

กฎหมายการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกันในสหราชอาณาจักร
Law Authorizing a State to Access or Obtain Information of People
Communication in United Kingdom*

รัฐสภา จูรีมาส, ดิสพล จันศิริ, ณัชชญา ทองจันทร์

สุรวุฒิ ศิริบรรณากุล, เนตรชลิสา โตวงศ์**

Rattasapa Chureemas et al. **

บทคัดย่อ

ปัจจุบันอำนาจในการเข้าถึงข้อมูลส่วนบุคคลสื่อสารถึงกันนั้นสามารถพบเห็นได้ในหลายประเทศ โดยเฉพาะอย่างยิ่งกลุ่มประเทศยุโรป ที่มีการออกมาตรการให้อำนาจแก่เจ้าหน้าที่หรือหน่วยงานของรัฐ สามารถกระทำการเพื่อเข้าถึงหรือเพื่อให้ได้มาซึ่งข้อมูลการติดต่อสื่อสารของบุคคลซึ่งอยู่ในประเทศนั้น โดยมุ่งกระทำเพื่อหาแนวทางหรือมาตรการในการป้องกันความเสียหายที่อาจเกิดขึ้นแก่รัฐตนได้ อาทิ การติดต่อสื่อสารในลักษณะที่อาจมีผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางเศรษฐกิจของประเทศ อาชญากรรมร้ายแรง หรือความปลอดภัยสาธารณะของประชาชน

* บทความนี้สรุปจากโครงการศึกษาวิจัยการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกันในสหราชอาณาจักร, รัฐสภา จูรีมาสและคณะ ได้รับทุนสนับสนุนในการศึกษาวิจัยจากสถาบันพระปกเกล้า, 2562.

** รัฐสภา จูรีมาส (ผู้ดำเนินการหลัก) ผู้รับผิดชอบหลักสูตรนิติศาสตรบัณฑิต คณะสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ, ดร. ดิสพล จันศิริ ผู้รับผิดชอบหลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ, ผู้ช่วยศาสตราจารย์ณัชชญา ทองจันทร์ ผู้ช่วยศาสตราจารย์ประจำ คณะนิติศาสตร์มหาวิทยาลัยอัสสัมชัญ, สุรวุฒิ ศิริบรรณากุล ผู้ช่วยคณบดีฝ่ายกิจการนักศึกษา คณะนิติศาสตร์ มหาวิทยาลัยอัสสัมชัญ, นางสาวเนตรชลิสา โตวงศ์ ที่ปรึกษากฎหมายอิสระ

** Rattasapa Chureemas (Corresponding Author), Lecturer's Responsible to the Bachelor of Laws Program, School of Social Science, Srinakharinwirot University; Dr. Disaphol Chansiri, Lecturer's Responsible to the Master of Laws Program, School of Law, Assumption University; Assistant Professor Nachatchaya Thongjan, Assistant Dean to Administrative Affairs, School of Law, Assumption University; Surawut Siribannakul, Assistant Dean to Student Affairs, School of Law, Assumption University; Miss Nethshalyssa Towong, Independent Legal Consultant.

จากการศึกษาพบว่าในแต่ละประเทศนั้นมีกฎหมายและข้อกำหนดในการเข้าถึงข้อมูลส่วนบุคคลที่สื่อสารที่แตกต่างกัน ในการให้อำนาจแก่บุคคลเพื่อกระทำการโดยชอบด้วยกฎหมาย ภายใต้การสร้างสมดุลระหว่างอำนาจในการเข้าถึงข้อมูลการติดต่อสื่อสารระหว่างบุคคลและการคุ้มครองข้อมูลส่วนบุคคลของประชาชน จากการศึกษากฎหมายของประเทศไทยในปัจจุบัน ในประเด็นการเข้าถึงหรือได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกันนั้น ยังพบว่าไม่มีความชัดเจนในการกำหนดมาตรการหรือแนวทางในการบังคับใช้กฎหมาย ทั้งยังไม่อำนวยความสะดวกในการปฏิบัติงานของเจ้าหน้าที่อีกประการหนึ่ง

ทั้งนี้ ในหลายประเทศรวมทั้งสหราชอาณาจักร ได้กำหนดกฎหมายที่เกี่ยวข้องในการให้อำนาจหรือรับรองอำนาจแห่งรัฐในการเข้าถึงข้อมูลของบุคคลที่สื่อสารกัน ตลอดจนสิทธิในการสอดแนม (Surveillance) ข้อมูลดังกล่าวด้วย ซึ่งกำหนดไว้ในกระบวนการสอบสวนและสืบสวน (Investigatory Powers) โดยเจ้าพนักงานของรัฐที่เกี่ยวข้อง การศึกษากฎหมายของสหราชอาณาจักรย่อมนำไปสู่การสร้างกฎหมายอันเป็นแบบแผนในการให้อำนาจแก่รัฐเพื่อเข้าถึงหรือได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกันได้อย่างมีประสิทธิภาพ

คำสำคัญ: การสอบสวน, การสืบสวน, การสอดแนม, การสกัดข้อมูล

Abstract

Nowadays, the authority to access or obtain information of people communication in the state, especially the Europe union have issued the authorities' measure for government officer or government sector who access or obtain information of people communication in those states. Additionally, the aim for finding the various approaches or measures to protect the damage can appear to the government sector. For instance, the communication in term of affecting national security, economic stability, the serious crime, and public safety for people.

From the research, the researcher found that each State has its own law and regulation to access different information of people communication, which entitles the authority to access legally. Moreover, under controlling the balance between the powers to access information of people communication and protecting the personal information of people. From the research of Thai studying currently, the issue of access or obtain

information of people communication has not been appeared for the measurement and the method for using the legal clearly.

Additionally, many states include the United Kingdom has recognized the law which related to giving the power or certify the state to access or obtain information of people communication along with the right of detect (Surveillance) for the information. Also, it has been identified in the process of investigation (Investigatory Powers) by the related government officer. Studying in the United Kingdom law will lead the tradition of using its law to access and obtain information of people communication efficiently.

Keywords: Inquiry, Investigation, Surveillance, Interception

บทนำ

การอนุญาตให้รัฐกระทำการเข้าถึงหรือกระทำการเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกันนั้น ย่อมเสมือนเป็นการยอมรับการให้อำนาจแก่รัฐในการล่วงล้ำถึงข้อมูลส่วนบุคคลอย่างไม่เหมาะสม อันเป็นสิทธิเสรีภาพของประชาชนขั้นพื้นฐานในการที่จะติดต่อสื่อสารระหว่างกัน ฉะนั้น จึงกล่าวได้ว่าเป็นการกระทำที่กระทบต่อสิทธิส่วนบุคคลอันเป็นหนึ่งในหลักสิทธิมนุษยชนซึ่งได้รับรองโดยองค์การสหประชาชาติ ที่จะต้องได้รับความคุ้มครอง หรือกระทำการภายใต้การควบคุมอย่างเคร่งครัด¹ โดยเฉพาะอย่างยิ่งการเข้าถึงข้อมูลส่วนบุคคลสื่อสารถึงกันในลักษณะการเข้าถึงในเนื้อหาของสื่อสาร (Content) ที่เป็นลักษณะเข้าถึงรายละเอียดของข้อความในการสื่อสารของบุคคลนั้นด้วย

