

การศึกษาและการวิเคราะห์เชิงนิติปรัชญาจากการกระทำของแฮ็กเกอร์หมวกเทา
A study and legal philosophy analysis of Grey Hat Hacker's action

จารุชา หมายสวัสดิ์

Jarucha Maisawat

จารุพร กัลยาวัฒนเจริญ

Charuporn Kanrayawatthanajaroen

ศุภกร วีระเพ็ชร

Supakorn Veerapetch

สุวิจักขณ์ กิระวิทยา

Suvijuck Kiravitaya

พลิชฐ์ นริสรกุล

Pasit Naritkul

นิสิตในหลักสูตรนิติศาสตรบัณฑิต (ปริญญาตรี)

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330

LL. B Candidates

Faculty of Law, Chulalongkorn University, Phayathai Road, Wangmai, Pathumwan, Bangkok 10330

Corresponding author e-mail: 6340026934@student.chula.ac.th

(Received: March 29, 2024; Revised: April 1, 2024; Accepted: April 1, 2024)

บทคัดย่อ

ในยุคโลกาภิวัตน์ที่เทคโนโลยีสารสนเทศมีการพัฒนาอย่างก้าวกระโดด ทำให้อาชญากรรมไซเบอร์เป็นหนึ่งในอาชญากรรมที่ต้องเฝ้าระวัง แต่อย่างไรก็ดี อาชญากรทางไซเบอร์เหล่านี้ก็อาจจะได้เจตนาที่มุ่งร้ายเสมอไป แม้จะมีความเสียหายเกิดขึ้น อาชญากรเหล่านี้เป็นกลุ่มแฮ็กเกอร์หมวกเทา หรือที่เรียกกันในนามว่า Gray Hat Hacker อันจัดว่าเป็นกลุ่มอาชญากรที่ไม่มีความชัดเจนทางศีลธรรม เช่น กลุ่มนักเคลื่อนไหวที่ใช้เทคโนโลยีในการแฮ็กข้อมูล (Hacktivist) และผู้ให้เบาะแส (Whistleblower)

แฮ็กเกอร์หมวกเทานั้นมักจะมีเป้าหมายเป็นหน่วยงานหรือองค์กรต่าง ๆ ที่มองว่าไม่ถูกต้อง/ไม่สอดคล้องกับแนวคิดของพวกเขา ไม่ว่าจะเป็นประเด็นความเห็นทางการเมืองหรือการดำเนินการบางอย่าง จึงได้มีการก่ออาชญากรรมไซเบอร์เพื่อเป็นการต่อต้าน

ในบทความนี้ทำการศึกษาและวิเคราะห์หลักการทางนิติปรัชญาต่าง ๆ เช่น การอภิปรายของฮาร์ทและฟูลเลอร์ ความคิดเห็นของดอว์กิน เพื่อพิสูจน์ความชอบธรรมจากการกระทำของแฮ็กเกอร์หมวกเทา

คำสำคัญ : แฮ็กเกอร์หมวกเทา, อาชญากรรมไซเบอร์, นิติปรัชญา

Abstract

In the age of globalization, technology has been evolving persistently. Putting cybercrimes at the forefront of specific priority crime threats. However, cybercrimes do not

always communicate the bad intentions of the miscreant. These criminals may fall into the category of morally ambiguous felons or gray-hat hackers, such as hacktivists and whistleblowers.

These morally ambiguous hackers typically target entire Industries or specific organizations that they consider to not align with their political views or practices. In which they respond with a cyber-attack.

This article aims to discuss the principles of the philosophy of law that may justify gray-hat hackers' actions. For instance, Hart and Fuller's Debate on Law and Morality Ronald Dworkin's theory may confer validity on gray-hat hackers' actions.

Keywords : Gray-hat hackers, Cybercrimes, Philosophy of law

1. บทนำ

ในยุคโลกาภิวัตน์เทคโนโลยีได้พัฒนาไปไกลและอาชญากรรมไซเบอร์เป็นอาชญากรรมที่ต้องเฝ้าระวัง การกระทำของกลุ่มที่ไม่มีความชัดเจนทางศีลธรรมอย่างกลุ่มแฮ็กเกอร์หมวกเทา จึงเป็นเรื่องที่ต้องพิจารณา อย่างถี่ถ้วนเพื่อให้สอดคล้องกับสภาพสังคมที่เปลี่ยนไป

ด้วยเหตุนี้ บทความนี้จึงต้องการที่จะยกแนวคิดและหลักการของนักปรัชญากฎหมายไม่ว่าจะเป็น สำนักคิดทางกฎหมายบ้านเมืองหรือสำนักคิดทางกฎหมายธรรมชาติ

เนื่องจากแฮ็กเกอร์หมวกเทานั้นมักจะมีเป้าหมายเป็นหน่วยงานหรือองค์กรต่าง ๆ ที่มองไม่เห็นทางการเมืองหรือการดำเนินการบางอย่าง ซึ่งแฮ็กเกอร์เหล่านี้มองว่าไม่ถูกต้อง จึงได้มีการก่ออาชญากรรมไซเบอร์ เพื่อเป็นการต่อต้าน จึงเป็นการกระทำที่สะท้อนถึงพื้นฐานของกฎหมายธรรมชาติโดยตรงคือกฎหมายนั้นมีรากฐานมาจากศีลธรรมต่าง ๆ ที่มีอยู่ในธรรมชาติ แม้จะขัดต่อหลักกฎหมายบ้านเมืองที่มองว่ากฎหมายนั้นมาจากรัฐธำมณีปัตย์

ดังนั้น บทความฉบับนี้จึงมุ่งเน้นที่จะตอบคำถามว่าการกระทำของแฮ็กเกอร์หมวกเทานั้นมีแนวคิด และหลักการของสำนักกฎหมายใดบ้างที่จะพิสูจน์ความชอบธรรมของการกระทำของแฮ็กเกอร์เหล่านี้

โดยในหัวข้อที่ 2 จะเป็นการบรรยายถึงความหมาย ความเป็นมา ประเภท และลักษณะแต่ละประเภทของแฮ็กเกอร์

