างชาติและการซื้อขายแลกเปลี่ยนสินค้ากันมากขึ้น

---

[1] Motion Picture Association of America, **The cost of content theft by the number** [Online], 12 September 2013. Available from http://msl1.mit.edu/furdlog/docs/2011-08_mpaa_infographic.pdf.

[2] จักรกฤษณ์ ควรพจน์, **การตอบโต้ทางการค้าของสหรัฐฯ ผ่านมาตรา 301 และสิทธิจีเอสพี: ศึกษากรณีการบังคับใช้สิทธิตามสิทธิบัตรยาของไทย,** (กรุงเทพฯ: โครงการ WTO Watch, 2551), 10.

[3] “DSI จับเครือข่ายใช้สื่อออนไลน์ขายสินค้าละเมิดลิขสิทธิ์”, **เดลินิวส์** [Online], 17 ตุลาคม 2555. แหล่งที่มา tnews.teenee.com/crime/86914.html.

ประกอบกับแนวโน้มของการใช้อินเทอร์เน็ตในการติดต่อสื่อสารในปัจจุบัน ย่อมส่งผลให้เกิดงานอันมีลิขสิทธิ์ในรูปแบบออนไลน์มากมายที่จะเข้าสู่ประเทศไทย และทำให้เศรษฐกิจของประเทศพัฒนาและเติมโตขึ้นมาก แต่หากไม่มีกระบวนการที่จะคุ้มครองลิขสิทธิ์และยังไม่มีการปราบปรามอย่างมีประสิทธิภาพ ยังคงให้มีการละเมิดลิขสิทธิ์อย่างแพร่หลายอยู่ดังเช่นปัจจุบัน ต่างชาติก็คงจะเลี่ยงการมาลงทุน หรือการนำเทคโนโลยีและลิขสิทธิ์ใหม่ ๆ เข้ามายังประเทศไทย และจะทำให้เศรษฐกิจของประเทศถดถอยไม่สามารถก้าวทันประเทศเพื่อนบ้านได้

การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นการกระทำโดยใช้อินเทอร์เน็ตเป็นสื่อกลางในการกระทำความผิด พยานหลักฐานสำคัญที่เกิดขึ้นจากการกระทำดังกล่าวคือ ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ที่กระทำการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต เพื่อสามารถหาตัวผู้กระทำความผิดและเป็นหลักฐานสำคัญในการมัดตัวผู้กระทำความผิดเพื่อลงโทษต่อไปได้ ซึ่งข้อมูลเหล่านี้รวมเรียกว่า ข้อมูลจราจรทางคอมพิวเตอร์ อันมีลักษณะของข้อมูลที่เกิดขึ้นแล้วต้องมีการจัดเก็บไว้ไม่เช่นนั้นข้อมูลดังกล่าวจะสูญหายไป โดยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้มีผู้มีหน้าที่ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อให้สามารถมีพยานหลักฐานในการนำตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์มาลงโทษ แต่ในส่วนของกฎหมายลิขสิทธิ์ไม่มีกฎหมายกำหนดไว้เป็นการเฉพาะว่าบุคคลใดมีหน้าที่ต้องเก็บข้อมูลเหล่านี้ไว้ แม้ผู้ให้บริการอินเทอร์เน็ตมีหน้าที่จัดเก็บข้อมูลเหล่านี้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อยู่แล้ว แต่ก็จัดเก็บไว้ด้วยวัตถุประสงค์เพื่อให้พนักงานเจ้าหน้าที่สามารถขอได้สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นหลัก ในการขอข้อมูลจราจรทางคอมพิวเตอร์ก็มีการกำหนดพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ให้มีอำนาจเป็นการเฉพาะพนักงานสอบสวนตามกฎหมายอาญาไม่มีอำนาจจะขอข้อมูลดังกล่าวได้

ดังนั้น เมื่อมีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตอันไม่ใช่ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงทำให้การสืบสวนสอบสวนคดีประสบอุปสรรคในการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์มาเป็นพยานหลักฐาน โดยในทางปฏิบัติพบว่ามีการตีความการละเมิดลิขสิทธิ์ให้เป็นความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การดัดแปลงงานอันมีลิขสิทธิ์ เมื่อมีการกระทำต่อข้อมูลที่มีลิขสิทธิ์ซึ่งมีลักษณะเป็นข้อมูลคอมพิวเตอร์ ก็จะดำเนินคดีในฐานะแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของบุคคลอื่นโดยมิชอบและทำให้เกิดความเสียหาย ซึ่งมีบทลงโทษและหลักการในการพิจารณาแตกต่างจากกฎหมายลิขสิทธิ์ จึงเห็นได้ว่าไม่ตรงตามเจตนารมณ์ของกฎหมายเกี่ยวกับการลงโทษผู้กระทำละเมิดลิขสิทธิ์ และจากการศึกษาขั้นตอนการได้มาซึ่งพยานหลักฐานในคดีละเมิดลิขสิทธิ์ พบว่าไม่มีกฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการ

สืบสวนสอบสวนคดีลิขสิทธิ์ที่ให้อำนาจพนักงานเจ้าหน้าที่ในการสืบสวนไว้เป็นการเฉพาะ จึงเป็นอำนาจของพนักงานสืบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยสำนักงานตำรวจแห่งชาติได้มอบหมายงานที่เกี่ยวข้องกับคดีละเมิดทรัพย์สินทางปัญญาให้เป็นหน้าที่ของ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) และสำหรับคดีพิเศษ กรมสืบสวนคดีพิเศษ (DSI) ได้มอบหมายให้ สำนักคดีทรัพย์สินทางปัญญา (สคป.) มีอำนาจในการสืบสวนคดีละเมิดทรัพย์สินทางปัญญาที่เกี่ยวข้องกับแหล่งผลิต หรือแหล่งที่เก็บสินค้าละเมิดทรัพย์สินทางปัญญา แม้ทั้งสองหน่วยงานข้างต้นจะมีการกำหนดหน่วยพิเศษสำหรับคดีทรัพย์สินทางปัญญา แต่สำหรับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นเรื่องที่ต้องใช้ความรู้ความเชี่ยวชาญทางเทคโนโลยีมากกว่าคดีละเมิดลิขสิทธิ์ทั่วไป เพื่อให้เกิดประสิทธิภาพในการปราบปรามผู้กระทำความผิด อีกทั้งในการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ซึ่งเป็นพยานหลักฐานสำคัญจะต้องมีอำนาจเฉพาะที่กฎหมายให้ไว้เท่านั้น ซึ่งพนักงานสืบสวนทั่วไปไม่มีอำนาจดังกล่าว และทั้งสององค์กรดังกล่าวก็มิได้มีการผ่านการอบรมหลักสูตรของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่จะสามารถปฏิบัติหน้าที่ดังเช่นพนักงานเจ้าหน้าที่ดังกล่าวได้

นอกจากนั้น ข้อมูลจราจรทางคอมพิวเตอร์ที่เป็นพยานหลักฐานสำคัญของการละเมิดลิขสิทธิ์อินเทอร์เน็ต มีลักษณะของข้อมูลที่สามารถแก้ไขเปลี่ยนแปลงได้ง่ายหากไม่มีระบบป้องกันหรือรักษาความปลอดภัยของข้อมูล ดังนั้น วิธีการจัดเก็บ ตลอดจนการได้มาซึ่งพยานหลักฐาน จนถึงชั้นพิจารณาคดีจะต้องมีขั้นตอนที่มีมาตรฐานเพื่อให้พยานหลักฐานนั้นมีความถูกต้องแท้จริง มีความน่าเชื่อถือ ซึ่งประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการ พ.ศ. 2550 ข้อ 8 วางหลักการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ว่าผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย โดยเก็บในสื่อที่สามารถรักษาความถูกต้องแท้จริง มีการเก็บรักษาความลับของข้อมูล รวมถึงชั้นความลับในการเข้าถึงข้อมูล โดยข้อมูลนั้นจะต้องสามารถระบุผู้ใช้บริการเป็นรายบุคคลได้ ซึ่งเป็นว่าเป็นเพียงหลักการวางกรอบในการจัดเก็บโดยไม่มีต้นแบบมาตรฐานที่แต่ละผู้ให้บริการจะต้องปฏิบัติตามหรือยึดถือและปฏิบัติให้เป็นแนวทางเดียวกัน จึงส่งผลให้การกำหนดมาตรฐานการจัดเก็บขึ้นอยู่กับผู้ให้บริการแต่ละรายว่าจะกระทำแบบใด ซึ่งผู้ให้บริการรายใหญ่อาจจะมีนวัตกรรมทางการจัดเก็บที่ดีเยี่ยม แต่ผู้ให้บริการรายย่อยอาจไม่มีข้อมูลเพียงพอเกี่ยวกับมาตรฐานการจัดเก็บและอาจส่งผลให้เกิดความบกพร่องหรือสูญหายซึ่งข้อมูลจราจรทางคอมพิวเตอร์ที่จะนำมาใช้เป็นพยานหลักฐาน ซึ่งประเทศไทยยังไม่มีการกำหนดหลักการหรือขั้นตอนในการพิสูจน์ดังกล่าวให้ชัดเจน ทำให้เมื่อนำข้อมูลจราจรทางคอมพิวเตอร์มาเป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต หากถูกโต้แย้งเรื่องความ

ถูกต้องแท้จริงในมาตรฐานการจัดเก็บ ย่อมเกิดปัญหาว่ามาตรฐานการจัดเก็บแบบใดที่ถือว่าถูกต้องและพยานหลักฐานที่หามาได้นั้นจะมีความเชื่อถือได้มากน้อยเพียงใด

นอกจากมาตราฐานการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แล้ว ระยะเวลาในการจัดเก็บเป็นสิ่งสำคัญเช่นเดียวกัน เนื่องจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต เป็นการกระทำที่เกิดขึ้นได้รวดเร็ว แต่บางครั้งอาจใช้เวลากว่าจะพบการกระทำความผิด หรือต้นตอที่กระทำความผิด โดยปัจจุบัน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้มีการจัดเก็บเป็นระยะเวลา 90 วัน ซึ่งหากเป็นการกระทำละเมิดที่ซับซ้อนผ่านหลายช่องทาง การดำเนินการสืบสวนกว่าจะพบต้นตอของการกระทำความผิดอาจต้องใช้ระยะเวลามากกว่า 90 วันอันทำให้ไม่มีข้อมูลดังกล่าวจัดเก็บอยู่และส่งผลให้ไม่สามารถหาข้อมูลต้นตอของการกระทำความผิดเพื่อเป็นหลักฐานเชื่อมไปยังผู้กระทำความผิดตัวจริง และทำให้ไม่สามารถนำตัวผู้กระทำความผิดมาดำเนินคดีต่อไปได้

เมื่อกฎหมายลิขสิทธิ์ของไทยในปัจจุบันยังไม่มีการแก้ไขเปลี่ยนแปลงประการใด ทั้งที่การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้เกิดขึ้นอย่างแพร่หลาย อีกทั้งพยานหลักฐานที่เกิดจะอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เป็นส่วนใหญ่ ทำให้เกิดปัญหาเรื่องการจัดเก็บ การรวบรวมพยานหลักฐานและความน่าเชื่อถือของพยานหลักฐานดังกล่าวที่จะใช้ในการพิจารณาคดี ซึ่งปัจจุบันไม่มีกฎหมายทรัพย์สินทางปัญญาของไทยฉบับใดที่บัญญัติเกี่ยวกับอำนาจในการสืบสวนสอบสวนไว้ รวมถึงไม่มีการกำหนดหลักเกณฑ์เฉพาะเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต ทั้งที่ต้องใช้ความรู้ในทางเทคโนโลยีมากกว่าการตัดสินคดีทั่วไป ผู้เขียนจึงมุ่งศึกษาเพื่อให้ถึงปัญหาของการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต ว่าอุปสรรคที่มีมากน้อยเพียงใดและจะมีแนวทางในการแก้ไขเพื่อให้สามารถ ป้องกันและปราบปรามการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ และเป็นแนวทางในการพัฒนากฎหมายลิขสิทธิ์ของไทยให้เท่าทันเทคโนโลยีและการพัฒนาเศรษฐกิจในอนาคต

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาข้อมูลจราจรทางคอมพิวเตอร์ที่เกิดจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.2.2 เพื่อศึกษาการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.2.3 เพื่อศึกษาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.2.4 เพื่อศึกษาความน่าเชื่อถือและลักษณะของข้อมูลจราจรทางคอมพิวเตอร์ที่สามารถนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.2.5 เพื่อศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายอเมริกาและสหภาพยุโรป เกี่ยวกับการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.3 สมมติฐาน

การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตมีความแตกต่างจากการละเมิดลิขสิทธิ์โดยทั่วไป เพราะมีส่วนที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ต ที่ใช้ในการเชื่อมต่อข้อมูลและทำให้เกิดการกระทำความผิดขึ้นได้ โดยการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตของไทยยังไม่มีการกล่าวถึงหรือแก้ไขให้มีความครอบคลุมความผิดใหม่แต่อย่างใด อีกทั้งพยานหลักฐานสำคัญสำหรับการกระทำเกิดขึ้นในรูปแบบของข้อูลจราจรทางคอมพิวเตอร์ ซึ่งต้องใช้ความเชี่ยวชาญและอำนาจเฉพาะตามที่กฎหมายให้ไว้เท่านั้นในการรวบรวมเพื่อให้ข้อมูลมีความถูกต้องแท้จริงและเป็นพยานหลักฐานที่ได้มาโดยชอบด้วยกฎหมายได้ หากมีการศึกษาถึงปัญหาและอุปสรรคของการจัดเก็บและการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เพื่อนำไปใช้ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต และเปรียบเทียบกับกฎหมายของต่างประเทศ จะทำให้สามารถวางกฎเกณฑ์และพัฒนากฎหมายให้มีมาตรการในการป้องกันและปราบปรามการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้อย่างมีประสิทธิภาพมากขึ้น

1.4 ขอบเขตการศึกษา

การวิจัยนี้มุ่งศึกษาเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตโดยศึกษาจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กฎหมายที่เกี่ยวกับการนำสืบพยานหลักฐาน และเปรียบเทียบกฎหมายเกี่ยวกับลิขสิทธิ์และคอมพิวเตอร์ในประเทศสหรัฐอเมริกาและสหภาพยุโรปเพื่อวิเคราะห์ถึงปัญหาการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.5 คำจำกัดความ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

1.6 ระเบียบวิธีวิจัย

การวิจัยนี้ใช้วิธีวิจัยเชิงเอกสารโดยการรวบรวมเอกสาร หนังสือกฎหมาย ตำรา วิทยานิพนธ์ คำพิพากษา ที่เกี่ยวข้องกับเรื่องที่ทำการวิจัย ทั้งของประเทศไทย และต่างประเทศศึกษาเอกสารหรือกฎหมายที่รวบรวมดังกล่าว รวมถึงเรื่องที่เคยมีการศึกษามาก่อนในอดีตอย่างเป็นระบบ โดยทำการวิเคราะห์ข้อมูลดังกล่าวด้วยทฤษฎี แนวคิดของนักนิติศาสตร์ หรือแนวคิดทางกฎหมายเพื่อให้เห็นถึงแนวทางการพัฒนากฎหมายลิขสิทธิ์ให้มีประสิทธิภาพเท่าทันการพัฒนาของเทคโนโลยีได้

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.7.1 เข้าใจลักษณะเฉพาะของข้อมูลจราจรทางคอมพิวเตอร์ที่เกิดจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1.7.2 เข้าใจปัญหาและอุปสรรคในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตของกฎหมายไทย กฎหมายอเมริกา และกฎหมายสหภาพยุโรป

1.7.3 เข้าใจปัญหาและอุปสรรคของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์ของกฎหมายไทย กฎหมายอเมริกา และกฎหมายสหภาพยุโรป

1.7.4 ทราบถึงแนวทางที่เหมาะสมในการแก้ไขปัญหาและอุปสรรคในการได้มา และการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์ของไทย

1.7.5 ทราบถึงแนวทางที่เหมาะสมในการป้องกันและปราบปรามการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

บทที่ 2
การละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

การละเมิดลิขสิทธิ์บนอินเทอร์เน็ต จะเกิดขึ้นได้ต้องมีการเชื่อมต่อผ่านระบบอินเทอร์เน็ตโดยคอมพิวเตอร์หรืออาจเป็นอุปกรณ์อิเล็กทรอนิกส์อื่น โดยหลักฐานที่เกิดขึ้นจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตที่สำคัญคือข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งบอกได้ว่าต้นทางและปลายทางในการเชื่อมต่ออินเทอร์เน็ตและกระทำความผิดเป็นจุดใด และกระทำโดยอุปกรณ์อิเล็กทรอนิกส์หรือคอมพิวเตอร์เครื่องใดสืบต่อเชื่อมโยงให้สามารถสืบสวนจากการกระทำความผิดไปหาผู้กระทำผิดได้ ข้อมูลจราจรทางคอมพิวเตอร์จึงมีความสำคัญอย่างยิ่งในการใช้เป็นพยานหลักฐานของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตดังนี้

1) ปัจจุบันการติดต่อสื่อสารได้พัฒนาอย่างทั่วถึง และการเชื่อมต่ออินเทอร์เน็ตสามารถกระทำได้ผ่านอุปกรณ์ต่าง ๆ มากกว่าทำได้เพียงแค่บนคอมพิวเตอร์ จึงสามารถเชื่อมต่อไปยังอินเทอร์เน็ตได้ทุกสถานที่ เช่นเดียวกันกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตย่อมสามารถกระทำได้ทุกสถานที่เช่นกัน การที่ข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานสำคัญสำหรับการสานต่อว่าใครกระทำการเชื่อมต่ออย่างใด ย่อมช่วยให้การร้องทุกข์ กล่าวโทษสามารถกระทำได้โดยง่ายขึ้นว่ามีการละเมิดลิขสิทธิ์เกิดขึ้นจริง เพราะอย่างน้อยก็มีหลักฐานอ้างอิงได้ว่าผู้กระทำความผิด เช่น ละเมิดลิขสิทธิ์โดยการทำซ้ำ เผยแพร่ต่อสาธารณะชนหรือดัดแปลงโดยไม่ได้รับอนุญาตอันทำให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์ มีการกระทำจากแหล่งใด และสามารถสืบเสาะหาตัวผู้กระทำความผิดได้ง่ายขึ้น ส่งผลให้ผู้สร้างสรรค์เกิดความมั่นใจในการสร้างสรรค์ผลงานที่อาจเกิดการเผยแพร่ในทางอินเทอร์เน็ตได้มากขึ้น

2) ข้อมูลจราจรทางคอมพิวเตอร์เป็นเบาะแสพื้นฐานที่จำเป็นต้องมีสำหรับการสืบสวนสอบสวนคดีความผิดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต คือ ไอพีแอดเดรส ซึ่งเป็นตัวบ่งชี้ผู้ต้องสงสัย และการสืบสวนจึงขยายผลจากไอพีแอดเดรส อันทำให้ทราบถึงที่ตั้งของผู้ต้องสงสัย อีกทั้งยังสามารถขยายไปถึงเครือข่ายที่เกี่ยวข้องกับผู้ต้องสงสัยได้ด้วย อาจกล่าวได้ว่า ไอพีแอดเดรสเป็นหลักฐานตั้งต้นที่สำคัญมาก นอกจากนั้น ข้อมูลจราจรทางคอมพิวเตอร์สำคัญอีกประการคือ ข้อมูลรูปแบบการกระทำบนระบบอินเทอร์เน็ต ว่าเป็นลักษณะใด เพื่อสามารถปรับกับบทความผิดของผู้กระทำในการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้ ซึ่งหากไม่มีข้อมูลดังกล่าว ก็ไม่สามารถดำเนินการสืบสวนสอบสวนคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตให้ไปถึงตัวผู้กระทำความผิดได้

3) ข้อมูลจราจรทางคอมพิวเตอร์เกิดขึ้นในทุกจุดของการสื่อสารข้อมูลบนระบบคอมพิวเตอร์และอินเทอร์เน็ต โดยตามกฎหมายผู้ให้บริการเชื่อมต่ออินเทอร์เน็ตและผู้ให้บริการที่เกี่ยวกับระบบคอมพิวเตอร์ในการติดต่อสื่อสาร จะจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ ดังนั้น แม้ผู้กระทำ

ความผิดจะลบข้อมูลการกระทำบนเครื่องของตัวเองและเครื่องผู้เสียหายออกทั้งหมด แต่ว่าการเชื่อมต่อที่เป็นหลักฐานข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บโดยผู้ใช้บริการไม่สามารถถูกลบได้โดยผู้กระทำความผิด

4) ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดและนิยามขึ้น ซึ่งแม้พระราชบัญญัติดังกล่าวมิได้มีการกล่าวถึงการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต แต่ในทางปฏิบัติย่อมมีความเกี่ยวข้องกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตด้วย เพราะมีการติดต่อสื่อสารของระบบคอมพิวเตอร์ และมีการจัดเก็บไว้โดยผู้ให้บริการ ดังนั้น การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตจึงสามารถหาพยานหลักฐานได้โดยอาศัยอำนาจของศาลเพื่อขอข้อมูลจากผู้ให้บริการ แต่ทั้งนี้ ไม่สามารถอาศัยอำนาจพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ได้หากไม่ได้มีความเกี่ยวข้องกับความผิดตามพระราชบัญญัตินี้

เห็นได้ว่าข้อมูลจราจรทางคอมพิวเตอร์มีความสำคัญอย่างยิ่งสำหรับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเพื่อจะเป็นหลักฐานสำคัญสำหรับการนำไปสู่ตัวผู้ต้องสงสัยและผู้กระทำความผิดต่อไป ซึ่งหากไม่มีข้อมูลดังกล่าว หลักฐานเกี่ยวกับการละเมิดบนอินเทอร์เน็ตก็ไม่สามารถย้อนกลับไปหาผู้กระทำความผิดได้ ซึ่งในบทนี้จะได้กล่าวรายละเอียดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตและหลักเกณฑ์รวมถึงแนวทางปฏิบัติในการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

2.1 การละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

2.1.1 สถานการณ์ของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

2.1.1.1 สถานการณ์ของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตในต่างประเทศ

ในปัจจุบันโลกดิจิตอลและเศรษฐกิจเชื่อมโยงกันอย่างแนบแน่น โดยเฉพาะตั้งแต่ปี 1990 เทคโนโลยีที่เอื้อการถ่ายเทข้อมูลทำให้เกิดการลงทุนอย่างกว้างขวางอันส่งผลกระทบต่อการขยายตัวทางเศรษฐกิจอย่างมีนัยยะสำคัญ ไม่ว่าจะเป็นภาคเอกชน หรือภาครัฐต่างล้วนได้รับประโยชน์จากการใช้อินเทอร์เน็ตอย่างแพร่หลาย ความนิยมอย่างล้นหลามของอินเทอร์เน็ตและธุรกิจบนหน้าอินเทอร์เน็ตทั้งหลายนี้ทำให้เกิดรูปแบบการค้าแบบใหม่ขึ้น ซึ่งสิ่งเหล่านี้ย่อมมีผลกระทบต่อวงการกฎหมายโดยเฉพาะอย่างยิ่งกฎหมายที่เกี่ยวข้องกับการคุ้มครองลิขสิทธิ์บนอินเทอร์เน็ต ที่จะต้องมีการพัฒนาและให้สามารถครอบคลุมกับความผิดใหม่ ๆ ที่อาจจะเกิดขึ้นในอนาคต จุดเริ่มต้นคือเมื่อประมาณปี ค.ศ. 1990 เกิดระบบ World Wide Web ซึ่งเริ่มใช้ในระบบของมหาวิทยาลัย และพัฒนามาจนกลายเป็นที่แพร่หลายช่วงประมาณ ค.ศ. 2000 ทำให้อินเทอร์เน็ตกลายสภาพจากเดิมที่เป็นโครงสร้างพื้นฐานทางเทคโนโลยี มาเป็นเครือข่ายที่เชื่อมโยงผู้คนเข้าด้วยกันโดยผ่าน World Wide Web และ เว็บไซต์ดอทคอมซึ่งถูกใช้ประโยชน์ในหลายแง่มุมไม่ว่าจะเป็นการแลกเปลี่ยนแบ่งปัน

ความคิด ข้อมูล สินค้าหรือบริการต่าง ๆ ซึ่งต่อมาได้พัฒนาจนถูกนำมาใช้ในทางการทหาร และเครื่องมือการค้นหาบนอินเทอร์เน็ตได้กลายมาเป็นสิ่งที่เชื่อมโยงการพาณิชย์อิเล็กทรอนิกส์ให้เข้ากับชีวิตคนในสังคม

การพัฒนาของเทคโนโลยีและอินเทอร์เน็ตส่งผลให้เกิดพัฒนาการทางลิขสิทธิ์ที่เปลี่ยนไปตามเทคโนโลยี โดยลิขสิทธิ์ต่าง ๆ ถูกทำให้เป็นงานดิจิตอลเพื่อให้คอมพิวเตอร์สามารถทำการอ่านข้อมูลได้ ดังนั้นงานอันมีลิขสิทธิ์ที่แต่เดิมมีการแพร่หลายอยู่ในวงจำกัดจึงสามารถแพร่หลายอย่างอิสระไปในโลกของอินเทอร์เน็ตได้อย่างรวดเร็วและมีประสิทธิภาพ อย่างไรก็ตาม การที่งานอันมีลิขสิทธิ์สามารถเผยแพร่และแลกเปลี่ยนบนอินเทอร์เน็ตได้อย่างรวดเร็วนั้นทำให้เกิดการส่งต่องานในรูปแบบใหม่ และเกิดช่องทางใหม่ในการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต จนมีผู้กล่าวว่า “The Internet has been described as “the world's biggest copy machine”[1] หรือ “อินเทอร์เน็ตเปรียบเสมือนเครื่องถ่ายสำเนาขนาดใหญ่ที่สุดในโลก”เพื่อสื่อให้เห็นว่าอินเทอร์เน็ตเป็นสื่อที่สามารถทำซ้ำอันเป็นการละเมิดลิขสิทธิ์ได้มากที่สุดในโลก โดยงานอันมีลิขสิทธิ์ที่ปรากฏอยู่บนอินเทอร์เน็ตได้แก่ งานประพันธ์ ภาพยนตร์ ศิลปะ โปรแกรมคอมพิวเตอร์ที่ถูกถ่ายไปเป็นข้อมูลดิจิตอล ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ต่าง ๆ

ตั้งแต่ปี ค.ศ. 2000[2] งานเขียนต่าง ๆ อย่างเช่นหนังสือหรือหนังสือพิมพ์เหมาะกับการทำให้เป็นดิจิตอลมากอย่างน่าเหลือเชื่อมีหลักฐานชี้ให้เห็นว่าหนังสืออิเลกทรอนิกส์ (e-book) นั้นได้รับความนิยมมากขึ้น ห้องสมุดกว่า 7300 ที่ได้ให้บริการหนังสืออิเล็กทรอนิกส์เป็นร้อยเป็นพันโดยไม่คิดค่าบริการ โดยเฉพาะที่ไม่ใช่ภาษาอังกฤษ ห้องสมุดออนไลน์ (e-library)ได้เสนอบทความต่าง ๆ กว่า 10,000 บทความออนไลน์ ในขณะเดียวกันที่มีการเก็บข้อมูลสำหรับหนังสือดิจิตอลไว้ที่ห้องสมุดหนังสือพิมพ์ออนไลน์ก็ได้รับความนิยมอย่างน่าประหลาดใจเห็นได้จากหนังสือพิมพ์ นิวยอร์กไทม์ที่มีผู้เข้าเยี่ยมชมเว็บไซต์ nytimes.com ได้ถึง 1.28 ล้าน ซึ่งมากกว่ายอดขายของหนังสือพิมพ์นิวยอร์กไทมส์ต่อสัปดาห์ (1.2 ล้านฉบับต่อสัปดาห์) มีนักข่าว นักประพันธ์จำนวนไม่น้อยที่หันไปใช้ Blog ในการเขียน ข่าวหรือบทความโดยไม่ต้องพึ่งผู้แจกจ่ายสิ่งพิมพ์ตามบ้านอีกต่อไป ในด้านของศิลปะศิลปินจำนวนมากก็หันมาทำ การสะสมผลงานของตนให้เป็นดิจิตอล เช่น Artnet ได้เปิดให้ผู้เข้าเยี่ยมชมได้ชมผลงานจากจิตรกรกว่า 1600 คน และสถานที่แสดงผลงานกว่า 1300 ที่ อีกแขนงหนึ่งก็มี

---

[1] World Intellectual Property Organization, **The inpact of the internet to intellectual property law** [Online], 5 April 2014a. Available from http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap3. html#3a.

[2] Gromov, G. R., **History of Internet and World Wide Web: The roads and crossroads of internet history** [Online] 5 April 2014. Available from http://www.netvalley.com /intvalnext.html.

ศิลปินที่สร้างสรรค์งานศิลปะของตนด้วยเทคโนโลยีดิจิตอล เห็นได้จาก เว็บไซต์ Digital Art Museum ที่ให้เข้าชมผลงานดังกล่าวได้ออนไลน์[3]

เพื่อให้การคุ้มครองลิขสิทธิ์สามารถพัฒนาทันเทคโนโลยีที่มีการเปลี่ยนแปลงดังที่ได้กล่าวมาข้างต้น เมื่อวันที่ 20 ธันวาคม ค.ศ. 1996 องค์การทรัพย์สินทางปัญญาโลก (WIPO) จึงได้จัดทำข้อตกลงระหว่างประเทศขึ้นสองฉบับ ที่เรียกรวมกันว่า “สนธิสัญญาอินเทอร์เน็ต” ได้แก่ สนธิสัญญาลิขสิทธิ์ของ WIPO (WIPO Copyright Treaty – WCT) และ สนธิสัญญาว่าด้วยการคุ้มครองสิทธินักแสดงและสิ่งบันทึกเสียง (WIPO Performances and Phonograms Treaty – WPPT) สนธิญญาทั้งสองมีวัตถุประสงค์คุ้มครองครอบคลุมสิทธิทางเศรษฐกิจและทางศีลธรรมสำหรับนักแสดง ผู้ผลิตสิ่งบันทึกเสียง และให้สิทธิแก่เจ้าของงานอันมีลิขสิทธิ์ในระดับสูงขึ้นกว่าอนุสัญญากรุงเบิร์นและอนุสัญญากรุงโรม โดยเฉพาะอย่างยิ่งในเรื่องละเมิดลิขสิทธิ์จากการใช้ประโยชน์ในรูปแบบดิจิตอลบนเครือข่ายอินเทอร์เน็ตซึ่งสนธิสัญญานี้ มีผลบังคับใช้เมื่อวันที่ 20 พฤษภาคม ค.ศ. 2002 [4]

2.1.1.2 สถานการณ์ของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตในประเทศไทย

ประเทศไทยเข้าร่วมเป็นภาคีสมาชิกความตกลงระหว่างประเทศเกี่ยวกับการคุ้มครองลิขสิทธิ์ครั้งแรกใน พ.ศ. 2474 โดยเข้าเป็นภาคีในอนุสัญญากรุงเบิร์นเพื่อคุ้มครองงานวรรณกรรมและศิลปกรรม และเพื่ออนุวัตรการตามอนุสัญญาดังกล่าว ประเทศไทยจึงตราพระราชบัญญัติคุ้มครองวรรณกรรมและศิลปกรรม พ.ศ. 2474 อีกทั้ง ประเทศไทยเข้าเป็นภาคีองค์การทรัพย์สินทางปัญญาโลกในปี พ.ศ. 2532 และผูกพันในข้อตกลง TRIPs ขององค์การการค้าโลกในปี พ.ศ. 2538 อย่างไรก็ตามยังมีข้อตกลงระหว่างประเทศอีกหลายฉบับที่ประเทศไทยไม่ได้เข้าร่วม เช่น สนธิสัญญาลิขสิทธิ์ขององค์การทรัพย์สินทางปัญญาโลก (WIPO Copyright Treaty – WCT) และสนธิสัญญาว่าด้วยการคุ้มครองสิทธินักแสดงและสิ่งบันทึกเสียง (WIPO Performances and Phonograms Treaty – WPPT)ซึ่งสนธิสัญญาลิขสิทธิ์ทั้งสองฉบับนี้มีความสำคัญมากในยุคดิจิตอลดังเช่นปัจจุบัน[5]

สนธิสัญญาฉบับแรกที่เข้าร่วมคือ ในรัชสมัยประบาทสมเด็กพระปกเกล้าเจ้าอยู่หัว โดยให้สัตยาบันต่ออนุสัญญาเบิร์น ค.ศ. 1806 ซึ่งได้แก้ไข ณ กรุงเบอร์ลิน เมื่อวันที่ 13 พฤศจิกายน ค.ศ. 1908 และสำเร็จบริบูรณ์โดยโปรโตคอลเพิ่มเติม ซึ่งลงนามกัน ณ กรุงเบอร์ลิน เมื่อวันที่ 20

---

[3] World Intellectual Property Organization, **The migration of intellectual property to the internet** [Online] 5 April 2014b. Available from http://www.wipo.int/copyright/en/ecommerce/ip_survey/ chap2.html.

[4] ปิยาภรณ์ คุณชื่น, **ปัญหาการละเมิดลิขสิทธิ์ผ่านระบบอินเทอร์เน็ต** (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2552), 12.

[5] เรื่องเดียวกัน, 10.

มีนาคม ค.ศ. 1914 ด้วยเหตุนี้ประเทศไทยจึงมีพัฒนากฎหมายทรัพย์สินทางปัญญา และทำให้มีการตราพระราชบัญญัติเครื่องหมายการค้าฉบับแรกคือ พระราชบัญญัติลักษณะเครื่องหมายการค้าและยี่ห้อการค้า พ.ศ. 2457[6] จนกระทั่งปี พ.ศ. 2474 ประเทศไทยได้เข้าเป็นภาคีอนุสัญญากรุงเบิร์นว่าด้วยการคุ้มครองวรรณกรรมและศิลปกรรม พ.ศ. 2474 จึงได้มีการประกาศใช้" พระราชบัญญัติคุ้มครองวรรณกรรมและศิลปกรรม พ.ศ. 2474" และ "พระราชบัญญัติเครื่องหมายการค้า พ.ศ. 2574" ขึ้น และในปี พ.ศ. 2521 มีการเปลี่ยนแปลงกฎหมายโดยการตราพระราชบัญญัติลิขสิทธิ์ฉบับใหม่ชื่อว่า "พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2521" โดยได้ยกเลิกพระราชบัญญัติคุ้มครองวรรณกรรมและศิลปกรรมพ.ศ. 2547 โดยสิ้นเชิง ทั้งนี้ พระราชบัญญัติลิขสิทธิ์มีการบังคับใช้เรื่อยมาจนถึง พ.ศ. 2537 โดยไม่เคยมีการแก้ไขเลย[7] จนกระทั่งมีการตราพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ด้วยเหตุผลที่ว่า "พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2521 ได้ใช้บังคับมาเป็นเวลานานแล้ว บทบัญญัติต่าง ๆ จึงไม่สอดคล้องกับสถานการณ์ทั้งภายในและภายนอกประเทศที่ได้เปลี่ยนแปลงไปโดยเฉพาะการพัฒนาและการขยายตัวทางเศรษฐกิจ การค้าและอุตสาหกรรมของประเทศและระหว่างประเทศ สมควรที่จะได้มีการปรับปรุงมาตรการการคุ้มครองด้านลิขสิทธิ์ให้มีประสิทธิภาพยิ่งขึ้นเพื่อรองรับการเปลี่ยนแปลงดังกล่าว และเพื่อส่งเสริมให้มีการสร้างสรรค์งานในด้านวรรณกรรม ศิลปกรรม และงานด้านอื่น ๆ ที่เกี่ยวข้องมากยิ่งขึ้นจึงจำเป็นต้องตราพระราชบัญญัตินี้" ซึ่งมีผลใช้บังคับตั้งแต่วันที่ 21 มีนาคม 2538 การปรับปรุงกฎหมายลิขสิทธิ์ในครั้งนี้เพื่อปรับปรุงกฎหมายทรัพย์สินทางปัญญาให้สอดคล้องกับมาตรฐานสากลที่ประเทศไทยมีความผูกพันอยู่คือ ข้อตกลง TRIPs ในฐานะที่ประเทศไทยเป็นสมาชิกของ GATT ซึ่งได้เปลี่ยนมาเป็นองค์กรการค้าโลก (WTO) และมาตรฐานตามอนุสัญญาว่าด้วยการคุ้มครองงานวรรณกรรมและศิลปกรรม ทำ ณ กรุงเบิร์น (อนุสัญญาเบิร์น Berne Convention for the Protection of Literary and Artistic Works) ฉบับแก้ไข ณ กรุงปารีส ค.ศ. 1971 เนื่องจากข้อตกลง TRIPs กำหนดไว้ว่าประเทศสมาชิกจะต้องปฏิบัติตามอนุสัญญาเบิร์นฉบับดังกล่าว ประเทศไทยจึงแจ้งเปลี่ยนความผูกพันจากอนุสัญญา เบิร์น ฉบับ Berlin Act 1908 มาเป็น Paris Act 1971 แทนโดยแจ้งเปลี่ยนแปลงต่อ WIPO และได้รับการยอมรับให้มีผลตั้งแต่วันที่ 2 กันยายน พ.ศ. 2538 และได้มีการใช้พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 มาจนถึงปัจจุบัน

---

[6] วัส ติงสมิตร, **คำอธิบายกฎหมายเครื่องหมายการค้า**, (กรุงเทพฯ: นิติธรรม, 2545), 2.

[7] ธัชชัย ศุภผลศิริ, "วิเคราะห์ประเด็นทางกฎหมายในการแก้ไขพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2521: เฉพาะกรณีความสัมพันธ์กับสหรัฐอเมริกา", **วารสารกฎหมาย** 12, 1(กรกฎาคม 2531): 13, อ้างถึงใน ปิยาภรณ์ คุณชื่น, **ปัญหาการละเมิดลิขสิทธิ์ผ่านระบบอินเทอร์เน็ต** (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2552), 16.

2.1.2 ความหมายและรูปแบบของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

2.1.2.1 ความหมายของเครือข่ายอินเทอร์เน็ต

อินเทอร์เน็ตเป็นเครือข่ายคอมพิวเตอร์ขนาดใหญ่ซึ่งประกอบด้วยเครือข่ายต่าง ๆ ที่เชื่อมโยงถึงกันและโยงใยกันทั่วโลก ทั้งนี้ บนเครือข่ายอินเทอร์เน็ตจะใช้มาตรฐานการสื่อสารด้วยโปรโตคอล TCP/ IP (Transmission Control Protocol/ Internet Protocol) โดยการใช้งานจะเป็นการใช้บริการผ่านผู้ให้บริการอินเทอร์เน็ต หรือเรียกว่า ISP (Internet Service Provider) ซึ่งปัจจุบันเครือข่ายอินเทอร์เน็ตเป็นเครือข่ายที่ใช้ในการติดต่อสื่อสารเป็นหลักในชีวิตประจำวัน ไม่ว่าจะเป็นการใช้งานผ่านโทรศัพท์เคลื่อนที่ หรือผ่านเครื่องคอมพิวเตอร์ก็ตาม โดยปกติในทางเทคนิคเครื่องคอมพิวเตอร์ 2 เครื่องจะไม่สามารถรับ – ส่ง ข้อมูลหรือติดต่อระหว่างกันได้ การรับส่งข้อมูลหรือสื่อสารข้อมูลระหว่างคอมพิวเตอร์ 2 เครื่องต้องมีผู้ให้บริการเชื่อมต่อ (Hosting) และ/ หรือ “ผู้ให้บริการอินเทอร์เน็ต” ซึ่งจะทำหน้าที่ในการให้บริการรับ-ส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ด้วยกัน รวมถึงการให้บริการเชื่อมต่อการรับ-ส่งข้อมูลผ่านระบบอินเทอร์เน็ต การส่งผ่านข้อมูลระหว่างเครื่องคอมพิวเตอร์ 2 เครื่องนั้นต้องมีตำแหน่งต้นทางและปลายทางที่ใช้ในการรับส่งข้อมูล อันได้แก่ จุดส่งข้อมูล (Sender’s Point), จุดรับข้อมูล (Recipient’s Point) โดยมีระบบมาตรฐาน (Protocal) ที่ใช้รับ-ส่งข้อมูลระหว่างกัน และมักเป็นมาตรฐานโปรโตคอลแบบเดียวกัน มาตรฐานโปรโตคอลที่ใช้ในปัจจุบันคือ ระบบ TCP/ IP นอกจากนั้น การส่งข้อมูลจากต้นทางไปยังปลายทางโดยผ่านระบบคอมพิวเตอร์นั้น ทั้งต้นทางและปลายทางในการรับส่งข้อมูลจะต้องมีหมายเลขประจำตัวของเครื่องคอมพิวเตอร์ที่แสดงตำแหน่งในการรับส่งข้อมูล ซึ่งจะทำให้ข้อมูลนั้นรับและส่งอย่างถูกต้อง ในทางเทคนิคเรียกหมายเลขประจำตัวเครื่องคอมพิวเตอร์หรือตำแหน่งที่อยู่บนอินเทอร์เน็ตนี้ว่า “ไอพีแอดเดรส (IP Address)”

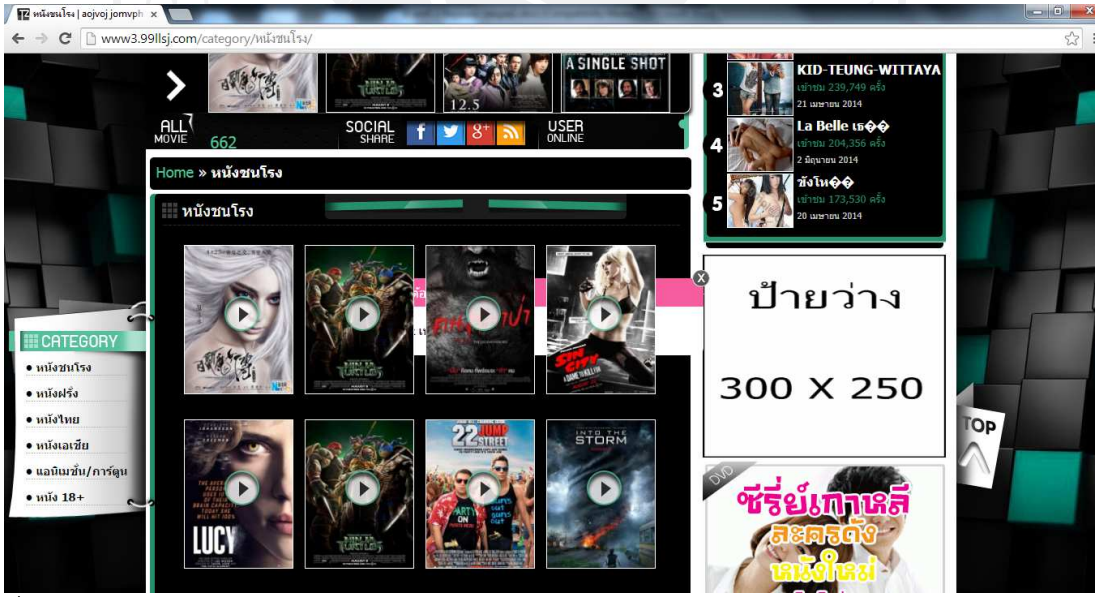
2.1.2.2 รูปแบบการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

ลักษณะของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตมีลักษณะที่แพร่หลายมากกว่าการละเมิดลิขสิทธิ์ทั่วไป เนื่องจากอินเทอร์เน็ตมีการเชื่อมต่อจากผู้คนทั่วโลก สามารถเข้าถึงข้อมูลเดียวกันได้พร้อม ๆ กัน ทั้งนี้ การกระทำละเมิดบางประการกฎหมายที่มีอยู่ในปัจจุบันอาจจะยังพัฒนาหรือครอบคลุมไปไม่ถึง เช่นการสนับสนุนหรือยินยอมให้ใช้เครือข่ายหรือเซอร์เวอร์เพื่อเป็นที่ฝากข้อมูลอันละเมิดลิขสิทธิ์ของผู้อื่นมาเผยแพร่และแจกจ่ายให้แก่บุคคลอื่น ๆ โดยแม้ผู้เป็นเจ้าของเว็บไซต์หรือเซอร์เวอร์จะไม่ได้เป็นผู้กระทำการละเมิดลิขสิทธิ์ด้วยตนเองแต่การยินยอมให้ใช้เว็บไซต์ในการกระทำดังกล่าว ก็ทำให้เกิดความเสียให้แก่เจ้าของผลงานได้อย่างมหาศาลเช่นกัน โดยรูปแบบของการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้แก่

(1) การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตโดยการทำซ้ำและเผยแพร่ข้อมูลละเมิดลิขสิทธิ์

การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตโดยผู้ให้บริการเว็บไซต์ได้นำงานอันมีลิขสิทธิ์ของผู้อื่นมาใช้ในเว็บไซต์ตนเพื่อประโยชน์ในทางการค้า โดยอาจมีการดัดแปลงงานของผู้อื่นแล้วนำมาใช้ เช่น การนำพาดหัวข่าวหรือข่าวของสำนักข่าวชื่อดังหลาย ๆ สำนักมาลงในเว็บไซต์ของตนเองโดยไม่ได้รับอนุญาต ซึ่งเว็บไซต์ของตนเป็นเว็บเกี่ยวกับขายสินค้าทั่วไป แต่นำข้อมูลข่าวดังกล่าวมาใช้เพื่อดึงดูดให้เกิดการเข้าชมเว็บไซต์มากยิ่งขึ้น เป็นต้น หรือกรณีเว็บไซต์ให้บริการดูหนังละเมิดลิขสิทธิ์ออนไลน์นำงานอันมีลิขสิทธิ์มาเผยแพร่เพื่อหากำไรโดยมิได้รับอนุญาต ในลักษณะของการเก็บค่าบริการรายวัน รายเดือน หรือรายปี หรือบางครั้งเป็นการให้บริการโดยไม่เสียค่าใช้จ่าย แต่หวังผลทางการค้าสำหรับค่าโฆษณาภายในเว็บไซต์แทน โดยมีตั้งแต่หนังที่ยังเข้าฉายอยู่ในโรงภาพยนตร์ จนถึงหนังที่พึ่งออกจากโรงภาพยนตร์อันแสดงให้เห็นถึงลักษณะที่เป็นการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตอย่างชัดเจน

ภาพที่ 2.1: เว็บไซต์เผยแพร่ภาพยนตร์ละเมิดลิขสิทธิ์ออนไลน์



ที่มา: ดูหนังออนไลน์ฟรีใหม่ ๆ Aojvoj Jomvphd. (ม.ป.ป.). สืบค้นจาก http://www3.99llsj.com.

หรือการละเมิดลิขสิทธิ์โดยใช้โปรแกรมคอมพิวเตอร์ในการทำซ้ำและเผยแพร่ข้อมูลละเมิดลิขสิทธิ์ผ่านระบบอินเทอร์เน็ต กรณีตัวอย่างเช่น บริษัท ก. พัฒนาและสร้างโปรแกรมเพื่อทำซ้ำข้อมูลบทความวิเคราะห์ข่าวอันมีลิขสิทธิ์โดยไม่ได้รับอนุญาตจาก ข. เจ้าของ

ผลงาน (เป็นลักษณะของการดึงข้อมูลจากเว็บไซต์ของ ข. เข้ามาสู่โปรแกรมที่ ก. พัฒนาขึ้นเพื่อให้ผู้ใช้งานสามารถรับชมหรืออ่านงานอันมีลิขสิทธิ์ของ ข. ผ่านทางโปรแกรมของ ก. ด้วยการเชื่อมต่ออินเทอร์เน็ตได้โดยที่ไม่ได้รับอนุญาต อันเป็นลักษณะของการทำซ้ำและเผยแพร่งานอันมีลิขสิทธิ์โดยไม่ได้รับอนุญาต เป็นการละเมิดลิขสิทธิ์ ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ซึ่งการละเมิดลิขสิทธิ์ในลักษณะนี้เป็นการละเมิดลิขสิทธิ์ในรูปแบบใหม่ที่เกิดขึ้นพร้อมกับเทคโนโลยีและอินเทอร์เน็ต ซึ่งหากไม่มีการเชื่อมต่ออินเทอร์เน็ตในการใช้โปรแกรมดังกล่าว การละเมิดลิขสิทธิ์ย่อมไม่เกิดขึ้น ดังนั้นการกระทำเช่นนี้ย่อมเป็นการละเมิดลิขสิทธิ์อย่างหนึ่ง นอกจากนั้น ผู้ให้บริการแก่ ก. ในการให้ ก. นำเสนอโปรแกรมดังกล่าวให้แก่บุคคลทั่วไปได้ดาวโหลดเพื่อใช้งาน ก็อาจมีความผิดฐานละเมิดลิขสิทธิ์ด้วยเช่นเดียวกัน เนื่องจากเป็นผู้ควบคุมระบบคอมพิวเตอร์ของตนเอง การยินยอมให้มีโปรแกรมที่พัฒนาหรือสร้างขึ้นเพื่อละเมิดลิขสิทธิ์อันส่งผลให้เกิดการละเมิดลิขสิทธิ์ ย่อมต้องรับผิดในการกระละเมิดลิขสิทธิ์บนอินเทอร์เน็ตด้วย

(2) การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตโดยการแลกเปลี่ยนการเผยแพร่ข้อมูลอันละเมิดลิขสิทธิ์

รูปแบบการแลกเปลี่ยนข้อมูลอันละเมิดลิขสิทธิ์ ปรากฏอย่างแพร่หลายมาเป็นระยะเวลานานโดยการแลกเปลี่ยนข้อมูลผ่านผู้ให้บริการเว็บไซต์กลาง เพื่อให้ผู้ใช้บริการสามารถอัพโหลดและดาวโหลดข้อมูลผ่านเว็บไซต์ ทั้งนี้ ผู้ให้บริการไม่ได้มีการควบคุมหรือมาตรการรองรับเพื่อป้องกันการละเมิดลิขสิทธิ์แต่อย่างใด โดยการป้องกันความรับผิดของตนกระทำเพียงการระบุไว้ว่าไม่ยินยอมหรือสนับสนุนให้มีการแบ่งปันหรืออัพโหลดงานอันละเมิดลิขสิทธิ์ แต่ในทางปฏิบัติ งานที่มีการอัพโหลดโดยผู้ใช้งานทั่วไป เป็นงานที่มีไว้เพื่อใช้ส่วนตัวเท่านั้นโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ให้ทำซ้ำหรือเผยแพร่ต่อสาธารณะชน เมื่อปรากฏว่ามีการนำเข้าสู่ระบบของผู้ให้บริการเว็บไซต์ และสมาชิกทุกท่านสามารถจะดาวโหลดหรือรับชมงานอันละเมิดลิขสิทธิ์ได้ ถึงแม้ว่าผู้อัพโหลดจะไม่ได้ทำเพื่อหากำไร แต่การกระทำดังกล่าวย่อมก่อให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์ จึงเป็นกรณีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตด้วย

ตัวอย่างเช่น เว็บไซต์ 4Shared ซึ่งเป็นเว็บไซต์ให้บริการแลกเปลี่ยนข้อมูลโดยไม่เสียค่าใช้จ่ายแก่สมาชิกจากการสำรวจของ Google ได้เปิดเผยว่าในปี พ.ศ. 2555 คาที่มีการค้นหามากที่สุดสาหรับการใช้งาน Google คือคำว่า 4Shared [8] โดยเป็นคำที่ติดอันดับคาค้นหามากที่สุดติดต่อกันเป็นระยะเวลา 3 ปีซ้อนโดยรูปแบบการให้บริการคือให้ผู้ใช้บริการสามารถจัดเก็บข้อมูล

[8] “กูเกิลเผย คำค้น ยอดนิยมของไทยปี 2012 4shared-แรงเงา-the voice-Gangnam Style ติดอันดับ”, **มติชน** [Online], 17 เมษายน 2557. แหล่งที่มา http://www.matichon.co.th/news_detail.php?newsid=1355385174&grpid=03&catid=03.

และแลกเปลี่ยนข้อมูลไฟล์ต่าง ๆ ผ่านเว็บไซต์ได้โดยไม่เสียค่าใช้จ่าย ทีมงานประกอบด้วยผู้เชี่ยวชาญเฉพาะด้านไม่ว่าจะเป็นการเขียนโปรแกรมออกแบบเว็บไซต์ และการสื่อสารการตลาด 4Shared ก่อตั้งขึ้นในปี 2005 และเป็นที่รู้จักมากขึ้นเรื่อย ๆ ในเหล่าผู้ใช้ออนไลน์ในทั่วโลก ผู้ใช้สามารถอัพโหลดจัดเก็บและดาวน์โหลดเพลง วิดีโอ รูปภาพ และไฟล์หรือเอกสารอื่น ๆ ไม่ว่าจะเป็นประเภทใดก็ตาม หลักการสำคัญของธุรกิจคือการตอบสนองความต้องการของผู้ใช้ ด้านการแลกเปลี่ยนและจัดเก็บข้อมูลออนไลน์ บริการจากช่องทางการให้บริการดังกล่าวซึ่งสามารถนาไปสู่การแลกเปลี่ยนข้อมูลที่ละเมิดทรัพย์สินทางปัญญาบนอินเทอร์เน็ตได้นั้น จากความเสี่ยงที่จะถูกเจ้าของทรัพย์สินทางปัญญาฟ้องร้องได้ 4Shared จึงมีมาตรการเพื่อป้องกันดังกล่าวโดยได้ให้เหตุผลเกี่ยวกับมาตรการที่เว็บไซต์ได้มีขึ้นเพื่อป้องกันการละเมิดลิขสิทธิ์ดังนี้ 4Shared ไม่มีหน้าที่จะต้องตรวจดูสิ่งที่ถูกอัพโหลด โดยผู้ใช้บางครั้งจึงอาจพบสิ่งที่ไม่ถูกกฎหมายได้ ทาง 4Shared มีนโยบายว่าหากมีการพบไฟล์ที่ผิดกฎหมายและได้ถูกทำให้พบได้ด้วยระบบค้นหาของทางเว็บไซต์ และทางเว็บไซต์เปิดรับการแจ้งเตือนจากผู้ใช้อื่นๆและจะยกเลิก ลิงค์ที่เข้าถึงไฟล์นั้นทันที ทางเว็บไซต์มีการเตือนโดยชัดแจ้งว่าปฏิเสธความรับผิดชอบใด ๆ ที่เก็บรักษาไว้โดยผู้ใช้บริการเว็บไซต์ ผู้ใช้แต่ละคนมีความรับผิดโดยลำพังต่อสิ่งที่ได้ถูกอัพโหลดขึ้นและแนะนาให้ผู้ใช้ไม่อัพโหลดหากไม่แน่ใจว่าไฟล์ดังกล่าวละเมิดต่อกฎหมายหรือไม่ อย่างไรก็ตามการกำหนดจำกัดความรับผิดของเว็บไซต์นี้จะสามารถจำกัดความรับผิดได้จริงเพียงใดต้องพิจารณาเป็นกรณีตามแต่ความเสียหายที่เกิดขึ้นว่าผู้ให้บริการเว็บไซต์ได้ควบคุมตามสมควรแล้วหรือไม่เพื่อไม่ให้เกิดการละเมิดลิขสิทธิ์ขึ้นบนความควบคุมของตนเอง

(3) Browsing (เบราว์ซิ่ง)

เมื่อมีการใช้งานอินเทอร์เน็ตในการเปิดหน้าเว็บไซต์ เครื่องคอมพิวเตอร์จะทาการจัดเก็บเนื้อหาหน้าเว็บไซต์นั้นไว้ชั่วคราวน์ในหน่วยความจาเข้าถึงโดยสุ่มหรือแรม (Random Access Memory: RAM) ซึ่งเป็นหน่วยความจาชั่วคราว เพื่อที่จะแสดงหน้าเว็บบนหน้าจอเครื่องคอมพิวเตอร์ จึงเป็นประเด็นว่าการก่อให้เกิดการทำซ้ำเช่นนี้เป็นการละเมิดลิขสิทธิ์หรือไม่[9]

ในสหรัฐอเมริกา และสหภาพยุโรปตีความการทำซ้ำชั่วคราวว่าถือเป็นทำซ้ำด้วยเช่นกัน เพียงแต่มีข้อยกเว้นให้การทำซ้ำเหล่าสามารถกระทำได้เพราะเป็นเพียงผลอันไม่อาจหลีกเลี่ยงได้ของเทคโนโลยีและเป็นการชั่วคราว เป็นการกระทำที่ทำได้ภายใต้มาตา 177 ของกฎหมายลิขสิทธิ์สหรัฐอเมริกา และในสหภาพยุโรป การทำซ้ำชั่วความเป็นส่วนสำคัญของเทคโนโลยีและมีวัตถุประสงค์เดียวคือเพื่อทำให้เกิดการส่งสัญญาบนเครือข่ายระหว่างบุคคลที่สามโดยคนกลาง

[9] สราวุธ ปิติยาศักดิ์, **กฎหมายเทคโนโลยีสารสนเทศ**, (กรุงเทพฯ: นิติธรรม, 2555).

