# บทที่ 6

## บทสรุป และข้อเสนอแนะ

ในปัจจุบันระบบคอมพิวเตอร์และอินเทอร์เน็ตเข้ามามีบทบาทกับการดำรงชีวิตของมนุษย์ ทำให้การดำรงชีวิตในรูปแบบเดิมเปลี่ยนแปลงไป เกิดกิจกรรมใหม่ๆมากมายที่ต้องอาศัยอินเทอร์เน็ตเป็นสื่อกลาง ผู้คนนับพันล้านคนจากทั่วโลกมีความจำเป็นที่จะต้องพึ่งพาเทคโนโลยีประเภทนี้

เมื่อกิจกรรมต่างๆเกิดขึ้นบนโลกของอินเทอร์เน็ต อาชญากรรมคอมพิวเตอร์ (Computer crime) หรือการกระทำความผิดบนอินเทอร์เน็ต (Cyber crime) ก็ตามมาด้วย ส่งผลให้เกิดความเสียหายต่อเศรษฐกิจ สังคมและความมั่นคงของชาติ จึงปัญหาสำคัญที่ประเทศต่างๆทั่วโลกต่างหาหนทางแก้ไข แต่การใช้กฎหมายที่มีความล้าหลังและมาตรการต่างๆที่มีอยู่เดิมเข้าไปจัดการผู้กระทำความผิดเหล่านั้นยังมีข้อจำกัด อย่างไรก็ดี บัญญัติกฎหมายเกี่ยวกับความผิดประเภทมีความละเอียดอ่อนและซับซ้อน เพราะกฎหมายที่บัญญัติขึ้นใหม่จะต้องมีความยืดหยุ่นในการปรับใช้กับการกระทำผิดที่จะเกิดขึ้นโดยอาศัยนวัตกรรรมและเทคโนโลยีใหม่ๆที่จะเกิดขึ้นในอนาคต และจะต้องสอดคล้องกับกฎหมายของประเทศอื่นๆด้วย เพราะการกระทำความผิดอาจเกิดขึ้นที่ใดก็ได้ในโลก อีกทั้งกฎหมายที่บัญญัติขึ้นใหม่และมาตรการต่างๆที่นำมาใช้จะต้องมีประสิทธิภาพและไม่กระทบสิทธิเสรีภาพของประชาชนเกินสมควร

แนวทางการควบคุมอาชญากรรมคอมพิวเตอร์และการกระทำความผิดบนอินเทอร์เน็ตของแต่ละประเทศทั่วโลกมีแนวทางที่คล้ายคลึงกันคือจะบัญญัติกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติควบคู่กันไป โดยกฎหมายสารบัญญัติจะต้องกำหนดฐานความผิดเกี่ยวกับอาชญากรรมเหล่านี้โดยเฉพาะ เช่น การกำหนดฐานความผิดการเข้าถึงคอมพิวเตอร์โดยมิชอบ (Illegal access), การดักข้อมูลคอมพิวเตอร์ (Illegal interception), การรบกวนข้อมูลคอมพิวเตอร์ (Data interference), การรบกวนระบบคอมพิวเตอร์(System interference), การใช้อุปกรณ์โดยมิชอบ(Misuse of device), การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related forgery), การฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์ (Computer-related fraud), การกระทำความผิดเกี่ยวกับภาพลามกอนาจารเด็ก (Offences related to child pornography),

ความผิดอันเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิเกี่ยวเนื่อง (Offences related to infringements of copyright and related rights), ความผิดฐานพยายามและช่วยเหลือหรือสนับสนุน( Attempt and aiding or abetting) และอาจมีการปรับเปลี่ยนหรือกำหนดฐานความผิดอื่นๆที่สอดคล้องกับสภาพสังคมของแต่ละประเทศ ในส่วนของกฎหมายวิธีสบัญญัติได้ถูกกำหนดให้เหมาะสมกับลักษณะของการกระทำความผิด เช่น กำหนดอำนาจและวิธีปฏิบัติของเจ้าหน้าที่ที่เกี่ยวข้อง การรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ให้มีความเหมาะสม