จากการศึกษาพบว่าในแต่ละประเทศนั้นมีกฎหมายและข้อกำหนดในการเข้าถึงข้อมูลส่วนบุคคลสื่อสารที่แตกต่างกัน ในการให้อำนาจแก่บุคคลเพื่อกระทำการโดยชอบด้วยกฎหมาย อย่างไรก็ตาม การกระทำเพื่อเข้าถึงข้อมูลติดต่อสื่อสารของบุคคลจำเป็นต้องวางมาตรการเพื่อลดโทษการเข้าถึงข้อมูลโดยมิชอบ ซึ่งโดยเฉพาะการรักษาความเป็นส่วนตัวและความมั่นคงของชาติ นอกจากนี้ประเด็นที่จำเป็นต้องพิจารณาอีกประการหนึ่ง คือ การสร้างความสมดุลระหว่างอำนาจในการเข้าถึงข้อมูลการติดต่อสื่อสารระหว่างบุคคลและการคุ้มครองข้อมูลส่วนบุคคลของประชาชน เนื่องจากการเข้าถึงข้อมูลส่วนบุคคลสื่อสารกัน

¹ Privacy and Human Right, An International Survey of Privacy Laws and Practice, <http://gilc.org/privacy/survey/intro.html>, (last visited 12 December 2018).

บางอย่างนั้นอาจหลีกเลี่ยงไม่ได้ที่จะต้องดำเนินการสืบสวนและรวบรวมข้อมูล ซึ่งต้องคำนึงถึงข้อเท็จจริงว่า การใช้เทคโนโลยีเดียวกันในการเข้าถึงข้อมูลสื่อสารอาจจำเป็นต้องล่วงล้ำเข้าไปยังข้อมูลที่อาจกระทบต่อ สิทธิส่วนบุคคลได้ ดังนั้น จึงควรจะต้องมีการหาแนวทางแก้ไขด้วยการกำหนดนโยบายทางกฎหมาย

การเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันเป็นมาตรการเพื่อกระทำให้ได้มาซึ่งข้อมูล ข่าวสารของประชาชนอันเป็นการละเมิดสิทธิส่วนบุคคล ซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญและหลักสากล อย่างไรก็ตาม แม้ว่าการเข้าถึงและการได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันนั้นจะเป็นการละเมิดสิทธิ ดังที่กล่าวมาแล้ว แต่ในบางกรณีจำเป็นอย่างยิ่งที่ต้องให้รัฐมีอำนาจดำเนินการภายใต้กฎหมายเพื่อ ดำเนินการอย่างใดอย่างหนึ่ง เพื่อการเข้าถึงข้อมูลดังกล่าวโดยความจำเป็นเฉพาะกรณีที่กำหนดภายใต้ กฎหมายนั้นๆ

จากการศึกษากฎหมายของประเทศไทยในปัจจุบัน ในประเด็นการเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคล สื่อสารถึงกันนั้น พบว่ากฎหมายไทยที่มีการประกาศใช้อยู่ได้มีการบัญญัติรับรองอำนาจรัฐให้มีสิทธิเข้าถึง และได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันแล้ว แต่เมื่อพิจารณาในเชิงลึกของกฎหมายดังกล่าวจะเห็นได้ว่าแม้ จะมีลักษณะ รูปแบบ แนวทาง วิธีการ ในการให้อำนาจรัฐในการเข้าถึงข้อมูลดังกล่าว แต่การกำหนด แนวทางและอำนาจแตกต่างกัน ทั้งที่เป็นกฎหมายอันมีลักษณะทับซ้อน เชื่อมโยงในการบังคับใช้ ก่อให้เกิด ความไม่มีเอกภาพในการบังคับใช้ ซึ่งประเด็นนี้มีความแตกต่างกับกฎหมายในบางประเทศที่กำหนด กฎหมายแบบแผนแม่บทในการให้อำนาจรัฐในการดำเนินการดังกล่าว ที่หน่วยงานต่างๆ ต้องถือปฏิบัติตาม ดังเช่นกฎหมายของสหราชอาณาจักรที่ผู้วิจัยมุ่งเน้นศึกษา

ทั้งนี้ ในหลายประเทศรวมทั้งสหราชอาณาจักร ได้กำหนดกฎหมายที่เกี่ยวข้องในการให้อำนาจหรือ รับรองอำนาจแห่งรัฐในการเข้าถึงข้อมูลของบุคคลที่สื่อสารกัน ตลอดจนสิทธิในการสอดแนม (Surveillance) ข้อมูลดังกล่าวด้วย ซึ่งกำหนดไว้ในกระบวนการสอบสวนและสืบสวน (Investigatory Powers) โดยเจ้า พนักงานของรัฐที่เกี่ยวข้อง ซึ่งมีอำนาจในการออกคำสั่งให้มีการดักข้อมูล การบันทึกข้อมูล และการถอด ความที่มีการสื่อสารทางโทรคมนาคม รวมถึงการสืบสวนคดีอาชญากรรมของหน่วยงานอื่นซึ่งบังคับใช้ กฎหมายด้วยนั้น อาจมีความจำเป็นต้องได้รับการอนุญาตโดยกำหนดบุคคลซึ่งมีคุณสมบัติเฉพาะเพื่อให้ สามารถเข้าถึงข้อมูลนี้ได้โดยตรง

สหราชอาณาจักร มีกฎหมายเกี่ยวกับการเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันบังคับใช้ อยู่ในปัจจุบัน โดยกำหนดลักษณะการเข้าถึงเป็น 2 ลักษณะ กล่าวคือ 1. การตรวจสอบ ตรวจสอบตรา หรือสอด แแนม ข้อมูลที่บุคคลได้มีการสื่อสารกัน (Surveillance) 2. อำนาจในการเข้าถึงข้อมูลที่บุคคลสื่อสารถึงกัน ภายใต้อำนาจเฉพาะในการสืบสวนสอบสวนที่กฎหมายให้อำนาจไว้ (Investigatory Powers) ซึ่งให้อำนาจ เจ้าพนักงานบังคับใช้รวมถึงสถานการณ์บางอย่างซึ่งถูกระบุโดยหน่วยข่าวกรองด้วย อย่างไรก็ตามกฎหมาย

ดังกล่าวได้สร้างกรอบการเข้าถึงข้อมูลต้องมีการแจ้งเป็นลายลักษณ์อักษรโดยระบุว่าเกี่ยวข้องกับบุคคลหรือหน่วยงานใด เป็นต้น

โดยมุ่งศึกษาอำนาจในการเข้าถึงข้อมูลที่บุคคลสื่อสารถึงกันตามกฎหมายการสืบสวนเพื่อการเข้าถึงซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน (The Regulation of Investigatory Powers Act 2000 (RIPA) และ The Investigatory Powers Act 2016 (IPA)) ทั้งนี้ในส่วนของ IPA นั้นเนื่องจากมีรายละเอียดเป็นจำนวนมาก ผู้วิจัยจึงมุ่งศึกษาในข้อกำหนดในการเข้าถึงข้อมูลหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันในประเด็นทั่วไปเท่านั้น

1. หลักการให้รัฐสามารถเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน ตามกฎหมายของสหราชอาณาจักร

