บทที่ 2

การกระทำความผิดบนอินเทอร์เน็ต

2.1 เครือข่ายอินเทอร์เน็ต

2.1.1 ความหมายและการทำงานของเครือข่ายอินเทอร์เน็ต

ความหมายของเครือข่ายอินเทอร์เน็ต

โดยทั่วไปแล้วความหมายของอินเทอร์เน็ต อาจหมายถึงระบบเครือข่ายสาธารณะสากลของระบบเครือข่ายต่างๆ (A public international network of network)[1] โดยอินเทอร์เน็ตเป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ เครื่องคอมพิวเตอร์ทุกเครื่องทั่วโลก สามารถติดต่อสื่อสารถึงกันได้โดยใช้มาตรฐานในการรับส่งข้อมูลที่เป็นหนึ่งเดียว หรือที่เรียกว่าโปรโตคอล (Protocol) ซึ่งโปรโตคอลที่ใช้บนระบบเครือข่ายอินเทอร์เน็ต มีชื่อว่า ทีซีพี/ไอพี (TCP/IP : Transmission Control Protocol/Internet Protocol)[2] มีลักษณะเสมือนใยแมงมุมครอบคลุมทั่วโลก ในแต่ละจุดที่เชื่อมต่ออินเทอร์เน็ตนั้นสามารถสื่อสารกันได้หลายเส้นทางโดยไม่กำหนดตายตัวโดยไม่จำเป็นต้องไปตามเส้นทางตรง อาจจะผ่านจุดอื่นหรือเลือกไปเส้นทางอื่นได้หลากหลายเส้นทาง

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (Nectec) ได้ให้ความหมายของคำว่าอินเทอร์เน็ตไว้ดังนี้ *"อินเทอร์เน็ต คือ เครือข่ายของเครือข่ายคอมพิวเตอร์ระบบต่าง ๆ ที่เชื่อมโยงกัน มาจากคำว่า Inter Connection Network"*

---

[1] ไพจิตร สวัสดิสาร, การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์, (กรุงเทพมหานคร: โรงพิมพ์ชวนพิมพ์, 2547), หน้า 21.

[2] http://www.nectec.or.th/courseware/internet/internet-tech/0001.html.

คณะกรรมการกิจการโทรคมนาคมแห่งชาติ ให้คำจำกัดความของคำว่าอินเทอร์เน็ตไว้ดังนี้ *"อินเทอร์เน็ต หมายความว่า เครือข่ายคอมพิวเตอร์ และ/หรืออุปกรณ์สื่อสารอิเล็กทรอนิกส์ใด ๆที่ เชื่อมโยงกันเป็นเครือข่ายทั่วโลก และมีการสื่อสารข้อมูลโดยใช้มาตรฐานอินเทอร์เน็ต โปรโตคอล(Internet Protocol หรือ Transmission Control Protocol/Internet Protocol : TCP/IP) ร่วมกัน"*[3]

นอกจากคำว่าอินเทอร์เน็ต แล้วยังมีคำอื่นที่นิยมใช้เรียกเครือข่ายอินเทอร์เน็ตอีก เช่นคำว่า "Cyberspace" หรือการติดต่อสื่อสารแบบไร้มิติ ซึ่งบัญญัติโดยนักเขียนชื่อว่า William Gibson เพื่อใช้ในนวนิยายวิทยาศาสตร์ของตน ซึ่งในปัจจุบันคำว่า Cyberspace หมายถึงเครือข่ายคอมพิวเตอร์หลายเครือข่ายที่แยกกัน แต่สามารถติดต่อสื่อสารกันได้ แม้จะใช้กฎเกณฑ์หรือมาตรฐาน ที่แตกต่างกัน ดังนั้น ตามความหมายของ Cyberspace ในกรณีนี้ Internetจึงเป็นเพียงเครือข่ายหนึ่งของ Cyberspace เท่านั้น[4]

ประวัติของอินเทอร์เน็ต

การค้นคว้าวิจัยเกี่ยวกับอินเทอร์เน็ต (Internet) เริ่มขึ้นในปี พ.ศ.2512 โดยเป็นโครงการของหน่วยงานชื่อ APRANET (Advanced Research Project Agency) สังกัดกระทรวงกลาโหมของสหรัฐอเมริกา (U.S.Department of Defense – DoD) โดยมีวัตถุประสงค์ใช้เป็นฐานข้อมูลทางการทหาร เพื่อใช้เป็นเครือข่ายการสื่อสารที่ยากต่อการทำลายแม้จะถูกโจมตีด้วยระเบิดปรมาณู เนื่องจากเครือข่ายนี้ไม่มีจุดศูนย์กลางแต่ให้คอมพิวเตอร์แต่ละเครื่องมีลักษณะเป็น(Node) คือสามารถรับ เก็บ และส่งข้อมูลเป็นช่วง[5] หากมีบางส่วนของเครือข่ายถูกทำลายหรือชำรุด ระบบการสื่อสารนี้ก็ยังสามารถทำงานต่อไปได้

เดิมทีเดียว APRANET เป็นเพียงเครือข่ายทดลองที่ตั้งขึ้นเพื่อสนับสนุนงานวิจัยด้านการทหารในยุคสงครามเย็น ระหว่างฝ่ายคอมมิวนิสต์และฝ่ายเสรีประชาธิปไตย แต่ต่อมาใน

---

[3] "ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ: หลักเกณฑ์และวิธีการขอรับใบอนุญาตการให้บริการอินเทอร์เน็ต ข้อ3" ราชกิจจานุเบกษา (22มิถุนายน 2548)

[4] http://elearning.nectec.or.th

[5] เลอสรร ธนสุกาญจน์, จิตตภัทร เครือวรรณ และสุธรรม อยู่ในธรรม, กฎหมายสำหรับบริการอินเทอร์เน็ตในประเทศไทย (กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2541), หน้า 12.

ปี พ.ศ. 2512 ได้มีการปรับปรุงหน่วยงานโดยได้รับเงินทุนสนับสนุนจากหลายฝ่ายและตั้งชื่อเรียกหน่วยงานใหม่ว่า ดาร์พา (DARPA : Defense Research Project Agency) พร้อมกับเปลี่ยนแปลงนโยบายในการดำเนินการ และในปี 2518 ดาร์พาได้โอนหน้าที่ดูแลรับผิดชอบในส่วนของหน่วยงาน APRANET ให้แก่ หน่วยการสื่อสารของกองทัพของกองทัพสหรัฐ(Defense Communications Agencyหรือ DCA)(ปัจจุบันคือ Defense Informations Systems Agency)[6]

ในปี พ.ศ.2526 APRANET ได้แบ่งเครือข่ายออกเป็น 2 ส่วน คือ เครือข่ายด้านการวิจัยใช้ชื่อ APRANET และ เครือข่ายที่ใช้ในการทหารใช้ชื่อว่า "มิลเน็ต" (MILNET : MILitary NETwork) ซึ่งเชื่อมต่อเครือข่ายโดยใช้โปรโตคอล TCP/IP (Transmission Control Protocol / Internet Protocol) กับคอมพิวเตอร์ทุกเครื่องในเครือข่าย โดยคอมพิวเตอร์ทุกเครื่องที่จะเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตต้องเพิ่มโปรโตคอล TCP/IPลงไปเสมอ จึงจะสื่อสารและเชื่อมต่อคอมพิวเตอร์เครื่องอื่นๆได้ ซึ่งการเชื่อมต่อโดยวิธีการนี้ถือเป็นมาตรฐานของระบบอินเทอร์เน็ตจนถึงปัจจุบัน ในปี พ.ศ. 2528 มูลนิธิวิทยาศาสตร์แห่งชาติอเมริกา (National Science Foundation หรือ NSF) ได้สร้างเครือข่ายเชื่อมโยงซุปเปอร์คอมพิวเตอร์ จำนวน 6 แห่งเข้าด้วยกัน ชื่อว่า NFSNET และในปี พ.ศ. 2533 APRANET ได้ถูกแทนที่ด้วย NFSNET และเครือข่ายอื่นๆ ซึ่งภายหลังได้มีการเชื่อมเครือข่ายต่างๆเข้าด้วยกันจนกลายเป็นเครือข่ายอินเทอร์เน็ตขนาดใหญ่ดังเช่นในปัจจุบัน

ในประเทศไทย ได้มีการใช้งานอินเทอร์เน็ตเป็นครั้งแรกประมาณปี พ.ศ. 2529 โดยเป็นการวิจัยเพื่อการศึกษาของสถาบันการศึกษาต่างๆ และได้มีการพัฒนาระบบเรื่อยมาจนกระทั่ง ปี พ.ศ. 2538 จึงได้มีการเปิดบริการอินเทอร์เน็ตเชิงพาณิชย์ โดย "บริษัทอินเทอร์เน็ตแห่งประเทศไทย จำกัด" โดยเป็นการถือหุ้นระหว่างการสื่อสารแห่งประเทศไทย องค์การโทรศัพท์แห่งประเทศไทย และสำนักงานพัฒนาวิทยาศาสตร์ และเทคโนโลยีแห่งชาติ สวทช.ถือได้ว่าเป็นบริษัทผู้ให้บริการอินเทอร์เน็ตรายแรกของประเทศไทย

---

[6] http://www.computerhistory.org/exhibits/internet_history.

การทำงานของเครือข่ายอินเทอร์เน็ต

อินเทอร์เน็ต โดยหลักแล้วประกอบไปด้วยเครื่องคอมพิวเตอร์ สายโทรศัพท์ และโมเด็ม การทำงานของอินเทอร์เน็ตจะอยู่ในลักษณะของข่ายงานสวิตช์ข้อมูล (Packet Switch) โดยคอมพิวเตอร์ที่เป็นเครื่องส่งจะแบ่งแยกข้อความออกเป็นหน่วยและขนาดความจำที่เหมาะสม เรียกว่ากลุ่มข้อมูล (Packet) ซึ่งแต่ละกลุ่มข้อมูลจะบรรจุเลขที่อยู่ของคอมพิวเตอร์ปลายทางไว้ด้วย กลุ่มข้อมูลนี้จะถูกส่งไปในข่ายงานและผ่านอุปกรณ์ที่เรียกว่า Router ซึ่งมีหน้าที่ในการอ่านเลขที่อยู่ปลายทางของแต่ละกลุ่มข้อมูล เพื่อที่จะส่งข้อมูลเหล่านั้นไปตามทิศทางได้อย่างเหมาะสม

เมื่อกลุ่มข้อมูลเดินทางไปถึงจุดหมายแล้ว คอมพิวเตอร์ที่เป็นเครื่องรับจะทำหน้าที่รวบรวมข้อมูลที่ได้รับมาจัดเรียงลำดับและส่งข้อมูลนั้นไปยังโปรแกรมที่เหมาะสมและการที่จะทำให้ระบบอินเทอร์เน็ตทำงานได้ อันเป็นผลทำให้คอมพิวเตอร์ทุกเครื่องจะติดต่อสื่อสารถึงกันได้ คือการให้คอมพิวเตอร์เหล่านั้นรู้จักและใช้ภาษาเดียวกัน โดยใช้วิธีควบคุมส่งผ่านตามมาตรฐานอินเทอร์เน็ต TCP/IP ซึ่งเป็นข้อตกลงที่กำหนดการสื่อสารถึงกันไว้[7]

2.1.2 **บุคคลที่เกี่ยวข้องกับระบบเครือข่ายอินเทอร์เน็ต**

ในระบบอินเทอร์เน็ตจะมีบุคคลต่างๆ ที่เข้ามาเกี่ยวข้องหรือมีส่วนร่วมอยู่มากมาย ซึ่งจำแนกออกเป็นประเภทใหญ่ๆดังนี้

1.) <u>ผู้ใช้คอมพิวเตอร์</u> ซึ่งต่อเชื่อมอยู่กับระบบเครือข่ายอินเทอร์เน็ตหรือผู้ใช้อินเทอร์เน็ต หรือผู้ค้นหาข้อมูลข่าวสารทางเครือข่ายอินเทอร์เน็ต

2.) <u>ผู้ให้บริการอินเทอร์เน็ตหรือไอเอสพี (ISP Internet Service Provider)</u> ซึ่งผู้ใช้อินเทอร์เน็ตจะมิได้เข้าใช้อินเทอร์เน็ตโดยตรง แต่จะกระทำผ่านผู้ให้บริการเข้าใช้อินเทอร์เน็ต (Access Provider) ซึ่งแบ่งออกเป็น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) เป็นผู้ให้บริการเพิ่มเติมการเข้าใช้อินเทอร์เน็ต เช่นบริการเก็บ(Host) ข้อมูลที่ผู้ให้บริการ หรือผู้ใช้ หรือบุคคลที่สามจัดทำขึ้น ผู้ให้บริการเข้าใช้อินเทอร์เน็ต(Internet Access Provider) และผู้ให้บริการออนไลน์ (On-Line Service Provider) ซึ่งเป็นผู้ให้บริการข้อมูลแก่สมาชิกในระบบปิดของตน

---

[7] ฐนวรรษ นิติธรรมวิศรุต, "อาชญากรรมทางคอมพิวเตอร์: ศึกษาเฉพาะกรณีการเผยแพร่ภาพและสื่อลามกผ่านทางอินเทอร์เน็ตที่มีคนไทยเป็นผู้เสียหาย," วิทยานิพนธ์ (น.ม. จุฬาลงกรณ์มหาวิทยาลัย, 2544) หน้า 47.

ผู้จัดทำข้อมูลดังกล่าวอาจเป็นผู้ให้บริการเอง หรือบุคคลที่สามที่มีสัญญากับผู้ให้บริการ ในปัจจุบันผู้ให้บริการออนไลน์ มักให้บริการเข้าใช้อินเทอร์เน็ตด้วย

3.) ผู้จัดทำข้อมูล (Content Provider) อาจเป็นผู้ประพันธ์ฐานข้อมูล, ผู้ประพันธ์เรื่อง ,ผู้พิมพ์ผู้โฆษณาข้อความของตนลงสู่อินเทอร์เน็ต ซึ่งผู้จัดทำข้อมูลในอินเทอร์เน็ตมิได้จำกัดเฉพาะเพื่อการค้า คือบุคคลทั่วไปสามารถเป็นผู้จัดทำข้อมูลได้โดยทำลงในกลุ่มข่าว หรือจัดทำเว็บเพจของตนเอง ซึ่งทำให้ผู้ใช้อินเทอร์เน็ตสามารถเข้าถึงผู้อ่านหรือผู้ใช้อินเทอร์เน็ตได้ทั่วโลก

4.) ผู้ทำการลิงค์(Link) ข้อมูลในเครือข่ายอินเทอร์เน็ต

5.) เจ้าของเว็บไซต์ (WebSite) หรือเจ้าของโฮมเพจ(Home page)

6.) เว็บมาสเตอร์ (WebMaster) คือผู้แลเว็บเพจต่างๆเรียกว่าเป็น Administrator ของเว็บเพจ ส่วนใหญ่ผู้สร้างเว็บเพจ จะเรียกว่าเป็น Web Master

7.) ผู้ดูแลหรือเจ้าของ Server ต่างๆ[8]

2.1.3 บริการและกิจกรรมการใช้อินเทอร์เน็ต

บริการต่าง ๆบนเครือข่ายอินเทอร์เน็ต[9]

1. บริการไปรษณีย์อิเล็กทรอนิกส์ (Electronic mail หรือ Email) บริการประเภทนี้เป็นระบบส่งข้อความ(Message) จากต้นทางไปยังปลายทาง(End-to end delivery system) โดยใช้Simple Mail transfer Protocol (SMTP) โปรโตคอลนี้ใช้หลักการ Spooling คือข้อความที่ต้องการส่งจะถูกเข้าคิว (Queue) ไว้ในSpooler เพื่อส่งต่อไปยังสถานีปลายทาง หากไม่สามารถส่งได้ก็อาจจะลองใหม่อีก แต่เมื่อพยายามส่งแล้วหลายครั้งไม่สำเร็จข้อความก็จะถูกส่งกลับมายังต้นทางหรือทิ้งไปเลยก็ได้

---

[8] เรื่องเดียวกัน หน้า 41.

[9] เลอสรร ธนสุกาญจน์,จิตตภัทร เครือวรรณ และสุธรรม อยู่ในธรรม, กฎหมายสำหรับบริการอินเทอร์เน็ตในประเทศไทย, หน้า 46-54.

นอกจากโปรโตคอลSMTPแล้ว เครือข่ายอินเทอร์เน็ตยังมี POP(Post office protocol) ซึ่งช่วยให้ผู้ใช้สามารถทำ Remote Accessเข้า Mail box ได้ ซึ่งต้องการรับส่งไปรษณีย์อิเล็กทรอนิกส์ได้ในขณะที่เข้าไปใน WWW อยู่ เช่น โดยใช้โปรแกรม Internet explorer เป็นต้น

2. บริการสนทนากลุ่ม (Internet relay chat หรือ IRC) บริการประเภทนี้ผู้ใช้จะสามารถสนทนากันได้เกือบจะทันที โดยผู้สนใจอื่นที่อยู่บนอินเทอร์เน็ตสามารถเข้าร่วมวงสนทนาได้ด้วย

3. กลุ่มความสนใจเฉพาะ(Usenet newsgroup) Usenet ย่อมาจาก User's Network ซึ่งเริ่มต้นมาจากผู้ใช้คอมพิวเตอร์ในระบบUnix ที่ต้องการสื่อสารกันเอง จึงถือเป็นการบริการที่เริ่มต้นจากผู้ใช้ โดยผู้ใช้ แต่ยังต้องติดต่อกันผ่านสายโทรศัพท์ ต่อมาเมื่อมีผู้ใช้มากขึ้น การส่ง Newsfeed ต้องเสียค่าใช้จ่าย คือค่าโทรศัพท์ทางไกลมากขึ้นเรื่อยๆจึงได้มีผู้หาทางส่ง Newsfeed ผ่านทางอินเทอร์เน็ต

4.การหาตัว(Finger) เป็นบริการสำหรับหาข้อมูลเกี่ยวกับผู้ใช้หรือหาว่าผู้ใช้กำลังอยู่บนอินเทอร์เน็ตหรือไม่หรือหาว่าคอมพิวเตอร์เครื่องหนึ่งบนอินเทอร์เน็ตมีผู้ใช้รายใดกำลังเปิดเครื่องอยู่บ้าง

ข้อมูลเกี่ยวกับผู้ใช้แบ่งได้สามส่วน คือชื่อ/สังกัดของผู้ใช้ ข้อมูลการต่อเข้าระบบของผู้ใช้ และข้อมูลส่วนเพิ่มเติม (Plan) ซึ่งปกติผู้ใช้เป็นผู้เขียนไว้เองเพื่อให้สาธารณชนเรียกดูได้

5. การเข้าถึงคอมพิวเตอร์ระยะไกล (Telnet) เป็นบริการที่ทำให้โปรแกรมบนคอมพิวเตอร์ต้นทาง (Host machine ซึ่งเรียกว่า Telnet client) สามารถเข้าถึงทรัพยากรต่างๆในคอมพิวเตอร์อีกเครื่องหนึ่ง (เรียกว่า Telnet server)

6. การรับส่งข้อมูล(FTP) โปรโตคอลการรับส่งแฟ้มข้อมูลสามารถทำให้ผู้ใช้ Telnet ไปที่ปลายทางโดยอัตโนมัติ และ Upload หรือ Download แฟ้มข้อมูลระหว่างเครื่องต้นทางหรือ Download แฟ้มข้อมูลไปยังเครื่องที่สามได้

7. ระบบการค้นข้อมูล(Archie และ Gopher) Archie เป็นบริการช่วยค้นข้อมูล (Search) จาก Anonymous FTP site โดยที่ผู้ใช้ต้องเรียกผ่านอินเทอร์เน็ตเข้าไปที่ Archie server ตัวใดตัวหนึ่งแล้วพิมพ์ Search string

Gopher พัฒนาโดยมหาวิทยาลัย Minnesota ช่วยให้ผู้ใช้เรียกดูข้อมูลได้ทำนองเดียวกับFTP แต่มีความสะดวกมากกว่า

8. บริการสารสนเทศพื้นที่กว้าง (Wide Area Information services หรือ WAI) เป็นระบบสืบค้นสารสนเทศจากเครือข่ายอินเทอร์เน็ต ซึ่งได้รับการพัฒนาขึ้นมาจากบริษัท Thinking Machines แต่ต่อมาแยกตัวออกมาเป็น WAIS,Inc. โดย WAI สามารถสืบค้นข้อมูลในอินเทอร์เน็ตโดยใช้คอมพิวเตอร์แบบขนาน(Connection Machine) ซึ่งระบบนี้รับคำสั่งสืบค้นเป็นภาษามนุษย์ได้ทั้งยังมีความรวดเร็วมาก