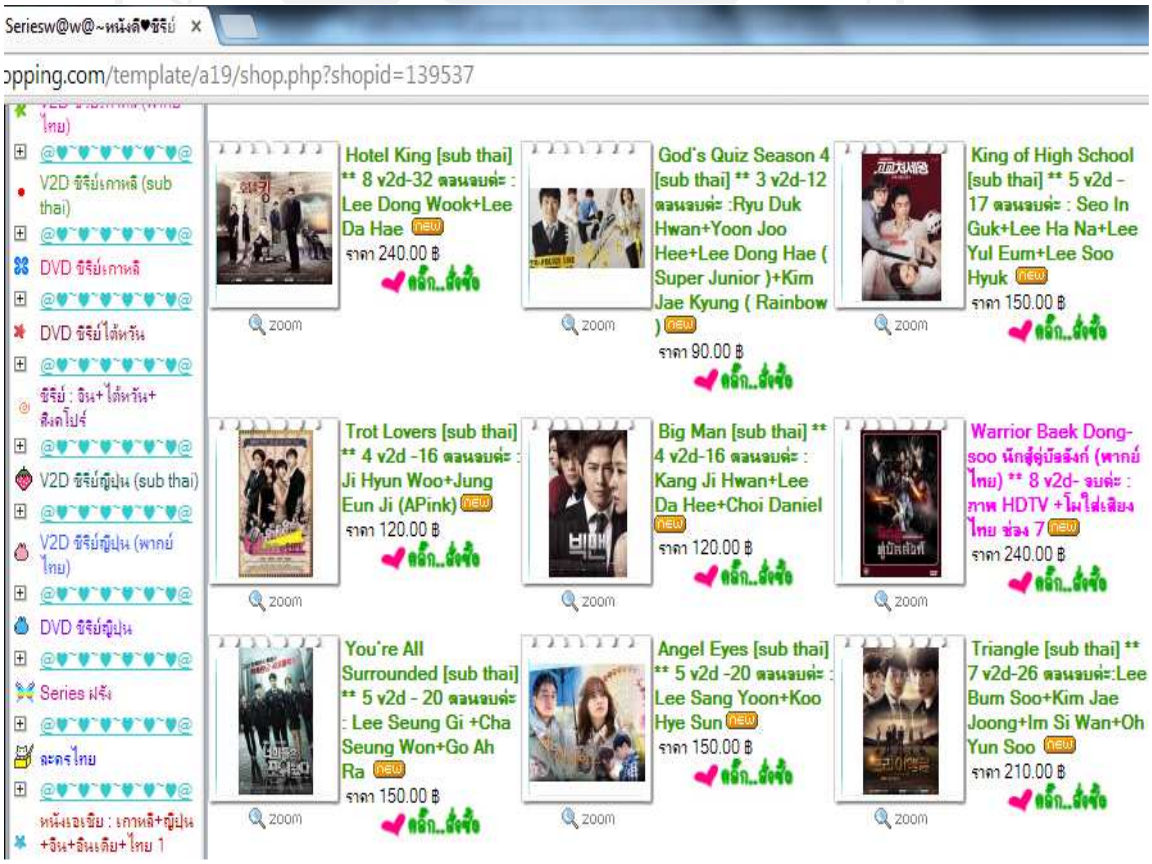
ย่อมเป็นข้อยกเว้นสิทธิผู้เดียวในการทำซ้ำของเจ้าของลิขสิทธิ์ตามความในมาตรา 2 จึงสามารถกระทำได้

สำหรับกฎหมายของประเทศไทยมีการให้ความหมายของการทำซ้ำไว้อย่างกว้างว่ารวมถึงการทำซ้ำทุกวิธี ดังนั้นการทำซ้ำชั่วคราวในแรมจึงอาจถือเป็นการทำซ้ำตามกฎหมายไทยด้วย อย่างไรก็ตาม ในร่างพระราชบัญญัติลิขสิทธิ์ ฉบับที่ ..... พ.ศ. ....ที่กำลังเข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติ มีข้อยกเว้นเกี่ยวกับการทำซ้ำชั่วคราวหรือการทำซ้ำเพื่อความจำเป็นว่าไม่มีความผิดเกี่ยวกับการละเมิดลิขสิทธิ์

(4) เว็บไซต์ขายสินค้าละเมิดลิขสิทธิ์

เว็บไซต์ที่ขายสินค้าละเมิดลิขสิทธิ์ซึ่งไม่ได้รับอนุญาตเป็นตัวแทนขายสินค้าจากเจ้าของลิขสิทธิ์ และไม่ได้รับอนุญาตให้มีการใช้สิทธิอื่นใดไม่ว่าจะเป็นการทำซ้ำ เผยแพร่ต่อสาธารณะชน โดยตัวอย่างเว็บไซต์เหล่านี้ที่พบทั่วไปเช่น เว็บไซต์ขายซีดีละเมิดลิขสิทธิ์

ภาพที่ 2.2: เว็บไซต์ขายสินค้าละเมิดลิขสิทธิ์



ที่มา: serieswawa.com. (ม.ป.ป.). สืบค้นจาก http://www.serieswawa.com.

2.1.3 กฎหมายเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

2.1.3.1 การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตตาม Convention On Cybercrime (อนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ค.ศ. 2001)

1) หลักการและเหตุผลในการร่างกฎหมาย

ในคำนำของ อนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ค.ศ. 2001 (Preambel of Convention on Cybercrime 2011, Budapest) ได้ให้เหตุผลของการบัญญัติอนุสัญญาฉบับนี้ไว้โดยสรุปได้ว่า เนื่องด้วยสภายุโรปได้คำนึงถึงความเปลี่ยนแปลงของเทคโนโลยีและผลกระทบจากความเสี่ยงที่เครือข่ายคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์อาจถูกใช้เพื่อการกระทำความทางทางอาญา จึงมีการจัดทำอนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ค.ศ. 2001 โดยมีวัตถุประสงค์ในการคุ้มครองสังคมให้ปลอดภัยจากอาชญากรรมทางคอมพิวเตอร์ โดยเน้นว่าอนุสัญญาฉบับนี้มุ่งหมายเพื่อช่วยให้การสอบสวนคดีอาญาและการดำเนินคดีความผิดทางอาญาที่เกี่ยวข้องกับระบบและข้อมูลคอมพิวเตอร์นั้นมีประสิทธิผลมากขึ้น และเพื่อให้สามารถรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์เกี่ยวกับการกระทำความผิดทางอาญานั้น ด้วยอาศัยความร่วมมือระหว่างประเทศที่มีอนุสัญญาฉบับนี้เป็นแนวทางในการปฏิบัติร่วมกัน ซึ่งมีการกำหนดข้อตกลงร่วมกันได้แก่

(1) การกระทำความผิดทางคอมพิวเตอร์แบบใดบ้างที่ถือเป็นการกระทำความผิดทางอาญาหรือต้องกำหนดให้มีมาตรการลงโทษเบื้องต้นอย่างไร

(2) แนวทางการบัญญัติกฎหมายวิธีพิจารณาความที่ประเทศภาคีพึงมีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

(3) แนวทางการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อใช้เป็นพยานหลักฐาน

(4) การกำหนดให้ต้องมีหน่วยงานที่มีอำนาจในการปราบปรามการกระทำความผิดอาญาทางคอมพิวเตอร์ และมีแนวทางปฏิบัติในการใช้อำนาจดังกล่าว

(5) แนวทางในการให้ความร่วมมือระหว่างประเทศเพื่อการรวมรวบข้อมูลและพยานหลักฐานอย่างรวดเร็ว เพื่อนำไปสู่การหาตัวผู้กระทำความผิดได้ต่อไป

2) ความเกี่ยวข้องกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

อนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ จะมุ่งป้องกันการละเมิดลิขสิทธิ์ตามความหมายที่ระบุในกฎหมายของประเทศนั้น โดยเป็นไปตามหน้าที่ที่กำหนดไว้ในบทบัญญัติแห่งปารีส ลงวันที่ 24 กรกฎาคม ค.ศ. 1971 ซึ่งปรับปรุงอนุสัญญากรุงเบิร์นว่าด้วยการคุ้มครองวรรณกรรมและงานศิลปะ และ คุ้มครองสิทธิของผู้แสดง

ผู้ผลิตเสียงและองค์กรวิทยุกระจายเสียง (อนุสัญญากรุงโรม) ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในสิทธิแห่งทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาของโลกว่าด้วยผู้แสดงและผู้ผลิตเสียง โดยมิได้มีการกล่าวถึงเครื่องหมายการค้าหรือสิทธิบัตรว่าจะต้องมีการคุ้มครองทางอาชญากรรมทางคอมพิวเตอร์ด้วย

ในอนุสัญญาดังกล่าวได้กล่าวถึงฐานความผิดที่แต่ละประเทศจะต้องพึงจัดให้มีเพื่อให้เป็นไปตามอนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ค.ศ. 2001 โดยมีการกำหนดเรื่องเกี่ยวกับลิขสิทธิ์ไว้ใน ข้อ 10 ดังนี้

“ข้อ 10[10] ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง

(1) ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในประเทศนั้น ซึ่งการละเมิดลิขสิทธิ์ตามความหมายที่ระบุในกฎหายของประเทศนั้น โดยเป็นไปตามหน้าที่ที่กำหนดไว้ในบทบัญญัติแห่งปารีส ลงวันที่ 24 กรกฎาคม ค.ศ. 1971 ซึ่งปรับปรุงอนุสัญญากรุงเบิร์นว่าด้วยการคุ้มครองวรรณกรรมและงานศิลปะ ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในสิทธิแห่งทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาโลกว่าด้วยลิขสิทธิ์ ยกเว้นธรรมสิทธิ์ตามที่กำหนดไว้ในบรรดาข้อตกลงดังกล่าว ทั้งนี้การละเมิดลิขสิทธิ์ดังกล่าวได้กระทำโดยเจตนาเพื่อการค้าและโดยวิธีการของระบบคอมพิวเตอร์นั้น

(2) ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็น เพื่อกำหนดให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในประเทศนั้น โดยเป็นไปตามหน้าที่ที่กำหนดไว้ในอนุสัญญาระหว่างประเทศว่าด้วยการคุ้มครองผู้แสดง ผู้ผลิตเสียงและองค์กรวิทยุ กระจายเสียง (อนุสัญญากรุงโรม) ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในสิทธิแห่งทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาของโลกว่าด้วยผู้แสดงและผู้ผลิตเสียง ยกเว้นธรรมสิทธิ์ตามที่กำหนดไว้ในบรรดาข้อตกลงดังกล่าว ทั้งนี้การละเมิดสิทธิ์ดังกล่าวได้กระทำโดยเจตนาเพื่อการค้าและโดยวิธีการของระบบคอมพิวเตอร์นั้น

(3) ประเทศภาคีอาจสงวนสิทธิ์ที่จะไม่กำหนดให้การกระทำดังกล่าวตามความในวรรค 1 และ 2 ของข้อนี้ต้องรับผิดทางอาญาก็ได้ ภายใต้เงื่อนไขว่าได้มีวิธีการแก้ไขเยียวยาอย่างอื่น ๆ ไว้ให้แล้ว และการสงวนสิทธิ์นั้นมิได้ทำให้ลดทอนหน้าที่ระหว่างประเทศของประเทศภาคีนั้นตามที่กำหนดไว้ในหลักเกณฑ์ระหว่างประเทศที่กล่าวถึงในวรรค 1 และ 2 ของข้อนี้”

---

[10] **อนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรม [Convention on Cybercrime]**, แปลโดย กิตติพงษ์ กิตยารักษ์, ชาติ ชัยเดชสุริยะ และณัฐวสา ฉัตรไพฑูรย์ (กรุงเทพฯ: เดือนตุลา), 12.

จากบทบัญญัติดังกล่าวแสดงให้เห็นถึงลักษณะของการละเมิดลิขสิทธิ์ในรูปแบบใหม่ที่เกิดขึ้นในยุค ดิจิตอล คือการละเมิดลิขสิทธิ์ซึ่งใช้วิธีการทางคอมพิวเตอร์ ทั้งนี้ กฎหมายนี้ได้ระบุว่าชัดเจนในส่วนหนึ่งว่า การกระทำที่จะเป็นการละเมิดลิขสิทธิ์ได้จะต้องเป็นการกระทำเพื่อการค้า มิได้กำหนดในกรณีอื่นไว้ว่าจะต้องกำหนดให้เป็นความผิดทางอาญาด้วย ดังนั้นจึงเป็นดุลยพินิจของแต่ละประเทศว่าจะมีวิธีการกำหนดฐานความผิดใหม่อย่างไรในส่วนของความผิดเกี่ยวกับการละเมิดลิขสิทธิ์ผ่านระบบคอมพิวเตอร์และลักษณะที่มีการเผยแพร่อย่างกว้างขวางคือการละเมิดลิขสิทธิ์ผ่านระบบอินเทอร์เน็ตเพราะลักษณะของระบบคอมพิวเตอร์ที่จะมีการเชื่อมต่อสู่สาธารณะในปัจจุบันได้ที่เป็นขนาดใหญ่และเกิดการละเมิดลิขสิทธิ์ได้มากที่สุดก็คือระบบอินเทอร์เน็ต

ทั้งนี้ กฎหมายดังกล่าวทำให้เกิดมุมมองใหม่ได้ว่ากฎหมายลิขสิทธิ์ที่บังคับใช้อยู่ในปัจจุบัน กับกฎหมายลิขสิทธิ์เป็นรูปแบบของการกระทำบนระบบคอมพิวเตอร์ควรจะมีวิธีการหรือรูปแบบที่แตกต่างกัน หรือมีสถานะในการบังคับใช้และการลงโทษแตกต่างกันหรือไม่เพียงใด เนื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นความผิดที่พัฒนามาจากการกระทำความผิดทั่วไปเช่นเดียวกัน แต่กฎหมายกำหนดลักษณะแยกไว้ต่างหากเฉพาะที่จะให้แต่ละประเทศป้องกันการละเมิดลิขสิทธิ์ เนื่องด้วยลักษณะทางคอมพิวเตอร์มีลักษณะพิเศษที่สามารถเข้าถึงและแบ่งปันข้อมูลได้ง่าย ทำให้ความเสียหายสามารถกระจายได้ง่ายกว่าความผิดโดยทั่วไปด้วย การที่อนุสัญญาฉบับนี้กำหนดให้ต้องมีการกำหนดโทษไว้เพื่อให้มีกระบวนการจัดการการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้เช่นเดียวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบอื่น ซึ่งเพิ่มเติมขึ้นมาจากการละเมิดลิขสิทธิ์โดยทั่วไปที่แต่ละประเทศให้ความคุ้มครองอยู่แล้ว

2.1.3.2 การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตตามกฎหมายไทย

2.1.3.2.1 พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537

1) หลักการและเหตุผลของกฎหมาย

กฎหมายให้สิทธิ์ผู้สร้างสรรค์มีลิขสิทธิ์ในงานของตน โดยหลักทั่วไปของกฎหมายลิขสิทธิ์ ตามข้อตกลงในอนุสัญญากรุงเบิร์น ทันทีที่ผู้สร้างสรรค์ได้สร้างสรรค์งานขึ้น ย่อมได้รับความคุ้มครองตามกฎหมายทันที ทั้งในประเทศของผู้สร้างสรรค์และประเทศอื่นที่เป็นภาคีของอนุสัญญาดังกล่าว ไม่จำเป็นต้องประกาศให้ใครรับรอง ซึ่งแตกต่างจากสิทธิบัตร และเครื่องหมายการค้าที่ต้องมีขั้นตอนปฏิบัติก่อนได้รับความคุ้มครอง อย่างไรก็ตาม เพื่อความสะดวกในการพิสูจน์สิทธิ ตามกฎหมายไทยได้กำหนดเงื่อนไขไว้ สองกรณี คือกรณีที่ยังไม่มีการโฆษณา กับ กรณีที่มีการโฆษณางานนั้นแล้ว โดยลิขสิทธิ์ หมายถึง สิทธิแต่เพียงผู้เดียวที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้นโดยการแสดงออกตามงานประเภทต่าง ๆ เป็นผลงานที่เกิดจากการใช้สติปัญญา ความรู้ความสามารถ และความวิริยะอุตสาหะในการสร้างสรรค์งานให้เกิดขึ้นซึ่งถือว่าเป็นทรัพย์สินทางปัญญาประเภทหนึ่ง

2) สิ่งที่กฎหมายคุ้มครอง

กฎหมายได้กำหนดสิ่งที่คุ้มครอง คืองานที่มีลิขสิทธิ์ไว้ใน มาตรา 6 โดยมีเนื้อหาดังนี้ “งานอันมีลิขสิทธิ์ตามพระราชบัญญัตินี้ ได้แก่ งานสร้างสรรค์ประเภทวรรณกรรม นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ หรืองานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ ของผู้สร้างสรรค์ไม่ว่างาน ดังกล่าวจะแสดงออกโดยวิธีหรือรูปแบบอย่างใด” ทั้งนี้ สำหรับคำว่างานสร้างสรรค์ พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 ให้ความหมายว่า “สร้างให้มีให้เป็นขึ้น, เนรมิต” ดังนั้น งานสร้างสรรค์จึงต้องเป็นงานที่สร้าง หรือทำขึ้นใหม่ มิใช่งานที่มีอยู่แล้ว สำหรับผู้สร้างสรรค์ มาตรา 4 ให้คำนิยามว่า “ผู้ทำหรือก่อให้เกิดงานโดยความคิดริเริ่มของตนเอง” อันหมายความว่า การที่ผู้สร้างสรรค์จะได้ลิขสิทธิ์ บุคคลนั้นจะต้องได้ทำหรือก่อให้เกิดงานโดยใช้ความวิริยะอุตสาหะในการสร้างสรรค์ และงานดังกล่าวมีต้นกำเนิดมาจากบุคคลนั้น มิได้คัดลอกหรือทำซ้ำ)[11] งานอันมีลิขสิทธิ์ตามพระราชบัญญัติฉบับนี้มีต่อไปนี้

งานวรรณกรรม ได้แก่ หนังสือจุลสาร สิ่งเขียน สิ่งพิมพ์ โปรแกรมคอมพิวเตอร์ลิขสิทธิ์ในงานเขียนต่าง ๆ เช่น หนังสือ นิยาย เรื่องสั้น บทความ และสิ่งพิมพ์ต่าง ๆ และในปี พ.ศ. 2537 กฎหมายบัญญัติให้รวมโปรแกรมคอมพิวเตอร์เป็นงานวรรณกรรมด้วย

งานนาฏกรรม งานที่เกี่ยวกับการเต้นรำ ได้แก่ งานเกี่ยวกับการรำ การเต้น การทำท่า หรือการแสดงที่ประกอบขึ้นเป็นเรื่องราว การแสดงโดยวิธีใบ้

งานศิลปกรรม เป็นงานที่มีขอบเขตกว้าง ได้แก่ งานทางด้านจิตรกรรม ประติมากรรม ภาพพิมพ์ สถาปัตยกรรม ภาพถ่าย ภาพประกอบแผนที่ โครงสร้างศิลปะประยุกต์ และรวมทั้งภาพถ่ายและแผนผังของงานดังกล่าวด้วย

งานดนตรีกรรม ได้แก่ ทำนองและเนื้อร้อง หรือทำนองอย่างเดียว และรวมถึงโน้ตเพลงที่ได้แยกและเรียบเรียงเสียงประสานแล้ว

งานโสตทัศน์วัสดุ ได้แก่ วิดีโอเทป แผ่นเลเซอร์ดิสก์

งานภาพยนตร์ ได้แก่ โสตทัศน์วัสดุประกอบด้วยลำดับภาพที่สามารถนำออกฉายต่อเนื่องได้อย่างภาพยนตร์ หรือบันทึกลงบนวัสดุอื่น เพื่อนำออกฉายต่อเนื่องได้อย่างภาพยนตร์ และรวมถึงเสียงประกอบภาพยนตร์

งานสิ่งบันทึกเสียง ได้แก่ เทปเพลง แผ่นคอมแพ็คดิสก์

---

[11] คมน์ทนงชัย ฉายไพโรจน์, **กฎหมายทรัพย์สินทางปัญญาฉบับสมบูรณ์,** (กรุงเทพฯ: บานานาสวีท, 2555), 51.

งานแพร่เสียงแพร่ภาพ ได้แก่ งานนำออกเผยแพร่ทางสถานีวิทยุกระจายเสียง หรือโทรทัศน์

งานอื่นใด อันเป็นงานแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ[12]

อย่างไรก็ตาม งานบางประเภทที่เป็นเรื่องเกี่ยวกับข้อมูลข่าวสาร ข้อเท็จจริง และกฎหมาย ซึ่งเป็นสิ่งที่ต้องเผยแพร่ให้ทุกคนได้รู้ และเป็นสิ่งที่เกิดขึ้นซึ่งทุกคนสามารถพูดถึงได้เพื่อไม่ให้เกิดความสับสนหรือเป็นประโยชน์แก่ผู้ที่พบข้อเท็จจริงดังกล่าวก่อนเท่านั้นกฎหมายจึงให้ความหมายงานที่ไม่มีลิขสิทธิ์ ไว้ชัดเจน ได้แก่ งานประเภทข่าวประจำวัน ข้อเท็จจริงที่เป็นข่าวสาร รัฐธรรมนูญ กฎหมาย ระเบียบ คำสั่ง ประกาศ และข้อบังคับของทางราชการ คำพิพากษา คำสั่ง หรือคำวินิจฉัย รายงานของทางราชการ คำแปล และการรวบรวมสิ่งดังกล่าวข้างต้นที่หน่วยงานของรัฐทำขึ้น ดังปรากฏตามมาตรา 7

3) ความเกี่ยวข้องกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

เจ้าของลิขสิทธิ์ย่อมมีสิทธิแต่ผู้เดียวที่จะกระทำการใดๆต่องานของตน รวมทั้งการอนุญาตให้บุคคลอื่นใช้สิทธิในงานของตนด้วย โดยผู้ที่มิใช่เจ้าของงานหากกระทำใด ๆ แก่งานนั้นจะถือเป็นการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ซึ่งกำหนดไว้ 5 ลักษณะดังนี้

(1) การทำซ้ำหรือดัดแปลง

ตามคำนิยามของพระราชบัญญัติฉบับนี้ได้ให้ความหมายไว้ค่อนข้างชัดเจนว่า “ทำซ้ำ” หมายความรวมถึง คัดลอกไม่ว่าโดยวิธีใด ๆ เลียนแบบ ทำสำเนา ทำแม่พิมพ์ บันทึก เสียง บันทึกภาพ หรือบันทึกเสียงและภาพ จากต้นฉบับ จากสำเนา หรือจากการโฆษณาในส่วนอันเป็นสาระสำคัญ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน สำหรับในส่วนที่เกี่ยวกับโปรแกรมคอมพิวเตอร์ให้หมายความถึง คัดลอกหรือทำสำเนาโปรแกรมคอมพิวเตอร์จากสื่อบันทึกใด ไม่ว่าด้วยวิธีใดๆในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำงานขึ้นใหม่ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน

“ดัดแปลง” หมายความว่า “ทำซ้ำโดยเปลี่ยนรูปใหม่ ปรับปรุงแก้ไขเพิ่มเติม หรือจำลองงานต้นฉบับในส่วนอันเป็นสาระสำคัญโดยไม่มีลักษณะเป็นการจัดทำงานขึ้นใหม่ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน

ในส่วนที่เกี่ยวกับวรรณกรรม ให้หมายความรวมถึง แปลวรรณกรรม เปลี่ยนรูปวรรณกรรมหรือรวบรวมวรรณกรรมโดยคัดเลือกและจัดลำดับใหม่

---

[12] อำนวย แสงสว่าง, **กฎหมายทรัพย์สินทางปัญญา**, (กรุงเทพฯ: อักษราพิพัฒน์, 2544).

ในส่วนที่เกี่ยวกับโปรแกรมคอมพิวเตอร์ ให้หมายความรวมถึง ทำซ้ำโดยเปลี่ยนรูปใหม่ ปรับปรุง แก้ไขเพิ่มเติมโปรแกรมคอมพิวเตอร์ในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่

ในส่วนที่เกี่ยวกับนาฏกรรม ให้หมายความรวมถึง เปลี่ยนงานที่มิใช่นาฏกรรมให้เป็นนาฏกรรม หรือเปลี่ยนนาฏกรรมให้เป็นงานที่มิใช่นาฏกรรม ทั้งนี้ ไม่ว่าในภาษาเดิมหรือต่างภาษากัน

ในส่วนที่เกี่ยวกับศิลปกรรม ให้หมายความรวมถึง เปลี่ยนงานที่เป็นรูปสองมิติหรือสามมิติ ให้เป็นรูปสามมิติหรือสองมิติ หรือทำหุ่นจำลองจากงานต้นฉบับ

ในส่วนที่เกี่ยวกับดนตรีกรรม ให้หมายความรวมถึง จัดลำดับเรียบเรียงเสียงประสานหรือเปลี่ยนคำร้องหรือทำนองใหม่”

(2) การเผยแพร่ต่อสาธารณชน

“เผยแพร่ต่อสาธารณชน” หมายความว่า “ทำให้ปรากฏต่อสาธารณชน โดยการแสดง การบรรยาย การสวด การบรรเลง การทำให้ปรากฏด้วยเสียงและหรือภาพ การก่อสร้าง การจำหน่าย หรือโดยวิธีอื่นใดซึ่งงานที่ได้จัดทำขึ้น

(3) การให้เช่าต้นหรือสำเนางานโปรแกรมคอมพิวเตอร์

(4) การจัดทำโสตทัศนวัสดุ ภาพยนตร์ และสิ่งบันทึกเสียงหรืองานแพร่เสียงแพร่ภาพทั้งหมดหรือบางส่วน

(5) การแพร่เสียง แพร่ภาพซ้ำทั้งหมดหรือบางส่วน

เมื่อการละเมิดลิขสิทธิ์ในลักษณะข้างต้นทั้ง 5 ประการเกิดขึ้นบนระบบคอมพิวเตอร์ เช่น การนำภาพซึ่งมีลิขสิทธิ์ของผู้อื่นมาใช้โดยไม่ได้รับอนุญาต หรือการให้บริการชมหนังออนไลน์โดยเสียค่าสมาชิก ซึ่งมิได้ขออนุญาตจากเจ้าของลิขสิทธิ์ นับว่าเป็นการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต และลงโทษผู้กระทำผิดโดยใช้พระราชบัญญัติฉบับนี้ได้ อย่างไรก็ตาม การกระทำบางประการแม้จะกระทำต่องานอันมีลิขสิทธิ์โดยไม่ได้รับอนุญาตก็อาจได้รับการยกเว้นว่าไม่เป็นการกระทำละเมิดได้หากเป็นการกระทำที่ไม่ขัดต่อการแสดงหาประโยชน์ตามปกติของเจ้าของลิขสิทธิ์ และไม่กระทบกระเทือนต่อสิทธิ์ของเจ้าของลิขสิทธิ์เกินสมควร เช่น การศึกษาวิจัยงานที่มิใช่เพื่อแสวงหากำไร เป็นต้น[13] โดยกฎหมายได้กำหนดข้อยกเว้นของการละเมิดลิขสิทธิ์ไว้ใน มาตรา 32 จำนวน 8 ลักษณะดังนี้

(1) การทำวิจัยหรือทำการศึกษางานอันมีลิขสิทธิ์ เช่นการทำสำเนางานศิลปะเพื่อใช้ศึกษาวิธีการทางเทคนิคใหม่ ๆ การทำสำเนาหนังสือทั้งฉบับเพื่อใช้

---

[13] คมน์ทนงชัย ฉายไพโรจน์, **กฎหมายทรัพย์สินทางปัญญาฉบับสมบูรณ์,** 19.

ประกอบการทำวิจัยหรือทำการศึกษา ทั้งนี้การกระทำดังกล่าวจะต้องมิใช่การกระทำเพื่อหากำไร เช่น การถ่ายเอกสารหนังสือไว้หลายชุดเพื่อใช้ขายแก่นักศึกษาที่ต้องการมาซื้อ แบบนี้เป็นการกระทำของผู้ขายเองเพื่อหากำไรจากการขายงานทำซ้ำมิใช่กรณีที่ได้รับยกเว้นดังเช่นที่นักศึกษามาขอถ่ายสำเนาเพื่อใช้ในการศึกษา

(2) ใช้เพื่อประโยชน์ของตนเอง หรือเพื่อประโยชน์ของตนเองและบุคคลในครอบครัวหรือญาติสนิทโดยความหมายของคำว่าบุคคลในครอบครัวหมายถึงเฉพาะแต่ครอบครัวและญาติสนิทจริง ๆ เท่านั้น ไม่นับรวมไปถึงลูกพี่ลูกน้องด้วย[14]

(3) ติชม วิจารณ์ หรือแนะนำผลงานโดยมีการรับรู้ถึงความเป็นเจ้าของลิขสิทธิ์ในงานนั้นโดยการกระทำดังกล่าวจะต้องไม่กระทำเพื่อหาผลกำไร หากการกระทำติชม หรือวิจารณ์โดยมีการหารายได้จากการวิจารณ์ดังกล่าว เช่นทำเป็นหนังสือติชมหรือวิจารณ์ผลงานเพื่อออกจำหน่าย เช่นนี้ถือเป็นการละเมิดลิขสิทธิ์

(4) เสนอรายงานข่าวทางสื่อสารมวลชนโดยมีการรับรู้ถึงความเป็นเจ้าของลิขสิทธิ์ในงานนั้นโดยการเสนอรายงานข่าวจะต้องเป็นการให้ข่าวเท่านั้นจะหากำไรจากงานอันมีลิขสิทธิ์ไม่ได้

(5) ทำซ้ำ ดัดแปลง นำออกแสดง หรือทำให้ปรากฏ เพื่อประโยชน์ในการพิจารณาของศาลหรือเจ้าพนักงานซึ่งมีอำนาจตามกฎหมาย หรือในการทำรายงานพิจารณาดังกล่าว การกำหนดในข้อนี้เป็นข้อยกเว้นเพื่อให้เกิดความยุติธรรมในชั้นศาล อย่างไรก็ตามการเปิดเผยดังกล่าวยังคงอยู่ภายใต้ข้อบังคับที่ว่าจะไม่กระทบต่อการแสดงหากำไรของเจ้าของลิขสิทธิ์

(6) ทำซ้ำ ดัดแปลง นำออกแสดง หรือทำให้ปรากฏโดยผู้สอน เพื่อประโยชน์ในการสอนของตน อันมิใช่การกระทำเพื่อหากำไร ได้รับการยกเว้นเพราะกฎหมายต้องการให้โอกาสสาธารณชนได้รับรู้ความรู้ทางวิชาการซึ่งจะช่วยพัฒนาความรู้คนในสังคมและนำไปพัฒนาสังคมและพัฒนาวิชาการในด้านนั้นให้เจริญยิ่งขึ้นต่อไป

(7) ทำซ้ำ ดัดแปลงบางส่วนของงาน หรือตัดทอนหรือทำบทสรุปโดยผู้สอนหรือสถาบันศึกษา เพื่อแจกจ่ายหรือจำหน่ายแก่ผู้เรียนในชั้นเรียนหรือในสถาบัน ทั้งนี้ ต้องไม่เป็นการกระทำเพื่อหากำไร

(8) นำงานนั้นมาใช้เป็นส่วนหนึ่งในการถามและตอบในการสอบเนื่องจากเป็นการกระทำเพื่อการศึกษาโดยแท้จริง กฎหมายจึงกำหนดให้เป็นข้อยกเว้นไว้

---

[14] จิตฤดี วีระเวสล์, **สรุปย่อหลักกฎหมายทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ**, (กรุงเทพฯ: อภิโชติ, 2555), 65.

ทั้งนี้ การกระทำทั้งแปดประการข้างต้นจะได้รับการยกเว้นว่าไม่เป็นการละเมิดลิขสิทธิ์ก็ต่อเมื่อเข้าเงื่อนไขประกอบอีกสองประการคือ

ประการแรก การกระทำนั้นต้องไม่ขัดต่อการแสดงหาประโยชน์จากงานอันมีลิขสิทธิ์ตามปกติของเจ้าของลิขสิทธิ์

ประการที่สองการกระทำนั้นต้องไม่กระทบกระเทือนถึงสิทธิอันชอบด้วยกฎหมายของเจ้าของลิขสิทธิ์เกินสมควร

หากขาดเงื่อนไขประการใดประการหนึ่ง แม้จะเป็นการกระทำเพื่อแปดประการข้างต้นก็ยังถือว่าเป็นการละเมิดลิขสิทธิ์และต้องมมีความผิดตามพระราชบัญญัตินี้

4) มาตรการลงโทษการละเมิดลิขสิทธิ์ตามกฎหมายไทย

พระราชบัญญัติลิขสิทธิ์กำหนดโทษไว้ทั้งโทษปรับและโทษจำคุกเป็นกฎหมายที่มีโทษทางอาญา โดยมีมาตรการลงโทษดังต่อไปนี้

(4.1) ผู้กระทำการละเมิดลิขสิทธิ์ โดยการทำซ้ำ เผยแพร่หรือให้เช่าต่อสารธารณะชนซึ่งงานโสตทัศนวัสดุ ภาพยนตร์ หรือสิ่งบันทึกเสียง ตามมาตรา 28 และ 29 หรือ ละเมิดสิทธิของนักแสดง โดยการเผยแพร่ บันทึกการแสดง หรือทำซ้ำสิ่งบันทึกการแสดง รวมถึงการเผยแพร่ซึ่งการแสดงโดยไม่ได้รับอนุญาตจากนักแสดงตามมาตรา 44 และ 45 ประกอบมาตรา 52 จะมีความผิดทางอาญาต้องระวางโทษปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาทตามที่บัญญัติไว้ในมาตรา 69 และ ถ้าการกระทำความผิดดังกล่าวเป็นการกระทำเพื่อการค้าผู้กระทำต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงสี่ปี หรือปรับตั้งแต่หนึ่งแสนบาทถึงแปดแสนบาท หรือทั้งจำทั้งปรับ ตามมาตรา 69 วรรค 2

(4.2) ผู้กระทำการหากำไรจากงานอันมีลิขสิทธิ์ของผู้อื่นโดยรู้อยู่แล้วหรือควรรู้ว่างานนั้นมีลิขสิทธิ์ โดยขาย มีไว้ขาย เสนอขาย ให้เช่า เผยแพร่ต่อสาธารณชน แจกจ่ายในลักษณะที่จะทำให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์ หรือนำเข้ามาในราชอาณาจักร อันเป็นการละเมิดลิขสิทธิ์ตามมาตรา 30 ต้องระวางโทษระวางโทษปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนบาท ตามมาตรา 70 และถ้าการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำเพื่อการค้า ผู้กระทำต้องระวางโทษจำคุกตั้งแต่สามเดือนถึงสองปี หรือปรับตั้งแต่ห้าหมื่นบาทถึงสี่แสนบาท หรือทั้งจำทั้งปรับตามมาตรา 70 วรรค 2

2.1.3.2.2 การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1) หลักการและเหตุผลของกฎหมาย

ในการประชุมครั้งที่ 6/2549 ของภานิติบัญญัติแห่งชาติเมื่อวันพุธที่ 15 พฤศจิกายน 2549 ได้พิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยมีหลักการคือ “ให้มีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์” และเหตุผล

คือ “เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูลแก้ไขหรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบหรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจารย่อมก่อให้เกิดความเสียหายกระทบกระเทือนต่อเศรษฐกิจสังคมและความมั่นคงของรัฐรวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชนสมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าวจึงจำเป็นต้องตราพระราชบัญญัตินี้”โดยสภามีมติรับหลักการ และตั้งคณะกรรมาธิการวิสามัญขึ้นคณะหนึ่งเพื่อพิจารณาร่างพระราชบัญญัติฉบับนี้ โดยพิจารณาแล้วเสร็จในเดือนพฤษภาคม 2550 มีการลงมติให้ความเห็นชอบในวาระ 3 และนายกรัฐมนตรีนำร่างพระราชบัญญัติขึ้นทูลเกล้าฯและพระมหากษัตริย์ได้ทรงลงพระปรมาภิไธย โดยได้มีการประกาศลงในราชกิจจานุเบกษาเมื่อวันที่ 18 มิถุนายน 2550

2) ความเกี่ยวข้องกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

เมื่อพิจารณาจากหลักการและเหตุผลแล้วกฎหมายนี้มีขึ้นเพื่อต้องการป้องกันและปราบปรามการกระทำใด ๆ บนระบบคอมพิวเตอร์ที่จะก่อให้เกิดความเสียหายแก่สังคมและบุคคลอื่นได้ ซึ่งการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตก็เป็นหนึ่งในสิ่งที่กระทำให้เกิดการทำลายระบบเศรษฐกิจและสังคมที่กระทำบนระบบคอมพิวเตอร์เช่นเดียวกัน แต่กฎหมายฉบับนี้ก็มิได้พูดถึงหรือมุ่งประเด็นเกี่ยวกับลิขสิทธิ์แต่อย่างใด อย่างไรก็ตามกฎหมายฉบับนี้ไม่ได้มีการกล่าวถึงการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตหรือผ่านระบบคอมพิวเตอร์ไว้โดยตรง แต่มีบทบัญญัติซึ่งในทางปฏิบัติมีการนำมาปรับใช้กับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้ดังนี้

(2.1) ความผิดเกี่ยวกับการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ถูกกำหนดให้มีความผิดตามมาตรา 9 แห่งพระราชบัญญัติฉบับนี้ เนื่องจากข้อมูลคอมพิวเตอร์นั้น หากถูกตัดทอนหรือเปลี่ยนแปลง อาจส่งผลให้ข้อมูลที่มีอยู่สูญหายหรือเสียหายได้ โดยลักษณะการกระทำความผิดตามฐานนี้นั้นอาจกระทำด้วยตนเองโดย กระทำผ่านคีย์บอร์ดของคอมพิวเตอร์เครื่องนั้นโดยตรง หรือ กระทำโดยระยะไกล (Remote Access) เช่น การปล่อยไวรัสคอมพิวเตอร์ เมล์บอมพ์ โทรจัน รวมถึงการส่งโปรแกรมไม่พึงประสงค์[15] โดยการส่งไวรัสเข้าคอมพิวเตอร์ไวรัสจะเข้าไปแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของเครื่อง ๆ นั้น และอาจส่งไวรัสกระจายไปยังเครื่อง

[15] ไพบูลย์ อมรภิญโญเกียรติ, **คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550**, (กรุงเทพฯ: โปรวิชั่น, 2553), 52.

อื่น ๆ ต่อไปกฎหมายจึงกำหนดบทลงโทษเพื่อป้องกันการกระทำความผิดไว้

สำหรับส่วนของการละเมิดลิขสิทธิ์ กรณีที่แก้ไขเปลี่ยนแปลงงานอันมีลิขสิทธิ์ซึ่งมีรูปแบบเป็นข้อมูลคอมพิวเตอร์ โดยเข้าลักษณะความผิดตามมาตรา 9 ลักษณะเป็นเช่นเดียวกับการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ในส่วนของการดัดแปลง หรือแก้ไขงานอันมีลิขสิทธิ์ อันเป็นความผิดฐานละเมิดลิขสิทธิ์อยู่ในตัว ย่อมสามารถปรับเข้าสู่กฎหมายทั้งสองฉบับได้ อย่างไรก็ตาม ในส่วนของการทำซ้ำ และเผยแพร่ต่อสาธารณชนซึ่งงานอันมีลิขสิทธิ์ อันเป็นการละเมิดลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ไม่ปรากฏในมาตรา 9 หรือมาตราอื่น ๆ ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้น หากเกิดกรณีความผิดละเมิดลิขสิทธิ์บนอินเทอร์เน็ตในลักษณะนี้ ย่อมไม่สามารถนำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาปรับใช้ได้

(2.2) ความผิดเกี่ยวกับการเผยแพร่ข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย

มาตรา 14 และ 16 การกระทำความผิดจะเป็นความผิดในแง่ของเนื้อหาของข้อมูลคอมพิวเตอร์ที่มีลักษณะเป็นข้อมูลคอมพิวเตอร์ปลอมหรือข้อมูล คอมพิวเตอร์อันเป็นเท็จ หรือ ข้อมูลรูปภาพที่มีการตัดต่อดัดแปลง ที่ผู้กระทำนำไปเผยแพร่หรือทำให้แพร่หลาย โดยลักษณะการกระทำความผิดคือการนำข้อมูลดังกล่าวเข้าสู่ระบบคอมพิวเตอร์ ไม่ว่าระบบคอมพิวเตอร์นั้นจะเป็นของใครก็ตาม เช่น การส่งข้อมูลคอมพิวเตอร์ปลอมผ่านทางอีเมล์ หรือแม้แต่การเขียนข้อมูลคอมพิวเตอร์ดังกล่าวลงบนกระดานข้อความในเว็บไซต์ของตนเองก็เป็นความผิดเช่นเดียวกัน เพราะมีการนำเข้าสู่ระบบคอมพิวเตอร์แล้ว ทั้งนี้ ข้อมูลคอมพิวเตอร์ปลอมหรือเท็จ อาจเป็นข้อมูลที่มีการลอกเลียนมาจากข้อมูลแท้ที่มีลิขสิทธิ์หรือมีทรัพย์สินทางปัญญาอยู่ หรือ รูปภาพที่มีการดัดแปลงแล้วกระทำความผิดในส่วนนี้ก็อาจเป็นรูปที่ถูกดัดแปลงโดยละเมิดลิขสิทธิ์ได้เช่นเดียวกัน ส่วนนี้จึงเป็นอีกส่วนหนึ่งที่มีความเกี่ยวโดยงกับการละเมิดทรัพย์สินทางปัญญา ซึ่งการกระทำบางอย่างอาจมีความผิดทั้งในทางทรัพย์สินทางปัญญาและทางอาชญากรรมทางคอมพิวเตอร์ด้วย

แต่แม้ทั้งสองมาตราดังกล่าวข้างต้นจะเกิดการเกี่ยวโยงกับกฎหมายทรัพย์สินทางปัญญา แต่เมื่อพิจารณาศึกษาถึงเจตนารมณ์ของกฎหมายในแต่ละมาตรานั้นๆในช่วงที่ยกร่างกฎหมายฉบับดังกล่าวพบว่าไม่ได้มีการกล่าวถึงทรัพย์สินทางปัญญาแต่อย่างใด ดังนั้นแม้โดยหลักการภาพรวมอาจนับรวมทรัพย์สินทางปัญญาที่จะได้รับความคุ้มครองด้วยตามกฎหมายนี้ แต่บทบัญญัติข้างต้นไม่ใช่ลักษณะของการกำหนดความผิดเพื่อลงโทษผู้กระทำการละเมิดทรัพย์สินทางปัญญาแต่อย่างใด จึงต้องศึกษาและวิเคราะห์ต่อไปว่าทางปฏิบัติในปัจจุบันที่มีการนำสองมาตราดังกล่าวมาใช้กับคดีที่ความจริงแล้วเป็นการละเมิดทรัพย์สินทางปัญญาโดยมีระบบคอมพิวเตอร์เข้ามาเกี่ยวข้องด้วยเท่านั้นโดยไม่ได้เป็นการทำลายระบบคอมพิวเตอร์แต่อย่างใด จะควร

นำมาใช้บังคับเช่นนี้ต่อไปหรือไม่ หรือโดยหลักการแล้วสามารถนำมาใช้ได้อย่างที่ใช้อยู่ในปัจจุบันหรือไม่ เนื่องจากบทลงโทษมีความผิดร้ายแรงกว่าความผิดในทางทรัพย์สินทางปัญญา จึงอาจเกิดประเด็นในทางกระบวนการยุติธรรมได้ว่าความผิดเหล่านี้เหมาะสมสำหรับเหตุที่ละเมิดทรัพย์สินทางปัญญาเพียงอย่างเดียวหรือไม่

(2.3) ความรับผิดของผู้ให้บริการกับการเผยแพร่ข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย

ในกรณีที่เกิดการกระทำความผิดตามมาตรา 14 เกี่ยวกับการเปลี่ยนแปลงหรือนำเข้าข้อมูลจราจรงาคอมพิวเตอร์ที่เป็นเท็จ นอกจากตัวผู้กระทำโดยตรงจะมีความผิดแล้วกฎหมายได้กำหนดความผิดเกี่ยวกับผู้ให้บริการที่จงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดดังกล่าวมีความผิดและต้องระวางโทษเช่นเดียวกับผู้ที่กระทำความผิดด้วย ตามมาตรา 15 ดังนั้นในการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต หากเข้าสู่ลักษณะของการกระทำดังกล่าวย่อมส่งผลให้ผู้ให้บริการต้องร่วมรับผิดกับผู้กระทำความผิดด้วย ซึ่งตามกฎหมายลิขสิทธิ์ยังไม่ได้มีการกล่าวมาถึงผู้ให้บริการที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์ดังกล่าวพระราชบัญญัติฉบับนี้ จึงอาจเป็นประเด็นสงสัยว่า ผู้ให้บริการจะต้องรับผิดในการละเมิดลิขสิทธิ์ที่เกิดขึ้นบนการควบคุมหรือดูแลการให้บริการของตนเองอย่างไร และเป็นธรรมต่อผู้ให้บริการแล้วหรือสำหรับการบังคับใช้กฎหมายในลักษณะดังกล่าว

อย่างไรก็ตาม ร่างพระราชบัญญัติลิขสิทธิ์ (ฉบับที่....) พ.ศ ..... ที่ผ่านการพิจารณาจากคณะรักษาความสงบแห่งชาติเมื่อวันที่ 13 สิงหาคม พ.ศ. 2557 และเสนอสู่การพิจารณาสภานิติบัญญัติ ได้มีการวางหลักเกณฑ์เพิ่มเติมเกี่ยวกับลิขสิทธิ์โดยมีการกล่าวถึงการละเมิดลิขสิทธิ์คอมพิวเตอร์ลิขสิทธิ์ โดยมีหลักการว่าหากมีการละเมิดลิขสิทธิ์ในระบบคอมพิวเตอร์ของผู้ให้บริการเกิดขึ้นเจ้าของลิขสิทธิ์สามารถร้องขอต่อศาลเพื่อสั่งให้ผู้ให้บริการระงับการเผยแพร่หรือการกระทำใดแก่ผู้มูลดังกล่าวที่เกิดการละเมิดลิขสิทธิ์ขึ้นได้ตามร่างพระราชบัญญัติลิขสิทธิ์ฯ มาตรา 32/3 โดยผู้ให้บริการในมาตราดังกล่าวได้ให้ความหมายว่า

“(1) ผู้ให้บริการในการเข้าสู่อินเทอร์เน็ตหรือติดต่อกันโดยประการอื่นผ่านระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น”

ดังนั้น การละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของผู้ให้บริการจึงหมายถึงการละเมิดลิขสิทธิ์บนระบบอินเทอร์เน็ตหรือระบบที่มีการติดต่อสื่อสารผ่านผู้ให้บริการ อันส่งผลให้เกิดแนวปฏิบัติใหม่ขึ้นเมื่อมีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต คือเจ้าของลิขสิทธิ์สามารถร้องขอต่อศาลเพื่อมีคำสั่งบังคับแก่ผู้ให้บริการต่อไปหากมีหลักฐานเพียงพออันเชื่อได้

ว่ามีการกระทำความผิดเกิดขึ้นบนระบบของผู้ให้บริการ ซึ่งแตกต่างจากเดิมที่มิได้กล่าวถึงการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตไว้แต่อย่างใด และการที่ปรับมาเข้าสู่พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 ก็ไม่ได้มีการกำหนดหน้าที่ของผู้ให้บริการว่าจะต้องดำเนินการอย่างไร เพียงแต่เป็นการกำหนดความผิดไว้หากมีการกระทำผิดตามมาตรา 14 ในพระราชบัญญัตินี้

ทั้งนี้ ในมาตรา 32/4 ของร่างพระราชบัญญัติลิขสิทธิ์ ยังมีการกล่าวถึงข้อยกเว้นความผิดของผู้ให้บริการไว้ในวรรคท้ายว่า “ในกรณีที่ผู้ให้บริการไม่ใช่ผู้ควบคุมริเริ่ม หรือสั่งการให้มีการละเมิดลิขสิทธิ์ในระบบคอมพิวเตอร์ของผู้ให้บริการ และผู้ให้บริการนั้นได้ดำเนินการตามคำสั่งศาลตามวรรคสี่แล้วผู้ให้บริการไม่ต้องรับผิดเกี่ยวกับการกระทำที่อ้างว่าเป็นการละเมิดลิขสิทธิ์ที่เกิดขึ้นก่อนศาลมีคำสั่งและหลังจากคำสั่งศาลเป็นอันสิ้นผลแล้ว” ดังนั้นหากร่างพระราชบัญญัติลิขสิทธิ์นี้ผ่านการพิจารณาและบังคับใช้ จะส่งผลให้ผู้ให้บริการที่ดำเนินการตามคำสั่งศาลเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตย่อมไม่ต้องรับผิดเกี่ยวกับการกระทำความผิดที่อ้างว่าเป็นการละเมิดลิขสิทธิ์ที่เกิดขึ้นบนระบบคอมพิวเตอร์ของตน ซึ่งแตกต่างจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ไม่มีการกำหนดข้อยกเว้นให้แก่ผู้ให้บริการไว้แต่ประการใด นอกจากนั้นจะส่งผลให้เกิดความคุ้มครองในทางลิขสิทธิ์บนอินเทอร์เน็ตมากยิ่งขึ้น โดยผู้ให้บริการซึ่งปรากฏการละเมิดลิขสิทธิ์บนการให้บริการของตนจะต้องระมัดระวังเพื่อให้ให้ถูกคำสั่งจากศาลเพราะอาจจะกระทบต่อการให้บริการของตนในทางธุรกิจได้ เช่นถูกสั่งให้ระงับการให้บริการเป็นการชั่วคราวจนกว่าจะมีการนำงานอันละเมิดลิขสิทธิ์ออกจากระบบการให้บริการของตน เป็นต้น

(2.4) ความผิดเกี่ยวกับการหลีกเลี่ยงมาตรการทางเทคโนโลยี

กฎหมายให้ความคุ้มครองแก่ข้อมูลคอมพิวเตอร์ที่มาตรการป้องกันการเข้าถึง ซึ่งบุคคลอื่นไม่สามารถเข้าถึงได้ และหากมีการเข้าถึงข้อมูลดังกล่าวโดยมิชอบยอมมีความผิดตามมาตรา 7[16] และกรณีที่งานอันมีลิขสิทธิ์ ซึ่งถือเป็นข้อมูลคอมพิวเตอร์ มีการใช้มาตรการทางเทคโนโลยีเพื่อป้องกันการเข้าถึงไว้ (Technological Protection Measures – TPM) งานนั้นก็ได้รับความคุ้มครองตามมาตรา 7 ด้วย[17]

มาตรการป้องกันการเข้าถึงอาจเป็นการใส่รหัส หรือการใช้โปรแกรมสำเร็จรูปในการจัดเก็บข้อมูลโดยต้องมีวิธีการเฉพาะที่ระบุตัวตนก่อนเข้าสู่ข้อมูลจึงจะสามารถ

---

[16] มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ”.

[17] อรพรรณ พนัสพัฒนา, “บทบาทของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการป้องกันงานอันมีลิขสิทธิ์”, **วารสารกฎหมายทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ** 10 (2550): 38-73.