1. <u>ประเทศสหรัฐอเมริกา</u>

ในประเทศสหรัฐอเมริกา การดำเนินคดีกับผู้กระทำความผิดสามารถปรับเข้ากับฐานความผิดที่กำหนดไว้ในกฎหมายต่างๆ เช่น Computer fraud and abuse (18 U.S.C. § 1030), Wiretap Act (18 U.S.C. § 2510 ), CAN-SPAM Act(15 U.S.C. § 7704 ), Identity theft and assumption deterrence act of 1998. (18 U.S.C. § 1028), Wire fraud (18 U.S.C. § 1343), Access device fruad (18 U.S.C. § 1029) เป็นต้น ส่วนในกฎหมายที่เกี่ยวข้องกับการดำเนินการในชั้นสืบสวนสอบสวนจะต้องอยู่ภายใต้รัฐธรรมนูญแก้ไขครั้งที่ 4 (Fourth Amendment) และบทบัญญัติในหมวด 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, และ 18 U.S.C. §§ 3121-27 ซึ่งพอจะกล่าวโดยสรุปได้ดังนี้

1.) <u>การค้นและยึดคอมพิวเตอร์โดยมีหมาย</u>

มีการกำหนดให้จัดตั้งคณะผู้ทำการค้นซึ่งประกอบด้วยเจ้าหน้าที่ในคดี พนักงานอัยการและผู้ชำนาญทางเทคนิค โดยเจ้าหน้าที่ในคดีจะทำการศึกษาว่าในคดีนั้นจะต้องแสวงหาพยานหลักฐานใด และ คำรับรอง(Affidavit)มีเหตุสมควร(Probable cause) ที่จะออกหมายค้นหรือไม่ และดำเนินการขอหมายต่อศาล ส่วนผู้เชี่ยวชาญทางเทคนิคจะอธิบายถึงข้อจำกัดของการค้นให้เจ้าหน้าที่ในคดีและพนักงานอัยการเข้าใจ และวางแผนการค้นเพื่อให้ได้มาซึ่งพยานหลักฐาน และพนักงานอัยการจะทำการพิจารณาว่าหมายค้นและกระบวนการในการค้นชอบด้วยรัฐธรรมนูญและชอบด้วยกฎหมายวิธีพิจารณาหรือไม่ โดยแต่ละฝ่ายจะประสานงานให้ความร่วมมือซึ่งกันและกัน

โดยพื้นฐานวิธีการในการค้นคอมพิวเตอร์มีหลากหลายวิธี แต่อาจแบ่งได้ 4 ประเภท ดังนี้

1) ค้นคอมพิวเตอร์และพิมพ์ข้อมูลจากคอมพิวเตอร์ลงบนกระดาษในเวลาเดียวกัน 2) ค้นคอมพิวเตอร์และทำสำเนาอิเล็กทรอนิกส์ในเวลาเดียวกัน 3) สร้างสำเนาอิเล็กทรอนิกส์ ข้อมูลทั้งหมดที่บรรจุในสถานที่นั้นและนำมาสร้างใหม่นอกสถานที่นั้นแล้วนำสำเนาอิเล็กทรอนิกส์ที่ได้มาพิจารณา 4) ยึดอุปกรณ์และย้ายอุปกรณ์เหล่านั้นออกจากสถานที่นั้น จากนั้นนำมาพิจารณาเนื้อหานอกสถานที่นั้น ซึ่งการดำเนินการในการขอหมายเจ้าหน้าที่จะพิจารณาจากหลักการดำเนินคดีอาญา 2 ประการคือ

ก.) <u>กรณีที่อุปกรณ์คอมพิวเตอร์นั้นเป็นสิ่งผิดกฎหมาย, พยานหลักฐาน, ใช้เป็นเครื่องมือในการทำความผิด หรือได้มาจากการกระทำความผิด</u> เจ้าหน้าที่สามารถยึดคอมพิวเตอร์ได้ เมื่อได้ทำการค้นตามหมายค้น หากพบอุปกรณ์คอมพิวเตอร์ที่เป็นสิ่งผิดกฎหมาย, หลักฐาน,ใช้เป็นเครื่องมือในการทำความผิดหรือได้มาจากการกระทำความผิด