ในหัวข้อที่ 3 จะเป็นการพูดถึงแนวคิดและหลักการเชิงนิติปรัชญาที่เกี่ยวข้องกับแฮ็กเกอร์โดยในเบื้องต้นจะเป็นการอธิบายแนวคิดของ ฮาร์ท (Herbert Lionel Adolphus Hart) ในเรื่อง Rules of Recognition หรือ แนวคิดที่สำคัญเรื่องกฎที่กำหนดกฎเกณฑ์การรับรองความเป็นกฎหมายที่สมบูรณ์ แนวคิดของฟูลเลอร์ (Lon L. Fuller) และแนวคิดของดวอร์กิน (Ronald Dworkin)

ในหัวข้อที่ 4 จะมีการวิเคราะห์เชิงนิติปรัชญาจากการกระทำของแฮ็กเกอร์หมวกเทา

ในหัวข้อที่ 5 จะมีการสรุปความคิดรวบยอดในการพิสูจน์ความชอบธรรมของการกระทำของกลุ่มแฮ็กเกอร์หมวกเทา

2. ความหมาย ความเป็นมา ประเภท และลักษณะแต่ละประเภทของแฮ็กเกอร์

ความปลอดภัยทางไซเบอร์ หรือ Cyber Security เป็นเทคโนโลยี กระบวนการและวิธีปฏิบัติที่ถูกออกแบบมาเพื่อปกป้องเครือข่าย อุปกรณ์ โปรแกรมและข้อมูลจากการโจมตี ความเสียหายหรือการเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต หรือแฮ็กเกอร์ แต่คำว่าแฮ็กเกอร์ตามพจนานุกรมนั้นมักหมายถึงผู้ที่สนใจเรียนรู้คอมพิวเตอร์อย่างจริงจังจนเกินไปและที่มีความชำนาญในการใช้คอมพิวเตอร์ไปในทางที่ผิดกฎหมาย ซึ่งเป็นการแสดงนิยามของแฮ็กเกอร์หมวกดำ ซึ่งเป็นประเภทย่อยคำว่าของคำแฮ็กเกอร์เท่านั้น เมื่อความหมายในพจนานุกรม ไม่สามารถนิยามความหมายของคำนี้ได้ครอบคลุม จึงสามารถอนุมานได้ว่ากฎหมายที่บังคับใช้อยู่ นั้นก็ยังไม่สามารถออกกฎหมายที่ครอบคลุมทุกประเภทของแฮ็กเกอร์ได้

โดยคำว่าแฮ็กเกอร์นั้นสามารถแบ่งได้เป็น 3 ประเภทใหญ่ ๆ คือ แฮ็กเกอร์หมวกดำ แฮ็กเกอร์หมวกขาว และแฮ็กเกอร์หมวกเทา โดยแต่ละประเภทมีลักษณะดังต่อไปนี้

แฮ็กเกอร์หมวกดำ (Black Hat Hacker) เป็นแฮ็กเกอร์ที่มีเจตนาสร้างความเสียหายแก่เป้าหมายเพื่อผลประโยชน์ส่วนตัว

แฮ็กเกอร์หมวกขาว (White Hat Hacker) เป็นแฮ็กเกอร์ประเภทเดียวที่ถูกจัดว่าเป็นความปลอดภัยทางไซเบอร์ เนื่องจากแฮ็กเกอร์กลุ่มนี้ถูกว่าจ้างจากนิติบุคคลหรือปัจเจกชนเพื่อให้ทำการเจาะระบบเพื่อหาช่องโหว่และจุดอ่อนแอของระบบนั้น จึงเป็นแฮ็กเกอร์ประเภทเดียวที่ได้รับความคุ้มครองจากกฎหมาย

แฮ็กเกอร์หมวกเทา (Grey Hat Hacker) นั้นเป็นแฮ็กเกอร์ที่จะทำการเจาะระบบเพื่อเอาข้อมูลต่าง ๆ มาโดยผิดกฎหมายเช่นเดียวกับแฮ็กเกอร์หมวกขาว แต่ไม่มีเจตนาสร้างความเสียหาย แต่ในบางกรณีจะมีสร้างความเสียหายบ้าง แต่ความเสียหายนั้นเกิดจากการรักษาความสงบเรียบร้อยและศีลธรรมอันดีของสังคม ทำให้การกระทำทางไซเบอร์หลายรูปแบบสามารถนำมาจัดเป็นประเภทย่อยของแฮ็กเกอร์ประเภทนี้ได้ เช่น Hacktivist และ Whistleblower

Hacktivist หรือกลุ่มนักเคลื่อนไหวที่ใช้เทคโนโลยีในการแฮ็กข้อมูล โดยอาจเคลื่อนไหวตามลำพังหรืออาจทำงานรวมกันเป็นกลุ่ม นักเคลื่อนไหวเหล่านี้มีเป้าหมายในการเคลื่อนไหวได้หลายประเด็น แต่โดยรวมแล้วเป็นการเคลื่อนไหวต่อต้านเพื่อให้เกิดความเปลี่ยนแปลงด้านความเสมอภาคและเสรีภาพ เช่น กลุ่มแฮ็กเกอร์ที่มีชื่อว่า “แอนโนนิมัส” (Anonymous) ที่ในช่วงแรกนั้นเป็นแฮ็กเกอร์หมวกเทาตามคำนิยามทั่วไป แต่การกระทำที่ทำให้กลุ่ม Anonymous ได้กลายเป็น Hacktivist คือการปฏิบัติการในปี ค.ศ. 2008 ที่ได้โจมตีลัทธิไซแอนโทโลจี (Church of Scientology) โดยรูปแบบ Distributed Denial of Service (DDoS) ซึ่งเป็นการโจมตีทางไซเบอร์รูปแบบหนึ่งที่มีรูปแบบการโจมตี คือ แฮ็กเกอร์จะทำการส่งคำขอเข้าถึงข้อมูลจากหลายที่ไปยังเว็บไซต์ที่ต้องการโจมตีพร้อม ๆ กัน ทำให้เว็บไซต์นั้นมีปริมาณ Traffic มากเกินกว่าที่ Server ของเว็บไซต์นั้นจะสามารถรองรับได้¹ ส่งผลให้เว็บไซต์ของไซแอนโทโลจีไม่สามารถใช้งานได้อย่างต่อเนื่องเป็นเวลานานกว่าหนึ่งสัปดาห์ ควบคู่ไปกับการประท้วงที่สำนักงานไซแอนโทโลจีหลายแห่ง หรือการที่กลุ่ม Anonymous มีความพยายามโจมตีกลุ่มผู้ก่อการร้าย ISIS โดยทำการสกัดยุทธวิธีหาแนวร่วมของ ISIS ไม่ว่าผ่านเว็บไซต์และโซเชียลมีเดียต่อเนื่อง² แม้เจตนารมณ์ของกลุ่ม Anonymous ยังไม่เป็นที่แน่ชัด แต่ก็มีความวิพากษ์วิจารณ์ได้คาด