เข้าสู่ข้อมูลที่จัดเก็บไว้ได้ เป็นต้น ซึ่งการกระทำโดยมิชอบในที่นี้ คือ การกระทำโดยมีเจตนาผ่านมาตรการป้องกันการเข้าถึง แล้วเข้าถึงข้อมูลดังกล่าวโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล รวมถึงกรณีที่รู้รหัสมาโดยมิชอบแล้วนำรหัสดังกล่าวมาใส่เพื่อเข้าสู่ข้อมูล โดยเจ้าของข้อมูลไม่ได้อนุญาต แต่หากเป็นกรณีที่เจ้าของข้อมูลตั้งการจดจำรหัสผ่านไว้ เช่นนี้จะถือว่ามีมาตรการป้องกันไม่ได้ เพราะว่าทุกคนสามารถกดเพื่อเข้าตามที่เจ้าของข้อมูลได้ใส่รหัสไว้ เช่นนี้ไม่เป็นความผิดตามมาตรา 7

สำหรับความคุ้มครองตามมาตรา 7 นี้ ทำให้เกิดประเด็นสงสัยว่า ที่ห้ามหลีกเลี่ยงการเข้าถึงงานอันมีลิขสิทธิ์ได้นั้น เป็นการขยายสิทธิ แต่เพียงผู้เดียวของเจ้าของลิขสิทธิ์ตามมาตรา 15 ของพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 หรือไม่ โดยอรพรรณ พนัสพัฒนา เห็นว่า มาตรา 7 มีไว้เพื่อปกป้องข้อมูลของบุคคลในระบบคอมพิวเตอร์จากการล่วงรู้ของบุคคลอื่น ซึ่งการคุ้มครองอยู่ภายใต้กฎหมายเรื่องความผิดเกี่ยวกับคอมพิวเตอร์ มิใช่เป็นการขยายสิทธิ์แต่เพียงผู้เดียวซึ่งเป็นสาขาของกฎหมายทรัพย์สินทางปัญญาแต่อย่างใด

อย่างไรก็ตาม ประเด็นปัญหาของการใช้มาตรา 7 กับมาตรการป้องกันการเข้าถึงข้อมูลลิขสิทธิ์นั้น พบว่ามีข้อยกเว้นเพียงประการเดียวคือการเข้าถึงข้อมูลคอมพิวเตอร์ เพื่อนำไปใช้เป็นพยานหลักฐานโดยพนักงานเจ้าหน้าที่ซึ่งได้รับอนุญาตจากศาล ทั้งที่ข้อมูลดังกล่าวที่มีมาตรการป้องกันการเข้าถึงอาจเป็น กฎหมาย หรืองานอันไม่มีลิขสิทธิ์ หรืองานลิขสิทธิ์ที่หมดอายุความคุ้มครองแล้ว หรืองานที่อาจเป็นประโยชน์ต่อสาธารณะชนซึ่งอาจใช้ได้โดยเป็นธรรมนั้นจะไม่มีการยกเว้นให้สามารถเข้าถึงได้[18] ซึ่งในส่วนของพระราชบัญญัติลิขสิทธิ์มีข้อยกเว้นในเรื่องดังกล่าวไว้มากกว่า

ทั้งนี้ ร่างพระราชบัญญัติลิขสิทธิ์ (ฉบับที่....) พ.ศ..... ได้กำหนดความผิดเกี่ยวกับการละเมิดมาตราการทางเทคโนโลยีไว้เป็นการเฉพาะ ในมาตรา 53/4 และมีการกำหนดข้อยกเว้นกรณีที่มิให้ถือว่าเป็นการละเมิดมาตราการทางเทคโนโลยีไว้ด้วย ดังนั้นในอนาคตหากพระราชบัญญัติแบบนี้บังคับใช้ เมื่อปรากฏว่ามีเข้าถึงงานอันมีลิขสิทธิ์ด้วยวิธีการละเมิดมาตราการป้องกันทางเทคโนโลยีตามมาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นอกจากจะมีความผิดตามพระราชบัญญัติดังกล่าวแล้ว ยังต้องมีความผิดตามพระราชบัญญัติลิขสิทธิ์ อันเป็นเรื่องเกี่ยวกับลิขสิทธิ์โดยเฉพาะอีกด้วย

[18] เรื่องเดียวกัน, 66.

2.2 พยานหลักฐานที่เกิดจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

2.2.1 พยานหลักฐานทั่วไป

ในการกระทำความผิดทุกการกระทำย่อมก่อให้เกิดพยานหลักฐาน ผู้กระทำความผิดบางคนจึงพยายามที่จะลบหรือทำลายหลักฐานเพื่อไม่ให้สามารถสืบไปยังตัวผู้กระทำความผิดได้ เช่นเดียวกับการการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต การกระทำความผิดย่อมประกอบด้วย ผู้กระทำ สิ่งที่ใช้ในการกระทำความผิด สิ่งที่ถูกกระทำความผิด และผู้เสียหาย แม้การกระทำความผิดจะเป็นการกระทำบนระบบอินเทอร์เน็ตและพยานหลักฐานส่วนใหญ่อยู่ในรูปของข้อมูลดิจิตอลหรือข้อมูลคอมพิวเตอร์ แต่ก็ยังคงปรากฏพยานหลักฐานในลักษณะของพยานหลักฐานทั่วไปอันได้แก่ เครื่องคอมพิวเตอร์ที่ใช้ในการกระทำความผิด ภาพหรือกล้องวงจรปิด พยานบุคคลที่เห็นว่าบุคคลใดเป็นผู้กระทำความผิด หรือพยานผู้เชี่ยวชาญ

ตามหลักกฎหมายการแบ่งพยานหลักฐานสามารถแบ่งด้วยลักษณะ เนื้อหาสาระ หรือวิธีการนำพยานหลักฐานเข้าสืบก็ได้การแบ่งพยานหลักฐานที่เป็นที่ยอมรับกันทั่วไป คือการแบ่งพยานหลักฐานเป็นสามประเภทได้แก่ พยานบุคคล พยานเอกสาร และพยานวัตถุ ทั้งในตำรากฎหมายลักษณะพยานของต่างประเทศและของไทยเรา[19] ประมวลกฎหมายวิธีพิจาณาความอาญา มาตรา 226 ก็บัญญัติรับรองว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคล ซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีความผิดหรือบริสุทธ์ ให้อ้างเป็นพยานหลักฐานได้” อนึ่ง บทบัญญัติอันเกี่ยวด้วยพยานหลักฐานในประมวลกฎหมายวิธีพิจารณาความแพ่งก็ดี ในประมวลกฎหมายวิธีพิจารณาความอาญาก็ดี ได้แยกบัญญัติพยานทั้ง 3 ประเภทนี้ออกจากกัน เพราะพยานหลักฐานทั้ง 3 ประเภทนี้มีวิธีการนำสืบและข้อห้ามบางประการแตกต่างกัน ทั้งพยานหลักฐานบางประเภทเหมาะสมหรือมีน้ำหนักแตกต่างกันด้วย[20] โดยพยานแต่ละประเภทมีลักษณะดังนี้

พยานบุคคล คือบุคคลที่มาเบิกความให้ข้อเท็จจริงในคดีต่อศาล ศาลรับรู้ข้อเท็จจริงจากพยานชนิดนี้โดยการที่พยานเล่าเรื่อง หรือตอบคำถามของศาลหรือคู่ความเกี่ยวกับข้อเท็จจริงหรือเหตุการณ์ที่พยานได้เห็นได้ฟังหรือได้ทราบมาก่อน ความจริงแล้วสิ่งที่เป็นพยานหลักฐานก็คือ คำเบิกความหรือถ้อยคำของพยาน หาใช่ตัวพยานเองไม่ ฉะนั้นเมื่อกล่าวถึงพยานชนิดนี้จึงหมายถึง คำเบิกความของพยาน หรือบางทีก็เรียกว่าเป็น พยานถ้อยคำ และเนื่องจากศาลต้องบันทึกคำเบิกความของพยานเป็นลายลักษณ์อักษรเก็บรวมไว้ในสำนวนเพื่อเป็นพยานหลักฐานในการวินิจฉัยคดี พยานบุคคลจึงหมายถึง

---

[19] โอสถ โกศิน, **คำอธิบายกฎหมายลักษณะพยานหลักฐาน**, พิมพ์ครั้งที่ 3 (กรุงเทพฯ: หอรัตนชัยการพิมพ์, 2538).

[20] โสภณ รัตนากร, **คำอธิบายกฎหมายลักษณะพยาน**, พิมพ์ครั้งที่ 9 (กรุงเทพฯ: นิติบรรณการ, 2551).

บันทึกคำพยานที่ปรากฏอยู่ในสำนวน ซึ่งใช้ในการตัดสินคดีนั้นเองด้วย แต่ถ้าบันทึกคำพยานดังกล่าวนำไปใช้ในอีกคดีหนึ่งก็อาจกลายเป็นพยานเอกสารไป[21]

พยานเอกสาร หมายถึง ข้อมูลที่บันทึกไว้ในสื่อชนิดใดก็ตามสามารถพิสูจน์ข้อเท็จจริงที่พิพาทในคดีได้และนำสืบชนิดที่บันทึกข้อมูลดังกล่าวนั้นมาใช้เป็นพยานหลักฐาน[22] และหมายถึงสิ่งซึ่งมีการบันทึกตัวอักษร ตัวเลข รูปรอยหรือเครื่องหมายซึ่งสามารถแสดงข้อความหรือความหมายอย่างใดอย่างหนึ่งให้ศาลดูได้[23] หรือข้อความใด ๆ ในเอกสารที่มีการอ้างอิงเป็นพยานโดยอาศัยการสื่อความหมายของข้อความนั้นพิสูจน์ความจริง[24]

พยานวัตถุ ได้แก่วัตถุหรือสิ่งใดที่อาจพิสูจน์ความจริงต่อศาลได้โดยการตรวจดูมิใช่โดยการอ่านหรือพิจารณาข้อความที่บันทึกไว้[25] หรือ สิ่งของใด ๆ ที่คู่ความอ้างอิงให้ศาลตรวจดูเพื่อประโยชน์แก่คดีของตน พยานวัตถุมีความสำคัญมากในคดีอาญาเพราะเป็นพยานที่ดีที่สุดในการพิสูจน์ว่าข้อเท็จจริงบางประเด็นได้เกิดขึ้น เช่นยาเสพติด หรือไม้ของกลางในคดี ปลอกกระสุนปืน บาดแผลที่ถูกทำร้าย สถานที่เกิดเหตุของกลางจากการละเมิดทรัพย์สินทางปัญญา ส่วนในคดีแพ่งส่วนมากอาจเป็นการไปตรวจดูที่ดินพิพาทเพื่อดูหลักเขตที่ฟ้องร้องกัน

การรับฟังพยานวัตถุไม่มีข้อจำกัดโดยกฎหมายดังนั้นพยานวัตถุที่มีการอ้างอิงในบัญชีพยานโดยถูกต้องตามระเบียบแล้วก็สามารถนำเข้าสืบได้เสมอและไม่มีข้อบังคับว่าข้อเท็จจริงใดจะต้องพิสูจน์ด้วยพยานวัตถุหรือห้ามพิสูจน์ด้วยพยานวัตถุ จึงอยู่ในดุลพินิจของคู่ความที่จะพิจารณาว่าควรนำสืบข้อเท็จจริงด้วยพยานวัตถุหรือไม่[26]

ดังนั้น ลักษณะของพยานหลักฐานทั่วไปจะเป็นวัตถุที่สามารถจับต้องได้หรือเป็นพยานบุคคลที่สามารถให้ถ้อยคำ ผู้ที่รับฟังหรือพิจารณาพยานหลักฐานจะสามารถเข้าใจและเห็นพยานหลักฐานดังกล่าวได้ด้วยตัววัตถุหรือถ้อยคำพยานนั้น ๆ และพิจารณาไตร่ตรองได้ด้วยตนเองว่าพยานหลักฐานดังกล่าวมีความน่าเชื่อถือมาอกน้อยเพียงใด เมื่อประกอบกับการกระทำและพยานแวดล้อมอื่น ๆ ทำให้ในส่วนของการจัดเก็บ และได้มาซึ่งพยานหลักฐานทั่วไปจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตนั้นเป็นไปตามขั้นตอนปกติ พนักงานสอบสวนย่อมมีอำนาจในการได้มาซึ่งพยานหลักฐานต่าง ๆ และสืบหาตัวผู้กระทำความผิดต่อไป ซึ่งแตกต่างจากพยานหลักฐานอิเล็กทรอนิกส์ที่มีความสลับซับซ้อนของข้อมูลที่

---

[21] ปิติกุล จีระมงคงพาณิชย์, **คำอธิบายกฎหมายลักษณะพยานว่าด้วยพยานเอกสาร**, พิมพ์ครั้งที่ 3 (กรุงเทพฯ: เดือนตุลา, 2552).

[22] เรื่องเดียวกัน, 52.

[23] โสภณ รัตนากร, **คำอธิบายกฎหมายลักษณะพยาน**, 55.

[24] โอสถ โกศิน, **คำอธิบายกฎหมายลักษณะพยานหลักฐาน**.

[25] โสภณ รัตนากร, **คำอธิบายกฎหมายลักษณะพยาน**, 55.

[26] โอสถ โกศิน, **คำอธิบายกฎหมายลักษณะพยานหลักฐาน**.

จะต้องใช้ความเชี่ยวชาญเฉพาะด้านเกี่ยวกับลักษณะเฉพาะของข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถจัดเก็บข้อมูลอิเล็กทรอนิกส์ให้มีความถูกต้องและคงความน่าเชื่อถือเพื่อให้ใช้เป็นพยานหลักฐานได้

2.2.2 พยานหลักฐานอิเล็กทรอนิกส์

การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตมีลักษณะการกระทำส่วนใหญ่อยู่บนระบบคอมพิวเตอร์และอินเทอร์เน็ต พยานหลักฐานที่จะนำไปสู่การจับกุมผู้กระทำความผิดได้ส่วนใหญ่จึงเป็นพยานหลักฐานในรูปของข้อมูลคอมพิวเตอร์ ซึ่งตามหลักกฎหมายลักษณะพยานนั้นได้กำหนดพยานไว้เพียง 3 ประเภท แต่สำหรับข้อมูลคอมพิวเตอร์ ที่เกิดจากการกระทำในทางคอมพิวเตอร์นั้น เกิดจากร่องรอยต่าง ๆ ที่ปรากฏเป็นลักษณะของข้อมูลอิเล็กทรอนิกส์ซึ่งไม่มีรูปแบบที่คงตัวแน่นอน โดยมีคุณสมบัติเฉพาะที่หากพิจารณาตามหลักเกณฑ์ในการจัดแบ่งพยานแบบดั้งเดิมซึ่งเป็นหลักเกณฑ์ที่ได้ตราไว้ก่อนที่จะมีพยานหลักฐานเหล่านี้ ทำให้ไม่อาจจัดกลุ่มเข้าเป็นพยานหลักฐานประเภทใดได้โดยตรงหรือชัดเจนแต่อย่างไรก็ตามเมื่อมีการใช้ระบบคอมพิวเตอร์มากขึ้น มีการติดต่อสื่อสาร ทำธุรกรรม โดยระบบคอมพิวเตอร์มากขึ้นจึงมีความจำเป็นอยู่เองที่ระบบกฎหมายจะต้องปรับตัวให้สอดคล้อง ซึ่งจะเห็นได้จากการที่เริ่มมีกฎหมายบัญญัติออกมารับรองข้อมูลในรูปแบบนี้ ถึงแม้ว่าอาจจะยังไม่สมบูรณ์มากนัก แต่เป็นการแสดงให้เห็นว่าพยานหลักฐานเหล่านี้ สามารถนำเข้าสู่กระบวนการทางกฎหมายและสามารถรับฟังเป็นพยานหลักฐานได้ เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในส่วนของกฎหมายลิขสิทธิ์ ปรากฏอยู่ในข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2540 ข้อ 33 ว่า “ศาลอาจรับฟังข้อมูลที่บันทึกโดยเครื่องคอมพิวเตอร์หรือประมวลผลโดยเครื่องคอมพิวเตอร์เป็นพยานหลักฐานในคดีได้..” โดยพยานหลักฐานอิเล็กทรอนิกส์ มีความหมาย ลักษณะและหลักเกณฑ์การจัดเก็บพยานหลักฐานดังต่อไปนี้

2.2.2.1 ความหมายของพยานหลักฐานอิเล็กทรอนิกส์

พยานหลักฐานอิเล็กทรอนิกส์ (Digital Evidence) หมายถึงข้อมูลหลักฐานที่ถูกจัดเก็บหรือ ถูก แปลงสภาพให้อยู่ในรูปดิจิตอล โดยคู่ความฝ่ายที่ยื่นต่อศาล โดยก่อนที่จะรับฟังศาลจะต้องพิจารณาถึงความเกี่ยวพันกับคดีและความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ดังกล่าวนั้นก่อนว่าพยานหลักฐานบอกเล่าหรือเป็นสำเนาดังกล่าวสามารถรับฟังได้หรือต้องใช้ต้นฉบับอย่างไร

หรือ พยานหลักฐานอิเล็กทรอนิกส์หมายถึง สิ่งที่แสดงหรือสามารถยืนยันการกระทำความผิด ซึ่งอยู่ในรูปแบบดิจิตอลหรือรูปแบบอิเล็กทรอนิกส์ ที่ต้องมีการจัดเก็บข้อมูลดังกล่าวไว้ด้วยวิธีการทางอิเล็กทรอนิกส์

2.2.2.2 พยานหลักฐานอิเล็กทรอนิกส์ที่เกิดจากการละเมิดลิขสิทธิ์อินเทอร์เน็ต

การละเมิดลิขสิทธิ์บนอินเทอร์เน็ต จะต้องมีสื่อในการกระทำความผิดอันได้แก่ คอมพิวเตอร์ และระบบอินเทอร์เน็ตที่ใช้เชื่อมต่อข้อมูลเข้าสู่การละเมิดบนอินเทอร์เน็ตได้ เมื่อการดำเนินการต้องกระทำผ่านคอมพิวเตอร์จึงทำให้หลักฐานการกระทำและข้อมูลต่าง ๆ ถูกจัดเก็บใน

รูปแบบดิจิตอลหรืออิเล็กทรอนิกส์ โดยหลักฐานที่เกิดจากการกระทำความผิดได้แก่

1) ข้อมูลคอมพิวเตอร์ เกิดในขั้นตอนที่มีการกระทำผ่านระบบคอมพิวเตอร์หรือผ่านระบบอินเทอร์เน็ตทั้งหลาย โดยกฎหมายให้ความหมายข้อมูลคอมพิวเตอร์ไว้ครอบคลุมข้อมูลที่อยู่ในรูปแบบดิจิตอลที่เชื่อมต่อกับการประมวลผลของระบบคอมพิวเตอร์ทั้งหมด ตามที่จะได้กล่าวต่อไป

2) ข้อมูลจราจรทางคอมพิวเตอร์ เป็นข้อมูลการติดต่อของระบบคอมพิวเตอร์ที่ผู้ใช้คอมพิวเตอร์ใช้เชื่อมต่ออินเทอร์เน็ตไปกระทำกิจกรรมต่าง ๆ โดยถือว่าเป็นข้อมูลคอมพิวเตอร์ชนิดหนึ่งที่มีความสำคัญในการบ่งบอกถึงการติดต่อสื่อสารของระบบคอมพิวเตอร์

โดยรายละเอียดและลักษณะของข้อมูลทั้งสองเป็นดังนี้

(1) ข้อมูลคอมพิวเตอร์

(1.1) ความหมายของข้อมูลคอมพิวเตอร์

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย[27]

ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ให้คำจำกัดความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร อย่างไรก็ตามการให้หมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์นั้น ก็แต่เฉพาะข้อมูลอิเล็กทรอนิกส์ที่มีการเชื่อมต่อเข้ากับระบบคอมพิวเตอร์เท่านั้น หากข้อมูลอิเล็กทรอนิกส์ เช่น โทรเลข โทรพิมพ์ หรือโทรสาร ไม่เกี่ยวหรือเชื่อมกับระบบคอมพิวเตอร์กรณีเช่นนี้ก็ไม่อยู่ในความหมายของข้อมูลคอมพิวเตอร์

ตามความหมายใน Convention on Cybercrime ให้คำจำกัดความคำว่า[28] ข้อมูลคอมพิวเตอร์ หมายถึง สิ่งใดที่ใช้เป็นตัวแสดงออกของข้อเท็จจริง ข้อมูลหรือความคิด ในรูปแบบที่เหมาะสมจะใช้ในการประมวลผลลงในระบบคอมพิวเตอร์ รวมถึงโปรแกรมที่เหมาะจะให้ระบบคอมพิวเตอร์ทำหน้าที่ได้

ตามบันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ..... เรื่องเสร็จที่ 258/2548 กำหนดความหมายของ

---

[27] คำนิยามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

[28] Article 1Definitions ... b. “ computer data” means any representative of facts, information or concepts in aform suitable for processing in acomputer system, including a pro sutable to cause a computer system to perform a function; ...

“ข้อมูลคอมพิวเตอร์” หมายถึงเฉพาะข้อมูลคอมพิวเตอร์ที่อยู่ในระบบคอมพิวเตอร์ที่สามารถประมวลผลได้เท่านั้นจึงจะได้รับความคุ้มครองตามพระราชบัญญัตินี้ ส่วนข้อมูลที่ถูกจัดเก็บในรูปแบบอื่น เช่น แผ่นดิสก์หรืออุปกรณ์อื่นใดที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์ ไม่จัดว่าเป็นข้อมูลคอมพิวเตอร์[29]

ดังนั้น ข้อมูลคอมพิวเตอร์หมายถึง ข้อมูล ข้อความ หรือชุดคำสั่ง หรือสิ่งใด ๆ ที่อยู่ในรูปแบบอิเล็กทรอนิกส์หรือดิจิตอลจัดเก็บด้วยระบบคอมพิวเตอร์ ไม่ว่าจะจัดเก็บอยู่ในลักษณะของข้อความ ภาพ เสียง หรือสัญญาณต่าง ๆ เช่น แฟ้มข้อมูล ไฟล์ภาพถ่าย ข้อความเสียง ข้อความสั้น หรือชุดคำสั่งใด หากระบบคอมพิวเตอร์สามารถอ่านข้อมูลดังกล่าวได้ ก็ถือว่าข้อมูลนั้นเป็น “ข้อมูลคอมพิวเตอร์”

(1.2) ลักษณะของข้อมูลคอมพิวเตอร์

ข้อมูลคอมพิวเตอร์เป็นข้อมูลที่ถูกจัดเก็บอยู่ในถังข้อมูลของคอมพิวเตอร์ที่มีลักษณะของการประมวลผลข้อมูลที่มองไม่เห็นด้วยตาเปล่าการเข้าถึงข้อมูลและแก้ไขข้อมูลสามารถทำได้โดยง่ายโดยผู้เปิดข้อมูลไม่ทราบว่ามีการแก้ไขหรือไม่ แต่หากมีการตั้งระบบรักษาความปลอดภัยทางคอมพิวเตอร์ที่ใช้ป้องกันในการเข้าถึงข้อมูลและตรวจสอบการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ก็จะทำให้ช่วยเพิ่มความยากในการแก้ไขเปลี่ยนแปลงได้ระดับที่สูงพอสมควร ทั้งนี้ เนื่องจากข้อมูลคอมพิวเตอร์เป็นข้อมูลที่มีความหลากหลายมาก จึงมีลักษณะที่หลากหลายด้วยคือ อาจถูกจัดเก็บเป็นไฟล์เสียงไว้ในคอมพิวเตอร์ หรือในอุปกรณ์อื่นเช่น แฟลสไดร์ฟ หรือ โทรศัพท์มือถือ

ข้อมูลคอมพิวเตอร์เป็นสิ่งที่ไม่สามารถจับต้องได้และสามารถจัดเก็บไว้ได้ต่อเมื่อมีอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เท่านั้น การที่ข้อมูลคอมพิวเตอร์ถูกถ่ายทอดมาเก็บไว้เป็นกระดาษเช่นนั้นก็กลายสภาพเป็นข้อมูลเอกสารเป็นเอกสารที่สื่อความหมายถึงข้อมูลคอมพิวเตอร์ได้ แต่ไม่สามารถจัดได้ว่าการถ่ายทอดข้อมูลคอมพิวเตอร์ลงในเอกสาร จะถือว่าเอกสารเป็นข้อมูลคอมพิวเตอร์ด้วยได้ เพราะเอกสารฉบับนั้นคอมพิวเตอร์ไม่สามารถประมวลผลได้ แม้ปัจจุบันเราจะเห็นสัญลักษณ์ QR Code ซึ่งเป็นสัญลักษณ์ที่สามารถอ่านค่าได้ด้วยระบบคอมพิวเตอร์ โดยจะมีลักษณะพิเศษคือ QR Code สามารถจัดเก็บบนกระดาษ หรือบนวัตถุใด ๆ ก็ได้ที่สามารถแสดงภาพได้ เนื่องจากเป็นลักษณะของการแปลงข้อมูลคอมพิวเตอร์ให้อยู่ในรูปภาพ โดยไม่จำเป็นต้องเก็บในระบบคอมพิวเตอร์อย่างเดียวแต่อย่างใด อนึ่ง QR Code เป็นสื่อนำไปสู่ข้อมูลคอมพิวเตอร์เท่านั้น แม้คอมพิวเตอร์สามารถอ่านค่าแล้วประมวลผลจาก QR Code เท่านั้น แต่QR Code ไม่ได้อยู่ในลักษณะของข้อมูลดิจิตอล แต่เป็นในรูปของภาพสัญลักษณ์เท่านั้น จึงไม่จัดว่าเป็นข้อมูลคอมพิวเตอร์

---

[29] สำนักงานคณะกรรมการกฤษฎีกา, บันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ..... เรื่องเสร็จที่ 258/2548, 11 –12.

(1.3) ข้อมูลคอมพิวเตอร์ที่เกิดจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

งานอันมีลิขสิทธิ์ในยุคดิจิตอลที่ถูกเปลี่ยนรูปแบบจากงานลิขสิทธิ์ทั่วไปให้เป็นข้อมูลทางดิจิตอลนั้น งานอันมีลิขสิทธิ์เหล่านี้เมื่อสามารถประมวลผลด้วยคอมพิวเตอร์ได้ จึงจัดว่าเป็นข้อมูลคอมพิวเตอร์ทั้งหมด ดังนั้น หลักฐานที่เป็นข้อมูลคอมพิวเตอร์ประการแรกคือ งานอันมีลิขสิทธิ์ที่ถูกทำให้อยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ ไม่ว่าจะเป็นภาพยนตร์ เพลง หรือรูปภาพ หรืออื่น ๆ ที่ถูกจัดเก็บอยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ ถือว่าเป็นพยานหลักฐานชิ้นสำคัญประการแรกที่ต้องมีเนื่องจากเป็นงานต้นฉบับที่ทำให้เกิดการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตขึ้น

ข้อมูลคอมพิวเตอร์ที่เกิดจากการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตประการต่อมา คือ ข้อมูลคอมพิวเตอร์ที่ถูกสร้างขึ้นเพื่อลอกเลียนหรือทำละเมิดทรัพย์สินทางปัญญา อันเป็นพยานหลักฐานสำคัญที่แสดงถึงการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตว่าเกิดขึ้นด้วยข้อมูลคอมพิวเตอร์ใด เช่น ไฟล์หนังที่สำเนาจากไฟล์ข้อมูลหนังต้นฉบับ เป็นต้น

ข้อมูลคอมพิวเตอร์ที่เป็นส่วนประกอบหรือหลักฐานประกอบจากการกระทำความผิด เช่น ข้อมูลคอมพิวเตอร์เกี่ยวกับการเชื่อมต่อข้อมูล ช่องทางที่ใช้ในการละเมิดลิขสิทธิ์ หรือช่วงเวลา หรือข้อมูลประกอบอื่น ๆ ที่ประกอบให้เกิดการละเมิดลิขสิทธิ์นั้น โดยทางกฎหมายเรียกว่า ข้อมูลจราจรทางคอมพิวเตอร์

(2) ข้อมูลจราจรทางคอมพิวเตอร์หรือ Traffic Data

ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลคอมพิวเตอร์ประเภทหนึ่งที่เป็นพยานหลักฐานสำคัญในการบอกถึงการติดต่อของระบบคอมพิวเตอร์ อันจะเป็นหลักฐานของการกระทำต่าง ๆ ผ่านระบบคอมพิวเตอร์ เช่นเดียวกันกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต หากไม่สามารถค้นหาข้อมูลจราจรทางคอมพิวเตอร์ได้อาจทำให้ไม่สามารถสืบหาได้ว่าการกระทำความผิดดังกล่าวมีต้นกำเนิดมากจากจุดใดและสืบต่อไปว่าใครเป็นผู้กระทำ โดยข้อมูลจราจรทางคอมพิวเตอร์นั้น มีลักษณะเฉพาะ และกฎหมายก็มีมาตรการเฉพาะสำหรับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ ผู้เขียนจึงศึกษาในส่วนนี้เพื่อให้เข้าใจถึงความหมาย และลักษณะของข้อมูลจราจรทางคอมพิวเตอร์ ที่เป็นพยานหลักฐานสำคัญในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต ว่ามีกฎหมายกำหนดไว้เช่นใด และมีปัญหาอุปสรรคในการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวอย่างไร

(2.1) ความหมายของข้อมูลจราจรทางคอมพิวเตอร์

คำว่า ข้อมูลจราจรทางคอมพิวเตอร์หรือ “Traffic Data”ปรากฏใน Convention on Cybercrime ของสภาแห่งยุโรป

“traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system

that formed a part in that chain of communication, indicating the communication's origin, route, time, date, size, duration, or type of underlying service.

มีคำแปล[30] ดังนี้ "ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลคอมพิวเตอร์ใดที่เกี่ยวข้องกับการติดต่อสื่อสารโดยวิธีการของระบบคอมพิวเตอร์ ซึ่งเกิดขึ้นโดยระบบคอมพิวเตอร์ซึ่งได้จัดรูปในส่วนของเส้นทางยึดโยงของการติดต่อสื่อสาร อันบ่งชี้ถึงกำเนิด ทิศทาง เส้นทาง เวลา วันที่ ขนาด ระยะเวลา หรือประเภทของการบริการที่ใช้นั้น"

ข้อมูลจราจรทางคอมพิวเตอร์ ปรากฏคำนิยามอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3 บัญญัติว่า "ในพระราชบัญญัตินี้ "ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น"

และประกาศกระทรวงเทคโนโลยีและสารสนเทศเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดคำนิยามไว้ใน ข้อ 4 กำหนดว่า "ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น"

ไพบูลย์ อมรภิญโญเกียรติ ได้อธิบายเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ไว้ดังนี้ เมื่อมีการรับ-ส่งข้อมูลผ่านทางระบบอินเทอร์เน็ตแต่ละครั้ง ระบบคอมพิวเตอร์แม่ข่ายหรือเซิร์ฟเวอร์ของผู้ส่ง (Sender) จะทำการบันทึกข้อมูล เวลาที่เริ่มส่ง ตำแหน่งที่ส่ง ชนิดและปริมาณของข้อมูลที่ส่ง ที่อยู่หรือตำแหน่งของคอมพิวเตอร์แม่ข่ายหรือเซิร์ฟเวอร์ที่ทำหน้าที่เป็นผู้รับ (Recipient) ระบบคอมพิวเตอร์แม่ข่ายหรือเซิร์ฟเวอร์ของผู้รับข้อมูลจะบันทึกข้อมูลแบบเดียวกัน ข้อมูลดังกล่าวนี้ที่ส่งผ่านคอมพิวเตอร์/ เครือข่าย รวมถึงบันทึกข้อมูลการเข้า/ ออกระบบอินเทอร์เน็ต ทั้งหมดนี้รวมเรียกว่า "ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data)"

พรเพชร วิชิตชลชัย ให้ความหมายคำว่า "ข้อมูลจราจรทางคอมพิวเตอร์" หมายถึงข้อมูลที่แสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ซึ่งจะแสดงถึงแหล่งกำเนิด เช่น IP Address ของเครื่อง ชื่อที่อยู่ของผู้ใช้ บริการที่มีการลงทะเบียน ข้อมูลของผู้ให้บริการ (Service Provider) ลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใด วันเวลาของการส่งข้อมูล และข้อมูลทุกประเภทที่เกิดจากการสื่อสาร (Communication) ผ่าน "ระบบ

---

[30] **อนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรม [Convention on Cybercrime],** 12.

คอมพิวเตอร์” การสื่อสารผ่านระบบคอมพิวเตอร์นั้นจะต้องมีระบบเครือข่ายคอมพิวเตอร์และมีผู้ให้บริการซึ่งผู้ให้บริการจะมีข้อมูลจราจรทางคอมพิวเตอร์อยู่ในระบบคอมพิวเตอร์ของตน

แนวทางการจัดทำข้อมูลจราจรทางคอมพิวเตอร์ ได้อธิบาย ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลคอมพิวเตอร์ที่เกิดขึ้นจากระบบคอมพิวเตอร์อันเป็นส่วนหนึ่งของการติดต่อสื่อสาร ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารนั้น ได้แก่ หมายเลขโทรศัพท์ เลขที่อยู่ของไอพีแอดเดรส (Internet Protocol Address) ส่วนข้อมูลปลายทาง ได้แก่ เลขที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ (e-mail Address) หรือที่อยู่เว็บไซต์ (URL) ที่ผู้ใช้บริการอินเทอร์เน็ตเข้าไปสืบค้นข้อมูล เป็นต้น นอกจากนั้นยังหมายรวมถึงข้อมูลต่าง ๆ เกี่ยวกับเวลาที่มีการติดต่อสื่อสาร วันที่ จำนวนตัวเลขของผู้ที่ติดต่อสื่อสารหรือลักษณะของการใช้บริการหรือประเภทของการติดต่อสื่อสาร เช่น การโอนแฟ้มข้อมูลหรือการติดต่อในรูปของไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น

เมื่อพิจารณาจากบทบัญญัติและคำนิยามที่นักกฎหมายแต่ละท่านได้อธิบายไว้ จึงอาจกล่าวได้ว่า ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลที่แสดงรายละเอียดการกระทำบนระบบคอมพิวเตอร์เมื่อมีการติดต่อสื่อสารกัน อันแสดงให้เห็นถึงระบบคอมพิวเตอร์ที่ส่งข้อมูล และรับข้อมูลของการติดต่อสื่อสารนั้น ช่วงเวลาและระยะเวลาที่มีการติดต่อสื่อสาร ลักษณะของข้อมูลที่รับส่ง และเส้นทางที่ใช้ในการส่งข้อมูลดังกล่าว หรืออาจกล่าวได้ว่าข้อมูลทางจราจรทางคอมพิวเตอร์เป็นร่องรอยที่เกิดขึ้นเมื่อมีการติดต่อสื่อสารของระบบคอมพิวเตอร์ แต่จะหายไม่หากไม่มีการจัดเก็บร่องรอยดังกล่าวไว้

(2.2) ลักษณะของข้อมูลจราจรทางคอมพิวเตอร์

จากคำนิยามข้างต้นแสดงให้เห็นว่าข้อมูลจราจรทางคอมพิวเตอร์จะเกิดขึ้นได้ก็ต่อเมื่อมีการสื่อสารของระบบคอมพิวเตอร์ไม่ว่าจะกระทำผ่านเครือข่ายคอมพิวเตอร์ในรูปแบบใดก็ตาม ลักษณะสำคัญคือจะต้องมีการเชื่อมโยงถึงกันได้ โดยการเชื่อมโยงนี้จะมีเพื่อให้ระบบคอมพิวเตอร์ตั้งแต่สองระบบขึ้นไปสามารถรับส่งข้อมูล และการเชื่อมโยงในแต่ละครั้งจะเกิดข้อมูลจราจรทางคอมพิวเตอร์อันได้แก่ ตำแหน่งต้นทางและปลายที่ใช้ในการรับส่งข้อมูลให้แก่กัน ระยะเวลาที่รับส่งข้อมูล ปริมาณข้อมูลที่มีการติดต่อสื่อสาร รวมทั้งลักษณะของข้อมูล

เมื่อพิจารณาจากความหมายและการเกิดข้อมูลจราจรทางคอมพิวเตอร์จะพบว่าข้อมูลจราจรทางคอมพิวเตอร์มีลักษณะเป็นข้อมูลที่แสดงถึงการติดต่อสื่อสารของระบบคอมพิวเตอร์เท่านั้นโดยไม่มีเนื้อหาของข้อมูลที่สื่อสารดังกล่าว และเกิดขึ้นจากกลไกของการสื่อสารทางเทคนิคของระบบคอมพิวเตอร์ไม่ได้เกิดจากเจตนาของมนุษย์ เป็นร่องรอยที่เกิดจากการติดต่อสื่อสารอย่างแท้จริง ซึ่งการเกิดข้อมูลดังกล่าวมีอยู่อย่างกระจัดกระจาย คือข้อมูลเกิดขึ้นในหลายช่วงของการสื่อสาร ทั้งต้นทาง ปลายทาง และเครือข่ายที่เชื่อมต่อการติดต่อสื่อสาร ทั้งนี้ ข้อมูลจราจรทาง

คอมพิวเตอร์ที่ถูกจัดเก็บไว้เป็นข้อมูลอิเล็กทรอนิกส์ชนิดหนึ่งที่มีธรรมชาติคือสามารถแก้ไขเปลี่ยนแปลงได้ง่าย

อนึ่ง ด้วยลักษณะของข้อมูลจราจรทางคอมพิวเตอร์นั้นเกิดขึ้นเมื่อมีการสื่อสารของระบบคอมพิวเตอร์ และเมื่อการสื่อสารนั้นสิ้นสุดลง ข้อมูลจราจรทางคอมพิวเตอร์จึงหายไปด้วย มิใช่ข้อมูลที่จะคงอยู่ตลอดไป ดังนั้น เพื่อให้มีข้อมูลจราจรทางคอมพิวเตอร์ตามที่กฎหมายกำหนด ผู้ให้บริการจึงต้องมีอุปกรณ์หรือระบบที่จะบันทึกข้อมูลจราจรทางคอมพิวเตอร์นั้นไว้ ข้อมูลที่นำมาใช้เป็นพยานหลักฐานจึงเป็นข้อมูลที่เกิดจากการบันทึกมาอีกทอดหนึ่ง คือบันทึกข้อมูลที่เกิดขึ้นจริงในขณะสื่อสาร ซึ่งหากในขั้นตอนการบันทึกนี้มีความผิดพลาดก็อาจเกิดการแก้ไขเปลี่ยนแปลงได้ และนอกจากนั้นแล้ว เมื่อมีการบันทึกข้อมูลดังกล่าวไว้ ข้อมูลจราจรทางคอมพิวเตอร์ก็จะถูกจัดเก็บในรูปแบบของข้อมูลคอมพิวเตอร์ ซึ่งหากสามารถเข้าถึงข้อมูลดังกล่าวได้ ผู้ใช้ก็จะสามารถเปิดอ่าน แก้ไข เพิ่มเติม ตัดทอนได้โดยผ่านโปรแกรมคอมพิวเตอร์ ด้วยลักษณะดังกล่าวจึงให้เกิดประเด็นที่ต้องพิจารณาความถูกต้องแท้จริงของข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บดังนี้

ก) ข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกอยู่นั้นเป็นข้อมูลที่ตรงกันกับที่ปรากฏบนอุปกรณ์ขณะที่มีการการสื่อสารข้อมูลหรือไม่ เพราะอาจมีเหตุทางเทคนิคที่จะทำให้ข้อมูลนั้นบกพร่องได้

ข) ข้อมูลจราจรทางคอมพิวเตอร์ที่บันทึกอยู่นั้นบันทึกได้ครบถ้วนสมบูรณ์หรือไม่ หากไม่ปรากฏข้อมูลจราจรบันทึกอยู่ จะเป็นการยืนยันว่าไม่มีการสื่อสารข้อมูลเกิดขึ้นได้หรือไม่ เพราะอาจมีเหตุทางเทคนิคที่จะทำให้ข้อมูลนั้นบกพร่องได้

ค) โดยปกติแล้วข้อมูลคอมพิวเตอร์นั้นจะเป็นข้อมูลที่รักษาความถูกต้องแท้จริงได้ยากการเปลี่ยนแปลงข้อมูลสามารถกระทำได้โดยง่ายและทุกเวลาและเมื่อมีการเปลี่ยนแปลงแล้วก็การตรวจสอบอาจทำได้เพียงบางครั้งและต้องใช้กระบวนการที่ซับซ้อน ดังนั้นข้อมูล คอมพิวเตอร์ที่ต้องการให้มีการรักษาความถูกต้องแท้จริงนั้น จะต้องมีกรรมวิธีเฉพาะเจาะจงที่ป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลเหล่านั้นโดยมนุษย์หรือโดยความผิดพลาดของระบบปฏิบัติการ

ด้วยลักษณะที่เปลี่ยนแปลงง่ายของข้อมูลจราจรทางคอมพิวเตอร์นี้เอง จึงอาจส่งผลกระทบต่อความน่าเชื่อถือในการใช้ข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐาน เพราะมีประเด็นให้สงสัยได้ว่าข้อมูลดังกล่าวมีความถูกต้องหรือไม่ โดยอาจมีการอ้างต่อศาลเพื่อให้มีการพิสูจน์ความถูกต้องของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้ และหากเป็นความผิดที่มีโทษทางอาญา เช่นโทษทางอาญาของกฎหมายลิขสิทธิ์ วิธีการในการตีความและนำสืบจึงต้องทำโดยยึดหลักของกฎหมายอาญาการนำสืบว่ามีการกระทำความผิดจึงต้องมีการสืบจนกว่าจะปราศจากข้อสงสัย โดยจะต้องพิสูจน์ทั้งกระบวนการตั้งแต่การจัดเก็บว่ามีความน่าเชื่อถืออย่างไร จนข้อมูลนั้นมาถึงกระบวน

การพิจารณา ดังนั้น กฎหมายและหลักเกณฑ์เกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ จึงมีความสำคัญอย่างยิ่งในในการนำข้อมูลมาใช้เป็นพยานหลักฐานเพื่อนำตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์มาลงโทษ

2.3 การได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

กระบวนการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เริ่มต้นขึ้นเมื่อมีการกระทำความผิดเกิดขึ้นแล้วพนักงานเจ้าหน้าที่ได้รับทราบถึงการกระทำความผิดดังกล่าว ไม่ว่าจะโดยได้รับแจ้งจากผู้เสียหายโดยตรง หรือจากขอข้อมูลโดยหน่วยงานอื่นซึ่งเกี่ยวข้อง เพื่อนำไปใช้หาตัวผู้กระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ โดยผู้ที่เกี่ยวข้องกับกระบวนการในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวได้แก่ (1) ผู้กระทำความผิดซึ่งก่อให้เกิดหลักฐานข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องจัดเก็บ (2) ผู้ให้บริการซึ่งมีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (3) ผู้ได้รับความเสียหายจากการกระทำความผิดแจ้งเรื่องไปยังพนักงานเจ้าหน้าที่ (4) พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีอำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ โดยขั้นตอนในการได้มาคือพนักงานเจ้าหน้าที่มีหมายเรียกไปยังผู้ให้บริการเพื่อประมวลผลข้อมูลจราจรทางคอมพิวเตอร์และผู้ให้บริการประมวลผลข้อมูลตามที่มีหมายเรียกและส่งกลับให้แก่พนักงานเจ้าหน้าที่ฯเพื่อนำข้อมูลดังกล่าวไปใช้เป็นพยานหลักฐานในการนำตัวผู้กระทำความผิดมาลงโทษต่อไป

ทั้งนี้ การได้มาซึ่งพยานหลักฐานตามหลักทั่วไปปรากฏในประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 266 ได้วางหลักไว้ว่าพยานหลักฐานที่จะนำมาอ้างได้จะต้องไม่ใช่พยานหลักฐานที่เกิดขึ้นจากกาจูงใจ คำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายหรือกฎหมายอื่นอันว่าด้วยการสืบพยาน หรือมีการเรียกหลักการนี้ว่า “หลักผลไม้มีพิษ” คือ พยานหลักฐานที่เกิดจากการกระทำโดยมิชอบไม่สามารถนำมาใช้เป็นหลักฐานเอาผิดแก่ผู้กระทำความผิดในคดีอาญาได้ไม่ว่ากรณีใด ๆ โดยไม่มีการให้ดุลยพินิจไว้ และกรณีที่พยานหลักฐานนั้นเกิดขึ้นโดยชอบแต่กระบวนการในการได้มาเป็นกระบวนการที่ไม่ชอบด้วยกฎหมาย แม้อาจจะนำพยานหลักฐานมาใช้ได้ตามที่กฎหมายได้เป็นดุลยพินิจของผู้พิพากษาในกรณีที่การนำพยานหลักฐานดังกล่าวมาใช้จะเป็นคุณประโยชน์แก่การอำนวยความยุติธรรมมากกว่าผลเสียอันเกิดจากผลกระทบต่อมาตรฐานระบบงานยุติธรรมทางอาญาหรือสิทธิเสรีภาพพื้นฐานของประชาชน โดยตรงคำนึงถึงปัจจัยต่างๆตามที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 266/1 แต่ส่วนใหญ่ในทางปฏิบัติพบว่ามีน้อยมากเนื่องจากการกระทบสิทธิของประชาชนเพื่อให้ได้มาซึ่งพยานหลักฐานเป็นการที่ไม่ถูกต้องแต่กฎหมายเปิดช่องไว้สำหรับกรณีพิเศษที่มีความจำเป็นอย่างยิ่งที่จะต้องใช้พยานหลักฐานนั้นตามหลักการและเหตุผลในมาตรา 266/1 ดังนั้น สำหรับความผิดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตก็เช่นเดียวกัน การรวบรวมพยานหลักฐานและได้มาซึ่งพยานหลักฐาน ในเบื้องต้นได้กล่าวถึง

การเกิดขึ้นของพยานหลักฐานอิเล็กทรอนิกส์ไปแล้วว่าเกิดจากลักษณะใด และมีการจัดเก็บเช่นใด หรือเรียกได้ว่าเป็นขั้นตอนของการเกิดพยานหลักฐานอิเล็กทรอนิกส์ขึ้น หากมีการประมวลผลของระบบคอมพิวเตอร์ เกิดพยานหลักฐานและจัดเก็บอย่างถูกต้องก็กล่าวได้ว่าพยานหลักฐานนั้นเกิดขึ้นโดยชอบด้วยกฎหมาย แต่การเกิดขึ้นโดยชอบด้วยกฎหมายอย่างเดียวไม่เพียงพอในการนำพยานหลักฐานมาใช้ประการต่อมาที่สำคัญคือการได้มาซึ่งพยานหลักฐานโดยชอบด้วยกฎหมาย

การได้มาซึ่งพยานหลักฐานโดยชอบด้วยกฎหมาย หมายความว่าการได้พยานหลักฐานมาโดยอาศัยอำนาจตามกฎหมายและปฏิบัติตามขั้นตอนที่กฎหมายกำหนดครบถ้วนถูกต้องทุกประการ เมื่อเป็นเช่นนี้ พยานหลักฐานก็สามารถนำมาใช้ได้ ส่วนของการละเมิดลิขสิทธิ์นับว่าเป็นความผิดอาญา เมื่อมีการกระทำความผิดเกิดขึ้น พนักงานสอบสวนมีหน้าที่ต้องเริ่มการสอบสวนโดยทันที และสิ่งแรกของการสอบสวนก็คือการหาเบาะแสหรือพยานหลักฐานโดยเจ้าหน้าที่ผู้มีอำนาจ โดยการได้มาซึ่งพยานหลักฐานเกี่ยวกับการละเมิดลิขสิทธิ์โดยพนักงานเจ้าหน้าที่ปรากฏในพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ซึ่งได้กำหนดให้มีพนักงานเจ้าหน้าที่เพิ่มเติมโดยให้ถือเป็นพนักงานเจ้าหน้าที่ตามกฎหมายอาญา เพื่อให้มีอำนาจในการค้น ยึด อายัด หรือหมายเรียกพยานในความผิดเกี่ยวกับลิขสิทธิ์ การที่พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 กำหนดพนักงานเจ้าหน้าที่เพิ่มเติมจากประมวลกฎหมายวิธีพิจารณาความอาญาทั่วไป ด้วยวัตถุประสงค์ต้องการให้เกิดประสิทธิภาพในการสืบสวนสอบโดยให้ผู้ที่มีความรู้ความเชี่ยวชาญด้านลิขสิทธิ์เข้ามาเป็นผู้หาพยานหลักฐานในคดีและนอกจากเจ้าหน้าที่ตามพระราชบัญญัติโดยตรงแล้วยังมีหน่วยงานอื่นที่มีอำนาจในการสืบสวนสอบสวนคดีเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต โดยหลักเกณฑ์การได้มาซึ่งพยานหลักฐานที่ชอบด้วยกฎหมายของพนักงานเจ้าหน้าที่แต่ละพระราชบัญญัติรวมถึงหน่วยงานอื่นที่มีอำนาจมีดังนี้

2.3.1 พนักงานเจ้าหน้าที่ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

2.3.1.1 เขตอำนาจ

พนักงานเจ้าหน้าที่มีอำนาจกระทำการใด ๆ ได้ตามที่กฎหมายกำหนดเพื่อประโยชน์ในการปฏิบัติการให้เป็นไปตามพระราชบัญญัติลิขสิทธิ์ โดยมีอำนาจกระทำได้ทั่วราชอาณาจักร

2.3.1.2 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่

1) มาตรา 67 อำนาจของพนักงานเจ้าหน้าที่

มาตรา 67 เพื่อประโยชน์ในการปฏิบัติการให้เป็นไปตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นเจ้าพนักงานตามประมวลกฎหมายอาญา และให้พนักงานเจ้าหน้าที่มีอำนาจและหน้าที่ดังต่อไปนี้

(1) เข้าไปในอาคาร สถานที่ทำการ สถานที่ผลิต หรือสถานที่เก็บสินค้าของบุคคลใดในเวลาระหว่างพระอาทิตย์ขึ้นถึงพระอาทิตย์ตก หรือในเวลาทำการของสถานที่นั้น

หรือเข้าไปในยานพาหนะ เพื่อตรวจค้นสินค้า หรือตรวจสอบเมื่อมีเหตุอันควรสงสัยว่ามีการกระทำความผิดตามพระราชบัญญัตินี้

(2) ยึดหรืออายัดเอกสารหรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิด เพื่อประโยชน์ในการดำเนินคดีในกรณีมีเหตุอันควรสงสัยว่ามีการกระทำความผิดตามพระราชบัญญัตินี้

(3) สั่งให้บุคคลใด ๆ มาให้ถ้อยคำหรือให้ส่งบัญชี เอกสาร หรือหลักฐานอื่นในกรณีมีเหตุอันควรเชื่อว่าถ้อยคำ สมุดบัญชี เอกสาร หรือหลักฐานดังกล่าวมีประโยชน์แก่การค้นพบหรือใช้เป็นพยานหลักฐานในการพิสูจน์การกระทำความผิดตามพระราชบัญญัตินี้

ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ ให้ผู้ซึ่งเกี่ยวข้องอำนวยความสะดวกตามสมควร

2) มาตรา 71 บทลงโทษกรณีไม่ทำตามคำขอของพนักงานเจ้าหน้าที่

มาตรา 71 ผู้ใดไม่มาให้ถ้อยคำหรือไม่ส่งเอกสารหรือวัตถุใด ๆ ตามที่คณะกรรมการหรือคณะอนุกรรมการสั่งตามมาตรา 60 วรรคสาม ต้องระวางโทษจำคุกไม่เกินสามเดือน หรือปรับไม่เกินห้าหมื่นบาท หรือทั้งจำทั้งปรับ

2.3.2 อำนาจของกรมสอบสวนคดีพิเศษ สำนักคดีทรัพย์สินทางปัญญา (สคป.)

2.3.2.1 เขตอำนาจ

พนักงานสอบสวนคดีพิเศษมีขึ้นเพื่อรับผิดชอบเกี่ยวกับคดีอาญาบางประเภทที่กำหนดให้อยู่ในอำนาจหน้าที่ของกรมสอบสวนคดีพิเศษ และโดยที่คดีดังกล่าวจำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านเป็นผู้ดำเนินการสืบสวนและสอบสวน รวมทั้งกำหนดอำนาจหน้าที่ดังกล่าว เพื่อให้การป้องกันและปราบปรามการกระทำความผิดอาญาดังกล่าวอย่างมีประสิทธิภาพ[31] โดยเขตอำนาจของพนักงานสอบสวนคดีพิเศษคือ คดีที่มีความผิดตามบัญชีแนบท้ายพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ซึ่งคดีความผิดเกี่ยวกับกฎหมายลิขสิทธิ์ปรากฏอยู่ใน **(18)** โดยเป็นคดีที่ลักษณะอย่างใดอย่างหนึ่งดังนี้ คือ มีความซับซ้อนที่ต้องใช้การสอบสวนพิเศษ มีผลกระทบต่อความมั่นคงของประเทศ มีลักษณะกระทำความผิดข้ามชาติ หรือมีผู้ทรงอิทธิพลเป็นตัวการ เป็นต้น ซึ่งกำหนดไว้ในมาตรา 21 ดังนั้นหากความผิดเกี่ยวกับกฎหมายลิขสิทธิ์ที่ถูกทำขึ้นโดยมีลักษณะหนึ่งลักษณะได้ตามมาตรา 21 พนักงานสอบสวนคดีพิเศษก็ย่อมมีอำนาจในการสืบสวนสอบสวนคดีดังกล่าวได้

2.3.2.2 อำนาจหน้าที่ของพนักงานสอบสวนคดีพิเศษ

มาตรา 24 เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจดังต่อไปนี้ด้วย

---

[31] หมายเหตุท้ายพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547.

(1) เข้าไปในเคหสถาน หรือสถานที่ใด ๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

(2) ค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษหรือซึ่งอาจใช้เป็นพยานหลักฐานได้

(3) มีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์การ หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชีเอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(4) มีหนังสือสอบถาม หรือเรียกบุคคลใด ๆ มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือหรือส่งบัญชีเอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(5) ยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (1) (2) (3) และ (4)

การใช้อำนาจตามวรรคหนึ่ง ให้พนักงานสอบสวนคดีพิเศษปฏิบัติตามข้อบังคับที่ กคพ. กำหนดเฉพาะการใช้อำนาจตามวรรคหนึ่ง (1) นอกจากพนักงานสอบสวนคดีพิเศษต้องดำเนินการเกี่ยวกับวิธีการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาแล้ว ให้พนักงานสอบสวนคดีพิเศษแสดงความบริสุทธิ์ก่อนการเข้าค้น รายงานเหตุผลและผลการตรวจค้นเป็นหนังสือต่อผู้บังคับบัญชาเหนือขึ้นไป และบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อที่ทำให้สามารถเข้าค้นได้เป็นหนังสือให้ไว้แก่ผู้ครอบครองเคหสถานหรือสถานที่ค้น แต่ถ้าไม่มีผู้ครอบครองอยู่ ณ ที่นั้น ให้พนักงานสอบสวนคดีพิเศษส่งมอบสำเนาหนังสือนั้นให้แก่ผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ และหากเป็นการเข้าค้นในเวลากลางคืนภายหลังพระอาทิตย์ตก พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้า ในการเข้าค้นต้องเป็นข้าราชการพลเรือนตำแหน่งตั้งแต่ระดับ 7 ขึ้นไปด้วย

ให้พนักงานสอบสวนคดีพิเศษผู้เป็นหัวหน้าในการเข้าค้นส่งสำเนาบันทึกเหตุสงสัยตามสมควรและเหตุอันควรเชื่อตามวรรคสาม และสำเนาบันทึกการตรวจค้นและบัญชีทรัพย์ที่ยึดหรืออายัดต่อศาลจังหวัดที่มีอำนาจเหนือท้องที่ที่ทำการค้น หรือศาลอาญาในเขตกรุงเทพมหานครภายในสี่สิบแปดชั่วโมงหลังจากสิ้นสุดการตรวจค้น เพื่อเป็นหลักฐาน

พนักงานสอบสวนคดีพิเศษระดับใดจะมีอำนาจหน้าที่ตามที่ได้กำหนดไว้ตามวรรคหนึ่งทั้งหมดหรือแต่บางส่วน หรือจะต้องได้รับอนุมัติจากบุคคลใดก่อนดำเนินการให้เป็นไปตามที่

อธิบดีกำหนด โดยทำเอกสารให้ไว้ประจำตัวพนักงานสอบสวนคดีพิเศษผู้ได้รับอนุมัตินั้นและพนักงานสอบสวนคดีพิเศษผู้นั้นต้องแสดงเอกสารดังกล่าวต่อบุคคลที่เกี่ยวข้องทุกครั้ง

2.3.3 อำนาจพนักงานสอบสวนตามกฎหมายอาญา

2.3.3.1 เขตอำนาจ

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ของสำนักงานตำรวจแห่งชาติ ใช้อำนาจไปตามประมวลกฎหมายวิธีพิจารณาความอาญาที่ให้อำนาจพนักงานสอบสวนในการสืบสวนสอบสวนสำหรับการกระทำความผิดอาญาที่เกิดขึ้นโดยสำนักงานตำรวจแห่งชาติกำหนดให้ กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี[32] จำนวนสองกองกำกับการมีอำนาจหน้าที่เกี่ยวกับความผิดในการละเมิดทรัพย์สินทางปัญญาซึ่งรวมถึงลิขสิทธิ์ด้วยโดยเฉพาะ อันได้แก่

กองกำกับการ 3 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปราม อาชญากรรมที่เกี่ยวกับการละเมิดทรัพย์สินทางปัญญา สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการละเมิดทรัพย์สินทางปัญญาและความผิดที่เกี่ยวเนื่อง ในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย เพื่อให้เกิดประสิทธิภาพและความเข้าใจในการทำงานเฉพาะด้านทรัพย์สินทางปัญญา

กองกำกับการ 4 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับการละเมิดทรัพย์สินทางปัญญาทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการละเมิดทรัพย์สินทางปัญญาทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร ยกเว้นในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

2.3.3.2 อำนาจหน้าที่ของพนักงานสอบสวน

พนักงานสอบสวนตามประมวลกฎหมายอาญามีอำนาจหน้าที่ในการสืบสวนสอบสวนเพื่อให้ทราบข้อเท็จจริง และเพื่อรวบรวมพยานหลักฐานมาใช้ประกอบการนำตัวผู้กระทำความผิดมาลงโทษ โดยกฎหมายให้อำนาจไว้ใน ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131 ให้พนักงานสอบสวนรวบรวมหลักฐานทุกชนิด เท่าที่สามารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริงและ

---

[32] กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการที่เรียกชื่ออย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ. 2548 ข้อ 12(ฎ).