9. โทรศัพท์โทรภาพและโทรทัศน์ผ่านอินเทอร์เน็ต (Internet phone) ผู้ใช้ที่ต่อเข้าเครือข่ายอินเทอร์เน็ตสามารถหาซอฟแวร์สำหรับโทรศัพท์ทางไกลตอบโต้กันสองคนหรือมากกว่านั้น ข้อดีของบริการประเภทนี้คือสามารถใช้โทรศัพท์ โทรภาพ และโทรทัศน์ในการติดต่อทางได้โดยไม่ต้องจ่ายค่าโทรศัพท์ทางไกล แต่อาจมีปัญหากรณีที่มีการให้การผูกขาดบริการโทรศัพท์ แต่มีการวางInternet backbone ต่างหากจากระบบโทรศัพท์ทางไกล

10. เกมส์สำหรับเล่นบนเครือข่ายคอมพิวเตอร์(Multi-User Dungeon, Multi-User Dimension หรือ MUD) เกมส์ประเภทนี้พัฒนาจากการพิมพ์เป็นตัวหนังสือจนมีรูปภาพ มีเสียง ตลอดจนภาพเคลื่อนไหว และ Virtual reality ซึ่งปัญหาของบริการประเภทนี้คือทำให้ผู้เล่นเกิดการเสพติดจนสูญเสียเวลาในการประกอบการงานอันเป็นประโยชน์อย่างอื่น

กิจกรรมการใช้งานอินเทอร์เน็ต

ในปัจจุบันการใช้งานในระบบเครือข่ายอินเทอร์เน็ตถือเป็นมาตรฐานสากลในการติดต่อสื่อสารหรือสืบค้นข้อมูลสารสนเทศต่างๆจากทุกมุมโลก ไม่ว่าจะเป็นข้อมูลทางวิชาการ การบริการด้านความบันเทิง การประกอบธุรกิจ ฯลฯ ทำให้ผู้ใช้บริการอินเทอร์เน็ตสามารถเข้าถึงข้อมูลข่าวสารได้รวดเร็วด้วยค่าใช้จ่ายที่ไม่สูงนัก

จากผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในปี 2548 ได้จัดประเภทและจัดอันดับกิจกรรมการใช้งานอินเทอร์เน็ตในประเทศไทยดังนี้[10]

1. รับ/ส่งจดหมายอิเล็กทรอนิกส์(E-Mail)
2. ค้นหาข้อมูล (Information Search)
3. สนทนา (Chat)
4. เล่นเกม (Game)
5. ติดตามข่าว (News,Timely,Report)
6. อ่านหรือแสดงความคิดเห็นในเว็บบอร์ด (Webboard)
7. เรียนรู้/หาความรู้ผ่านอินเทอร์เน็ต(E-Leaning)
8. ดาวโหลดซอฟต์แวร์ (Software Download)
9. ฟังเพลงออนไลน์ (Online Music)
10. สร้างเว็บไซต์ของตนเอง
11. ชมสินค้า
12. ดาวน์โหลดเพลง (Music Download)
13. ดาวน์โหลดละคร/ภาพยนตร์/การ์ตูน
14. เขียนเว็บบอร์ด/ไดอารี่/บล็อก
15. ดาวน์โหลดเกม
16. ส่งรูปขึ้นเว็บ
17. ชมทีวีออนไลน์ผ่านอินเทอร์เน็ต
18. โทรศัพท์ผ่านอินเทอร์เน็ต
20. ประชุมทางไกลผ่านอินเทอร์เน็ต
21. อื่นๆ

---

[10] ฝ่ายพัฒนานโยบายและกฎหมาย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ , งานผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2548. (กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2548), หน้า 71-72.

ตารางที่ 2.1 สถิติการใช้งานอินเทอร์เน็ตและจำนวนประชากรโลกในช่วง ปี ค.ศ.2000-2007 [11]

ภูมิภาคต่างๆของโลก	จำนวนประชากร (ปี2007)	จำนวนประชากรคิดเป็น%ต่อประชากรโลก	จำนวนผู้ใช้อินเทอร์เน็ต	%ต่อจำนวนประชากรผู้ใช้อินเทอร์เน็ต	%การใช้ต่อประชากรโลก	การเติบโตของผู้ใช้ ปี2000-2007
แอฟริกา	933,448,292	14.2 %	33,334,800	3.6 %	3.0 %	638.4% %
เอเชีย	3,712,527,624	56.5 %	398,709,065	10.7 %	35.8 %	248.8% %
ยุโรป	809,624,686	12.3 %	314,792,225	38.9 %	28.3%	199.5 %
ตะวันออกกลาง	193,452,727	2.9 %	19,424,700	10.0 %	1.7 %	491.4 %
อเมริกาเหนือ	334,538,018	5.1 %	233,188,086	69.7 %	20.9%	115.7 %
ลาตินอเมริกา/คาริบเบียน	556,606,627	8.5 %	96,386,009	17.3 %	8.7 %	433.4 %
โอเชียเนีย/ออสเตรเลีย	34,468,443	0.5 %	18,439,541	53.5 %	1.7 %	142.0 %
ยอดรวมทั่วโลก	6,574,666,417	100.0 %	1,114,274,426	16.9 %	100.0 %	208.7 %

2.2 ความผิดที่กระทำบนอินเทอร์เน็ต

2.2.1 ประเภทของการกระทำความผิดโดยใช้คอมพิวเตอร์

การกระทำความผิดโดยใช้คอมพิวเตอร์หรืออาชญากรรมคอมพิวเตอร์ ถือเป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่ง ที่ผู้กระทำความผิดส่วนใหญ่มีความรู้ความสามารถในการใช้คอมพิวเตอร์เป็นอย่างดี ซึ่งก่อให้เกิดความเสียหายได้รวดเร็ว มีชื่อเรียกที่แตกต่างกันอยู่มากมาย เช่น[12] Computer crime, E-crime, Information technology crime, Computer related crime Computer misuse, Computer Abuse, Electronic crime หรือ Hitech Crime เป็นต้น

---

[11] http://www.internetworldstats.com/stats.htm.

[12] สุนทร เปลี่ยนสี, "แนวความคิด หลักการและสาระสำคัญของร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์," วารสารกฎหมายปกครอง เล่ม24,ตอน2 (2549): หน้า 100.

นอกจากนี้ ยังมีการต่อต้านการใช้คำว่า "อาชญากรรมคอมพิวเตอร์" และมีการเสนอให้ใช้คำว่า "ความผิดทางอาญาอันเกี่ยวกับคอมพิวเตอร์"แทน เพราะเห็นว่ามีความเหมาะสมกว่า เพราะได้หมายรวมถึงการกระทำต่างๆมากมายต่อคอมพิวเตอร์[13] และรวมถึงการกระทำความผิดโดยใช้คอมพิวเตอร์ในการกระทำผิดอาญาทั่วไป

การให้คำนิยามหรือคำจำกัดความของการกระทำความผิดลักษณะนี้ยังเป็นปัญหาในด้านกฎหมายว่ามีความหมายครอบคลุมเพียงใด ดังนั้นการแบ่งประเภทของการกระทำความผิดโดยใช้คอมพิวเตอร์ จึงแตกต่างกันไป ทั้งนี้อาจอยู่กับหลายปัจจัย เช่น แนวคิดของนักกฎหมายที่แตกต่างกัน บทบัญญัติของกฎหมายที่แตกต่างกันในแต่ละรัฐหรือในแต่ละประเทศ เป็นต้น

ศาสตราจารย์ วีระพงษ์ บุญโญภาส ได้กล่าวถึงนิยามของอาชญากรรมคอมพิวเตอร์ไว้ดังนี้ *"อาชญากรรมคอมพิวเตอร์ มีการให้นิยามไว้เป็น 2 นัย นัยแรก อาชญากรรมคอมพิวเตอร์ หมายความถึงการกระทำใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ และทำให้ผู้เสียหายนั้นได้รับความเสียหาย ในขณะเดียวกันก็ทำให้ผู้กระทำความผิดนั้นได้รับประโยชน์*

นัยที่สอง อาชญากรรมคอมพิวเตอร์ หมายความถึงการกระทำใดๆ ที่เป็นความผิดทางอาญา ซึ่งจะต้องใช้ความรู้เกี่ยวกับคอมพิวเตอร์ในการกระทำความผิดนั้น ซึ่งแน่นอนว่าการสืบสวน การฟ้องร้อง หรือการดำเนินคดีทั้งหลายจะต้องใช้ความรู้ในส่วนของคอมพิวเตอร์ด้วย"[14]

การแบ่งประเภทของการกระทำความผิดโดยพิจารณาจากวิธีการที่ใช้

วิธีการในการประกอบอาชญากรรมคอมพิวเตอร์มีอยู่มากมายหลายวิธีและมีชื่อเรียกต่างๆกันไป เช่น Data Diddling อาจเรียกว่า Tempering หรือ Wiretapping อาจเรียกว่า Eavesdropping ก็ได้ อย่างไรก็ดี อาจแบ่งประเภทตามวิธีการกระทำความผิด ได้ดังนี้[15]

---

[13] วีระพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ,(กรุงเทพฯ: นิติธรรม, 2540), หน้า 159.

[14] สถาบันกฎหมายอาญา, "กฎหมายอาชญากรรมทางคอมพิวเตอร์ : แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที,"รายงานการสัมมนาทางวิชาการ โครงการเวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย,2542: 16.

[15] จุลเจษฎ์ ฉัตราคม, "พาณิชย์อิเล็กทรอนิกส์ : อาชญากรรมคอมพิวเตอร์กับพัฒนาการของสัญญาและกฎหมาย," ดุลพาห, 47 ฉบับที่2: 15.

1. Data Diddling หรือ Tampering คือ การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตก่อนหรือระหว่างที่กำลังบันทึกข้อมูลลงไปในระบบคอมพิวเตอร์ การเปลี่ยนแปลงข้อมูลดังกล่าวนี้สามารถกระทำโดยบุคคลใดก็ได้ที่สามารถเข้าไปถึงตัวข้อมูล ตัวอย่างเช่น พนักงานเจ้าหน้าที่ที่มีหน้าที่บันทึกเวลาการทำงานของพนักงานทั้งหมด ทำการแก้ไขตัวเลขชั่วโมงการทำงานของคนอื่นมาลงเป็นชั่วโมงการทำงานของตนเอง ซึ่งข้อมูลดังกล่าวหากถูกแก้ไขเพียงเล็กน้อย พนักงานแต่ละคนแทบจะไม่สงสัยเลย

2. Trojan Horse คือ โปรแกรมที่ปรากฏให้เห็นในการทำงานที่เป็นประโยชน์แต่ได้ซ่อนรหัสคำสั่งที่จะทำความเสียหาย ให้แก่ระบบที่กำลังดำเนินงานนั้นได้ ม้าโทรจันนี้จะไม่เหมือนไวรัสเนื่องจากไม่สามารถติดลงไปในแผ่นบันทึกอื่นได้ ในขณะที่ไวรัสจะติดไปกับแผ่นบันทึกและแพร่เข้าไปในคอมพิวเตอร์เครื่องอื่นๆ

3. Salami Techniques คือ วิธีการปัดเศษจำนวนเงิน เช่น ทศนิยมตัวที่ 3 หรือปัดเศษทิ้งให้เหลือแต่จำนวนเงินที่สามารถจ่ายได้ แล้วนำเศษทศนิยมหรือเศษที่ปัดทิ้งมาใส่ในบัญชีของตนเองหรือของผู้อื่นซึ่งจะทำให้ผลรวมของบัญชียังคงสมดุลย์ (Balance) และจะไม่มีปัญหากับระบบควบคุมเนื่องจากไม่มีการนำเงินออกจากระบบบัญชี นอกจากใช้กับการปัดเศษเงินแล้ววิธีนี้อาจใช้กับระบบการตรวจนับของในคลังสินค้า

4. Trap Doors คือ โปรแกรมที่ลวงผู้ใช้คอมพิวเตอร์ที่มีสิทธิในการใช้ระบบเพื่อจะได้รู้รหัสผ่าน(Password) หรือบัญชีผู้ใช้ โดยจะสร้างหน้าจอปลอมที่มีลักษณะคล้ายหน้าจอจริงเพื่อลวงให้ผู้ใช้ใส่รหัสผ่านและผู้กระทำความผิดสามารถเรียกข้อมูลที่เก็บไว้ขึ้นดูได้ในภายหลัง

5. Logic bombหรือ Fork Bomb คือ โปรแกรมที่จะทำงานเมื่อเป็นไปตามเงื่อนไขที่กำหนดเพื่อติดตามและแก้ไขระบบ โดยจะมีลักษณะคล้ายการระเบิดและทำให้โปรแกรมหยุดการทำงาน หรือเกิดความเสียหายแก่ข้อมูลทั้งหมด โดยโปรแกรมจะเริ่มทำงานต่อเมื่อมีสภาวะหรือสภาพการณ์ตามที่ผู้สร้างโปรแกรมกำหนด สามารถใช้ติดตามดูความเคลื่อนไหวของระบบบัญชี ระบบเงินเดือนแล้วทำการเปลี่ยนแปลงตัวเลขดังกล่าว

6. Asynchronous Attack คือ เนื่องจากการทำงานของระบบคอมพิวเตอร์เป็นการทำงานแบบ Asynchronous คือสามารถทำงานหลายๆ อย่างพร้อมกัน โดยการประมวลผลข้อมูลเหล่านั้นจะเสร็จไม่พร้อมกัน ผู้ใช้งานจะทราบว่างานที่ประมวลผลเสร็จหรือไม่ก็ต่อเมื่อเรียกงานนั้น

มาดู ระบบดังกล่าวก่อให้เกิดจุดอ่อน ผู้กระทำความผิดจะฉวยโอกาสในระหว่างที่เครื่องกำลังทำงานเข้าไปแก้ไขเปลี่ยนแปลงหรือกระทำการอื่นใดโดยที่ผู้ใช้ไม่ทราบว่ามีการกระทำผิดเกิดขึ้น

7. Scavenging คือ วิธีการที่จะได้ข้อมูลที่ทิ้งไว้ในระบบคอมพิวเตอร์หรือบริเวณใกล้เคียง หลังจากเสร็จการใช้งานแล้ว วิธีที่ง่ายที่สุดคือ ค้นหาตามถังขยะที่อาจมีข้อมูลสำคัญไม่ว่าจะเป็นเบอร์โทรศัพท์หรือรหัสผ่านหลงเหลืออยู่ หรืออาจใช้เทคโนโลยีที่ซับซ้อนทำการหาข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์เมื่อผู้ใช้เลิกใช้งานแล้ว

8. Data Leakage คือ หมายถึงการทำให้ข้อมูลรั่วไหลออกไป อาจโดยตั้งใจหรือไม่ก็ตาม เช่นการแผ่รังสีของคลื่นแม่เหล็ก ไฟฟ้าในขณะที่กำลังทำงาน คนร้ายอาจตั้งเครื่องดักสัญญาณไว้ใกล้กับเครื่องคอมพิวเตอร์เพื่อรับข้อมูลตามที่ตนเองต้องการ

9. Piggybacking คือ วิธีการดังกล่าวสามารถทำได้ทั้งทางกายภาพ (Physical) การที่คนร้ายจะลักลอบเข้าไปในประตูที่มีระบบรักษาความปลอดภัย คนร้ายจะรอให้บุคคลที่มีอำนาจหรือได้รับอนุญาตมาใช้ประตูดังกล่าว เมื่อประตูเปิดและบุคคลคนนั้นได้เข้าไปแล้ว คนร้ายก็ฉวยโอกาสตอนที่ประตูยังไม่ปิดสนิทแอบเข้าไปได้ ในทางอิเล็กทรอนิกส์ก็เช่นกัน อาจเกิดขึ้นในกรณีที่ใช้สายสื่อสารเดียวกันกับผู้ที่มีอำนาจใช้หรือได้รับอนุญาต เช่นใช้สายเคเบิลหรือโมเด็มเดียวกัน

10. Impersonation คือ การที่คนร้ายแกล้งปลอมเป็นบุคคลอื่นที่มีอำนาจหรือได้รับอนุญาต เช่น เมื่อคนร้ายขโมยบัตรเอทีเอ็มของเหยื่อได้ ก็จะโทรศัพท์และแกล้งทำเป็นเจ้าพนักงานของธนาคารและแจ้งให้เหยื่อทราบว่ากำลังหาวิธีป้องกันมิให้เงินในบัญชีของเหยื่อ จากนั้นจึงบอกให้เหยื่อเปลี่ยนรหัสประจำตัว (Personal Identification Number: PIN) โดยให้เหยื่อบอกรหัสเดิมก่อน คนร้ายจึงทราบหมายเลขรหัส และได้เงินของเหยื่อไป

11. Wiretapping หรือ Eavesdropping หรือ Packet Sniffer คือ การดักฟังสัญญาณการสื่อสารโดยมีเจตนาที่จะได้รับประโยชน์จากการเข้าสู่ระบบเพื่อเข้าถึงข้อมูล โดยการใช้โปรแกรมสำหรับดักจับข้อมูลเพื่อให้ได้มาซึ่ง เลขประจำตัว(ID) รหัสผ่าน (Password) ข้อมูลบัตรเครดิต และข้อมูลสำคัญอื่นๆ โปรแกรมที่นิยมใช้ในการกระทำผิดประเภทนี้ มีชื่อว่า Sniffer[16]

---

[16] ไพจิตร สวัสดิสาร, การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์, (กรุงเทพมหานคร : โรงพิมพ์ชวนพิมพ์, 2547), หน้า 107.

12. Computer Forgery คือ การปลอมแปลงข้อมูลหรือการตัดต่อข้อมูลคอมพิวเตอร์

13. Computer Fruad คือ การฉ้อโกงข้อมูลทางคอมพิวเตอร์ เช่น การฉ้อโกงบัตรเครดิตหรือเงินอิเล็กทรอนิกส์หรือการเข้ารหัสลับของผู้มีสิทธิเพื่อให้ได้มาซึ่งประโยชน์ในทางทรัพย์สิน[17]

14. Unauthorized Reproduction of a Protected Computer Program คือ การผลิตเพื่อจำหน่ายซึ่งโปรแกรมของผู้อื่นโดยไม่ได้รับอนุญาต

15. Theft of Service (การขโมยบริการ) เจ้าของเครื่องคอมพิวเตอร์อาจจะต้องสูญเสียรายได้คิดเป็นมูลค่ามหาศาล จากการที่มีบุคคลอื่นมาใช้ประโยชน์ และบริการจากเครื่องคอมพิวเตอร์โดยไม่ยอมจ่ายค่าใช้บริการ การกระทำดังกล่าวเรียกว่า การขโมยบริการ ซึ่งแต่ละบริการก็มักจะส่งผลตอบแทนแก่ผู้ขโมยบริการอย่างมากมาย การฟ้องผู้กระทำความผิดในข้อหาลักทรัพย์ธรรมดาก็เป็นการยากที่ศาลจะลงโทษเพราะบริการที่ถูกลักขโมยมักจะเป็นสิ่งที่ไม่มีรูปร่างโดยธรรมชาติ[18]

นอกจากที่ได้กล่าวมาแล้วยังมีการกระทำความผิดในรูปแบบที่อื่นๆบนเครือข่ายอินเทอร์เน็ตอีก เช่น เทคนิคการโจมตีแบบ Phishing[19] (มาจากคำว่า Password + Havesting+Fishing)[20] คือ การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ (Email Spoofing) และทำการสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ Phishing สามารถทำได้โดยการขโมยหรือนำเครื่องหมายหรือสัญลักษณ์ตลอดจนรูปลักษณ์ของธนาคารหรือสถาบันการเงินที่มีชื่อเสียง และบัตรเครดิตประเภทต่างๆของผู้ประกอบการ การให้

---

[17] จุลเจษฎ์ ฉัตราคม, ดุลพาห,47 ฉบับที่2: 15.

[18] http://www.judiciary.go.th/jti/research/detail/chatchawan_4.doc

[19] โกเมน พิบูลย์โรจน์, Thaicert(Nectec), เอกสารเผยแพร่เรื่องเทคนิคการโจมตีแบบPhishing , เผยแพร่ 1 มิถุนายน 2547.