¹ Kanlaya Wonggate, 'DDoS คืออะไร? ทำไมเว็บไซต์ชื่อดังถึงล่ม?' (Nipa Cloud, 17 ธันวาคม 2564) <<https://nipa.cloud/th/blog/what-ddos-is>>

² จักรกฤษณ์ สิริริน, 'Activist + Hacker = Hacktivist' (Matichon Weekly, 14 ตุลาคม 2565) <https://www.matichonweekly.com/column/article_613116>

เดว่ากลุ่ม Anonymous จะโจมตีผู้ใดก็ตามที่ขัดขวางเสรีภาพในการรับข่าวสารของประชาชน³ หรือกลุ่มนักเคลื่อนไหวที่ใช้เทคโนโลยีอีกกลุ่มหนึ่งที่เรียกตัวเองว่า Impact Team ได้ทำการเจาะข้อมูลของเว็บไซต์ Ashley Madison โดยประกาศว่าจะเผยแพร่ข้อมูลเว้นแต่บริษัทแม่ของแมดิสันจะปิดเว็บไซต์ลง เนื่องจากเป็นเว็บไซต์สำหรับผู้แต่งงานแล้วที่ไม่ได้มองหา “ความรัก” แต่มองหา “ความสัมพันธ์” ตามที่ค่านิยมของโฆษกของ Ashley Madison ได้กล่าวไว้เมื่อเว็บไซต์ได้เข้ามาเปิดบริการในประเทศไทย แต่คำเปรยของเว็บไซต์นี้อาจแสดงถึงเป้าหมายของเว็บไซต์นั้นได้ดีว่า “Life is Short. Have an Affair.” หรือ “ชีวิตมันสั้น อย่าก้มหน้าต้องมึน” ซึ่งทำให้เกิดปัญหาเชิงศีลธรรมตามมาแม้ตัวเว็บไซต์จะประกาศว่าไม่สนับสนุนการนอกใจก็ตาม⁴ เมื่อบริษัทแม่ของแมดิสันไม่ได้ทำการปิดบริการเว็บไซต์ Ashley Madison ลง Impact Team จึงได้ทำการเปิดเผยข้อมูลทั้งหมด ไม่ว่าจะเป็นข้อมูลที่น่าจะต้องถูกลบออกจากระบบด้วย ในกรณีที่ลูกค้าเริ่มรู้สึกผิดต่อคู่สมรสของตัวเอง และอยากเลิกใช้บริการจึงจ่ายค่าบริการเพิ่มเพื่อลบข้อมูลนั้น⁵ การเผยแพร่นี้สร้างความเสียหายเป็นอย่างมากและทำให้ผู้ใช้บริการจบชีวิตตัวเองลงอย่างน้อย 2 คน แต่ Hacktivist หรือกลุ่มนักเคลื่อนไหวที่ใช้เทคโนโลยีในการแฮ็กข้อมูลนี้มักไม่ถูกดำเนินคดีหรือตรวจสอบจากภาครัฐ

Whistleblower หรือผู้ให้เบาะแส เป็นบุคคลที่เตือนภัยหรือเปิดโปงว่าองค์กร หน่วยงาน หรือประเทศได้มีการกระทำที่ผิดกฎหมาย ซึ่งในบางกรณีผู้ให้เบาะแสก็ต้องทำการเจาะระบบหรือกระทำการบางอย่างที่ผิดกฎหมายเพื่อเปิดโปงองค์กรนั้น เช่น เอ็ดเวิร์ด โจนส์ สโนว์เดน อดีตผู้รับจ้างทางเทคนิคของสำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา (NSA) และอดีตนักวิเคราะห์ข่าวกรองแห่ง CIA หน่วยงานราชการด้านข่าวกรองต่างชาติของพลเมืองของรัฐบาลกลางสหรัฐ ได้ออกมาเปิดเผยว่า รัฐบาลสหรัฐอเมริกาได้ทำการดักฟังและเก็บข้อมูลของประชาชนผ่านทางโทรศัพท์และอินเทอร์เน็ต และได้แพร่ไวรัสคอมพิวเตอร์ชนิดมัลแวร์สู่เครือข่ายคอมพิวเตอร์มากกว่า 5,000 เครือข่ายทั่วโลกเพื่อเก็บข้อมูล การเปิดโปงในครั้งนี้ทำให้สโนว์เดนต้องหลบหนีออกจากประเทศ⁶ และถูกฟ้องทั้งหมด 3 ข้อหา ได้แก่ จารกรรมข้อมูล เผยข้อมูลด้านกลาโหมโดยไม่ได้รับอนุญาต และขโมยทรัพย์สินของรัฐบาล ซึ่งมีโทษจำคุกรวมกันสูงสุดถึง 30 ปี ในขณะเดียวกัน Whistleblower ในกรณีอื่น เช่น ในกรณีของเธรานอส (Theranos) สตาร์ทอัพเครื่องตรวจเลือดซึ่งอ้างว่าเป็นเครื่องตรวจเลือดที่สามารถจับโรคภัยได้ด้วยเลือดไม่กี่หยดในเวลาอันรวดเร็ว ซึ่ง Tyler Shultz และ Erika Cheung อดีตนักวิทยาศาสตร์ของบริษัทได้ออกมาเปิดเผยว่าเทคโนโลยีตรวจเลือดที่กล่าวอ้างของเธรานอสนั้น แท้จริงแล้วใช้งานไม่ได้ตามที่โฆษณาเอาไว้ ซึ่งการเปิดโปงในครั้งนี้ทำให้เอลิซาเบธ โฮล์มส์ ผู้ก่อตั้งบริษัทเธรานอสกับนวัตกรรมที่จะเข้ามาพลิกโฉมวงการแพทย์นี้ มีความผิดฐานความผิดฉ้อโกง 4 ข้อหาจากทั้งหมด 11 ข้อหา โดยมี 3 ข้อหาที่เป็น ‘Wire fraud’ หรือการฉ้อโกงผ่านการสื่อสารอิเล็กทรอนิกส์ และอีก 1 ข้อหาเป็นข้อหาสมคบกันฉ้อโกง (Conspiracy to commit wire fraud) แต่ละข้อหาโทษจำคุกสูงสุด 20 ปี และผู้ให้เบาะแสทั้งสองนั้นกลายเป็นพยานในคดี แม้ทั้งสองกรณีจะมีจุดมุ่งหมายเพื่อเปิดโปงว่าองค์กร หน่วยงาน หรือประเทศได้มีการกระทำที่ผิดกฎหมายเช่นเดียวกัน