การดำเนินการต่างๆ เพื่อการเข้าถึงข้อมูลที่มีการติดต่อสื่อสารถึงกันนั้น ซึ่งดำเนินการโดยหน่วยงานภาครัฐ เพื่อต่อสู้กับอาชญากรรมหรือการสร้างความมั่นคงในความปลอดภัยให้แก่ประชาชนนั้นเป็นเหตุผลหนึ่งว่า การเข้าถึงข้อมูลการสื่อสารดังกล่าวนั้นอาจมีทำงานที่เผยแพร่ไปในวงกว้างมากเกินไปจนความจำเป็นแม้ว่าจะดำเนินการโดยหน่วยงานภาครัฐที่ถูกจัดตั้งแล้วก็ตาม ทั้งนี้การดำเนินการต่างๆ นั้นอาจไม่สอดคล้องกับมาตรฐานของหลักสิทธิมนุษยชนสากล เป็นเหตุให้จำเป็นต้องมีการสร้างกลไกที่มีลักษณะเป็นการเฉพาะในการกำหนดแนวทาง วิธีการ มาตรการ ในการให้อำนาจแก่รัฐและหน่วยงานเท่าที่จำเป็นเพื่อให้อำนาจในการเข้าถึงข้อมูลที่บุคคลทำการสื่อสารถึงกัน อันเป็นที่มาของการจัดตั้งพระราชบัญญัติอำนาจการสอบสวนในปี ค.ศ. 2000 หรือ RIPA ซึ่งมีบทบาทหลักในการกำกับดูแลหน่วยงานของรัฐในการเข้าถึงข้อมูลสื่อสารอันจำเป็นที่ต้องสอดคล้องกับกฎหมายสิทธิมนุษยชน โดยผ่านข้อกำหนดของกฎหมายที่ชัดเจนและคำนึงถึงวัตถุประสงค์หลักในการจัดการ กำกับดูแล การใช้อำนาจ และหน้าที่ตามกฎหมาย ให้มีลักษณะเป็นกลไกหลักในการดำเนินการเข้าถึงข้อมูลตามกฎหมายเพื่อไม่ให้เกิดการกระทำที่อาจนำไปสู่การกระทำที่มิชอบ หรือกระทำเกินกว่าความจำเป็น²

ในความจริงแล้วการเข้าถึงข้อมูลสื่อสารในปัจจุบันนี้ประชาชนทั่วไปมีช่องทางหลากหลายที่สามารถเข้าถึงข้อมูลดังกล่าวได้ แต่การตระหนักถึงการเข้าถึงข้อมูลอย่างเปิดเผยโดยใช้อำนาจตามกฎหมายนั้น ยังไม่เป็นที่รู้จักหรือรับรู้ของประชาชนมากนัก เหตุผลสำคัญคือประชาชนส่วนใหญ่ยังไม่ตระหนักถึงเหตุผลหรือข้อเสียในเรื่องนี้ ดังนั้น หน่วยงานภาครัฐจึงจำเป็นต้องให้มีการควบคุมโดยกำหนดให้มีขั้นตอน

² Robin Simcox in The Henry Jackson Society, “Investigatory Powers Review” (2014) <https://terrorismlegislationreviewer.independent.gov.uk/wpcontent/uploads/2015/06/Submissions-H-Z.pdf>, (last visited 10 September 2018).

กระบวนการ และวิธีการป้องกัน ภายใต้การกำกับดูแลของคณะกรรมการผู้จัดการการสื่อสาร อีกทั้งในกรณี
ที่หน่วยงานรัฐอื่นๆ ที่ไม่ใช่หน่วยงานตามพระราชบัญญัติ หากยังไม่สามารถเข้าถึงข้อมูลสื่อสารดังกล่าวได้
อาจอาศัยอำนาจทางกฎหมายของหน่วยงานตามกฎหมายโดยการร้องขอหน่วยงานผู้มีความอำนาจกำกับดูแล
ตามพระราชบัญญัตินี้ดังกล่าวเป็นกรณีๆ ไป เพื่อเข้าถึงข้อมูลดังกล่าวเมื่อมีเหตุเกี่ยวพันตามกฎหมาย

สำหรับสหราชอาณาจักรนั้นกำลังเผชิญกับความหลากหลายต่อภัยคุกคาม ทั้งในด้านความมั่นคง
ของประเทศตามหลักทฤษฎีของเฮนรี แจ็คสัน (Henry Jackson) ที่เป็นกรอบยุทธศาสตร์ความมั่นคง
แห่งชาติของรัฐบาลสหราชอาณาจักร ในปี พ.ศ. 2553 ระบุว่า “ปัจจุบันความผิดพลาดทางกฎหมายเกิด
จากการโจมตีทางไซเบอร์ (Cyber) โดยไม่ได้มีเจตนาใช้อาวุธเคมี อาวุธนิวเคลียร์ หรือ อาวุธชีวภาพรวมถึง
อุบัติเหตุขนาดใหญ่หรืออันตรายจากธรรมชาติ” ในขณะที่ “ความรุนแรง” จากการก่อการร้ายระหว่าง
ประเทศนั้นได้มีการเกิดขึ้นอย่างต่อเนื่อง ซึ่งนั่นหมายความว่าแนวโน้มในการเกิดการโจมตีอาจเป็นไปได้สูง
มากกว่าอดีต ทั้งนี้ผู้เชี่ยวชาญด้านความมั่นคงและการต่อต้านการก่อการร้ายแห่งสหราชอาณาจักรกล่าวว่า
“มีการกระทำอย่างร้ายแรงต่อการก่อการร้ายในประเทศนี้เป็นประจำทุกๆ ปีหรือสองครั้งต่อปี”³

ในขณะที่ความก้าวหน้าทางเทคโนโลยีได้ทำให้ความพยายามของรัฐต่อการต่อต้านภัยคุกคามจาก
การก่อการร้ายเป็นไปได้ยากลำบากมากขึ้น สืบเนื่องมาจาก ผู้อำนวยการสำนักงานสื่อสารข้อมูลรัฐบาล
(Government Communications Headquarters - GCHQ) ได้แสดงความคิดเห็นว่า “เชื่อว่าการ
เปลี่ยนแปลงทางเทคโนโลยีมีส่วนทำให้ผู้ก่อการร้ายสะดวกต่อการทำงานในขณะที่อินเทอร์เน็ตช่วยให้พวกเขา
สามารถสื่อสารข้อมูลได้อย่างง่ายยิ่งขึ้น ซึ่งทำให้พวกเขามีช่องทางในการสื่อสารและก่อกิจกรรม
อาชญากรรม รวมทั้งกระจายโฆษณาชวนเชื่อเพื่อสร้างแนวร่วม ทำให้ผู้ก่อการร้ายสามารถสร้างแผนการใน
การวางแผนเผยแพร่กิจกรรมอาชญากรรมนี้ไปสู่ประชาชนได้อย่างสะดวกยิ่งขึ้น” ในทำนองเดียวกัน Sir
Malcolm Rifkind ประธานคณะกรรมการข่าวกรองและความมั่นคงแห่งรัฐสภา (The Intelligence and
Security Committee of Parliament - ISC) ได้กล่าวว่า “หัวใจของการพัฒนาเครือข่ายความหวาดกลัว
ระหว่างประเทศซึ่งคุกคามความปลอดภัยของเรามากที่สุดคือการเพิ่มขึ้นและการแพร่กระจายของ
อินเทอร์เน็ตไปสู่ประชาชน”⁴ ซึ่งแสดงให้เห็นถึงเหตุปัจจัยสำคัญที่รัฐบาลแห่งสหราชอาณาจักร จำเป็นต้อง

³ Morton Halperin, “Multilateral Standards for Electronic Surveillance for Intelligence Gathering” *Investigatory Powers Review*, 2, <https://terrorismlegislationreviewer.independent.gov.uk/wpcontent/uploads/2015/06/Submissions-H-Z.pdf>, (last visited 9 December 2018).