ข.) <u>กรณีที่อุปกรณ์คอมพิวเตอร์ นั้นเป็นเพียงสิ่งบรรจุพยานหลักฐานในการกระทำผิดอาญา</u> ในกรณีนี้ต่างจากกรณีข้างต้นเพราะเจ้าหน้าที่ต้องระบุรายละเอียดในคำรับรองให้ชัดเจน และไม่สามารถยึดได้ทันทีเช่นกรณีข้างต้น เพราะไม่ถือว่าอุปกรณ์คอมพิวเตอร์เหล่านี้เป็นพยานหลักฐานในตัวเอง แต่มิได้หมายความว่าห้ามยึดเสียทีเดียว โดยเจ้าหน้าที่รัฐอาจยึดได้หากไม่มีทางเลือกอื่นซึ่งอาจกระทำได้เพื่อให้ได้มาซึ่งพยานหลักฐานนั้น

การการยึดและค้นคอมพิวเตอร์ที่เป็นเครือข่ายคอมพิวเตอร์ มิใช่คอมพิวเตอร์ส่วนบุคคล เจ้าหน้าที่ยังต้องใช้ความระมัดระวังเป็นพิเศษมิให้ละเมิดต่อกฎหมายอื่นที่เกี่ยวข้อง ได้แก่

1.) <u>Privacy Protection Act (PPA)</u> ที่ต้องการคุ้มครองบุคคลภายนอกที่เพียงแต่นำเสนอข้อมูลเกี่ยวกับความผิด ไม่ให้ถูกค้นหรือยึดทั้งที่ตนมิได้มีส่วนร่วมในการกระทำความผิด

2.) <u>Electronic communications Privacy Act (ECPA)</u> การค้นและยึดข้อมูลในเครือข่ายคอมพิวเตอร์ เจ้าหน้าที่ของรัฐควรที่จะต้องพยายามทุกวิถีทางเพื่อคุ้มครองสิทธิของบุคคลภายนอก โดยเจ้าหน้าที่จะหลีกเลี่ยง การค้น หรือ ยึด คอมพิวเตอร์ของผู้ให้บริการทั้งหมด

นอกจากนี้หากการค้นเกี่ยวข้องกับหลายท้องที่เจ้าหน้าที่ยังต้องพิจารณาว่าสมควรมีการออกหมายฉบับ (Multiple warrants)หรือไม่ หรือมีเหตุสมควรที่จะต้องขอออกหมายที่ไม่ต้องแจ้งเตือน (No-Knock Warrants) หรือ หมายซุ่มสังเกต (Sneak-and-peak Warrants)หรือไม่

2.) <u>การค้นและยึดคอมพิวเตอร์โดยไม่ต้องมีหมาย</u>

โดยหลักแล้วการค้นจะต้องมีหมาย ตามความคุ้มครองของ Fourth Amendment แต่แนวบรรทัดฐานของศาลถือว่า การค้นโดยไม่มีหมายจะไม่ถือเป็นการละเมิด Fourth Amendment หากเป็นไปตามเงื่อนไขประการใด ประการหนึ่งในสอง ประการดังต่อไปนี้

ก. หากการกระทำของหน่วยงานของมิได้ล่วงละเมิดต่อ "ความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวของบุคคล (Person's reasonable expectation of privacy)" ถือเป็นการค้นโดยชอบ ดังนั้น การค้นนี้ไม่จำเป็นต้องมีหมาย เช่น การค้นในสาธารณสถาน, การสูญเสียการครอบครองทรัพย์สินนั้นให้บุคคลภายนอก,การค้นโดยเอกชน (Private search), การใช้เทคโนโลยีเพื่อให้ได้มาซึ่งข้อมูล(Use of technology to obtain information)