³ K. Bott, 'Hacktivist เขาคือใครในสงครามไซเบอร์?' (GQ Thailand, 24 เมษายน 2560) <<https://www.gqthailand.com/culture/article/who-is-hacktivist>>

⁴ 'สัมพันธ์ลับสุดหมิ่นเหม่? แบบ Ashley Madison' (Forbes Thailand, 16 เมษายน 2558) <<https://forbesthailand.com/forbes-life/ashley-madison>>

⁵ มาร์ค Blognone, 'เมื่อเว็บไซต์ “หาซู่” โดนแฮ็ก!!' (Thairath, 27 สิงหาคม 2558) <<https://www.thairath.co.th/news/tech/521084>>

⁶ 'Isolated, therefore I am' (The 101.World, 28 มิถุนายน 2560) <<https://www.the101.world/isolated-therefore-i-am/?fbclid=IwAR2ncqDljxsw9OVsTmx29zw-dFop0iVWOsxesENnjZrGZf5dGDp-D0KUNM>>

จากกรณีในข้างต้นจึงทำให้เกิดคำถามว่าอะไรคือขอบเขตของแอ็กเกอร์หมวกเทาแบบกลุ่มนักเคลื่อนไหวที่ใช้เทคโนโลยีในการแอ็กข้อมูล และผู้ให้เบาะแส ที่จะไม่ถูกดำเนินคดีหรือตรวจสอบจากภาครัฐ แม้ว่าการกระทำเหล่านี้จะถือว่าเป็นอาชญากรรมคอมพิวเตอร์เมื่อพิจารณาจากกฎหมายในแง่ข้อเท็จจริง (Positivism) หรือกฎหมายบ้านเมือง นำไปสู่การพิจารณาประกอบหลักแนวคิดทางกฎหมายที่เกี่ยวข้องต่อไป

3. แนวคิดและหลักการเชิงนิติปรัชญาที่เกี่ยวข้องกับแอ็กเกอร์

ในความคิดเห็นของฮาร์ทนั้นฮาร์ทมองว่ากฎหมายและศีลธรรมนั้นเป็นสิ่งที่เกี่ยวข้องกันแต่อย่างใด ไม่จำเป็นต้องมีการพิจารณาถึงศีลธรรมแต่อย่างใดเลยก็สามารถสร้างกฎหมายให้สมบูรณ์ได้ หากเพียงแต่เราสามารถนำศีลธรรมในการตัดสินว่าเป็นกฎหมายที่ชอบด้วยศีลธรรมหรือไม่ โดยการสมบูรณ์ของกฎหมายนั้นเพียงแค่ทำตามวิธีการบัญญัติกฎหมายให้ถูกต้องก็เป็นพอ เพียงเท่านั้นก็จะสมบูรณ์เป็นกฎหมายได้แล้ว นอกจากนี้กฎหมายที่ขาดศีลธรรมก็ยังสามารถสมบูรณ์เป็นกฎหมายได้หากได้กระทำตามขั้นตอนที่กล่าวมาข้างต้นอย่างถูกต้อง จะเห็นได้ว่า กฎหมายและศีลธรรมในความคิดของฮาร์ทนั้นถูกแบ่งแยกกันอย่างชัดเจน⁷ ไม่มีความเกี่ยวข้องกันแต่อย่างใด เพียงแต่สามารถใช้ศีลธรรมเข้ามาเพื่อพิจารณาว่ากฎหมายนั้นเป็นกฎหมายที่ดีหรือไม่เพียงเท่านั้น

นอกจากนี้ ในความคิดเห็นของฮาร์ทนั้นฮาร์ทยังมองว่ากฎหมายนั้นมีอยู่ 2 ประเภท กล่าวคือ กฎหมายปฐมภูมิ และกฎหมายทุติยภูมิ โดยกฎหมายปฐมภูมินั้น คือ กฎหมายที่ถูกกำหนดเพื่อสร้างหน้าที่ของบุคคลในสังคมว่าต้องทำอะไรและห้ามทำอะไร และกฎหมายทุติยภูมินั้น คือ กฎหมายที่คนในสังคมยอมรับและนำเข้ามาปรับใช้กับสภาพสังคมนั้น โดยที่เรียกว่ากฎแห่งการยอมรับ (Rule of recognition) ซึ่งเป็นการยอมรับกฎหมายปฐมภูมิเข้ามาเป็นกฎของสังคมนั้น⁸ เพราะฉะนั้นสิ่งที่สำคัญในการที่จะเป็นกฎของสังคมหรือกฎหมายนั้นต้องได้รับการยอมรับจากผู้ใช้อย่างแน่นอน อย่างไรก็ตาม ในขั้นของการยอมรับกฎหมายทุติยภูมินั้นการยอมรับนั้นเป็นเพียงการยอมรับจากฝ่ายนิติบัญญัติเท่านั้น โดยที่ประชาชนในสังคมนั้นต้อง “ปฏิบัติตามกฎหมายปฐมภูมิ” แต่ไม่จำเป็นต้อง “ยอมรับ” กฎหมายทุติยภูมิ มีเพียงแค่ฝ่ายนิติบัญญัติเท่านั้นที่จำเป็นต้อง “ยอมรับ” กฎหมายทุติยภูมิเท่านั้น และทั้งประชาชนและนิติบัญญัติไม่มีความจำเป็นต้อง “ยอมรับ” กฎหมายปฐมภูมิ แต่อย่างไรก็ดี กฎหมายก็ต้องได้รับการยอมรับจากทางใดทางหนึ่ง มิเช่นนั้นก็จะไม่เป็นกฎหมาย เนื่องจากจะไม่มีใครกดดันทางสังคมหากว่าคนในสังคมทั้งหมดไม่ได้ยอมรับกฎหมาย เพราะฉะนั้นกฎหมายจึงไม่ได้ตั้งอยู่บนพื้นฐานของศีลธรรมหรืออำนาจ แต่ตั้งอยู่บนการยอมรับของผู้มีอำนาจนิติบัญญัติ⁹

ในทางกลับกันแล้ว มุมมองถึงความเกี่ยวข้องระหว่างกฎหมายและศีลธรรมมีความแตกต่างกันอย่างสิ้นเชิงสำหรับนักนิติปรัชญาสำนักกฎหมายธรรมชาติอย่าง Lon Fuller ซึ่งเห็นว่ากฎหมายคือ “องค์รวมแห่งพฤติกรรมมนุษย์ในการกำกับกฎ”¹⁰ ฟูลเลอร์เชื่อว่าจุดประสงค์ของกฎหมายคือ เพื่อคงไว้ซึ่งประสงค์แห่ง

⁷ Kaila Morin, 'Bridging the conceptual gap between law and morality: a critical response to H.L.A. Hart's the concept of law' (2011) 1 UCL Journal of Law and Jurisprudence 120, 125.