⁴ News, B., “UK Surveillance Powers Explained” (2015) <https://www.bbc.com/news/uk-34713435>, (last visited 9 December 2018).

วางมาตรการหรือกำหนดเครื่องมือ ที่เป็นกลไกสำคัญเพื่อป้องกันการเกิดอาชญากรรมที่กระทบต่อความมั่นคงของประเทศ

2. หลักเกณฑ์และเงื่อนไขการให้รัฐสามารถเข้าถึงและได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกัน กระบวนการได้มา การใช้ และการเก็บรักษาข้อมูลส่วนบุคคลสื่อสารถึงกัน ตามกฎหมายของ สหราชอาณาจักร (The Investigatory Powers Act 2016)

หลักในการบังคับใช้กฎหมายเกี่ยวกับเข้าถึงและได้มาซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกัน รวมถึงการสอดแนมข้อมูล (Surveillance) ของสหราชอาณาจักร⁵ อยู่ภายใต้ความตกลงตามอนุสัญญาแห่งสหภาพยุโรปว่าด้วยสิทธิมนุษยชน ข้อที่ 8 (European Convention on Human Rights - ECHR)⁶ ซึ่งกำหนดให้การกระทำการสอดแนมของรัฐสมาชิกต้องกระทำภายใต้ข้อกำหนดแห่งอนุสัญญาดังกล่าว กล่าวคือ “การแทรกแซงความเป็นส่วนตัวภายใต้ความคุ้มครองสิทธิส่วนบุคคลจะกระทำได้เท่าที่จำเป็นเพื่อวัตถุประสงค์ในด้านความมั่นคง ความปลอดภัยสาธารณะหรือความมั่นคงทางเศรษฐกิจ เพื่อการป้องกันอาชญากรรม” ทั้งนี้ เจตจำนงของอนุสัญญาเป็นการสร้างเงื่อนไขสำคัญว่าจำเป็นต้องมีกฎหมายกำหนดอำนาจและรายละเอียดในการกระทำการดังกล่าวไว้เป็นการเฉพาะ อย่างชัดเจนและมีผลบังคับใช้อย่างเป็นรูปธรรมจึงจะสามารถกระทำการล่วงล้ำได้โดยชอบ⁷ โดยสามารถจำแนกเจตจำนงได้ ดังนี้

1. มาตรการทางกฎหมายในการเข้าสอดแนมหรือเข้าถึงข้อมูลของประชาชนต้องมีกฎหมายภายในกำหนดไว้เป็นการเฉพาะในการเข้าถึงข้อมูลดังกล่าวของประชาชน
2. ต้องกำหนดขอบเขตของกฎหมายในการบังคับใช้ วิธีการ กระบวนการในการได้มาซึ่งข้อมูล และข้อกำหนดเกี่ยวกับการเก็บรักษาข้อมูล และการกำหนดผู้มีอำนาจในการกระทำไว้อย่างชัดเจน
3. ภายใต้บังคับของกฎหมายดังกล่าวจำเป็นต้องแสดงถึงผลอันคาดหมายได้ว่าได้กระทำไปเพื่อจุดประสงค์ใดเป็นการเฉพาะ

ซึ่งจากการจำแนกกรณีตามอนุสัญญา ECHR ข้อที่ 8 แสดงให้เห็นว่า การออกกฎหมายที่ให้อำนาจในการเข้าแทรกแซงข้อมูลนั้น ต้องมีการตรากฎหมายที่ให้อำนาจในการเข้าถึงซึ่งข้อมูลดังกล่าวเป็นการเฉพาะ ทั้งต้องกำหนดกระบวนการในการได้มาตลอดจนผู้มีอำนาจที่จะกระทำการดังกล่าวตามกฎหมายไว้

⁵ Ian J. Lloyd, *Information Technology Law*, 8th edited, (Great Britain, United Kingdom: Oxford University Press, 2017), pp. 22-23.

⁶ ECHR, Article 8 of “Right to respect for private and family life”.

⁷ ECHR, *Factsheet – Mass Surveillance*, (Echr.coe.int, 2018), https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf, (last visited 2 December 2018).

เป็นการเฉพาะด้วย และการกระทำดังกล่าวต้องแสดงให้เห็นปรากฏตามกรอบวัตถุประสงค์ที่กฎหมายกำหนดไว้ นั้น จึงจะสามารถกระทำการเช่นนั้นได้

นอกจากนี้ ECHR ได้กำหนดข้อเสนอแนะต่อรัฐในการที่จะบังคับใช้กฎหมายเกี่ยวกับการแทรกแซงข้อมูลของประชาชน ซึ่งอ้างอิงจากกรณีศึกษา *Klass & Others v Germany*⁸ โดยให้เหตุผลในการพิจารณาเห็นว่า ในยุคที่สังคมถูกคุกคามจากรูปแบบการจารกรรมและการก่อการร้ายที่มีความซับซ้อนขึ้น การใช้อำนาจของรัฐในการป้องกันภัยดังกล่าวถือเป็นเรื่องจำเป็นที่ต้องกระทำ อย่างไรก็ตามการให้อำนาจแก่รัฐในการกระทำการดังกล่าวย่อมถือเป็นการกระทำที่กระทบต่อสิทธิส่วนบุคคลที่ได้รับความคุ้มครองทั้งในอนุสัญญา ECHR และสิทธิพื้นฐานตามรัฐธรรมนูญ

จากกรณีศึกษา *Klass & Others v Germany*⁹ นำมาสู่บรรทัดฐานในการพิจารณาคดีที่เกี่ยวข้องกับ สหราชอาณาจักรในคดีของ *Kennedy v. the United Kingdom*¹⁰ แสดงให้เห็นว่าศาลอังกฤษยอมรับข้อกำหนดของอนุสัญญาในเรื่องการบังคับใช้กฎหมายในการเข้าแทรกแซงข้อมูลที่บุคคลสื่อสารถึงกันเพื่อวัตถุประสงค์ในการสืบสวนสอบสวนในการป้องกันภัยที่อาจเกิดขึ้นแก่รัฐหรือประชาชนได้ ซึ่งในคดี *Kennedy v the United Kingdom* ศาลกล่าวว่า “ถ้าการกระทำเพื่อการเข้าสอดแนมหรือกระทำเพื่อดักข้อมูลของประชาชน หากได้ดำเนินการตามข้อพึงปฏิบัติที่กำหนดโดยรัฐ อย่างเพียงพอและดำเนินการตามกระบวนการอำนาจของกฎหมายและกระบวนการในการออกหมายเพื่อการกระทำนั้นแล้ว ย่อมสามารถกระทำได้โดยไม่เป็นการฝ่าฝืนสิทธิของประชาชนแต่อย่างใด”¹¹ ดังนั้นจึงกล่าวได้ว่า การกระทำใดๆ เพื่อการเข้าถึงข้อมูลของประชาชนจำเป็นต้องอาศัยอำนาจตามกฎหมายเป็นการเฉพาะ และต้องดำเนินการภายใต้ข้อกำหนดของกฎหมายอย่างเคร่งครัด นอกจากนี้จากการศึกษาพบว่าจำเป็นอย่างยิ่งในการให้ความสำคัญการเก็บรักษาซึ่งข้อมูลที่ได้รับมาเพราะหากดำเนินการจัดเก็บอย่างไม่รอบคอบย่อมอาจเป็นอันตรายต่อบุคคลผู้เป็นเจ้าของข้อมูลได้