ข. การค้นที่ไม่มีหมายที่ล่วงละเมิดต่อ ความต้องการที่เหมาะสมที่ในการมีความเป็นส่วนตัวของบุคคล จะถือว่า เหมาะสม (Reasonable) และชอบด้วยรัฐธรรมนูญ หากอยู่ในกรณีที่เป็นข้อยกเว้นของการค้นที่ต้องมีหมาย ได้แก่ การค้นที่เป็นไปตามหลักความยินยอม (Consent), สถานการณ์ฉุกเฉิน (Exigent Circumstances), สิ่งที่พบเห็นได้โดยง่าย (Pain View), การค้นอันเนื่องมาจากการจับกุมโดยชอบด้วยกฎหมาย(Search Incident to Lawful Arrest), การค้นเพื่อแสดงรายละเอียด(Inventory searches), การค้นบริเวณพรมแดน (Border Searches), ความร่วมมือระหว่างประเทศ (International Issue)

3.) <u>ควบคุมทางอิเล็กทรอนิกส์ในเครือข่ายสื่อสาร</u> เป็นการเฝ้าระวังผู้กระทำความผิด หรือตรวจสอบกิจกรรมต่างๆบนอินเทอร์เน็ตซึ่งการใช้มาตรการเหล่านี้ มีกฎหมายที่เกี่ยวข้องคือ

(1 ) Pen/Trap statute (18 U.S.C. §§ 3121-3127) มุ่งรวบรวมข้อมูลที่ระบุที่อยู่หรือตัวผู้ใช้ ในลักษณะที่มิใช่เนื้อหา (Non-content) หากเทียบกับการสื่อสารทางโทรศัพท์ก็อาจเทียบได้กับหมายเลขโทรศัพท์(Phone number)

(2) Wiretap statute(18 U.S.C. §§ 2510-2522 การรวบรวมข้อมูลในลักษณะเนื้อหา(Content) หรืออาจเทียบได้กับเนื้อหาบทสนทนา (Conversation) ที่พูดคุยผ่านทางโทรศัพท์

มาตรการทั้งสองมีหลักเกณฑ์ควบคุมที่แตกต่างกันเพื่อป้องกันมิให้เจ้าหน้าที่ใช้อำนาจโดยมิชอบ หากเจ้าหน้าที่ฝ่าฝืนอาจทำให้ต้องรับผิดในทางแพ่ง ทางอาญา หรือมีผลต่อการรับฟังเป็นพยานหลักฐานนั้นได้

2. <u>ประเทศสิงคโปร์</u>

การดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์สำหรับประเทศสิงคโปร์ โดยฐานความผิดต่างๆถูกบัญญัติไว้ใน Computer Misuse Act ในส่วนของการดำเนินคดีอาญาได้บัญญัติไว้ทั้งในประมวลกฎหมายวิธีพิจารณาความอาญา และในกฎหมาย Computer Misuse Act ดังนี้

1.) <u>อำนาจเข้าถึงคอมพิวเตอร์ (Power to access computer)</u> ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 125A ให้อำนาจเจ้าพนักงานเข้าถึงคอมพิวเตอร์ หากคอมพิวเตอร์เหล่านั้นถูกใช้หรือสงสัยว่าถูกใช้เกี่ยวกับ Seizable offence (ความผิดที่กฎหมายประเทศสิงคโปร์กำหนดให้จับได้โดยไม่ต้องมีหมาย)

2.) <u>อำนาจถอดรหัสของข้อมูล (Power to access decryption information)</u> หลักการนี้ถูกบัญญัติไว้ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 125B โดยมีเนื้อหาสัมพันธ์กับมาตรา125A ที่ได้กล่าวมาแล้วข้างต้นเพื่อให้อำนาจเจ้าหน้าที่ถอดรหัสของข้อมูลได้ด้วย