[20] http:// www.thaicert.nectec.or.th

สินเชื่อทางอินเทอร์เน็ต มาประกอบเข้ากับการหลอกลวงเหยื่อหรือผู้ใช้ให้เปิดเผยข้อมูล ในปัจจุบันต่างประเทศมีการตื่นตัวในการแก้ปัญหา Phishing เช่นประเทศญี่ปุ่นมีการตั้งศูนย์บริการสายด่วนให้คำแนะนำในการป้องกัน Phishing (Anti-Phishing hotline)[21] ส่วนในประเทศไทยยังไม่ตื่นตัวกับปัญหา Phishing เท่าที่ควร ทั้งๆที่การกระทำความผิดประเภทนี้เกิดขึ้นในประเทศไทยแล้ว ซึ่งคดีที่มีผู้ถูกหลอกลวงสูญเสียทรัพย์สินไปมูลค่ามากที่สุดเป็นจำนวนเงิน 16 ล้านบาท โดยอีเมล์หลอกลวงส่งมาจากประเทศไนจีเรีย[22]

เทคนิคการโจมตีแบบ Phishing ยังมีการกระทำความผิดแบบ Vishing คือสปายแวร์ที่มีการโจมตีแบบฟิชชิงโดยใช้เครือข่ายวอยส์โอเวอร์ไอพี (VoIP) เป็นหลัก[23] เพื่อให้ได้มาซึ่งข้อมูลทางการเงินหรือข้อมูลสารสนเทศอื่นๆ หรือ การกระทำความผิดแบบ Botnet (roBOT NETwork) ซึ่งเป็นภัยต่อผู้ใช้อินเทอร์เน็ตรูปแบบใหม่ที่เขียนด้วยโปรแกรมประสงค์ร้าย (Malware) ที่ซับซ้อนและมีรูปแบบหลากหลายกว่าไวรัส หรือหนอนคอมพิวเตอร์ (Worm) หลายเท่า Botnet สร้างขึ้นเพื่อส่ง แสปมเมลล์(Spammail) และมีการนำBotnet ไปใช้กับการกระทำผิดอื่นๆ ด้วย เช่น กรรโชกทรัพย์[24]

การแบ่งประเภทของการกระทำความผิดโดยพิจารณาจากการใช้คอมพิวเตอร์ที่เกี่ยวกับกระบวนการ และฮาร์ดแวร์/ซอฟแวร์

ในการแบ่งประเภทของอาชญากรรมคอมพิวเตอร์ อาจแบ่งแยกโดยพิจารณาจากกระบวนการ (Process-oriented Approach) และฮาร์ดแวร์/ซอฟแวร์ (Hardware/Software-oriented approach) ได้ดังนี้[25]

---

[21] National police academy (Alumni Association for national police academy), Crime in japan in 2004

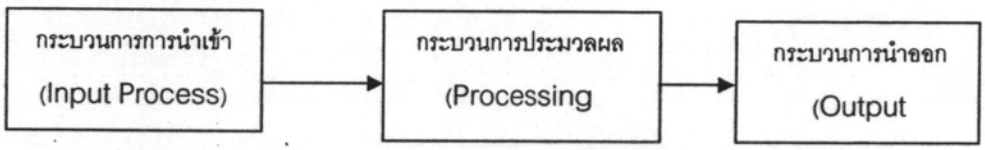
[22] ญาณพล ยั่งยืน , "ร่วมวิพากษ์ร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...." การเสวนารับฟังความคิดเห็นจัดโดยสมาคมผู้ดูแลเว็บไทย วันที่ 21 ธันวาคม 2549.

[23] http://en.wikipedia.org/wiki/Vishing

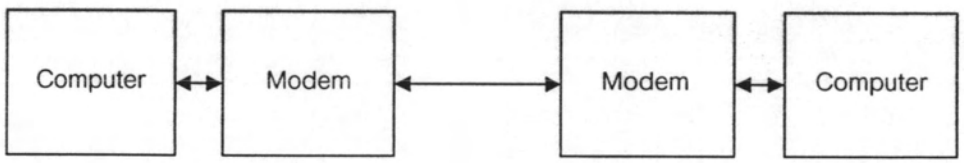
[24] กมล เขมะรังสี และกิติศักดิ์ จิรวรรณกูล, เอกสารเผยแพร่เรื่องบอตเน็ต ภัยรูปแบบใหม่บนอินเทอร์เน็ต เผยแพร่เมื่อ 10 สิงหาคม 2548

[25] ไพจิตร สวัสดิสาร, การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์, หน้า 114-115.

1. Process-oriented Approach การแบ่งประเภทโดยพิจารณาจากขั้นตอนการทำงานของเครื่องคอมพิวเตอร์ โดยจะเริ่มจากกระบวนการนำเข้า (Input process) โดยนำข้อมูลดิบป้อนเข้าสู่คอมพิวเตอร์ เพื่อเข้าสู่ขั้นตอนประมวลผล (Processing) และขั้นตอนสุดท้ายเป็นขั้นตอนการนำข้อมูลออก (0utput) นอกจากนี้ยังมีกระบวนการสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์การกระทำ



รูปที่ 2.1 การแสดงขั้นตอนการทำงานของเครื่องคอมพิวเตอร์



รูปที่ 2.2 แสดงขั้นตอนสื่อสารข้อมูลคอมพิวเตอร์(Transmission)[26]

การกระทำความผิดอาจแบ่งได้โดยพิจารณาจากขั้นตอนการทำงานของคอมพิวเตอร์ดังนี้[27]

1.1 Input process เช่น การสับเปลี่ยนdisk การทำลายข้อมูล การป้อนข้อมูลเท็จ การลักข้อมูลข่าวสาร (Data) (Computer Espionage)การลักใช้บริการหรือเข้าไปโดยไม่มีอำนาจ (Unauthorized access) ตัวอย่างสำหรับกรณีดังกล่าว เช่น[28]

1. การใช้ข้อมูลปลอม เพื่อให้คอมพิวเตอร์สั่งจ่ายเงินแก่อาชญากรหรือผู้สมคบ
2. การป้อนข้อมูลเพื่อปิดบังพยานหลักฐานการกระทำความผิดอื่นๆ

---

[26] เรื่องเดียวกัน หน้า 114.

[27] เรื่องเดียวกัน หน้า 114 -115.

[28] วีระพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ, หน้า 159.

3. การใช้ Password โดยไม่มีสิทธิ

4. การเพิ่มเติมข้อมูลที่ไม่เป็นจริงและลบล้างข้อมูลที่ถูกต้องที่ได้บันทึกไว้ของศูนย์ข้อมูลคอมพิวเตอร์ (Computer credit bureau files)

1.2 Processing เช่น การทำลายข้อมูลและระบบโดยใช้ไวรัส (Computer Subotage) การทำลายข้อมูลและโปรแกรม (Damage to data and program) การสับเปลี่ยนข้อมูลและโปรแกรม (Alteration of data and program) การเปลี่ยนแปลงข้อมูลและโปรแกรม (Alteration of data and program)

1.3 Transmission เช่น การดักฟัง (Wiretapping) การดูดสัญญาณข้อมูล (Unauthorized interception) การก่อกวนในระบบเครือข่าย (Networking Malfeasance)

1.4 Output เช่น การขโมยขยะ (Sewaging) การขโมยprintout หรือการใช้ข้อมูลprintoutอันเป็นเท็จ การกระทำความผิดโดยใช้คอมพิวเตอร์ส่วนใหญ่จะมุ่งประสงค์ต่อผลลัพธ์(Output)ของระบบคอมพิวเตอร์ คดีที่เกิดขึ้นส่วนใหญ่ผลลัพธ์(Output) ที่ได้จากคอมพิวเตอร์จะมาจากข้อมูลอันเป็นเท็จที่ใส่เข้าไป(Input) ทำให้ผลลัพธ์ออกมาผิดพลาด เช่นในคดี UNITED STATES v. JONES โดยข้อเท็จจริงในคดีนี้ปรากฏว่าจำเลยใช้ข้อมูลอันเป็นเท็จ เพื่อจะทำให้คอมพิวเตอร์พิมพ์ตั๋วแลกเงินอันแท้จริงโดยใส่ชื่อจำเลยลงไป แม้บุคคลใดจะอ้างว่ากรณีดังกล่าวเป็นความผิดอาญาอันเกี่ยวเนื่องกับกระบวนการป้อนข้อมูล (Input) หรือแสดงผลลัทธ์ (Output) ก็ตาม ก็ไม่ได้มีความแตกต่างกันเลย[29]

2.Hardware/Software-oriented approach

ก. การกระทำต่อเครื่องโดยตรง อาจแบ่งได้ 3 ประเภทคือ

1. การกระทำต่อ Hardware โดยแท้จริงแล้วกระทำผิดในลักษณะนี้เป็นการกระทำทางกายภาพต่อคอมพิวเตอร์และส่วนประกอบต่างๆของคอมพิวเตอร์ เช่น การทำลายคอมพิวเตอร์และส่วนประกอบของคอมพิวเตอร์ การลักเครื่องคอมพิวเตอร์ เป็นต้น การกระทำผิดต่างๆเหล่านี้ สามารถลงโทษผู้กระทำความผิดได้ตามกฎหมายที่มีบัญญัติไว้อยู่เดิม โดยไม่ต้อง

---

[29] เรื่องเดียวกัน, หน้า 164.

บัญญัติกฎหมายเพิ่มเติมแต่อย่างใด เช่น ตามตัวอย่างที่กล่าวไว้ข้างต้นก็อาจลงโทษผู้กระทำความผิดในฐานทำให้เสียทรัพย์หรือลักทรัพย์ ตามประมวลกฎหมายอาญาได้

2 .*การกระทำต่อ Software* เช่น การลอกเลียนหรือทำสำเนาโดยไม่ได้รับอนุญาต การขโมยโปรแกรม การทำลายโปรแกรม การยุ่งเกี่ยวโดยมิชอบ เป็นต้น

3 *การกระทำต่อ Data and Communication เช่น* การขโมยข้อมูล การทำลายข้อมูล การแก้ไขข้อมูล การขโมยบริการสื่อสาร การฉ้อโกง การทำให้เครือข่ายเสียหาย และในบางกรณีอาจมีการคาบเกี่ยวกับการกระทำต่อHardwareด้วย เช่นการทำลายเครื่องคอมพิวเตอร์เพื่อลบล้างข้อมูลภายในเครื่อง

ข.การกระทำต่อคอมพิวเตอร์ซึ่งเป็นเป้าหมาย

การกระทำผิดใน การลักษณะนี้จะมุ่งประสงค์เพื่อให้ได้มาซึ่งข้อมูลทางคอมพิวเตอร์หรือ ทำให้ระบบขัดข้องเสียหาย เช่น การลอบเข้าไปขโมยข้อมูลต่างๆที่เก็บไว้ในคอมพิวเตอร์ โดยวิธีการต่างๆ เช่น Data diddling, Trojan Horse, Asynchronous Attack, Logic bomb, Superzapping เป็นต้น

ค.การกระทำความผิดโดยใช้คอมพิวเตอร์เป็นเครื่องมือ

เป็นการกระทำความผิดโดยอาศัยคอมพิวเตอร์เป็นเครื่องมือ เช่นการเผยแพร่ภาพลามก การเล่นการพนันโดยอาศัยเครือข่าย การหมิ่นประมาทโดยการโฆษณา การปลอมแปลงบัตรบริการเงินด่วน (ATM)หรือบัตรเครดิต การปลอมเอกสาร การลักลอบโอนเงินหรือการขโมยรหัสผ่าน(Password) โดยวิธีการต่างๆ เช่น Trap Doors, Salami Techniques เป็นต้น

ง. การใช้คอมพิวเตอร์ในการประกอบอาชญากรรม

การกระทำผิดโดยใช้คอมพิวเตอร์เป็นเครื่องมือช่วยในการกระทำความผิดประเภทอื่นๆ เช่นการเก็บข้อมูลเกี่ยวกับการพนันไว้ในคอมพิวเตอร์ การฉ้อโกงหรือยักยอกบนเครือข่าย เป็นต้น

ลักษณะของอาชญากรคอมพิวเตอร์ (Categories of Computer Criminals)[30]

1. *พวกหัดใหม่ (Novice)* บุคคลประเภทนี้มิได้เป็นอาชญากรโดยแท้จริง เพียงแค่ใช้โอกาสในตำแหน่งหน้าที่ที่มีอยู่ เข้าไปดำเนินการกับข้อมูลคอมพิวเตอร์ เพื่อเข้าไปยังฐานข้อมูลนั้นๆ และมีเป็นจำนวนมาก ที่เป็นลูกจ้าง หรือพนักงานของหน่วยงานนั้นๆ เอง

2. *พวกวิกลจริต (Deranged persons)* ลักษณะของบุคคลประเภทนี้ มักกระทำอะไรโดยปราศจากเหตุผล ชอบทำลาย เป็นผู้ป่วยทางจิตและมีอันตรายโดยทั่วไป ไม่สามารถควบคุมตนเองได้ และจะทำลายระบบ ซอฟท์แวร์ หรือแฟ้มข้อมูลต่างๆ

3. *เป็นกลุ่มที่ประกอบอาชญากรรมในลักษณะองค์กร (Organized crime)* เป็นพวกที่ประกอบ อาชญากรรมโดยหาผลประโยชน์จากคอมพิวเตอร์ มีการกระทำร่วมเป็นกลุ่ม มีความรู้คอมพิวเตอร์เป็นอย่างดี สามารถใช้ในการหลบหลีกหรือยับยั้งการสืบสวนติดตามจับกุมของเจ้าหน้าที่ได้

4. *พวกมืออาชีพ (Career)* เป็นพวกกระทำผิด โดยสันดานถึงแม้ว่าจะถูกจับกุมแล้วเมื่อพ้นโทษออกมา ก็จะกระทำความผิดซ้ำอีก

5. *พวกหัวพัฒนา (Con artists)* เป็นพวกที่ชอบใช้ความก้าวหน้าทางคอมพิวเตอร์ ให้ได้มาซึ่งผลประโยชน์ทางการเงิน

6. *พวกช่างคิดช่างฝัน (Ideologues)* เป็นพวกที่กระทำผิดเนื่องจากมีความเชื่อถือในสิ่งหนึ่งสิ่งใดอย่างรุนแรง เป็นพวกก้าวร้าวชอบแสดงตัวเองว่ามีจุดเด่น หรือมีอำนาจเหนือบุคคลอื่น

7. *พวก Hacker/Cracker* เป็นพวกที่จงใจ และเจตนาเข้าถึงระบบของคอมพิวเตอร์ และแฟ้มข้อมูล โดยแยกความหมายของ Hacker/Cracker ได้ดังนี้

---

[30] สุปรียา อภิวัฒนากร, "อาชญากรรมทางคอมพิวเตอร์ : ศึกษากรณีการหลอกลวงทางอินเทอร์เน็ต," วิทยานิพนธ์ (น.ม. จุฬาลงกรณ์มหาวิทยาลัย, 2545)

7.1 Hacker หมายถึง บุคคลผู้ที่เป็นอัจฉริยะ มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์โดยเจาะผ่านระบบ รักษาความปลอดภัยของคอมพิวเตอร์ได้ แต่อาจไม่แสวงหาผลประโยชน์

7.2 Cracker หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดี จนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูล หรือทำให้เครื่องคอมพิวเตอร์เสียหาย รวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

2.2.2 รูปแบบและลักษณะของการกระทำความผิดบนอินเทอร์เน็ต

การกระทำความผิดบนอินเทอร์เน็ต (Cyber Crime) คือ การกระทำความผิดบนเครือข่ายอินเทอร์เน็ต ซึ่งในที่นี้หมายรวมถึงการกระทำความผิดโดยใช้คอมพิวเตอร์(Computer Crime)ด้วย แต่การกระทำความผิดบนอินเทอร์เน็ต (Cyber Crime) เป็นการกระทำความผิดบนเครือข่ายอินเทอร์เน็ตเท่านั้น ไม่รวมถึงการกระทำความผิดต่อ Hardware ที่มุ่งกระทำความผิดต่อคอมพิวเตอร์ในทางกายภาพ เช่น การลักคอมพิวเตอร์หรือการทำให้คอมพิวเตอร์เสียหายในทางกายภาพ และไม่หมายรวมถึงการกระทำความผิดบนเครือข่ายอื่นที่ไม่ใช่อินเทอร์เน็ต เช่น การโกงภายในธนาคารหรือภายในบริษัทเดียวกันที่แม้เป็นการกระทำความผิดบนเครือข่ายแต่เครือข่ายดังกล่าวไม่ใช่เครือข่ายอินเทอร์เน็ต การกระทำความผิดนั้นก็เป็นเพียงการกระทำความผิดโดยใช้คอมพิวเตอร์ (Computer Crime) เท่านั้น เพราะเป็นการกระทำความผิดในหน่วยงานนั้นๆเอง ไม่ได้ออนไลน์เชื่อมต่อกับผู้ใช้งานอื่นบนระบบอินเทอร์เน็ต[31] และแตกต่างจาก Hi-Tech Crime ที่ครอบคลุมถึงการกระทำผิดทุกชนิดที่เกี่ยวกับเทคโนโลยี เช่น การโกงมือถือ โกงค่าโทรศัพท์ หรือการแอบตั้งเกตเวย์โทรทางไกลไปต่างประเทศ เป็นต้น

ดังนั้น การกระทำความผิดตามที่ได้กล่าวมาแล้วตามหัวข้อที่ 2.2.1 ประเภทของการกระทำความผิดโดยใช้คอมพิวเตอร์ หากได้กระทำลงบนเครือข่ายอินเทอร์เน็ตแล้ว ถือว่าเป็นการกระทำความผิดบนอินเทอร์เน็ต (Cyber Crime) เช่น Data Diddling , Trojan Horse, Salami Techniques, Trap Doors, Logic bomb, Asynchronous Attack, Scavenging,8.Data

---

[31] "ญาณพล ยั่งยืน : กับงานสอบสวนคดีพิเศษบนโลกอาชญากรรมออนไลน์" บทสัมภาษณ์นักวิชาการ http://www.Thaicleannet.com .

Leakage, Piggybacking, Impersonation,Wiretapping,Computer Forgery,Computer Fruad,Unauthorized Reprodvation of a Protected Computer Program,Theft of Service การกระทำผิดโดยใช้คอมพิวเตอร์ต่างๆเหล่านี้หากได้กระทำบนเครือข่ายอินเทอร์เน็ตแล้วย่อมเป็นการกระทำความผิดบนอินเทอร์เน็ต (Cyber Crime)

นอกจากนี้ ยังสามารถแยกประเภทของการกระทำความผิดบนอินเทอร์เน็ตได้เป็น 9 ประเภท ดังนี้[32]

1. การลักลอบการขโมยใช้บริการสารสนเทศ (Theft of Information Service) เป็นการขโมยข้อมูลเพื่อที่จะใช้ประโยชน์ในการลักลอบเข้าไปใช้บริการโทรคมนาคม เช่น การขโมยข้อมูลเกี่ยวกับศูนย์โทรศัพท์เพื่อที่จะสามารถควบคุมการใช้โทรศัพท์ของหน่วยงานใดหน่วยงานหนึ่งโดยเอาข้อมูลนั้นมาเป็นประโยชน์แก่ตน เช่น การลักลอบใช้โทรศัพท์ฟรี รวมถึงการขโมยข้อมูลจากผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อขโมยใช้บริการ หรือขโมยการรับบริการจากประชาชนทั่วไป ทำให้บุคคลดังกล่าวต้องรับภาระในค่าบริการเป็นต้น

2 .การใช้อินเทอร์เน็ตในการอำนวยความสะดวกแก่การประกอบอาชญากรรมรูปแบบดั้งเดิม (Communication in Furtherance of Criminal Conspiracies) คือการที่ผู้กระทำความผิดนำเอาเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ตมาใช้ในการกระทำความผิดรูปแบบเดิม เช่น อาชญากรรมธรรมดาทั่วไปที่ทำผิดเกี่ยวกับการขนหรือค้ายาเสพติด ใช้การสื่อสารผ่านเครือข่ายอินเทอร์เน็ตในการประกอบอาชญากรรม รวมถึงการใช้คอมพิวเตอร์ในการปกปิดหรือกลบเกลื่อนการกระทำความผิดของตนไม่ให้ผู้อื่นล่วงรู้ ด้วยวิธีการที่เรียกว่า EnCryption หรือการตั้งรหัสการสื่อสารขึ้นมาระหว่างผู้ร่วมกระทำความผิดด้วยกันซึ่งผู้อื่นไม่อาจเข้าใจได้

3. การละเมิดทรัพย์สินทางปัญญา (Telecommunication Piracy) เป็นการใช้เครือข่ายอินเทอร์เน็ตในการละเมิดลิขสิทธิ์ เช่น การดัดแปลง ทำซ้ำ หรือเผยแพร่งานอันมีลิขสิทธิ์โดยไม่ได้รับอนุญาต โดยในปัจจุบันการรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตสามารถทำได้

---

[32] สถาบันกฎหมายอาญา, "กฎหมายอาชญากรรมทางคอมพิวเตอร์ : แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที,"รายงานการสัมมนาทางวิชาการ โครงการเวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย, หน้า 11-13. ; อณิญพิไล เงินวิจิตร, "ปัญหาการค้นและยึดพยานหลักฐานทางอิเล็กทรอนิกส์", วิทยานิพนธ์ (น.ม. จุฬาลงกรณ์มหาวิทยาลัย, 2544)

โดยง่ายและรับส่งข้อมูลได้รวดเร็วเป็นปริมาณมาก การละเมิดทรัพย์สินทางปัญญาจึงเป็นอีกหนึ่งปัญหาสำคัญที่ยากต่อการป้องกันและปราบปราม

4. การเผยแพร่สิ่งผิดกฎหมาย (Pornography and Other Offensive Content) การใช้คอมพิวเตอร์และการสื่อสารผ่านเครือข่ายเพื่อเผยแพร่ภาพลามกอนาจารรวมถึงข้อมูลที่ไม่สมควร หรือการเผยแพร่ข้อมูลที่ขัดต่อกฎหมายและศีลธรรม เช่น ภาพลามกอนาจารของเด็ก วิธีการก่ออาชญากรรมหรือการผลิตวัตถุระเบิด