⁸ William C. Starr, 'Law and Morality in H.L.A. Hart's Legal Philosophy' (1984) 67 Marquette Law Review 673, 677.

⁹ Michael Payne, 'The Basis of Law in Hart's "The Concept of Law"' (1978) 9 The Southwestern Journal of Philosophy 11, 12-13.

¹⁰ Lon Fuller, *The Morality of Law*, rev. ed. (Yale University Press, 1969) 106.

ศีลธรรมและต้องการทำให้หลักแนวคิดอันเป็นธรรมชาติอย่างประเด็นของศีลธรรมมีความเป็นรูปธรรมมากขึ้น ด้วยการตั้งหลักนิติธรรม¹¹ เพื่อตัดสิน “ความชอบธรรม” ของกฎหมาย

แนวคิดของฟุลเลอร์ในประเด็นของความเกี่ยวข้องระหว่างศีลธรรมนั้นเป็นการขัดกับฮาร์ทที่เห็นว่ากฎหมายไม่ใช่สิ่งที่ต้องพิเคราะห์ว่าชอบธรรมในเชิงของแนวคิดทางศีลธรรมหรือไม่ ถึงแม้จะเป็นกฎหมายที่ขัดต่อสามัญสำนึกก็มิได้ทำให้กฎหมายไม่เป็นกฎหมายแต่อย่างใด โดยฟุลเลอร์มองว่าการมีอยู่ของหลักนิติธรรมเช่นนี้ถือเป็นการสร้างบรรทัดฐานทั่วไปที่ทำให้สังคมมี “หน้าที่ทางศีลธรรม” ที่จะยอมรับกฎหมายที่เป็นไปตามหลักเช่นนั้น และเป็นการแสดงให้เห็นถึงจุดประสงค์ในการเคารพกฎหมายไม่ใช่แค่เพียงเพราะกฎหมายเป็นสิ่งที่ตราโดยฝ่ายนิติบัญญัติ และหน้าที่ทางศีลธรรมเช่นว่านี้จะมีหรือไม่มีย่อมแล้วแต่กรณี หากรัฐบาลเองมีการละเมิดกฎหมายหรือมีการใช้กฎหมายบังคับอย่างไม่เท่าเทียมหรือเป็นไปด้วยอคติ ผู้คนในสังคมย่อมไม่มีหน้าที่ที่ต้องเคารพการปกครองเช่นนั้น¹² กรณีหนึ่งที่น่าสนใจจากการโต้แย้งถ้อยความคิดโดยฟุลเลอร์เห็นได้จากตัวอย่างเรื่องกฎหมายนาซีที่ตรากฎหมาย ซึ่งเห็นโดยวิญญูชนทั่วไปว่าเป็นกฎหมายที่สร้างความแตกแยกและเหยียดหยามสิทธิของมนุษย์จากความแตกต่างทางเชื้อชาติที่ถึงแม้ว่าฮาร์ทไม่ได้แสดงความเห็นเป็นประจักษ์ว่านาซีเป็นกลุ่มอำนาจที่ขัดต่อศีลธรรมหรือไม่ แต่มองตามแนวคิดสำนักกฎหมายบ้านเมืองของฮาร์ทกฎหมายดังกล่าวนี้มีความชอบธรรม เนื่องจากเป็นกฎหมายที่ออกโดยกระบวนการนิติบัญญัติที่ถูกต้อง แม้ว่าเนื้อหาสาระของกฎหมายนั้นจะขัดต่อหลักศีลธรรมก็ตามก็ต้องเชื่อฟังเพราะกฎหมายคือกฎหมาย ฟุลเลอร์จึงมองว่าแนวคิดแบบสำนักกฎหมายบ้านเมือง “กรุยทาง” ให้กับฮิตเลอร์¹³ ทั้งนี้ ฮาร์ทได้แสดงถ้อยความคิดเกี่ยวกับ minimum content of law ที่สอดคล้องกับความเห็นของฟุลเลอร์ แต่มิได้เป็นการขัดกับความคิดว่ากฎหมายและศีลธรรมไม่จำเป็นต้องคาบเกี่ยวกันอยู่ดี การวิพากษ์ของฟุลเลอร์ได้แสดงถึงมุมมองที่กว้างยิ่งขึ้นของการตราและการเกิดของกฎหมาย โดยยึดความเป็นนามธรรมของ “ศีลธรรม” ประกอบการอธิบาย แม้จะไม่ปรากฏว่าฟุลเลอร์ได้อธิบายชัดเจนว่าศีลธรรมคืออะไร แต่การวางแนวเช่นว่าสำหรับการหา “ความชอบธรรม” ของกฎหมายนั้นเป็นการแสดงให้เห็นถึงวิธีที่หลักบางอย่างมีการจำกัดอำนาจของฝ่ายนิติบัญญัติผู้ร่าง และเหตุที่ปัจเจกชนในสังคมจะเชื่อฟังกฎหมายแม้จะขัดต่อแนวคิดทางศีลธรรมที่เป็นปัจเจกของตนเนื่องว่ากฎหมายเช่นนั้นมี “ความชอบธรรม” ตามประการที่ฟุลเลอร์เสนอ