3.) <u>บทคุ้มครองการสืบสวนโดยตำรวจและเจ้าหน้าที่ตามกฎหมาย (Saving for investigations by police and law enforcement officers)</u> หลักการนี้บัญญัติไว้ในกฎหมาย Computer Misuse Act โดยกำหนดบทคุ้มครองตำรวจและเจ้าหน้าที่ที่กระทำการโดยชอบด้วยกฎหมาย

4.) <u>การป้องกันหรือการตอบโต้ ภัยคุกคามต่อความมั่นคงของชาติ และกรณีอื่น</u> (Preventing or countering threats to national security, etc ) หลักการนี้บัญญัติไว้ในกฎหมาย Computer Misuse Act มาตรา 15 A โดยให้ความสำคัญกับการป้องกันสาธารณูปโภคพื้นฐานที่จำเป็น โดยให้อำนาจเจ้าหน้าที่สามารถใช้จัดการกับสถานการณ์ฉุกเฉินที่ถูกโจมตีทางไซเบอร์ได้อย่างรวดเร็ว แต่มาตรการนี้จะต้องใช้อย่างจำกัดสำหรับวัตถุประสงค์ในการป้องกันหรือตอบโต้การกระทำที่เป็นภัยต่อความมั่นคงของชาติหรือสาธารณูปโภคพื้นฐานที่จำเป็นเท่านั้น ซึ่งกำหนดหลักเกณฑ์ไว้เป็นพิเศษเพื่อมิให้นำไปใช้กับการดำเนินคดีกับผู้กระทำผิดหรือใช้กับความผิดอาญาทั่วไป

5.) <u>การจับกุมโดยตำรวจโดยไม่ต้องมีหมาย(Arrest by police without warrant)</u> เพื่อประโยชน์ในการดำเนินคดีจึงได้มีการกำหนดให้ฐานความผิดตามกฎหมาย Computer Misuse Act เป็นความผิดที่สามารถจับกุมได้โดยไม่ต้องมีหมาย ทั้งนี้ ตามมาตรา 16

3. <u>ประเทศอินเดีย</u>

ในประเทศอินเดีย การกำหนดฐานความผิดและการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้บัญญัติไว้ใน The Information technology Act , 2000 แต่กฎหมายฉบับนี้มีวัตถุประสงค์เพื่อควบคุมการติดต่อสื่อสารและการรวบรวมข้อมูลในทางการค้าอิเล็กทรอนิกส์ (Electronic commerce) จึงมิได้กำหนดหลักการในการดำเนินคดีอาญาไว้เท่าที่ควรเพียงกำหนดให้เจ้าหน้าที่ที่ทำการสืบสวนต้องเป็นพนักงานตำรวจที่มียศไม่ต่ำกว่าชั้นรองผู้กำกับการ (มาตรา78) และกำหนดให้อำนาจพนักงานตำรวจหรือพนักงานอื่นในการเข้าไป,ค้น หรือใช้วิธีการอื่น(Power of police officer and other officers to enter, search, etc. ) โดยเจ้าพนักงานตำรวจที่มียศไม่ต่ำกว่าชั้นรองผู้กำกับการ หรือ พนักงานอื่นที่กฎหมายกำหนดให้มีอำนาจเข้าไปในสถานที่สาธารณะให้ค้นและจับได้โดยไม่ต้องมีหมาย (มาตรา80)

4. <u>สหภาพยุโรป</u>

อนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime of 2001) แบ่งออกได้เป็น 2 ส่วนหลักๆ คือ ส่วนที่เกี่ยวกับการกำหนดฐานความผิด และส่วนที่เกี่ยวกับกฎหมายวิธีสบัญญัติ โดยกำหนดให้หลักการตามอนุสัญญานี้ครอบคลุม1.) ฐานความผิดต่างๆที่กำหนดไว้ในอนุสัญญานี้ 2.)ความผิดอาญาอื่นๆที่ถูกกระทำโดยผ่านทางระบบคอมพิวเตอร์3.) การเก็บรวบรวมพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์สำหรับความผิดอาญา และได้กำหนดมาตรการสำคัญต่างๆไว้ ดังนี้