5. การฟอกเงินทางอิเล็กทรอนิกส์ (Electronic Monney Laudering) ซึ่งใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเป็นเครื่องมือทำให้สามารถกลบเกลื่อนอำพรางตัวตนของผู้กระทำความผิดได้ง่ายขึ้นและการชำระเงินเนื่องจากการพาณิชย์อิเลคโทรนิคส์ (Electronic commerce)

6. การทำลายและการก่อการร้ายทางอิเล็กทรอนิกส์ (Electronic Vandalism and Terrorism) อันธพาลทางคอมพิวเตอร์หรือพวกก่อการร้าย ซึ่งไม่เพียงแต่เฉพาะผู้มีจิตใจชั่วร้ายเท่านั้นแต่ยังมีพวกท้าทายทางเทคนิค อยากรู้อยากเห็นว่าสามารถเข้าไปแทรกแซงระบบข้อมูลคอมพิวเตอร์ของผู้อื่นได้มากน้อยเพียงใด อันธพาลทางคอมพิวเตอร์ เปรียบได้กับเด็กเกเรตามท้องถนนที่ชอบวาด พ่นสีให้เลอะเทอะอันธพาลดังกล่าวจะทำเช่นเดียวกันคือเข้าไปในเครือข่ายคอมพิวเตอร์ แล้วทำลายข้อมูลหรือตัดต่อดัดแปลงภาพหรือกระทำสิ่งที่ไม่สมควรต่างๆ เพื่อรบกวนผู้อื่น

7. การก่อการร้ายทางอินเทอร์เน็ต (Terrorist) คือ การเผยแพร่ข้อมูลข่มขู่บุคคลหรือองค์กรใดองค์กรหนึ่ง รวมถึงการเจาะระบบ (Hacking)เข้าไปแทรกแซงทำลายระบบเครือข่ายสาธารณูปโภค เช่น การจ่ายน้ำ จ่ายไฟ หรือการจราจร

8. การหลอกลวงในการขายสินค้าและการลงทุนผ่านทางเครือข่ายคอมพิวเตอร์ (Telemaleting Fruad) คือการหลอกลวงค้าขายหรือชวนลงทุนหลอกลวงผ่านเครือข่ายอินเทอร์เน็ต โดยไม่ได้ให้บริการจริง หรือชักชวนให้เข้าร่วมลงทุนแต่ไม่ได้มีกิจกรรมเหล่านั้นจริงๆ หรือโฆษณาหลอกขายสินค้า

9. การเข้าแทรกแซงข้อมูลและนำเอาข้อมูลเหล่านั้นมาเป็นประโยชน์ต่อตนโดยมิชอบ เช่น การที่สามารถผ่านอินเทอร์เน็ตเข้าไปแล้วเข้าไปเจาะล้วงเอาความลับเกี่ยวกับรหัสหมายเลขของบัตรเครดิต เพื่อนำมาเป็นประโยชน์ในการก่ออาชญากรรมต่อไป หรือแม้กระทั่งการล้วงความลับทางการค้าซึ่งสามารถทำได้โดยผ่านทางอินเทอร์เน็ตซึ่งอาจเป็นลักษณะของการดักฟังข้อมูลเพื่อที่จะนำมาเป็นประโยชน์กับกิจการของตนเอง

10. การโอนเงินโดยไม่มีสิทธิโดยชอบด้วยกฎหมาย เมื่อสามารถเข้าไปในเครือข่ายคอมพิวเตอร์ของธนาคารได้แล้วจะใช้เทคโนโลยีทางคอมพิวเตอร์ไปเปลี่ยนแปลงดัดแปลงข้อมูล และโอนทรัพย์สินหรือเงินจากบัญชีหนึ่งเข้าไปอีกบัญชีหนึ่งได้โดยที่ไม่ได้มีการเปลี่ยนถ่ายทรัพย์สินกันจริง แต่ผลคือสามารถได้ทรัพย์สินนั้นมาด้วยการผ่านทางคอมพิวเตอร์

2.2.3 ความเสียหายที่เกิดจากการกระทำความผิดบนอินเทอร์เน็ต

ความเสียหายที่เกิดจากการกระทำความผิดบนอินเทอร์เน็ต มีทั้งส่วนที่ประเมินความเสียหายเป็นเงินได้ เช่น ความเสียหายที่ประเมินค่าจากจำนวนเงินที่ถูกหลอกลวงไป ค่าติดตั้งระบบรักษาความปลอดภัย ค่าจ้างผู้ซ่อมแซมระบบ ค่าใช้จ่ายในการกู้ระบบ เป็นต้น และความเสียหายที่ไม่อาจประเมินความเสียหายเป็นเงินได้ เช่น เวลาที่ต้องใช้ในการลงโปรแกรมคอมพิวเตอร์ใหม่ ความเสียหายต่อสังคมและศีลธรรมอันดี ความเสียหายต่อสังคม การเมือง และเศรษฐกิจ เป็นต้น

รายงานความเสียหายในประเทศสหรัฐอเมริกา[33]

ความเสียหายจากการกระทำความผิดบนอินเทอร์เน็ตในประเทศสหรัฐอเมริกาสามารถตรวจสอบได้จากรายงานของ Internet Crime Complaint Center (IC3) โดยในปี พ.ศ.2549 ศูนย์แห่งนี้ได้รับเรื่องร้องเรียนเกี่ยวกับการกระทำผิดบนอินเทอร์เน็ต 207,492 รายการ โดยการร้องเรียนส่วนใหญ่เป็นการฉ้อโกงหลากหลายประเภท ยกตัวอย่างเช่น การฉ้อโกงการประมูล(Internet auction fraud) การไม่ส่งมอบสินค้า การฉ้อโกงบัตรสินเชื่อและบัตรเงินฝาก เช่นเดียวกับการร้องเรียนเรื่องอื่นที่ไม่ใช่การฉ้อโกง อย่างเช่นการบุกรุกระบบคอมพิวเตอร์ การส่งอีเมล์มาถึงโดยผู้รับไม่ต้องการ(Spam/Unsolicited email) และภาพลามกอนาจารเด็ก

---

[33] International white collar crimes center and the Federal Bureau of Investigation Internet, Internet crime report , 1 January - December 2006.

ความเสียหายในคดีฉ้อโกงอาจคำนวณได้ตามจำนวนเงินที่สูญเสียไปเนื่องจากการฉ้อโกงเหล่านั้น ซึ่งมีมูลค่าทั้งสิ้น 198.44 ล้านดอลลาร์ ซึ่งคิดเป็นค่าเฉลี่ยได้เท่ากับ 723.00 ดอลลาร์ต่อหนึ่งกรณีร้องเรียน ซึ่งอาจจำแนกได้ ดังนี้

การฉ้อโกงการประมูลทางอินเทอร์เน็ต (Internet auction fraud) มีการรายงานมากที่สุด คิดเป็นเป็น 44.9 เปอร์เซ็นต์ของการร้องเรียนทั้งหมด, การไม่ส่งมอบของ และ/หรือ การไม่ชำระเงิน คิดเป็น 19 เปอร์เซ็นต์ของการร้องเรียนทั้งหมด, การฉ้อโกงเช็คคิดได้เป็น 4.9 เปอร์เซ็นต์ของการร้องเรียนทั้งหมด นอกจากนี้ยังมีการรายงานเกี่ยวกับการฉ้อโกงบัตรเครดิต/เดบิต การฉ้อโกงข้อมูลคอมพิวเตอร์ การฉ้อโกงข้อมูลลับ และการฉ้อโกงสถาบันการเงิน

การจัดอันดับตามมูลค่าเสียหายอันดับแรกได้แก่ การหลอกลวงทางอีเมล์ประเภท Nigerian Letter มูลค่า 5,100 ดอลลาร์ การฉ้อโกงเช็ค มูลค่า 3,744 ดอลลาร์และการฉ้อโกงการลงทุนอื่นๆ มูลค่า 2,695 ดอลลาร์

ตามรายงานฉบับนี้ผู้กระทำความผิด 75.2 เปอร์เซ็นต์เป็นผู้ชาย และครึ่งหนึ่งอาศัยอยู่ในรัฐCalifornia, New York, Florida, Texas, Pennsylvaniaและ Tennessee นอกจากนี้ยังมีรายงานจำนวนมากที่แสดงว่าผู้กระทำผิดอาศัยอยู่นอกสหรัฐ เช่น Canada, India,Germany เป็นต้น และผู้เสียหายส่วนใหญ่เป็นชาย(ในอัตราส่วนคิดเป็น 1.69ดอลลาร์ ต่อทุกๆ 1 ดอลลาร์ที่ผู้หญิงเสีย)

จดหมายอิเล็กทรอนิกส์ (E-mail) ถือเป็นช่องทางหลักในการกระทำความผิด (คิดเป็น 73.9 เปอร์เซ็นต์) และอีกส่วนหนึ่งกระทำผิดผ่านทางเว็บเพจ (36.0%)

นอกจากนี้ ยังมีการกระทำผิดอื่นๆอีกเช่น การหลอกลวงเกี่ยวกับมือปืนรับจ้าง (Hit man scams) การทำ Phishing และการหลอกลวงด้วยการใช้เช็คที่มีการปลอมแปลง

รายงานความเสียหายในประเทศญี่ปุ่น[34]

หนังสือพิมพ์ Japan Times ได้นำเสนอรายงานการกระทำความผิดบนอินเทอร์เน็ตที่บันทึกโดยสำนักงานตำรวจแห่งชาติ โดยในครึ่งปีแรก มี 1,802 คดี เพิ่มขึ้น 11.8 เปอร์เซ็นต์จากปีที่แล้ว

การกระทำผิดฐานการเข้าถึงคอมพิวเตอร์โดยมิชอบ (Illegal access) เพิ่มขึ้นอย่างรวดเร็ว เป็น 265 ราย เพิ่มขึ้น 33.8 เปอร์เซ็นต์ จากสถิติที่สำนักงานตำรวจแห่งชาติเริ่มรวบรวมข้อมูลในปี 2000

นอกจากนี้ยังมีการรายงานการกระทำผิดอื่น เช่น การฉ้อโกงบนอินเทอร์เน็ต(Fraud abusing computer networks) มีสถิติสูงสุดคือ733 โดยคดีที่พบส่วนใหญ่คือคดีเกี่ยวกับการประมูลทางอินเทอร์เน็ต, การค้าประเวณีของผู้เยาว์ที่อายุต่ำกว่า 18 ปี (Prostitution involving minors under 18) ซึ่งแพร่หลายในเว็บไซต์หาคู่นัด (Dating Web sites) มี 169 คดี ,การละเมิดกฎหมายเครื่องหมายการค้า เช่น การลวงขายสินค้าที่ใช้เครื่องหมายการค้าปลอมในการประมูลทางอินเทอร์เน็ต มี 106 คดี ,การฉ้อโกงทางอินเทอร์เน็ต โดยการโจมตีแบบ Phishing มีทั้งหมด 102 คดี

รายงานความเสียหายในประเทศไทย

ตามรายงานที่ได้นำเสนอในการประชุมคณะกรรมาธิการ[35] ได้ชี้แจงเกี่ยวกับการกระทำความผิดบนอินเทอร์เน็ตในประเทศไทย ซึ่งมีหลากหลายรูปแบบ เช่น การขโมยโดเมนเนม Sanook.com Thailand.com Narak.com, การจดโดเมนเนมชื่อคล้ายบริษัทที่มีชื่อเสียง แล้วขู่บังคับให้ซื้อโดเมนเนมนั้น มิฉะนั้นจะเปลี่ยนเว็บโป๊ ให้บริษัทนั้นเสียชื่อ, การแอบเปลี่ยนชื่อ ที่อยู่ผู้รับเงินโฆษณา แบนเนอร์, การแอบใช้ Internet Account , พนักงาน แอบใช้โปรแกรมขโมย Password ของผู้บริหารและพนักงานในองค์กร, พนักงานใช้ E-mail ขององค์กร ไปในทางเสียชื่อเสียง, การลักลอบใช้สัญญาณ Wireless internet, การส่งไวรัส, การส่งSpam,การแอบเข้ามานำฐานข้อมูลไปเข้ารหัส เพื่อเรียกค่าไถ่ (Ransom) , การแฮกส์เพื่อดู ลบ แก้ไข หรือทำลายข้อมูล , การดักข้อมูลในเครือข่าย, การกระทำผิดรูปแบบของDenial of service(DOS) เป็นต้น

---

[34] Japan Times (18 August 2006)

[35] ญาณพล ยั่งยืน, เอกสารนำเสนอในการประชุมคณะกรรมาธิการวิสามัญ ประกอบการพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 29 พฤศจิกายน 2549 (เอกสารไม่ตีพิมพ์เผยแพร่)

2.3 แนวคิดและหลักการที่เกี่ยวข้องกับการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ต

การควบคุมกิจกรรมทุกประเภทบนอินเทอร์เน็ตเป็นสิ่งที่ทำได้ยาก ด้วยเหตุที่อินเทอร์เน็ตเป็นเครือข่ายสาธารณะ ไม่มีผู้ใดเป็นเจ้าของแต่เพียงผู้เดียวเพราะความเป็นเจ้าของกระจายไปยังพื้นที่ต่างๆที่มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ต จึงเป็นพื้นที่ที่เปิดโอกาสให้มีการกระทำความผิดได้ง่ายและมีปัจจัยหลายประการที่ผู้กระทำความผิดรอดพ้นจากการถูกดำเนินคดี

ในปัจจุบันรัฐบาลของแต่ละรัฐต่างมีความจำเป็นที่จะต้องปรับปรุงกฎหมายและแสวงหามาตรการในการควบคุม ป้องกันและปราบปรามการกระทำความผิดบนอินเทอร์เน็ตตามความสามารถและนโยบายของแต่ละรัฐ แต่กฎหมายและมาตรการเหล่านั้นย่อมจะต้องกระทบกระเทือนสิทธิเสรีภาพ ปิดกั้นเสรีภาพในการแสดงความคิดเห็นของประชาชนและกระทบสิทธิเสรีภาพด้านอื่นอีกหลายประการ

จึงต้องพิจารณาถึงความเหมาะสมในใช้กฎหมายและการนำมาตรการใดๆมาใช้ว่าอาจกระทบต่อสิทธิเสรีภาพของประชาชนมากน้อยเพียงใด ในขณะเดียวกันก็ต้องตระหนักว่ากฎหมายและมาตรการเหล่านั้นต้องให้อำนาจแก่เจ้าหน้าที่ของรัฐมากพอสมควรด้วย เพราะการกระทำความผิดบนอินเทอร์เน็ตมีลักษณะที่ซับซ้อน การดำเนินคดีทำได้ยาก หากเจ้าหน้าที่ของรัฐไม่มีอำนาจอย่างเพียงพอแล้วก็ไม่สามารถดำเนินคดีได้อย่างรวดเร็วและมีประสิทธิภาพ

ในหัวข้อ 2.3 นี้จึงเป็นการศึกษาเกี่ยวกับการใช้อำนาจของรัฐในการตรากฎหมาย การใช้มาตรการในการรักษาความสงบเรียบร้อยของสังคมเพื่อให้รัฐและเจ้าหน้าที่รัฐใช้อำนาจได้โดยชอบธรรม รวดเร็วและมีประสิทธิภาพ และในขณะเดียวกันก็ต้องไม่ลิดรอนสิทธิและเสรีภาพของประชาชนเกินสมควร

หลักประกันสิทธิและเสรีภาพของประชาชน

แนวคิดในการบังคับใช้กฎหมายโดยเคารพหลักสิทธิและเสรีภาพ เป็นแนวคิดของนักคิดนักปราชญ์ชาวตะวันตก ซึ่งตรงกันข้ามกับแนวคิดของชาติตะวันออกที่มองว่ากฎหมายเป็นเครื่องมือในการกำหนดหน้าที่ของบุคคลเพื่อการอยู่ร่วมกันในสังคม กฎหมายของชาติตะวันออกในยุคโบราณจึงไม่ได้มีแนวคิดเรื่องสิทธิและเสรีภาพดังเช่นในปัจจุบัน

สำหรับประเทศไทย ในช่วงก่อนที่จะมีการใช้กฎหมายตราสามดวง กฎหมายต่างๆของประเทศไทยในสมัยนั้นก็ไม่มีแนวคิดในเรื่องสิทธิและเสรีภาพเช่นเดียวกัน กฎหมายในสมัยนั้นจึงเป็นการกำหนดหน้าที่และบทลงโทษเท่านั้น แต่เมื่อมีการใช้กฎหมายตราสามดวงแล้ว พบว่ารัฐได้ให้การปกป้องคุ้มครองสิทธิขั้นต่ำแก่ประชาชน เช่น กฎหมายกำหนดว่าภายในเขตแดนประเทศไทยหาได้มีใครอยู่เหนือกฎหมายไม่ การมีกฎหมายป้องกันการกล่าวโทษผู้อื่นโดยไม่เป็นธรรม เป็นต้น แม้กฎหมายในยุคนั้นจะไม่มีแนวคิดเรื่องสิทธิและเสรีภาพดังเช่นในปัจจุบัน แต่ก็เป็นการเหมาะสมกับยุคสมัยและรูปแบบการปกครองในสมัยนั้นแล้ว เพราะเป็นการบัญญัติกฎหมายเพื่อป้องกันการใช้อำนาจอย่างไร้ทำนองคลองธรรม[36] เมื่อประเทศไทยประสบปัญหาเกี่ยวกับสิทธิเสรีภาพนอกอาณาเขตและการรุกรานจากประเทศมหาอำนาจ จึงจำเป็นต้องปรับปรุงกฎหมายที่รองรับสิทธิบางประการของประชาชนของประเทศ ประเทศไทยจึงได้เริ่มใช้กฎหมายวิธีพิจารณาความแบบใหม่ ในสมัย ร.ศ.115 ซึ่งถือเป็นจุดเริ่มต้นของการใช้กฎหมายที่คำนึงถึงสิทธิผู้ต้องหาตามกฎหมายสมัยใหม่[37]

ต่อมา ประเทศไทยได้รับแนวคิดเกี่ยวกับรัฐธรรมนูญเช่นเดียวกับอารยประเทศ โดยรัฐธรรมนูญอย่างเป็นทางการฉบับแรก คือ พระราชบัญญัติธรรมนูญการปกครองแผ่นดินสยาม ชั่วคราวพุทธศักราช 2475 ไม่ได้มีบทบัญญัติที่รับรองสิทธิเสรีภาพของประชาชนแต่อย่างใด มีเพียงบทบัญญัติที่ให้ประชาชนมีสิทธิเลือกตั้งเท่านั้น เนื่องจากประเทศไทยถูกปกครองโดยระบอบสมบูรณาญาสิทธิราชมาโดยตลอด จึงไม่มีความรู้ความเข้าใจในเรื่องสิทธิเสรีภาพ จนกระทั่งมีการใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2492 ซึ่งเป็นรัฐธรรมนูญฉบับแรกที่มีการรองรับแนวคิดเรื่องสิทธิและเสรีภาพไว้ และแนวความคิดเหล่านี้ก็สืบต่อมาในรัฐธรรมนูญที่ได้บัญญัติไว้ภายหลัง

รัฐธรรมนูญถือว่าเป็นหัวใจสำคัญในการให้หลักประกันสิทธิเสรีภาพของประชาชน รัฐธรรมนูญแห่งราชอาญาจักรไทย พ.ศ.2540 ได้รับการยอมรับยอมโดยทั่วไปว่าเป็นรัฐธรรมนูญที่วางบทบัญญัติเกี่ยวกับสิทธิและเสรีภาพของประชาชนไว้เป็นอย่างดี[38] แต่อย่างไรก็ดีในขณะจัดทำ

---

[36] เกียรติขจร วัจนะสวัสดิ์ และคณะ, สิทธิมนุษยชนและกระบวนการยุติธรรม ทางอาญาในประเทศไทย,(กรุงเทพฯ: สถาบันไทยคดีศึกษา มหาวิทยาลัยธรรมศาสตร์และมูลนิธิโครงการตำรา สมาคมสังคมศาสตร์และมนุษยศาสตร์, 2529), หน้า 22-38.

[37] เรื่องเดียวกัน, หน้า 38-39.

[38] บรรเจิด สิงคเนติ, หลักพื้นฐานของสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ (กรุงเทพฯ : วิญญูชน, 2547), หน้า 169.