ปัจจุบันสหราชอาณาจักรมีภัยคุกคามที่มีผลต่อความปลอดภัยของสาธารณะ ซึ่งถือเป็นประเด็นที่กระทบความมั่นคงของชาติ Home Secretary, Amber Rudd ได้กล่าวเพิ่มเติมแก่กรณีนี้ว่า “ด้วยเทคโนโลยีอินเทอร์เน็ตในปัจจุบันที่เปลี่ยนแปลงไป และเป็นช่องทางสำคัญในการก่ออาชญากรรมขึ้น ดังนั้นเราจำเป็นต้องสร้างมาตรการเพื่อป้องกันการกระทำดังกล่าวเพื่อต่อสู้กับอาชญากรรมที่ท้าทาย อย่างไรก็ตาม

⁸ Andrew Murray, *Information Technology Law*, 3rd edited, (Great Britain, United Kingdom: Oxford University Press, 2016), pp. 590-593.

⁹ Ibid.

¹⁰ ECHR, op. cit

¹¹ Ibid.

ตาม การใช้อำนาจตามกฎหมายฉบับนี้จะอยู่ภายใต้สิทธิความคุ้มครองโดยการที่จะกระทำการใดๆ ต้องกระทำตามกฎหมายอย่างเคร่งครัด”¹²

2.1 อำนาจในการดักข้อมูล (Interception)¹³

ซึ่งถือเป็นข้อกำหนดและเงื่อนไขหลักที่นำไปบังคับใช้แก่กรณีอื่นๆ ในพระราชบัญญัติฉบับนี้ ด้วย โดยการดักข้อมูลตามพระราชบัญญัตินี้มีความหมายว่า การให้อำนาจแก่บุคคลใดๆ สามารถเข้าดำเนินการดักข้อมูลสื่อสารจากการโทรคมนาคม หรือ โทรเลข หรือไปรษณีย์ของบุคคลได้¹⁴

ทั้งนี้ การดำเนินเข้าดักข้อมูลที่บุคคลสื่อสารกันนั้นจะกระทำได้ก็แต่โดยอยู่ภายใต้บังคับของ มาตรา 6 แห่งพระราชบัญญัตินี้ที่ถือเป็นการกระทำการดักข้อมูลโดยชอบด้วยกฎหมายเท่านั้น กล่าวคือ อาศัยอำนาจตามหมายซึ่งออกโดยรัฐ การได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูล หรือภายใต้หลักการยินยอม ตามมาตรา 44 ถึง 52 ของพระราชบัญญัตินี้ หรือกรณีที่น่าจะเป็นเพื่อการบันทึกและจัดเก็บข้อมูลตามที่ กฎหมายกำหนดหรือตามหมายของศาลที่ได้รับการร้องขอจากผู้มีอำนาจ¹⁵ อย่างไรก็ตาม กฎหมายฉบับนี้ การดักข้อมูลนั้น ไม่รวมถึงการกระทำการสื่อสารในลักษณะแพร่ภาพและกระจายเสียง เป็นต้น¹⁶

2.2 การขออนุญาตเพื่อดำเนินการดักข้อมูล

อยู่ภายใต้บังคับมาตรา 15 แห่งพระราชบัญญัติฉบับนี้ ซึ่งแบ่งลักษณะการขออนุญาตใน 3 ลักษณะตามแต่ลักษณะของการใช้หมายเพื่อวัตถุประสงค์ที่แตกต่างกัน¹⁷ กล่าวคือ

1. หมายเพื่อการดักข้อมูล¹⁸ หมายถึง การออกหมายในลักษณะทั่วไปเพื่อการดักฟังข้อมูลสื่อสารทางระบบโทรเลข ระบบโทรคมนาคม หรือทางช่องทางติดต่อสื่อสารอื่นซึ่งให้อำนาจไว้ การเข้าถึง เพื่อให้ได้มาซึ่งข้อมูลทุกชนิดจากข้อมูลสื่อสารทางระบบโทรเลข ระบบโทรคมนาคม หรือทางช่องทาง

¹² “Investigatory Powers Bill receives Royal Assent” <https://www.gov.uk/government/news/investigatory-powers-bill-receives-royal-assent>, (last visited 4 December 2018).

¹³ Interception of Communications Draft Code of Practice, p.10.

¹⁴ Investigatory Powers Act 2016, Section 4.

¹⁵ Investigatory Powers Act 2016, Section 6.

¹⁶ Investigatory Powers Act 2016, Section 5.

¹⁷ Investigatory Powers Act 2016, Section 15.

¹⁸ Interception of Communications Draft Code of Practice, p. 30.

ติดต่อสื่อสารอื่นซึ่งให้อำนาจไว้ หรือเพื่อการระทำการเปิดเผยข้อมูลจากข้อมูลที่ได้รับมาตามหมายจากบุคคลที่หมายได้ให้อำนาจในการเข้าถึง¹⁹

2. หมายเพื่อการตรวจสอบ²⁰ หมายถึง การออกหมายเพื่อให้บุคคลใดๆ มีอำนาจในการเข้าตรวจสอบเนื้อหาที่เกี่ยวข้องเป็นการเฉพาะ ภายใต้บังคับของมาตรา 152 (4) ซึ่งเป็นการเข้าถึงข้อมูลส่วนบุคคลเป็นกรณีเฉพาะ และต้องดำเนินการภายใต้หลักการการดักข้อมูลขนาดใหญ่ตามส่วนที่ 6 ของพระราชบัญญัติฉบับนี้²¹

3. หมายเพื่อดำเนินการช่วยเหลือภายใต้ความร่วมมือ²² โดยมุ่งเน้นในการดำเนินการดักข้อมูลภายใต้ข้อตกลงหรือความร่วมมือระหว่างสหภาพยุโรปหรือในระหว่างประเทศ ตลอดจนการออกหมายในลักษณะความร่วมมือเพื่อดำเนินการเปิดเผยข้อมูลตามที่ได้มีการร้องขอภายใต้ความร่วมมือระหว่างประเทศ²³

2.3 ผู้มีอำนาจในการออกหมาย

พระราชบัญญัตินี้กำหนดให้ผู้มีอำนาจในการออกหมายในกรณีเป็นการทั่วไปเพื่อทำการดักข้อมูลเป็นอำนาจเฉพาะของบุคคลตามมาตรา 18 แห่งพระราชบัญญัตินี้²⁴ กล่าวคือ

1. Head of Intelligence Service
2. Director General of the National Crime Agency;
3. The Commissioner of Police of the Metropolis;
4. The Chief Constable of the Police Service of Northern Ireland;
5. The Chief Constable of the Police Service of Scotland;
6. The Commissioners for Her Majesty's Revenue and Customs;
7. The Chief of Defense Intelligence;
8. บุคคลผู้มีอำนาจภายใต้ข้อตกลงความร่วมมือระหว่างประเทศ หรือองค์กรที่กำหนดไว้

เป็นการเฉพาะ

¹⁹ Investigatory Powers Act 2016, Section 15 (2).

²⁰Interception of Communications Draft Code of Practice, p. 32.

²¹ Investigatory Powers Act 2016, Section 15 (3).