1.) <u>การเก็บรักษาข้อมูลคอมพิวเตอร์โดยไม่ชักช้า (Expedited preservation of stored data)</u> เพื่อรักษาความถูกต้องของข้อมูลไว้อย่างสมบูรณ์เท่าที่จะทำได้ จึงกำหนดให้เจ้าหน้าที่รัฐสามารถเรียกข้อมูลคอมพิวเตอร์จากผู้ให้บริการได้อย่างรวดเร็ว (มาตรา16)

2.) <u>การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์โดยไม่ชักช้าและการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์บางส่วน (Expedited preservation and partial disclosure of traffic data)</u> การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์(Traffic data) จะต้องทำโดยรวดเร็วเช่นกัน เพื่อให้เจ้าหน้าที่สามารถทราบถึงเส้นทางการสื่อสาร และข้อมูลเบื้องต้นที่ทำให้สามารถระบุตัวผู้ใช้บริการได้ (มาตรา17)

3. <u>การสั่งให้จัดทำ(Production order)</u> ในการดำเนินคดีให้เกิดประสิทธิภาพจะต้องบันทึกและเก็บรักษาข้อมูลบางประเภทไว้ จึงกำหนดให้ผู้ให้บริการจัดเก็บข้อมูลที่ทำให้สามารถระบุตัวผู้ครอบครองหรือใช้คอมพิวเตอร์ นอกเหนือจากข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์ และส่งมอบข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ (มาตรา18)

4.) <u>การค้นและยึดซึ่งข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ (Search and seizure of stored computer data)</u> การค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ควรกำหนดให้มีความแตกต่างจากการวิธีการค้นและยึดตามปกติ เช่น หากข้อมูลที่ต้องการถูกเก็บไว้ในระบบคอมพิวเตอร์อื่น การค้นอาจจะถูกขยายผลไปยังระบบคอมพิวเตอร์อื่นได้ด้วย และต้องให้อำนาจเจ้าหน้าที่ในการจัดทำและรักษาสำเนาของข้อมูลคอมพิวเตอร์ และรักษาความสมบูรณ์ของข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ (มาตรา 19)

5.) <u>การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบReal-time (Real time collection of traffic data)</u> การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบReal-time เป็นการรวบรวมข้อมูลที่มิได้เกี่ยวข้องกับเนื้อหา(Non-Content) แต่เป็นการรวบรวมข้อมูลที่แสดงถึงต้นทางและปลายทางของการสื่อสาร (มาตรา 20)

6.) <u>การดักการสื่อสารของเนื้อหาข้อมูล(Interception of content data)</u> หลักการนี้แตกต่างจากมาตรการข้างต้น เพราะการดำเนินการโดยวิธีการนี้เป็นการดักเนื้อหาของข้อมูล(Content) มิใช่เพียงข้อมูลที่แสดงต้นทางและปลายทางการสื่อสารเท่านั้น

7.) <u>การส่งเสริมความร่วมมือระหว่างประเทศ</u>อนุสัญญาฉบับนี้กำหนดให้ประเทศสมาชิกจัดต้องศูนย์ความร่วมมือและประสานงานเพื่อให้ความช่วยเหลือกันในการสืบสวนและสอบสวนคดีที่เกี่ยวกับการกระทำความผิดบนเครือข่ายอินเทอร์เน็ต

สำหรับประเทศไทยเมื่อได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้ว ได้เพิ่มเติมหลักการพิเศษที่แตกต่างจากประมวลกฎหมายวิธีพิจารณาความอาญา คือ

<u>ก.) กำหนดให้มีหนักงานเจ้าหน้าที่</u> มีอำนาจหลักตามมาตรา18 แบ่งเป็นกรณีที่ไม่ต้องอนุญาตจากศาลก่อน ได้แก่ มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ, เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ,สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่ (มาตรา 18 (1) –(3)) และกรณีที่ต้องขออนุญาตจากศาลก่อน ได้แก่ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์, สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่, ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด, ถอดรหัสลับของข้อมูล คอมพิวเตอร์ของบุคคลใด, ยึดหรืออายัดระบบคอมพิวเตอร์ (มาตรา 18 (4) –(8))