จากที่ได้กล่าวมาข้างต้น นอกจากการที่ฟุลเลอร์ได้ออกมาวิพากษ์งานเขียนทางวิชาการของฮาร์ท ยังคงมีนักวิชาการอีกหนึ่งท่านที่ได้ออกมาแสดงความคิดเห็นวิพากษ์งานของฮาร์ทอย่างชัดเจนอีกหนึ่งท่านคือ ดวอร์กิน โดยดวอร์กินได้ออกมาแสดงความคิดเห็นวิพากษ์งานของฮาร์ทในเรื่อง “การใช้ดุลพินิจของศาลนอกเหนือกฎหมาย” ในความคิดเห็นของฮาร์ท ซึ่งในที่นี้ฮาร์ทมองว่าการใช้ดุลพินิจนั้นเป็นเรื่องที่ศาลสามารถกระทำได้ในกรณีที่ไม่มีกฎหมายบัญญัติไว้ ในขณะที่ดวอร์กินมองว่าการใช้ดุลพินิจดังกล่าวนี้เป็นการใช้ “หลักการ”¹⁴ (Principle) ทางกฎหมายอยู่นั่นเอง

ซึ่งหลักการที่ดวอร์กินมองนั้นตั้งอยู่บนพื้นฐานของมาตรฐานทางศีลธรรมของประชาชน ในการที่จะให้ศาลสามารถวินิจฉัยหรือตัดสินออกมาได้ยุติธรรมมากที่สุดแม้จะไม่มีกฎหมายบัญญัติไว้ หรืออาจกล่าวได้ว่าหลักการนั้นคือ กฎหมายธรรมชาตินั่นเอง จึงแสดงให้เห็นว่าดวอร์กินได้มองว่ากฎหมายนั้นต้องควบคู่ไปกับศีลธรรม ไม่สามารถใช้กฎหมายเพียงอย่างเดียวเพื่อประกอบการพิจารณาคดีที่มีความยุ่งยากซับซ้อนได้

¹¹ Ibid 39.

¹² Ibid 40.

¹³ Fuller, *supra* note 63 pp.483-84, 465-66; Fuller, *supra* note 44, p.659.

¹⁴ Scott J. Shapiro, 'The "Hart-Dworkin" Debate: A short guide for the perplexed,' (5 March 2007) 9.

4. บทวิเคราะห์เชิงนิติปรัชญาจากการกระทำของแฮ็กเกอร์หมวกเทา

จากที่ได้กล่าวไปในข้างต้นจะเห็นได้ว่า การกระทำของแฮ็กเกอร์หมวกเทานั้น บางส่วนก็ไม่ถูกตรวจสอบและดำเนินคดีจากรัฐ แต่บางส่วนก็ถูกตรวจสอบและดำเนินคดีจากรัฐทั้งที่เป็นการกระทำที่มีองค์ประกอบความผิดในลักษณะเดียวกัน ดังนั้นแล้วเมื่อนำมาพิจารณากับหลักนิติปรัชญาที่เกี่ยวข้องหลักเกณฑ์ที่จำต้องนำมาพิจารณาเป็นหลักคือ การกระทำของพวกเขาเหล่านั้นถือว่าขัดกับหลักกฎหมายของรัฐหรือไม่ ซึ่งจึงจำเป็นต้องแยกพิจารณาดังนี้

จากการวิเคราะห์ สามารถตีความได้ว่าเมื่อเป็นการที่กลุ่มแฮ็กเกอร์หมวกเทากระทำต่อเอกชน ก็มักจะ ไม่ถูกตรวจสอบและดำเนินคดีจากรัฐ แต่ผู้ที่ถูกให้เบาะแส หรือถูกเปิดโปงข้อมูลจะเป็นฝ่ายที่ได้รับความเสียหายแทน หรือบ้างถูกดำเนินคดีจากรัฐ ดังเช่นในกรณีของ Ashley Madison หรือกรณีของ Tyler Shultz และ Erika Cheung ที่ออกมาเปิดโปง เธรานอส จนทางบริษัทได้มีฐานความผิด 11 ข้อหาด้วยกัน

ซึ่งเมื่อกฎหมายนั้นได้ถูกกำหนดมาเพื่อสร้างหน้าที่ของบุคคลในสังคมว่าต้องทำอะไรและห้ามทำอะไร หากว่าการกระทำของพวกเขาเหล่านั้นมิได้เป็นการที่ขัดหรือแย้งกับกฎหมายของรัฐซึ่งจะทำให้ได้รับบทลงโทษ การกระทำประเภทนี้จึงย่อมไม่ขัดและสอดคล้องกับแนวคิดของฮาร์ท แต่เมื่อพิจารณาการกระทำของแฮ็กเกอร์หมวกเทาส่วนนี้ ไม่ว่าจะเป็น Hacktivist หรือ Whistleblower ต่างก็ล้วนมีความผิดฐานเจาะระบบข้อมูลของผู้อื่นโดยที่ไม่ได้รับอนุญาต หรือเปิดโปงข้อมูลของบุคคลอื่นจนได้รับความเสียหายทั้งสิ้น¹⁵ ซึ่งถือว่าเป็นบทบังคับของกฎหมายที่กำหนดเอาไว้ ดังนั้น เมื่อการกระทำเหล่านั้นล้วนแล้วแต่ขัดกับหลักกฎหมายของรัฐ กล่าวคือ Hacktivist และ Whistleblower ต่างก็ได้กระทำการที่ขัดต่อหลักการและแนวคิดของฮาร์ททั้งสิ้น แต่อย่างไรก็ดี รัฐก็ไม่ได้มีนโยบายที่จะตรวจสอบและดำเนินคดีแก่การกระทำดังกล่าวสักเท่าไรตามที่ได้กล่าวไปในข้างต้น ซึ่งแท้ที่จริงแล้วก็ควรที่จะได้รับการลงโทษจากรัฐ ดังนั้น จึงอาจตั้งคำถามได้ว่า การที่รัฐมีมาตรการบังคับแต่ไม่ปรับใช้กับความผิดที่เกิดขึ้นนั้นถือว่าชอบในแง่ของศีลธรรมหรือไม่ ทั้งที่การเจาะระบบข้อมูลของผู้อื่นรวมถึงเปิดโปงข้อมูลของผู้อื่นต่างเป็นสิ่งที่สังคมให้ความสำคัญ และมองว่าเป็นความผิดที่ผู้ถูกเจาะระบบนั้นไม่ควรได้รับความชอบธรรม ยกตัวอย่างเช่น กฎหมาย GDPR¹⁶ ที่ให้ความสำคัญให้ความสำคัญคุ้มครองสิทธิส่วนบุคคลของพลเมือง ไม่ให้กิจการออนไลน์ทั้งหลายเก็บรวบรวมและนำเอาข้อมูลส่วนตัวของแต่ละคนไปใช้ตามใจชอบ โดยกรณีที่กระทำการขัดต่อหลักกฎหมายดังกล่าว ยกตัวอย่างเช่น กรณีของ Google ที่ถูกสำนักงานด้านการคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศส (CNIL) ปรับเป็นเงินจำนวน 50 ล้านยูโร ในฐานะละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (GDPR) เนื่องจากไม่มีการแจ้งการใช้ข้อมูล