พฤติการณ์ต่าง ๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา และสำหรับการได้มาซึ่งพยานหลักฐาน ได้ปรากฏอยู่อยู่ในมาตรา 132 บัญญัติว่า “เพื่อประโยชน์แห่งการรวบรวมหลักฐาน ให้พนักงานสอบสวนมีอำนาจดั่งต่อไปนี้

(1) ตรวจตัวผู้เสียหายเมื่อผู้นั้นยินยอม หรือตรวจตัวผู้ต้องหา หรือตรวจสิ่งของหรือที่ทางอันสามารถอาจใช้เป็นพยานหลักฐานได้ ให้รวมทั้งทำภาพถ่าย แผนที่ หรือภาพวาดจำลอง หรือพิมพ์ลายนิ้วมือ ลายมือหรือลายเท้า กับให้บันทึกรายละเอียดทั้งหลายซึ่งน่าจะกระทำให้คดีแจ่มกระจ่างขึ้น

ในการตรวจตัวผู้เสียหายหรือผู้ต้องหาตามวรรคหนึ่ง หากผู้เสียหายหรือผู้ต้องหาเป็นหญิง ให้จัดให้เจ้าพนักงานซึ่งเป็นหญิงหรือหญิงอื่นเป็นผู้ตรวจ ทั้งนี้ ในกรณีที่มีเหตุอันสมควร ผู้เสียหายหรือผู้ต้องหาจะขอนำบุคคลใดมาอยู่ร่วมในการตรวจนั้นด้วยก็ได้

(2) ค้นเพื่อพบสิ่งของ ซึ่งมีไว้เป็นความผิด หรือได้มาโดยการกระทำผิด หรือได้ใช้หรือสงสัยว่าได้ใช้ในการกระทำผิด หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ แต่ต้องปฏิบัติตามบทบัญญัติแห่งประมวลกฎหมายนี้ว่าด้วยค้น

(3) หมายเรียกบุคคลซึ่งครอบครองสิ่งของ ซึ่งอาจใช้เป็นพยานหลักฐานได้ แต่บุคคลที่ถูกหมายเรียกไม่จำต้องมาเอง เมื่อจัดส่งสิ่งของมาตามหมายแล้ว ให้ถือเสมือนได้ปฏิบัติตามหมาย

(4) ยึดไว้ซึ่งสิ่งของที่ค้นพบหรือส่งมาดั่งกล่าวไว้ในอนุมาตรา (2) และ (3)

แต่ทั้งนี้ เนื่องจากการกระทำความผิดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นความผิดอาญาซึ่งผู้เสียหายสามารถร้องทุกข์หรือกล่าวโทษแก่พนักงานสอบสวนตามกฎหมายวิธีพิจารณาความอาญาได้ โดยหน้าที่ของพนักงานสอบสวนเมื่อทราบว่ามีการกระทำความผิดกฎหมายอาญา จะต้องดำเนินการสืบสวนสอบสวนโดยไม่ชักช้า พนักงานสอบสวนจึงต้องดำเนินการให้ได้มาซึ่งพยานหลักฐาน อย่างไรก็ตามสำหรับส่วนของพยานหลักฐานอิเล็กทรอนิกส์ เช่นข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวพนักงานสอบสวนจะต้องประสานไปยังเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพื่อขอข้อมูลจึงจะสามารถนำไปใช้เป็นพยานหลักฐานในการสืบสวนสอบสวนต่อไปได้ โดยกฎหมายได้กำหนดเรื่องดังกล่าวไว้ในระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในข้อ 5 กำหนดให้พนักงานสอบสวนเมื่อได้รับคำร้องทุกข์กล่าวโทษแล้วให้ประสานกับพนักงานเจ้าหน้าที่เพื่อประโยชน์ในการแสวงหาพยานหลักฐานประกอบการกระทำความผิดแสดงให้เห็นว่าพนักงานสอบสวนไม่มีอำนาจด้วยตนเองในการขอข้อมูลจราจรทางคอมพิวเตอร์ เพราะการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์เป็นการกระทำที่ละเมิดสิทธิ

เสรีภาพในการติดต่อสื่อสาร จึงต้องมีกฎหมายเฉพาะเจาะจงให้อำนาจไว้ไม่เช่นนั้นผู้ให้บริการจะมีความผิดหากเปิดเผยข้อมูลดังกล่าวแก่บุคคลอื่น

โดยทั่วไปเพื่อให้ได้มาซึ่งพยานหลักฐานพนักงานสอบสวนมีอำนาจที่จะหมายเรียกบุคคลซึ่งครอบครองสิ่งของซึ่งอาจใช้เป็นพยานหลักฐานได้ ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 132 (3)[33] แต่ในกรณีของข้อมูลจราจรทางคอมพิวเตอร์ซึ่งแสดงถึงการติดต่อสื่อสาร กฎหมายได้ให้ความคุ้มครองไว้เป็นการเฉพาะในหลายบทบัญญัติ ได้แก่

(ก) รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 36[34]

(ข) พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 74[35] ซึ่งกำหนดบทลงโทษแก่ผู้ที่เปิดเผยข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย

(ค) พระราชบัญญัติการประกอบกิจการโทรคมนาคมฯ มาตรา 50[36] และพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับวิทยุกระจายเสียง วิทยุโทรทัศน์ และ กิจการ

---

[33] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 “เพื่อประโยชน์แห่งการรวบรวมหลักฐานให้พนักงานสอบสวนมีอำนาจดังต่อไปนี้...

(3) หมายเรียกบุคคลซึ่งครอบครองสิ่งของซึ่งอาจใช้เป็นพยานหลักฐานได้ แต่บุคคลที่ถูกหมายเรียกไม่จำต้องมาเองเมื่อจัดส่งสิ่งของมาตามหมายแล้ว ให้ถือเสมือนได้ปฏิบัติตามหมาย...”.

[34] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 “มาตรา 36 บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใดเพื่อให้ ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลมีติดต่อถึงกัน จะกระทำมิได้เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่ง กฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน”.

[35] พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

“มาตรา 74 ผู้ใดกระทำด้วยประการใด ๆ เพื่อดักรับไว้ใช้ประโยชน์หรือเปิดเผยข้อความข่าวสารหรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมายต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่แสนบาทหรือทั้งจำทั้งปรับ”.

[36] พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

“มาตรา 50 ให้คณะกรรมการกำหนดมาตรการเพื่อคุ้มครองผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม

ให้ผู้รับใบอนุญาตมีหน้าที่ปฏิบัติตามมาตรการที่คณะกรรมการกำหนดตามวรรคหนึ่ง

เมื่อพบว่ามีบุคคลใดกระทำการละเมิดสิทธิของผู้ใช้บริการตามวรรคหนึ่ง ให้ผู้รับใบอนุญาตหรือคณะกรรมการ ดำเนินการเพื่อระงับการกระทำดังกล่าวและแจ้งให้ผู้ใช้บริการทราบโดยเร็ว”.

โทรคมนาคม พ.ศ. 2543 มาตรา 51(11) ซึ่งกำหนดเป็นอำนาจหน้าที่ คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (“กทช.”) ในอันที่จะคุ้มครองสิทธิในความเป็นส่วนตัวและเสรีภาพของบุคคลในการสื่อสารถึงกันโดยทางโทรคมนาคม

(ง) ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการ โทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคลสิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม ข้อ 4 (1) (3) และ ข้อ 14[37]

จึงมีประเด็นสงสัยว่าพนักงานสอบสวนจะสามารถอาศัยอำนาจทั่วไปตามมาตรา 132 เพื่อขอข้อมูลจราจรทางคอมพิวเตอร์ได้หรือไม่ ซึ่งปรากฏในบันทึกสำนักงานคณะกรรมการกฤษฎีกา เรื่อง อำนาจของเจ้าพนักงานตำรวจในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสมทางอินเทอร์เน็ต และของพนักงานสอบสวนตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา เรื่องเสร็จที่ 343/2549 ที่มีความเห็นว่า

“กรณีที่พนักงานสอบสวนใช้อำนาจตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ออกหมายเรียกเอกสารที่เกี่ยวข้องเพื่อให้เข้าถึงข้อมูลทางโทรคมนาคมนั้น หากพนักงานสอบสวนต้องการทราบข้อมูลเกี่ยวกับชื่อ ที่อยู่และหมายเลขโทรศัพท์ที่ใช้เชื่อมต่ออินเทอร์เน็ตตลอดจนรายละเอียดการเชื่อมต่อที่ระบุระยะเวลาเข้าสู่ระบบและออกจากระบบ ของผู้ใช้บริการเพื่อที่จะรู้ตัวผู้กระทำความผิดเท่านั้น ข้อมูลดังกล่าวมิใช่ข้อความในสิ่งสื่อสารที่บุคคลติดต่อกันซึ่งต้องห้ามตามมาตรา 36 วรรคสองของรัฐธรรมนูญแห่งราชอาณาจักรไทย หรือเป็นข้อมูลข่าวสารอันเป็นรายละเอียดที่ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดตามที่พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดไว้ ดังนั้น ถ้าปรากฏว่าข้อมูลที่พนักงานสอบสวนต้องการทราบปรากฏอยู่ในเอกสาร ก็อาจออกหมายเรียกบุคคลซึ่งครอบครองเอกสารให้จัดส่งเอกสารนั้นมาให้ได้”

---

[37] ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม ใช้บังคับเมื่อวันที่ 16 สิงหาคม 2549

“ข้อ 4 (1) เปิดเผยข้อมูลส่วนบุคคลต่อหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และปฏิบัติครบถ้วนตามกระบวนการที่กฎหมายนั้นบัญญัติ”

“ข้อ 4 (3) ส่งข้อมูลตามข้อ 14”

“ข้อ 14 ผู้รับใบอนุญาตมีหน้าที่ส่งข้อมูลส่วนบุคคลที่ผู้รับใบอนุญาตครอบครอง ให้แก่คณะกรรมการและสำนักงานเมื่อคณะกรรมการและสำนักงานร้องขอ เพื่อประโยชน์ในการปฏิบัติงานกำกับดูแลการประกอบกิจการโทรคมนาคมตามกฎหมายของคณะกรรมการและสำนักงาน”.

เมื่อพิจารณากฎหมายที่คุ้มครองการข้อมูลการติดต่อสื่อสาร ประกอบกับความเห็นของสำนักงานคณะกรรมการกฤษฎีกา ย่อมกล่าวได้ว่าข้อมูลจราจรทางคอมพิวเตอร์ที่เป็นข้อมูลเกี่ยวกับการติดต่อสื่อสาร ผู้มีอำนาจเฉพาะตามที่กฎหมายกำหนดเท่านั้นจึงจะมีอำนาจได้มาซึ่งข้อมูลดังกล่าวได้ แต่สำหรับพนักงานสอบสวนนั้น หากต้องการข้อมูลจราจรทางคอมพิวเตอร์ จะต้องประสานไปยังพนักงานเจ้าหน้าที่ตามพระราชบัญญัติคอมพิวเตอร์เท่านั้น การอาศัยอำนาจตามกฎหมายอื่นเพื่อให้ได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ของพนักงานสอบสวน จึงสามารถทำได้เฉพาะข้อมูลเกี่ยวกับชื่อ ที่อยู่และหมายเลขโทรศัพท์ที่ใช้เชื่อมต่ออินเทอร์เน็ต ตลอดจนรายละเอียดการเชื่อมต่อที่ระบุระยะเวลา Login และ Logout ของผู้ใช้บริการ โดยข้อมูลดังกล่าวจะต้องปรากฏอยู่ในเอกสารเท่านั้นจึงจะสามารถขอข้อมูลได้ ซึ่งข้อมูลนอกเหนือจากนี้ พนักงานสอบสวนไม่สามารถอาศัยอำนาจตามมาตรา 132 เพื่อขอข้อมูลได้

2.3.4 อำนาจของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2.3.4.1 เขตอำนาจ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 ได้ให้อำนาจแก่พนักงานเจ้าหน้าที่กรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัติฉบับนี้ เจ้าหน้าที่สามารถขอข้อมูล หรือเข้าถึงข้อมูล และกระทำโดยประการอื่นให้ได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ เพื่อประโยชน์ในการใช้เป็นพยานหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

อนึ่ง การใช้อำนาจบางอย่างของเจ้าหน้าที่อาจเป็นการกระทบต่อสิทธิและเสรีภาพของประชาชน กฎหมายจึงได้ควบคุมอำนาจดังกล่าวโดยการให้พนักงานเจ้าหน้าที่ต้องขออนุญาตศาลก่อนมีการใช้อำนาจบางประการ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 19 บัญญัติว่า “การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่า บุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว .....”

2.3.4.2 อำนาจหน้าที่ของพนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนสอบสวนเฉพาะคดีที่เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้น โดยมีอำนาจสองลักษณะดังนี้

ก. การใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งไม่ต้องขออนุญาตศาล ได้แก่การใช้อำนาจตามมาตรา 18 อนุ (1) (2) และ (3)

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัติมาให้ถ้อยคำหรือชี้แจงเป็นหนังสือ หรือส่งเอกสารข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ใช้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตร 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

ข. การใช้อำนาจของพนักงานเจ้าหน้าที่ซึ่งต้องขออนุญาตศาลการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 รวม 5 ประการตาม (4) (5) (6) (7) หรือ (8) ต้องขออนุญาตศาลตามวิธีการที่บัญญัติไว้ในมาตรา 19 ก่อน[38]

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าว ให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับรหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดของผู้กระทำความผิดตามพระราชบัญญัตินี้

---

[38] พรเพชร วิชิตชลชัย, **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** [Online], ม.ป.ป. แหล่งที่มา www.coj.go.th/home/document/computer_miss_2550.pdf.

นอกจากอำนาจข้างต้น พนักงานเจ้าหน้าที่ยังมีอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาเนื่องจากมาตรา 29 บัญญัติว่าในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ให้อำนาจพนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษและมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

2.3.5 แนวทางปฏิบัติในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์

จากการสัมภาษณ์พนักงานสอบสวน ซึ่งได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้ข้อมูลว่า ในทางปฏิบัติในคดีเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเกิดขึ้นซึ่งจะต้องใช้ข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐาน เมื่อผู้พนักงานสอบสวนผู้รับผิดชอบต้องการข้อมูลจราจรทางคอมพิวเตอร์ ก็จะส่งหนังสือมาให้พนักงานสอบสวนที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อดำเนินการขอข้อมูลจากผู้ให้บริการมาเป็นพยานหลักฐานให้ โดยวิธีการขอข้อมูลดังกล่าวทำโดย พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ส่งหมายเรียกเอกสารแก่ผู้ให้บริการที่เกี่ยวข้องเพื่อตรวจสอบข้อมูลโดยจะระบุรายละเอียด การกระทำความผิด ช่วงเวลาที่ขอให้ตรวจสอบ ชื่อผู้ใช้บริการที่ขอให้ตรวจสอบ หรือหมายเลขโทรศัพท์ หรือหมายเลข IP Address ต้นทางที่ใช้ในการเชื่อมต่ออินเทอร์เน็ตในการกระทำความผิด หรือ URL ที่เกิดการกระทำความผิด และจะได้รับการตอบกลับจากผู้ให้บริการเป็นจดหมายแจ้งเกี่ยวกับรายละเอียดที่ต้องการโดยมีข้อมูลเฉพาะส่วนที่เกี่ยวข้องกับผู้ให้บริการรายดังกล่าวส่งมาให้แก่พนักงานเจ้าหน้าที่ผู้ออกหมาย และเมื่อได้ข้อมูลจากผู้ให้บริการแต่ละรายแล้ว ก็จะมาพิจารณาประกอบการสืบสวนเพื่อเชื่อมโยงหาพยานหลักฐานเพิ่มเติมเพื่อให้มีพยานหลักฐานเพียงพอที่จะระบุตัวผู้กระทำความผิดและเป็นพยานหลักฐานในการลงโทษผู้กระทำความผิดต่อไป

จากการสัมภาษณ์ผู้จัดการฝ่ายงานความมั่นคงข้อมูลสารสนเทศของผู้ให้บริการอินเทอร์เน็ตพร้อมโทรศัพท์เคลื่อนที่รายหนึ่งพบว่า เมื่อได้รับหมายเรียกข้อมูลจราจรทางคอมพิวเตอร์จากพนักงานเจ้าหน้าที่แล้ว ผู้ให้บริการจะดำเนินการตรวจสอบว่ามีความเกี่ยวข้องกับผู้ให้บริการในส่วนใด และในช่วงระยะเวลาดังกล่าวมีข้อมูลเกี่ยวกับสิ่งที่พนักงานเจ้าหน้าที่ขอรายละเอียดมาอย่างไรบ้าง โดยการเข้าสู่ระบบที่ต้องใช้รหัสเฉพาะผู้มีอำนาจในการเข้าถึงได้เท่านั้น โดยเมื่อเข้าระบบแล้วจะสามารถเลือกเวลาเพื่อตรวจสอบข้อมูลได้ ทั้งหมายเลขโทรศัพท์ และการเชื่อมต่ออินเทอร์เน็ตที่เกี่ยวข้อง และเมื่อได้ข้อมูลจราจรทางคอมพิวเตอร์ในรูปแบบของเลขรหัสเรียบร้อย ผู้ให้บริการก็จะดำเนินการถอดเลขรหัสดังกล่าวให้เป็นข้อมูลปกติในรูปแบบไฟล์ Word หรือ ไฟล์ Excel โดยจัดพิมพ์เป็นข้อมูลธรรมดาแล้วแนบท้ายเอกสารหนังสือตอบกลับหมายเรียกของพนักงานเจ้าหน้าที่ โดยจะไม่มีการแนบข้อมูล

ต้นฉบับที่เริ่มประมวลผลให้แก่พนักงานเจ้าหน้าที่เนื่องจากข้อมูลจะต้องมีการแปลความหมายให้เรียบร้อยก่อน

2.3.6 สรุปเรื่องอำนาจในการได้มาซึ่งพยานหลักฐานกับคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

สำหรับคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต มีลักษณะของการกระทำและข้อมูลที่อยู่บนระบบคอมพิวเตอร์ หากพิจารณาจากหลักการที่เคยมีมา ผู้ที่จะสืบสวนและหาพยานหลักฐานในกรณีนี้จึงควรเป็นผู้ที่มีความรู้ทั้งทางด้านลิขสิทธิ์และความรู้ทางเทคโนโลยีสารสนเทศพอสมควร เพื่อให้เข้าใจระบบการทำงานของคอมพิวเตอร์ การเกิดข้อมูลพยานหลักฐานจราจรทางคอมพิวเตอร์ รวมไปถึงการจัดเก็บข้อมูลดังกล่าว แต่ตามที่ได้กล่าวมาข้างต้นพบว่า ผู้ที่มีอำนาจในการหาพยานหลักฐานในคดีลิขสิทธิ์เป็นหลักคือ เจ้าหน้าที่ตามพระราชบัญญัติลิขสิทธิ์ โดยปัจจุบันกลับยังไม่มีการกำหนดคุณสมบัติหรือหน่วยงานเฉพาะดังกล่าวขึ้นอย่างชัดเจนแต่อย่างใดในทางตรงกันข้าม เมื่อมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ออกมาใช้บังคับ ได้มีการกำหนดให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นผู้มีอำนาจในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ เมื่อมีการกำหนดอำนาจเฉพาะเช่นนี้ จึงส่งผลให้ เจ้าหน้าที่ตามกฎหมายอื่นหากไม่มีอำนาจเฉพาะจะขอข้อมูลจราจรทางคอมพิวเตอร์มิได้ เว้นแต่ผ่านพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

และจากข้อมูลข้างต้นพบว่า ตามความเห็นของคณะกรรมการกฤษฎีกาเรื่องเรื่องเสร็จที่ 343/2549 ที่มีความเห็นว่า พนักงานสอบสวนตามประมวลกฎหมายอาญา มีอำนาจขอเฉพาะชื่อ และที่อยู่ของผู้กระทำความผิดที่ปรากฏบนเอกสารเท่านั้น ไม่สามารถขอข้อมูลจราจรทางคอมพิวเตอร์ที่มีลักษณะบ่งบอกถึงการสื่อสารของระบบคอมพิวเตอร์ได้ เมื่อพนักงานสอบสวนตามประมวลกฎหมายอาญาไม่มีอำนาจในการได้มาซึ่งข้อจราจรทางคอมพิวเตอร์ เจ้าหน้าที่ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ซึ่งอาศัยอำนาจตามพระราชบัญญัติดังกล่าวประกอบกับการให้เป็นเจ้าหน้าที่ตามประมวลกฎหมายอาญา จึงไม่มีอำนาจในการขอข้อมูลจราจรทางคอมพิวเตอร์ด้วยเช่นกัน เพราะกฎหมายมิได้ให้อำนาจไว้เป็นการเฉพาะ สิ่งที่กฎหมายให้อำนาจไว้นั้นมีข้อความลักษณะเดียวกันกับพนักงานสอบสวนตามกฎหมายอาญาเท่านั้น และสำหรับผู้มีอำนาจขอข้อมูลดังกล่าวได้ก็คือ พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีอำนาจจำกัดเฉพาะความผิดตามพระราชบัญญัติว่าด้วยกากระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เท่านั้น หากในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตคดีใดไม่ได้มีความผิดทางตามพระราชบัญญัตินี้เกิดขึ้น พนักงานเจ้าหน้าที่ก็ไม่มีอำนาจที่จะขอข้อมูลจราจรทางคอมพิวเตอร์หรือพยานหลักฐานอิเล็กทรอนิกส์อื่น ๆ ให้ได้ จึงเหลือเพียงพนักงานสอบสวนคดีพิเศษเท่านั้นที่มีอำนาจในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ แต่ก็ต้องเป็นกรณีเฉพาะที่อยู่ในอำนาจการสืบสวนดังกล่าว คือเฉพาะคดีที่มีลักษณะพิเศษและเป็นคดีใหญ่ที่กระทบต่อเศรษฐกิจของประเทศ ด้วยเหตุนี้จึงทำให้การสืบหาพยานหลักฐานในกรณีละเมิดลิขสิทธิ์บน

อินเทอร์เน็ตทำได้ยาก และอาจส่งผลให้พยานหลักฐานนั้นไม่สามารถนำไปใช้ได้เพราะเจ้าหน้าที่ตามกฎหมายไม่มีอำนาจที่จะได้มาซึ่งพยานหลักฐานตามหลักที่ว่าพยานหลักฐานที่ได้มาโดยไม่ชอบไม่สามารถรับฟังได้

2.4 หลักการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

2.4.1 หลักการทั่วไปของจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ด้วยเหตุที่ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลที่สามารถนำสืบถึงรายละเอียดได้ว่าการกระทำความผิดเกิดขึ้นจากผู้ใช้คอมพิวเตอร์เครื่องใด เวลาที่กระทำความผิดคือเวลาใด โดยมีหลักฐานคือเส้นทางการสื่อสารข้อมูล ไปยังเครื่องปลายทางยืนยัน และสามารถระบุได้ว่าเป็นข้อมูลประเภทใด มีการกระทำความผิดมากน้อยประการใด ข้อมูลจราจรทางคอมพิวเตอร์จึงมีความสำคัญอย่างยิ่งในการเป็นพยานหลักฐานนำสืบหาตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์มาลงโทษได้ โดยหากไม่มีข้อมูลดังกล่าว หรือข้อมูลได้รับความเสียหายอันทำให้ข้อมูลบางส่วนหายไป ก็เป็นการยากที่จะนำสืบได้ว่าการกระทำเกิดขึ้นจากแหล่งใด หรือมีการกระทำเกิดขึ้นจริงหรือไม่

ความสำคัญของข้อมูลจราจรทางคอมพิวเตอร์ปรากฏอย่างชัดเจนในหลักการและเหตุผลของประกาศกระทรวงฯ อันได้แสดงถึงวัตถุประสงค์ของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ว่า “... ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำ เนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว” ซึ่งข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้สามารถนำไปใช้เป็นพยานหลักฐานได้ตั้งแต่ชั้นของการสืบสวนอันเป็นชั้นของรวบรวมข้อเท็จจริงว่ามีการกระทำความผิดทางอาญาหรือไม่โดยผู้ใด หรือในชั้นของการสอบสวนในลักษณะเป็นการรวบรวมพยานหลักฐานเพื่อยืนยันการกระทำความผิดของผู้ต้องหา ไปจนถึงนำไปใช้เป็นพยานหลักฐานในกระบวนการพิจารณาคดี

กฎหมายที่กำหนดผู้ที่มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 26 กำหนดว่า

“ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปี เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า เก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท”

เมื่อพิจารณาตามมาตรา 26 ผู้ให้บริการย่อมมีหน้าที่จัดเก็บข้อมูล 2 ประการ[39] คือ

ก. ข้อมูลจราจรทางคอมพิวเตอร์ หรือ Traffic data ผู้ให้บริการจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน โดยผู้ให้บริการประเภทใดมีหน้าที่จัดเก็บอะไรบ้าง และเก็บอย่างไรนั้น เป็นไปตามประกาศของรัฐมนตรีว่าการกระทรวงเทคโนโลยีและสารสนเทศ

ข. ข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ อันได้แก่ชื่อ นามสกุล หมายเลขประจำตัวประชาชน โดยกฎหมายกำหนดให้เก็บข้อมูลไว้อย่างน้อยเก้าสิบวันนับแต่วันที่การใช้บริการสิ้นสุด โดยไม่ได้มีกำหนดเพิ่มเติมว่าจะต้องมีระบบการจัดเก็บอย่างไร ขอให้ข้อมูลที่จัดเก็บนั้นถูกต้องและสามารถบ่งบอกถึงตัวผู้ใช้บริการได้แท้จริงก็เพียงพอต่อกฎหมายแล้ว ซึ่งหากผู้ให้บริการไม่จัดเก็บข้อมูลดังกล่าวเอาไว้จะมีความผิดและต้องชำระค่าปรับเป็นเงินจำนวน 500,000 บาท

เนื่องจากข้อมูลของผู้ใช้บริการเป็นข้อมูลที่มิได้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ กฎหมายจึงกำหนดแต่เพียงให้มีการจัดเก็บข้อมูลดังกล่าวที่ถูกต้อง คือพิจารณาจากหลักฐานการแสดงตนเช่น บัตรประชาชน ทะเบียนบ้าน ที่แสดงต่อผู้ใช้บริการเท่านั้น ในขณะที่ ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลอิเล็กทรอนิกส์กฎหมายจึงต้องมีการกำหนดหลักการและวิธีการจัดเก็บเพิ่มเติมตามประกาศของรัฐมนตรีว่าการกระทรวงเทคโนโลยีและสารสนเทศ เพื่อให้ข้อมูลนั้นมีความปลอดภัยและถูกต้อง โดยผู้ให้บริการเป็นผู้มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

2.4.2. ข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องจัดเก็บ

ข้อมูลจราจรทางคอมพิวเตอร์ที่กฎหมายให้จัดเก็บนั้นมีหลายประเภทหลายรูปแบบตามแต่จะกำหนดให้ผู้ให้บริการจัดเก็บแบบใด ข้อมูลจราจรทางคอมพิวเตอร์ที่ปรากฏอยู่ในประกาศกระทรวงเทคโนโลยีและสารสนเทศ เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อพิจารณาจากลักษณะการเกิดของข้อมูลจราจรทางคอมพิวเตอร์สามารถแยกข้อมูลจราจรทางคอมพิวเตอร์ตามประกาศกระทรวงฯออกได้เป็น 2 ประเภท คือ

ก. ข้อมูลจราจรทางคอมพิวเตอร์โดยแท้ หมายถึง ข้อมูลที่เกิดขึ้นเมื่อมีการติดต่อสื่อสารของระบบคอมพิวเตอร์ อันได้แก่

(1) Log หมายถึง บันทึกข้อมูลเหตุการณ์ ซึ่งขึ้นอยู่กับว่าจะเป็นบันทึกเหตุการณ์หรือข้อมูลของสิ่งใด เช่น Log ซึ่งบันทึกการเข้าถึงเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย เป็นต้น

---

[39] เรื่องเดียวกัน, 53.

(2) IP Address หมายถึง หมายเลขประจำตัวของเครื่องคอมพิวเตอร์ที่ใช้ติดต่อกันผ่านเครือข่ายอินเทอร์เน็ต ซึ่งตามปกติแต่ละเครื่องบนเครือข่ายอินเทอร์เน็ตจะมีหมายเลข IP ที่ไม่ซ้ำกัน ทำให้สามารถอ้างอิงถึงตัวตนถึงกันและกันได้[40]

(3) ข้อมูลเชื่อมต่อ Cell ID หมายถึงข้อมูลที่แสดงว่า Cell ID ใดเป็นจุดที่ใช้ในการติดต่อสื่อสาร ซึ่งข้อมูลนี้จะเกิดขึ้นเมื่อมีการติดต่อสื่อสารของระบบคอมพิวเตอร์

(4) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล คือ ข้อมูลจราจรทางคอมพิวเตอร์โดยแท้ตามคำนิยาม คือเมื่อมีการติดต่อสื่อสารของระบบคอมพิวเตอร์จะต้องมีการใช้เส้นทางในการส่งข้อมูลระหว่างระบบคอมพิวเตอร์

(5) ข้อมูลหมายเลข Port เปรียบเสมือนหมายเลขถนนหรือช่องทางที่จะให้ข้อมูลจราจรทางคอมพิวเตอร์เดินทางไปได้ โดยข้อมูลจราจรทางคอมพิวเตอร์จะแสดงให้เห็นว่าเป็นหมายเลข Port ใด

(6) ข้อมูลเกี่ยวกับวัน เวลาที่ใช้บริการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ เป็นข้อมูลที่เกิดขึ้นพร้อมกับการใช้บริการ จึงเป็นข้อมูลจราจรทางคอมพิวเตอร์โดยแท้

ข. ข้อมูลที่กฎหมายถือว่าเป็นข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลดังกล่าวโดยลักษณะของข้อมูลเป็นข้อมูลที่เกิดขึ้นหรือมีอยู่แม้ไม่เกิดการติดต่อสื่อสารของระบบ แต่ผู้ให้บริการต้องจัดเก็บในฐานะที่เป็นข้อมูลที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ซึ่งเป็นข้อมูลจราจรทางคอมพิวเตอร์ตามคำนิยามของกฎหมายด้วย ข้อมูลที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

(1) ชื่อและที่อยู่ของผู้ใช้บริการ ข้อมูลในส่วนนี้เป็นข้อมูลที่ผู้ให้บริการจะต้องจัดเก็บข้อมูลโดยขอจากผู้ใช้บริการ มิได้เกิดขึ้นในขั้นตอนของการติดต่อสื่อสารแต่อย่างใด แต่เกี่ยวข้องกับการติดต่อสื่อสาร คือบ่งบอกได้ว่าใครเป็นผู้ติดต่อสื่อสาร

(2) ข้อมูลที่สามารถระบุตัวบุคคล หมายถึง กรณีที่มีการใช้บริการอินเทอร์เน็ตสาธารณะหรือในร้านอินเทอร์เน็ต รวมทั้งการเชื่อมต่ออินเทอร์เน็ตแบบไร้สาย จะต้องมีวิธีการเก็บข้อมูลผู้ใช้บริการเพื่อให้สามารถระบุตัวบุคคลที่ใช้บริการได้

(3) เวลาการเข้าใช้และเลิกใช้บริการของผู้ให้บริการ หมายถึง ต้องมีการจัดเก็บว่าผู้ใช้บริการรายใด ใช้บริการตั้งแต่เวลาเท่าใด ถึงเท่าใด เพื่อให้สามารถระบุช่วงเวลาที่มีการใช้บริการกับ ช่วงเวลาที่เกิดข้อมูลจราจรทางคอมพิวเตอร์ได้ว่าเป็นช่วงเวลาเดียวกันหรือไม่

(4) หมายเลขเครื่องที่ใช้ IP Address ตามที่ได้กล่าวไปแล้วว่า IP Address หมายถึงหมายเลขประจำตัวเครื่องที่ใช้ในการติดต่อสื่อสารถึงกัน แต่เนื่องด้วยลักษณะของหมายเลขดังกล่าวจะมีการเปลี่ยนแปลงทุกครั้งที่มีการเชื่อมต่อเข้าสู่ระบบอินเทอร์เน็ตหรือระบบของผู้ใช้บริการใหม่ ดังนั้น จึงต้อง

---

[40] โอภาส เอี่ยมสิริวงศ์, **วิทยาการคอมพิวเตอร์และเทคโนโลยี (ฉบับปรับปรุง),** (กรุงเทพฯ: ซีเอ็ดยูเคชั่น, 2551), 318.

มีการจัดเก็บว่า เครื่องคอมพิวเตอร์เครื่องใด ใช้ หมายเลข IP Address นั้นในขณะที่เกิดการติดต่อสื่อสาร

โดยลักษณะที่แตกต่างกันของข้อมูลจราจรทางคอมพิวเตอร์และของผู้ให้บริการแต่ละประเภท การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อจะนำมาใช้เป็นพยานหลักฐานจึงมีความแตกต่างกันไปด้วย โดยประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลัก เกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ข้อ 7 ได้กำหนดไว้ว่าผู้ให้บริการประเภทใดจะต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ประเภทใด ดังนี้

ผู้ให้บริการประเภทผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง มีลักษณะของการให้บริการที่เป็นการเชื่อมต่อผ่านทางเครือข่ายโทรศัพท์ สายเชื่อมต่อสัญญาณ หรือผ่านดาวเทียม เนื่องจากอุปกรณ์ในการติดต่อสื่อสารหรือกระจายภาพและเสียง ถือเป็นส่วนหนึ่งของระบบคอมพิวเตอร์ที่อาจเกิดการกระทำความผิดขึ้นกับอุปกรณ์หรือใช้อุปกรณ์ดังกล่าวในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ อีกทั้งการติดต่อสื่อสารของระบบคอมพิวเตอร์จะต้องอาศัยเส้นทางในการเชื่อมต่ออาจเป็นการเชื่อมต่อผ่านสายส่งสัญญาณโทรศัพท์ หรือการส่งสัญญาณเชื่อมต่อผ่านดาวเทียม ดังนั้นเพื่อให้มีข้อมูลเส้นทางการติดต่อสื่อสารจัดเก็บไว้ กฎหมายจึงกำหนดให้ผู้ให้บริการประเภทนี้ต้องเก็บข้อมูลดังต่อไปนี้

(1) ข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิด ต้นทาง ปลายทาง และทางสายที่ผ่านของการติดต่อสื่อสารของระบบคอมพิวเตอร์ หมายถึง ข้อมูลระบบชุมสายโทรศัพท์พื้นฐาน หรือ วิทยุมือถือและระบบตู้โทรศัพท์สาขา รวมไปถึงหมายเลขโทรศัพท์ หรือ เลขหมายวงจร เพื่อให้สามารถระบุได้ว่าการติดต่อสื่อสารดังกล่าวเริ่มต้น หรือมีเส้นทางการเชื่อมต่ออย่างไร และให้เก็บชื่อ ที่อยู่ของผู้ใช้บริการหรือผู้ใช้งานที่ลงทะเบียน ซึ่งเป็นข้อมูลที่ผู้ให้บริการมีหน้าที่เก็บอยู่แล้วตาม มาตรา 26 วรรคสอง ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และสำหรับอย่างสุดท้าย ข้อมูลเกี่ยวกับ วันที่ เวลา และที่ตั้งของ Cell ID หรือตัวส่งสัญญาณซึ่งมีการใช้บริการ เพื่อสามารถระบุได้ว่ามีการใช้งานเมื่อใด เวลาใด และบริเวณใด อย่างละเอียด

(2) ข้อมูลที่สามารถระบุวันที่ เวลา และระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์เพื่อให้ทราบช่วงเวลาที่มีการกระทำได้อย่างชัดเจน อันจะเชื่อมโยงกับการกระทำความผิดได้อย่างถูกต้อง

(3) ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้โทรศัพท์มือถือหรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย อันได้แก่ 1) ที่ตั้ง Label ในการเชื่อมต่อ ณ สถานที่เริ่มติดต่อสื่อสาร 2) ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถืออันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร และ 3) จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

ผู้ให้บริการประเภทผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ และผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่าง ๆ เป็นลักษณะของผู้ให้บริการเข้าถึงเครือข่ายต่าง ๆ

หรือให้ใช้ระบบคอมพิวเตอร์โดยตัวผู้ให้บริการเป็นช่องทางผ่านให้ผู้ใช้บริการสามารถเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ หรือเครือข่ายอินเทอร์เน็ตเพื่อติดต่อสื่อสารกับผู้อื่นต่อไปได้ กฎหมายกำหนดให้ผู้ให้บริการประเภทนี้ต้องจัดเก็บข้อมูลดังต่อไปนี้

(1) ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย ได้แก่ ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย เป็นข้อมูลที่บันทึกเกี่ยวกับการเชื่อมต่อว่าเชื่อมต่อไปไหนอย่างไรบ้าง ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่ายด้วย และ ข้อมูลเกี่ยวกับวัน และเวลาติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ เพื่อให้สามารถระบุเวลาที่ผู้กระทำผิดเข้ามาในระบบ หรือกระทำการในระบบ รวมทั้งข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ และ ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบ หรือ เรียกว่า Assigened IP Address ซึ่งจะเป็นตัวที่ให้ไว้เวลาผู้ใช้บริการเข้ามาในระบบ เพื่อจะสามารถระบุได้ว่า ระบบคอมพิวเตอร์ใดเป็นผู้ใช้บริการใด ไม่อย่างนั้นจะไม่มีรหัสที่จะตามจากผู้ใช้บริการได้หากไม่มี IP Address และสุดท้าย ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification) ซึ่งจะบ่งบอกได้ว่าผู้ที่เชื่อมต่อเข้ามาคือใครโดยดูจากหมายเลขที่ใช้เป็นสายเรียกเข้ามาในการเชื่อมต่ออินเทอร์เน็ต อย่างไรก็ดี ปัจจุบันการเชื่อมต่ออินเทอร์เน็ตได้พัฒนาการเชื่อมต่อได้โดยไม่ต้องใช้หมายเลขโทรศัพท์ในการเรียกเข้า ดังนั้น จึงควรต้องมีการประกาศเพิ่มเติมเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องจัดเก็บ เพื่อให้สามารถระบุถึงผู้ที่เชื่อมต่ออินเทอร์เน็ตได้อย่างชัดเจน เช่นเดียวกับหมายเลขสายที่เรียกเข้ามา

(2) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (E-mail Servers) ได้แก่ ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ ซึ่งรวบรวมไว้ด้วย ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ผู้ส่ง และ ผู้รับ ข้อมูลที่บ่งบอกถึงสถานะในการตรวจสอบ เป็นต้น รวมทั้ง IP Address ของผู้ใช้บริการ และผู้ที่เชื่อมต่อกับระบบอยู่ รวมถึงข้อมูลวันเวลาที่มีการเชื่อมต่อ ชื่อผู้ใช้งาน และ ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์

(3) ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูลอันได้แก่ ข้อมูล Log ข้อมูลวันและเวลา การติดต่อของเครื่องที่เข้ามาใช้บริการ และ หมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้บริการ รวมถึง ชื่อผู้ใช้งาน และ ข้อมูลตำแหน่ง ชื่อไฟล์ ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป เพื่อทราบได้ว่าใครเข้ามาเพื่ออัพโหลด หรือดาวโหลด อะไรบ้าง หากเป็นข้อมูลที่มีละเมิดผู้อื่น จะได้สามารถหาตัวผู้กระทำความผิดมาลงโทษได้ด้วยหลักฐานดังกล่าว

(4) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ เช่นเดียวกับอย่างอื่นที่ต้องมีการเก็บ Log บันทึกการเข้าถึงเครื่องผู้ให้บริการเว็บ วัน และเวลาการติดต่อ ข้อมูล IP Address เพื่อบ่งบอกผู้กระทำ

ความผิดในเบื้องต้น และสิ่งที่เพิ่มขึ้นมาคือข้อมูลคำสั่งการใช้งานระบบ และข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล หรือ Uniform Resource Identifier (URI) เช่น ตำแหน่งของเว็บเพ็จ เพื่อให้รู้ผู้ใช้บริการเข้ามาทำการอย่างใดบ้าง

(5) ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet) ได้แก่ ข้อมูล Log วันและเวลาใช้บริการ รวมไปถึง ข้อมูลหมายเลข Port ในการใช้งาน ข้อมูลชื่อเครื่องให้บริการ และข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งแล้ว

(6) ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต ได้แก่ข้อมูล Log วันและเวลาติดต่อของผู้ใช้บริการ และข้อมูลชื่อเครื่องบนเครือข่ายและ หมายเลขเครื่องของผู้ใช้บริการที่เชื่อมต่ออยู่ในขณะนั้น

ผู้ให้บริการประเภทผู้ให้บริการร้านอินเทอร์เน็ต กฎหมายกำหนดให้เก็บข้อมูลที่สามารรถระบุตัวบุคคล เวลาของการเข้าใช้และเลิกใช้บริการคือสามารถรู้ได้ว่าใคร ใช้บริการคอมพิวเตอร์เครื่องใด เวลาใดถึงเวลาใด รวมทั้งหมายเลขเครื่องที่ใช้ IP Address โดยกฎหมายกำหนดเช่นนี้เนื่องจากเจตนารมณ์ที่จะสามารถนำสืบถึงตัวผู้กระทำความผิดที่แท้จริงได้หากมีการกระทำความผิดผ่านระบบคอมพิวเตอร์ของร้านอินเทอร์เน็ตดังกล่าว คือ เมื่อมีการกระทำผิดจากร้านอินเทอร์เน็ต โดยทราบเวลาและหมายเลข IP Address ซึ่งไปปรากฏที่เครื่องของผู้ให้บริการ จะสามารถสืบมายังร้านอินเทอร์เน็ต และตรวจสอบว่าใครเป็นผู้ใช้ IP Address นั้นในเวลาที่มีการกระทำความผิด โดยหากไม่มีการเก็บข้อมูลตรงนี้ไว้ แม้ผู้ให้บริการรายใหญ่จะเก็บข้อมูลมากเท่าใดก็ตาม แต่เส้นทางการสืบสวนก็จะสิ้นสุดลงที่ร้านอินเทอร์เน็ต เพราะไม่ได้เก็บข้อมูลผู้ใช้บริการไว้เป็นต้น

ในส่วนของผู้ให้บริการประเภทผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น กฎหมายกำหนดให้ เก็บข้อมูลรหัสประจำตัวของผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือ เลขประจำตัวของผู้ขายสินค้าหรือบริการ หรือผู้ใช้บริการ และที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการด้วย อีกทั้งให้เก็บ บันทึกข้อมูลการเข้าใช้บริการ และในกรณีผู้ให้บริการเว็บบอร์ด หรือบล็อก จะต้องเก็บข้อมูลของผู้ประกาศข้อมูลด้วย

การกำหนดให้เก็บข้อมูลดังกล่าวนั้นหากแบ่งตามลักษณะของการสื่อสารข้อมูลคอมพิวเตอร์ที่ผู้ให้บริการแต่ละประเภทจะพึงมีต่อผู้ใช้บริการ จะแบ่งได้เป็น 2 กลุ่มใหญ่ คือ กลุ่มแรกได้แก่ผู้ให้บริการประเภทผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง ผู้ให้บริการประเภทผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ และผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่าง ๆ จะเป็นการให้บริการในลักษณะที่เป็นสื่อกลางในการเชื่อมต่อสื่อสารของระบบคอมพิวเตอร์ ระหว่างผู้ใช้บริการกับผู้อื่น หรือผู้ให้บริการรายอื่น โดยไม่มีลักษณะของการให้บริการข้อมูล เพราะเป็นการให้บริการเป็นทางผ่านในการเชื่อมต่อให้แก่ผู้ใช้บริการเท่านั้น ดังนั้นข้อมูลที่ปรากฏบนเครื่องคอมพิวเตอร์ของผู้ให้บริการประเภทนี้จึงมีเพียงว่า ระบบคอมพิวเตอร์ใด เชื่อมต่อไปยังระบบ

คอมพิวเตอร์อื่นใด ในเวลาหนึ่งเวลาใด โดยปริมาณข้อมูลที่มากขนาดไหน ส่วนจะเป็นข้อมูลการกระทำอะไรนั้น ผู้ให้บริการประเภทนี้จะไม่มีข้อมูลดังกล่าว

ส่วนผู้ให้บริการอีกกลุ่มหนึ่งได้แก่ ผู้ให้บริการประเภทผู้ให้บริการร้านอินเทอร์เน็ตและผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น โดยผู้ให้บริการกลุ่มนี้จะไม่ใช่ผู้ให้บริการในการเข้าถึงเครือข่ายเพื่อนำไปสู่การติดต่อสื่อสาร แต่จะเป็นผู้ให้บริการใช้ระบบคอมพิวเตอร์ซึ่งจะปรากฏประเภทบริการ หรือลักษณะการใช้บริการให้มีการจัดเก็บอย่างชัดเจน เช่นร้านอินเทอร์เน็ต หรือร้านเกมออนไลน์ ก็จะทราบว่าผู้ใช้บริการได้ใช้บริการอะไรบ้าง เป็นใครเข้ามาใช้บริการโดยละเอียด หรือผู้ให้บริการแอพพลิเคชั่น หรือ เว็บบอร์ด ก็จะทราบว่า ผู้ใช้บริการได้โพสต์ข้อความลักษณะใดไว้ หรือมีการใช้บริการรูปแบบใดหรือลักษณะใดเอาไว้ในเว็บบอร์ดหรือ แอพพลิเคชั่นที่มีการให้บริการอยู่ ซึ่งเห็นได้ว่าข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการประเภทนี้จะสามารถบอกรายละเอียดเกี่ยวกับการใช้บริการได้มากกว่ากลุ่มแรก อย่างไรก็ตาม ผู้ให้บริการประเภทนี้จะไม่มีข้อมูลว่าช่องทางการเชื่อมต่อเข้ามานั้น มีปลายทางอยู่ ณ แห่งหนใด โดยจะสามารถรู้ IP Address ได้เท่านั้น ซึ่งจะต้องนำข้อมูล IP Address ดังกล่าวไปตรวจสอบต่อว่าเป็นของใคร เป็น IP ที่ผู้ให้บริการประเภทใดกำหนด เพื่อหาช่วงเวลา และปลายที่ผู้ใช้บริการเชื่อมต่อต่อไป จากผู้ให้บริการกลุ่มแรก

ดังนั้น ไม่ว่าจะเป็นผู้ให้บริการประเภทใดก็ตาม หน้าที่ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์มีความสำคัญมาก เพราะการเชื่อมต่อหรือใช้บริการแต่ละครั้ง ผู้ใช้บริการจะเชื่อมต่อไปยังผู้ให้บริการเกือบทุกประเภท หากผู้ให้บริการประเภทที่เกี่ยวข้องไม่ได้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ ส่วนที่ผู้อื่นเก็บไว้เมื่อนำไปสืบสวนก็จะมาจบลงที่ผู้ให้บริการซึ่งไม่ได้มีการจัดเก็บไว้ทำให้ไม่สามารถสืบสวนต่อเพื่อหาตัวผู้กระทำผิดมาลงโทษได้ อันส่งผลกระทบต่อผู้ที่จัดเก็บข้อมูลถูกต้องก็ไม่สามารถนำข้อมูลไปใช้ประโยชน์ได้เต็มที่ และส่งผลกระทบต่อความยุติธรรมที่ไม่สามารถหาตัวผู้กระทำความผิดมาลงโทษได้

2.4.3 วิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

วิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของประเทศไทย มีหลักการกำหนดไว้ในประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการ พ.ศ. 2550 ข้อ 8 บัญญัติว่า “การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

(1) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(2) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือ การทำ Data Archiving หรือ ทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้ให้บริการองค์กรกำหนดให้สามารถเข้าถึงข้อมูล

ดังกล่าวได้ เช่น ผู้ตรวจสอบ ระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ ตามพระราชบัญญัตินี้

(3) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(4) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือบริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(5) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ 1 ถึงข้อ 4 ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ 1 ถึงข้อ 4 ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการเช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย”

พิจารณาจากบทบัญญัติดังกล่าว พบว่าหลักการสำคัญของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้มีวิธีที่มั่นคงปลอดภัยนี้ หมายถึง ระบบหรืออุปกรณ์ที่จัดเก็บข้อมูลจะต้องมีคุณภาพที่สามารถเก็บรักษาความถูกต้องสมบูรณ์ของข้อมูล และโดยมีระบบป้องกันมิให้มีการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้ สามารถจำแนกหลักการของความมั่นคงปลอดภัยได้เป็น 2 ประเภท ประเภทแรกคือความมั่นคงปลอดภัยของระบบกับข้อมูลที่จัดเก็บ และประเภทที่สองคือความมั่นคงปลอดภัยในวิธีการปฏิบัติงาน

สำหรับความมั่นคงปลอดภัยของระบบและข้อมูลที่จัดเก็บนั้น มีหลักการสำคัญ 3 ประการคือ

(ก) เก็บในสื่อที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้คำว่าถูกต้องแท้จริงหรือภาษาอังกฤษใช้คำว่า Integrity นั้นปรากฏอยู่ใน Convention On Cybercrime ใน Article 16 เช่นเดียวกัน ซึ่งมีเนื้อหาว่า “... the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary,...” จากประโยคดังกล่าวมีผู้แปลไว้ว่า “บุคคลนั้นมีหน้าที่จะต้องเก็บรักษาและคงไว้ซึ่งความถูกต้องของข้อมูลคอมพิวเตอร์ดังกล่าวสำหรับช่วงระยะเวลาหนึ่งเท่าที่จำเป็น...” การเก็บในสื่อที่รักษาความ “ครบถ้วนถูกต้องแท้จริง” ตามความหมายดังกล่าวมีความหมายว่าอย่างไร เริ่มต้นผู้เขียนจึงพิจารณาโดยการแยกคำดังกล่าวออกมาพิจารณาดังนี้

ครบถ้วน หมายความถ้วน, เต็มจำนวนที่กำหนดไว้[41]

ถูกต้องมีความหมายตรงตัวและเข้าใจได้ว่ามีความถูกต้อง

แท้จริง หมายความว่าจริงแน่นอน[42]

การเก็บในสื่อที่ครบถ้วนถูกต้องแท้จริง จึงหมายถึง สื่อที่จะสามารถรักษาความครบถ้วนในข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องจัดเก็บตามหน้าที่ที่กฎหมายกำหนดสำหรับผู้ให้บริการแต่ละประเภท โดยสามารถจัดเก็บไว้ได้อย่างถูกต้องคือเกิดไม่ความบกพร่องอันอาจทำให้ข้อมูลมีการเปลี่ยนแปลง และมีความแท้จริง คือเป็นข้อมูลจริงแน่นอนมิได้มีการแก้ไขเปลี่ยนแปลงแต่ประการใด

ตามหลักการจับเก็บข้อมูลจราจรทางคอมพิวเตอร์นั้น ข้อมูลจราจรทางคอมพิวเตอร์ที่จะสามารถนำมาใช้ได้จะต้องเป็นข้อมูลที่มีความครบถ้วน ถูกต้อง แท้จริง โดยไม่อาจแก้ไขเปลี่ยนแปลงได้ เมื่อพิจารณาจากระบบการจัดเก็บข้อมูลคอมพิวเตอร์ในปัจจุบัน ในทางเทคนิคมีโปรแกรมที่สามารถบีบอัดข้อมูลโดยที่เนื้อหาของข้อมูลยังคงเป็นเช่นเดิมอยู่ได้ เช่น รูปภาพที่มีขนาดใหญ่ เมื่อย่อให้เล็กลงก็ยังเป็นรูปภาพที่สวยและมีรายละเอียดคงเดิมอยู่ เช่นเดียวกันกับข้อมูลจราจรทางคอมพิวเตอร์ ที่อาจจะมีการใช้เนื้อที่จำนวนมาก แต่หากมีการบีบอัดก็จะใช้พื้นที่น้อยลง โดยข้อมูลที่สามารถสื่อความหมายได้ยังคงเดิม โดยใช้โปรแกรมที่มีมาตรฐานสากล ซึ่งในต่างประเทศก็มีการกำหนดวิธีการนี้เพื่อใช้เก็บข้อมูลให้ได้มากยิ่งขึ้นเช่นเดียวกัน สำหรับประเทศไทย ยังไม่ปรากฏประเด็นในเรื่องดังกล่าวว่าสามารถทำได้หรือไม่ เนื่องจากผู้ให้บริการกลัวว่าจะเป็นการฝ่าฝืนกฎหมาย หากมีการบีบอัดข้อมูล โดยแม้ว่าข้อมูลดังกล่าวจะยังสามารถให้ข้อมูลจราจรทางคอมพิวเตอร์ได้ครบเหมือนกัน แต่ด้วยคำว่าครบถ้วนถูกต้องแท้จริงที่กฎหมายกำหนดนั้น อาจหมายถึงห้ามมีการเปลี่ยนแปลงใด ๆ แม้การบีบข้อมูลเพื่อให้มีข้อมูลที่เล็กลง

(ข) มีระบบการรักษาความลับ หรือชั้นความลับที่เข้าถึง

เนื่องจากข้อมูลจราจรทางคอมพิวเตอร์นี้ เป็นข้อมูลส่วนบุคคลชนิดหนึ่งที่สามารถระบุได้ว่าผู้ใช้บริการคนใดใช้บริการอะไรเป็นประจำ มีการติดต่อสื่อสารกับใครอยู่บ้าง หากมีการนำข้อมูลดังกล่าวออกเปิดเผยย่อมมีความผิดตามพระราชบัญญัตินี้ และนอกจากนั้นยังเป็นการเป็นการละเมิดสิทธิส่วนบุคคลอีกด้วย อย่างไรก็ตามเนื่องจากกฎหมายได้ให้อำนาจและกำหนดให้มีการจัดเก็บข้อมูลดังกล่าวผู้ให้บริการจึงสามารถจัดเก็บและเปิดเผยแก่ผู้มีอำนาจ ซึ่งมิใช่ผู้ใช้บริการได้ ดังนั้นการรักษาความลับจึงเป็นสิ่งสำคัญ แต่อย่างไรก็ตามการจัดเก็บข้อมูลดังกล่าว ย่อมไม่สามารถดำเนินการไปได้หากไม่มีมนุษย์เป็นผู้กระทำ เมื่อมนุษย์สามารถเข้ามาเกี่ยวข้องกับระบบจัดเก็บ และมีโอกาสเปลี่ยนแปลงระบบ หรือนำ

---

[41] พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2542, **ครบถ้วน** [Online], 20 เมษายน 2557. แหล่งที่มา http://rirs3.royin.go.th/new-search/word-search-all-x.asp.