ตามพระราชบัญญัตินี้พนักงานเจ้าหน้าที่ยังมีบทบาทในการใช้อำนาจอื่นตามพระราชบัญญัตินี้ ได้แก่ การร้องขอต่อศาลให้ระงับการเผยแพร่ซึ่งข้อมูลคอมพิวเตอร์(มาตรา20), การร้องขอต่อศาลให้ห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์(มาตรา21), อำนาจในการสั่งให้ผู้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีเฉพาะราย(มาตรา26)และประสานงานในเรื่องการจับ การควบคุม ค้น การสืบสวนและสอบสวนระหว่างพนักงานเจ้าหน้าที่กับพนักงานสอบสวนผู้รับผิดชอบ (มาตรา29) และพระราชบัญญัตินี้ยังวางเงื่อนไขการใช้อำนาจของพนักงานเจ้าหน้าที่ไว้ ได้แก่ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ให้แก่บุคคลใดหรือต้องรับผิดแม้เป็นการกระทำให้พยานรั่วไหลโดยประมาทและเอาผิดกับผู้ล่วงรู้ข้อมูลเหล่านั้นด้วย (มาตรา 22-24)

ข.) กำหนดให้มีการใช้มาตรการพิเศษ เพื่อประโยชน์ในการสืบสวนสอบสวนได้กำหนดให้เพิ่มมาตรการเหล่านี้นอกเหนือจากที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา คือ

1.) การปิดกั้น (Block) เว็บไซต์ (มาตรา 20)

2.) การห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์(มาตรา 21)

3.) การให้ผู้ให้บริการมีหน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา26) นอกจากนี้ยังกำหนดให้รับฟังพยานหลักฐานอิเล็กทรอนิกส์ได้ (มาตรา25)

## ข้อเสนอแนะ

จากที่ได้ศึกษาและวิเคราะห์พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ผู้เขียนมีข้อเสนอแนะดังต่อไปนี้

### ก. แก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550และกฎหมายอื่น รวมถึงประกาศและระเบียบที่เกี่ยวข้อง

1. ควรกำหนดให้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้สามารถใช้ครอบคลุมถึงการกระทำความผิดอาญาอื่นที่กระทำผิดโดยใช้ระบบ

คอมพิวเตอร์หรือกระทำผิดบนอินเทอร์เน็ตหรือใช้ในการรวบรวมพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์ด้วย

2. ควรเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพื่อให้สามารถลงโทษกับผู้กระทำความผิดร้ายแรง แม้อยู่ในขั้นตอนตระเตรียมการกระทำความผิด

3. ควรเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่ให้อำนาจพนักงานเจ้าหน้าที่สามารถขออนุญาตศาลได้อย่างรวดเร็วยิ่งขึ้น เช่น ให้พนักงานเจ้าหน้าที่ขออนุญาตศาลผ่านทางโทรศัพท์ โทรสาร ฯลฯ ได้ในกรณีเร่งด่วน

4. ควรเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่วางหลักเกณฑ์กำหนดขอบเขตการใช้ดุลยพินิจของพนักงานเจ้าหน้าที่ เช่น กำหนดให้พนักงานเจ้าหน้าที่หลีกเลี่ยงการยึดหรืออายัดระบบคอมพิวเตอร์ทั้งระบบในกรณีที่ระบบคอมพิวเตอร์นั้นเป็นเครือข่ายคอมพิวเตอร์

5. ควรแก้ไขมาตรการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา21 ให้มีความรวดเร็วและมีประสิทธิภาพยิ่งขึ้น

6. ควรเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ที่ให้พนักงานเจ้าหน้าที่สามารถประสานงานร่วมกับเจ้าหน้าที่ของต่างประเทศได้สะดวก เช่น ให้พนักงานเจ้าหน้าที่สามารถส่งมอบข้อมูลให้เจ้าหน้าที่ของต่างประเทศช่วยถอดรหัสได้ โดยไม่ถือเป็นความผิดและไม่ต้องขออนุญาตจากศาล

7. ควรเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยเพิ่มข้อสันนิษฐานตามกฎหมายในการระบุตัวผู้กระทำความผิด

8. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารควรออกระเบียบเกี่ยวกับการยึดและอายัด โดยกำหนดหลักเกณฑ์ที่ชัดเจนและรัดกุม

ข. <u>ศึกษาเพิ่มเติมในประเด็นต่าง ๆ</u> ดังต่อไปนี้

1. ศึกษาแนวทางการบัญญัติกฎหมายเฉพาะเกี่ยวกับหลักเกณฑ์และวิธีการในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสม

2. ศึกษาแนวทางการแก้ไขเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 หรือประมวลกฎหมายวิธีพิจารณาความอาญาหรือบัญญัติกฎหมายใหม่ที่ให้อำนาจศาลสามารถมีคำสั่งคุ้มครองชั่วคราวระหว่างดำเนินคดีอาญาบางฐานได้ เช่น คดีหมิ่นประมาทที่กระทำบนอินเทอร์เน็ต

3. ศึกษาแนวทางในการเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อให้อำนาจพนักงานเจ้าหน้าที่ทำการค้นได้อย่างต่อเนื่องโดยไม่ต้องขอออกหมายฉบับใหม่ ในกรณีที่การรวบรวมพยานหลักฐานเกี่ยวพันหลายสถานที่

4. ศึกษาแนวทางในการเพิ่มเติมบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และประมวลกฎหมายวิธีพิจารณาความอาญาในการให้อำนาจพนักงานเจ้าหน้าที่สามารถจับ ค้น ยึด อายัด หรือทำสำเนาได้โดยไม่ต้องมีหมาย ในบางกรณี เช่น กรณีฉุกเฉินอย่างยิ่ง

5. ศึกษาแนวทางการนำมาตรการ Real time collection of traffic data และมาตรการ Intercept of content data มาใช้ เพื่อเฝ้าระวังหรือสอดแนมการกระทำความผิดบนอินเทอร์เน็ต

6. ศึกษาแนวทางการนำมาตรการป้องกันหรือตอบโต้ภัยคุกคามต่อความมั่นคงของชาติมาใช้ เพื่อให้อำนาจพนักงานเจ้าหน้าที่อย่างเพียงพอที่จะสามารถระงับปัญหาที่เป็นภัยร้ายแรงของชาติได้อย่างรวดเร็วก่อนความเสียหายจะเกิดขึ้น

7. ศึกษาแนวทางการออกระเบียบเกี่ยวกับการค้นที่กำหนดให้พนักงานเจ้าหน้าที่ต้องดำเนินการเป็นคณะ ซึ่งในคณะจะต้องประกอบด้วยผู้เชียวชาญด้านคอมพิวเตอร์และผู้เชี่ยวชาญด้านกฎหมาย

ค. <u>ข้อเสนออื่น ๆ</u>

1. ควรยกเลิกประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ที่ 5/2549

2. ควรแต่งตั้งพนักงานเจ้าหน้าที่ที่มีความเชี่ยวชาญด้านคอมพิวเตอร์อย่างแท้จริง เช่น ผ่านการอบรมหลักสูตรตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนดไว้

3. สร้างความตื่นตัวให้ประชาชนตระหนักถึงภัยของอาชญากรรมคอมพิวเตอร์เพื่อส่งเสริมความร่วมมือจากประชาชนในการแจ้งเบาะแสการกระทำความผิด

4. จัดตั้งศูนย์ 24/7 network เพื่อส่งเสริมความร่วมมือระหว่างประเทศ

5. หน่วยงานที่เกี่ยวข้องควรจัดทำคู่มือการดำเนินคดีให้ชัดเจนและเผยแพร่ต่อสาธารณชน เช่น เผยแพร่ผ่านเว็บไซต์