¹⁵ กฎหมายสหรัฐอเมริกา ได้บัญญัติกฎหมายเรื่องการสกัดกั้นการสื่อสารทางสาย ทางปาก หรือทางอิเล็กทรอนิกส์ ไว้ใน The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030,1 ไม่ว่าจะเป็น Trespassing in Government Cyberspace (18 U.S.C. 1030(a)(3)) ซึ่งเป็นเรื่องการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตไม่ว่าจะโดยเจตนา หรือเพื่อเข้าถึงเอกสารที่ทางราชการมีอำนาจครอบครองแต่เพียงผู้เดียว โดยผู้ใดที่พยายามเข้าถึงนั้นต้องโทษจำคุกไม่มากกว่า 1 ปี หรือ ปรับไม่เกิน 3,474,000 บาท หากเป็นองค์กรต้องโทษปรับไม่เกิน 6,948,000 บาท ผู้ใดเข้าถึงจะต้องโทษจำคุกไม่มากกว่า 10 ปี หรือปรับไม่เกิน 8,685,000 บาท หากเป็นองค์กรต้องโทษปรับไม่เกิน 17,370,000 บาท.

Obtaining Information by Unauthorized Computer Access (18 U.S.C. 1030(a)(2)) หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต.

¹⁶ ข้อบังคับทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ('GDPR') เป็นกฎหมายของยุโรปที่ควบคุมข้อมูลส่วนบุคคลในพื้นที่เศรษฐกิจยุโรป GDPR มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2018 GDPR เป็นการปฏิรูปที่สำคัญที่สุดของกฎหมายคุ้มครองข้อมูลของยุโรป.

ส่วนบุคคลกับผู้ใช้งานในรูปแบบที่เหมาะสมและด้วยภาษาที่เข้าใจง่าย อีกทั้งไม่ได้ขอความยินยอมการใช้ข้อมูลส่วนตัวจากผู้ใช้งานเพื่อใช้ทำแคมเปญโฆษณาแบบเจาะกลุ่มเป้าหมาย¹⁷

แม้กรณีในข้างต้นจะเป็นข้อบังคับและบทลงโทษสำหรับผู้ควบคุมข้อมูล แต่ก็แสดงให้เห็นได้ว่า สังคมนั้นต่างก็ให้ความสำคัญกับการคุ้มครองข้อมูล และความปลอดภัยของข้อมูล อันทำให้การถูกเจาะข้อมูลนั้นไม่เป็นที่ยอมรับและต้องมีมาตรการบังคับให้ได้รับการลงโทษ

เมื่อกฎหมายปฐมภูมิล้วนเป็นกฎหมายที่คนในรัฐนั้นจำต้องปฏิบัติตาม ส่วนกฎหมายพหุภูมิเป็นกฎหมายที่เพียงฝ่ายนิติบัญญัติเท่านั้นที่จำเป็นต้องยอมรับและบังคับใช้ตามแนวคิดของฮาร์ทเพื่อทำให้กฎหมายชั้นปฐมภูมิได้มีการถูกบังคับใช้ให้ออกมาเป็นรูปธรรม ดังนั้น เมื่อฝ่ายนิติบัญญัติได้นำกฎหมายมาบังคับใช้กับกรณีของแฮ็กเกอร์หมวกเทาบางส่วนที่กระทำต่อเอกชนเพื่อให้มีความสอดคล้องกับกฎหมายชั้นปฐมภูมิที่เป็นบรรทัดฐานของสังคม จึงถือว่าเป็นการขัดกับหลักการดังกล่าวนั่นเอง อันจะทำให้กฎหมายนั้นไม่มีความเป็นกฎหมายตามไปด้วย

กรณีของของแฮ็กเกอร์หมวกเทาที่ได้ทำการเปิดโปงการกระทำของรัฐ จากที่เคยได้กล่าวไปในเบื้องต้น จะเห็นได้ว่า องค์ประกอบความผิดนั้นล้วนแล้วแต่มีลักษณะที่เหมือนกัน กล่าวคือ เปิดโปงการกระทำของผู้จ้าง แต่รัฐไม่ได้มีความผิดหรือได้รับการลงโทษ กลับกันแล้วเป็นฝ่ายที่เปิดโปงข้อมูลของรัฐที่ได้มีฐานความผิด¹⁸

แน่นอนว่า เมื่อกระทำการอันเป็นการขัดต่อหลักกฎหมายของภาครัฐ ก็ย่อมต้องได้รับบทลงโทษ อันเป็นการที่สอดคล้องต่อหลักการและแนวคิดของฮาร์ทแล้วว่าด้วยเรื่องการกระทำที่ขัดหรือแย้งต่อรัฐย่อมต้องได้รับบทลงโทษ แต่อย่างไรก็ดี เมื่อองค์ประกอบความผิดนั้นมีลักษณะที่เหมือนกันกับกรณีที่ได้กระทำกับเอกชน แต่ก็อาจเกิดคำถามว่าทำไมฝ่ายแฮ็กเกอร์หมวกเทาที่กระทำต่อเอกชนจึงไม่ได้รับโทษดังเช่นฝ่ายที่กระทำต่อรัฐ ดังนั้น จึงสามารถตีความและตั้งคำถามได้ว่า กฎหมายดังกล่าวมีความชอบธรรมและเป็นการเลือกปฏิบัติหรือไม่