[42] เรื่องเดียวกัน.

ข้อมูลไปเปิดเผย กฎหมายจึงกำหนดให้ต้องมีการรักษาความลับในการเข้าถึง โดยผู้ที่จะทำหน้าที่ดังกล่าว องค์กรหรือเจ้าของซึ่งเป็นผู้ให้บริการจะต้องมีการคัดสรรผู้ที่จะมาดูแลระบบที่สามารถไว้วางใจได้ ไม่อย่างนั้นผู้ให้บริการก็อาจมีความผิดตามพระราชบัญญัติ และเพื่อเป็นการรักษาความน่าเชื่อถือ และความถูกต้องไม่ให้มีการแก้ไขเปลี่ยนแปลงดังกล่าว ผู้ให้บริการจะต้องจัดทำระบบที่มีการป้องกันการแก้ไขไว้ด้วย

(ค) ข้อมูลที่จัดเก็บสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ ภาษาอังกฤษได้ระบุว่า “Identification and Authentication”

ตามพจนานุกรมฉบับราชบัณฑิตยสถาน แปลความหมายไว้ดังนี้

Identification หมายความว่า การพิสูจน์รูปพรรณ หรือ การระบุ [43]

Authentication มีความหมายว่า การพิสูจน์ตัวจริง[44]

เมื่อพิจารณาประกอบกับเจตนารมณ์ของประกาศดังกล่าวที่มุ่งนำตัวผู้กระทำความผิดมาลงโทษ การกำหนดให้ข้อมูลที่จัดเก็บสามารถ “ระบุรายละเอียดได้” จึงหมายถึงข้อมูลนั้นสามารถระบุพิสูจน์รูปพรรณและตัวจริงของผู้กระทำความผิดได้ว่าเป็นใคร โดยประการแรกข้อมูลต้องสามารถระบุได้ว่าต้นทางของการกระทำความผิดหรือระบบคอมพิวเตอร์ที่ใช้ในการกระทำความผิดคือเครื่องใดหรือเป็นของบุคคลใด และมีรายละเอียดเกี่ยวกับผู้ใช้ระบบคอมพิวเตอร์ในเวลาดังกล่าวว่าคือใคร เช่น กรณีมีผู้ใช้บริการร้านอินเทอร์เน็ต Café เพื่อโพสต์ข้อความหมิ่นประมาท การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่มีความมั่นคงปลอดภัยจะต้องสามารถระบุได้ว่าการกระทำความผิดนั้นมีจุดกำเนิดมาจากคอมพิวเตอร์เครื่องใดโดยจะมีข้อมูลเป็นหมายเลข IP Address ของคอมพิวเตอร์เครื่องใดซึ่งอาจเป็นของร้านอินเทอร์เน็ตร้านใดร้านหนึ่ง และต่อมาเมื่อทราบว่าเป็นร้านอินเทอร์เน็ตร้านใดแล้ว จึงตรวจสอบว่าในเวลาที่มีการกระทำความผิดใครเป็นผู้ใช้คอมพิวเตอร์เครื่องดังกล่าว ก็จะสามารถทราบได้ว่าผู้กระทำความผิดที่แท้จริงคือใคร ลักษณะเช่นนี้เองเรียกว่าเป็นการจัดเก็บที่สามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ตามที่กฎหมายกำหนด

สำหรับความมั่นคงปลอดภัยในวิธีการปฏิบัติงานคือ การจัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้การส่งมอบข้อมูลนั้นเป็นไปด้วยความรวดเร็ว โดยเป็นหน้าที่ของผู้

---

[43] โครงการจัดทำฐานข้อมูลงานวิชาการของราชบัณฑิตยสถาน ฐานข้อมูล ศัพท์นิติศาสตร์ อังกฤษ-ไทย และไทย-อังกฤษ, **Identification** [Online], วันที่ 20 เมษายน 2557. แหล่งที่มา http://rirs3.royin.go.th/coinages /webcoinage.php.

[44] โครงการจัดทำฐานข้อมูลงานวิชาการของราชบัณฑิตยสถาน ฐานข้อมูลศัพท์เทคโนโลยีสารสนเทศ อังกฤษ-ไทย, **Authentication** [Online], วันที่ 20 เมษายน 2557. แหล่งที่มา http://rirs3.royin.go.th/coinages /webcoinage.php.

ให้บริการที่จะต้องพิจารณาคัดสรรบุคคลผู้มีหน้าที่ดังกล่าวให้เป็นผู้ที่มีความไว้วางใจ และเชื่อถือได้ว่าจะไม่มีการแก้ไขเปลี่ยนแปลงข้อมูล หรือการนำข้อมูลดังกล่าวไปเปิดเผยแก่บุคคลอื่นนอกจากที่กฎหมายกำหนดให้มีหน้าที่เข้าถึงหรือขอข้อมูลดังกล่าวได้ เนื่องจากหากมีการกระทำดังกล่าวเกิดขึ้นย่อมเป็นความผิดตามพระราชบัญญัตินี้ และส่งผลต่อข้อมูลจราจรทางคอมพิวเตอร์อันทำให้ไม่สามารถนำไปใช้เป็นพยานหลักฐานได้เนื่องจากไม่มีความถูกต้อง และถือว่าผู้ให้บริการไม่มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามวิธีการที่กฎหมายกำหนด ย่อมมีความผิดตามพระราชบัญญัติเมื่อมีการเรียกข้อมูลดังกล่าวเช่นกัน

ในทางปฏิบัติสำหรับการตรวจสอบว่าผู้ให้บริการมีการจัดเก็บที่เป็นไปตามกฎหมายกำหนดหรือไม่ ตามข้อมูลจากการสัมภาษณ์ เจ้าหน้าที่กรมสอบสวนคดีพิเศษ ซึ่งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีความเห็นเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ว่า ด้วยระบบการให้บริการและการขอข้อมูลจราจรทางคอมพิวเตอร์ ย่อมเป็นการตรวจสอบเองในตัว ว่ามีการให้บริการตามมาตรฐานหรือไม่ คือ หากผู้ให้บริการรายใดไม่มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อนำสืบผู้กระทำความผิด ผู้ที่ประสงค์จะกระทำความผิดก็จะไปใช้ผู้ให้บริการรายนั้น และเมื่อมีการกระทำผิดปรากฏหลายการกระทำ ประกอบกับการไม่สามารถให้ข้อมูลจราจรทางคอมพิวเตอร์แก่เจ้าหน้าที่เมื่อมีการเรียกข้อมูลได้ ผู้ให้บริการรายนั้นก็จะถูกตรวจสอบและลงโทษ หรือมีคำสั่งให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่ถูกต้องต่อไป[45]

นอกจากวิธีการเก็บรักษาที่จะต้องมีความมั่นคงปลอดภัยแล้วนั้น เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการแต่ละประเภทเก็บมีความถูกต้องและสามารถนำมาใช้ประโยชน์ได้จริง การจัดเก็บข้อมูลจึงต้องมีการตั้งนาฬิกาบนอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที ตามประกาศกระทรวงฯ ข้อ 9 เพื่อให้ข้อมูลที่ผู้ให้บริการแต่ละที่จัดเก็บไว้สามารถนำมาเชื่อมโยงถึงกันได้อย่างถูกต้อง

อย่างไรก็ตาม นอกจากการกำหนดมาตรฐานและหลักการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อเป็นแนวทางให้แก่ผู้ให้บริการแล้ว ปัจจุบันยังไม่มีการกำหนดแนวทางที่จะตรวจสอบหรือยืนยันความถูกต้องและความน่าเชื่อถือของข้อมูลที่ผู้ให้บริการแต่ละรายเก็บไว้ว่ามีระบบจัดการที่เป็นไปตามมาตรฐานจริงหรือไม่ มีหน่วยงานใดยืนยัน หรือคอยตรวจสอบให้เป็นไปตามมาตรฐานนั้นอยู่เสมอ ดังนั้นหากเกิดการกระทำความผิดที่มิได้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ก็เป็นกรณีที่มาเรียกค่าปรับ

---

[45] วิเชาวน์ รักพงษ์ไพโรจน์, **ความสัมฤทธิผล ความคุ้มค่าในทางเศรษฐกิจ และทางเลือกอื่นของการเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,** (กรุงเทพฯ: สำนักงานศาลยุติธรรม, 2554).

หรือมีคำสั่งในภายหลัง ซึ่งเทียบไม่ได้กับข้อมูลจราจรทางคอมพิวเตอร์ไม่ได้เก็บไว้อันอาจส่งผลต่อการสืบสวนให้ไม่สามารถดำเนินการต่อไปได้

2.4.4 ผู้มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ได้ให้นิยามผู้ให้บริการไว้ ในมาตรา 3 ดังนี้

“ผู้ให้บริการ” หมายความว่า

1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

กระทรวงเทคโนโลยีและสารสนเทศ ได้ประกาศเรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 กำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยอาศัยอำนาจตามความในมาตรา 26 วรรค 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550” โดยแบ่งประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เป็น 2 ประเภทใหญ่ เช่นเดียวกับนิยามในพระราชบัญญัติฯ โดยสามารถรสรูปประเภทของผู้ให้บริการได้ดังนี้

(2.1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ซึ่งสามารถจำแนกย่อยได้ 4 ประเภท

(2.1.1) ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) อันได้แก่ ผู้ให้บริการโทรศัพท์พื้นฐาน ผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการวงจรเช่า เช่น ผู้ให้บริการ ADSL หรือ Fiber optic ผู้ให้บริการ ATM รวมทั้งผู้ให้บริการดาวเทียม

(21.2) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการ อันได้แก่ ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สายผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด อีกทั้งผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัทหรือ สถาบันการศึกษา

(2.1.3) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) อันได้แก่ ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting) หรือ

ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ และผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต

(2.1.4) ผู้ให้บริการร้านอินเทอร์เน็ต อันได้แก่ ผู้ให้บริการร้านอินเทอร์เน็ต และ ผู้ให้บริการร้านเกมออนไลน์

(2.2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น คือ ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content and Application Service Provider) อันได้แก่ ผู้ให้บริการเว็บบอร์ด (Web Board) หรือผู้ให้บริการบล็อก (Blog) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ รวมไปถึงผู้ให้บริการเว็บเซอร์วิส และ ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ หรือ ธุรกรรมทางอิเล็กทรอนิกส์

จากคำนิยามดังกล่าว เห็นได้ว่าผู้ให้บริการ มีตั้งแต่ผู้ให้บริการรายใหญ่ ไปจนถึงผู้ให้บริการรายใหญ่เช่น ผู้ให้บริการโทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต ไปจนถึงผู้ให้บริการรายย่อย เช่น ร้านอินเทอร์เน็ตคาเฟ่ หรือ เว็บบอร์ด โดยกฎหมายกำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์สำหรับผู้ให้บริการทุกราย ซึ่งการกำหนดหน้าที่ดังกล่าว เป็นการสร้างภาระใหม่ให้แก่ผู้ให้บริการ ในการสร้างระบบเพื่อให้สามารถจัดเก็บข้อมูลได้ รวบถึงการหากพื้นที่ในการรองรับข้อมูลที่จะต้องจัดเก็บ ซึ่งเกิดขึ้นมากมายในแต่ละวัน

ทั้งนี้ ผู้เขียนมีข้อสังเกตว่า ผู้ให้บริการ เป็นผู้ที่มีความเกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ในรูปแบบที่เป็นสาธารณะ ซึ่งผู้กระทำความผิดอาจเป็นใครก็ได้ที่ใช้บริการของผู้ให้บริการดังกล่าวมาเป็นสื่อในการกระทำความผิดต่อบุคคลอื่น แต่สำหรับผู้ให้บริการระบบอินทราเน็ตหรือระบบการเชื่อมต่อคอมพิวเตอร์ซึ่งใช้ภายในองค์กรเท่านั้นไม่เป็นผู้ให้บริการที่มีหน้าที่ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายนี้ เนื่องด้วยเจตนารมณ์ของกฎหมายไม่ได้ต้องการบังคับดูแลระบบอินทราเน็ตให้มีหน้าที่ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์[46] เห็นได้จากลักษณะของการติดต่อสื่อสารในรูปแบบอินทราเน็ต (Intranet) เป็นเครือข่ายเช่นเดียวกันกับเครือข่ายอินเทอร์เน็ต แต่ใช้ในการติดต่อสื่อสารหรือดำเนินธุรกรรมบนเครือข่ายภายในองค์กร[47] ดังนั้นแม้จะมีการติดต่อสื่อสารระหว่างระบบคอมพิวเตอร์ แต่เป็นระบบคอมพิวเตอร์ภายในเท่านั้นมิได้มีการติดต่อสื่อสารไปยังนอกองค์กรอันไม่ส่งผลกระทบต่อบุคคลอื่น ดังนั้นในการเชื่อมต่ออินทราเน็ตภายในองค์กรหากเกิดปัญหา ก็เป็นปัญหาภายในของตัวองค์กรหรือนิติบุคคลนั้นเอง ไม่กระทบต่อบุคคลอื่น กฎหมายจึงมิได้เข้าไปควบคุมหรือให้มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในส่วนนี้

---

[46] มานิตย์ จุมปา, **คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์**, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: วิญญูชน, 2554), 55.

[47] โอภาส เอี่ยมสิริวงศ์, **วิทยาการคอมพิวเตอร์และเทคโนโลยี (ฉบับปรับปรุง)**, 318.

2.4.5 ภาระหน้าที่ของผู้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์หรือผู้ให้บริการ

เมื่อกฎหมายกำหนดให้หน้าที่ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์เป็นของผู้ให้บริการจึงก่อให้เกิดภาระต่อผู้ให้บริการเพราะการจัดเก็บข้อมูลจราจรนั้นมีปริมาณข้อมูลจำนวนมาก โดยมีวิธีการจัดเก็บที่มีความมั่นคงปลอดภัยตามกฎหมาย ในการจะกระทำการดังกล่าวได้ผู้ให้บริการต้องการมีลงทุนสำหรับส่วนนี้เพิ่มเติมจากการลงทุนทั่วไปที่ได้มีการวางแผนหรืองบประมาณไว้ ซึ่งหากการออกกฎหมายเป็นการกระทบต่อเอกชนจนไม่สามารถประกอบธุรกิจได้ก็จะส่งผลกระทบต่อการผู้ใช้บริการในวงกว้างต่อไป อีกทั้งหากสร้างภาระมากเกินอาจทำให้เกิดการหลีกเลี่ยงและไม่ปฏิบัติตามกฎหมายได้ ในประเด็นนี้จึงต้องศึกษาถึงขั้นตอนการยกร่างหรือการพิจารณากฎหมายดังกล่าวว่ามีหลักการไว้ว่าอย่างไร

ก. ค่าใช้จ่ายในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตามมาตรา 26 ได้กำหนดให้ผู้ให้บริการต้องมีการเก็บข้อมูลจราจรทางคอมพิวเตอร์ เป็นระยะเวลาอย่างน้อย 90 วัน ซึ่งการเก็บข้อมูลดังกล่าวย่อมทำให้เกิดภาระในการเก็บข้อมูลจราจรทางคอมพิวเตอร์แก่ผู้ให้บริการเป็นจำนวนมหาศาล โดยผู้ให้บริการประเภทที่มีผู้ใช้บริการในวงกว้างก็จะมีภาระค่าใช้จ่ายสูง และผู้ให้บริการประเภทที่มีผู้ใช้บริการในวงแคบกว่าก็จะมีค่าใช้จ่ายลดลงมาตามลำดับ

จากการศึกษาและพิจารณารายงานการประชุมของคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ..... สภานิติบัญญัติแห่งชาติ นั้น พบว่าในขั้นตอนการพิจารณาร่างพระราชบัญญัตินี้ได้มีการกล่าวถึง งบประมาณที่ต้องใช้ในการจัดหาและจัดการเก็บข้อมูลดังกล่าวด้วยเนื่องจากการเจ็บข้อมูลก็ต้องมีทั้ง Software และ Hardware ซึ่งต้องมีการลงทุนเพิ่มเติมเพราะค่าใช่จ่ายในการลงทุนเก็บข้อมูลเท่าที่ประมาณการไว้ก็หลักหลายล้านบาท และการลงทุนดังกล่าวจะมีจำนวนมหาศาลเพียงใดเมื่อเทียบกับผลประโยชน์ที่จะได้รับจากการเก็บข้อมูลนั้นไว้[48] ภาระของผู้ให้บริการ คือการให้มีการเก็บข้อมูลจำนวนมหาศาลที่เกิดขึ้นทุกวินาที เพราะทุกครั้งที่มีการสื่อสารของระบบคอมพิวเตอร์จะเกิดข้อมูลข้อมูลจราจรทางคอมพิวเตอร์ และผู้ให้บริการก็มีหน้าที่จะต้องเก็บและเสียค่าใช้จ่ายในการเก็บข้อมูลและระบบการจัดเก็บข้อมูลเพื่อให้สามารถมีข้อมูลตามที่กฎหมายกำหนดไว้ได้ จำเป็นต้องใช้ค่าใช้จ่ายจำนวนมาก อันทำให้เกิดต้นทุนที่สูงขึ้น ทั้งนี้ ภาระจะมีมากหรือน้อยนั้นส่วนสำคัญขึ้นอยู่กับระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว หากกฎหมายกำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์มากขึ้นเท่าใด ภาระก็จะเพิ่มขึ้นมากขึ้นเท่านั้น การกำหนดระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์จึงต้องคำนึงถึงความคุ้มค่าทาง

---

[48] มรกต กุลธรรมโยธิน, **รายงานการประชุม คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ....สภานิติบัญญัติแห่งชาติ ครั้งที่ 2**, 29 พฤศจิกายน 2549.

เศรษฐกิจในการจัดเก็บและการนำไปใช้ซึ่งข้อมูลดังกล่าวด้วย เพราะภาระหน้าที่ดังกล่าวย่อมกระทบไปถึงสังคมโดยส่วนรวมต่อไป

ข. ระยะเวลาในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

การกำหนดให้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นเวลา 90 วัน ก่อให้เกิดภาระที่เพิ่มขึ้นอย่างมากต่อผู้ให้บริการ ทั้งผู้ที่ไม่ได้เคยเก็บข้อมูลดังกล่าวไว้ และผู้ที่เก็บข้อมูลไว้แต่ไม่เก็บนานถึง 90 วัน ซึ่งประเด็นนี้ได้มีการถกกันในที่ประชุมคณะกรรมาธิการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ว่าระยะเวลาใดเป็นระยะเวลาที่เหมาะสมว่าควรจะเก็บไว้ ซึ่งมีการเสนอทั้ง 30 วัน 90 วัน[49] โดยพิจารณาจากเหตุและผลที่ว่าเหมาะสมและเป็นธรรมต่อสังคมทั้งหมดแล้วหรือไม่ เป็นภาระหน้าที่แก่ผู้ให้บริการมากเกินไปหรือไม่ โดยแบ่งเป็นประเด็นที่ควรพิจารณาได้ดังนี้

ก) ความเหมาะสมของระยะเวลาในการเก็บข้อมูลจราจร

ข) ภาระที่ผู้ให้บริการต้องแบกรับในการเก็บข้อมูลจราจรทางคอมพิวเตอร์

ซึ่งในที่ประชุมคณะกรรมาธิการร่างฯ ได้มีการเปิดสัมมนาเพื่อรับฟังความเห็นจากประชาชนและมีการเชิญตัวแทนผู้ประกอบการที่มีสถานะเป็นผู้ให้บริการประเภทต่าง ๆ เข้ามาแจ้งข้อมูล ให้คณะกรรมาธิการได้ทราบเพื่อประกอบการพิจารณา โดยในเบื้องต้น ร่างกฎหมายได้กำหนดระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ที่ 30 วัน ซึ่งมีการถกเถียงกันแล้วเห็นว่าระยะเวลาดังกล่าวหากมีการเก็บไว้ก็คงนำไปใช้ประโยชน์ได้ยากไม่ได้ไปตามวัตถุประสงค์ที่กฎหมายต้องการ เพราะว่าเมื่อมีการกระทำผิดระยะเวลากว่าจะรู้ว่ามีการกระทำความผิดเกิดขึ้น หรือกว่าจะรวบรวมข้อมูลเพื่อขอข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ ก็จะเกินระยะเวลา 30 วันดังกล่าวแล้ว ทั้งนี้คณะกรรมการได้มีการแจ้งข้อมูลเกี่ยวกับสถิติเฉลี่ยการดำเนินคดีเพื่อหาตัวผู้กระทำความผิด อัตราเฉลี่ยที่จะพบการกระทำความผิดและเริ่มสอบสวนได้ว่าจะนำหลักฐานจากที่ใดบ้าง จะใช้เวลาประมาณ 90 วัน ดังนั้นเพื่อให้ได้ผลสามารถนำข้อมูลดังกล่าวมาใช้ประโยชน์ทางกฎหมายได้ จึงต้องกำหนดให้มีการจัดเก็บอย่างน้อย 90 วัน สำหรับบางประเทศมีการกำหนดให้จัดเก็บข้อมูลเป็นเวลา 1 ปี หรือ 2 ปี[50] เพื่อสามารถนำข้อมูลมาใช้ได้ในระยะเวลายาวพอสมควร

กฎหมายกำหนดภาระหน้าที่ของผู้ให้บริการดังกล่าวโดยมีการพิจารณาถึงความเหมาะสมของการบังคับใช้และผลดีผลเสียจากการคำนวณและความเห็นของผู้ที่เกี่ยวข้องแล้วจึงกำหนดภาระหน้าที่ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ขึ้นตามมาตรา 26 โดยให้ทุกฝ่ายสามารถร่วมมือกันในการ

---

[49] อัครวัฒน์ เทพหัสดิน ณ อยุธยา, **รายงานการประชุม คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ....สภานิติบัญญัติแห่งชาติครั้งที่ 15**, 8 มีนาคม 2550.

[50] สุรางคณา วายุภาพ, **รายงานการประชุม คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... สภานิติบัญญัติแห่งชาติครั้งที่ 15**, 8 มีนาคม 2550.

จัดเก็บข้อมูลและนำข้อมูลไปใช้ได้อย่างมีประสิทธิภาพตามเจตนารมณ์ของกฎหมายที่จะนำตัวผู้กระทำความผิดมาลงโทษ เนื่องจากข้อมูลจราจรที่เก็บไว้ดังกล่าวจะสามารถนำไปขยายผลนำตัวผู้กระทำความผิดมาลงโทษได้ต่อไป

อย่างไรก็ตาม โดยมีอัตราผู้ใช้คอมพิวเตอร์มากยิ่งขึ้นเพิ่มเป็นสองเท่า ทุก ๆ สามปี ดังนั้น การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ย่อมมีมากขึ้นด้วยตามลำดับ ในขณะที่ความผิดเพิ่มมากขึ้น แต่กฎหมายเกี่ยวกับคอมพิวเตอร์กลับไม่ได้มีการเปลี่ยนแปลง หรือมีโครงการศึกษาเพิ่มเติมเกี่ยวกับภาระหน้าที่ในการจัดเก็บและระยะเวลาในการจัดเก็บว่ามีความเหมาะสมในการนำข้อมูลจราจรทางคอมพิวเตอร์มาใช้หรือไม่ รวมทั้ง การสืบสวนสอบสวนที่นับวัน ผู้ร้ายจะยิ่งเก่งระบบคอมพิวเตอร์มากยิ่งขึ้น ทำให้การจะตรวจสอบว่ามีการกระทำความผิดเกิดขึ้นจะต้องใช้เวลานานมากยิ่งขึ้น ซึ่งเมื่อก่อนอาจมีการใช้ระยะเวลาเฉลี่ยในการสืบสวนหรือพบการกระทำความผิดเพียง 90 วัน แต่ปัจจุบันอาจต้องใช้เวลามากยิ่งขึ้น เพราะมีการกระทำความผิดที่แนบเนียนและซับซ้อนมากขึ้น การที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กำหนดให้เก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้เป็นระยะเวลา 90 วันโดยยังไม่มีการเปลี่ยนแปลงมาเป็นระยะเวลากว่า 5 ปี นี้ จะต้องมีการหาข้อมูลและวิเคราะห์ต่อไปว่าระยะเวลาดังกล่าวเหมาะสมกับการบังคับใช้ในปัจจุบันหรือไม่ สามารถนำข้อมูลจราจรทางคอมพิวเตอร์มาเป็นพยานหลักฐานในการนำตัวผู้กระทำความผิดมาลงโทษ แต่ทั้งนี้นอกจากจะคำนึงถึงระยะเวลาที่จะนำข้อมูลดังกล่าวมาเป็นพยานหลักฐานแล้ว จะต้องคำนึงถึง ภาระของผู้ให้บริการที่จะต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วย

2.4.6 สรุปเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

กฎหมายที่ระบุเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้นั้น เป็นเพียงแนวทางในการจัดเก็บเพื่อระบุตัวผู้กระทำความผิดและวันเวลาที่กระทำความผิด โดยต้องมีมาตรการที่รักษาความสมบูรณ์ของข้อมูลตามสมควรซึ่งขึ้นอยู่กับประเภทและขนาดขององค์กรรวมถึงงบประมาณแต่ละกรณี ๆ ไป แต่ไม่ได้หมายความว่าผู้ใช้บริการทุกรายต้องจัดเก็บในมาตรฐานแบบเดียวกันทั้งหมดตามที่ระบุไว้ในประกาศกระทรวงไอซีที[51] จะเห็นได้จากประกาศดังกล่าวผู้ให้บริการแต่ละประเภทมีข้อมูลที่ต้องจัดเก็บแตกต่างกัน อนึ่ง ผู้ให้บริการทุกรายยังคงมีหน้าที่ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยใช้วิธีการที่มั่นคงปลอดภัยตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการ พ.ศ. 2550 ข้อ 8 ซึ่งได้มีกำหนด 5 ประการตามที่ได้กล่าวมาแล้วนั้น

[51] ไพบูลย์ อมรภิญโญเกียรติ, **คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550,** 100.

บทที่ 3
แนวทางมาตรฐานและกฎหมายต่างประเทศเกี่ยวกับการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

ข้อมูลจราจรทางคอมพิวเตอร์ที่นำมาใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตจะมีความน่าเชื่อถือหรือไม่ ข้อมูลดังกล่าวถูกเปลี่ยนแปลงระหว่างกระบวนการประมวลผลข้อมูลหรือไม่ หรือจัดเก็บไว้อย่างถูกต้องไม่มีความคลาดเคลื่อนหรือไม่ สิ่งเหล่านี้ขึ้นอยู่กับกระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยกระบวนการจัดเก็บที่ดีสามารถพิจารณาได้จากมาตรฐานการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งในระดับสากล มาตรฐานการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์มีกระบวนการในการตรวจสอบย้อนกลับเพื่อให้แน่ใจว่าการจัดเก็บมีความถูกต้องแท้จริงและไม่มีการเปลี่ยนแปลงซึ่งข้อมูล และทำให้มั่นใจได้ว่าข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวสามารถนำไปใช้เป็นพยานหลักฐานได้ โดยในบทนี้จะได้กล่าวถึงมาตรฐานการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เป็นที่ยอมรับและใช้ในระดับสากล รวมถึงกระบวนการจัดเก็บและการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ของสหรัฐอเมริกาและสหภาพยุโรป เพื่อเปรียบเทียบให้เห็นถึงข้อดีและข้อเสียของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในแต่ละรูปแบบ

3.1 มาตรฐานการจัดเก็บข้อมูลสารสนเทศแบบ COBIT

COBIT เป็นแนวทางสำหรับการกำกับดูแลและการบริหารการจัดการองค์กรทางด้านไอที่สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (Information Systems Audit and Control Association: ISACA) ได้พัฒนาคิดค้นขึ้น เพื่อเป็นระบบรวบรวมความรู้หรือข้อมูลต่าง ๆ ที่องค์กรต้องการสำหรับการนำไปปรับใช้เพื่อให้องค์กรมีการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ดี และเพื่อพัฒนาองค์กรให้เข้าสู่การเป็นองค์กรที่มี “ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ” หรือ IT Governance กล่าวคือ สามารถบริหารจัดการระบบสารสนเทศขององค์กรให้สามารถใช้งานได้อย่างมีประสิทธิภาพ มีความคุ้มค่ากับการลงทุน และมีการบริหารจัดการที่โปร่งใสสามารถตรวจสอบได้ โดยโคบิตจะรวบรวมตัววัด (Measures) เครื่องบ่งชี้ (Indicators) ขั้นตอนการปฏิบัติงาน (Processes) และแนวทางการปฏิบัติที่ดีที่สุด (Best Practices) ซึ่งเป็นข้อมูลที่มีโครงสร้าง สามารถเข้าใจและนำไปใช้ได้โดยง่ายอีกทั้งเป็นที่ยอมรับกันโดยทั่วไป โดยมีการนำไปประยุกต์ใช้โดยองค์มากมาย รวมทั้งจากลุ่มธุรกิจ กลุ่มไอที กลุ่มบริหารความเสี่ยง กลุ่มผู้รักษาความมั่นคงปลอดภัย เป็นต้น สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA International) หรือเรียกกันทั่วไปว่า “ISACA” ได้พัฒนากรอบวิธีปฏิบัติ COBIT (COBIT Framework) จากประสบการณ์ใช้งานจริงมากกว่า 15 ปี มาตั้งแต่ปี 1996 จากเวอร์ชั่น 1- 2- 3 - 4/4.1 และในปัจจุบัน COBIT ได้พัฒนาให้อยู่

ในเวอร์ชั่น 5 ซึ่งได้เริ่มประกาศให้ใช้อย่างเป็นทางการในปี 2012[1] โดย COBIT 5 ตั้งอยู่บนพื้นฐานของหลักการสำคัญ 5 ประการ ในการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร ดังนี้

หลักการที่ 1 ตอบสนองความต้องการของผู้มีส่วนได้เสีย

องค์กรตั้งอยู่เพื่อที่สร้างคุณค่าสำหรับผู้มีส่วนได้เสีย โดยการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด COBIT 5 ให้กระบวนการที่จำเป็นทั้งหมดและปัจจัยเอื้ออื่น ๆ ที่ใช้สนับสนุนการสร้างคุณค่าแก่ธุรกิจจากการใช้ไอที เพราะว่าทุกองค์กรมีวัตถุประสงค์ที่แตกต่างกัน องค์กรสามารถปรับแต่ง COBIT 5 ให้เหมาะกันบริบทของตนผ่านทางการส่งทอดเป้าหมาย (Goal Cascade) การแปลงเป้าหมายองค์กรในภาพรวมไปสู่เป้าหมายในระดับที่สามารถบริหารจัดการได้ มีความเฉพาะเจาะจง มีความเกี่ยวข้องกับไอที และการเชื่อมโยงหรือเปรียบเทียบเป้าหมายนี้กับกระบวนการหรือแนวปฏิบัติหนึ่ง ๆ

หลักการที่ 2 ครอบคลุมทั่งทั้งองค์กรอย่างครบวงจร

COBIT 5 บูรณาการการกำกับดูแลไอทีระดับองค์กรเข้าไปในการกำกับดูแลองค์กร:

ครอบคลุมทุกหน้าที่งานและกระบวนการภายในองค์กร COBIT 5 ไม่เน้นเพียงแค่ “หน้าที่งานด้านไอที” เท่านั้น แต่จะถือว่าสารสนเทศและเทคโนโลยีที่เกี่ยวข้องเป็นสินทรัพย์ที่ทุกคนในองค์กรจำเป็นต้องดูแลเช่นเดียวกับสินทรัพย์อื่น ๆ

พิจารณาการกำกับดูแลและการบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับไอทีทั้งหมด เพื่อให้ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร ได้แก่การรวมทุกคนและทุกสิ่ง ทั้งภายในและภายในนอกที่เกี่ยวข้องกับการกำกับดูแลและการบริหารจัดการสารสนเทศและไอทีที่เกี่ยวข้อง

หลักการที่ 3 ประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว

มีมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับไอทีจำนวนมาก ซึ่งแต่ละอย่างก็ให้แนวทางเกี่ยวกับกิจกรรมของไอทีในด้านใดอ้านหนึ่ง COBIT 5 ได้นำมาครฐานและกรอบการดำเนินงานที่เกี่ยวข้องอื่น ๆ มาจัดให้สอดคล้องกันในภาพรวม จึงสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่น ๆ สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

หลักการที่ 4 เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล

การกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรที่มีประสิทธิภาพและประสิทธิผลต้องใช้วิธีปฏิบัติแบบองค์รวมที่ได้พิจารณาถึงองค์ประกอบหลาย ๆ อย่าง ซึ่งมีปฏิสัมพันธ์ต่อกัน COBIT 5 ระบุถึงกลุ่มของปัจจัยเอื้อที่ใช้สนับสนุนการนำระบบการกำกับดูแลและการบริหารจัดการไอทีระดับ

---

[1] สันติพัฒน์ อรุณธารี, **การพัฒนากลยุทธ์ทางธุรกิจไปสู่กลยุทธ์ทางด้านไอทีด้วยโคบิต 5** [Online], 1 พฤษภาคม 2557. แหล่งที่มา http://pumpkrub.blogspot.com/2013/02/5.html.

องค์กรไปใช้งานอย่างครอบคลุม ปัจจัยเอื้อนิยามได้อย่างกว้าง ๆ ว่าเป็นสิ่งที่สามารถช่วยในการบรรลุวัตถุประสงค์ขององค์กร กรอบการดำเนินกงานของ COBIT 5 ระบุถึงปัจจัยเอื้อ 7 ประเภทดังนี้

(1) หลักการ นโยบาย และกรอบการดำเนินงาน

(2) กระบวนการ

(3) โครงสร้างการจัดการองค์กร

(4) วัฒนธรรม จริยธรรม และพฤติกรรม

(5) สารสนเทศ

(6) บริการ โครงสร้างพื้นฐาน และระบบงาน

(7) บุคลากร ทักษะ และศักยภาพ

หลักการที่ 5 แบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ

กรอบการดำเนินงานของ COBIT 5 ระบุความแตกต่างอย่างชัดเจนระหว่างการกำกับดูแลและการบริหารจัดการ หลักสองประการนี้ครอบคุลมถึงกิจกรรมที่ต่างกันต้องการโครงสร้างการจัดองค์กรที่แตกต่างกัน และใช้เพื่อจุดประสงค์ที่แตกต่างกัน ในมุมมองของ COBIT 5 ความแตกต่างหลัก ๆ ที่เดินชัดระหว่างการกำกับดูแลและการบริหารจัดการคือ

(1) การกำกับดูแล ทำให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสียได้รับการประเมินเพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้บรรลุซึ่งมีความสมดุลและเห็นขอบร่วมกัน การกำหนดทิศทางผ่านการจัดลำดับความสำคัญและการตัดสินใจ และการเฝ้าติดตามผลการดำเนินงานและการปฏิบัติตามเทียบกับทิศทางและวัตถุประสงค์ที่ได้ตกลงร่วมกันในองค์กรส่วนใหญ่ คณะกรรมการบริหารเป็นผู้รับผิดชอบการกำกับดูแลโดยรวมภายใต้การชี้นำของประธานกรรมการ ในองค์กรขนาดใหญ่และมีความซับซ้อน หน้าที่บางประการสำหรับการกำกับดูแลอาจมอบหมายให้กับหน่วยงานที่จัดตั้งขึ้นเป็นพิเศษในระดับที่เหมาะสม

(2) การบริหารจัดการ ผู้บริหารวางแผน สร้าง ดำเนินงาน และเฝ้าติดตามกิจกรรมต่าง ๆ ให้สอดคล้องกับทิศทางที่กำหนด โดยหน่วยงานกำกับดูแล (Governance Body) เพื่อบรรลุวัตถุประสงค์ขององค์กร โดยในองค์กรส่วนใหญ่ การบริหารจัดการรับผิดชอบโดยผู้บริหารระดับสูงภายใต้การชี้นำของประธานเจ้าหน้าที่บริหาร (CEO)

เมื่อนำหลักการทั้ง 5 ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล ซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด เพื่อยังประโยชน์ให้ผู้มีส่วนได้เสีย ทั้งนี้ บางองค์กรสามารนำมาตรฐาน หรือ แนวทางปฏิบัติอื่น ๆ ที่มีจุดมุ่งหมายที่ต้องการจะเน้นที่การควบคุมเฉพาะจุดใดจุดหนึ่ง มาประยุกต์ใช้ร่วมกับโคบิตได้ เช่น กลุ่มมาตรฐานของ ISO/IEC 27000 (ISO/IEC 27000 Series), ISO/IEC 27001, ISO/IEC 27002 ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการรักษาความ

ปลอดภัยของเทคโนโลยีสารสนเทศ หรือ มาตรฐาน ISO/IEC 9001: 2000 ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการจัดการความต้องการทางด้านคุณภาพของระบบ (Quality Management Systems Requirement) หรือ มาตรฐานของ Information Technology Infrastructure Library (ITIL) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการให้บริการด้านเทคโนโลยีสารสนเทศที่มีคุณภาพ หรือ มาตรฐาน Capability Maturity Model Integration (CMMI) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการพัฒนาและผลิตซอร์ฟแวร์ที่มีคุณภาพ รวมไปถึงมาตรฐาน Projects in Controlled Environments 2 (PRINCE2) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการบริหารจัดการโครงการที่มีประสิทธิภาพ เป็นต้น เนื่องจากโคบิตเป็นกรอบการปฏิบัติที่บอกให้ผู้ปฏิบัติทราบว่าต้องการอะไรบ้าง (What to do) แต่ไม่มีรายละเอียดในแง่ของวิธีการปฏิบัติที่จะนำไปสู่จุดนั้น (How to do) ดังนั้นผู้ปฏิบัติจึงควรนำมาตรฐาน หรือแนวทางปฏิบัติอื่น ๆ เข้ามาช่วยเสริมในส่วนของรายละเอียดที่เจาะลึกลงไปในเรื่องที่ต้องการได้

3.2 มาตรฐานการจัดเก็บข้อมูล ISO 27001: 2013

ISO (International Organization for Standardization) หรือเรียกว่า องค์การระหว่างประเทศว่าด้วยการมาตรฐาน เป็นผู้พัฒนาที่ใหญ่ที่สุดของโลกของมาตรฐานสากลแบบสมัครใจ ซึ่งมาตรฐานสากลกำหนดลักษณะเฉพาะสำหรับสินค้า บริการ และการปฏิบัติที่ดี เพื่อช่วยให้อุตสาหกรรมมีประสิทธิภาพมากขึ้นและมีคุณภาพ การพัฒนาผ่านฉันทามติระดับโลกที่จะช่วยในการทำลายอุปสรรคในการค้าระหว่างประเทศลง[2]

โดยองค์การนี้ได้ถูกก่อตั้งขึ้นตั้งแต่ ค.ศ. 1947 และได้สร้างมาตรฐานต่าง ๆ มาแล้วกว่า 19500 มาตรฐานที่ครอบคลุมทั้งเรื่อง เทคโนโลยีและธุรกิจ ตั้งแต่ความปลอดภัยด้านอาหารไปจนถึงด้านคอมพิวเตอร์ รวมทั้งด้านเกตรกรรม และสุขภาพ

มาตรฐาน (Standard)[3]

หมายถึง เอกสารที่จัดทำขึ้นจากการเห็นพ้องต้องกัน และได้รับ ความเห็นชอบจากองค์กรอันเป็นที่ยอมรับกันทั่วไป เอกสารดังกล่าววางกฎระเบียบแนวทางปฏิบัติหรือลักษณะเฉพาะแห่งกิจกรรม

---

[2] International Organization for Standardization, **About ISO** [Online], 5 May 2014a. Available from http://www.iso.org/iso/home/about.htm.

[3] International Organization for Standardization, **Standards** [Online]**,** 5 May 2014b. Available from http://www.iso.org/iso/home/about.htm.

หรือผลที่เกิดขึ้นของกิจกรรมนั้น ๆ เพื่อให้เป็นหลักเกณฑ์ใช้กันทั่วไปจนเป็นปกติวิสัย โดยมุ่งให้บรรลุถึงความสำเร็จสูงสุดตามข้อกำหนดที่วางไว้

องค์กรระหว่างประเทศว่าด้วยมาตรฐานได้กำหนดมาตรฐานการจัดเก็บข้อมูล ไว้ใน ISO/IEC 27001:2013 โดยมีรายละเอียดเกี่ยวกับ ระบบบริหารจัดการความมั่นคงสาระสนเทศ (ISMS หรือ Information Security Management System) จำนวน 7 ข้อ และ มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสาระสนเทศ (Control Objective and Control) จำนวน 14 ข้อดังนี้

3.2.1 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS หรือ Information Security Management System)

ข้อกำหนดหลักที่ต้องปฏิบัติตามในการขอการรับรองตามมาตรฐาน ISO/IEC 27001: 2013

ข้อ 1 บริบทขององค์กร (Context of the Organization)

1.1) การทำความเข้าใจองค์กรและบริบทขององค์กร (Understanding the Organization and Its Context)

1.2) การกำหนดความจำเป็นและความคาดหวังของผู้ที่เกี่ยวข้อง (Understanding the Needs and Expectations of Interested Parties)

1.3) การกำหนดขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Determining the Scope of the Information Security Management System)

1.4) ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System)

ข้อ 2 ภาวะผู้นำ (Leadership)

2.1) ภาวะผู้นำและการให้ความสำคัญ (Leadership and Commitment)

2.2) นโยบาย (Policy)

2.3) บทบาทหน้าที่ความรับผิดชอบและอำนาจหน้าที่ (Organizational Roles, Responsibilities and Authorities)

ข้อ 3 การวางแผน (Planning)

3.1) การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Actions to Address Risks and Opportunities) เปรียบเทียบมาตรการที่กำหนดไว้กับมาตรการใน Annex A และตรวจสอบว่าไม่มีมาตรการข้อใดที่ละเลยไป

3.2) วัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศและแผนการบรรลุวัตถุประสงค์ (Information Security Objectives and Plans to Achieve Them)

ข้อ 4 การสนับสนุน (Support)

4.1) ทรัพยากร (Resources)

4.2) สมรรถนะ (Competence)

4.3) การสร้างความตระหนัก (Awareness)

4.4) การสื่อสารให้ทราบ (Communication)

4.5) สารสนเทศที่เป็นลายลักษณ์อักษร (Documented Information)

ข้อ 5 การดำเนินการ (Operation)

5.1) การวางแผนที่เกี่ยวข้องกับการดำเนินการและการควบคุม (Operational Planning and Control)

5.2) การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessment)

5.3) การจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Treatment)

ข้อ 6 การประเมินประสิทธิภาพและประสิทธิผล (Performance evaluation)

6.1) การเฝ้าระวังการวัดผลการวิเคราะห์และการประเมิน (Monitoring, Measurement, Analysis and Evaluation)

6.2) การตรวจประเมินภายใน (Internal Audit)

6.3) การทบทวนของผู้บริหาร (Management Review)

ข้อ 7 การปรับปรุง (Improvement)

7.1) ความไม่สอดคล้องและการดำเนินการแก้ไข (Nonconformity and Corrective Action)

7.2) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

3.2.2 มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ (Control Objectives and Controls)

1) นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1.1) ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security) วัตถุประสงค์เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

2) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

2.1) โครงสร้างภายในองค์กร (Internal Organization)

วัตถุประสงค์เพื่อให้มีการกำหนดกรอบการบริหารจัดการโดยต้องมีการเริ่มต้นและควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

2.2) อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile Devices and Teleworking) วัตถุประสงค์เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

3) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security)

3.1) ก่อนการจ้างงาน (Prior to Employment) วัตถุประสงค์เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา

3.2) ระหว่างการจ้างงาน (During Employment) วัตถุประสงค์เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

3.3) การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and Change of Employment) วัตถุประสงค์เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

4) การบริหารจัดการทรัพย์สิน (Asset Management)

4.1) หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets) วัตถุประสงค์เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

4.2) การจัดชั้นความลับของสารสนเทศ (Information Classification) วัตถุประสงค์เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

4.3) การจัดการสื่อบันทึกข้อมูล (Media Handling) วัตถุประสงค์เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาตการเปลี่ยนแปลงการขนย้าย การลบหรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

5) การควบคุมการเข้าถึง (Access Control)

5.1) ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirements of Access Control) วัตถุประสงค์เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

5.2) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) วัตถุประสงค์เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

5.3) หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) วัตถุประสงค์ เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

5.4) การควบคุมการเข้าถึงระบบ (System and Application Access Control) วัตถุประสงค์เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

6) การเข้ารหัสข้อมูล (Cryptography)

6.1) มาตรการเข้ารหัสข้อมูล (Cryptographic Controls) วัตถุประสงค์เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลและป้องกันความลับการปลอมแปลงหรือความถูกต้องของสารสนเทศ

7) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

7.1) พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Areas) วัตถุประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตความเสียหายและการแทรกแซงการทำงานที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

7.2) อุปกรณ์ (Equipment) วัตถุประสงค์เพื่อป้องกันการสูญหายการเสียหายการขโมยหรือการเป็นอันตรายต่อทรัพย์สินและป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

8) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security)

8.1) ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities) วัตถุประสงค์เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

8.2) การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware) วัตถุประสงค์เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

8.3) การสำรองข้อมูล (Backup) วัตถุประสงค์เพื่อป้องกันการสูญหายของข้อมูล

8.4) การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring) วัตถุประสงค์เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

8.5) การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of operational Software) วัตถุประสงค์เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

8.6) การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management) วัตถุประสงค์เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

8.7) สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems AuditConsiderations) วัตถุประสงค์เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

9) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

9.1) การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management) วัตถุประสงค์เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

9.2) การถ่ายโอนสารสนเทศ (Information Transfer) วัตถุประสงค์เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

10) การจัดหาการพัฒนาและการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

10.1) ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security Requirements of Information Systems) วัตถุประสงค์เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

10.2) ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes) วัตถุประสงค์เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

10.3) ข้อมูลสำหรับการทดทดสอบ (Test Data) วัตถุประสงค์เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

11) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier Relationships)

11.1) ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship) วัตถุประสงค์เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

11.2) การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management) วัตถุประสงค์เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

12) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

12.1) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of Information Security Incidents and Improvements) วัตถุประสงค์เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

13) ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

13.1) ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Continuity) วัตถุประสงค์ เพื่อให้สามารถรักษาความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศคงอยู่กับระบบการจัดการที่ต่อเนื่องทางธุรกิจขององค์กร

13.2) การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies) วัตถุประสงค์เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

14) ความสอดคล้อง (Compliance)

14.1) ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements) วัตถุประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมายระเบียบข้อบังคับหรือสัญญาจ้างที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและที่เป็นความต้องการด้านความมั่นคงปลอดภัย

14.2) การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews) วัตถุประสงค์เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

3.3 National Security Agency (NSA): หน่วยงานความมั่นคงแห่งสหรัฐอเมริกา

3.3.1 เกี่ยวกับ NSA

NSA มีภารกิจหลักในการรักษาข้อมูลความลับของชาติเพื่อไม่ให้ชาวต่างชาติเข้ามารับทราบข้อมูลสำคัญระดับชาติได้ รวมไปถึงการดำเนินการจัดเก็บข้อมูลข่าวกรอง การประมวลผลข้อมูล และ

การคัดแยกข้อมูล ของชาวต่างชาติที่ได้จัดเก็บและคัดแยกไว้เพื่อพัฒนาความรู้ และเพื่อสนับสนุนปฏิบัติการทางทหาร นอกจากนั้นหน่วยงานนี้ยังมีหน้าที่สร้างเครือข่ายเพื่อเอาชนะผู้ก่อการร้ายทั้งองค์กรร้ายในและนอกประเทศ รวมถึงการคุ้มครองสิทธิและเสรีภาพของประชาชนตามกฎหมายสหรัฐอเมริกา

ตามคำสั่งของฝ่ายบริการที่ 12333 ซึ่งเผยแพร่เมื่อวันที่ 4 ธันวาคม ค.ศ. 1981 ได้กำหนดบทบาทและความรับผิดชอบของ NSA ให้มีหน้าที่จัดเก็บ (Collect) ประมวลผล (Process) วิเคราะห์ (Analyze) ผลิต (Produce) และ (Disseminate) สัญญาณข้อมูลข่าวกรองและข้อมูลข่าวกรองของต่างชาติ และ ป้องกันข้อมูลความลับ เพื่อวัตถุประสงค์ในการสนับสนุนประเทศชาติและภารกิจของหน่วยงานต่าง ๆ โดยการดำเนินการให้อยู่ภายใต้กฎหมายและข้อบังคับต่าง ๆ สำหรับหน่วยงาน และมีการวางกระบวนการดำเนินการสำหรับการประมวลผล การแปลงสัญญาณ และการส่งต่อซึ่งข้อมูลข่าวกรองที่ได้มาภายใต้การควบคุมบริหารอย่างเป็นระบบและปลอดภัย[4]

3.3.2 แนวทางการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของ NSA

หน่วยงาน NSA[5] ใช้เป็นหลักการในการจัดเก็บข้อมูลตาม มาตรา 702 ของกฎหมาย Foreign Intelligence Surveillance Act หรือ FISA ซึ่งวางแนวทางเกี่ยวกับการตรวจสอบและจัดเก็บข้อมูลข่าวกรองของชาวต่างชาติซึ่งไม่รวมถึงประชาชนของสหรัฐอเมริกาที่อาศัยอยู่นอกประเทศอเมริกา เพื่อสร้างกระบวนการและแนวทางการดำเนินการสำหรับการจัดเก็บข้อมูลการติดต่อสื่อสารของผู้ก่อการร้ายชาวต่างชาติ โดยมีรายละเอียดของ มาตรา 702 ดังนี้[6]

1) กระบวนการนี้จัดเก็บได้เฉพาะเป้าหมายที่เป็นข้อมูลข่าวกรองของชาวต่างชาติเกี่ยวกับติดต่อสื่อสารของชาวต่างชาตินั้นที่อยู่นอกประเทศสหรัฐอเมริกา

2) รัฐบาลไม่สามารถตั้งเป้าหมายแก่คนสัญชาติอเมริกาไม่ว่าจะอยู่แห่งใดของโลกก็ตามภายใต้กฎหมายนี้ แม้ว่าเป้าหมายดังกล่าวจะอยู่นอกประเทศหากวัตถุประสงค์เป็นไปเพื่อให้ได้ข้อมูลบางส่วนซึ่งเป็นข้อมูลของผู้ที่อาศัยในสหรัฐอเมริกา

---

[4] National Security Agency, **Mission** [Online], 7 May 2014. Available from http://www.nsa.gov/about/mission/index.shtml.

[5] Office of the Director of National Intelligence, **Section 702 of the Foreign Intelligence Surveillance Act** [Online], 10 May 2014. Available from http://icontherecord.tumblr.com/topics/section-702.

[6] Federation of American Scientists, **Section 702** [Online], 12 May 2014. Available from http://www.fas.org/irp/news/2013/06/nsa-sect702.pdf.

3) ภายใต้กฎหมายนี้จะมีการออก Certification หรือการรับรองการจัดเก็บข้อมูลประจำปีโดยศาลและได้รับการรับรองโดยหน่วยงานอัยการและหน่วยงานข่าวกรองของสหรัฐอเมริกาด้วย

4) การรับรองนี้จะเป็นการกำหนดความหมายประเภทของการกระทำของชาวต่างชาติที่เหมาะสมจะเป็นเป้าหมายในการจัดเก็บข้อมูล และโดยการกำหนดกระบวนการสำหรับเป้าหมายเฉพาะเจาะจง และกระบวนการปฏิบัติอย่างน้อยที่สุด ซึ่งจะถูกกำหนดโดยหน่วยงานอัยการร่วมกับหน่วยข่าวกรองและได้รับการอนุมัติโดยศาล

5) การจัดเก็บข้อมูลการติดต่อสื่อสารใด ๆ ที่เกี่ยวข้องกับประชาชนของสหรัฐอเมริกาจะต้องถูกทำลายหากไม่ได้เป็นการจัดเก็บตามวัตถุประสงค์ที่ให้อำนาจไว้หรือเป็นหลักฐานในคดีอาชญากรรม

6) เมื่อเป้าหมายที่ไม่ใช่ประชาชนสหรัฐและอยู่นอกประเทศสหรัฐอเมริกาได้เดินทางเข้ามาในประเทศหรือความจริงแล้วปรากฏในเวลาต่อมาว่าเป็นประชาชนสหรัฐอเมริกา จะต้องมีการยกเลิกการกำหนดเป้าหมายดังกล่าวทิ้ง

7) ข้อมูลใด ๆ ก็ตามที่ถูกจัดเก็บขึ้นหลังจากที่เป้าหมายต่างชาติได้เดินทางเข้าสหรัฐอเมริกาจะต้องได้รับการทำลายเว้นแต่จะเป็นข้อมูลที่มีลักษณะเฉพาะซึ่งได้รับการอนุมัติเป็นพิเศษจากศาลเฉพาะทางเกี่ยวกับการรวบรวมข้อมูลข่าวกรอง

จากหลักการดังกล่าวข้างต้นอาจสรุปแนวทางการกำหนดเป้าหมายและวิธีการจัดเก็บและรวบรวมข้อมูลตาม มาตรา 702[7] ดังนี้

1) การจำกัดเป้าหมายภายใต้กฎหมาย

รัฐบาลไม่สามารถกำหนดเป้าหมายใด ๆ ได้หากศาลไม่อนุญาตตามขั้นตอนของ มาตรา 702 ในการจัดเก็บข้อมูล โดยจะต้องมีความเหมาะสม ข้อมูลข่าวสาร เป็นข่าวกรอกของชาวต่างชาติ และวัตถุประสงค์เพื่อได้มาซึ่งข้อมูลซึ่งมีเป้าหมายเป็นชาวต่างชาติที่เชื่อได้ว่าอยู่นอกประเทศสหรัฐอเมริกา ทั้งนี้ มาตรา 702 ไม่สามารถนำมาใช้กับเป้าหมายใด ๆ กฎตามที่เป็นคนสัญชาติหรือเชื้อชาติอเมริกา หรือ เป้าหมายใด ๆ ก็ตามที่อาศัยอยู่ในสหรัฐอเมริกา อีกทั้ง ไม่สามารถนำไปใช้กับคนอเมริกาที่อยู่นอกประเทศได้หากวัตถุประสงค์เพื่อรวบรวมข้อมูลจากบุคลที่อาศัยอยู่ภายในสหรัฐอเมริกา

2) วิธีการจัดเก็บและรวบรวมข้อมูล

มาตรา 702 มีความเกี่ยวข้องในการเป็นส่วนช่วยการจัดเก็บข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์ของผู้ให้บริการและยังเป็นตัวผลักดันให้เกิดการตรวจสอบในตนเอง อย่างไรก็ตาม ภายใต้ มาตรา 702 รัฐบาลสหรัฐไม่สามารถได้ไปซึ่งข้อมูลจากเซอร์เวอร์ของผู้ให้บริการจัดเก็บข้อมูล

---

[7] Office of the Director of National Intelligence, **Section 702 of the Foreign Intelligence Surveillance Act**.