²² Interception of Communications Draft Code of Practice, p 34.

²³ Investigatory Power Act 2016, Section 15 (4).

²⁴ Investigatory Power Act 2016, Section 18.

นอกจากอำนาจตามมาตรา 18 ที่กำหนดบุคคลตามที่พระราชบัญญัติกำหนดไว้ให้มีอำนาจในการออกหมายแล้ว พระราชบัญญัติฉบับนี้ได้กำหนดอำนาจพิเศษให้แก่รัฐมนตรี (Secretary of State) เป็นผู้ที่มีอำนาจในการออกหมายเพื่อดำเนินการดักข้อมูลโดยอาศัยอำนาจแทนบุคคลตามที่ระบุไว้ในมาตรา 18 ได้²⁵ ซึ่งอำนาจของรัฐมนตรี (Secretary of State) แม้เป็นอำนาจพิเศษแต่จะกระทำได้อีกแต่โดยภายใต้เงื่อนไขอย่างเคร่งครัดตามมาตรา 19 ประกอบมาตรา 20²⁶

ในกรณีอาศัยอำนาจตามมาตรา 19 ประกอบมาตรา 20 แห่งพระราชบัญญัตินี้ กำหนดให้ในกรณีที่เป็นการทั่วไป และไม่ใช้กรณีเร่งด่วนตามมาตรา 24 เมื่อรัฐมนตรี (Secretary of State) พิจารณาเห็นชอบแล้วตามเงื่อนไขและวิธีการที่กำหนดไว้ให้ดำเนินการส่งหมายเช่นนั้นไปยังศาล (Judicial Commissioners) จะต้องดำเนินการพิจารณาความจำเป็นในการออกหมายของรัฐมนตรี (Secretary of State) ตามมาตรา 23 แห่งพระราชบัญญัตินี้ด้วย จึงจะสามารถดำเนินการบังคับใช้หมายซึ่งออกโดยอำนาจของรัฐมนตรีตามมาตรา 19 ประกอบมาตรา 20 ได้ ซึ่งระบบนี้เรียกว่า “Double Lock System หรือ Safeguard” ซึ่งเป็นมาตรการป้องกันการแทรกแซง หรือใช้อำนาจของรัฐมนตรีโดยมิชอบ และในกรณีที่ศาลพิจารณาไม่เห็นชอบต่อการขออนุญาตออกหมายแก่กรณีดังกล่าวแล้ว ให้ถือเป็นคำสั่งอันเป็นที่สุดไม่สามารถอุทธรณ์การพิจารณาใดๆ ได้อีก²⁷ ทั้งนี้การปฏิเสธไม่เห็นชอบต่อการออกหมายจำเป็นต้องแสดงเหตุผลประกอบคำพิจารณาเช่นนั้นมาพร้อมกับคำสั่งดังกล่าวด้วย²⁸

2.4 ระยะเวลาในการบังคับใช้หมาย

กรณีหมายเพื่อการดักข้อมูล หมายเพื่อการตรวจสอบหมายเพื่อดำเนินการช่วยเหลือภายใต้ความร่วมมือ พระราชบัญญัติฉบับนี้กำหนดให้สามารถกระทำได้ภายใน 6 เดือนนับแต่วันที่ได้รับอนุมัติหมาย อย่างไรก็ตาม กรณีที่เป็นหมายเร่งด่วนกำหนดให้มีระยะเวลา 5 วันนับแต่วันที่ออกหมาย เว้นแต่จะได้รับอนุมัติให้ขยายเวลาออกไปโดยรัฐมนตรี (Secretary of State) ²⁹

²⁵ Investigatory Powers Act 2016, Section 19.

²⁶ Interception of Communications Draft Code of Practice, pp. 37 – 38.

²⁷ Interception of Communications Draft Code of Practice, p. 43.

²⁸ Ibid.

²⁹ Investigatory Powers Act 2016, Section 32.

ทั้งนี้ การการขยายระยะเวลาหมายดังกล่าวจะกระทำได้แต่โดยภายในระยะเวลาของหมายซึ่งยังมีผลบังคับใช้อยู่ ภายใน 30 วันก่อนหมายดังกล่าวสิ้นอายุ หากปรากฏแก่กรณีว่ากระทำเกินเวลาที่กำหนดดังกล่าวย่อมไม่อาจกระทำการขยายเวลาได้³⁰

2.5 ผลของการกระทำการดัักข้อมูลติดต่อสื่อสารหรือให้ได้มาซึ่งข้อมูลโดยมิชอบ

พระราชบัญญัติฉบับนี้ กำหนดอำนาจ หน้าที่ วิธีการในการดำเนินการเพื่อกระทำการดัักข้อมูล ติดต่อสื่อสาร หรือได้มาซึ่งข้อมูลติดต่อสื่อสารอย่างเคร่งครัด ตั้งแต่การกำหนดตัวบุคคลผู้มีอำนาจที่จะกระทำได้ เงื่อนไขในการออกหมายเพื่อดัักข้อมูลติดต่อสื่อสาร หรือการร้องขอเพื่อเข้าถึงข้อมูลติดต่อสื่อสาร ที่ต้องดำเนินการภายใต้พระราชบัญญัตินี้ ซึ่งหากไม่ดำเนินการตามขั้นตอนดังกล่าว คณะกรรมการตามพระราชบัญญัตินี้ หรือรัฐมนตรีผู้รับมอบอำนาจ หรือศาลแล้วแต่กรณี มีอำนาจสั่งระงับหรือยกเลิกกิจกรรมดังกล่าวได้ทันที

อย่างไรก็ตาม นอกจากเงื่อนไขดังกล่าวมาแล้วนั้น ในกรณีที่มีการดำเนินการใดๆ เพื่อดัักข้อมูลติดต่อสื่อสารหรือกระทำให้ได้มาซึ่งข้อมูลติดต่อสื่อสารโดยไม่ปฏิบัติตามขั้นตอนดังกล่าว หรือในกรณีจงใจไม่ปฏิบัติตามขั้นตอนดังกล่าว พระราชบัญญัติอำนาจสอบสวน ค.ศ. 2016 กำหนดให้การกระทำอันฝ่าฝืนดังกล่าวถือเป็นความผิดตามพระราชบัญญัติฉบับนี้ และผู้กระทำการฝ่าฝืนอาจต้องรับโทษตามแต่กรณี

1. ผลของการกระทำการดัักข้อมูลติดต่อสื่อสารโดยมิชอบ³¹

การดำเนินการดัักข้อมูลติดต่อสื่อสารย่อมกระทำการโดยชอบด้วยกฎหมายเฉพาะการกระทำภายใต้บังคับมาตรา 6 ของพระราชบัญญัตินี้เท่านั้น ซึ่งรวมถึงการกระทำภายใต้ความยินยอมของผู้ถูกดัักข้อมูลดังกล่าวตามมาตรา 44 ถึง มาตรา 52 ด้วย

หากปรากฏว่าบุคคลใดเจตนากระทำการดัักข้อมูลติดต่อสื่อสารโดยมิชอบในสหราชอาณาจักรโดยไม่กระทำการภายใต้เงื่อนไขของพระราชบัญญัตินี้ ย่อมถือเป็นกระทำความผิดอาญาตามมาตรา 3 (1) อย่างไรก็ตาม การกระทำโดยไม่ได้ดำเนินการตามพระราชบัญญัตินี้ไม่ถือว่าเป็นความผิดอาญาเฉพาะ เมื่อเป็นการกระทำที่ได้รับอนุญาต หรือยินยอม เพื่อควบคุมและจัดการข้อมูลของเอกชนซึ่งหมายถึงผู้มีหน้าที่ในบริษัทของหน่วยงานข้อมูลติดต่อสื่อสารของเอกชนเองตามมาตรา 3 (2)

ทั้งนี้ ผู้กระทำความผิดอาญา ย่อมมีโทษจำคุกสูงสุด 2 ปี หรือปรับอย่างไม่จำกัดจำนวน (ตามดุลยพินิจของศาล)

³⁰ Investigatory Powers Act 2016, Section 33.