วิทยานิพนธ์ฉบับนี้ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540 ได้ถูกประกาศยกเลิกแล้ว ในวันที่ 19 กันยายน พ.ศ. 2549[39] และได้ประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2549 เมื่อวันที่ 1 ตุลาคม 2549 แต่รัฐธรรมนูญฉบับชั่วคราวนี้ ก็ไม่ได้กำหนดรับรองสิทธิเสรีภาพของประชาชนไว้โดยชัดแจ้ง มีเพียงบทบัญญัติในมาตรา 3[40] ที่พออนุมานได้ว่ายังมีการรองรับแนวคิดในเรื่องนี้ไว้ และต่อมาเมื่อได้มีการประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550 แนวคิดในเรื่องการรับรองหลักประกันสิทธิเสรีภาพก็ถูกบรรจุไว้ในรัฐธรรมนูญฉบับนี้

แนวคิดเกี่ยวกับสิทธิและเสรีภาพ

สิทธิเสรีภาพ เป็นคำที่มีความหมายกว้างและมีเนื้อหาใกล้เคียงกัน โดยมีจากแนวคิดในทางปรัชญา ของนักคิด นักปราชญ์ที่มีมาตั้งแต่สมัยโรมัน ซึ่งพอจะอธิบายความหมายของสิทธิและเสรีภาพแยกกันได้ ดังนี้

สิทธิ หมายถึง อำนาจที่กฎหมายรับรองให้แก่บุคคลในอันที่จะกระทำการเกี่ยวข้องกับทรัพย์หรือบุคคลอื่น และคุ้มครองบุคคลในอันที่จะเรียกร้องให้บุคคลอื่นกระทำการอย่างใดอย่างหนึ่ง ให้เกิดประโยชน์แก่ตน[41]

เสรีภาพ หมายถึง อำนาจในการตัดสินใจของบุคคล โดยสามารถเลือกได้ว่าจะกระทำการหรือไม่กระทำการใดๆตามความสมัครใจ ตราบเท่าที่จะไม่ถูกบังคับให้กระทำการหรือไม่กระทำการใดๆที่ขัดกับความประสงค์ของตน[42]

---

[39] ประกาศคณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ฉบับที่ 3

[40] มาตรา 3 "ภายใต้บังคับบทบัญญัติแห่งรัฐธรรมนูญนี้ ศักดิ์ศรีความเป็นมนุษย์ สิทธิเสรีภาพ และความเสมอภาค บรรดาที่ชนชาวไทยเคยได้รับความคุ้มครองตามประเพณีการปกครองประเทศไทยในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และตามพันธกรณีแห่งประเทศ ที่ประเทศไทยมีอยู่แล้ว ย่อมได้รับการคุ้มครองตามรัฐธรรมนูญนี้"

[41] วรพจน์ วิศรุตพิชญ์, สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 (กรุงเทพฯ: วิญญูชน, 2543)หน้า 21.

[42] เกรียงไกร เจริญธนาวัฒน์, หลักกฎหมายว่าด้วยสิทธิและเสรีภาพ(กรุงเทพฯ: วิญญูชน, 2547)หน้า 24.

การจำแนกสิทธิเสรีภาพ อาจแยกออกได้ 5 ประเภทดังนี้[43]

1) ความมั่นคงในชีวิตร่างกายหรือเสรีภาพในชีวิตร่างกาย สิทธิเหล่านี้ได้แก่ เสรีภาพกรรมสิทธิ์ ความมั่นคงปลอดภัยและการต่อต้านการกดขี่ข่มเหง เสรีภาพดังกล่าวเป็นเสรีภาพขั้นพื้นฐานที่สำคัญที่สุดที่ช่วยให้มนุษย์รวมกลุ่มกันเป็นสังคมได้

2) เสรีภาพในชีวิตส่วนตัว ได้แก่เสรีภาพในเคหสถาน เสรีภาพในการติดต่อสื่อสาร เสรีภาพในความลับส่วนบุคคล เสรีภาพในข้อมูลส่วนบุคคล เสรีภาพประเภทนี้เป็นสิทธิเสรีภาพที่ให้ความสำคัญกับสิทธิเสรีภาพของแต่ละบุคคล เพราะบุคคลแต่ละคนมีสิทธิที่จะรักษาเรื่องส่วนตัวของตนมิให้คนอื่นล่วงรู้

3) เสรีภาพในตัวบุคคล คือ เสรีภาพที่จะกระทำการใดๆได้ตามความประสงค์ของตน บุคคลอื่นจะขัดขวางการกระทำใดๆอันเกี่ยวกับเนื้อตัวร่างกายโดยชอบด้วยกฎหมายของบุคคลนั้นไม่ได้ เช่นเสรีภาพในการเดินทาง

4) เสรีภาพทางปัญญาและศีลธรรม จะให้ความสำคัญกับความคิด ความเชื่อ และการแสดงออกของมนุษย์ได้อย่างเสรี เช่นเสรีภาพในการแสดงออก เสรีภาพในการแสดงความคิดเห็น เสรีภาพเกี่ยวกับความเชื่อและการนับถือศาสนา เสรีภาพในทางวิชาการ เสรีภาพในการรวมตัวเป็นกลุ่มชุมนุมหรือประท้วง เป็นต้น

5) เสรีภาพด้านเศรษฐกิจสังคม เสรีภาพประเภทนี้จะเกี่ยวข้องกับการประกอบอาชีพ เช่น เสรีภาพในกรรมสิทธิ์ เสรีภาพในการทำงาน เป็นต้น

ดังที่ได้กล่าวมาแล้วข้างต้น จะเห็นได้ว่าสิทธิเสรีภาพเป็นเรื่องของการให้อำนาจตัดสินใจแก่บุคคลในการกระทำการใดได้อย่างอิสระ ซึ่งอาจเกิดปัญหาต่อสังคมโดยรวมได้หากมีการใช้อำนาจนั้นอย่างไร้ขอบเขต จึงมีความจำเป็นที่รัฐจะต้องจำกัดสิทธิเสรีภาพนั้นโดยวิธีการบัญญัติกฎหมายออกมาเพื่อจำกัดสิทธิเสรีภาพนั้นหรือใช้อำนาจรัฐในการจำกัดสิทธิเสรีภาพเพื่อคุ้มครองประชาชนในสังคมหรือจัดระเบียบการใช้สิทธิเสรีภาพเพื่อประโยชน์ต่อสังคมโดยรวม

---

[43] เรื่องเดียวกัน, หน้า 26.

สิทธิเสรีภาพในการแสดงความคิดเห็น

ในการบัญญัติกฎหมายเพื่อควบคุมการกระทำความผิดบนอินเทอร์เน็ต มีความจำเป็นที่จะต้องพิจารณาการกระทบกระเทือนสิทธิเสรีภาพในการแสดงความคิดเห็นเป็นประเด็นสำคัญ จึงมีความจำเป็นที่จะต้องศึกษาสิทธิเสรีภาพประเภทนี้เป็นการเฉพาะ โดยสิทธิเสรีภาพในการแสดงความคิดเห็นนี้ได้ถูกกำหนดในเอกสารด้านสิทธิมนุษยชนฉบับแรก คือ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน พ.ศ. 2491 (Universal Declaration of Human Rights หรือ UDHR) ซึ่งเป็นการการประกาศเจตนารมณ์ความร่วมมือระหว่างประเทศที่มีความสำคัญในการวางกรอบเบื้องต้นเกี่ยวกับสิทธิมนุษยชน โดยได้กล่าวถึง สิทธิเสรีภาพในการแสดงความเห็นไว้ในปฏิญญาสากลฉบับนี้[44] และแนวคิดนี้ยังได้ปรากฏในเอกสารความร่วมมือระหว่างประเทศอีกหลายฉบับ[45]

ในปัจจุบัน ประเทศไทยยอมรับแนวคิดเกี่ยวกับรัฐธรรมนูญ การรับรองสิทธิเสรีภาพในการแสดงความคิดเห็นจึงถูกบัญญัติไว้ในรัฐธรรมนูญด้วย เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 39[46] รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2549 มาตรา 3[47]

เมื่อได้มีการประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 แนวคิดนี้ก็ได้รับการรับรองคุ้มครองโดยบัญญัติไว้ในมาตรา 45 ดังนี้ "บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น

---

[44] เช่น มาตรา12 "การเข้าไปแทรกสอดโดยพลการในกิจส่วนตัว ครอบครัว เคหะสถาน การส่งข่าวสาร..." , มาตรา 18 "บุคคลมีสิทธิในเสรีภาพแห่งความคิด มโนธรรม และศาสนา..." , มาตรา 19 "บุคคลมีสิทธิในเสรีภาพแห่งความเห็นและการแสดงออก สิทธินี้รวมถึงเสรีภาพที่จะยึดมั่นในความเห็นโดยปราศจากการแทรกสอดและที่จะแสวงหารับ ตลอดจนแจ้งข่าว รวมทั้งความคิดเห็นโดยผ่านสื่อใดๆ และโดยมิต้องคำนึงถึงเขตแดน"

[45] เช่น International Covenant on Civil and Political Rights –ICCPR ที่ประเทศไทยเข้าเป็นภาคีเมื่อปี พ.ศ.2539 โดยได้กำหนดรองรับสิทธิประเภทนี้ไว้ใน ข้อ 19 "1.บุคคลทุกคนมีสิทธิที่จะมีความคิดเห็นโดยปราศจากการแทรกแซง 2. บุคคลทุกคนมีสิทธิในเสรีภาพแห่งการแสดงออก ...."

[46] มาตรา 39"บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น..."

[47] มาตรา 3 "ภายใต้บังคับบทบัญญัติแห่งรัฐธรรมนูญนี้ ศักดิ์ศรีความเป็นมนุษย์ สิทธิเสรีภาพ และความเสมอภาค บรรดาที่ชนชาวไทยเคยได้รับความคุ้มครองตามประเพณีการปกครองประเทศไทยในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และตามพันธกรณีแห่งประเทศ ที่ประเทศไทยมีอยู่แล้ว ย่อมได้รับการคุ้มครองตามรัฐธรรมนูญนี้"

การจำกัดเสรีภาพตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิ เสรีภาพ เกียรติยศ ชื่อเสียง สิทธิในครอบครัวหรือความเป็นอยู่ส่วนตัวของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกันหรือระงับความเสื่อมทรามทางจิตใจหรือสุขภาพของประชาชน

การสั่งปิดกิจการหนังสือพิมพ์หรือสื่อมวลชนอื่นเพื่อลิดรอนเสรีภาพตามมาตรานี้จะกระทำมิได้

การห้ามหนังสือพิมพ์หรือสื่อมวลชนอื่นเสนอข่าวสารหรือแสดงความคิดเห็นทั้งหมดหรือบางส่วน หรือการแทรกแซงด้วยวิธีการใด ๆ เพื่อลิดรอนเสรีภาพตามมาตรานี้ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง

การให้นำข่าวหรือบทความไปให้เจ้าหน้าที่ตรวจก่อนนำไปโฆษณาในหนังสือพิมพ์หรือสื่อมวลชนอื่น จะกระทำมิได้ เว้นแต่จะกระทำในระหว่างเวลาที่ประเทศอยู่ในภาวะสงคราม แต่ทั้งนี้จะต้องกระทำโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งได้ตราขึ้นตามวรรคสอง..."

เหตุผลในการจำกัดสิทธิและเสรีภาพ

การจำกัดสิทธิและเสรีภาพสามารถกระทำได้โดยพิจารณาจากความมุ่งหมายได้ 3 ประการดังนี้[48]

1. เพื่อคุ้มครองสิทธิของบุคคลอื่น เป็นกรณีที่รัฐเข้ามาควบคุมการใช้สิทธิเสรีภาพขัดกันของผู้คนในสังคม โดยมาจากแนวความคิดที่ว่ามนุษย์ทุกคนมีความเสมอภาคเท่าเทียมกัน มนุษย์ทุกคนจึงต้องเคารพสิทธิของบุคคลอื่น

2. เพื่อการดำรงอยู่และเพื่อความสามารถในการทำภาระหน้าที่ของรัฐ

2.1 การดำรงอยู่ของรัฐ ความมั่นคงของรัฐมีความสำคัญต่อปลอดภัยของคนในชาติ ดังนั้นรัฐจึงมีอำนาจโดยชอบที่จะจำกัดสิทธิเสรีภาพของบุคคลได้ โดยหลักแล้วการจำกัดสิทธิเสรีภาพในลักษณะนี้จะเป็นการป้องกันรัฐจากการรุกรานนอกประเทศ เช่นการกำหนดให้

---

[48] บรรเจิด สิงคเนติ, หลักพื้นฐานของสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ ตามรัฐธรรมนูญ, หน้า 147

ประชาชนมีหน้าที่ป้องกันการรุกรานจากรัฐต่างประเทศประชาชนจึงมีหน้าที่ป้องกันประเทศโดยต้องเข้ารับราชการทหาร เป็นต้น ส่วนการป้องกันการรบกวนกิจการภายในประเทศ รัฐก็อาจกระทำได้ในกรณีที่มีความรุนแรงจริงๆเพื่อป้องกันการจลาจลภายในรัฐเท่านั้น[49]

2.2 ความสามารถในการทำภาระหน้าที่ของรัฐ เป็นการจำกัดสิทธิและเสรีภาพในรูปแบบของการกำหนดหน้าที่ให้แก่พลเมืองของตน โดยรัฐจะออกกฎหมายเพื่อกำหนดรายละเอียดของหน้าที่ของพลเมือง

3. เพื่อประโยชน์สาธารณะหรือเพื่อความสงบเรียบร้อยของประชาชน

3.1 ประโยชน์สาธารณะ การดำเนินกิจการของรัฐจะต้องเป็นการตอบสนองคนส่วนใหญ่ มิใช่เพื่อผลประโยชน์ของเอกชนหรือคนกลุ่มหนึ่งกลุ่มใดเท่านั้น

3.2 ความสงบเรียบร้อยของประชาชน กฎหมายของไทยได้ยอมรับหลักการเกี่ยวกับความสงบเรียบร้อยของประชาชนไว้ในกฎหมายโดยทั่วไป เช่นดังที่บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ แต่ยากที่จะหาคำจำกัดความของคำว่า "ความสงบเรียบร้อยของประชาชน" อย่างไรก็ดีมีผู้ให้ความหมายของคำดังกล่าวว่า หมายถึง ประโยชน์โดยทั่วไปของประเทศชาติและสังคม[50]

การจำกัดเสรีภาพนั้นรัฐจะไม่จำกัดโดยเด็ดขาดเสียทีเดียว แต่จะจำกัดตามความเหมาะสมของสภาพสังคม (Relative) เช่น การห้ามชุมนุมในที่สาธารณะในสภาวะสงคราม แต่สิทธิเสรีภาพบางประเภทรัฐไม่สามารถตรากฎหมายมาจำกัดได้เลย (Absolute) เช่น เสรีภาพในการนับถือศาสนา เสรีภาพทางด้านมโนธรรมและความคิด เป็นต้น[51]

---

[49] เรื่องเดียวกัน, หน้า 150

[50] อุกฤษ มงคลนาวิน, "ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน", บทบัณฑิตย์ ล. 32, ต.1 พ.ศ.2518, หน้า 13.

[51] เกรียงไกร เจริญธนาวัฒน์, หลักกฎหมายว่าด้วยสิทธิและเสรีภาพ, หน้า 33.

สิทธิมนุษยชนในกระบวนยุติธรรมทางอาญา

นอกจากจะต้องพิจารณาเกี่ยวกับการจำกัดสิทธิเสรีภาพตามรัฐธรรมนูญดังที่ได้กล่าวมาแล้ว รัฐยังต้องพิจารณาถึงความเหมาะสมในการนำมาตรการใดๆมาใช้ เพราะมาตรการเหล่านั้นย่อมกระทบต่อประชาชนทั่วไปทั้งตัวผู้กระทำความผิดและผู้ที่ไม่มีส่วนเกี่ยวข้องกับการกระทำความผิด ดังนั้น กระบวนยุติธรรมทางอาญาในทุกขั้นตอนไม่ว่าจะเป็นการสืบสวน สอบสวน การค้นตัวบุคคลหรือสิ่งของ การค้นในที่สาธารณะหรือในเคหสถาน การจับกุม การระงับการก่อภัย การป้องกันภัย การฟ้องร้อง การดำเนินคดี การพิจารณาพิพากษา การบังคับโทษให้เป็นไปตามคำพิพากษา รวมถึงการนิรโทษกรรม รัฐจะต้องอำนวยให้แก่สังคมรัฐอย่างเหมาะสมและพอดี เพราะอาจเป็นการกระทบสิทธิของประชาชนเกินสมควร ซึ่งหลักการนี้ประเทศสหรัฐอเมริกาเรียกว่าหลักการ Due process of Law[52] จึงจำเป็นต้องพิจารณาความเหมาะสมในการดำเนินคดีอาญากับผู้กระทำความผิดในแต่ละขั้นตอนว่ากระทบต่อสิทธิมนุษยชนอย่างไรบ้าง เช่น

1.สิทธิที่จะไม่ถูกตรวจกักหรือดักการสื่อสาร การควบคุมหรือสอดส่องการสื่อสารของประชาชนอาจช่วยให้รัฐทราบถึงความเคลื่อนไหวของอาชญากรรมได้ แต่การควบคุมหรือสอดส่องการสื่อสารนั้น หากไม่มีหลักเกณฑ์ที่เป็นธรรมหรือเจ้าหน้าที่ใช้อำนาจตามอำเภอใจอาจกระทบต่อสิทธิความเป็นส่วนตัว (right to privacy) ของประชาชนทั่วไป ดังนั้น ในการจำกัดสิทธิดังกล่าวรัฐจะพิจารณาจากประเด็นสำคัญ 2 กรณีต่อไปนี้ ได้แก่

1.ข้อห้ามในการดักหรือเข้าล่วงรู้ข้อความในการสื่อสารโดยทั่วไป โดยหลักแล้วจะต้องคำนึงถึงความเหมาะสมว่ามีความจำเป็นมากน้อยเพียงใดในการตรวจ กักหรือดักข่าวสาร เช่น มีเหตุอันควรเชื่อว่าผู้นั้นเป็นผู้กระทำความผิด หรือเกี่ยวข้องกับการกระทำความผิด และมีความจำเป็นที่จะต้องอาศัยข้อเท็จจริงจากการสนทนาของผู้นั้น จึงจะใช้วิธีการดักฟังการสนทนาได้ โดยจะต้องใช้ดุลพินิจในการอนุญาตให้ใช้วิธีการดังกล่าวเป็นกรณีไป

---

[52] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา, พิมพ์ครั้งที่5 (กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2549), หน้า 9.