การติดต่อสื่อสารอิเล็กทรอนิกส์ของสหรัฐอเมริกา โดยข้อมูลดังกล่าวทั้งหมดจะต้องจัดเก็บไว้ได้ก็โดยการอนุมัติของศาลตามกฎหมาย ทั้งนี้แนวทางการจัดเก็บข้อมูลของผู้บริการจะเป็นไปตามแนวทางที่กำหนดโดยพนักงานอัยการและผู้อำนวยการของหน่วยข่าวกรองแห่งชาติ (The Director of National Intelligence) ทั้งนี้ การจัดเก็บ (Collection) จะไม่จำเป็นต้องได้รับการอนุมัติสำหรับเป้าหมายทุก ๆ ครั้ง โดยจะมีการวางแนวทางการอนุมัติประจำปีโดยหน่วยงานอัยการและหน่วยข่าวกรองแห่งชาติซึ่งจะกำหนดประเภทของข่าวกรองที่จะจัดเก็บไว้ภายใต้กระบวนการใด ๆ ต่อไป (Office of the Director of National Intelligence, n.d.)

อย่างไรก็ตามในกระบวนการรวบรวมข้อมูลของ NSA จะมีการจัดตั้งหน่วยงานภายในที่ดูและเกี่ยวกับกับจัดเก็บข้อมูลการติดต่อสื่อสารทั้งหมดที่เกิดขึ้นในต่างประเทศซึ่งอาจมีความเกี่ยวข้องกับการก่อการร้ายไว้ด้วยระบบปฏิบัติการทางอิเล็กทรอนิกส์ขั้นสูงขององค์กรโดยการจัดเก็บข้อมูลการติดต่อสื่อสารในทุกประเภทไว้ในการประมวลผลของคอมพิวเตอร์โดยไม่สามารถเข้าไปดูได้ และหากต้องการดูข้อมูลดังกล่าวจึงจะดำเนินการตามกระบวนการติดต่อข้อมูลใน มาตรา 702 ต่อไป เพื่อให้เกิดการจัดเก็บข้อมูลไว้ก่อนแล้วสามารถนำข้อมูลมาใช้ได้ แล้วจึงจัดก็บข้อมูลโดยละเอียดต่อไปสำหรับเป้าหมายที่จะต้องถูกติดตาม ทั้งนี้ การบันทึกข้อมูลอินเทอร์เน็ตจัดเก็บไว้อย่างน้อยกมากกว่าหนึ่งปีในฐานข้อมูลของ MARINA ซึ่งเป็นที่ใช้ในการวิเคราะห์ข้อมูล[8]

3.4 กฎหมายลิขสิทธิ์กับอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริกา

ภายใต้กฎหมายอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริกา Cyber Crime Law of United State of America ได้กำหนดให้กฎหมายลิขสิทธิ์เป็นความผิดทางอาชญากรรมคอมพิวเตอร์ด้วยในประมวลกฎหมายอาญาและวิธีพิจารณาความอาญาบทที่ 18 มาตรา 2319 Criminal Infringement of a Copyright หรือ บทที่ว่าด้วยอาชญากรรมจากการปลอมแปลงลิขสิทธิ์ ซึ่งจะทำให้การหาพยานหลักฐานเป็นไปตามกฎหมาย Cybercrime ของสหรัฐอเมริกา โดยกระบวนการให้การดำเนินการของกฎหมายอาชญากรรมทางคอมพิวเตอร์ได้แก่ อำนาจในการจัดเก็บและรวบรวมซึ่งข้อมูลอิเล็กทรอนิกส์จากบุคคลที่สามรวมถึงผู้ให้บริการอินเทอร์เน็ต และการเข้าถึงข้อมูลการติดต่อสื่อสารอิเล็กทรอนิกส์และการเข้าถึงการค้นหาหรือยึดพยานหลักฐานทางอิเล็กทรอนิกส์ได้[9]

---

[8] James Ball, “NSA stores metadata of millions of web users for up to a year, secret files show”, **Theguardian** (November 30, 2013). [Online], Available from http://www.theguardian .com/world/2013/sep/30/nsa-americans-metadata-year-documents.

[9] Computer Crime and Intellectual Property Section, U.S. Department of Justice, **Cyber Crime Law of United States,** (n.p.: N.P., 2006), 47.

โดยผู้มีอำนาจที่กฎหมายอาชญากรรมทางคอมพิวเตอร์ได้กำหนดไว้ในกฎหมาย Cybercrime of United States โดยภาพรวมดังนี้

ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 18 มาตรา 2510-2522 กำหนดเกี่ยวกับการดักรับซึ่งข้อมูลการติดต่อสื่อสารอิเล็กทรอนิกส์ หรือการติดต่อสื่อสารผ่านสายโทรศัพท์หรือปากเปล่า

ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 18 มาตรา 2701-2712 การจัดเก็บและการเปิดเผยข้อมูลที่จัดเก็บไว้ซึ่งข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์หรือผ่านสายสัญญาณ

3.5 การดักรับข้อมูลการติดต่อสื่อสารอิเล็กทรอนิกส์ หรือการติดต่อสื่อสารผ่นสายโทรศัพท์หรือปากเปล่าตามกฎหมายสหรัฐอเมริกา

ปรากฏใน ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญาของอเมริกาบทที่ 18

มาตรา 2516 อำนาจในการได้มาโดยการดักรับการติดต่อสื่อสารทางสายโทรศัพท์ทางปากเปล่าหรือทางอิเล็กทรอนิกส์

(1) อัยการสูงสุด รองอัยการสูงสุด รองอัยการสูงสุด หรือผู้ช่วยอัยการสูงสุดใด ๆ ที่ทำหน้าที่ผู้ช่วยอัยการสูงสุดหรือรองผู้ช่วยอัยการสูงสุดหรือทำหน้าที่รองผู้ช่วยอัยการสูงสุดในแผนกคดีอาญาหรือฝ่ายความมั่นคงแห่งชาติ ที่ได้รับมอบหมายเป็นพิเศษโดยอัยการสูงสุด อาจยื่นคำร้องต่อผู้พิพากษาที่มีอำนาจและอาจบังคับใช้แก่ผู้พิพากษาที่มีอำนาจสอดคล้องตามมาตรา 2518 ของบทนี้เพื่ออนุญาตหรืออนุมัติการดักรับการติดต่อสื่อสารผ่านสายโทรศัพท์ด้วยปากเปล่าโดยสำนักสืบสวนกลางหรือหน่วยงานของรัฐบาลกลางที่มีความรับผิดชอบในการตรวจสอบการกระทำผิดกฎหมายเป็นที่โปรแกรมจะทำเมื่อการสกัดกั้นดังกล่าวอาจให้หรือได้ให้หลักฐานของ....

(2) หลักการดำเนินการของอัยการในรัฐใด ๆ หรือหลักการดำเนินการของอัยการของส่วนราชการใดถ้าอัยการดังกล่าวมีอำนาจตามกฎหมายของรัฐนั้นที่จะยื่นคำขอแก่ผู้พิพากษาในศาลประจำรัฐที่มีอำนาจในการอนุญาตหรืออนุมัติการดักรับการติดต่อสื่อสารผ่านทางโทรศัพท์ ทางปากเปล่าหรือทางอิเล็กทรอนิกส์ และหรือยื่นต่อผู้พิพากษาซึ่งมีอำนาจสอดคล้องตามบทบัญญัติมาตราที่ 2518 ของบทนี้พร้อมด้วยคำขอตามข้อบังคับของของรัฐเพื่อมีคำสั่งอนุญาตหรืออนุมัติการดักรับการติดต่อสื่อสารผ่านทางโทรศัพท์ ทางปากเปล่าหรือทางอิเล็กทรอนิกส์โดยเจ้าหน้าที่สืบสวนหรือเจ้าหน้าที่บังคับใช้กฎหมายซึ่งมีความรับผิดชอบในการสืบสวนการกระทำผิดกฎหมายตามที่ปรากฏในคำขอเมื่อการดำเนินการดักฟังอาจมีหรือมีพยานหลักฐานเกี่ยวกับการกระทำความผิด ในคดีฆาตกรรม, ลักพาตัว, การพนัน, การปล้น การติดสินบน กรรโชก หรือการซื้อขายยาเสพติดกัญชาหรือยาเสพติดที่เป็นอันตรายอื่น ๆ หรือ ความผิดทางอาญาอื่น ๆ ที่เป็นอันตรายต่อชีวิต ร่างกาย หรือ ทรัพย์สินและมี

อัตราโทษจำคุกเป็นระยะเวลานานกว่าหนึ่งปี ซึ่งกำหนดไว้ ในกฎหมายของรัฐที่มีผลบังคับให้อำนาจในการดักรับข้อมูลดังกล่าวหรือการกระทำอื่นใดในลักษณะเดียวกันที่ได้กล่าวมาแล้ว

(3) อัยการของรัฐบาลหนึ่งรัฐบาลใด (ดังที่กำหนดไว้เพื่อวัตถุประสงค์ตามวิธีพิจารณาความอาญาของสหพันธ์รัฐ) อาจมีอำนาจทำคำร้องขอแก่ผู้พิพากษาสหพันธ์รัฐที่มีอำนาจและผู้พิพากษานั้นมีความสอดคล้องกับมาตรา 2518 ในหมวดกฎหมายนี้เพื่อให้มีคำสั่งอนุญาตหรืออนุมัติให้ดักรับข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์โดยเจ้าหน้าที่สืบสวนหรือเจ้าหน้าที่บังคับใช้กฎหมายที่มีความรับผิดชอบในการสืบสวนกระทำความผิดกฎหมายที่ระบุไว้ในคำร้องขอซึ่งจะได้ทำขึ้นเมื่อมีเหตุการณ์ที่ต้องจัดให้มีการดักรับข้อมูลหรือต้องมีการจัดเก็บพยานหลักฐานในความผิดทางอาญาใดของรัฐบาลกลาง

3.6 การจัดเก็บและการเปิดเผยข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์ตามกฎหมายสหรัฐอเมริกา

ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญาของอเมริกาบทที่ 18 ส่วนที่ 121[10] ได้วางหลักเกณฑ์การจัดเก็บข้อมูลการติดต่อสื่อสารผ่านสายโทรศัพท์หรือผ่านทางอิเล็กทรอนิกส์และการเข้าถึงข้อมูลการติดต่อสื่อสารที่ถูกจัดเก็บไว้ (Stored wire and electronic communications and transactional records access) ไว้ดังนี้

มาตรา 2701 การเข้าถึงข้อมูลที่จัดเก็บไว้โดยไม่ชอบด้วยกฎหมาย (Unlawful access to stored communications) เป็นการกำหนดข้อห้ามมิให้ผู้ที่ไม่มีอำนาจเกี่ยวข้องเข้าถึงหรือทำการดักเก็บหรือจัดเก็บข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์ได้

มาตรา 2702 การเปิดเผยข้อมูลการติดต่อสื่อสารหรือบันทึกการติดต่อสื่อสารของลูกค้า

(1) บุคคลหรือนิติบุคคลผู้ให้บริการในการติดต่อสื่อสารทางอิเล็กทรอนิกส์แก่สาธารณะ (A person or entity providing an electronic communication service to the public) จะต้องไม่ทำการเปิดเผยแก่บุคคลหรือนิติบุคคลใดซึ่งเนื้อหาขอการติดต่อสื่อสารที่จัดเก็บไว้ในรูปอิเล็กทรอนิกส์จากการให้บริการ

(2) บุคคลหรือนิติบุคคลที่ให้บริการประมวลผลคอมพิวเตอร์ระไกลแก่สาธารณะ (A person or entity providing remote computing service to the public)” จะต้องไม่ทำการเปิดเผยแก่บุคคลหรือนิติบุคคลใดซึ่งเนื้อหาของการติดต่อสื่อสารซึ่งครอบครองหรือรักษาไว้ในรูปอิเล็กทรอนิกส์จากการให้บริการ

---

[10] Ibid, 60.

(A) ในนามของสมาชิกหรือลูกค้าในการให้บริการเช่นนั้น และ ได้รับข้อมูลด้วยการการส่งสัญญาทางอิเล็กทรอนิกส์(หรือสร้างขึ้นโดยวิธีการประมวลผลคอมพิวเตอร์ของการติดต่อสื่อสารที่ได้รับจากการส่งสัญญาณผ่านทางอิเล็กทรอนิกส์)จากสมาชิกหรือลูกค้าในการให้บริการนั้น

(B) แต่เพียงผู้เดียวสำหรับวัตถุประสงค์เพื่อการจัดเก็บหรือประมวลผลของคอมพิวเตอร์ให้บริการแก่ผู้ใช้บริการหรือลูกค้าดังกล่าว ในกรณีที่ผู้ให้บริการไม่ได้รับอนุญาตในการเข้าถึงเนื้อหาของการสื่อสารดังกล่าวเพื่อวัตถุประสงค์ในการให้บริการอื่นนอกเหนือจากการจัดเก็บหรือคอมพิวเตอร์การประมวลผลคอมพิวเตอร์และ

(3) ผู้ให้บริการประมวลผลคอมพิวเตอร์ระยะไกลหรือบริการการสื่อสารทางอิเล็กทรอนิกส์แก่สาธารณะ (A provider of remote computing service or electronic communication service to the public) จะไม่เปิดเผยบันทึกหรือข้อมูลอื่นๆที่เกี่ยวข้องกับการใช้บริการหรือลูกค้าของบริการดังกล่าว (ไม่รวมถึงเนื้อหาของการสื่อสารที่ครอบคลุมตามความในวรรค (1) หรือ (2)) แก่หน่วยงานใดๆของรัฐ

มาตรา 2703 การร้องขอให้เปิดเผยข้อมูลการติดต่อสื่อสารหรือบันทึกการติดต่อสื่อสารของลูกค้า

(a) หน่วยงานราชการสามารถขอให้เปิดเผยข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์และทางโทรศัพท์จากผู้ให้บริการซึ่งมีการจัดเก็บข้อมูลอิเล็กทรอนิกส์ไว้ในระบบเป็นระยะเวลาไม่เกิน 180 วัน ตามวิธีการออกหมายในกฎระเบียบของรัฐบาลกลางวิธีการพิจารณาความอาญา (หรือกรณีศาลของรัฐที่ใช้วิธีการออกหมายตามวิธีการของรัฐซึ่งออกโดยศาลที่มีอำนาจ หน่วยงานราชการอาจขอข้อมูลที่มีการจัดเก็บไว้เกินกว่า 180 วันได้ในกรณีที่เป็นไปตามอนุ (b)

(b) เนื้อหาของการติดต่อสื่อสารผ่านสายโทรศัพท์หรือผ่านทางอิเล็กทรอนิกส์ในการให้บริการประมวลผลคอมพิวเตอร์ระยะไกล

(1) หน่วยงานราชการสามารถอาจขอให้เปิดเผยซึ่งเนื้อหาของข้อมูลการติดต่อสื่อสารไม่ว่าทางสายโทรศัพท์หรือข้อมูลอิเล็กทรอนิกส์จากผู้ให้บริการประมวลผลคอมพิวเตอร์ระยะไกลด้วยวิธีการตามวรรค (2) ในมาตรานี้

(A) โดยไม่ต้องมีการส่งหนังสือแจ้งผู้ใช้บริการหรือลูกค้า หน่วยงานราชการสามารถขอให้เปิดเผยซึ่งเนื้อหาของข้อมูลการติดต่อสื่อสารไม่ว่าทางสายโทรศัพท์หรือข้อมูลอิเล็กทรอนิกส์จากผู้ให้บริการประมวลผลคอมพิวเตอร์ระยะไกล โดยการออกหมายแจ้งตามวิธีการออกหมายในกฎระเบียบของรัฐบาลกลางวิธีการพิจารณาความอาญา (หรือกรณีศาลของรัฐที่ใช้วิธีการออกหมายตามวิธีการของรัฐ) ออกโดยศาลซึ่งมีอำนาจ

(B) โดยมีการส่งหนังสือแจ้งให้ผู้ใช้บริการหรือลูกค้าทราบ หน่วยงานราชการสามารถออกหมายทางปกครองตามที่ตนได้รับอำนาจตามกฎหมาย ทั้งนี้ บางกรณีอาจต้องมีการขอหมายศาลหากเป็นการขอข้อมูลเฉพาะบางอย่างที่ห้ามมิให้มีเพียงการออกหมายทางปกครอง

(2) การร้องขอตามวรรค (1) ด้วยความเคารพต่อข้อมูลการติดต่อสื่อสารผ่านสายโทรศัพท์หรือผ่านทางอิเล็กทรอนิกส์ที่ครอบครองหรือเก็บรักษาไว้ของการให้บริการ

(A) ในนามของสมาชิกหรือลูกค้าในการให้บริการเช่นนั้น และ ได้รับข้อมูลด้วยวิธีการการส่งสัญญาทางอิเล็กทรอนิกส์ (หรือสร้างขึ้นโดยวิธีการประมวลผลคอมพิวเตอร์ของการติดต่อสื่อสารที่ได้รับจากการส่งสัญญาณทางอิเล็กทรอนิกส์)จากสมาชิกหรือลูกค้าในการให้บริการประมวลผลคอมพิวเตอร์ระยะไกลนั้น

(B) แต่เพียงผู้เดียวสำหรับวัตถุประสงค์เพื่อการจัดเก็บหรือประมวลผลของคอมพิวเตอร์ให้บริการแก่ผู้ใช้บริการหรือลูกค้าดังกล่าว ในกรณีที่ผู้ให้บริการไม่ได้รับอนุญาตในการเข้าถึงเนื้อหาของการสื่อสารดังกล่าวเพื่อวัตถุประสงค์ในการให้บริการอื่นนอกเหนือจากการจัดเก็บหรือคอมพิวเตอร์การประมวลผลคอมพิวเตอร์

ทั้งนี้ ใน มาตรา 2703(f) ได้กำหนดเกี่ยวกับการจัดเก็บพยานหลักฐานตามกฎหมายไว้ดังนี้

(f) ข้อกำหนดการจัดเก็บไว้ซึ่งพยานหลักฐาน

(1) ในกรณีทั่วไป ผู้ให้บริการในการติดต่อสื่อสารผ่านสายหรือผ่านทางอิเล็กทรอนิกส์หรือผู้ให้บริการประมวลผลคอมพิวเตอร์ระยะไกล เมื่อได้รับการร้องขอจากรัฐบาลจะต้องดำเนินการตามความจำเป็นที่รัฐบาลร้องขอทีละขั้นตอนเพื่อให้สามารถจัดเก็บบันทึกและพยานหลักฐานอื่นๆที่อยู่ในความครอบครองในระหว่างที่รอศาลมีคำสั่งหรือมีกระบวนการอื่นต่อไป

(2) ระยะเวลาในการเก็บรักษา บันทึกตามที่ปรากฏในวรรค (1) จะต้องจัดให้มีการจัดเก็บรักษาไว้เป็นระยะเวลา 90 วัน และอาจขยายระยะเวลาการจัดเก็บอีก 90 วันหากมีการร้องขอจากหน่วยงานราชการ

มาตรา 2704 การจัดเก็บสำรองข้อมูล.

หน่วยงานราชการภายใต้ข้อบังคับที่ 2703(b)(2) อาจออกหมายเรียกหรือคำสั่งศาลเพื่อให้ผู้ให้บริการที่เกี่ยวข้องโดยตรงกับการสร้างสำเนาเนื้อหาหรือข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์ที่ต้องการ ดำเนินการจัดเก็บการติดต่อสื่อสารดังกล่าวนั้นไว้ โดยไม่ต้องส่งหมายหรือคำสั่งศาลให้แก่ผู้ใช้บริการหรือลูกค้าอีก ทั้งนี้ผู้ให้บริการจะต้องทำสำเนาสำรองการจัดเก็บข้อมูลให้รวดเร็วที่สุดเท่าที่จะสามารถปฏิบัติได้ในฐานะการประกอบธุรกิจเช่นนั้นและยืนยันให้หน่วยงานราชการทราบว่าได้ดำเนินการสำเนาข้อมูลที่ต้องการเก็บไว้แล้ว โดยการจัดเก็บสำเนาข้อมูลจะต้องเริ่มสร้างสำเนาภายในสองวันนับแต่วันที่ได้รับหมายหรือคำสั่งศาล

มาตรา 2706 การจ่ายค่าชดเชยค่าใช้จ่ายหรือค่าเสียหาย

(a) ค่าใช้จ่าย – ยกเว้นผู้ให้บริการตามอนุ (c) หน่วยงานราชการที่ได้รับเนื้อหาข้อมูลหรือบันทึกการติดต่อสื่อสารหรือข้อมูลอื่นใดภายใต้บทบัญญัติมาตราที่ 2702 , 2703 หรือ 2704 ในพระราชบัญญัตินี้ จะต้องจ่ายค่าชดเชยให้แก่บุคคลหรือหน่วยงานที่รวบรวมหรือจัดเก็บไว้ซึ่งข้อมูลดังกล่าวเพื่อชดเชยค่าใช้จ่ายที่สูญเสียในจำนวนที่ปกติจะต้องเสียในกรณีเช่นนั้นและซึ่งเป็นค่าใช้จ่ายโดยตรงจากการค้นหาข้อมูลดังกล่าวมาทำการรวบรวม หรือนำมาประมวลผลใหม่หรือการจัดเก็บไว้ซึ่งข้อมูล โดยค่าชดเชยดังกล่าวรวมถึงค่าใช้จ่ายใด ๆ ที่จำเป็นที่เกิดขึ้นจากการขัดขวางการทำงานปกติของการจัดเก็บข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์หรือขัดขวางผู้ให้บริการในการประมวลผลคอมพิวเตอร์ในการจัดเก็บข้อมูลดังกล่าวนั้น

(b) จำนวน – จำนวนค่าธรรมเนียมที่ต้องเตรียมตามข้อ (a) จะต้องได้รับการพิจารณาตกลงระหว่างหน่วยงานราชการและบุคคลหรือหน่วยงานซึ่งจัดเก็บข้อมูลดังกล่าวหรืออาจไม่ต้องมีการตกลงอาจใช้การกำหนดค่าธรรมเนียมโดยศาลที่เป็นผู้ออกคำสั่งหรือหมายให้รวบรวมข้อมูลดังกล่าว (หรือยื่นต่อศาลก่อนหน้าที่จะมีการดำเนินการในทางอาญาที่เกี่ยวข้องกับข้อมูลที่จะต้องนำไปใช้ในกรณีที่ไม่มีคำสั่งศาลเกี่ยวกับการสร้างข้อมูลดังกล่าว)

(c) ข้อยกเว้น – ข้อบังคับตามข้อ (a) ในส่วนกฎหมายนี้ไม่นำมาบังคับในกับบันทึกหรือข้อมูลอื่นใดที่มีการจัดเก็บไว้ตามปกติธรรมของผู้ให้บริการในการติดต่อสื่อสารทั่วไปซึ่งเกี่ยวข้องกับบันทึกช่องทางโทรศัพท์หรือรายชื่อโทรศัพท์ซึ่งได้รับมาตามบทบัญญัติส่วนที่ 2703 อย่างไรก็ตามศาลอาจออำคำสั่งให้มีการจ่ายค่าชดเชยตามข้อ (a) ได้หากเห็นว่าข้อมูลที่มีการร้องขอนั้นมีจำนวนมากกว่าตามปกติธรรมดาในการจัดเก็บหรือกรณีที่เห็นว่าการร้องขอทำให้เกิดภาระเกิดสมควรในการจัดเก็บข้อมูล

มาตรา 2707 การดำเนินการทางแพ่ง

(a) ผลของการกระทำ -. ยกเว้นตามที่บัญญัติไว้ในมาตรา 2703 (จ), ผู้ให้บริการใดๆในการให้บริการการสื่อสารทางอิเล็กทรอนิกส์, สมาชิก หรือบุคคลอื่น ซึ่งได้รับความเสียหายจากการกระทำละเมิดใด ๆ ตามบทบัญญัตินี้ซึ่งการดำเนินการให้เกิดการละเมิดโดยรู้หรือที่โดยทั่วไปย่อมรู้ได้ถึงการละเมิด อาจดำเนินการทางแพ่งเพื่อขอชดเชยจากบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่สหรัฐอเมริกาซึ่งมีส่วนร่วมในการละเมิดเพื่อบรรเทาความเสียหายตามความเหมาะสม

มาตรา 2708 การเยียวยาเป็นพิเศษ

การเยียวยาและบทลงโทษที่บัญญัติไว้ในบทนี้เป็นเพียงการเยียวยาและลงโทษสำหรับการละเมิดที่ไม่ปรากฏในรัฐธรรมนูญสำหรับบทนี้

มาตรา 2709 บันทึกการเข้าถึงโทรศัพท์หรือการแลกเปลี่ยนสัญญาณสื่อสารของการก่อการร้าย

(a) หน้าที่ในการจัดเก็บ – ผู้ให้บริการจัดเก็บข้อมูลการติดต่อสื่อสารผ่านสายโทรศัพท์หรือผ่านทางอิเล็กทรอนิกส์จะต้องดำเนินการตามขั้นตอนเกี่ยวกับการจัดเก็บไว้ซึ่งข้อมูลสมาชิกและบันทึกค่าใช้จ่ายการโทรหรือการติดต่อสื่อสารผ่านทางอิเล็กทรอนิกส์ที่อยู่ในความดูแลหรือครอบครองของตนตามที่สำนักงานสืบสวนกลางกำหนดไว้ภายใต้ข้อ (b)

(b) (ข) หนังสือแสดงคำร้องขอ - ผู้อำนวยการสำนักงานสืบสวนกลางหรือผู้รักษาการในตำแหน่งหรือเจ้าหน้าที่ผู้มีตำแหน่งไม่ต่ำกว่ารองผู้ช่วยผู้อำนวยการที่สำนักงานใหญ่ของสำนักงานสืบสวนกล่าวหรือเจ้าหน้าที่พิเศษในสำนักงานที่ได้รับมอบหมายจากผู้อำนวยการ อาจ

(1) เรียกขอชื่อ ที่อยู่ ความยาวของการบริการ และบันทึกการเรียกเก็บค่าบริการทั้งโทรระยะสั้นและโทรทางไกลของบุคคลหรือนิติบุคคล ถ้ากรรมการ (หรือ ผู้มีอำนาจจัดการแทน) ให้การรับรองโดยการเขียนถึงผู้ให้บริการการติดต่อสื่อสารผ่านสายโทรศัพท์หรือผ่านทางอิเล็กทรอนิกส์ โดยการร้องขอดังกล่าวต้องระบุว่า ชื่อ ที่อยู่ ระยะเวลาในการให้บริการ และบันทึกการเรียกเก็บบริการติดต่อสื่อสาร ว่ามีความเกี่ยวข้องกับการตรวจสอบที่มีอำนาจกระทำได้ เพื่อป้องกันการก่อการร้ายระหว่างประเทศ หรือกิจกรรมของหน่วยสืบราชการลับ โดยมีเงื่อนไขว่าการตรวจสอบดังกล่าวแก่คนของประเทศสหรัฐอเมริกาไม่ได้เป็นเพียงการกระทำบนพื้นฐานของการกระทำทั่วไปซึ่งได้รับการคุ้มครองจากกฎหมายรัฐธรรมนูญแห่งสหรัฐอเมริกา และ

(2) เรียกขอชื่อ ที่อยู่ ความยาวของการบริการ ของบุคคลหรือนิติบุคคล ถ้ากรรมการ (หรือ ผู้มีอำนาจจัดการแทน) ให้การรับรองโดยการเขียนถึงผู้ให้บริการการติดต่อสื่อสารผ่านสายโทรศัพท์หรือผ่านทางอิเล็กทรอนิกส์ โดยระบุว่าข้อมูลที่ต้องการมีความเกี่ยวข้องกับการตรวจสอบที่มีอำนาจกระทำได้ เพื่อป้องกันการก่อการร้ายระหว่างประเทศ หรือกิจกรรมของหน่วยสืบราชการลับ โดยมีเงื่อนไขว่าการตรวจสอบดังกล่าวแก่คนของประเทศสหรัฐอเมริกาไม่ได้เป็นเพียงการกระทำบนพื้นฐานของการกระทำทั่วไปซึ่งได้รับการคุ้มครองจากกฎหมายรัฐธรรมนูญแห่งสหรัฐอเมริกา

(c) ห้ามมิให้มีการเปิดเผยข้อมูลเฉพาะบางอย่าง

(1) ในกรณีที่ผู้อำนวยการสำนักงานสืบสวนกลางแห่งสหรัฐอเมริกาหรือผู้รักษาการในตำแหน่งหรือเจ้าหน้าที่ผู้มีตำแหน่งไม่ต่ำกว่ารองผู้ช่วยผู้อำนวยการที่สำนักงานใหญ่ของสำนักงานสืบสวนกล่าวหรือเจ้าหน้าที่พิเศษในสำนักงานที่ได้รับมอบหมายจากผู้อำนวยการ รับรองว่า มีบางอย่างที่อาจส่งผลให้เป็นอันตรายต่อความมั่นคงแห่งชาติของประเทศสหรัฐอเมริกา, มีการรบกวนการสืบสวนกระบวนการทางอาญา, การต่อต้านการก่อการร้าย การต่อต่อการแทรกซึมโจรกรรมข้อมูล หรือ รบกวนต่อความสัมพันธ์ ทางการทูต หรือ เป็นอันตรายต่อชีวิตหรือความปลอดภัยทางกายภาพของบุคคลใดบุคคลหนึ่ง ผู้บริการติดต่อสื่อสารแบบไร้สายหรือทางอิเล็กทรอนิกส์ หรือเจ้าหน้าที่ พนักงาน หรือตัวแทนดังกล่าว สามารถเปิดเผยให้แก่บุคคลใด ๆ ที่สำนักงานสืบสวนกลาง

แห่งสหรัฐอเมริกาได้ขอหรือได้รับการเข้าถึงข้อมูลตามระเบียบในมาตรานี้ (นอกเหนือจากผู้ที่เปิดเผยข้อมูลดังกล่าวมีความจำเป็นต้องปฏิบัติตามคำขอหรือ ทนายความเพื่อขอคำแนะนำทางกฎหมายหรือความช่วยเหลือทางกฎหมายที่เกี่ยวกับการร้องขอ)

(2) หนังสือแจ้งถึงทราบถึงการร้องขอต้องส่งไปยังบุคคลหรือนิติบุคคลซึ่งกำกับดูแลข้อมูลที่มิได้มีการเปิดเผยซึ่งได้รับการร้องขอตามข้อ (1)

(3) ผู้รับการเปิดเผยข้อมูลให้แก่บุคคลเหล่านั้นตามความจำเป็นต้องปฏิบัติตามคำขอหรือทนายความเพื่อขอคำแนะนำทางกฎหมายหรือความช่วยเหลือทางกฎหมายที่เกี่ยวกับการร้องขอใด ๆ จะต้องแจ้งให้บุคคลซึ่งได้รับการร้องขอให้เปิดเผยข้อมูลตามความเหมาะสมทราบ บุคคลใดที่ได้รับการเปิดเผยข้อมูลที่อยู่ภายใต้อนุนี้ต้องอยู่ภายใต้ข้อห้ามเช่นเดียวกันกับการเปิดเผยข้อมูลตามวรรค (1)

(4) ตามคำร้องขอของผู้อำนวยการสำนักงานสืบสวนกลางหรือผู้ได้รับการแต่งตั้งจากผู้อำนวยการ บุคคลใดที่กระทำหรือตั้งใจจะทำการเปิดเผยข้อมูลภายใต้มาตรานี้จะต้องแจ้งไปยังผู้อำวยการหรือผู้ได้รับการแต่งดังกล่าวเกี่ยวกับบุคคลซึ่งจะทำการเปิดเผยข้อมูลหรือบุคคลที่เปิดเผยข้อมูลแล้วก่อนทำการร้องขอ เว้นแต่นอกเหนือจากมาตรานี้บุคคลจะต้องแจ้งให้ผู้อำนวยการหรือผู้ได้รับการแต่ตั้งดังกล่าวทราบถึงการระบุตัวทนายความซึ่งทำการเผยข้อมูลหรือจะเปิดเผยข้อมูลเพื่อขอคำแนะนำทางกฎหมายหรือความช่วยเหลือทางกฎหมายที่เกี่ยวกับการร้องขอตามอนุ (a)

(d) การเผยแพร่โดยสำนักงาน -. สำนักงานสืบสวนกลางอาจเผยแพร่ข้อมูลและบันทึกที่ได้รับตามมาตรานี้ เพียงเท่าที่กำหนดไว้ ในแนวทางซึ่งได้รับการอนุมัติจากอัยการสูงสุดในการเก็บรวบรวมข่าวกรอง ต่างประเทศ และการตรวจสอบการโจรกรรมต่างประเทศที่ดำเนินการโดยสำนักงานสืบสวนกลาง และการเผยแพร่ตามสมควรไปยังหน่วยงานของสหรัฐอเมริกาในเฉพาะกรณีที่ปรากฏแน่ชัดว่าข้อมูลดังกล่าวมีความเกี่ยวข้องกับอำนาจหน้าที่ความรับผิดชอบของหน่วยงานนั้น

(e) ต้องมีการแจ้งให้สภารับทราบ - . ทุกระยะเวลาประจำครึ่งปี ผู้อำนวยการสำนักงานสืบสวน ต้องมีรายงานแจ้งอย่างเป็นทางการแก่คณะกรรมาธิการข่าวกรองของสภาผู้แทนราษฎร และคณะกรรมาธิการข่าวกรองของวุฒิสภา และคณะกรรมการตุลาการของสภาผู้แทนราษฎรและคณะกรรมการตุลาการของวุฒิสภา ให้ทราบเกี่ยวกับการร้องขอทั้งหมดที่เกิดขึ้นภายใต้หมวด (b) ของมาตรานี้

(f) ห้องสมุด - . ห้องสมุด (ตาม ที่กำหนดไว้ในมาตรา 213 (1) พระราชบัญญัติการให้บริการห้องสมุดและเทคโนโลยี (ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 20 มาตรา 9122 (1)) การให้บริการ ที่รวมถึงการเข้าถึงอินเทอร์เน็ต, หนังสือ, วารสาร นิตยสารหนังสือพิมพ์ หรือรูปแบบ อื่นที่คล้ายคลึงกัน ในการติดต่อสื่อสาร ในการพิมพ์ หรือ แบบดิจิตอลโดย ลูกค้า ของพวกเขา ใช้ ทบทวน การตรวจสอบ หรือ การไหลเวียน ไม่ถือว่าเป็นผู้ให้บริการการสื่อสารทาง

สายโทรศัพท์หรือทางอิเล็กทรอนิกส์ตามบทบัญญัตินี้ เว้นแต่ห้องสมุดที่มีการให้บริการตามความหมายที่กำหนดไว้ในมาตรา 2510 (15) (“บริการ การสื่อสารทางอิเล็กทรอนิกส์”) ของกฎหมายลักษณะนี้

มาตรา 2712 การกระทำทางแพ่งต่อประเทศสหรัฐอเมริกา

(a) กรณีทั่วไป -. บุคคลที่มีการรับความเสียหายโดยเจตนาละเมิดใดๆของบทนี้หรือในบทที่ 119 ของลักษณะนี้หรือมาตรา 106 (a), 305 (a) หรือ 405 (a) ของพระราชบัญญัติการเฝ้าระวังข่าวกรองต่างประเทศใด ๆ ปี 1978 (ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 50มาตรา 1801 et seq.) อาจเริ่มการดำเนินคดีต่อศาลแขวงแห่งสหรัฐอเมริกาเพื่อให้สหรัฐอเมริกาชดเชยค่าเสียหายเป็นตัวเงินคืน ในการกระทำดังกล่าวถ้าพิจารณาได้ความว่าผู้ได้รับความเสียหายได้รับความเสียหายจากการละเมิดของส่วนนี้หรือในส่วนที่ 119 ของลักษณะนี้หรือบทบัญญัติที่เฉพาะเจาะจงดังกล่าวข้างต้นของบทที่ 50 ศาลอาจประเมินเป็นความเสียหายดังนี้

(1) ความเสียหายที่เกิดขึ้นจริงแต่ไม่น้อยกว่าจำนวน 10,000 ดอลลาร์สหรัฐ แล้วแต่จำนวนใดจะสูงกว่า และ

(2) ค่าใช้จ่ายในการดำเนินคดีที่เกิดขึ้นตามสมควรแก่เหตุ

3.7 การจัดเก็บข้อมูลจราจรทางทางคอมพิวเตอร์ตามอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ มีกำหนดไว้ใน ข้อ 16 อนุ 2 คือ ให้แต่ละประเทศภาคีมีมาตรการให้บุคคลจัดเก็บและรักษาความถูกต้องของข้อมูลจราจรทางคอมพิวเตอร์ไว้

อนุสัญญาฯ ได้กำหนดหลักการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ใน ข้อ 16 และ 17 ดังนี้

ข้อ 16 การเข้าเก็บรักษาที่รวดเร็วของข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้

1) ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็นเพื่อให้หน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องของประเทศนั้นสามารถออกคำสั่งเรียกหรือรับเอาด้วยวิธีการอื่น ซึ่งการเก็บรักษาที่รวดเร็วของข้อมูลคอมพิวเตอร์ที่เฉพาะเจาะจง รวมถึงข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งถูกเก็บไว้โดยวิธีการของระบบคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งเมื่อมีเหตุผลอันควรเชื่อว่าข้อมูลคอมพิวเตอร์นั้นมีความเสี่ยงโดยเฉพาะที่จะสูญหายหรือถูกแก้ไขดัดแปลง

2) ในกรณีที่ประเทศภาคีได้นำหลักเกณฑ์ตามวรรค1ข้างต้นมาใช้โดยจะมีการออกคำสั่งให้บุคคลเก็บรักษาข้อมูลคอมพิวเตอร์เฉพาะเจาะจงซึ่งถูกเก็บไว้ในความครอบครองหรือควบคุมของบุคคลนั้นประเทศภาคีนั้นพึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็นที่กำหนดให้บุคคลนั้นมีหน้าที่จะต้องเก็บรักษาและคงไว้ซึ่งความถูกต้องของข้อมูลคอมพิวเตอร์ดังกล่าวสำหรับช่วง

ระยะเวลาหนึ่งเท่าที่จำเป็นแต่ไม่เกินเก้าสิบวันเพื่อให้หน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องสามารถแสวงหาข้อเท็จจริงจากข้อมูลคอมพิวเตอร์นั้นได้ ประเทศภาคีนั้นอาจกำหนดหลักเกณฑ์ให้มีการขยายระยะเวลาของคำสั่งดังกล่าวต่อไปได้

3) ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็นเพื่อกำหนดให้ผู้ที่ครอบครองข้อมูลคอมพิวเตอร์หรือบุคคลอื่นซึ่งมีหน้าที่จะต้องเก็บรักษาข้อมูลคอมพิวเตอร์นั้นเก็บเป็นความลับในเรื่องที่มีการใช้วิธีพิจารณาความดังกล่าวนั้นภายในช่วงระยะเวลาตามที่กำหนดไว้ในกฎหมายภายในประเทศภาคีนั้น

4) ให้อำนาจหน้าที่และวิธีพิจารณาความดังกล่าวในข้อนี้อยู่ภายใต้บังคับของข้อ 14 และ 15

ข้อ 17 การเข้าเก็บรักษาที่รวดเร็วและการเปิดเผยบางส่วนของข้อมูลจราจรทางคอมพิวเตอร์

1) ประเทศภาคีแต่ละประเทศโดยคำนึงถึงข้อมูลจราจรทางคอมพิวเตอร์ซึ่งต้องถูกเก็บรักษาตามข้อ 16 นั้น พึงจัดให้มีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็น เพื่อ

(ก) ทำให้เกิดความแน่นอนว่าการเก็บรักษาที่รวดเร็วสำหรับข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวนั้นจะมีการดำเนินการได้ โดยไม่คำนึงว่าผู้ให้บริการจำนวนหนึ่งหรือหลายรายมีส่วนเกี่ยวข้องกับการส่งต่อของการติดต่อสื่อสารนั้นหรือไม่ และ

(ข) ทำให้เกิดความแน่นอนว่าการเปิดเผยที่รวดเร็วของข้อมูลจราจรทางคอมพิวเตอร์ในจำนวนที่เพียงพอที่ดำเนินการโดยหน่วยงานที่มีอำนาจหน้าที่ของประเทศภาคีหรือโดยบุคคลที่ได้รับมอบหมายจากหน่วยงานดังกล่าวนั้น จะทำให้ประเทศภาคีนั้นสามารถบ่งชี้ได้ว่าผู้ให้บริการรายใดและเส้นทางผ่านใดที่การติดต่อสื่อสารนั้นมีการส่ง

2) ให้อำนาจเจ้าหน้าที่และวิธีพิจารณาความดังกล่าวในข้อนี้อยู่ภายใต้บังคับข้อ 14 และ 15

จะเห็นว่าข้อมูลจราจรทางคอมพิวเตอร์ซึ่งเป็นพยานหลักฐานสำคัญในการหาตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้น อนุสัญญาได้กำหนดให้ประเทศภาคีสมาชิกต้องมีมาตรการทางนิติบัญญัติและมาตรการอื่นที่จำเป็นเพื่อให้หน่วยงานที่มีอำนาจสามารถเรียกหรือได้มาด้วยวิธีอื่นซึ่งข้อมูลจราจรทางคอมพิวเตอร์ที่ถูกเก็บไว้ พร้อมทั้งต้องมีการควบคุมผู้มีหน้าที่จัดเก็บให้เก็บรักษาและคงไว้ซึ่งความถูกต้องของข้อมูลจราจรทางคอมพิวเตอร์สำหรับระยะเวลาเท่าที่จำเป็นแต่ไม่เกินเก้าสิบวัน (Article 16) นอกจากนั้นอนุสัญญาฯกำหนดให้ประเทศภาคีจะต้องมีมาตรการทางนิติบัญญัติหรือทางอื่นที่จำเป็นเพื่อกำหนดอำนาจหน้าที่และวิธีพิจารณาความ เกี่ยวกับความผิดอาญาที่ได้กระทำโดยวิธีการของระบบคอมพิวเตอร์ และ การรวบรวมพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์สำหรับความผิดทางอาญา (Article 14) เพื่อให้สามารถนำตัวผู้กระทำความผิดมาลงโทษได้อย่างมีประสิทธิภาพ

3.8 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (“Directive 2006/24/EC”)

ส่วนหนึ่งของเหตุผลที่มี Directive 2006/24/EC ฉบับนี้เพื่อเป็นการให้ความสำคัญแก่ข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลระบุที่อยู่เพื่อใช้ในการสืบสวน การค้นหา และการดำเนินคดีทางอาญา เนื่องจากการทำวิจัยและการปฏิบัติจริงของประเทศสมาชิกทั้งหลายพบว่ามีความจำเป็นที่จะต้องมั่นใจว่าข้อมูลดังกล่าวซึ่งเกิดขึ้นจากกระบวนการติดต่อสื่อสารจะต้องจัดให้มีการเก็บไว้เป็นระยะเวลาหนึ่งตามกฎหมายนี้

บทบัญญัติข้อ 3

1) ประเทศสมาชิกจะต้องกำหนดมาตรการเพื่อให้แน่ใจว่าข้อมูลที่ระบุไว้ในข้อ 5 ของคำสั่งนี้จะยังคงเป็นไปตามบทบัญญัติดังกล่าวเท่าที่ข้อมูลเหล่านั้นจะเกิดขึ้นหรือมีการประมวลผลโดยผู้ให้บริการแก่สาธารณะด้านการสื่อสารอิเล็กทรอนิกส์หรือของเครือข่ายการสื่อสารของประชาชนภายในเขตอำนาจของตนในกระบวนการของการจัดหาบริการด้านการสื่อสารที่เกี่ยวข้อง

2) หน้าที่ในการเก็บข้อมูลไว้ในวรรค 1 ให้หมายความรวมถึงการเก็บรักษาข้อมูลที่ระบุไว้ในข้อ 5 ที่เกี่ยวข้องกับความพยายามโทรที่ไม่ประสบความสำเร็จซึ่งข้อมูลเหล่านั้นถูกสร้างขึ้นหรือเกิดขึ้นและเก็บไว้ (ในเรื่องข้อมูลโทรศัพท์) หรือเข้าสู่ระบบ (ที่เกี่ยวกับข้อมูลอินเทอร์เน็ต) โดยผู้ให้บริการที่มีอยู่ทั่วไปในการให้บริการด้านการสื่อสารอิเล็กทรอนิกส์หรือของเครือข่ายการสื่อสารของประชาชนภายในเขตอำนาจของรัฐสมาชิกที่เกี่ยวข้องในกระบวนการของการจัดหาบริการด้านการสื่อสารที่เกี่ยวข้อง คำสั่งนี้จะไม่กำหนดต้องมีการเก็บรักษาไว้ซึ่งข้อมูลที่เกี่ยวข้องกับการโทรที่ไม่ได้มีการการเชื่อมต่อกับเครือข่าย

บทบัญญัติข้อ 5 ประเภทของข้อมูลที่ต้องมีการเก็บรักษา

1) ภายใต้ประเทศฉบับนี้ประเทศสมาชิกต้องกระทำให้มั่นใจว่าจะต้องมีการจัดเก็บไว้ซึ่งข้อมูลดังต่อไป

(a) ข้อมูลที่จำเป็นในการติดตามและระบุแหล่งที่มาของการติดต่อสื่อสาร

(b) ข้อมูลที่จำเป็นในการระบุแหล่งปลายทางของการติดต่อสื่อสาร

(c) ข้อมูลที่จำเป็นในการระบุวันเวลาและระยะเวลาของการติดต่อสื่อสาร

(d) ข้อมูลที่จำเป็นในการระบุประเภทของการติดต่อสื่อสาร

(e) ข้อมูลที่จำเป็นในการระบุอุปกรณ์การสื่อสารของผู้ใช้สิ่งที่ระบุว่าเป็นอุปกรณ์ของผู้นั้น

(f) ข้อมูลที่จำเป็นในการระบุตำแหน่งของอุปกรณ์การสื่อสารเคลื่อนที่

2) ไม่มีการเปิดเผยเนื้อหาของข้อมูลที่ได้จัดเก็บไว้ตาม **Directive 2006/24/EC** นี้

บทบัญญัติข้อ 6 ระยะเวลาการเก็บรักษา

ประเทศสมาชิกจะต้องมั่นใจว่าข้อมูลตามที่ระบุไว้ในข้อ 5 จะต้องได้รับการเก็บรักษาไว้เป็นระยะเวลาอย่างน้อย 6 เดือน และสูงสุดไม่เกินสองปีนับจากวันที่มีการติดต่อสื่อสาร

3.9 เปรียบเทียบการจัดเก็บและการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตระหว่างกฎหมายไทย กฎหมายอเมริกาและกฎหมายของยุโรป

3.9.1 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายสภายุโรปกำหนดให้เป็นหน้าที่ของผู้ให้บริการอันได้แก่ ผู้ให้บริการอินเทอร์เน็ตเน็ต ผู้ให้บริการโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ตคาเฟ่ รวมไปถึงผู้ให้บริการในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งประเทศไทยได้กำหนดไว้เช่นเดียวกับกหมายของสภายุโรปเนื่องจากเป็นตัวอย่างในการศึกษาก่อนจะมีการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทย ส่วนในกฎหมายอเมริกา นอกจากจะกำหนดให้เป็นหน้าที่ของผู้ให้บริการที่จะต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้เช่นเดียวกับสภายุโรปและไทยแล้ว กฎหมายอเมริกายังมีการกำหนดหน่วยงานกลาง คือหน่วยงาน NSA ที่คอยทำหน้าที่จัดเก็บข้อมูลจราจรทงาคอมพิวเตอร์ไว้แยกต่างหากจากผู้ให้บริการอีกส่วนหนึ่งเพื่อสามารถเรียกใช้ข้อมูลได้ในกรณีที่เกิดคดีเกี่ยวกับความมั่นคงของรัฐขึ้นเพื่อรักษาความมั่นคงทางเศรษฐกิจและอำนาจอธิปไตยของประเทศ

เรื่องระยะเวลาการจัดเก็บกฎหมายไทยกำหนดให้ผู้ให้บริการต้องจัดเก็บไว้เป็นระยะเวลาไม่น้อยกว่า 90 วัน และอาจเพิ่มระยะเวลาการจัดเก็บได้พนักงานเจ้าหน้าที่เห็นว่ามีเหตุจำเป็นให้ต้องเก็บเป็นระยะเวลานานขึ้นแต่ต้องไม่เกิน 1 ปี โดยมิได้มีการเยียวยาเกี่ยวกับค่าใช้จ่ายที่จะเกิดขึ้นกับผู้ให้บริการแต่อย่างใด แต่ในกฎหมายของสหรัฐอเมริการมีการกำหนดหน้าที่ผู้ให้บริการต้องจัดเก็บไว้เป็นระยะเวลาไม่น้อยกว่า 90 วันเช่นกัน แต่ในกรณีที่หน่วยงานของรัฐหน่วยงานใดต้องการให้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวไว้เป็นระยะเวลานานกว่าที่กฎหมายกำหนดจะต้องเป็นผู้รับผิดชอบในส่วนของค่าใช้จ่ายที่เพิ่มขึ้นแก่ผู้ให้บริการ ซึ่งจะช่วยเป็นการลดภาระผู้ให้บริการไม่ต้องรับภาระหนักเกินกว่าหน้าที่ปกติตามกฎหมาย ทั้งนี้ ในส่วนของสภายุโรปในช่วงปี ค.ศ. 2001 มีการกำหนดหน้าที่ผู้ให้บริการไว้ว่าต้องจัดเก็บเป็นระยะเวลาไม่น้อยกว่า 90 วัน แต่ต่อมาในปี ค.ศ. 2006 มีการประชุมสภายุโรปและเห็นว่าการจัดเก็บด้วยระยะเวลาเพียง 90 วันไม่เพียงต่อกระบวนการสืบสวนเพื่อนำตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์มาลงโทษ จึงมีการตรา Directive 2006/24/EC เพื่อกำหนดระยะเวลาการจัดเก็บใหม่สำหรับข้อมูลจราจรทางคอมพิวเตอร์ให้ผู้ให้

บริการต้องจัดเก็บไว้เป็นระยะเวลาไม่น้อยกว่า 180 วัน ทั้งนี้กฎหมายของสภายุโรปไม่ได้มีการวางหลักการว่าหน่วยงานรัฐจะต้องเข้ามาช่วยจัดเก็บหรือรับผิดชอบในส่วนของค่าใช้จ่ายของผู้ให้บริการที่เพิ่มขึ้นแต่อย่างใด

3.9.2 การได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์

ตามกฎหมายของสภายุโรปการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์โดยพนักงานเจ้าหน้าที่สามารถกระทำได้ภายใต้กฎหมายอาชญากรรมทางคอมพิวเตอร์เพราะได้มีการกำหนดความผิดเกี่ยวกับการละเมิดลิขสิทธิ์เป็นความผิดหนึ่งในอาชญากรรมทางคอมพิวเตอร์ ส่วนในกฎหมายอเมริกาพนักงานเจ้าหน้าที่ตามกฎหมายวิธีพิจารณาความอาญามีอำนาจที่จะขอข้อมูลเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และลิขสิทธิ์ด้วย จึงไม่มีปัญหาในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต ซึ่งทั้งสองรูปแบบดังกล่าวไม่มีปรากฏในประเทศไทย โดยประเทศไทยอำนาจในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เป็นของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งร้องขอได้เมื่อมีความผิดตามพระราชบัญญัติเกิดขึ้นเท่านั้น เมื่อความผิดฐานละเมิดลิขสิทธิ์บนอินเทอร์เน็ตมิได้เป็นความผิดตราพระราชบัญญัตินี้ จึงไม่มีกรณีที่พนักงานเจ้าหน้าที่จะสามารถใช้อำนาจเพื่อขอข้อมูลจราจรทางคอมพิวเตอร์มาใช้เป็นพยานหลักฐานต่อไปได้

บทที่ 4
บทวิเคราะห์

ในบทนี้ผู้เขียนจะได้วิเคราะห์ปัญหาในประเด็นต่าง ๆ เกี่ยวกับความเกี่ยวข้องข้อมูลจราจรทางคอมพิวเตอร์กับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต กระบวนการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์รวมไปถึงกระบวนการและมาตรฐานการจัดเก็บข้อมูลจราจรทางอคอมพิวเตอร์ ตลอดจนปัญหาเรื่องระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อนำไปสู่การวิเคราะห์ข้อเสนอแนะและแนวทางแก้ไขปัญหาต่าง ๆ เพื่อให้สามารถเกิดกระบวนการจัดเก็บและได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์อย่างมีประสิทธิภาพอันเกี่ยวโยงกับการใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

4.1 วิเคราะห์ปัญหาการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

4.1.1 ปัญหาอำนาจในการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 จัดได้ว่าเป็นกฎหมายอาญาประเภทหนึ่ง เพราะมีโทษทางอาญาสำหรับผู้กระทำความผิดเป็นหลัก จึงส่งผลให้ในการเก็บรวมรวมพยานหลักฐาน การสืบพยาน การสืบสวน สอบสวน ต้องดำเนินการไปตามกระบวนการทางอาญาปกติ แต่เมื่อมีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตมาเกี่ยวข้องกระบวนการดำเนินการจึงต้องมีความเกี่ยวข้องกับข้อมูลการติดต่อสื่อสารผ่านอินเทอร์เน็ต ซึ่งเป็นข้อมูลส่วนบุคคลที่กฎหมายรัฐธรรมนูญให้ความคุ้มครองสิทธิส่วนบุคคลไว้การจะสามารถได้มาซึ่งข้อมูลดังกล่าวก็โดยอาศัยอำนาจตามกฎหมายเท่านั้น โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัติเกี่ยวกับความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หน้าที่ของผู้ให้บริการที่ต้องจัดเก็บข้อมูลการติดต่อสื่อสารดังกล่าวไว้เพื่อใช้เป็นพยานหลักฐานในการสืบสวนการกระทำความผิด และแต่งตั้งเจ้าหน้าที่ตามพระราชบัญญัติฉบับนี้เป็นการเฉพาะ สำหรับการปฏิบัติหน้าที่และใช้อำนาจในการได้มาซึ่งข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์สำหรับการกระทำความผิดตามพระราชบัญญัติดังกล่าว แต่พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ไม่ได้มีการกำหนดในลักษณะของพนักงานเจ้าหน้าที่เป็นการเฉพาะและกระบวนการสืบสวนในทางอาญาเป็นไปตามวิธีปกติปกติคือดำเนินการโดยเจ้าหน้าที่ตำรวจซึ่งมิได้มีการบัญญัติให้อำนาจไว้เป็นการเฉพาะเพื่อได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว ดังนั้นเมื่อมีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเกิดขึ้นเจ้าหน้าที่ตำรวจจึงไม่สามารถใช้อำนาจของตนให้ได้มาซึ่งข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์ได้ด้วยอำนาจของตนเอง แต่ต้องอาศัยอำนาจศาลในการออกหมายเรียกพยานหลักฐาน