³¹ Interception of Communications Draft Code of Practice, pp. 15 – 16.

นอกจากนี้ พระราชบัญญัตินี้กำหนดให้คณะกรรมการสืบสวนตามพระราชบัญญัติฉบับนี้มีอำนาจกำหนดโทษปรับทางแพ่งสูงสุด 50,000 ปอนด์ ตามมาตรา 7 ซึ่งความผิดในส่วนนี้ย่อมมีความผิดหากผู้กระทำการฝ่าฝืน กระทำการให้ปรากฏว่า 1. ผู้กระทำความผิดตามมาตรา 3 กระทำความผิดโดยไม่มีเจตนาที่จะทำการดักข้อมูลติดต่อสื่อสารดังกล่าว 2. ผู้กระทำการดักข้อมูลติดต่อสื่อสารโดยไม่มีอำนาจภายในสหราชอาณาจักร 3. การติดต่อสื่อสารนั้นถูกดักข้อมูลติดต่อสื่อสารซึ่งส่งผ่านระบบโทรคมนาคมของรัฐ และ 4. ในขณะที่กระทำการดักข้อมูลติดต่อสื่อสาร ผู้กระทำความผิดอยู่ระหว่างการพยายามดำเนินการขอออกหมายเพื่อดำเนินการดักข้อมูลติดต่อสื่อสารดังกล่าว

2. ผลของการกระทำที่ได้มาซึ่งข้อมูลติดต่อสื่อสารโดยมิชอบ³²

การกระทำผิดในประเด็นเข้าถึงหรือได้มาซึ่งข้อมูลติดต่อสื่อสารโดยมิชอบตามพระราชบัญญัติฉบับนี้ แบ่งออกเป็น 2 ลักษณะ กล่าวคือ การเข้าถึงหรือได้มาซึ่งข้อมูลติดต่อสื่อสารกันโดยมิชอบ³³ และการเปิดเผยข้อมูลจากการเข้าถึงหรือได้มาซึ่งข้อมูลติดต่อสื่อสารโดยมิชอบ³⁴

1) การเข้าถึงหรือได้มาซึ่งข้อมูลติดต่อสื่อสารกันโดยมิชอบ

หากปรากฏแก่กรณีว่าเจ้าหน้าที่รัฐ หรือหน่วยงานของรัฐดำเนินการโดยรู้ถึงข้อเท็จจริง หรือโดยประมาทเลินเล่อต่อการเข้าถึง หรือได้มาซึ่งข้อมูลติดต่อสื่อสารกันจากผู้ให้บริการโทรคมนาคม หรือผู้ให้บริการไปรษณีย์โดยไม่มีอำนาจ บุคคลดังกล่าวมีความผิดและต้องระวางโทษตามพระราชบัญญัตินี้ กล่าวคือ โทษจำคุกสูงสุดไม่เกิน 12 เดือน หรือปรับไม่เกินกว่าโทษสูงสุดตามกฎหมายหรือทั้งจำทั้งปรับ

เว้นแต่สามารถพิสูจน์ได้ถึงการกระทำดังกล่าวว่าได้ดำเนินการโดยสำคัญผิดข้อเท็จจริงอย่างสุจริตว่าได้กระทำไปโดยมีอำนาจตามกฎหมาย³⁵

2) การเปิดเผยข้อมูลจากการเข้าถึงหรือได้มาซึ่งข้อมูลติดต่อสื่อสารโดยมิชอบ

การกระทำความผิดในส่วนนี้ มุ่งบังคับใช้กับผู้ให้บริการโทรคมนาคม รวมถึงลูกจ้างของผู้ให้บริการดังกล่าว หากกระทำการเปิดเผยข้อมูลโดยปราศจากเหตุผลอันสมควรโดยไม่มีอำนาจตามพระราชบัญญัติฉบับนี้ให้แก่บุคคลใด ผู้ให้บริการหรือบุคคลผู้กระทำการฝ่าฝืนต้องระวางโทษตาม

³² Communications Data Draft Code of Practice, p. 48.

³³ Investigatory Powers Act 2016, Section 11.

³⁴ Investigatory Powers Act 2016, Section 82.

³⁵ Interception of Communications Draft Code of Practice, pp. 90 – 91.

พระราชบัญญัตินี้ กล่าวคือ โทษจำคุกสูงสุดไม่เกิน 12 เดือน หรือ ปรับไม่เกินกว่าโทษสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ³⁶

3. บทสรุป

บทบาทสำคัญของการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลของบุคคลที่มีการติดต่อสื่อสารกัน ซึ่งเกิดจากความสัมพันธ์โดยตรงในการบริหารจัดการของรัฐหรือประเทศนั้นๆ ด้วยความจำเป็นเพื่อป้องกันภัยอันอาจเกิดขึ้นแก่รัฐในด้านต่างๆ ได้ โดยเฉพาะการเข้าถึงข้อมูลของบุคคลที่สื่อสารกันโดยหน่วยงานข่าวกรองแห่งชาติและการรักษาความปลอดภัยของสาธารณะ

ลักษณะของอำนาจภายใต้กฎหมายของสหราชอาณาจักรที่กำหนดให้อำนาจรัฐสามารถเข้าถึงข้อมูล หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน ได้สร้างเงื่อนไขและกลไกที่สำคัญเป็นลักษณะอำนาจเบ็ดเสร็จในการบังคับใช้กฎหมายเพื่อการเข้าถึงข้อมูลติดต่อสื่อสารระหว่างบุคคล โดยกำหนดหน่วยงานรัฐหรือเจ้าหน้าที่รัฐหากประสงค์จะดำเนินการใดๆ เพื่อให้ได้ข้อมูลการติดต่อสื่อสารนั้นต้องดำเนินการภายใต้กฎหมายฉบับเดียวกัน กล่าวคือพระราชบัญญัติอำนาจสืบสวน ค.ศ. 2016 (Investigatory Powers Act 2016) ซึ่งภายใต้พระราชบัญญัตินี้ดังกล่าวถือว่า สหราชอาณาจักรได้กำหนดเงื่อนไขและวิธีการในแต่ละขั้นตอนอย่างชัดเจน ไม่ว่าจะเป็นอำนาจในการดักข้อมูลการติดต่อสื่อสาร (Interception) อำนาจในการขอข้อมูลการติดต่อสื่อสารจากผู้ให้บริการ (Authorization to obtain Communication Data) อำนาจในการให้ผู้ให้บริการต้องกระทำการจัดเก็บข้อมูลการติดต่อสื่อสาร (Power of Data Retention)