เมื่อพิจารณาตามแนวคิดของฮาร์ท การที่กฎหมายนั้นจะมีความชอบธรรมหรือไม่ ก็ขึ้นอยู่กับว่ากฎหมายดังกล่าวเป็นกฎหมายที่ถูกออกโดยกระบวนการตรานิติบัญญัติที่ถูกต้อง หากกฎหมายที่ออกมาบังคับใช้ลงโทษ เอ็ดเวิร์ด สโนว์เด็น นั้นถูกออกโดยกระบวนการที่ถูกต้องตามนิติบัญญัติ กฎหมายดังกล่าวก็ถูกต้องแล้ว โดยไม่สนว่าเนื้อหาสาระภายในจะเป็นเช่นไรหรือว่าขัดต่อหลักการทางศีลธรรมหรือไม่ การกระทำของรัฐต่อสโนว์เด็นจึงล้วนมีความชอบธรรมในตัวเอง แต่หากว่ากันในด้านของศีลธรรม การกระทำของเขาล้วนแล้วแต่มีเจตนาที่ต้องการเปิดโปงการกระทำที่ไม่ถูกต้องของรัฐเพื่อแจ้งต่อสาธารณะชนให้ทราบโดยทั่วกัน กล่าวคือเป็นการกระทำที่อาจมีเจตนาที่ดีต่อคนส่วนมาก แต่มิได้มีเจตนาที่ดีต่อผู้ถูกกระทำนั้นคือตัวของรัฐ ดังนั้น การลงโทษผู้มีเจตนาที่ดีต่อคนหมู่มากนั้น จึงถือว่าผิดในด้านของศีลธรรมหรือไม่

หากพิจารณาและตีความแล้ว คำว่าศีลธรรมนั้นอาจมิได้มีมาตรวัดที่มีความชัดเจนและแน่นอน ในส่วนของฟูเลอร์เขามองว่า การมีอยู่ของหลักนิติธรรมเป็นการแสดงให้เห็นถึงจุดประสงค์ในการตรากฎหมาย และแสดงให้เห็นถึงการจำกัดอำนาจของฝ่ายนิติบัญญัติ แต่ก็ได้มีการอธิบายไว้อย่างชัดเจนว่าศีลธรรมคืออะไร ในส่วนของดอร์กิน ก็มองว่าเป็นหลักการที่ศาลจะสามารถใช้ในการวินิจฉัยคดีออกมาให้ดีที่สุดแต่เพียงเท่านั้น

¹⁷ ‘ผลกระทบเมื่อข้อมูลโดนแฮ็ก แนะนำวิธีการรับมืออย่างมืออาชีพ’ (PDPA Core, 29 พฤศจิกายน 2564) <<https://pdpacore.com/th/blogs/the-consequences-of-data-breach-and-how-to-handle>>

¹⁸ การเปิดโปงของสโนว์เด็น ทำให้ได้รับความผิดด้วยกันทั้งหมด 3 ข้อหา ได้แก่ โจรกรรมข้อมูล เผยแพร่ข้อมูลด้านกลาโหมโดยไม่ได้รับอนุญาต และลักทรัพย์สินของรัฐบาล ซึ่งมีโทษจำคุกรวมกันสูงสุดถึง 30 ปี.

จากการพิจารณาแล้ว จึงเห็นว่า เมื่อศีลธรรมนั้นมีได้มีหลักเกณฑ์ที่ถูกต้องอย่างตายตัว กล่าวคือขึ้นอยู่กับ การตีความและให้เหตุผลของแต่ละคน ดังนั้น การที่จะได้กฎหมายที่มีความสมเหตุสมผลและเหมาะสมกับการกระทำของแอ็กเทอร์หมวดหมู่มากที่สุด จำต้องพิจารณาโดยปราศจากหลักการทางด้านศีลธรรม กล่าวคือเมื่อกระทำการที่เป็นการขัดต่อหลักกฎหมายของรัฐแล้วก็ย่อมต้องได้รับการลงโทษ แต่หากว่าจะกล่าวว่าการกระทำของแอ็กเทอร์หมวดหมู่นั้นถูกหรือผิดตามศีลธรรมนั้นก็ไม่สามารถที่จะตีความได้

5. บทสรุป

การกระทำของแอ็กเทอร์หมวดหมู่จะถือว่าเป็นความผิดและควรได้รับการลงโทษหรือไม่ จะต้องพิจารณาจากมุมมองของผู้ใดหรือศีลธรรมของใคร ก็ดังเช่นที่ได้กล่าวมาในบทความนี้เกี่ยวกับการแนวคิดของนักปรัชญาท่านต่าง ๆ ไม่ว่าจะเป็น ฮาร์ท พูลเลอร์ หรือดวอร์กิน ซึ่งทั้งหมดนี้เป็นตัวแทนนักกฎหมายจากสำนักกฎหมายธรรมชาติและบ้านเมืองทั้งสิ้น แต่สิ่งหนึ่งที่ทำให้แนวคิดของทั้ง 3 คนนั้นเหมือนหรือแตกต่างกัน ล้วนแล้วแต่พิจารณาจากมุมมอง (Perspective) ของผู้ที่ได้กล่าวอ้างนั่นเอง โดยคนหนึ่งอาจมองในมุมมองของรัฐ (State) ที่เน้นไปในด้านของการปกครองคนหมู่มากเพื่อที่จะให้เกิดความสงบในสังคม (Society) ก็ย่อมมองได้ว่า “กฎหมายย่อมต้องเป็นกฎหมายไม่มีข้อยกเว้นผู้ใดฝ่าฝืนผู้นั้นต้องรับโทษ” ซึ่งกลับกันแล้วหากมองในอีกแง่หนึ่ง ก็อาจมองได้ว่าเมื่อมีเจตนาที่ดีก็ควรที่จะได้รับการยกเว้นความผิดหรือไม่ ในที่นี้ผู้เขียนได้ให้มองว่าศีลธรรมไม่สามารถนำมาใช้ในการพิจารณาเพื่อทำให้การกระทำอันเป็นความผิดได้รับการยกเว้นได้ ดังนั้น จึงเป็นประเด็นที่ทางผู้เขียนให้ความเห็นว่า ไม่ว่าเจตนาของแอ็กเทอร์ประเภทหมวดหมู่จะเป็นเช่นไร แต่การกระทำนั้นเมื่อกฎหมายว่าไว้ว่าเป็นความผิด จึงย่อมต้องถือตามกฎหมายที่กำหนดไว้โดยไม่มีการยกเว้นใด ๆ ทั้งสิ้น ไม่ว่าจะเป็นการเจาะข้อมูลและสร้างประโยชน์ให้แก่ฝั่งของภาครัฐหรือเอกชนมากเท่าใดก็ตาม อันเป็นการสรุปที่สอดคล้องกับแนวคิดของสำนักกฎหมายบ้านเมือง ที่ให้ความสำคัญกับบทบัญญัติที่รัฐได้ตราไว้เป็นหลัก