ซึ่งก่อนจะมีการออกหมายจะต้องมีหลักฐานประกอบพอสมควรที่ศาลจะเชื่อได้ว่าพยานหลักฐานนั้นมีความจำเป็นที่ต้องเรียกมาประกอบการสืบสวนสอบสวน ซึ่งข้อมูลจราจรทางคอมพิวเตอร์เป็นหลักฐานเบื้องต้นและเป็นพื้นฐาน ดังกล่าวเมื่อหลักฐานเบื้องต้นพนักงานสอบสวนเองไม่สามารถรวมรวบมาประกอบการขอออกหมายศาลได้ จึงทำให้เกิดอุปสรรคในกระบวนการปฏิบัติตามกระบวนการทางอาญา

ในทางปฏิบัติและการตีความของนักกฎหมายจากการสัมภาษณ์และจากบทความที่ได้กล่าวมาแล้วพบว่ามีการตีความให้การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นลักษณะความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพื่อให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้มีอำนาจเข้ามาดำเนินการได้ เนื่องจากหากไม่ใช่ความผิดตามพระราชบัญญัตินี้ก็จะเกิดปัญญาที่พนักงานเจ้าหน้าที่ไม่สามารถเข้ามาทำการสืบสวนได้และเจ้าหน้าที่ตำรวจก็ไม่มีอำนาจจะขอข้อมูลดังกล่าวได้ ทั้งนี้ แม้จะมีการตีความให้การกระทำบางอย่างจัดว่าเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่ด้วยเจตนารมณ์ของกฎหมาย พระราชบัญญัติลิขสิทธิ์ย่อมมุ่งคุ้มครองเรื่องลิขสิทธิ์ตามที่กฎหมายได้กำหนดไว้ อีกทั้งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในชั้นร่างพิจารณา ก็มิได้มีการกล่าวถึงการละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาอื่นแต่อย่างใด แต่มีขึ้นเพื่อคุ้มครองเกี่ยวกับการกระทำความผิดทางด้านคอมพิวเตอร์เป็นหลัก ดังนั้น การตีความโดยใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาปรับใช้กับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตจึงไม่ใช่สิ่งที่เจตนารมย์ของกฎหมายต้องการ ดังนั้น จึงกล่าวได้ว่าการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตของประเทศไทย ยังไม่ได้มีการวางหลักเกณฑ์หรือกฎหมายอย่างชัดเจนในทางปฏิบัติเกี่ยวกับการได้มาซึ่งพยานหลักฐาน

ในประเทศสหรัฐอเมริกาได้กำหนดให้ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์ที่มีลักษณะการกระบนอินเทอร์เน็ตตามกฎหมาย ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 18 มาตรา 2319 Criminal Infringement of a Copyright อยู่ภายใต้กฎหมายอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริกา Cyber Crime Law of United State of America โดยให้การสืบสวนสอบสวนเกี่ยวกับความผิดดังกล่าวสามารถกระทำได้โดยผู้มีอำนาจและกระบวนการเช่นเดียวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อื่น ๆ และในส่วนของสหภาพยุโรปกำหนดความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิ์ที่เกี่ยวข้องเป็นความผิดตามอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2011 ซึ่งมีการกำหนดกระบวนการจัดเก็บและการให้ได้มาซึ่งข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ดังกล่าวไว้เป็นการเฉพาะเช่นเดียวกัน ซึ่งการกำหนดในลักษณะเช่นของทั้งสหรัฐอเมริการและสภายุโรป ทำให้การสืบสวนและรวบรวมพยานหลักฐานมีกระบวนการดำเนินการในลักษณะของการสืบสวนการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ ดังเช่นที่บัญญัติไว้ใน ประมวลกฎหมาย

อาญาและวิธีพิจารณาความอาญา บทที่ 18 มาตรา 2510-2522 กำหนดเกี่ยวกับการดักรับซึ่งข้อมูลการติดต่อสื่อสารอิเล็กทรอนิกส์ หรือการติดต่อสื่อสารผ่านสายโทรศัพท์หรือปากเปล่า และ ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 18 มาตรา 2701-2712 การจัดเก็บและการเปิดเผยข้อมูลที่จัดเก็บไว้ซึ่งข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์หรือผ่านสายสัญญาณ ของสหรัฐอเมริกา และการกำหนดเป็นหลักการไว้ในอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2011

ด้วยเหตุดังกล่าวข้างต้นแม้ประเทศไทยจะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้สามารถใช้บังคับกับการกระทำความผิดต่าง ๆ เกี่ยวกับคอมพิวเตอร์ ซึ่งมีลักษณะในการจัดเก็บพยานหลักฐานและการสืบสวนได้มาซึ่งพยานหลักฐานแตกต่างจากการกระทำความผิดทั่วไป แต่กฎหมายไทยมิได้นำเรื่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาเชื่อมโยงและปรับใช้สำหรับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตโดยให้ถือว่าเป็นส่วนหนึ่งของการกระทำความผิดบนคอมพิวเตอร์ดังเช่นสภายุโรปและสหรัฐอเมริกาได้วางหลักไว้ จึงส่งผลให้กระบวนการในการสืบสวนเพื่อได้มาซึ่งพยานหลักฐานข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตไม่สามารถกระทำได้ดังเช่นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนั้น หากประเทศไทยแก้ไขเพิ่มเติมให้การละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นการกระทำอย่างหนึ่งตามความผิดของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็อาจทำให้ปัญหาเกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่หมดไปได้

4.1.2 ปัญหาวิธีการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ของพนักงานเจ้าหน้าที่

จากการสัมภาษณ์ผู้จัดการฝ่ายงานความมั่นคงข้อมูลสารสนเทศของผู้ให้บริการอินเทอร์เน็ตพร้อมโทรศัพท์เคลื่อนที่รายหนึ่งซึ่งมีตำแหน่งหน้าที่เกี่ยวข้องกับการรวบรวมและส่งมอบข้อมูลจราจรทางคอมพิวเตอร์ซึ่งจัดเก็บไว้ให้แก่พนักงานเจ้าหน้าที่ และจากการสัมภาษณ์ พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 เมื่อวันที่ 2 มีนาคม 2557 พบว่า เมื่อเกิดกรณีต้องทำการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ พนักงานเจ้าหน้าที่จะดำเนินการโดยการทำหนังสือแจ้งมายังผู้ใช้บริการว่าต้องการทราบข้อมูลจราจรทางคอมพิวเตอร์ในส่วนใด เช่น ต้องการทราบไอพีแอดเดรส วันหรือเวลาในการเชื่อมต่ออินเทอร์เน็ต หรือที่มาว่ามากจากที่อยู่ใด บริษัทใด ผู้ใช้บริการคนใด และมีการตอบรับจากผู้รับการสื่อสารทางอิเล็กทรอนิกส์นั้นหรือไม่ เมื่อได้จดหมายฉบับนี้แล้ว ทางผู้ประสานงานของผู้ให้บริการซึ่งมีหน้าที่ตรวจสอบข้อมูล ก็จะดำเนินการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ที่ได้จัดเก็บไว้ในระบบ เมื่อพบข้อมูลที่ต้องการแล้วก็ดำเนินการแปลงค่าข้อมูล และบันทึกข้อมูลดังกล่าวจัดทำเป็นเอกสารตอบกลับพนักงานเจ้าหน้าที่ว่าข้อมูลที่ตรวจสอบเป็นเช่นไร

โดยในส่วนของพนักงานเจ้าหน้าที่เมื่อได้รับข้อมูลมาในรูปแบบเอกสาร ก็ยึดถือเอกสารที่ได้รับการตรวจสอบจากผู้ให้บริการเป็นหลักฐานที่น่าเชื่อถือ โดยยึดหลักการว่าผู้ให้บริการย่อมมีการประกอบวิชาชีพที่ดีในการปฏิบัติตามกฎหมายเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยจะไม่น่าจะเกิดความผิดพลาดในกระบวนการจัดเก็บหรือการตรวจสอบข้อมูลขึ้นได้ พนักงานเจ้าหน้าที่จึงไม่ได้เข้าไปดูข้อมูลจากฐานข้อมูลของผู้ให้บริการเองโดยไม่จำเป็นซึ่งอาจกล่าวได้ว่าข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานบอกเล่าที่ได้มาจากการคัดลอกข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้อีกทอดหนึ่ง ดังนั้นย่อมอาจมีข้อสงสัยในขั้นตอนระหว่างการคัดลอกตั้งแต่ต้นว่ามีการคัดลอกที่ถูกต้องตรงกันจริงหรือไม่ก่อนการนำส่งให้แก่พนักงานเจ้าหน้าที่ และเอกสารที่คัดลอกมานั้นจะมีความน่าเชื่อถือเพียงใดเนื่องจากข้อมูลจราจรทางคอมพิวเตอร์และลักษณะการจัดเก็บ ด้วยลักษณะของการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวข้างต้นประกอบกับปัจจุบันยังไม่มีกฎหมายกำหนดขั้นตอนในรายละเอียดเกี่ยวกับการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ จึงมีประเด็นที่ต้องพิจารณาเกี่ยวกับการได้มาดังต่อไปนี้

1) ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลที่เกิดขึ้นจากระบบคอมพิวเตอร์ซึ่งมีการประมวลผลแล้วจัดเก็บไว้ทันที ทำให้ความถูกต้องแท้จริงของข้อมูลดังกล่าวมีอยู่ แต่ความน่าเชื่อถือนั้นจะลดลงเมื่อมีบุคคลเข้าไปเกี่ยวข้องกับข้อมูล ตั้งแต่กระบวนการประมวลผลข้อมูล แล้วทำการคัดลอกข้อมูล ซึ่งจะต้องมีการพิสูจน์ความน่าเชื่อถือของการปฏิบัติงานดังกล่าว ไม่ใช่พิสูจน์การเกิดของข้อมูลจราจรทางคอมพิวเตอร์ว่าเกิดขึ้นจริงหรือไม่

2) การที่พนักงานเจ้าหน้าที่ขอข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ และได้รับข้อมูลดังกล่าวแล้วนั้น พนักงานเจ้าหน้าที่ไม่อาจทราบได้ว่ากระบวนการจัดเก็บของผู้ให้บริการที่ตนขอข้อมูลดังกล่าวมีมาตรฐานในการจัดเก็บดังที่กฎหมายต้องการหรือไม่ เมื่อผู้ให้บริการได้รับการร้องขอจากพนักงานเจ้าหน้าที่ ก็จะมีการทำเรื่องไปถึงฝ่ายวิศกรรมที่เก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อให้ได้ข้อมูลดังกล่าวมา โดยฝ่ายวิศกรรมของผู้ให้บริการบางรายมีสิทธิเรียกข้อมูลดังกล่าวขึ้นมาดูเองได้โดยตรง และเมื่อได้ข้อมูลแล้วจึงคัดลอกส่งให้แก่ฝ่ายประสานงานตอบกลับเป็นหนังสือไปยังพนักงานเจ้าหน้าที่ ซึ่งเมื่อต้องการใช้ข้อมูลดังกล่าวก็ทำประสานงานเจ้าหน้าที่ทางเทคนิคเพื่อมาเบิกความประกอบให้ว่าได้คัดลอกโดยถูกต้อง ทั้งนี้ โดยไม่มีมาตรฐานยืนยันหลักการปฏิบัติงานที่เป็นกลางของรัฐในการเปรียบเทียบมาตรฐานและระบบการจัดการของผู้ให้บริการว่ามีความถูกต้องแท้จริงหรือไม่ ซึ่งหากมีข้อโต้แย้งเรื่องความถูกต้องแท้จริงหรือโต้แย้งเรื่องกระบวนการจัดเก็บ ก็จะเป็นปัญหาในการพิสูจน์ความถูกต้องแท้จริงได้

3) พนักงานเจ้าหน้าที่ให้ความเห็นว่าข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการส่งมอบให้นั้นเป็นข้อมูลที่ถูกต้องแล้วเนื่องจากผู้ให้บริการย่อมต้องปฏิบัติหน้าที่ตามกฎหมายเกี่ยวกับการเก็บรักษาข้อมูลคอมพิวเตอร์ไว้โดยป้องกันการเข้าถึงและการแก้ไขรวมทั้งคงไว้ซึ่งความถูกต้องแท้จริง

ของข้อมูล ซึ่งหากข้อเท็จจริงปรากฏภายหลังว่าข้อมูลที่พนักงานเจ้าหน้าที่ได้รับมีความผิดพลาดหรือไม่ถูกต้องตามความจริง ก็จะส่งผลให้เนื้อหาการสืบสวนต่างๆเปลี่ยนแปลงไปและอาจเกิดความเสียหายแก่ผู้ที่ถูกจับตัวผิด หรือสอบสวนผิดได้ ซึ่งผู้ให้บริการจะต้องรับผิดชอบจากข้อมูลที่ผิดดังกล่าว จึงทำให้พักงานเจ้าหน้าที่มีพื้นฐานในการเชื่อว่าผู้ให้บริการย่อมระมัดระวังตนในการปฏิบัติตามกฎหมาย อย่างไรก็ตามจากความเชื่อดังกล่าวส่งผลให้บางครั้งเมื่อข้อมูลที่ได้รับมาผิดพลาดย่อมไม่สามารถรู้หรือตรวจสอบการจัดเก็บของผู้ให้บริการอย่างมีระบบก่อน แต่ต้องรอให้เกิดปัญหาแล้วจึงจะมาตรวจสอบภายหลัง เช่นนี้ย่อมส่งผลเสียต่อทั้งผู้บริสุทธิ์ อีกทั้งยังไม่สามารถจับตัวผู้กระทำความผิดที่แท้จริงได้ ทำให้เกิดข้อบกพร่องในกระบวนการยุติธรรมขึ้นได้

4) ในกระบวนการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ พนักงานเจ้าหน้าที่จะได้รับเพียงเอกสารตอบจากผู้ให้บริการเกี่ยวกับข้อมูลที่ร้องขอไปเท่านั้น โดยผู้ให้บริการไม่จำเป็นต้องให้ข้อมูลอื่นๆเนื่องจากเป็นข้อมูลส่วนบุคคลของผู้ใช้บริการ ซึ่งทำให้ข้อมูลที่ได้รับขาดบริบทประกอบคือข้อมูลจราจรทางคอมพิวเตอร์ใกล้เคียง ซึ่งหากได้พิจารณาข้อมูลทั้งหมดอาจจะทำให้ทราบเหตุการณ์กระทำความผิดได้โดยละเอียดมากยิ่งขึ้นเพื่อเห็นความเชื่อมโยงของการกระทำต่าง ๆ

5) กรณีที่ผู้กระทำความผิดมีความชำนาญในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อาจส่งผลให้ยากที่จะพิสูจน์ความน่าเชื่อถือของข้อมูลจราจรทางคอมพิวเตอร์ เพราะพนักงานสอบสวนมิได้เป็นผู้จัดเก็บพยานหลักฐานเองแต่เป็นการขอรวบรวมมาอีกทอดหนึ่ง อันส่งผลต่อความน่าเชื่อถือของข้อมูลจราจรทางคอมพิวเตอร์เมื่อเทียบกับพยานหลักฐานอื่น ๆ ในคดีอาญา

6) ตามบทบัญญัติของกฎหมายพนักงานเจ้าหน้าที่มีอำนาจที่จะขอข้อมูลจราจรทางคอมพิวเตอร์มาเก็บไว้เอง แต่ในทางปฏิบัติไม่มีการเคยใช้อำนาจเช่นนี้ เนื่องจากพนักงานเจ้าหน้าที่ไม่มีอุปกรณ์หรือระบบในการเก็บรักษาข้อมูลดังเช่นที่ผู้ให้บริการมี อีกทั้งภารกิจหลักของพนักงานเจ้าหน้าที่คือการติดตามตัวผู้กระทำความผิด มิใช่การเก็บรักษาและดูแลรักษาข้อมูลโดยตรง ซึ่งต้องถือว่าข้อมูลที่จัดเก็บโดยผู้ให้บริการเป็นข้อมูลที่ถูกต้องแท้จริงแล้ว

เมื่อวิเคราะห์จากข้อมูลที่รวบรวมไว้ย่อมสรุปได้ว่าความน่าเชื่อถือของข้อมูลจราจรทางคอมพิวเตอร์มีน้อยความพยานวัตถุหรือประจักษ์พยาน เพราะอาจมีข้อโต้แย้งเกี่ยวกับกระบวนการจัดเก็บและความถูกต้องในการประมวลผลได้ อย่างไรก็ตามในส่วนของการประมวลผลข้อมูลแล้วคัดลอกข้อมูลนำส่งให้พนักงานเจ้าหน้าที่ พบว่าแม้ข้อมูลจะสามารถแก้ไขเปลี่ยนแปลงได้ แต่เนื่องจากผู้ที่เกี่ยวข้องอาจต้องรับผิดทางอาญาหากมีการแก้ไขเปลี่ยนแปลงข้อมูลดังกล่าว อีกทั้งมีความเป็นไปได้น้อยที่ผู้ใดผู้หนึ่งจะเปลี่ยนแปลงแก้ไขข้อมูลโดยจงใจให้ผู้อื่นได้รับโทษ และกระบวนการยุติธรรมก็เปิดโอกาสที่จำเลยสามารถต่อสู้ในข้อเหล่านี้ได้ ดั้งนั้นข้อมูลจราจรทางคอมพิวเตอร์จะรับฟังเป็นพยานหลักฐานได้มีน้ำหนักเพียงใดจึงขึ้นอยู่กับสภาการณ์ในแต่ละกรณีด้วย แต่ประเด็นที่เป็นปัญหาสำคัญคือมาตรฐานของกระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ว่ามีความถูกต้องและ

ครบถ้วนของข้อมูลหรือไม่เพียงใด เพราะหากไม่มีการจัดเก็บข้อมูลหรือจัดเก็บไว้ไม่ครบถ้วน จะส่งผลต่อการตรวจสอบที่ไม่มีข้อมูลจราจรทางคอมพิวเตอร์ให้สามารถตรวจสอบและสอบสวนต่อไปได้ แม้จะมีการกระทำเกิดขึ้นจริง แต่หากไม่มีหลักฐานว่ามีการกระทำจัดเก็บไว้ก็เสมือนว่าไม่ปรากฏร่องรอยในการกระทำและไม่สามารถสืบหากตัวผู้กระทำความผิดต่อไปได้อย่างไรก็ตาม ประเด็นปัญหาของวิธีการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ยังไม่มีกระบวนการที่เป็นหลักเกณฑ์แน่ชัดอันอาจส่งผลในการพิสูจน์และนำตัวผู้กระทำความผิดมาลงโทษได้

ประเทศสหรัฐอเมริกามีหน่วยงาน NSA ทำหน้าที่เกี่ยวกับการรักษาความมั่นคงของชาติและเพื่อให้สามารถรักษาความมั่นคงไว้ได้ กฎหมายจึงให้อำนาจในการจัดเก็บข้อมูลการติดต่อสื่อสารทั้งหมดรวมทั้งข้อมูลจราจรทางคอมพิวเตอร์บันทึกจัดเก็บไว้โดยหน่วยงานภายในของ NSA เอง แยกต่างหากจากส่วนที่ผู้ให้บริการมีหน้าที่จัดเก็บตามกฎหมายทั่วไป และเมื่อพบว่ามีการกระทำความผิดเกี่ยวกับการก่อการร้าย ก็จะดำเนินการนำดึงข้อมูลที่เกี่ยวข้องกับความสงสัยในการกระทำความผิดดังกล่าวมาพิจารณา และมีการจัดเก็บข้อมูลเพิ่มเติมให้รวมไปถึงการติดต่อสื่อสารด้วยในบางกรณี เมื่อเป็นลักษณะเช่นนี้ การได้มาซึ่งพยานหลักฐานและความถูกต้องจากการจัดเก็บ จึงสามารถควบคุมได้ด้วยตัวหน่วยงานในการใช้ระบบที่มาตรฐานและกระบวนการปฏิบัติงานที่พนักงานเจ้าหน้าที่สามารถเห็นข้อมูลได้โดยตรง ไม่เกิดความคลาดเคลื่อนในการคัดลอกแล้วส่งต่อระหว่างหน่วยงาน แต่เป็นการประมวลผลข้อมูลและนำมาใช้สำหรับพนักงานเจ้าหน้าที่ได้ทันที จึงทำให้ปัญหาในการได้มาซึ่งพยานหลักฐานไม่มีดังเช่นกระบวนการของไทย

4.2 วิเคราะห์ปัญหาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์

4.2.1 ลักษณะเฉพาะของข้อมูลจราจรทางคอมพิวเตอร์กับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1) ข้อมูลจราจรทางคอมพิวเตอร์นั้นไม่ใช่พยานหลักฐานที่เกิดขึ้นเองตามธรรมชาติ ข้อมูลเหล่านั้นเกิดขึ้นและปรากฏขึ้นได้เพราะการกระทำอย่างใดอย่างหนึ่งของมนุษย์ จากเครื่องมือที่เป็นต้นกำเนิดของข้อมูลเหล่านั้น โดยข้อมูลที่ปรากฏขึ้นและจัดเก็บนั้นอาจเกิดจากความจงใจในการหลอกระบบคอมพิวเตอร์ของผู้กระทำที่มีความชำนาญทางเทคนิค หรือมีการแก้ไขเปลี่ยนแปลงให้เข้าใจผิดตั้งแต่การเริ่มสร้างข้อมูลจราจรทางคอมพิวเตอร์ได้ เพราะทุก ๆ จุดของการจัดเก็บและส่งต่อข้อมูลอาจเกิดการถูกแก้ไขเปลี่ยนแปลงโดยไม่อาจตรวจสอบได้ ดังเช่น การใช้เทคนิคที่ซับซ้อนเพื่อหลอกระบบคอมพิวเตอร์ว่าเครื่องที่เชื่อมต่อเป็นเครื่องอื่นแต่ความจริงแล้ว เครื่องที่เชื่อมต่อเป็นอีกเครื่องหนึ่งเป็นต้น ซึ่งสิ่งเหล่านี้ต้องมีระบบที่ใช้ในการป้องกันและตรวจสอบให้พบตั้งแต่ขั้นตอนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้มั่นใจได้ว่าข้อมูลที่จัดเก็บมีความถูกต้องแท้จริง สำหรับการใช้เป็นหลักฐานการกระทำต่อไปในอนาคตได้

2) ข้อมูลจราจรทางคอมพิวเตอร์เป็นข้อมูลที่จัดเก็บจากบันทึกการทำงานของอุปกรณ์ทางคอมพิวเตอร์ เช่น RADIUS (RADIUS คือ อุปกรณ์ที่ใช้สำหรับตรวจสอบรายชื่อผู้ใช้ก่อนที่จะเข้าใช้เครือข่ายอินเทอร์เน็ต) เว็บเซิร์ฟเวอร์ หรือพร็อกซี่เซิร์ฟเวอร์ เป็นต้น ซึ่งอุปกรณ์เหล่านี้จะจัดเก็บข้อมูลตามคำสั่งที่ได้รับการตั้งค่าไว้ว่าต้องการจะจัดเก็บอะไรบ้าง และเมื่อจัดเก็บเสร็จแล้วก็จะมาอยู่ในรูปของแฟ้มข้อมูลคอมพิวเตอร์ เช่นเดียวกับแฟ้มข้อมูลที่เราใช้อยู่ในปัจจุบัน ซึ่งมีลักษณะที่สามารถเข้าถึง เปิดอ่าน และสามารถแก้ไขหรือเพิ่มเติมข้อความได้ ซึ่งอาจเกิดความคลาดเคลื่อนและไม่ถูกต้องของข้อมูลได้ในขั้นตอนนี้ เช่น หากมีแฟ้มข้อมูลมาและอ้างว่าเป็นข้อมูลที่เป็นบันทำการทำงานของ RADIUS ซึ่งในทางเทคนิคก็ไม่อาจยืนยันได้ว่า แฟ้มข้อมูลดังกล่าวเป็นบันทึกของ RADIUS จริง และเนื้อหาในแฟ้มนั้น เกิดจาก RADIUS จริง เพราะการทำปลอมแฟ้มข้อมูลดังกล่าวสามารถกระทำได้โดยง่าย และไม่ต้องใช้เครื่องมือที่สลับซับซ้อนแต่อย่างใด เมื่อแก้ไขเสร็จแล้วก็ยากที่จะรู้ได้ว่า มีการแก้ไขจากข้อมูลดั้งเดิมที่ไหนอย่างไรเป็นต้น ซึ่งการกระทำเช่นนี้สามารถป้องกันได้ด้วยระบบการรักษาความปลอดภัยของข้อมูลไม่ให้มีการแก้ไขเปลี่ยนแปลง ซึ่งเป็นสิ่งที่กฎหมายได้กำหนดไว้ว่าผู้ให้บริการซึ่งมีหน้าที่จัดเก็บข้อมูลดังกล่าวจะต้องจัดให้มีขึ้น

3) ข้อมูลจราจรทางคอมพิวเตอร์มีความน่าเชื่อถือน้อยกว่าพยานหลักฐานในลักษณะของพยานวัตถุและพยานเอกสารอื่น โดยมีลักษณะคล้ายพยานบอกเล่าทำให้ในการพิจารณาไม่สามารถพิจารณาตัวข้อมูลได้โดยลำพังแต่ต้องอาศัยการพิจารณาถึงกระบวนการจัดเก็บและการรักษาความปลอดภัยในการจัดเก็บข้อมูลดังกล่าวว่ามีความถูกต้องหรือมีการแก้ไขเปลี่ยนแปลงหรือไม่อย่างไร โดยเมื่อผู้ให้บริการไม่มีประโยชน์ได้เสียเกี่ยวกับการจัดเก็บข้อมูล จึงไม่มีแรงจูงใจในการสร้างหลักฐานเพื่อใส่ความผู้ใด อีกทั้งการจัดเก็บเป็นการทำตามหน้าที่โดยจัดเก็บข้อมูลของผู้ใช้บริการทุกคน ไม่มีการเลือกปฏิบัติ ดังนั้น จึงสันนิษฐานได้ว่าข้อมูลนั้นได้มาโดยถูกต้องแล้ว แต่อย่างไรก็ตามหากเกิดการโต้แย้งเกี่ยวกับความถูกต้องดังกล่าว ก็มีความจำเป็นที่ผู้ให้บริการจะต้องพิสูจน์ถึงลักษณะการจัดเก็บของตนว่ามีความถูกต้องแท้จริงเพียงใด ทั้งนี้ หากเป็นลักษณะเช่นนี้ในทุกกรณีย่อมจะเกิดภาระแก่ผู้ให้บริการในพิสูจน์ทุกครั้ง โดยไม่ได้มีมาตรฐานในการเปรียบเทียบการจัดเก็บหรือมาตรฐานรับรองที่ให้ไว้ยืนยันว่าการจัดเก็บของผู้ให้บริการมีความถูกต้องแท้จริงมาเป็นข้อสันนิษฐานเพื่อส่งผลไปยังผู้ถูกกล่าวหาที่จะต้องพิสูจน์ความไม่ถูกต้องดังกล่าวที่เกิดขึ้น มิใช่เพียงการโต้แย้งให้อำนาจพิสูจน์มาตกอยู่แก่ผู้จัดเก็บข้อมูลแต่อย่างใด

4) ข้อมูลจราจรทางคอมพิวเตอร์แม้เป็นพยานหลักฐานที่กฎหมายยอมรับให้นำไปใช้ได้แต่ยังไม่ปรากฏแน่ชัดว่าเป็นพยานหลักฐานประเภทใด จะเป็นพยานเอกสาร หรือพยานวัตถุ หรือพยานหลักฐานในรูปแบบใหม่คือพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งกฎหมายยังไม่เคยมีการนิยามไว้อย่างชัดเจน ปัจจุบันจึงเป็นการนำพยานดังกล่าวมาปรับใช้ในลักษณะว่าจะเป็นพยานเอกสารหรือพยานวัตถุแล้วแต่กรณี ซึ่งในทางปฏิบัติการนำส่งพยานหลักฐานนี้จึงมีความแตกต่างกันไปแล้วแต่การ

ปรับใช้ มิได้มีหลักเกณฑ์เกี่ยวกับพยานข้อมูลจราจรทางคอมพิวเตอร์ หรือพยานอิเล็กทรอนิกส์สำหรับกระบวนการนำไปใช้เป็นการเฉพาะ

วิเคราะห์โดยสรุปเกี่ยวกับลักษณะเฉพาะของข้อมูลจราจรทางคอมพิวเตอร์คือ ข้อมูลจราจรทางคอมพิวเตอร์มีประเด็นให้เกิดความสงสัยในเรื่องความน่าเชื่อถือในกระบวนการเกิดขึ้นของข้อมูล และการจัดเก็บข้อมูล และวิธีนำข้อมูลมาใช้ประกอบเป็นพยานหลักฐาน โดยความน่าเชื่อถือจะสามารถเกิดขึ้นได้ด้วยระบบการป้องกันและตรวจสอบการปลอมแปลงข้อมูลในการเกิดขึ้นของข้อมูลจราจรทางคอมพิวเตอร์และระบบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่มีความถูกต้องแท้จริงให้ไม่สามารถเข้าถึงข้อมูลเพื่อแก้ไขข้อมูลดังกล่าวได้โดยผู้ไม่เกี่ยวข้อง ซึ่งในปัจจุบันประเด็นเรื่องความน่าเชื่อถือยังไม่ปรากฏเป็นประเด็นโต้แย้งให้ต้องพิสูจน์กันมาก แต่ปัญหาดังกล่าวยังคงอยู่เพียงแต่มิได้มีการกล่าวขึ้นมาเป็นประเด็นกันเท่านั้นเพราะเป็นเรื่องทางเทคนิคที่จะต้องมีความรู้ในประเด็นความถูกต้องแท้จริงของข้อมูลจราจรทางคอมพิวเตอร์พอสมควรจึงจะสามารถโต้แย้งได้อย่างมีเหตุผลประกอบ ทั้งนี้ ด้วยลักษณะที่สามารถแก้ไขเปลี่ยนแปลงได้ง่ายนี้เอง ข้อมูลจราจรทางคอมพิวเตอร์จึงต้องมีกระบวนการจัดเก็บที่มีมาตรฐานเดียวกันเพื่อให้สามารถมีข้อมูลในการสืบสวนหาต้นตอของการกระทำได้ในทุกๆครั้งที่ต้องการ และมีความถูกต้องแท้จริงด้วย

4.2.2 ปัญหามาตรฐานในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต

1) กฎหมายได้กำหนดหลักเกณฑ์เบื้องต้นในการปฏิบัติของผู้มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้แล้วว่าผู้ให้บริการประเภทใดต้องจัดเก็บข้อมูลแบบใด และวิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์จะต้องให้ได้ผลลัพธ์อย่างไรบ้าง คือ มีความถูกต้องแท้จริง ไม่เกิดการแก้ไขเปลี่ยนแปลง และมีระบบรักษาความปลอดภัยของข้อมูลที่จัดเก็บ มีการจำกัดการเข้าถึงข้อมูลที่จัดเก็บไว้ และมีการกำหนดให้มีผู้ประสานงานกับหน่วยงานที่เกี่ยวข้อง จึงทำให้ผู้ให้บริการไม่ว่ารายใหญ่หรือเล็กสามารถปฏิบัติตามได้ตามสมควร แต่อย่างไรก็ตาม สิ่งสำคัญของการกำหนดหลักเกณฑ์ดังกล่าวคือหน่วยงานหรือองค์กรตรวจสอบความถูกต้องแท้จริง ซึ่งไม่มีปรากฏในกฎหมายที่จะให้มีการตรวจสอบได้โดยหน่วยงานใด เพื่อรับรองและวัดมาตรฐานการจัดเก็บของผู้ให้บริการแต่ละรายว่าเป็นไปตามกฎหมายกำหนดหรือไม่ ทำให้เมื่อมีการนำข้อมูลมาใช้เกิดปัญหาต่อความไม่มั่นใจในกระบวนการจัดเก็บของผู้ใช้บริการแต่ละรายได้

อนึ่ง ข้อมูลจราจรทางคอมพิวเตอร์ส่วนมากที่มีการร้องขอจะเป็นการขอจากผู้ให้บริการรายใหญ่เป็นส่วนใหญ่ เพราะผู้ให้บริการโครงข่ายอินเทอร์เน็ตจะต้องมีทุนมากในการให้บริการจึงเป็นผู้ให้บริการรายใหญ่เกือบทั้งหมด ซึ่งมาตรฐานการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ขององค์กรใหญ่ย่อมมีความน่าเชื่อถือได้ว่าจะปฏิบัติได้ดี ทำให้เมื่อมีการร้องขอแล้วสามารถเรียกขอข้อมูลจราจรทางคอมพิวเตอร์ได้โดยไม่ติดขัด อย่างไรก็ตาม การเชื่อและปฏิบัติไม่ใช่

มาตรฐานที่จะรับรองได้อย่างเป็นทางการว่าผู้ให้บริการรายใหญ่ดังกล่าวมีมาตรฐานการจัดเก็บตามที่กฎหมายกำหนด ส่งผลให้ในการนำพยานหลักฐานไปใช้ยังเกิดข้อโต้แย้งในความถูกต้องแท้จริงได้ ทั้งนี้ในส่วนของผู้ให้บริการรายย่อยที่ไม่มีกำลังในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์บางรายอาจเกิดการหลีกเลี่ยงไม่จัดเก็บและทำให้เกิดการขาดช่วงในการสืบสวนทำให้การสืบสวนชะงักได้แม้จะมีข้อมูลของผู้ให้บริการรายใหญ่แล้วก็ตามซึ่งหากเจ้าหน้าที่ตรวจสอบจากการขอข้อมูลแล้วปรากฏว่าไม่มีการจัดเก็บก็อาจมีคำสั่งให้ปรับปรุงแก้ไขให้ดำเนินการตามที่กฎหมายกำหนดได้ แต่ทั้งนี้ในส่วนก่อนหน้านั้นความเสียหายย่อมไม่อาจย้อนกลับไปจัดเก็บเพื่อมาช่วยในเรื่องการสืบสวนได้

2) มาตรฐานในการจัดเก็บข้อมูลของแต่ละผู้ให้บริการย่อมแตกต่างกันไปตามแต่ผู้ให้บริการนั้นๆจะเลือกใช้ ซึ่งช่องโหว่ของมาตรฐานการจัดเก็บของผู้ให้บริการบางรายอาจเกิดขึ้นได้เนื่องจากมาตรฐานที่เลือกใช้มิได้จำเป็นจะต้องถูกเข้ามาตรวจสอบโดยหน่วยงานใดของรัฐ แม้จะมีกฎหมายกำหนดแต่เมื่อไม่มีกระบวนการตรวจสอบ การบังคับใช้ให้เกิดการปฏิบัติตามกฎเป็นไปได้ยาก และเป็นกรณีที่ต้องรอให้เกิดความเสียหายก่อนแล้วจึงจะทราบว่าผู้ให้บริการรายใดมิได้มีการจัดเก็บข้อมูล

นอกจากกรณีที่ไม่มีหน่วยงานตรวจสอบมาตรฐานการจัดเก็บแล้ว เมื่อวิเคราะห์มาตรฐานที่กฎหมายกำหนดพบว่า เป็นเพียงการกำหนดในหลักเกณฑ์แบบกว้างว่าต้องกระทำในลักษณะใด โดยไม่ได้กำหนดให้มีมาตรฐานเปรียบเทียบ หรือมาตรฐานที่จะใช้รับรองว่ามีการจัดเก็บอย่างถูกต้องตามกฎหมายแล้ว และสามารถรักษาความถูกต้องแท้จริงของข้อมูลจราจรทางคอมพิวเตอร์ได้ เช่นกรณีร้านอินเทอร์เน็ตคาเฟ่ที่มีผู้เข้ามาใช้บริการ บางร้านให้มีการลงชื่อเข้าใช้ก่อนใช้บริการเพื่อให้สามารถตรวจสอบได้ แต่ไม่ได้มีการตรวจสอบบัตรประชาชนว่าตรงกับผู้ใช้บริการหรือไม่ ดังนั้นเมื่อมีการตรวจสอบย่อมพบข้อมูลที่ไม่ตรงตามความเป็นจริงได้ เป็นต้น ดังนั้น หากมีมาตรฐานที่เป็นตัววัดถึงความรับผิดชอบของผู้ให้บริการว่าได้มีการจัดเก็บไว้ตามมาตรฐานแล้วรับรองให้ก็จะทำให้เกิดความน่าเชื่อถือและมั่นใจในข้อมูลจราจรทางคอมพิวเตอร์ที่นำมาใช้ประกอบการสืบสวนและเป็นพยานได้ดียิ่งขึ้น

3) กระบวนการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้มีความถูกต้องแท้จริงและครบถ้วนตามกฎหมายนั้นจะต้องมีต้นทุนในการดำเนินการสูงพอสมควร ซึ่งอาจเป็นปัญหาต่อผู้ให้บริการทั้งรายเล็กและรายใหญ่ เนื่องจากแนวโน้มในการใช้งานของผู้บริโภคเพิ่มขึ้นทุกวัน อันเป็นผลให้เกิดการติดต่อสื่อสารกันมากขึ้นและเกิดข้อมูลจราจรทางคอมพิวเตอร์มากยิ่งขึ้น เมื่อต้องจัดเก็บไว้เป็นระยะเวลา 90 วันตามกฎหมาย จึงเกิดเป็นภาระแก่ผู้ให้บริการในการจัดเก็บข้อมูลดังกล่าวและอาจเป็นสาเหตุให้เกิดการหลีกเลี่ยงการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และส่งผลให้ข้อมูลจราจรทางคอมพิวเตอร์จัดเก็บไว้ไม่ครบถ้วนต่อไป

4) ในประเทศสหรัฐอเมริกามีหน่วยงานอิสระที่สร้างแผนสำหรับการบริการจัดการระบบสารสนเทศขององค์กร คือมาตรฐานการจัดการองค์กรสารสนเทศแบบ COBIT 5 ซึ่งวางหลักเกณฑ์เกี่ยวกับการปฏิบัติงานไว้โดยละเอียดว่าต้องมีการบริการจัดการอย่างไร ซึ่งหากมีการนำมาปรับใช้กับผู้มีหน้าที่จัดเก็บมูลจราจรทางคอมพิวเตอร์เพื่อให้การจัดเก็บข้อมูลเป็นไปในทิศทางเดียวกัน โดยมีหลักการ 5 ประการของ COBIT คือ

(1) ตอบสนองความต้องการของผู้มีส่วนได้เสียโดยผู้มีส่วนได้เสียในที่นี้คือผู้ให้บริการที่มีหน้าที่ต้องจัดเก็บข้อมูล พนักงานเจ้าหน้าที่ซึ่งมีหน้าที่รวบรวมข้อมูล ผู้กระทำความผิดที่จะต้องได้รับการติดตามสืบสวนจากข้อมูลดังกล่าวมาใช้เป็นพยานหลักฐาน และผู้ได้รับความเสียหายที่จะใช้ข้อมูลดังกล่าวเป็นหลักฐานในการกล่าวโทษผู้กระทำความผิด เพื่อให้ตอบสนองตามความต้องการของทุกคน ดังนั้นจะต้องมีการบริหารจัดการองค์กรให้ตอบสนองต่อความมีส่วนได้เสียได้ โดยตามหลักปัจจุบันผู้ให้บริการเป็นผู้รับภาระในค่าใช้จ่ายของการจัดเก็บแต่ผู้เดียว แต่ผู้ใช้บริการและพนักงานเจ้าหน้าที่ซึ่งใช้ประโยชน์จากข้อมูลดังกล่าวไม่ได้มีส่วนเสียในการจัดเก็บแต่อย่างใด ดังนั้นเมื่อพิจารณาถึงความมีส่วนได้เสียแล้วจึงนำไปดำเนินการวางแผนการในการปรับใช้บริหารทรัพย์ยากรและหาวิธีการจัดการส่วนได้เสียให้เหมาะสมกับแนวทางการดำเนินการให้เกิดประโยชน์สูงสุดต่อไป

(2) ครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร กล่าวคือหลักในการบริหารจัดการเรื่องความถูกต้องแท้จริงตามที่กฎหมายกำหนดต้องมีการนำมาปรับใช้ให้ครอบคลุมทั้งองค์กร เข้าใจภาพรวมและความสำคัญของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และปฏิบัติตามหน้าที่ของตนอย่างมีประสิทธิภาพ ไม่เข้าถึงข้อมูลที่ตนไม่ได้เกี่ยวข้องหรือเปิดเผยข้อมูลที่ตนมีหน้าที่เกี่ยวข้อง

(3) ประยุกต์ใช้กับกรอบการดำเนินงานที่เป็นหนึ่งเดียว กล่าวคือการนำมาตรฐานการจัดการที่เป็นที่ยอมรับในสากลโลกมาใช้กับการบริหารจัดการองค์กรเพื่อให้เกิดความเป็นหนึ่งเดียวกันในระบบปฏิบัติงานขององค์กรและของสากลซึ่งมีการใช้กันอย่างแพร่หลาย

(4) เอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล กล่าวคือกำหนดตั้งแต่เริ่มนโยบาย วิธีคิด วิธีดำเนินงาน กระประสานงาน วิธีการทำงาน ไปจนถึงการสรุปผล และข้อเสนอแนะสำหรับการปฏิบัติงานครั้งต่อไปให้มีความสอดคล้องเป็นระบบและมีประสิทธิภาพเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และการตรวจสอบการดำเนินการในแต่ละครั้งเพื่อพัฒนาปัจจัยเอื้อต่อไป

(5) แบ่งแยกการดูแลออกจากการบริหารจัดการ กล่าวคือหน่วยงานกำกับดูแลจะเป็นผู้วางแผนการปฏิบัติงานและควบคุมดูแลการปฏิบัติงานให้สามารถตอบสนองต่อผู้มีส่วนได้เสียได้ คือได้ข้อมูลจราจรทางคอมพิวเตอร์ที่มีความถูกต้องแท้จริงและจัดเก็บไว้อย่างครบถ้วน และส่วนการบริหารจัดการคือในภาคส่วนของการดูแลองค์กรโดยภาพรวมเพื่อให้การกำกับดูแลไม่กระทบ

ต่อการบริหารจัดการองค์กร โดยสามารถขับเคลื่อนองค์กรไปได้อย่างมีประสิทธิภาพและเป็นที่น่าเชื่อถือ

5) ทั้งนี้ องค์กรระหว่างประเทศว่าด้วยการมาตรฐาน หรือ ISO (International Organization for Standardization) ได้มีการกำหนดมาตรฐานการจัดเก็บข้อมูลสารสนเทศไว้ ไว้ใน ISO/IEC 27001: 2013 โดยมีรายละเอียดเกี่ยวกับ ระบบบริหารจัดการความมั่นคงสาระสนเทศ (ISMS หรือ Information Security Management System) จำนวน 7 ข้อ และ มาตรการการจัดการความมั่นคงปลอดภัยสำหรับสาระสนเทศ (Control Objective and Control) จำนวน 14 ข้อ ซึ่งมาตรฐานนี้เป็นที่ยอมรับในการนำไปใช้จากทั่วโลก โดยประเทศที่มีการใช้สูงสุดคือ ในปี 2005 คือ ญี่ปุ่น สหรัฐอเมริกา และอินเดีย และในปี 2012 สถิติที่มีการใช้มากที่สุดคือ โรมาเนีย จีน และญี่ปุ่น จะเห็นได้ว่าประเทศดังกล่าวข้างต้นเป็นประเทศที่มีความพัฒนาทางเทคโนโลยีล้ำหน้ามากกว่าประเทศไทยยังคังมีการนำมาตรฐานดังกล่าวไปใช้ สำหรับประเทศไทยอาจมีบางองค์กรที่นำหลักเกณฑ์นี้ไปใช้ในการดูแลความมั่นคงปลอดภัยของข้อมูลในองค์กร แต่หากสามารถนำมาตรฐานดังกล่าวมาใช้กับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้ในผู้ให้บริการทุกราย ก็จะทำให้เกิดแนวปฏิบัติที่เป็นไปในแนวทางเดียวกันและสามารถตรวจสอบพร้อมทั้งรับรองมาตรฐานดังกล่าวได้โดยหน่วยงานตรวจสอบมาตรฐานของ ISO โดยไม่จำเป็นต้องมีการใช้หน่วยงานของรัฐบาลซ้ำซ้อนแต่อย่างใด ก็จะทำให้เกิดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่มีมาตรฐานและเป็นที่ยอมรับในระดับสากล ทำให้สามารถนำข้อมูลจราจรทางคอมพิวเตอร์มาใช้ได้โดยมีความน่าเชื่อถืออีกทั้งสามารถยืนยันได้ว่ามีการจัดเก็บอย่างถูกต้องแท้จริงแล้ว ทำให้กระบวนการยุติสามารถดำเนินการได้รวดเร็วยิ่งขึ้น

ดังนั้น เมื่อวิเคราะห์มาตรฐานการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ของไทยเปรียบเทียบกับของต่างประเทศซึ่งมีการวางมาตรฐานในการบริหารจัดการและมาตรฐานเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศแล้วพบว่า มาตรฐานของกฎหมายไทยที่กำหนดไม่ได้มีการกำหนดประกาศหรือกฎเกณฑ์เพิ่มเติมจะมาเป็นแนวทางปฏิบัติให้แก่ผู้มีหน้าที่ต้องปฏิบัติตาม จึงยังส่งผลให้เกิดการจัดเก็บที่มีรูปแบบแตกต่างกันและไม่สามารถเปรียบเทียบมาตรฐานการจัดเก็บได้ว่าผู้มีหน้าที่ได้ปฏิบัติอย่างเพียงพอแล้วหรือไม่ ส่งผลให้บางครั้งเกิดความบกพร่องในการจัดเก็บสำหรับผู้มีหน้าที่บางรายและส่งผลต่อการสืบสวนหาตัวผู้กระทำความผิด ซึ่งหากมีการนำหลักบริหารจัดการสนสนเทศและมาตรฐานการจัดเก็บข้อมูล ของ ISO มาปรับใช้เป็นต้นแบบในการเปรียบเทียบให้แก่ผู้ใช้บริการที่ต้องปฏิบัติตามและได้รับการรับรองมาตฐาน ก็จะทำให้เกิดการจัดเก็บข้อมูลที่เป็นมาตรฐานเปรียบเทียบได้อีกทั้งยังมีหลักการบริการจัดการองค์กรเกี่ยวกับการจัดเก็บข้อมูลดังกล่าวตามกฎหมายด้วย ซึ่งจะช่วยให้มีข้อมูลจราจรทางคอมพิวเตอร์ที่ครบถ้วนถูกต้องแท้จริงเมื่อมีการร้องขอจากพนักงานเจ้าหน้าที่และมีกระบวนการปฏิบัติงานที่เป็นแนวปฏิบัติเดียวกันทั้งองค์กร และเมื่อปรับใช้กับ

หน่วยงานพนักงานเจ้าหน้าที่ที่เกี่ยวข้อง ก็จะทำให้ระบบทั้งระบบไปจนการนำตัวผู้กระทำความผิดมาลงโทษมีไปในทิศทางเดียวกัน และสามารถตรวจสอบได้ง่ายถึงความถูกต้องของข้อมูลซึ่งนำมาเป็นพยานหลักฐาน

4.2.3 ปัญหาระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้ในการสืบสวนกับภาระของผู้ให้บริการ

เนื่องด้วยลักษณะของข้อมูลจราจรทางคอมพิวเตอร์เกิดขึ้นเพียงชั่วคราวแล้วจะสูญหายไปหากไม่มีการจัดเก็บไว้ ดังนั้น มาตรา 26 วรรคหนึ่ง ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (พระราชบัญญัติ) ได้บัญญัติไว้ว่า “ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้” เพื่อให้พนักงานเจ้าหน้าที่สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้จากผู้ให้บริการเพื่อการสืบสวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้เมื่อพบการกระทำผิดในภายหลัง โดยระยะเวลาการจัดเก็บที่กฎหมายกำหนดคือไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลเข้าสู่ระบบ จึงทำให้มีประเด็นที่ต้องพิจารณาว่าในทางปฏิบัติระยะเวลาเก้าสิบวันเหมาะสมหรือไม่ โดยวิเคราะห์จากข้อมูลการวิจัยและบทสัมภาษณ์ดังนี้

1) จากการสอบถามผู้ให้บริการพบว่า ระยะเวลา 90 วันที่กำหนดไว้ตามกฎหมายไม่เป็นภาระเกินควรแก่ผู้ให้บริการ โดยก่อนมีการตรากฎหมายได้มีการแสดงความเห็นกันอย่างกว้างขวางและได้ข้อยุติเป็นระยะเวลา 90 วัน ทั้งนี้ ค่าใช้จ่ายในส่วนของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวผู้ให้บริการมีหน้าที่ต้องรับผิดชอบ ดังนั้น หากมีการเพิ่มหรือขยายระยะเวลาการจัดเก็บมากกว่า 90 วันอาจส่งผลกระทบต่อภาระค่าใช้จ่ายที่เพิ่มขึ้นมาก เนื่องจากผู้ใช้บริการเพิ่มขึ้นทุกวันและการติดต่อสื่อสารก็มีมากยิ่งขึ้นและทำให้ผู้ให้บริการอาจต้องผลักภาระในหน้าที่ดังกล่าวไปสู่ผู้ใช้บริการทำให้เกิดค่าใช้จ่ายในการใช้บริการมากยิ่งขึ้น

2) สำหรับความเห็นของพนักงานเจ้าหน้าที่พบว่า ระยะเวลาในการจัดเก็บข้อมูลจราจรทางคอมิพวเตอร์ควรจะมีการกำหนดให้จัดไว้นานที่สุดเท่าที่จะสามารถทำได้เพราะจะเป็นผลดีต่อการสืบสวนคดี เนื่องจากบางครั้ง กว่าจะทราบว่ามีการกระทำความผิดเกิดขึ้นหรือมีการแจ้งความหรือกว่าจะรู้ว่าควรต้องการข้อมูลส่วนไหนและใครเป็นผู้รับผิดชอบ อาจไม่สามารถรู้ถึงการกระทำความผิดนั้นได้ภายใน 90 วัน ส่งผลให้เมื่อทราบถึงการกระทำความผิดหลังระยะเวลาดังกล่าวจะไม่มีข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บไว้โดยผู้ให้บริการแล้ว ทำให้เกิดอุปสรรคในการสืบสวนหาตัวผู้กระทำความผิดไม่สามารถกระทำต่อได้ แม้จะเป็นคดีเกี่ยวกับกับความมั่นคงของชาติ ซึ่งกฎหมายกำหนดให้เจ้าพนักงานสามารถสั่งให้เก็บข้อมูลไว้ได้เกินกว่า 90 วัน แต่ในทางปฏิบัติก็ต้องอยู่ใน

เงื่อนไขที่ว่า พนักงานเจ้าหน้าที่ได้ทราบถึงคดีความมั่นคงนั้นก่อนจะครบระยะเวลา 90 วันอีกทั้งในส่วนขั้นตอนที่ต้องส่งสำนวนให้แก่พนักงานอัยการพบว่าระยะเวลาเพียง 90 วันในการสืบสวนของพนักงานสอบสวนและส่งสำนานให้แก่พนักงานอัยการพิจารณาว่าควรเรียกพยานหลักฐานเพิ่มเติมหรือไม่ เป็นระยะเวลาที่กระชั้นชิดมากและอาจไม่เพียงพอต่อการพิจารณาหรือกระบวนการอาจยังมาไม่ถึงการพิจารณาของพนักงานอัยการ เนื่องจากคดีความผิดเกี่ยวกับคอมพิวเตอร์เป็นคดีที่มีความซับซ้อนและต้องใช้ความชำนาญพิเศษเฉพาะด้าน จึงต้องใช้เวลามากกว่าการสืบสวนปกติ ย่อมทำให้โอกาสที่พนักงานอัยการจะสามารถขอให้พนักงานสอบสวนหาพยานหลักฐานจากข้อมูลจราจรทางคอมพิวเตอร์เพิ่มเติมนั้นเป็นไปได้ยาก

3) เมื่อพิจารณาถึงในชั้นร่างพระราชบัญญัติพบว่าระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นประเด็นหนึ่งที่มีการถกเถียงกันว่าควรจะมีระยะเวลาการจัดเก็บเท่าใดดี เพื่อมิให้กระทบต่อภาระของผู้ให้บริการมากเกินไปและเพื่อไม่ให้กระทบต่อกระบวนการสืบสวนหาตัวผู้กระทำความผิดเกี่ยวกับการได้มาซึ่งพยานหลัฐาน และได้ข้อสรุปที่ 90 วัน โดยในขณะนั้นคาดว่าเพียงพอในการจัดเก็บเพื่อสามารถเรียกใช้เป็นพยานหลักฐานและไม่เป็นภาระแก่ผู้ให้บริการมากจนเกินไป อีกทั้งข้อ อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ข้อ 16 ได้กำหนดระยะเวลาในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้จัดเก็บเป็นระยะเวลา 90 วันเช่นกัน แต่ต่อมาในปี ค.ศ. 2006 ได้มีการเปลี่ยนแปลงกฎระเบียบเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ระหว่างประเทศของสภายุโรปตามบทบัญญัติ Directive 2006/24/EC ของรัฐสภายุโรปและสภา 15 มีนาคม ค.ศ. 2006 เกี่ยวกับการเก็บรักษาข้อมูลที่สร้างหรือประมวลผลในการเชื่อมต่อกับบทบัญญัติของประเทศชาติที่มีบริการการสื่อสารอิเล็กทรอนิกส์หรือของเครือข่ายการสื่อสารสาธารณะและการแก้ Directive 2006/24/EC กำหนดให้ข้อมูลบางประเภทต้องจัดเก็บไว้เป็นระยะเวลาอย่างน้อย 6 เดือน ซึ่งข้อมูลประเภทต่างๆที่กำหนดไว้เป็นลักษณะของข้อมูลจราจรทางคอมพิวเตอร์ทั้งหมด จึงอาจกล่าวได้ว่า ปัจจุบันสภายุโรปมีการกำหนดให้ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้เป็นระยะเวลาอย่างน้อย 6 เดือน เพื่อเป็นการให้ความสำคัญแก่ข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลระบุที่อยู่เพื่อใช้ในการสืบสวน การค้นหา และการดำเนินคดีทางอาญา เนื่องจากการทำวิจัยและการปฏิบัติจริงของประเทศสมาชิกทั้งหลายพบว่ามีความจำเป็นที่จะต้องมั่นใจว่าข้อมูลดังกล่าวซึ่งเกิดขึ้นจากกระบวนการติดต่อสื่อสารจะต้องจัดให้มีการเก็บไว้เป็นระยะเวลาอย่างน้อย 6 เดือน