นอกจากนี้ กระบวนการและขั้นตอนต่างๆ ถูกกำหนดให้อยู่ภายใต้เงื่อนไข Double Lock System เพื่อให้การกระทำต่างๆ อยู่ในความรับผิดชอบและสามารถตรวจสอบ หรือยับยั้งการกระทำที่ไม่ชอบได้ ทั้งเงื่อนไขในการควบคุมโดยรัฐมนตรี (Secretary of State) การควบคุมโดยศาล (Judicial Commissioners) อำนาจในการตรวจสอบโดยหน่วยงาน Single Point of Contact และท้ายที่สุดกระบวนการทุกขั้นตอนดังกล่าวจำเป็นต้องอยู่ภายใต้การควบคุมโดยคณะกรรมการสืบสวนตามพระราชบัญญัติด้วย

4. ข้อเสนอแนะ

แม้ปรากฏว่าปัจจุบัน ประเทศไทยได้มีการตรากฎหมายเกี่ยวกับการให้อำนาจหน่วยงานของรัฐในการเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารกัน แต่เมื่อพิจารณาแล้วพบว่าประเทศไทยตรากฎหมายในลักษณะดังกล่าวหลายฉบับตามแต่หน่วยงานต่างๆ อาทิ การกำหนดใน มาตรา 25 แห่งพระราชบัญญัติการ

³⁶ Interception of Communications Draft Code of Practice, pp. 91 – 92.

สอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 14 จัดว่า แห่งพระราชบัญญัติป้องกันและปราบปรามยาเสพติดให้โทษ พ.ศ. 2519 มาตรา 18 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ มาตรา 30 เป็นต้น จากการศึกษาพบว่าแม้มีลักษณะเป็นการให้อำนาจรัฐในการเข้าถึงข้อมูลหรือได้มาซึ่งข้อมูลติดต่อสื่อสาร แต่ก็มีลักษณะไม่ครอบคลุมในทุกกรณี มีลักษณะกระจัดกระจายหลักเกณฑ์ที่กำหนดไว้ในกฎหมายฉบับต่างๆ มีความแตกต่างกัน บางฉบับให้อำนาจเฉพาะการขอข้อมูลจากผู้ให้บริการ บางฉบับสามารถเข้าถึงข้อมูลได้โดยตรง ซึ่งแตกต่างจากกรณีศึกษากฎหมายของสหราชอาณาจักร ที่บัญญัติกฎหมายฉบับเดียวเป็นกฎหมายแผนแม่บทในการกระทำเพื่อเข้าถึงข้อมูลหรือให้ได้มาซึ่งข้อมูลของบุคคลที่สื่อสารถึงกัน ก่อให้เกิดหลักปฏิบัติในแนวทางเดียวกันและสามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานภายใต้กฎหมายฉบับเดียวกันได้อย่างมีประสิทธิภาพ

ฉะนั้น จากการศึกษาของผู้วิจัยต่อกฎหมายของสหราชอาณาจักรแล้วนั้น ผู้วิจัยมีความเห็นว่ากฎหมายของสหราชอาณาจักรน่าจะสามารณนำมาเป็นแบบอย่างในการร่างกฎหมายเพื่อให้ประเทศไทยมีกฎหมายเกี่ยวกับการเข้าถึงหรือได้มาซึ่งข้อมูลติดต่อสื่อสารกัน ทั้งในประเด็นวิธีการดำเนินการร้องขอเข้าถึงข้อมูลที่ต้องดำเนินการอย่างเป็นขั้นตอนเพื่อการขออนุญาต เพื่อดักสกัดข้อมูลที่มีมูลเหตุอันต้องสงสัย (Interception) และกำหนดบุคคลผู้มีอำนาจเฉพาะในการอนุมัติให้กระทำการเช่นนั้น อีกประการหนึ่งที่ผู้วิจัยพบจากการศึกษากฎหมายสหราชอาณาจักรนั้นคือมาตรการ Double Lock System หรือมาตรการตรวจสอบสองชั้น พบว่าในกรณีที่มีการขออนุญาตหรือใช้อำนาจเฉพาะกรณีพิเศษในการเข้าถึงหรือได้มาซึ่งข้อมูลของบุคคลสื่อสารกันนั้น แม้ผู้มีอำนาจกระทำการหรือในกรณีพิเศษที่รัฐมนตรีผู้มีอำนาจจะอนุมัติเพื่อให้สามารถดำเนินการเช่นนั้นได้แล้ว แต่การขออนุญาตเช่นนั้นต้องได้รับการอนุมัติจากศาล (Judicial Commissioners) ด้วยจึงจะสามารถใช้อำนาจตามหมายได้โดยชอบด้วยกฎหมาย ซึ่งการดำเนินการเช่นนี้ถือเป็นมาตรการป้องกันการดำเนินการแทรกแซงของบุคคลบางกลุ่ม และถือเป็นการพิทักษ์ซึ่งสิทธิของผู้ถูกเข้าถึงข้อมูลดังกล่าวมิให้ถูกล่วงล้ำสิทธิเกินจำเป็น

นอกจากนี้ ผู้วิจัยเห็นว่าประโยชน์ของการตรากฎหมายแม่บทต่อการบังคับใช้ในประเด็นนี้ย่อมนำไปสู่ประโยชน์ของการแก้ไขเปลี่ยนแปลงได้ง่ายกว่าการดำเนินการแก้ไขกฎหมายหลายฉบับ ด้วยเหตุที่ปัจจัยการเปลี่ยนแปลงไปของสังคมและเทคโนโลยีมีความผกผันต่อข้อมูลติดต่อสื่อสารทั้งในปัจจุบันและอนาคตที่มีความก้าวหน้าอย่างรวดเร็วและมีอยู่ทุกซอกทุกมุม และด้วยประการที่กฎหมายของไทยที่เกี่ยวข้องกับการเข้าถึงหรือได้มาซึ่งข้อมูลบุคคลสื่อสารถึงกันนั้น มีหลายฉบับกระจัดกระจายจึงควรให้มีแต่กฎหมายฉบับเดียวเป็นเอกเทศและสามารถบังคับใช้ได้อย่างเป็นรูปธรรมยิ่งขึ้น

บรรณานุกรม

ECHR, Factsheet – Mass Surveillance, (Echr.coe.int, 2018), https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf, (last visited 2 December 2018).

Halperin, Morton, “Multilateral Standards for Electronic Surveillance for Intelligence Gathering” Investigatory Powers Review, 2, <https://terrorismlegislationreviewer.independent.gov.uk/wpcontent/uploads/2015/06/Submissions-H-Z.pdf>, (last visited 9 December 2018).

Lloyd, Ian J., Information Technology Law, 8th edited, (Great Britain, United Kingdom: Oxford University Press, 2017).

Murray, Andrew, Information Technology Law, 3rd edited, (Great Britain, United Kingdom: Oxford University Press, 2016).

News, B., “UK Surveillance Powers Explained” (2015) <https://www.bbc.com/news/uk-34713435>, (last visited 9 December 2018).

Privacy and Human Right, An International Survey of Privacy Laws and Practice, <http://gilc.org/privacy/survey/intro.html>, (last visited 12 December 2018).

Simcox, Robin in The Henry Jackson Society, “Investigatory Powers Review” (2014) <https://terrorismlegislationreviewer.independent.gov.uk/wpcontent/uploads/2015/06/Submissions-H-Z.pdf>, (last visited 10 September 2018).

Law

Investigatory Powers Act 2016

Investigatory Powers Bill (Explanatory Notes), Published April 2016

Investigatory Powers Bill. Factsheet – Authorization