2.ข้อห้ามเป็นพิเศษกรณีเป็นการปรึกษาหารือระหว่างผู้ถูกกล่าวหาในคดีอาญากับทนายความของผู้นั้น ในกรณีนี้กฎหมายจะให้ความคุ้มครองเป็นพิเศษมากกว่ากรณีแรก เพื่อป้องกันการแทรกแซงของรัฐต่อสิทธิมนุษยชนของผู้ถูกกล่าวหากับทนายความ[53]

2.สิทธิที่จะไม่ถูกตรวจค้นในสถานที่ส่วนบุคคล ตรวจค้นยานพาหนะ ตรวจค้นตัวหรือแสวงหาพยานหลักฐานจากเนื้อตัวร่างกายโดยมิชอบ การค้นไม่ว่าจะเป็นการค้นในสถานที่ส่วนบุคคล การค้นยานพาหนะ การค้นตัวบุคคลหรือการแสวงหาพยานหลักฐานจากเนื้อตัวร่างกายย่อมกระทบต่อสิทธิส่วนตัว ชีวิตครอบครัวและเคหสถาน ซึ่งอารยประเทศต่างให้การรับรอง[54] ซึ่งอาจจำแนกออกได้เป็น 3 กรณีได้แก่

1. การตรวจค้นสถานที่ส่วนบุคคล โดยหลักแล้วการเข้าตรวจค้นในสถานที่ส่วนบุคคลจะต้องมีหมายค้นหรือคำสั่งที่ออกโดยชอบและจะต้องมีเหตุผลที่มีน้ำหนักพอที่จะออกหมายค้นหรือคำสั่งได้ การค้นโดยไม่มีหมายค้นหรือคำสั่งจะกระทำได้ก็ต่อเมื่อเป็นกรณีที่กฎหมายกำหนดไว้ชัดแจ้งให้กระทำได้เฉพาะกรณีที่จำกัด เช่นกรณีฉุกเฉินและมีความจำเป็นอย่างยิ่งในการรักษาความสงบเรียบร้อยของสังคม และไม่ว่ากรณีใดๆการค้นจะต้องกระทำในขอบเขตที่เหมาะสม โดยทั่วไปแล้วหลายๆประเทศมีหลักการที่คล้ายคลึงกัน เช่น กฎหมายอังกฤษ อเมริกา เยอรมัน

2. การตรวจค้นยานพาหนะและตัวบุคคล ตามหลักกฎหมายอังกฤษได้กำหนดว่าเจ้าหน้าที่ตำรวจจะใช้อำนาจเรียกให้หยุดและตรวจค้นได้จะต้องมีเหตุผลตามสมควรที่ทำให้สงสัยว่าจะพบหลักฐานเกี่ยวกับความผิดหรือจะพบสิ่งของที่ได้จากการกระทำผิดหรือสิ่งผิดกฎหมายจากตัวบุคคลหรือภายในยานพาหนะนั้น สำหรับในประเทศไทยการค้นยานพาหนะส่วนบุคคลจำเป็นต้องพิจารณาว่ายานพาหนะอยู่ที่ใด หากอยู่ในที่รโหฐานก็จำเป็นต้องใช้หลักเกณฑ์ในเรื่องการค้นในที่รโหฐาน หากยานพาหนะนั้นอยู่ในที่สาธารณะก็อาจใช้หลักเกณฑ์ในการค้นในที่สาธารณะ เป็นต้น

---

[53] เช่น ประมวลกฎหมายวิธีพิจารณาความอาญามาตรา105 วรรค3 แต่อย่างไรก็ดี ตามพระราชบัญญัติข่าวกรองแห่งชาติ พระราชบัญญัติป้องกันและปราบปรามยาเสพติดฉบับแก้ไขเพิ่มเติม และพระราชบัญญัติการสอบสวนคดีพิเศษ มิได้ระบุถึงข้อห้ามนี้อย่างชัดเจน

[54] เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (The universal declaration of human right) ข้อ12, อนุสัญญาของสภายุโรปเพื่อการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (European convention for protection of human right and fundamental freedoms) ข้อ 8 เป็นต้น

3. การแสวงหาพยานหลักฐานจากเนื้อตัวร่างกายของบุคคล การแสวงหาพยานหลักฐานในลักษณะนี้ ในบางประเทศอาจมีปัญหาว่าขัดต่อสิทธิที่จะไม่ให้การเป็นโทษต่อตนเองของผู้ต้องหา(Privilege against self-incrimination)[55] ส่วนกฎหมายไทยได้ยอมรับการค้นในกรณีนี้ ต้องพิจารณาตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 132 ที่ให้อำนาจเจ้าหน้าที่ตรวจตัวผู้ต้องหา พิมพ์ลายนิ้วมือ ลายมือหรือลายเท้าได้

นอกจากสิทธิที่ได้กล่าวมาแล้ว ในการดำเนินคดีอาญารัฐยังต้องพิจารณาถึงสิทธิมนุษยชนในกระบวนยุติธรรมทางอาญา ด้านอื่นๆอีกด้วย เช่น สิทธิที่จะได้รับการสันนิษฐานไว้ก่อนว่าเป็นผู้บริสุทธิ์, สิทธิที่จะได้รับการแจ้งข้อกล่าวหา, สิทธิที่จะไม่ถูกฟ้องคดีอาญาโดยไม่เป็นธรรม, สิทธิที่จะไม่ถูกนำเอาพยานหลักฐานที่ได้มาโดยมิชอบมาใช้ในการพิสูจน์ความผิด เป็นต้น[56]

ดังที่ได้กล่าวมาแล้วข้างต้นว่ามาตรการที่รัฐจะนำมาใช้ในการควบคุม ป้องกันและปราบปรามการกระทำความผิดบนอินเทอร์เน็ต จะส่งผลกระทบต่อสิทธิเสรีภาพของประชาชนอย่างแน่นอน ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่รัฐจะต้องพิจารณาอย่างรอบคอบ ในการกำหนดมาตรการใดๆหรือการตรากฎหมายเพื่อควบคุมการกระทำความผิดบนอินเทอร์เน็ต โดยการใช้อำนาจรัฐในการกำหนดมาตรการทางกฎหมายต่างๆ ในการจับ การค้น การควบคุมตัวผู้ถูกจับ การสอบสวน การฟ้องคดีต่อศาล การพิจารณาคดีและการพิพากษาคดี จะต้องพยายามที่จะรักษาสมดุล(Balance)ระหว่าง อำนาจรัฐในการนำตัวผู้กระทำความผิดมาลงโทษ และ หลักประกันสิทธิเสรีภาพของประชาชน[57] เป้าหมายสองประการนี้ จะต้องไม่โน้มเอียงไปทางใดทางหนึ่งมากนัก

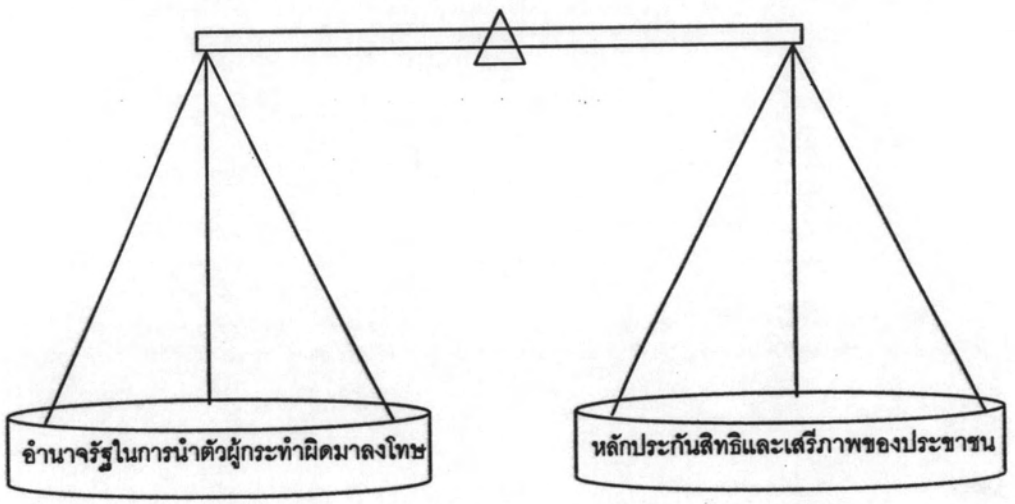
---

[55] ทั้งนี้ มีหลักเกณฑ์แตกต่างกันไปเช่น ศาลสิทธิมนุษยชนของยุโรปเห็นว่าสิทธินี้ไม่ได้ห้ามการให้อำนาจเจ้าพนักงานที่จะแสวงหาข้อมูลนั้นเองรวมถึงข้อมูลที่มาจากเนื้อตัวร่างกายของผู้ต้องหาหากมีกฎหมายบัญญัติอย่างชัดแจ้งเพื่อวัตถุประสงค์ที่จำเป็นในการดำเนินคดีและไม่เป็นการรบกวนสิทธิของบุคคลจนเกินสมควร ในสหรัฐอเมริกาและอังกฤษก็ยอมรับการแสวงหาพยานหลักฐานจากเนื้อตัวร่างกายของบุคคลเช่นเดียวกัน ส่วนกฎหมายเยอรมันการตรวจร่างกายตามหลักวิชาการแพทย์สามารถกระทำได้โดยไม่ต้องได้รับความยินยอมจากผู้ต้องหาแต่ต้องไม่กระทบต่อสุขภาพของผู้ต้องหานั้น และหากเป็นการตรวจดีเอ็นเอจะกระทำได้เฉพาะคดีที่กฎหมายกำหนดไว้

[56] ชาติ ชัยเดชสุริยะ, มาตรการทางกฎหมายในการคุ้มครองสิทธิมนุษยชนในกระบวนการยุติธรรมทางอาญา (กรุงเทพฯ: โรงพิมพ์เดือนตุลา, 2549), หน้า 36-153.

[57] คะนึง ฤาไชย, กฎหมายวิธีพิจารณาความอาญา เล่ม 1 ,พิมพ์ครั้งที่ 6 (กรุงเทพ:โครงการตำราและเอกสารการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2543), หน้า 17.

เพราะหากแต่ต้องคำนึงถึงความคล่องตัวในการนำตัวผู้กระทำความผิดมาลงโทษ ประชาชนก็อาจได้รับความเดือดร้อน เพราะเจ้าหน้าที่รัฐมีอำนาจมากเกินไป ดังนั้น รัฐจึงต้องรักษาสมดุลของการใช้อำนาจรัฐ และหลักประกันสิทธิเสรีภาพของประชาชนให้ได้[58]



รูปที่ 2.3 แสดงการรักษาสมดุล(Balance) ระหว่างอำนาจรัฐในการนำตัวผู้กระทำความผิดมาลงโทษ และหลักประกันสิทธิเสรีภาพของประชาชน

หลักการในการรักษาสมดุลระหว่าง อำนาจรัฐในการนำตัวผู้กระทำความผิดมาลงโทษ และ หลักประกันสิทธิเสรีภาพของประชาชน ได้ถูกหยิบยกขึ้นพิจารณาเป็นประเด็นสำคัญเป็นพิเศษในการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ดังนี้

"ในการค้นหรือยึดพยานหลักฐานของพนักงานเจ้าหน้าที่ที่ควรระวังมิให้ละเมิดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคลอื่นโดยไม่จำเป็น"[59]

"...ในการเสนอร่างกฎหมายต่อสภานิติบัญญัติแห่งชาตินั้น ข้อกังวลที่คณะกรรมาธิการวิสามัญได้รับฟังหรือได้มีการแปรญัตตินั้น คือ ร่างกฎหมายได้ให้อำนาจพนักงานเจ้าหน้าที่ซึ่งจะ

---

[58] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญาว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา, พิมพ์ครั้งที่5 (กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2549), หน้า 7-10.

[59] บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... ร่างที่สคก.ตรวจพิจารณาแล้ว เรื่องเสร็จที่ 257/2548

แต่งตั้งขึ้นอย่างมากมาย อันอาจก่อให้เกิดความเสี่ยงหรือผลกระทบที่ประชาชนหรือสังคมจะได้รับจากการใช้อำนาจหน้าที่โดยมิชอบของพนักงานเจ้าหน้าที่ดังกล่าว ดังนั้น การให้หน่วยงานที่เกี่ยวข้องในปัจจุบันซึ่งทำหน้าเกี่ยวกับการสืบสวน สอบสวน หรือดำเนินคดีในลักษณะที่เป็นการกระทำความผิดต่างๆ ทางคอมพิวเตอร์ ได้มาเล่าให้ฟังหรือให้ข้อมูลถึงสภาพข้อเท็จจริงปัญหาและอุปสรรคในการทำงาน ทั้งชั้นสืบสวน สอบสวน หรือดำเนินคดีต่อคณะกรรมาธิการวิสามัญเพื่อจะได้ทำให้คณะกรรมาธิการวิสามัญได้เห็นหรือเข้าใจสภาพปัญหาที่เกิดขึ้นชัดเจนยิ่งขึ้น และการนำเสนอดังกล่าวก็น่าจะเป็นประโยชน์ต่อการพิจารณาว่า การกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่นั้น ควรกำหนดไว้มากน้อยแค่ไหนเพียงใด โดยเฉพาะอย่างยิ่งในการใช้อำนาจที่มีความเสี่ยงจะกระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของประชาชน

อย่างไรก็ตาม การกระทำความผิดทางคอมพิวเตอร์ในบางครั้งก็อาจส่งผลกระทบหรือก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ดังนั้น การพิจารณาเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ เพื่อให้เกิดความสมดุลในการใช้อำนาจและปกป้องคุ้มครองสังคมได้อย่างเหมาะสม ..."[60]

2.4 กฎหมายสารบัญญัติที่กำหนดความผิดที่กระทำบนอินเทอร์เน็ต

การบัญญัติกฎหมายเพื่อลงโทษผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer crimes) หรือการกระทำความผิดบนอินเทอร์เน็ต (Cyber Crime) เป็นการยากที่จะกำหนดให้ชัดเจนลงไปว่ามีขอบเขตเพียงใด เพราะการหากกำหนดขอบเขตที่ไม่ชัดเจนแล้วอาจมีผลกระทบไปถึงขอบเขตของอาชญากรรมประเภทอื่นๆได้ ดังนั้น การในการบัญญัติกฎหมายจึงต้องให้ความสำคัญกับรายละเอียดเล็กน้อยอย่างรอบคอบ ประกอบกับความรู้และความชำนาญในด้านเทคโนโลยีคอมพิวเตอร์

---

[60] สรุปสาระสำคัญการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... เมื่อวันที่ 23 พฤศจิกายน 2549 เวลา 10.00 น.ณ ห้องประชุมคณะกรรมาธิการ หมายเลข 309 ชั้น 3 อาคารรัฐสภา 2

ประวัติของการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์มีจุดเริ่มต้นจากร่างกฎหมาย Ribicoff (The Ribicoff Bill)[61] โดยร่างกฎหมายฉบับนี้ต้องการบัญญัติฐานความผิดการใช้คอมพิวเตอร์โดยมิชอบ(Misuse of computers) และ The Bill S. 1766 (95th Congress) ได้สนับสนุนให้มีการออกกฎหมายFederal Computer Systems Protection Act of 1977 แม้ว่าร่างกฎหมายทั้งสองฉบับจะไม่ได้รับอนุมัติจากสภานิติบัญญัติ แต่ก็เป็นแนวทางการร่างกฎหมายของประเทศสหรัฐอเมริกา และเป็นการเตือนประเทศต่างๆทั่วโลกให้ตระหนักถึงความสำคัญในการบัญญัติกฎหมายให้ครอบคลุมถึงอาชญากรรมคอมพิวเตอร์

ส่วนการนิยามความหมายของคำว่าอาชญากรรมคอมพิวเตอร์เป็นครั้งแรก ได้มีการนำเสนอไว้ใน Criminal Justice Resouce Manual (1979)โดยการนำเสนอคำนิยามได้ให้ความหมายอย่างกว้างว่า "การกระทำใดๆอันละเมิดต่อกฎหมาย ที่ใช้ความรู้ด้านเทคโนโลยีคอมพิวเตอร์เป็นปัจจัยสำคัญเพื่อให้การฟ้องร้องดำเนินคดีบรรลุผล"[62] และได้มีการให้นิยามความหมายของอาชญากรรมคอมพิวเตอร์ในหลากหลายความหมาย เช่น

ในการศึกษาทิศทางกฎหมายนานาชาติเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (1986)ได้ให้คำนิยามของอาชญากรรมคอมพิวเตอร์ว่า*"การกระทำความผิดอันละเมิดต่อกฎหมายใดๆที่ได้ใช้ความรู้ด้านเทคโนโลยีคอมพิวเตอร์เป็นปัจจัยสำคัญในการกระทำความผิดนั้น"*[63]

องค์กรความร่วมมือและพัฒนาทางเศรษฐกิจ หรือ OECD (Organization for Economic Cooperation and Development) ได้ให้ข้อเสนอแนะเกี่ยวกับคำนิยามพื้นฐานของอาชญากรรมคอมพิวเตอร์ในปี 1986 ว่า *"อาชญากรรมอันเกี่ยวกับคอมพิวเตอร์พิจารณาจากการ*

---

[61] http://www.cybercrimelaw.net/content/history.html

[62] U.S. Department of Justice ,The criminal justice resource manual on computer crime, California, USA. "....Any illegal act for which knowledge of computer technology is essential for a successful prosecution..."

[63] Judge Stien Schjolberg and Amada M. Hubbard , "International telecommunication union", Hamonizing National Legal Approaches on Cybercrime. , WSIS thematic Meeting on Cybersecurity (Geneva,28june-1july2005) , p.4 "...Encompasses any illegal act for which knowledge of computer technology is essential for its perpetration...")

กระทำอันละเมิดต่อกฎหมายใดๆ,ความไร้จริยธรรมหรือการกระทำโดยไม่มีอำนาจที่เกี่ยวข้องกับระบบการประมวลผลอัตโนมัติและการสื่อสารข้อมูล"

คณะมนตรียุโรป(Council of Europe) ได้ให้ข้อเสนอแนะในปี 1989 เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ว่า *"การกระทำผิดอาญาใดๆ ที่การสืบสวนสอบสวนโดยมีอำนาจจะต้องเกี่ยวข้องกับกระบวนการประมวลผลข้อมูลหรือสื่อสารข้อมูลในระบบคอมพิวเตอร์หรือระบบการประมวลผลข้อมูลอิเล็กทรอนิกส์"*[64]

นอกจากนี้การกระทำความผิดบางประเภท เช่น การละเมิดลิขสิทธิ์ (Copy Infringements), ลัทธิชนชาติ (Racism), การแสดงความเกลียดชังชาวต่างชาติ(Xenophobia) หรือการเผยแพร่ภาพลามกอนาจารเด็ก(Child Pornography) ในหลายประเทศไม่จัดเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer crimes) หรือการกระทำความผิดบนอินเทอร์เน็ต (Cyber Crime) เพราะการละเมิดลิขสิทธิ์มีพื้นฐานจากหลักนิติกรรมและสัญญา ในหลายประเทศจึงไม่ถือเป็นการกระทำความผิดอาญา ส่วนการเผยแพร่ภาพลามกอนาจารเด็กก็ถือเป็นความผิดตามกฎหมายอาญาดั้งเดิมอยู่แล้ว

2.4.1 กฎหมายสารบัญญัติของต่างประเทศ

การบัญญัติกฎหมายสำหรับการกระทำผิดบนอินเทอร์เน็ตเป็นปัญหาสำคัญทั่วโลก เพราะการกำหนดรูปแบบของกฎหมายเพื่อควบคุมการกระทำผิดบนอินเทอร์เน็ตในปัจจุบันอาจส่งผลกระทบต่อผู้คนนับพันล้านคนในอนาคต การบัญญัติกฎหมายจึงควรที่จะมีความยืดหยุ่นต่อในการปรับใช้กับการกระทำผิดที่อาจจะเกิดขึ้นในอนาคตโดยอาศัยนวัตกรรมและเทคโนโลยีใหม่ๆ โดยจะต้องบัญญัติกฎหมายสำหรับการกระทำความผิดบนอินเทอร์เน็ตเป็นการเฉพาะให้มีความแตกต่างจากกฎหมายอาญาที่มีอยู่เดิม และต้องสามารถนำมาใช้ควบคุมการกระทำต่างๆบนสังคมออนไลน์ได้เช่นเดียวกับควบคุมการกระทำของมนุษย์ในสังคมปกติ

---

[64] "...encompassing any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or electronic data processing systems..."

การกระทำความผิดสามารถเกิดขึ้นได้ทั่วโลก จึงต้องบัญญัติกฎหมายให้มีความเป็นสากลและสอดคล้องกับประเทศอื่นๆ ด้วยเหตุนี้ องค์กรระหว่างประเทศจึงมีความพยายามร่วมกันที่จะสร้างบทบัญญัติที่เป็นมาตรฐานเพื่อให้แต่ละประเทศมีแนวทางการบัญญัติกฎหมายที่สอดคล้องไปในแนวทางเดียวกัน ดังที่จะได้กล่าวต่อไป

องค์กรความร่วมมือระหว่างประเทศ

ตามรายงานของที่ประชุมโลกว่าด้วยสังคมสารสนเทศ(World Summit on the Information Society (WSIS)) ณ กรุงเจนีวา วันที่ 28มิถุนายน-1กรกฎาคม พ.ศ.2548 ได้กล่าวถึงประเด็นความร่วมมือขององค์กรความร่วมมือระหว่างประเทศต่างๆไว้ ดังนี้[65]

1. ความพยายามของสหประชาชาติ(United Nations Efforts)

สหประชาชาติเป็นผู้นำเกี่ยวกับการพัฒนาในระดับสากลมาเป็นระยะเวลานานและมีการอภิปรายเกี่ยวกับความสัมพันธ์ด้านนี้หลายครั้ง โดยมีที่ประชุมโลกว่าด้วยสังคมสารสนเทศ(World Summit on the Information Society (WSIS)) เป็นผู้ร่วมวิจัยพัฒนา

1.1 มติสมัชชาใหญ่ของสหประชาชาติ(General Assembly Resolution) การประชุมคณะกรรมการของสมัชชาใหญ่ มีมติที่ประชุมที่สำคัญเกี่ยวกับอินเทอร์เน็ต เช่น มติที่ประชุมในหัวข้อ Development in the field of information and telecommunication in the context of international security[66], Combating the Criminal Misuse of Information Technology[67], Creation of Global Culture of Cybersecurity[68], Creation of Global Culture of Cybersecurity and the Protection of Criminal Information Infrastructures[69] เป็นต้น

---

[65] Judge Stien Schjolberg and Amada M. Hubbard , "International telecommunication union", Hamonizing National Legal Approaches on Cybercrime, pp. 5-10.

[66] "มติที่ 53/70" 4 ธันวาคม 1998; "มติที่54/49" 1ธันวาคม 1999; "มติที่55/28" 20 พฤศจิกายน 2000; "มติที่56/19" 29 พฤศจิกายน2001; "มติที่57/53" 22 พฤศจิกายน 2002; "มติที่58/32" 18 ธันวาคม 2003.