4) สำหรับกฎหมายอาชญากรรมทางคอมพิวเตอร์ของสหรัฐอเมริการกำหนดให้ระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ต้องมีการจัดเก็บไว้อย่างน้อย 90 วัน และอาจมีการขยายระยะเวลาการจัดเก็บเพิ่มขึ้นหากหน่วยงานราชการร้องขอตาม ประมวลกฎหมายอาญาและวิธีพิจารณาความอาญา บทที่ 18 ส่วนที่ 121 มาตรา 2703 ทั้งนี้ในส่วนของภาระของผู้ให้บริการที่

เพิ่มขึ้นจากการจัดเก็บข้อมูลที่เกินกว่า 90 วัน หน่วยงานที่ร้องขอจะต้องเป็นผู้ชดเชยค่าใช้จ่ายให้แก่ผู้ให้บริการ ซึ่งทำให้ผู้ให้บริการไม่ต้องรับภาระในส่วนที่เกินกว่าหน้าที่ปกติที่กฎหมายกำหนด และก็เป็นการสมประโยชน์หน่วยงานที่ต้องการข้อมูลซึ่งเป็นผู้ใช้ข้อมูลจึงต้องเสียค่าใช้จ่ายเพื่อให้ได้ข้อมูลที่ให้จัดเก็บเป็นระยะเวลาเพิ่มขึ้น

5) ในสหรัฐอเมริการนอกจากผู้ให้บริการเป็นผู้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แล้วหน่วยงานความมั่นคงของสหรัฐอเมริการ หรือ NSA ยังเป็นหน่วยงานหลักอีกหน่วยงานหนึ่งที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่มีการติดต่อสื่อสารผ่านมายังสหรัฐอเมริกาทั้งหมด โดยจัดเก็บไว้ด้วยหน่วยงานกลางโดยใช้งบประมาณของรัฐบาลกลางในการจัดเก็บเพื่อประโยชน์ในการคุ้มครองความมั่นคงของประเทศให้มีความมั่นคงปลอดภัย โดยระยะเวลาการจัดเก็บข้อมูลของหน่วยงาน NSA คือจัดเก็บไว้เป็นระยะเวลา 5 ปี เพื่อให้สามารถรวบรวมพยานหลักฐานได้ทุกอย่างที่ต้องการโดยไม่มีเรื่องของการสูญหายไปซึ่งข้อมูลแต่อย่างใด ดังนั้น จึงไม่จำเป็นที่หน่วยงานความมั่นคงของรัฐจะต้องขอข้อมูลจากผู้ให้บริการอีกเมื่อมีการจัดเก็บไว้ด้วยตนเองแล้ว ทำให้เรื่องระยะเวลาการจัดเก็บเพียง 90 วันของผู้ให้บริการไม่กระทบต่อคดีความมั่นคงและคดีร้ายแรงอื่น ๆ ของประเทศที่จะสามารถขอข้อมูลจากหน่วยงาน NSA เพื่อนำไปใช้ในการป้องกันผลประโยชน์ของประเทศได้

เมื่อวิเคราะห์ถึงปัญหาระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์แล้วย่อมพบว่าหากต้องการให้การสืบสวนสอบสวนสามารถครอบคลุมการกระทำความผิดทุกกรณีก็จะต้องมีการกำหนดให้มีการจัดเก็บข้อมูลไว้เป็นระยะเวลานาน อย่างเช่นหน่วยงาน NSA ของสหรัฐอเมริกา แต่ปัญหาเรื่องการจัดเก็บเป็นระยะเวลานานคือภาระค่าใช้จ่ายของการจัดเก็บข้อมูลดังกล่าวมีภาระที่สูงมากขึ้นกับระยะเวลาจัดเก็บที่เพิ่มขึ้น ซึ่งในกรณีปกติของสหรัฐอเมริกได้มีการแก้ไขปัญหานี้โดยเมื่อต้องการให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการเกินกว่า 90 วันตามปกติจะต้องมีการชดเชยค่าใช้จ่ายที่เกิดขึ้นโดยหน่วยงานที่ร้องขอเป็นผู้จ่าย อย่างไรก็ตามการกำหนดให้มีการร้องขอให้ขยายระยะเวลาก็ยังมีประเด็นปัญหาเรื่องหากไม่พบการกระทำความผิดก่อนระยะเวลาปกติที่กฎหมายกำหนดก็ย่อมไม่สามารถขอให้ขยายระยะเวลาได้ ดังนั้น ทางที่น่าจะเหมาะสมที่สุดคือการค้นหาความสมดุลระหว่างการสืบสวนซึ่งเป็นประโยชน์แก่รัฐและสังคมกับภาระหน้าที่ซึ่งผู้ให้บริการเอกชนจะต้องแบกรับ เพื่อให้เกิดความเต็มใจในการจัดเก็บและไม่หลีกเหลี่ยงการจัดเก็บ ทั้งนี้ ปัจจุบันกรณีที่สภายุโรปได้กำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นระยะเวลา 6 เดือน ก็ด้วยมีการทำวิจัยแล้วพบว่าจะต้องใช้ระยะเวลาในการจัดเก็บอย่างน้อย 6 เดือนจึงจะเหมาะสมและสามารถรวบรวมพยานหลักฐานข้อมูลจราจรทางคอมพิวเตอร์ที่สำคัญต่าง ๆ ได้ทัน ซึ่งสำหรับประเทศไทยยังไม่ปรากฏว่ามีการทำวิจัยเกี่ยวกับกระบวนการเปรียบเทียบเรื่องภาระของผู้ให้บริการกับความเหมาะสมในการหาพยานหลักฐานว่าควรใช้ระยะเวลาเท่าใด ทั้งนี้ นอกจากกรณีทั่วไปแล้วในส่วนของความมั่นคงของรัฐในประเทศไทยจะต้องขอข้อมูลผ่านผู้ใช้บริการซึ่งจัดเก็บข้อมูลไว้เป็นระยะเวลา

เพียง 90 วัน ซึ่งทำให้ในเหตุการร้ายแรงที่กระทบต่อความมั่นคงซึ่งมีความซับซ้อนในการสืบสวนหรือกว่าจะทราบถึงการกระทำดังกล่าวได้เกินระยะเวลาอาจส่งผลเสียต่อประเทศชาติได้ หากจะมีการนำวิธีการดังเช่นสหรัฐอเมริกามาใช้โดยการตั้งหน่วยงานกลางเพื่อจัดเก็บข้อมูลก็อาจช่วยให้เกิดความครอบคลุมของการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ได้มากยิ่งขึ้น

ทั้งนี้ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์นั้นเป็นประโยชน์แก่ทุกฝ่ายในสังคม กล่าวคือ ในส่วนของรัฐ หากสามารถปราบปรามการกระทำความผิดได้ก็จะทำให้เกิดเกิดความยุติธรรมภายในประเทศได้มากยิ่งขึ้น และสร้างบรรยากาศที่ดีในการทำธุรกิจเกี่ยวกับระบบคอมพิวเตอร์ส่งผลให้เศรษฐกิจขยายตัว และสร้างความเชื่อมั่นแก่นักลงทุน และสอดคล้องกับทิศทางเศรษฐกิจโลกที่อยู่บนพื้นฐานของเทคโนโลยีสารสนเทศ ในส่วนของผู้ให้บริการ เมื่อมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์อย่างถูกต้องสามารถตรวจสอบได้ก็จะเกิดความเชื่อมั่นในการให้บริการของผู้ให้บริการรายนั้นและในส่วนของประชาชนก็จะมีความเชื่อมั่นในการใช้งานว่าจะได้รับความคุ้มครองจากการกระทำความผิดได้อย่างมีประสิทธิภาพดังนั้น หากสามารถบริหารความรับผิดชอบในการจัดเก็บข้อมูลดังกล่าวให้กระจายอย่างทั่วถึงก็จะเป็นการยุติธรรมแก่ทุกฝ่ายและอาจกำหนดระยะเวลาที่เหมาะสมในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ต่อไปได้โดยแบ่งเบาภาระซึ่งทุกฝ่ายมิให้เกิดสภาพการบังคับให้ภาระตกแก่ผู้ให้บริการเพียงฝ่ายเดียว โดยรัฐอาจเข้ามาช่วยเหลือเรื่องค่าใช้จ่ายหรืออาจจะกำหนดระยะเวลาที่คิดว่าไม่กระทบผู้ให้บริการมากแต่สามารถตอบสนองต่อการทำงานจองการสืบสวนของพนักงานสอบสวนหรือพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้

บทที่ 5
บทสรุป และข้อเสนอแนะ

5.1 บทสรุป

5.1.1 บทสรุปปัญหาการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์

ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตลักษณะของการกระทำส่วนใหญ่อยู่บนระบบคอมพิวเตอร์ ส่งผลให้พยานหลักฐานสำคัญที่ใช้ในการสืบสวนสอบสวนคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ตคือ ข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งเป็นข้อมูลที่บอกถึงร่องรอยการกระทำบนอินเทอร์เน็ตว่าคอมพิวเตอร์ที่ส่งข้อมูลต้นทางมาจากไหน และส่งข้อมูลไปที่ไหน เวลาที่ส่งข้อมูลเท่าใด และลักษณะของข้อมูลที่ส่ง และที่กระทำขึ้นเป็นเช่นไร ด้วยพยานหลักฐานนี้จะทำให้พนักงานเจ้าหน้าที่สามารถสืบสวนสอบสวนจากการกระทำความผิดเที่ปรากฏบนอินเทอร์เน็ตสืบต่อไปยังตัวผู้กระทำความผิดต่อไปได้

อย่างไรก็ตาม เนื่องจากข้อมูลจราจรทางคอมพิวเตอร์ เป็นข้อมูลการติดต่อสื่อสารซึ่งกฎหมายให้ความคุ้มครองตามรัฐธรรมนูญและตามการประกอบกิจการโทรคมนาคม พ.ศ. 2544 ที่จะไม่ถูกเปิดเผยหรือถูกละเมิดสิทธิเสรีภาพในการติดต่อสื่อสาร จึงทำให้การได้มาซึ่งข้อมูลดังกล่าวต้องมีกฎหมายให้อำนาจไว้ชัดเจนจึงจะสามารถกระทำได้และทำได้เพียงแต่สมควรแก่กรณีเพื่อไม่เป็นการล่วงละเมิดสิทธิเสรีภาพในการติดต่อสื่อสารของประชาชน โดยปัญหาที่พบสำหรับการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์มีดังนี้

1) ปัญหาเรื่องบทบัญญัติของกฎหมายลิขสิทธิ์และกฎหมายอาญาไม่ได้มีการให้อำนาจไว้เป็นการเฉพาะ

พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 มีการกำหนดโทษทางอาญาสำหรับการละเมิดลิขสิทธิ์ ดังนั้น กระบวนการในการบังคับใช้กฎหมายและการสืบสวนสอบสวนจึงเป็นไปตามประมวลกฎหมายวิธีพิจารณาความทางอาญา อำนาจการสืบสวนสอบสวนเป็นของเจ้าหน้าที่ตำรวจและพนักงานสอบสวนตามประมวลกฎหมายดังกล่าว ซึ่งมีอำนาจในการรวบรวมพยานหลักฐานเพื่อสืบสวนหาตัวผู้กระทำความผิดโดยเร็ว โดยสามารถหมายเรียกเอกสารและหลักฐานที่เกี่ยวข้องกับการกระทำความผิดได้ อย่างไรก็ตาม เนื่องจากข้อมูลจราจรทางคอมพิวเตอร์ เป็นพยานหลักฐานที่เกี่ยวกับการสื่อสาร ซึ่งเป็นสิ่งที่กฎหมายรัฐธรรมนูญให้ความคุ้มครองไว้ไม่ให้มีการละเมิดสิทธิในการติดต่อสื่อสาร เว้นแต่จะมีกฎหมายกำหนดเป็นการเฉพาะ ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดไว้เป็นการเฉพาะแล้วว่าให้มีพนักงานเจ้าหน้าที่ตามพระราชบัญญัติมีอำนาจในการได้มาซึ่งข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์ ดังนั้น เมื่อปรากฏเจ้าหน้าที่ผู้มีอำนาจเฉพาะแล้ว ประมวลกฎหมายวิธิพิจารณาความอาญาซึ่งเป็นกฎหมาย

ทั่วไปจึงไม่สามารถนำมาใช้ได้กับกรณีของข้อมูลจราจรทางคอมพิวเตอร์ เจ้าหน้าที่ตำรวจและพนักงานสอบสวนตามประมวลกฎหมายดังกล่าวจึงไม่มีอำนาจได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ใช้เป็นพยานหลักฐานสำหรับการกระทำความผิดละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้

2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้อำนาจไว้เฉพาะ แต่ไม่รวมถึงความผิดเกี่ยวกับการละเมิดลิขสิทธิ์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้อำนาจแก่พนักงานเจ้าหน้าที่ สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการได้ เพื่อใช้ในการสืบสวนหาตัวผู้กระทำความผิดตามพระราชบัญญัตินี้ จึงทำให้พนักงานเจ้าหน้าที่ไม่สามารถใช้อำนาจดังกล่าวสำหรับกรณีการกระทำความผิดละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้ เนื่องจากไม่ใช่ความผิดตามพระราชบัญญัตินี้ ทั้งนี้ แม้ในทางปฏิบัติมีการนำความผิดตามพระราชบัญญัตินี้บางข้อซึ่งมีลักษณะใกล้เคียงกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตมาปรับใช้แทน แต่การปรับใช้และลงโทษดังกล่าวก็เป็นไปเพื่อการลงโทษความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งไม่สามารถตอบสนองการลงโทษและป้องกันการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตได้ แต่ทั้งนี้ หากจะนำพยานหลักฐานที่ได้มาดังกล่าวไปใช้ในคดีละเมิดลิขสิทธิ์บนอินเทอร์เน็ต ก็จะติดอุปสรรคที่ว่าเป็นพยานหลักฐานที่ได้มาเพื่อใช้สำหรับความผิดทางคอมพิวเตอร์เท่านั้น ไม่สามารถนำมาใช้ในคดีละเมิดลิขสิทธิ์ได้ เพราะวิธีการได้มาเพื่อใช้ในคดีละเมิดลิขสิทธิ์ พนักงานเจ้าหน้าที่ไม่มีอำนาจ การอาศัยอำนาจจากกรณีอื่นให้ได้มา ไม่สามารถนำมาอ้างว่าได้มาโดยถูกต้องและมาอำนาจเพื่อใช้ในคดีละเมิดลิขสิทธิ์ได้แต่อย่างใด

3) กระบวนการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ของพนักงานเจ้าหน้าที่ ไม่สามารถตรวจสอบถึงความถูกต้องของข้อมูลที่คัดลอกโดยผู้ให้บริการ และไม่ได้เห็นถึงข้อมูลต้นฉบับด้วยตนเอง

ด้วยบทบัญญัติของกฎหมายที่ให้พนักงานเจ้าหน้าที่สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์มาใช้เป็นพยานหลักฐานได้ จึงทำให้การได้มาซึ่งข้อมูลจราจรทางคอมพิวแตอร์เป็นไปในลักษณะของหมายเรียกเป็นหนังสือและหนังสือตอบจากผู้ให้บริการเป็นหนังสือ โดยระบุเพียงข้อมูลที่ต้องการโดยการแปลภาษาจากคอมพิวเตอร์แล้วและคัดกรองเฉพาะข้อมูลที่ต้องการเรียบร้อยแล้ว จึงส่งผลให้ ข้อมูลที่พนักงานเจ้าหน้าที่ได้รับ เป็นข้อมูลเดี่ยวที่ต้องการเท่านั้นโดยไม่มีบริบทแวดล้อมซึ่งอาจช่วยเหลือในการสืบสวนหาตัวผู้กระทำความผิดได้แต่พนักงานเจ้าหน้าที่อาจจะไม่เห็นหรืออาจจะคาดไม่ถึงขณะที่มีการขอข้อมูลดังกล่าว ซึ่งต่อมาเมื่อเห็นข้อมูลที่ขอครั้งแรกแล้ว หากต้องการจะขอข้อมูลบริบทเพิ่มเติม อาจจะไม่สามารถขอได้เนื่องจากเกินระยะเวลาการจัดเก็บข้อมูลจำนวน 90 แล้วก็เป็นได้ อีกทั้ง ในกระบวนการนี้หากมีความผิดพลาดในการคัดลอกข้อมูลหรือมีการแก้ไขข้อมูล หรือสร้างข้อมูลขึ้นมาเองโดยผู้ประสานงาน พนักงานเจ้าหน้าที่ย่อมไม่สามารถทราบได้ถึงการแก้ไขดังกล่าว เพราะไม่ได้เห็นถึงต้นฉบับของข้อมูล และไม่มีการตอบกลับที่ส่งมาพร้อมกับต้นร่างของข้อมูล

ที่ยังไม่ได้คัดกรอง ทั้งที่พนักงานเจ้าหน้าที่ซึ่งผ่านการอบรมแล้วมีความสามารถเพียงพอที่จะตีความข้อมูลดังกล่าวได้ด้วยตนเอง

4) ในสหรัฐอเมริกา และสภายุโรปกำหนดให้ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์เป็นความผิดหนึ่งที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ จึงส่งให้การสืบสวนสอบสวนและการจัดเก็บพยานหลักฐานเป็นไปตามกฎหมายอาชญากรรมทางคอมพิวเตอร์ ซึ่งมีกระบวนการให้การดำเนินการแยกต่างหากจากการสืบสวนทั่วไป

ประมวลกฎหมายของสหรัฐอเมริกากำหนดให้ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์เป็นความผิดหนึ่งในหมวดความผิดอาชญากรรมทางคอมพิวเตอร์ โดยกำหนดให้ใช้วิธีการในการสืบสวนสอบสวนเช่นเดียวกับการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ และสำหรับสภายุโรปก็ได้กำหนดให้ความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ครอบคลุมไปถึงความผิดเกี่ยวกับการละเมิดลิขสิทธิ์ด้วย กล่าวได้ว่าเป็นลักษณะเดียวกันกับอเมริกา ซึ่งส่งผลให้ เมื่อเกิดการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตจึ้น กระบวนการในการสืบสวนสอบสวนให้ได้มาซึ่งพยานหลักฐานและการจัดเก็บไว้ซึ่งข้อมูลดังกล่าวจะเป็นไปในทิศทางเดียวกับการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ ซึ่งเจ้าหน้าที่มีความรู้ความเชี่ยวชาญและมีบทบัญญัติเกี่ยวกับการดำเนินการที่ใช้เฉพาะกับอาชญากรรมทางคอมพิวเตอร์ให้สามารถนำมาปรับใช้ได้ จึงไม่เกิดปัญหาเรื่องอำนาจการได้มาซึ่งข้อมูลจราจรทางคออมพิวเตอร์ดังเช่นประเทศไทย

5.1.2 บทสรุปปัญหาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ข้อมูลจราจรทางคอมพิวเตอร์ มีลักษณะเฉพาะที่แตกต่างจากพยานหลักฐานทั่วไป คือเป็นข้อมูลอิเล็กทรอนิกส์ ที่เกิดขึ้นแล้วสูญหายไปหากไม่มีการจัดเก็บไว้ ดังนั้น กฎหมายจึงกำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้เป็นระยะเวลา 90 วัน เพื่อให้พนักงานเจ้าหน้าที่สามารถขอข้อมูลดังกล่าวจากผู้ให้บริการมาใช้ในการสืบสวนหาตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ต่อไปได้ โดยมีการกำหนดวิธีการจัดเก็บไว้ตามประกาศกระทรวงเทคโนโลยีและสารสนเทศเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ พ.ศ. 2550 ว่าต้องมีการจัดเก็บให้สามารถรักษาความถูกต้องแท้จริงและครบถ้วนของข้อมูลจราจรทางคอมพิวเตอร์ และต้องมีการจัดระบบรักษาความปลอดภัยให้ไม่มีการเข้าถึงข้อมูลดังกล่าวเพื่อเปลี่ยนแปลงได้ โดยไม่ได้มีหน่วยงานหรือองค์กรกลางในการตรวจสอบหรือวางมาตรฐานในทางปฏิบัติให้ปฏิบัติตาม โดยบทสรุปจากการศึกษาพบปัญหาของการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังนี้

1) บทบัญญัติเกี่ยวกับการจัดเก็บไม่มีหน่วยงานตรวจสอบและมาตรฐานในการเปรียบเทียบการจัดเก็บตามกฎหมาย

แม้ประกาศกระทรวงเทคโนโลยีและสารสนเทศเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ พ.ศ. 2550 จะกำหนดวิธีการเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ว่า

ต้องมีลักษณะอย่างไร และมีการจัดสรรให้มีสิ่งใดบ้าง แต่ไม่ปรากฏว่ามีการกำหนดให้ต้องมีหน่วยงานตรวจสอบ และไม่ได้มีการกำหนดมาตรฐานในเปรียบเทียบหรือรับรองให้แก่ผู้ให้บริการที่จะสามารถใช้ยืนยันได้ว่าตนได้ปฏิบัติหน้าที่ตามกฎหมายอย่างถูกต้องแล้ว แต่เป็นกรณีที่ต้องมีการตรวจสอบพบเองของพนักงานเจ้าหน้าที่ในกรณีที่ไม่สามารถขอข้อมูลได้ หรือเมื่อได้ข้อมูลแล้วพบว่าไม่ตรงกันกับผู้ให้บริการรายอื่นในกรณีเดียวกันนั้น ซึ่งหากเป็นกรณีที่จัดเก็บโดยผู้ให้บริการรายเดียวก็ย่อมไม่สามารถทราบถึงความผิดพลาดดังกล่าว และอาจเกิดการลงโทษผู้กระทำความผิดผิดคนเนื่องจากการสืบสวนจากพยานหลักฐานที่ไม่ถูกต้องได้ ดังนั้น กล่าวได้ว่า ปัญหาหลักของกระบวนการจัดเก็บคือไม่มีมาตรฐานในการเปรียบเทียบและไม่มีหน่วยงานที่จะช่วยตรวจสอบให้คำแนะนำหรือรับรองได้ว่าการดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการเป็นไปตามที่กฎหมายกำหนดและรักษาความถูกต้องแท้จริงได้ตามเจตนารมย์ของกฎหมายหรือไม่

2) ปัญหาความเหมาะสมของระยะเวลาในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

ผู้ให้บริการมีหน้าที่ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นระยะเวลา 90 วัน โดยเป็นภาระของผู้ให้บริการเองที่ต้องเสียค่าใช้จ่ายในการจัดเก็บเนื่องจากเป็นหน้าที่ตามกฎหมาย แต่ทั้งนี้ระยะเวลา 90 วันในทางปฏิบัติการสืบสวนสอบสวนพบว่าไม่เพียงพอต่อการสืบสวนสอบสวนคดีในหลายเรื่องที่รู้ภายเหตุการณ์ภายหลังระยะเวลาดังกล่าว เช่นกรณีการแฮกข้อมูลในระบบคอมพิวเตอร์กว่าเจ้าตัวจะรู้ข้อมูลว่าถูกแฮกแล้วนำไปใช้ เช่นการใช้บัตรเครดิต แม้จะมียอดที่ไม่ได้ใช้มาให้ตรวจสอบ แต่กว่าจะเจอต้นตอได้ว่ามีการใช้มาจากแหล่งใด จนกว่าจะมาสืบทราบได้ว่าการรู้ข้อมูลดังกล่าวเกิดจากการลักลอบเข้าสู่ระบบคอมพิวเตอร์ของผู้เสียหาย ก็ใช้เวลามากกว่า 90 วันแล้วซึ่งไม่สามารถตรวจสอบข้อมูลการเชื่อมต่อและแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์ได้ อย่างไรก็ตาม หากกฎหมายจะกำหนดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เกินกว่า 90 วัน ก็จะเป็นภาระแก่ผู้ให้บริการที่จะต้องรับภาระและภาระดังกล่าวอาจตกไปถึงผู้ใช้บริการและคุณภาพในการให้บริการเนื่องจากต้องเสียต้นทุนในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายมากยิ่งขึ้น ทั้งที่ ผู้ได้ประโยชน์คือผู้ใช้บริการที่ได้รับความเสียหาย และหน่วยงานของรัฐที่เกี่ยวข้องกับคดีดังกล่าว การกำหนดให้ความรับผิดชอบทั้งหมดตกแก่ผู้ให้บริการอาจส่งผลให้เกิดการหลีกเลี่ยงการจัดเก็บตามกฎหมายได้

3) ในประเทศยุโรปมีการกำหนดใหม่ให้จัดเก็บเป็นระยะเวลาอย่างน้อย 6 เดือน

ตามกฎหมายอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้กำหนดระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้เป็นระยะเวลา 90 วัน แต่ต่อมาเมื่อประเทศสมาชิกได้นำไปปฏิบัติและทำการวิจัยแล้วพบว่า ระยะเวลาเพียง 90 วันไม่สามารถตอบสนองต่อการต้องการข้อมูลสำคัญในการสืบสวนสอบสวนความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้ จึงมีการกำหนดบทบัญญัติใหม่ให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์บางประเภทที่สามารถเป็น

พยานหลักฐานสำคัญไว้เป็นระยะเวลาอย่างน้อย 6 เดือน ซึ่งเป็นระยะเวลาที่คำนวนแล้วสามารถตอบสนองการปฏิบัติงานในการสืบสวนสอบสวนได้

4) ในสหรัฐอเมริกามีการจ่ายค่าชดเชยกรณีที่หน่วยงานรัฐขอให้จัดเก็บข้อมูลเกินกว่าที่กฎหมายกำหนด และมีหน่วยงานกลางที่จัดเก็บข้อมูลสำรองสำหรับคดีความมั่นคงอีกหน่วยงานหนึ่ง

สหรัฐอเมริกากำหนดระยะเวลาสำหรับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการไว้ 90 วันเช่นเดียวกันของประเทศไทย โดยหน่วยางานที่เกี่ยวข้องหากเห็นว่ามีข้อมูลใดจำเป็นที่จะต้องให้จัดเก็บมากกว่านั้นก็อาจร้องขอไปยังผู้ให้บริการให้จัดเก็บได้ โดยจะต้องมีการจ่ายค่าชดเชยให้แก่ผู้ใช้บริการตามกฎหมายเท่าที่ผู้ใช้บริการต้องเสียค่าใช้จ่ายไปในส่วนที่เพิ่มขึ้น ซึ่งการกำหนดเช่นนี้ช่วยให้พยานหลักฐานส่วนที่หน่วยงานใดต้องการให้จัดเก็บไว้นานขึ้นก็สามารถทำได้โดยไม่เป็นภาระแก่ผู้ให้บริการมากเกินไป ซึ่งแตกต่างจากในประเทศไทยที่มีการกำหนดให้หากพนักงานเจ้าหน้าที่เห็นว่าข้อมูลใดควรต้องจัดเก็บนานกว่า 90 วันสามารถแจ้งให้ผู้ให้บริการจัดเก็บได้ไม่เกิน 1 ปี โดยไม่มีการจ่ายค่าชดเชยให้ ซึ่งอาจส่งผลต่อภาระของผู้ให้บริการมากจนเกินไป อีกทั้งผู้มีอำนาจยังหมายถึงเพียงกรณีของพนักงานเจ้าหน้าที่และคดีที่เกี่ยวกับความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้น หน่วยงานอื่นที่จะหาพยานหลักฐานเพื่อประโยชน์ของรัฐหรือเพื่อความมั่นคงด้านอื่นไม่สามารถกระทำได้ นอกจากนั้นแล้ว ในสหรัฐอเมริกาให้ความสำคัญมากกับความมั่นคงมาก โดยหน่วยงานความมั่นคงแห่งชาติ NSA ของสหรัฐอเมริกา มีการดำเนินการจัดเก็บข้อมูลการติดต่อสื่อสารทั้งหมดที่เกิดขึ้นผ่านมายังสหรัฐอเมริกา โดยบันทึกไว้เป็นระยะเวลานานกว่าการจัดเก็บของผู้ให้บริการทั่วไป โดยมีปรากฏตามข้อมูลจากหนังสือพิมพ์ว่ามีการจัดเก็บไว้เป็นระยะเวลานานกว่า 5 ปี เพื่อให้สามารถติดต่อและสืบสวนหาต้นตอของการกระทำความผิดได้เมื่อเกิดคดีที่เกี่ยวข้องกับความมั่นคงขึ้น ซึ่งส่วนใหญ่มีระยะเวลาในการวางแผนการดำเนินการและการติดต่อสื่อสารระหว่างผู้กระทำความผิดเป็นระยะเวลานานก่อนจะเกิดการกระทำความผิดขึ้น โดยหน่วยงานนี้ใช้งบประมาณของรัฐบาลในการบริหารจัดการและการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และข้อมูลที่ใช้มีการจัดเก็บถึงขั้นเนื้อหาการติดต่อสื่อสารสำหรับบางกรณีที่ต้องใช้เป็นพิเศษ โดยคดีที่สามารถขอข้อมูลจากหน่วยงาน NSA ได้จะต้องเป็นกรณีที่เกี่ยวข้องกับความมั่นคงเท่านั้น โดยหากเป็นกรณีทั่วไปหน่วยงานรัฐจะต้องขอข้อมูลจากผู้ให้บริการตามปกติ ไม่สามารถขอข้อมูลจาก NSA ได้ เนื่องด้วยวัตถุประสงค์ของการจัดเก็บข้อมูลทั้งหมดเพื่อความมั่นคง และระดับการจัดเก็บก็เป็นข้อมูลการติดต่อสื่อสารที่กฎหมายให้ความคุ้มครองแก่บุคคลในประเทศ จึงต้องมีการจำกัดเช่นนี้แม้จะมีการจัดเก็บไว้โดยหน่วยงานรัฐเองก็ตาม ซึ่งส่งผลให้ปัญหาในการสืบสวนอาชญากรรมทางคอมพิวเตอร์บางประการหากไม่ร้ายแรงถึงระดับความมั่นคง อาจไม่สามารถหาพยานหลักฐานมาสืบสวนได้หากเกินระยะเวลาการจัดเก็บ 90 วันตามปกติที่กฎหมายกำหนดไว้

5.2 ข้อเสนอแนะ

จากกรณีที่การได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ของไทยมีปัญหาเรื่องอำนาจในการได้มา ความรู้ทางเทคนิคและวิธีการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ของพนักงานเจ้าหน้าที่ อีกทั้งปัญหาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งยังไม่ปรากฏว่ามีหน่วยงานตรวจสอบกลาง หรือมาตรฐานที่ใช้ในการตรวจสอบการจัดเก็บว่ามีความถูกต้องแท้จริงหรือไม่ อีกทั้งระยะเวลาการจัดเก็บที่มีอยู่ในปัจจุบันไม่สามารถตอบสนองต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ได้ ประกอบกับแนวทางการดำเนินกระบวนการของไทยและของต่างประเทศตามที่ได้ศึกษาวิจัย ผู้เขียนจึงมีข้อเสนอแนะดังต่อไปนี้

1) กำหนดให้ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นความผิดอย่างหนึ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

การแก้ไขปัญหาเรื่องการสืบสวนสอบสวนคดีความผิดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตซึ่งปัจจุบันเจ้าพนักงานตำรวจไม่มีอำนาจในการขอพยานหลักฐานและพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็ไม่มีอำนาจเนื่องจากไม่ใช่ความผิดตามพระราชบัญญัตินั้น สามารถแก้ไขได้โดยการกำหนดให้ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์บนอินเทอร์เน็ตเป็นความผิดหนึ่งของความผิดเกี่ยวกับคอมพิวเตอร์ โดยทำการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเพิ่มมาตราความผิดใหม่ดังนี้ โดยมีเนื้อหาดังนี้

“มาตรา ..... ให้การกระทำความผิดเกี่ยวกับลิขสิทธิ์ ซึ่งใช้วิธีการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เป็นความผิดเกี่ยวกับคอมพิวเตอร์ตามพระราชบัญญัตินี้ด้วย”

โดยการกำหนดดังกล่าวจะทำให้การสืบสวนสอบสวนสามารถทำโดยวิธีการเฉพาะตามที่กฎหมายนี้ให้อำนาจแก่พนักงานเจ้าหน้าที่ไว้ และเป็นไปในแนวทางเดียวกับการสืบสวนสอบสวนความผิดเกี่ยวกับคอมพิวเตอร์ ส่งผลให้สามารถรวบรวมข้อมูลได้โดยเจ้าหน้าที่ผู้มีความชำนาญโดยตรงทางด้านคอมพิวเตอร์และมีอำนาจในการขอข้อมูล

ทั้งนี้ เนื่องคดีความผิดเกี่ยวกับคอมพิวเตอร์ และคดีละเมิดลิขสิทธิ์ เป็นคดีที่มีลักษณะแตกต่างกันในทางวิธีพิจารณา เนื่องจากคดีความผิดเกี่ยวกับคอมพิวเตอร์เป็นคดีที่อยู่ภายใต้อำนาจการพิจารณาของศาลอาญา แต่คดีละเมิดลิขสิทธิ์เป็นคดีที่อยู่ภายใต้อำนาจการพิจารณาของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง ตามพระราชบัญญัติจัดตั้งศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศและวิธีพิจารณาคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ. 2539 (“พระราชบัญญัติจัดตั้งศาลทรัพย์สินทางปัญญาฯ”) เพราะคดีลิขสิทธิ์เป็นคดีที่ต้องใช้ความรู้ความชำนาญพิเศษของศาลประกอบการพิจารณาคดียิ่งกว่าคดีทั่วไป ดังนั้นความผิดเกี่ยวกับ

ลิขสิทธิ์ซึ่งใช้วิธีการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เป็นความผิดตามพระราชบัญญัตินี้ด้วย เพื่อไม่ให้เกิดปัญหาว่าการกระทำในรูปแบบดังกล่าวจะอยู่ภายใต้อำนาจของศาลอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญาหรือภายใต้อำนาจของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ ควรกำหนดเพิ่มเติมเขตอำนาจศาลใน พระราชบัญญัติจัดตั้งศาลทรัพย์สินทางปัญญาฯ มาตรา 7 ดังนี้

“ (12) คดีเกี่ยวกับลิขสิทธิ์ ซึ่งใช้วิธีการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์หรือระบบคอมพิวเตอร์”

เพื่อให้การพิจารณาคดีละเมิดลิขสิทธ์บนอินเทอร์เน็ตเป็นอำนาจของศาลทรัพย์สินทางปัญญาฯซึ่งมีความรู้เฉพาะทางเป็นผู้พิจารณาตัดสินคดีดังเช่นคดีละเมิดลิขสิทธิ์อื่น ๆ เช่นเดียวกัน

2) จัดตั้งหน่วยงานกลางและจัดทำมาตรฐานจากต่างประเทศมาปรับใช้ เพื่อให้สามารถทำการรับรองว่ามีการจัดเก็บที่มีคุณภาพ และสามารถตรวจสอบได้

สำหรับการตรวจสอบความถูกต้องของผู้ให้บริการที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตามกฎหมาย ผู้เขียนเสนอแนะว่าควรมีการกำหนดให้มีหน่วยงานกลางในการตรวจสอบและรับรองมาตรฐานการจัดเก็บว่า การจัดเก็บของผู้ให้บริการรายใดที่ได้มาตรฐาน และให้องค์กรที่เกี่ยวข้องกับการให้บริการออกกฎหมายควรคุมว่าจะต้องปฏิบัติตามมาตรฐานที่กำหนดโดยหน่วยงานกลางตรวจสอบนี้ ก็จะทำให้เกิดการจัดเก็บข้อมูลที่มีความถูกต้องแน่นอนในการนำไปใช้และเป็นไปตามที่กฎหมายกำหนด อย่างไรก็ตาม เพื่อให้มีประสิทธิภาพและเป็นที่ยอมรับในระดับสากลในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ มาตรฐานที่จะนำมาจึงควรมีมาตรฐานและกระบวนการปฏิบัติที่กำหนดโดยหน่วยงานกลางนี้นำมาใช้ มิใช่เพียงตรวจสอบว่ารักษาความถูกต้องได้ตามกฎหมายเท่านั้น แต่ควรมีมาตรฐานและขั้นตอนสำหรับการปฏิบัติเพื่อให้ผู้ให้บริการมีวิธีปฏิบัติที่เหมือนกัน และทำให้พนักงานเจ้าหน้าที่สามารถขอข้อมูลและใช้ข้อมูลดังกล่าวได้อย่างมั่นใจ โดยการนำมาตรฐานการจัดเก็บข้อมูล ISO 27001: 2013 ขององค์การระหว่างประเทศว่าด้วยการมาตรฐานมาปรับใช้กับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของไทย อีกทั้งบูรณการกับระบบบริหารองค์กรสารสนเทศระบบ COBIT 5 เพื่อให้การบริหารองค์กรของผู้ให้บริการตอบสนองต่อมาตรฐานการจัดเก็บข้อมูลอย่างเป็นระบบ รวมไปถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการขอข้อมูลให้ใช้แนวทางปฏิบัติเกี่ยวกับการจัดเก็บข้อมูลเช่นเดียวกันหลังจากที่ได้รับข้อมูลไปจากผู้ให้บริการแล้ว เพื่อให้เกิดความสอดคล้องและถูกต้องของข้อมูลทั้งระบบ ก็จะส่งผลให้การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของไทย สามารถตรวจสอบได้ง่าย และมีการรับรอง อีกทั้งยังเป็นที่ยอมรับในระดับสากลถึงแนวทางการปฏิบัติด้านความปลอดภัยของเทคโนโลยีสารสนเทศ อันจะส่งเสริมให้เกิดการขยายตัวทางเศรษฐกิจเกี่ยวกับการใช้คอมพิวเตอร์ในการทำธุรกรรมต่างๆมากยิ่งขึ้นเนื่องจากมีความปลอดภัยในการนำตัวผู้กระทำความผิดมาลงโทษส่งผลให้มีการกระทำความผิดน้อยลงได้ นอกจากนั้น ให้หน่วยงานกลางกำหนดกระบวนการ

ในการคัดลอกข้อมูลและการนำส่งข้อมูลแก่พนักงานเจ้าหน้าที่เพื่อให้ได้ข้อมูลที่ถูกต้องแท้จริง และไม่ส่งผลถึงความน่าเชื่อถือของข้อมูลในขั้นตอนของการใช้เป็นพยานหลักฐานต่อไป

3) กำหนดหน่วยงานกลางโดยรัฐบาลเพื่อรวบรวมและจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์หลังจากระยะเวลาการจัดเก็บทั่วไปของผู้ให้บริการเพิ่มเติม เกี่ยวกับความผิดทางความมั่นคงอื่น ๆ หรือความผิดทางทรัพย์สินทางปัญญาที่อาจส่งผลกระทบร้ายแรงต่อเศรษฐกิจ

จากปัญหากรณีระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์มีผลต่อการสืบสวนที่ไม่สามารถหาพยานหลักฐานได้กรณีที่ทราบเหตุการณ์หรือการสืบสวนใช้ระยะเวลานานกว่า 90 วัน อีกทั้งหากเพิ่มระยะเวลาการจัดเก็บอาจเป็นภาระต่อผู้ให้บริการมากเกินไปและภาระดังกล่าว อาจตกแก่ผู้ใช้บริการในอนาคต ผู้เขียนจึงเสนอแนะแนวทางการแก้ไขปัญหานี้โดยการให้รัฐจัดสรรงบประมาณและตั้งหน่วยงานใหม่ขึ้นเพื่อจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เกี่ยวกับการติดต่อสื่อสารบนระบบอินเทอร์เน็ตและโทรศัพท์ทั้งหมด โดยค่าใช้จ่ายจัดสรรจากงบประมาณของรัฐบาลเพื่อให้รัฐเข้ามาเป็นผู้รับภาระสำหรับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวเพื่อรักษาความมั่นคงและปลอดภัยในการใช้อินเทอร์เน็ตและความมั่นคงของประเทศได้อย่างดียิ่งขึ้น โดยระยะเวลาการจัดเก็บขึ้นอยู่กับงบประมาณของรัฐและความเหมาะสม โดยอาจกำหนดให้จัดเก็บไว้เป็นระยะเวลา 3 – 5 ปี เพื่อให้สามารถสืบสวนสอบสวนในความผิดต่างได้อย่างยาวนาน รวมทั้งความผิดเกี่ยวกับความมั่งคงของประเทศ ทั้งนี้ เนื่องจากผู้ให้บริการยังคงมีหน้าที่สำหรับการจัดเก็บข้อมูลของลูกค้าในกรณีที่ลูกค้าขอข้อมูลของตนเองนั้น ก็อาจจะเป็นกรณีที่ในส่วน 90 วันที่มีการจัดเก็บข้อมูลตามเดิมนั้นให้ผู้ให้บริการเอกชนเป็นผู้ชำระค่าใช้จ่ายให้แก่หน่วยงานกลางในการจัดเก็บโดยคำนวณเป็นอัตราการจัดเก็บ 90 วันสำหรับข้อมูลที่จัดเก็บทุกครั้ง แล้วระยะเวลาหลังจากนั้นจึงเป็นภาระของรัฐบาลที่จะต้องบริหารจัดการต่อ ทั้งนี้ อาจให้ประชาชนหรือบุคคลที่ได้รับความเสียหายมีส่วนร่วมกับการรับภาระในการจัดเก็บดังกล่าว โดยอาจให้ผู้ที่กระทำความผิดจะต้องชำระส่วนของค่าใช้จ่ายที่เกิดขึ้นจากการสืบสวนสอบสวนการกระทำความผิดของผู้กระทำตามแต่สมควรแก่กรณีเพื่อแบ่งเบาภาระของรัฐบาลได้ด้วย ก็จะทำให้เกิดการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่แน่นอนโดยหน่วยงานรัฐ และไม่เกิดปัญหาเรื่องการคัดลอกและส่งต่อข้อมูล เนื่องจากกระทำโดยเจ้าหน้าที่รัฐเองซึ่งเป็นหน่วยงานที่จะควบคุมตรวจสอบได้ในทุกขั้นตอนมากกว่าการเข้าไปตรวจสอบหน่วยงานเอกชน

แต่ทั้งนี้ มีข้อพึงระวังเนื่องจากข้อมูลการติดต่อสื่อสารเป็นข้อมูลส่วนบุคคลหากรัฐบาลนำข้อมูลดังกล่าวไปใช้เพื่อผลประโยชน์ของตนเองหรือผลประโยชน์ทางการเมือง อาจจะส่งผลเสียมากกว่าผลประโยชน์ในการป้องกันประเทศจากอาชญากรรมทางคอมพิวเตอร์ได้

ผู้เขียนจึงมีข้อเสนอแนะสำหรับการทำวิจัยในครั้งต่อไปอาจศึกษาถึงความเหมาะสมของการตั้งองค์กรกลางในการจัดเก็บข้อมูลกับการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการติดต่อสื่อสารว่าหากมีหน่วยงานกลางในการรวบรวมข้อมูลจริง ควรจะมีการควบคุมการจัดเก็บและนำไปใช้ซึ่งข้อมูลการ

ติดต่อสื่อสารได้อย่างไร และอาจมีการศึกษาถึงระยะเวลาการจัดเก็บที่เหมาะสม ซึ่งสามารถตอบสนองความต้องการของกระบวนการยุติธรรมของไทยอย่างแท้จริงต่อไปได้

บรรณานุกรม

กูเกิลเผย “คำค้น” ยอดนิยมของไทยปี 2012 “4shared-แรงเงา-the voice-Gangnam Style” ติดอันดับ. (2555, 13 ธันวาคม). *มติชน*. สืบค้นจาก http://www.matichon.co.th/news_detail.php?newsid=1355385174&grpid=03&catid=03.

คมน์ทนงชัย ฉายไพโรจน์. (2555). *กฎหมายทรัพย์สินทางปัญญาฉบับสมบูรณ์*. กรุงเทพฯ: บานานาสวีท.

จักรกฤษณ์ ควรพจน์. (2551). *การตอบโต้ทางการค้าของสหรัฐฯ ผ่านมาตรา 301 และสิทธิจีเอสพี: ศึกษากรณีการบังคับใช้สิทธิตามสิทธิบัตรยาของไทย*. กรุงเทพฯ: โครงการ WTO Watch.

จิตฤดี วีระเวสล์. (2555). *สรุปย่อหลักกฎหมายทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ*. กรุงเทพฯ: อภิโชติ.

ดูหนังออนไลน์ฟรีใหม่ ๆ Aojvoj Jomvphd. (ม.ป.ป.). สืบค้นจาก http://www3.99llsj.com.

ปิติกุล จีระมงคงพาณิชย์. (2552). *คำอธิบายกฎหมายลักษณะพยานว่าด้วยพยานเอกสาร*. (พิมพ์ครั้งที่ 3). กรุงเทพฯ: เดือนตุลา.

ปิยาภรณ์ คุณชื่น. (2552). *ปัญหาการละเมิดลิขสิทธิ์ผ่านระบบอินเทอร์เน็ต*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยรามคำแหง.

ผู้ผลิตข่าวออนไลน์ฟ้อง Yengo.com ละเมิดลิขสิทธิ์-ศาลไต่สวนกลาง ธ.ค.นี้. (2555, 23 พฤศจิกายน). *เดลินิวส์*. สืบค้นจาก http://www.dailynews.co.th/technology/168514.

พณ.ลุยปราบสินค้าละเมิดบนเว็บไซต์-เฟซบุ๊ก. (2557, 23 กุมภาพันธ์). *โพสต์ทูเดย์*. สืบค้นจาก http://bit.ly/1cE93Of.

พรเพชร วิชิตชลชัย. (ม.ป.ป.). *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*. สืบค้นจาก www.coj.go.th/home/document/computer_miss_2550.pdf.

ไพบูลย์ อมรภิญโญเกียรติ. (2553). *คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550*. กรุงเทพฯ: โปรวิชั่น.

มานิตย์ จุมปา. (2554). *คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: วิญญูชน.

วัส ติงสมิตร. (2545). *คำอธิบายกฎหมายเครื่องหมายการค้า*. กรุงเทพฯ: นิติธรรม.

วิเชาวน์ รักพงษ์ไพโรจน์. (2554). *ความสัมฤทธิผล ความคุ้มค่าในทางเศรษฐกิจ และทางเลือกอื่นของการเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ. 2550*. กรุงเทพฯ: สำนักงานศาลยุติธรรม.

สราวุธ ปิติยาศักดิ์. (2555). *กฎหมายเทคโนโลยีสารสนเทศ*. กรุงเทพฯ: นิติธรรม.

สันติพัฒน์ อรุณธารี. (ม.ป.ป.). *การพัฒนากลยุทธ์ทางธุรกิจไปสู่กลยุทธ์ทางด้านไอทีด้วยโคบิต 5*. สืบค้นจาก http://pumpkrub.blogspot.com/2013/02/5.html.

โสภณ รัตนากร. (2551). *คำอธิบายกฎหมายลักษณะพยาน* (พิมพ์ครั้งที่ 9). กรุงเทพฯ: นิติบรรณการ.

อนุสัญญาระหว่างประเทศว่าด้วยการป้องกันและปราบปรามอาชญากรรม [Convention on Cybercrime] (กิตติพงษ์ กิตยารักษ์, ชาติ ชัยเดชสุริยะ และณัฐวสา ฉัตรไพฑูรย์, ผู้แปล). ม.ป.ท.: เดือนตุลา.

อรพรรณ พนัสพัฒนา. (ม.ป.ป.). *บทบาทของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการป้องกันงานอันมีลิขสิทธิ์*. สืบค้นจาก http://www.ipitc.coj.go.th/system/journal/Cr2007_CopyrightProtect.pdf.

อำนวย แสงสว่าง. (2544). *กฎหมายทรัพย์สินทางปัญญา*. กรุงเทพฯ: อักษราพิพัฒน์.

serieswawa.com. (ม.ป.ป.). สืบค้นจาก http://www.serieswawa.com.

โอภาส เอี่ยมสิริวงศ์. (2551). *วิทยาการคอมพิวเตอร์และเทคโนโลยี (ฉบับปรับปรุง)*. กรุงเทพฯ: ซีเอ็ดยูเคชั่น.

โอสถ โกศิน. (2538). *คำอธิบายกฎหมายลักษณะพยานหลักฐาน* (พิมพ์ครั้งที่ 3). กรุงเทพฯ: หอรัตนชัยการพิมพ์.

Computer Crime and Intellectual Property Section, U.S. Department of Justice. (2006). *Cyber Crime Law of United States*. N.P.: n.p.

Federation of American scientists. (n.d.). *Section 702*. Retrieved from http://www.fas.org/irp/news/2013/06/nsa-sect702.pdf.

International organization for standardization. (n.d.a). *About ISO.* Retrieved from http://www.iso.org/iso/home/about.htm.

International organization for standardization. (n.d.b). *Standards.* Retrieved from http://www.iso.org/iso/home/about.htm.

James Ball. (2013, November 30). NSA stores metadata of millions of web users for up to a year, secret files show. *Theguardian*. Retrieved from http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

National Security Agency. (n.d.). *Mission*. Retrieved from http://www.nsa.gov/about/mission /index.shtml.

Office of the Director of National Intelligence. (n.d.). *Section 702 of the Foreign Intelligence Surveillance Act.* Retrieved from http://icontherecord.tumblr.com/topics/section-702.

ประวัติผู้เขียน

ชื่อ - สกุล: นายสุรเชษฐ ชาติชาคร

ประวัติการศึกษา:

ปี พ.ศ. 2550	เข้าศึกษาในระดับปริญญานิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ สาขา กฎหมายทรัพย์สินทางปัญญา และเทคโนโลยีสารสนเทศ (รุ่นที่ 3)
ปี พ.ศ. 2549	นิติศาสตรบัณฑิต จากมหาวิทยาลัยกรุงเทพ (รุ่นที่ 18)
ปี พ.ศ. 2546	มัธยมศึกษาตอนปลาย จากโรงเรียนหอวัง

ประสบการณ์การทำงาน:

ปี พ.ศ. 2553 – ปัจจุบัน	นิติกร สำนักกฎหมายและวิชาการ สำนักงานศาลยุติธรรม
ปี พ.ศ. 2550 - 2552	ที่ปรึกษากฎหมาย ฝ่ายกฎหมาย บริษัท ทรูคอร์ปอเรชั่น จำกัด (มหาชน)

มหาวิทยาลัยกรุงเทพ

ข้อตกลงว่าด้วยการอนุญาตให้ใช้สิทธิในวิทยานิพนธ์/สารนิพนธ์

วันที่ 19 เดือน ธ.ค. พ.ศ. 2557.

ข้าพเจ้า (นาย/นาง/นางสาว) สุภาชัย ชาติวงศ์ อยู่บ้านเลขที่ 1155/246

ซอย ..... ถนน สุขุมวิท ตำบล/แขวง คลองเตย

อำเภอ/เขต คลองเตย จังหวัด กรุงเทพฯ รหัสไปรษณีย์ 10400

เป็นนักศึกษาของมหาวิทยาลัยกรุงเทพ รหัสประจำตัว 7504200029

ระดับปริญญา ☐ ตรี ☑ โท ☐ เอก

หลักสูตร นิติศาสตรมหาบัณฑิต สาขาวิชา - คณะ นิติศาสตร์

ซึ่งต่อไปนี้เรียกว่า **"ผู้อนุญาตให้ใช้สิทธิ"** ฝ่ายหนึ่ง และ

มหาวิทยาลัยกรุงเทพ ตั้งอยู่เลขที่ 119 ถนนพระราม 4 แขวงพระโขนง เขตคลองเตย กรุงเทพมหานคร 10110 ซึ่งต่อไปนี้เรียกว่า **"ผู้ได้รับอนุญาตให้ใช้สิทธิ"** อีกฝ่ายหนึ่ง

ผู้อนุญาตให้ใช้สิทธิ และ ผู้ได้รับอนุญาตให้ใช้สิทธิ ตกลงทำสัญญากันโดยมีข้อความดังต่อไปนี้

ข้อ 1. ผู้อนุญาตให้ใช้สิทธิขอรับรองว่าเป็นผู้สร้างสรรค์และเป็นผู้มีสิทธิแต่เพียงผู้เดียวในงานสารนิพนธ์/วิทยานิพนธ์หัวข้อ ปัญหาการจัดเก็บ และการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ เพื่อนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์ในอินเทอร์เน็ต

ซึ่งถือเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร นิติศาสตรมหาบัณฑิต ของมหาวิทยาลัยกรุงเทพ (ต่อไปนี้เรียกว่า **"สารนิพนธ์/วิทยานิพนธ์"**)

ข้อ 2. ผู้อนุญาตให้ใช้สิทธิตกลงยินยอมให้ผู้ได้รับอนุญาตให้ใช้สิทธิโดยปราศจากค่าตอบแทนและไม่มีกำหนดระยะเวลาในการนำสารนิพนธ์/วิทยานิพนธ์ ซึ่งรวมถึงแต่ไม่จำกัดเพียงการทำซ้ำ ดัดแปลง เผยแพร่ต่อสาธารณชน ให้เช่าต้นฉบับหรือสำเนางาน ให้ประโยชน์อันเกิดจากลิขสิทธิ์แก่ผู้อื่น อนุญาตให้ผู้อื่นใช้สิทธิโดยจะกำหนดเงื่อนไขอย่างหนึ่งอย่างใดด้วยหรือไม่ก็ได้ ไม่ว่าทั้งหมดหรือเพียงบางส่วน หรือการกระทำอื่นใดในลักษณะทำนองเดียวกัน

ข้อ 3. หากกรณีมีข้อขัดแย้งในปัญหาลิขสิทธิ์ในสารนิพนธ์/วิทยานิพนธ์ระหว่างผู้อนุญาตให้ใช้สิทธิกับบุคคลภายนอกก็ดี หรือระหว่างผู้ได้รับอนุญาตให้ใช้สิทธิกับบุคคลภายนอกก็ดี หรือมีเหตุขัดข้องอื่นๆ เกี่ยวกับลิขสิทธิ์ อันเป็นเหตุให้ผู้รับอนุญาตให้ใช้สิทธิไม่สามารถนำงานนั้นออกทำซ้ำ เผยแพร่ หรือโฆษณาได้ ผู้อนุญาตให้ใช้สิทธิยินยอมรับผิดและชดใช้ค่าเสียหายแก่ผู้ได้รับอนุญาตให้ใช้สิทธิในความเสียหายต่าง ๆ ที่เกิดขึ้นแก่ผู้ได้รับอนุญาตให้ใช้สิทธิทั้งสิ้น

สัญญานี้ทำขึ้นสองฉบับ มีข้อความเป็นอย่างเดียวกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้โดยละเอียดแล้ว จึงได้ลงลายมือชื่อให้ไว้เป็นสำคัญต่อหน้าพยาน และเก็บรักษาไว้ฝ่ายละฉบับ

ลงชื่อ.....ผู้อนุญาตให้ใช้สิทธิ

( )

ลงชื่อ.....ผู้ได้รับอนุญาตให้ใช้สิทธิ

(ดร.ชนันนา รอดสุทธิ)

ผู้อำนวยการสำนักหอสมุดและศูนย์การเรียนรู้

ลงชื่อ.....พยาน

(ผู้ช่วยศาสตราจารย์ ดร.ศิวพร หวังพิพัฒน์วงศ์)

คณบดีบัณฑิตวิทยาลัย

ลงชื่อ.....พยาน

(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

ผู้อำนวยการหลักสูตร/ ผู้รับผิดชอบหลักสูตร