[67] "มติที่ 55/63" 4 ธันวาคม 2000; "มติที่ 56/121" 19 ธันวาคม 2001

[68] "มติที่ 57/239" 20 ธันวาคม 2002

[69] "มติที่ 58/199" วันที่ 23 ธันวาคม 2003

1.2 ที่ประชุมโลกว่าด้วยสังคมสารสนเทศ(World Summit on the Information Society) หรือ WSIS โดยมีผู้เชี่ยวชาญจากทั่วโลกเพื่อพัฒนาศูนย์ควบคุมของแต่ละรัฐและกฎหมายเพื่อความปลอดภัยของระบบอินเทอร์เน็ต โดยได้มีการร่างเอกสารสำคัญคือ1.Geneva Declaration and plan of action และ 2.Ongoing Negotiations for Tunis Phase of the Summit นอกจากนี้ยังมีการหาแนวทางความร่วมมือร่วมกันในที่ประชุมอื่นๆของสหประชาชาติอีก เช่น Group of Government Expect on Information Security,International Telecommunications Union(ITU) Standard and working Groups, United Nations Crimes Congresses

2.กลุ่มประเทศอุตสาหกรรมชั้นนำ 8 ประเทศ (Group of Eight) หรือ G-8

ประเทศสมาชิกในกลุ่มจี-8 ได้พยายามจำแนกประเภทของ High-Tech Crime ไว้ในการประชุมปีค.ศ.1997 และได้มีการกำหนดหลักการเพื่อควบคุมอาชญากรรมคอมพิวเตอร์โดยมีหลักการที่น่าสนใจ เช่น[70] การพัฒนาบุคลากรให้มีความรู้ความสามารถและมีเครื่องมือที่เพียงพอในการรับมือกับคดีอาชญากรรมทางคอมพิวเตอร์รวมทั้งสามารถให้ความช่วยเหลือกับหน่วยงานต่างประเทศได้ การร่วมมือกับภาคอุตสาหกรรมซอฟต์แวร์ในการพัฒนาเทคโนโลยีที่ใช้สำหรับรวบรวมและเก็บรักษาหลักฐานอิเล็กทรอนิกส์ การจัดให้มีข่ายความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ที่มีเจ้าหน้าที่ปฏิบัติหน้าที่ตลอด 24 ชั่วโมง (24/7 network) เพื่อทำหน้าที่ให้การช่วยเหลือระหว่างประเทศ

3.การบัญญัติกฎหมายต้นแบบของกลุ่มประเทศในเครือจักรภพอังกฤษ(Commonwealth Model Legislation)

เป็นความร่วมมือโดยวัตถุประสงค์ที่ต้องการให้มีกฎหมายที่สอดคล้องกันสำหรับกลุ่มประเทศในเครือจักรภพอังกฤษ ในปี ค.ศ.2002 ที่ประชุมได้เสนอกฎหมายต้นแบบที่มีชื่อว่า Computer and Computer Related Crimes Act และวางแผนที่จะใช้เป็นแนวทางการร่างกฎหมายของประเทศที่เป็นสมาชิก โดยกฎหมายต้นแบบนี้ต้องการให้สามารถนำไปใช้เป็นต้นแบบให้กับประเทศอื่นที่ไม่ได้เป็นสมาชิกของกลุ่มได้อีกด้วย

---

[70] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 63.

4. องค์การรัฐอเมริกัน(organization of American states)

ในการประชุมเมื่อวันที่28-30 เมษายน ปี ค.ศ.2004 ได้พยายามบัญญัติกฎหมายโดยกลุ่มผู้เชี่ยวชาญเกี่ยวกับอาชญากรรมคอมพิวเตอร์ คณะผู้พิพากษาและคณะทนายความ โดยพิจารณาอนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime)และพิจารณาถึงความเป็นไปได้ที่จะเข้าร่วมกับอนุสัญญาดังกล่าว

5. สหภาพยุโรป(European Union)[71]

ในปี 1998 เมื่อคณะกรรมาธิการยุโรป (European Commission) ได้นำเสนอ Legal Aspects of Computer-Related Crime in the Information Society - COMCRIME studyต่อสภายุโรป (European Council) โดยมีเนื้อหาเกี่ยวกับภาพรวมของการก่ออาชญากรรมและแนวทางการแก้ไขด้านต่างๆ และต่อมาในปี 2000 European Council และ European Commission ได้จัดทำแผน eEurope Action ขึ้น และยังได้มีการจัดตั้ง EU Forum on Cybercrime ในด้านมาตรการทางกฎหมายโดยเฉพาะ European Commission ได้เสนอข้อเสนอที่เรียกว่า Council Framework Decision on attacks against information systems ต่อ European Commission ในปี ค.ศ. 2002

6.ความร่วมมือทางเศรษฐกิจในเอเชียแปซิฟิก (Asian Pacific Economic Cooperation)หรือAPEC[72]

กลุ่มความร่วมมือทางเศรษฐกิจในเอเชียแปซิฟิกหรือ APEC ได้เริ่มให้ความสำคัญกับปัญหาอาชญากรรมคอมพิวเตอร์อย่างจริงจัง ตั้งแต่ปี ค.ศ. 2001 เนื่องจากการผลักดันของสหรัฐอเมริกาที่ต้องการให้ประเทศต่างๆ ให้ความสำคัญกับปัญหาการก่อการร้าย ใน ปี ค.ศ. 2002 ได้มีการประกาศปฏิญญาเชี่ยงไฮ้ ซึ่งต่อมาในการประชุมครั้งที่ 26 ก็ได้มีจัดทำ APEC Cybersecurity Strategy ซึ่งมีประเด็นสำคัญที่น่าสนใจ เช่น การพัฒนากฎหมาย (Legal developments) การให้ข้อมูลและประสานความร่วมมือ (Information sharing and cooperation)

---

[71] เรื่องเดียวกัน, หน้า 59-61.

[72] เรื่องเดียวกัน, หน้า 64-68.

การจัดทำแนวปฏิบัติด้านเทคนิคและความมั่นคง (Security and technical guidelines)การสร้างความตื่นตัวให้กับประชาชน (Public awareness) การฝึกอบรมและให้ความรู้ (Training and Education) เป็นต้น

7.องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Coperation and Development)หรือOECD

ในปี ค.ศ.1983 ที่กรุงปารีสมีการประชุมอภิปรายเกี่ยวกับอาชญากรรมคอมพิวเตอร์และความจำเป็นที่จะแก้ไขประมวลกฎหมายอาญา โดยมีการรายการเกี่ยวกับการปลอมแปลงและฉ้อโกงบนคอมพิวเตอร์(Computer forgery and Computer fraud) การทำลายข้อมูลคอมพิวเตอร์และโปรแกรม(Damage to computer data and programmes) การล่วงละเมิดการป้องกันของโปรแกรมคอมพิวเตอร์(Infringement of a protected computer programme) การเข้าถึงคอมพิวเตอร์โดยไม่มีอำนาจ(Unauthorized access) การดักข้อมูลของระบบคอมพิวเตอร์(Interception of a computer system)

8.คณะมนตรียุโรป(Council of Europe)

คณะมนตรียุโรป เป็นองค์กรสากลแห่งแรกที่ริเริ่มในเรื่องอาชญากรรมคอมพิวเตอร์ ได้มีการประชุมหาแนวทางการควบคุมอาชญากรรมคอมพิวเตอร์หลายครั้งจนกระทั่ง มีการลงนามในอนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime) ที่เมือง Budapest ประเทศฮังการี เมื่อวันที่ 23 พฤศจิกายน 2001 อนุสัญญาฉบับนี้ถือเป็นบันทึกทางประวัติศาสตร์อันสำคัญของกฎหมายอาชญากรรมคอมพิวเตอร์ โดยอนุสัญญานี้ถูกใช้เป็นต้นแบบในการพิจารณาสนธิสัญญาระหว่างประเทศอื่นๆ เช่น กลุ่ม G-8,กลุ่ม APEC เป็นต้น

ฐานความผิดทางอาญาของอาชญากรรมคอมพิวเตอร์

ตามที่ได้กล่าวมาแล้วว่าประเทศต่างๆ มีความพยายามที่จะบัญญัติกฎหมายให้มีความเป็นสากลและสอดคล้องกับประเทศอื่นๆ เพื่อความสะดวกในการสร้างความร่วมมือร่วมกันและเพื่อให้เป็นไปตามสนธิสัญญา ดังนั้น การกำหนดฐานความผิดจึงมีความสอดคล้องกัน ตามรายงานของที่ประชุมโลกว่าด้วยสังคมสารสนเทศ(World Summit on the

Information Society (WSIS)) ณ กรุงเจนนีวา วันที่ 28มิถุนายน-1กรกฎาคม พ.ศ.2548 ได้กำหนดประเภทฐานความผิดไว้ ดังนี้

1.การเข้าถึงคอมพิวเตอร์โดยมิชอบ(Illegal access)

การเข้าถึงคอมพิวเตอร์โดยมิชอบ หมายถึง *"การเข้าถึงบางส่วนหรือทั้งหมดของระบบคอมพิวเตอร์โดยไม่มีสิทธิ โดยการล่วงล้ำมาตรการป้องกันด้วยเจตนาที่จะได้มาซึ่งข้อมูลคอมพิวเตอร์หรือเจตนาไม่สุจริตอื่น หรือในการติดต่อกับระบบคอมพิวเตอร์ที่ได้เชื่อมต่อกับระบบคอมพิวเตอร์อื่น"*[73]

ฐานความผิดนี้ถือเป็นฐานความผิดพื้นฐานของอาชญากรรมคอมพิวเตอร์ โดยมีแนวคิดที่จะให้ความคุ้มครองข้อมูล(Data) เพราะข้อมูลมีลักษณะที่สำคัญ 2 ประการคือ1.ข้อมูลเป็นบันทึกพฤติกรรมการดำรงชีวิตของมนุษย์และ 2.ข้อมูลเป็นองค์ประกอบที่สำคัญของคอมพิวเตอร์ โดยได้มีการเสนอให้การกระทำนี้เป็นความผิดอาญาโดยองค์กรความร่วมมือและพัฒนาทางเศรษฐกิจ (OECD) ในปี ค.ศ. 1986 และ คณะมนตรียุโรปในปี ค.ศ.1989

การเข้าถึงระบบคอมพิวเตอร์และเครือข่ายโดยมิชอบ รู้จักกันในชื่ออื่น เช่น Computer trespass, Cracking หรือ Hacking เป็นต้น การกระทำความผิดประเภทนี้ไม่จำเป็นต้องเป็นการเข้าถึงข้อมูลแต่เพียงอย่างเดียวเท่านั้น แต่อาจรวมถึงเข้าไปกระตุ้นให้ระบบรักษาความปลอดภัยของคอมพิวเตอร์ทำงานแม้ยังไม่สามารถเข้าไปถึงข้อมูลได้ก็อาจเป็นความผิดสำเร็จแล้ว และในการเข้าถึงข้อมูลนั้นไม่จำต้องพิจารณาว่าเนื้อหาสาระของข้อมูลนั้นเป็นสิ่งที่เข้าใจได้หรือไม่ และไม่สำคัญว่าข้อมูลนั้นจะถูกเก็บรักษาไว้ในส่วนใดของระบบคอมพิวเตอร์ การพิจารณาว่าความผิดสำเร็จหรือไม่นั้นไม่จำเป็นต้องพิจารณาว่าผู้กระทำความผิดได้ไปซึ่งข้อมูลใดๆ หรือไม่ เพียงแต่เข้าไปในระบบได้ก็ถือเป็นความผิดสำเร็จแล้ว แม้ว่าผู้กระทำความผิดมีเจตนาเพียงเข้าไปสำรวจในระบบเท่านั้น รวมถึงการเข้าไปสอดแนมด้วยวิธีการใดๆ การเข้าไปในระบบหมายถึงการเข้าไปโดยการเชื่อมต่อระบบเท่านั้นไม่จำเป็นต้องมีการเข้าไปตามความเป็นจริง และไม่ต้องพิจารณาว่าการเข้าไปในระบบนั้นจะก่อให้เกิดความเสียหายต่อระบบด้วยหรือไม่

---

[73] The Council of Europe Convention on Cybercrime : Article 2 - Illegal access: "...the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

การพิจารณาความผิดฐานนี้ จำเป็นต้องพิจารณาถึงการ"เข้าไป" โดยต้องตีความอย่างเคร่งครัด ดังนั้น การส่งอีเมล์หรือไฟล์ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ไม่ถือว่าเป็นการ"เข้าไป"ตามความหมายนี้ การเข้าไปจึงต้องเป็นการเข้าไปในระบบของคอมพิวเตอร์อื่นหรือในเครือข่ายหรือเข้าไปตรวจสอบรหัสผ่าน(Checking password) ในบางรัฐไม่ได้พิจารณาเพียงการเข้าไปเท่านั้นแต่ยังพิจารณาด้วยว่าการเข้าไปนั้น "ได้ไป" ซึ่งข้อมูลหรือไม่ เจตนาหรือไม่ปราศจากอำนาจหรือไม่ โดยการ "ได้ไป"ซึ่งข้อมูลรวมถึงการเข้าไปสังเกตการณ์และได้อ่านข้อมูลดังกล่าว[74] ซึ่งไม่ได้หมายความเฉพาะการดาวน์โหลดข้อมูลเท่านั้น

ในหลายประเทศพบว่าการกำหนด "การล่วงล้ำมาตรการป้องกัน" เป็นองค์ประกอบความผิดก่อให้เกิดปัญหาในการลงโทษผู้กระทำความผิดตามมา เช่น เมื่อพิจารณาความหมายของคำว่า "การล่วงล้ำมาตรการป้องกัน" (Infringing security measures) แล้วพบว่าการบัญญัติถ้อยคำดังกล่าวส่งเสริมให้ประชาชนใช้ระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์มากขึ้น ในขณะที่รัฐเพิกเฉยที่จะดำเนินคดีกับผู้กระทำความผิด เพราะหากผู้กระทำความผิดได้ล่วงล้ำระบบคอมพิวเตอร์โดยคอมพิวเตอร์ดังกล่าวไม่ได้ติดตั้งมาตรการป้องกันกฎหมายก็ไม่สามารถลงโทษผู้กระทำผิดได้

ตัวอย่างกฎหมายต่างประเทศที่กำหนดให้มีความผิดทันทีที่ "เข้าถึง" คอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ได้แก่ อังกฤษ มาเลเซีย สิงคโปร์ อิสราเอล ฝรั่งเศส ส่วนในบางประเทศได้กำหนดให้ผู้กระทำต้องรับโทษหนักขึ้น หากการเข้าถึงนั้นได้ก่อให้เกิดความเสียหายหรือเป็นการกระทำผิดโดยมีเจตนาเพื่อกระทำความผิดฐานอื่นต่อไป เช่น ประเทศออสเตรเลีย ฝรั่งเศส อิตาลี นอร์เวย์ สิงคโปร์

ประเทศที่กำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดต่อเมื่อได้ละเมิดระบบการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ได้แก่ ประเทศเยอรมัน อิตาลี ออสเตรเลีย เนเธอร์แลนด์ สวิตเซอร์แลนด์ ในขณะเดียวกัน ก็มีบางประเทศที่กำหนดให้ผู้กระทำต้องรับผิดหนักขึ้นหากการเข้าถึงดังกล่าวเป็นการละเมิดเกี่ยวกับระบบการรักษาความมั่นคง เช่น โปรตุเกส

---

[74] The U.S. Senate Judiciary Committee on U.S.C. 1030(a)(2): "Because the premise of this subsection is privacy protection, the Committee wishes to make clear that obtaining information in this context includes mere observation of the data."

จากตัวอย่างกฎหมายต่างประเทศที่ยกมาข้างต้น จะเห็นได้ว่าแนวทางการบัญญัติความผิดฐานเข้าถึงโดยมิชอบนั้นมีอยู่ด้วยกัน 3 แนวทาง กล่าวคือ[75]

แนวทางที่ 1 กฎหมายกำหนดให้เป็นความผิดทันทีเมื่อมีการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ

แนวทางที่ 2 กฎหมายกำหนดให้เป็นความผิดเฉพาะแต่กรณีได้ละเมิดหรือฝ่าฝืนระบบการรักษาความมั่นคงหรือปลอดภัยเท่านั้น

แนวทางที่ 3 กฎหมายกำหนดให้ผู้กระทำต้องรับผิดหนักขึ้นหากการเข้าถึงดังกล่าวเป็นการละเมิดระบบการรักษาความมั่นคงหรือปลอดภัย

2.การดักข้อมูลคอมพิวเตอร์(Illegal interception)

การดักข้อมูลคอมพิวเตอร์ หมายถึง *"การดักข้อมูลโดยไม่มีสิทธิ โดยวิธีการใด ซึ่งการส่งข้อมูลนั้นไม่ใช่การส่งข้อมูลคอมพิวเตอร์เป็นการสาธารณะ จากหรือภายในระบบคอมพิวเตอร์ รวมถึงการได้มาซึ่งข้อมูลคอมพิวเตอร์โดยการรับการแผ่สนามแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ โดยเจตนาไม่สุจริตหรือในการติดต่อกับระบบคอมพิวเตอร์ที่ได้เชื่อมต่อกับระบบคอมพิวเตอร์อื่น"*[76]

ความผิดฐานนี้อาจเป็นการดักข้อมูลภายในระบบคอมพิวเตอร์นั้นเองหรือระหว่างการส่งหรือรับข้อมูลระหว่างคอมพิวเตอร์กับอุปกรณ์คอมพิวเตอร์ก็ได้ และยังรวมถึงการได้มาซึ่งข้อมูลคอมพิวเตอร์โดยการดักรับการแผ่สนามแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ด้วย

ความผิดฐานนี้บัญญัติขึ้นเพื่อคุ้มครองการล่วงละเมิดสิทธิความเป็นส่วนตัว (Right to privacy)ในการติดต่อสื่อสารผ่านเทคโนโลยีอิเล็กทรอนิกส์ โดยแต่ละประเทศทั่ว

---

[75] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 36.

[76] The Council of Europe Convention on Cybercrime : Article 3 - Illegal interception: "...the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

โลกมีหลักเกณฑ์และมาตรฐานในการคุ้มครองที่แตกต่างกัน นอกจากนี้ ในบางกรณีกฎหมายอาจยกเว้นผู้ให้บริการ(Service providers) สามารถดักข้อมูลได้โดยไม่ถือเป็นความผิด เพราะผู้ให้บริการมีความจำเป็นที่จะติดตามความเคลื่อนไหวของข้อมูลจราจรทางคอมพิวเตอร์(Traffic data)ในเครือข่ายของตนที่อาจก่อให้เกิดความเสียหายกับเครือข่าย ผู้ให้บริการจึงมีความชอบธรรมที่จะป้องกันสิทธิและป้องกันทรัพย์สินของตนได้

การกระทำผิดฐานนี้นี้อาจเทียบได้กับการดักฟังและลักลอบบันทึกเสียงการสนทนาผ่านโทรศัพท์(Tapping and recording of oral telephone conversation) ฐานความผิดนี้จึงอาจจะปรับใช้การดักข้อมูลทุกประเภทที่เป็นการสื่อสารทางอิเล็กทรอนิกส์ การสื่อสารโดยทางโทรศัพท์ อีเมล์ หรือการรับส่งไฟล์ เนื้อหาของความผิดจะต้องครอบคลุมถึงการติดตามความเคลื่อนไหว(Monitoring) การตรวจตรา(Surveillance) การฟัง(Listening) เนื้อหาของข้อมูลที่สื่อสารโดยคอมพิวเตอร์ การติดตามความเคลื่อนไหวอาจกระทำโดยการเข้าไปนำข้อมูลนั้นออกมาโดยตรงหรือใช้โปรแกรมคอมพิวเตอร์ หรือใช้เครื่องมือแอบฟังทางอิเล็กทรอนิกส์(Electronic eavesdropping or tapping device)

ถ้อยคำที่ว่า"ไม่เป็นการสาธารณะ" (Non-public) ครอบคลุมเฉพาะข้อมูลคอมพิวเตอร์(Computer data) ไม่รวมถึงเนื้อหาของข้อมูล (Content of the data) ดังนั้น ข้อมูลสาธารณะที่สามารถเข้าถึงได้โดยง่าย (Public accessible information) จึงอาจไม่ใช่ความหมายของถ้อยคำว่า "ไม่เป็นการสาธารณะ"(Non-public)ก็ได้ หรือการสื่อสารระหว่างกันโดยต้องการให้การสื่อสารนั้นเป็นความลับไม่เปิดเผยเป็นการทั่วไป ก็ถือว่า "ไม่เป็นการสาธารณะ"(Non-public) เช่นเดียวกับการสื่อสารที่ไม่สามารถเข้าถึงได้โดยง่ายจนกว่าจะได้ชำระเงิน เช่น Pay-TV การรับส่งสัญญาณดังกล่าวกล่าวก็ถือว่า"ไม่เป็นการสาธารณะ"(Non-public) เช่นเดียวกัน

3.การรบกวนข้อมูลคอมพิวเตอร์(Data interference)

การรบกวนข้อมูล หมายถึง *"การทำลาย,ลบ,ทำให้เสื่อม,แก้ไข หรือระงับ ซึ่งกระทำต่อข้อมูลคอมพิวเตอร์โดยไม่มีสิทธิ"*

ความมุ่งหมายของฐานความผิดนี้ต้องการคุ้มครองข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์เช่นเดียวกับทรัพย์ที่มีรูปร่าง (Tangible Object) จึงได้ให้ความคุ้มครองการทำงานของระบบ การเก็บข้อมูล หรือโปรแกรมคอมพิวเตอร์ ดังนั้น การทำลาย ทำให้เสียหาย ทำให้

เสื่อมค่า หากได้กระทำต่อทรัพย์ย่อมเป็นความผิดอาญา การบัญญัติกฎหมายเพื่อป้องกันอาชญากรรมคอมพิวเตอร์ก็ได้ให้ความคุ้มครองข้อมูลจราจรทางคอมพิวเตอร์(Traffic data)หรือระบบคอมพิวเตอร์ด้วยแนวคิดและหลักการเดียวกัน ส่วนการลบข้อมูล(Erasure of data) หมายรวมถึงการลบข้อมูลเฉพาะที่สามารถอ่านได้ด้วยเครื่องมืออิเล็กทรอนิกส์(Readable electronically)และไม่ปรากฏในรูปแบบที่มนุษย์สามารถเข้าใจได้(Understandable to humans)

ฐานความผิดนี้อาจเทียบเคียงได้กับความผิดฐานทำให้เสียทรัพย์ตามกฎหมายอาญาดั้งเดิม ในบางรัฐการให้คำนิยามของคำว่า"ทรัพย์สิน"(Property)ให้รวมถึงข้อมูล(Data)ด้วย โดยใช้การตีความขยายความหมายของคำว่า"การกระทำให้เสื่อมประโยชน์"(Renders useless an object) ให้หมายรวมไปถึงการลบข้อมูล(Erasure of data) และรวมถึงการทำให้คอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติเช่นเดิม แต่อย่างไรก็ดีการใช้การตีความกฎหมายเพื่ออุดช่องว่างดังกล่าวไม่อาจใช้การได้ในทุกกรณีเพราะความแตกต่างกันด้านคุณธรรมทางกฎหมายที่กฎหมายอาญาดั้งเดิมต้องการคุ้มครองทรัพย์สินทางกายภาพเท่านั้น

ส่วนการดัดแปลงข้อมูล(Alteration)อาจหมายถึงการทำให้ลักษณะของข้อมูลเปลี่ยนแปลงไป ยกตัวอย่างเช่น การแก้ไขข้อคว่ามปกติเป็นข้อความหยาบโลน หรือการทำให้เว็บไซต์เปลี่ยนแปลงหน้าตาไป เป็นต้น หรือการเพิ่มเติมข้อมูลเข้าไปโดยไม่ได้ทำการลบข้อมูล เช่น การแก้ไขเพิ่มเติมเนื้อหาของข้อมูล

การระงับข้อมูล (Suppression) ครอบคลุมถึงการกระทำอันเป็นการขัดขวาง(Prevent) หรือทำให้หยุด(Terminate) ของการใช้งานข้อมูล เช่น ผู้กระทำความผิดได้ทำให้ข้อมูลหายไป(Disappear)โดยมิได้ลบข้อมูล

การทำลายและการทำให้เสื่อม (Damaging and Deterioration) เป็นถ้อยคำที่รวมการกระทำความผิดที่ทับซ้อนกันอยู่ แต่ทั้งสองคำนี้หมายรวมถึงการทำให้ข้อมูลคอมพิวเตอร์(DataXหรือข้อมูลจราจรทางคอมพิวเตอร์(Traffic data)ใช้ประโยชน์ได้ลดลง(Useless)หรือมีคุณค่าลดลง(Meaningless) รวมถึงการทำลายPassword และทำลายมาตรการป้องกันที่เจ้าของคอมพิวเตอร์ได้ติดตั้งไว้ และรวมถึงการทำลายระบบรักษาความปลอดภัยของเครือข่ายอินเทอร์เน็ต แม้ว่าจะไม่มีข้อมูลใดๆที่ถูกแก้ไขหรือถูกลบก็ตาม ความผิดฐานนี้รวมถึงไวรัสคอมพิวเตอร์ และรวมถึงโปรแกรมหรือคำสั่ง (Code)ใดๆที่ทำให้คอมพิวเตอร์ทำงานไม่ถูกต้องสมบูรณ์ เช่น โปรแกรมมุ่งประสงค์ร้าย(Malware) และ Logic bomb เป็นต้น

4.การรบกวนระบบคอมพิวเตอร์(System interference)

การรบกวนระบบ หมายถึง *"การสร้างอุปสรรคขัดขวางโดยไม่มีสิทธิซึ่งกระทำต่อการทำงานของระบบคอมพิวเตอร์โดยการนำเข้า การส่งผ่าน การทำลาย การลบ การทำให้เสื่อม แก้ไข หรือ ระงับ โดยกระทำต่อข้อมูลคอมพิวเตอร์"*[77]

ความผิดฐานนี้เป็นการกระทำผิดที่เข้าไปมีอำนาจโน้มน้าวการทำงานของคอมพิวเตอร์หรือทำให้ระบบไม่สามารถทำงานได้ เช่น การทำให้ระบบเสียหายโดยคอมพิวเตอร์จะถูกปิดภายหลังจากถูกจู่โจมจากการกระทำผิดแล้วโดยผู้ใช้ไม่สามารถควบคุมได้ หรือ ทำให้เครื่องคอมพิวเตอร์ประมวลผลได้ช้าลง หรือทำให้หน่วยความจำของเครื่องคอมพิวเตอร์ไม่พอสำหรับการประมวลผล(Run out of memory) หรือทำให้ระบบทำงานไม่ถูกต้อง(Process incorrectly) หรือ ข้ามขั้นตอนการประมวลผลที่ถูกต้อง(Omit correct process) การสร้างอุปสรรคขัดขวางต่อระบบคอมพิวเตอร์ที่สำคัญของรัฐหรือระบบคอมพิวเตอร์สาธารณะอาจสร้างความเสียหายต่อภาครัฐและสังคมในวงกว้าง โดยเป้าหมายจะเป็นคอมพิวเตอร์ที่ควบคุมระบบสาธารณูปโภคพื้นฐาน เช่น ระบบพลังงาน การกระจายข่าว การคมนาคมขนส่ง หรือการสื่อสารทางโทรศัพท์

ระยะเวลาที่เป็นอุปสรรคขัดขวางต่อการทำงานของระบบคอมพิวเตอร์จะยาวนานเพียงใดไม่สำคัญ การกระทำผิดอาจอยู่ในรูปแบบของ Denial of service(DOS) รวมถึงการบล็อกผู้ใช้มิให้สามารถใช้งานคอมพิวเตอร์ได้โดยการแก้ไขรหัสผ่านที่ถูกต้อง หรือการกระตุ้นเตือนว่ามีการโจมตีโดยรูปแบบของDos โดยไม่มีการโจมตีจริงๆ หรือการจำกัดมิให้ผู้ใดสามารถใช้คอมพิวเตอร์ได้ การโจมตีในรูปแบบแสปม(Spam)ถือเป็นการโจมตีแบบDosที่พบมากที่สุดโดยวิธีการส่งอีเมล์จำนวนมากหรือส่งข้อความที่ไม่ต้องการ (Unsolicite e-mail)ให้แก่ผู้ใช้บริการอินเทอร์เน็ตจำนวนมาก

---

[77] The Council of Europe Convention on Cybercrime : Article 5 - System interference: "...the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

5.การใช้อุปกรณ์โดยมิชอบ(Misuse of device)

การใช้อุปกรณ์โดยมิชอบ หมายถึง *"การผลิต ขาย จัดหาเพื่อใช้ นำเข้า แจกจ่ายหรือสร้างขึ้นโดยประการอื่น ซึ่ง :*

1.(a) อุปกรณ์ใดรวมถึงโปรแกรมคอมพิวเตอร์ที่ได้ออกแบบหรือดัดแปลง โดยมุ่งหมายที่จะใช้กระทำความผิดตามบทบัญญัติในมาตรา 2-5;

รหัสผ่าน รหัสเข้า หรือข้อมูลที่คล้ายคลึงกันโดยใช้เข้าสู่ระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วนโดยมุ่งหมายที่จะใช้กระทำความผิดตามบทบัญญัติในมาตรา 2-5, และ;

(b) การครอบครองซึ่งรายการใดๆ ที่ได้ระบุในข้อ (a)(1)(2)ข้างต้น โดยเจตนาที่จะใช้กระทำความผิดตามบทบัญญัติในมาตรา 2-5 ผู้ครอบครองมีความรับผิดตามกฎหมายหากได้ครอบครองรายการนั้นๆก่อนมีการยึดตามความรับผิดทางอาญา

2.จะต้องไม่ตีความมาตรานี้ ให้รวมถึงการผลิต ขาย จัดหาเพื่อใช้ นำเข้า แจกจ่ายหรือสร้างขึ้นโดยประการอื่น หรือครอบครองตามวรรคหนึ่งเป็นความผิดอาญา หากผู้กระทำไม่มีเจตนากระทำในการกระทำความผิดตามมาตรา2ถึง5ของอนุสัญญาฉบับนี้ เช่น การทดสอบโดยผู้มีอำนาจหรือป้องกันระบบคอมพิวเตอร์..."[78]

---

[78] The Council of Europe Convention on Cybercrime : Article 6 - Misuse of devices: "...the production, sale, procurement for use, import,distribution or otherwise making available of:

(a.) a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5;

a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Article 2-5, and;

(b.)the possession of an item referred to in paragraphs (a) (1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2-5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 .This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system..."

โดยการกระทำผิดลักษณะนี้ มุ่งประสงค์ในการลงโทษผู้ใช้อุปกรณ์หรือโปรแกรมคอมพิวเตอร์ในการกระทำผิด เช่น ไวรัสคอมพิวเตอร์หรือโปรแกรมมุ่งประสงค์ร้ายอื่นๆ หรือรหัสผ่าน(Password) หรือรหัสเข้า(Access code)หรือข้อมูลอื่นที่คล้ายกัน การครอบครอง ผลิต ขาย จัดหาเพื่อใช้ นำเข้า แจกจ่ายหรือสร้างขึ้นโดยประการอื่นโดยมีเจตนาที่จะใช้ในการกระทำผิด ถือเป็นการกระทำความผิดอาญา

อุปกรณ์คอมพิวเตอร์ ไวรัสและโปรแกรมมุ่งประสงค์ร้ายอื่น ที่ใช้เป็นเครื่องมือในการประกอบอาชญากรรมคอมพิวเตอร์ ถือเป็นอันตรายต่อเครือข่ายอินเทอร์เน็ตและระบบเศรษฐกิจที่ต้องสูญเสียค่าใช้จ่ายในการดูแลเครือข่ายอินเทอร์เน็ต ในหลายๆรัฐถือว่าผู้ครอบครองมีความผิดฐานนี้ก่อนพิจารณาความผิดฐานอื่นๆ

6.การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์(Computer-related forgery)

การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์ หมายถึง*"กระทำความผิดโดยเจตนาและปราศจากสิทธิ ในการป้อน แก้ไข การลบ ระงับ โดยกระทำต่อข้อมูลคอมพิวเตอร์ผลลัพธ์จากข้อมูลปลอมโดยมีความมุ่งหมายให้เข้าใจว่าเป็นข้อมูลที่แท้จริง ไม่ว่าข้อมูลนั้นจะสามารถอ่านได้โดยตรงหรือเข้าใจได้โดยง่ายหรือไม่ การพิจารณาความผิดฐานนี้จึงต้องพิจารณาจากเจตนาหลอกลวงหรือเจตนาทุจริตก่อนที่จะพิจารณาความรับผิดทางอาญา"*[79]

จุดมุ่งหมายของการบัญญัติฐานความผิดนี้เพราะในหลายประเทศมีกฎหมายคุ้มครองเอกสารที่สามารถมองเห็นได้หรือเอกสารที่มีรูปร่างเท่านั้น แต่ไม่รวมถึงข้อมูลคอมพิวเตอร์ด้วย จึงสมควรบัญญัติกฎหมายเฉพาะเพื่อเอาผิดกับผู้กระทำผิดประเภทนี้ เพราะข้อมูลคอมพิวเตอร์ก็มีความสำคัญในฐานะหลักฐานการแสดงสิทธิ(Evidence of any right)

---

[79] The Council of Europe Convention on Cybercrime : Article 7 – Computer-related forgery "...when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches."

ตัวอย่างเช่น การนำข้อมูลออกจากข้อมูลเดิม และการระงับข้อมูล (Suppression) เช่น การทำให้หยุด หรือปกปิดข้อมูล เพื่อหลอกลวงผู้อื่นให้เข้าใจว่าเป็นเอกสารที่แท้จริง หรือการโพสท์แถลงข่าวสารที่บิดเบือนเพื่อปรับเปลี่ยนราคาสินค้าในตลาด

การเผยแพร่ไฟล์คอมพิวเตอร์ปลอม หรือคอมพิวเตอร์เทมเพลท (Computer template)ปลอม ถือเป็นการกระทำที่ผิดกฎหมาย เช่น เทมเพลมที่ระบุข้อมูลปลอม ซึ่งโดยปกติแล้วจัดเก็บในรูปแบบของไฟล์รูปภาพ จึงสามารถแก้ไข ระบายสี และแบ่งแยกออกเป็นชั้นได้ โดยผู้กระทำผิดมีเจตนาจะให้คล้ายคลึงกับหน้าเว็บไซต์ของจริง

7. การฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์ (Computer-related fraud)

การฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์ หมายถึง *"กระทำความผิดโดยเจตนาและปราศจากสิทธิ ทำให้ผู้หนึ่งผู้ได้สูญเสียไปซึ่งทรัพย์สิน โดย*

a. การป้อน การแก้ไข การลบ ระงับซึ่งข้อมูลคอมพิวเตอร์,

b. การรบกวนการทำงานของระบบคอมพิวเตอร์,

ด้วยเจตนาหลอกลวงหรือเจตนาไม่สุจริต ปราศจากสิทธิ เพื่อให้ได้มาซึ่งผลประโยชน์ทางเศรษฐกิจแก่ผู้หนึ่งผู้ใดหรือผู้อื่น"[80]

การกระทำผิดฐานนี้เป็นการหลอกลวงโดยผ่านทางคอมพิวเตอร์ไม่ว่าวิธีการใด เพื่อให้ได้มาซึ่งเงิน ทรัพย์สิน หรือผลประโยชน์อื่นโดยเจตนาทุจริต ในหลายประเทศการฉ้อโกงถือเป็นความผิดดังเดิมตามประมวลกฎหมายอาญาอยู่แล้วจึงไม่มีความจำเป็นที่จะต้องบัญญัติกฎหมายใหม่ แต่สำหรับบางประเทศถือเป็นปัญหาทางกฎหมายที่ต้องบัญญัติความผิดฐานนี้ เช่นประเทศอังกฤษ

---

[80] The Council of Europe Convention on Cybercrime : Article 8 – Computer-related fraud "...when committed intentionally and without right, the causing of a loss of property to another person by:

a .any input, alteration, deletion or suppression of computer data,

b.any interference with the functioning of a computer system,with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."

เอกสารเผยแพร่เรื่องการฉ้อโกงทางคอมพิวเตอร์ของสำนักงานอัยการสูงสุดได้อธิบายว่า *"...ในกฎหมายอังกฤษจะไม่มีฐานความผิดประเภทที่ครอบคลุมเรื่องฉ้อโกง (Fraud) เป็นการทั่วไป หรือกล่าวอีกนัยหนึ่งว่าไม่มีความผิดฐานฉ้อโกงในกฎหมายอังกฤษ แม้ว่ามีฐานความผิดหลายๆฐานที่อาจถือได้ว่ามีเนื้อหาคล้ายเป็นส่วนหนึ่งหรือประเภทหนึ่งของการฉ้อโกง (ในทัศนะของกฎหมายอังกฤษ) เช่นความผิดฐานปลอมแปลง (ซึ่งอาจมีเจตนาหลอกลวงฉ้อฉลผู้อื่น) และความผิดฐานหลบเลี่ยงภาษี เป็นต้น แต่บทความผิดในฐานดังกล่าวก็เป็นเรื่องเฉพาะเจาะจงเกินกว่าที่จะถือได้ว่าเป็นบทความผิดฐานฉ้อโกง..."*[81] ดังนั้น ในประเทศซึ่งมีการบัญญัติฐานความผิดฉ้อโกงไว้แล้วจึงอาจปรับใช้ฐานความผิดเดิมกับการกระทำผิดในลักษณะนี้ได้

การฉ้อโกงบนอินเทอร์เน็ตอาจใช้วิธีการหลอกลวงในหลากหลายรูปแบบ เช่น การส่งคำเสนอปลอมหรือหลอกลวงซึ่งเกี่ยวข้องกับทรัพย์สิน สัญญา หรือแผนการลงทุนที่ไม่มีมูลความจริง ซึ่งอาจเป็นการฉ้อโกงบัตรเครดิต ฉ้อทางโกงเมล์(Mail fraud) หรือฉ้อโกงธนาคาร (Bank fraud)ฉ้อโกงสินค้า(Stock fraud)หรือฉ้อโกงระบบรักษาความปลอดภัยออนไลน์(Online securities fraud) โดยการใช้อินเทอร์เน็ตในการกำหนดราคาตลาดเอง โดยการสร้างให้ความต้องการในตลาดให้มากกว่าปริมาณสินค้า เพื่อให้สามารถขายสินค้าได้ในราคาสูง

เครื่องมือในการกระทำผิดนี้ได้แก่การส่งอีเมล์ที่ไม่ต้องการ (Unsolicite e-mail) จดหมายแจ้งข่าวอิเล็กทรอนิกส์(Electronic newsletters) ข้อความในกระดานสนทนาและเว็บไซต์(Message boards and websites) รวมถึง การฉ้อโกงป้ายราคา(Price tag fraud) โดยวิธีการเข้าไปแก้ไขเว็บไซต์ที่ค้าขายแบบE-commerceให้สินค้ามีราคาสูงขึ้น, การฉ้อโกงการประมูลออนไลน์(Online auction fraud) ซึ่งเป็นการฉ้อโกงบนอินเทอร์เน็ตที่เป็นที่รู้จักกันดี โดยใช้วิธีการ"Shell bidding" คือ การยื่นคำเสนอปลอมเพื่อสู้ราคาโดยผู้ขายและ/หรือผู้สมรู้ร่วมคิดเพื่อให้ผู้เข้าประมูลอื่นที่ต้องการสินค้าเข้าสู้ราคาส่งผลให้สินค้าที่ประมูลมีราคาสูงขึ้น

---

[81] ชาติ ชัยเดชสุริยะ สำนักงานวิชาการ (สำนักงานอัยการสูงสุด) , "กฎหมายและมุมมองเปรียบเทียบในประเทศอังกฤษและประเทศอื่นๆ" เอกสารเผยแพร่เรื่องการฉ้อโกงทางคอมพิวเตอร์ , www.tech.ago.go.th /doc/artical6.doc.

8.การกระทำความผิดเกี่ยวกับภาพลามกอนาจารเด็ก (Offences related to child pornography)

ความผิดฐานนี้กำหนดไว้ในอนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime) มาตรา 9 *"ความผิดเกี่ยวกับภาพเด็กในทางลามกอนาจาร...เมื่อมีการกระทำโดยเจตนาและปราศจากสิทธิสำหรับพฤติกรรมต่อไปนี้:*

a. การผลิตภาพเด็กในทางลามกอนาจารเพื่อวัตถุประสงค์ที่จะเผยแพร่ภาพนั้นผ่านระบบคอมพิวเตอร์

b. การเสนอหรือทำให้มีภาพเด็กในทางลามกอนาจารผ่านระบบคอมพิวเตอร์

c. การเผยแพร่หรือรับส่งภาพเด็กในทางลามกอนาจารผ่านระบบคอมพิวเตอร์

d. การผลิตภาพเด็กในทางลามกอนาจารผ่านระบบคอมพิวเตอร์ เพื่อบุคคลนั้นเอง หรือบุคคลอื่น;

e. การครอบครองภาพเด็กในทางลามกอนาจารในระบบคอมพิวเตอร์หรือในสื่อเก็บข้อมูลคอมพิวเตอร์

2. เพื่อวัตถุประสงค์ของวรรค 1 ข้างต้น คำว่า "ภาพเด็กในทางลามกอนาจาร" ให้หมายความรวมถึง สื่อลามกอนาจารที่แสดงภาพ:

a. ผู้เยาว์กระทำการแสดงพฤติกรรมทางเพศ;

b. บุคคลที่มีลักษณะเหมือนผู้เยาว์กระทำการแสดงพฤติกรรมทางเพศ

c. ภาพเหตุการณ์จริงที่ผู้เยาว์กระทำการแสดงพฤติกรรมทางเพศ

3.เพื่อวัตถุประสงค์ของวรรค 2 ข้างต้น คำว่า "ผู้เยาว์" ให้หมายความรวมถึงบุคคลทุกคนที่อายุต่ำกว่า 18 ปี อย่างไรก็ตาม รัฐภาคีอาจกำหนดเกณฑ์อายุ ที่ต่ำกว่านั้นได้ แต่ต้องไม่ต่ำกว่า 16 ปี..."

นอกจากฐานความผิดที่ได้กล่าวมาแล้วทั้ง 8 ฐานความผิด ยังมีการกำหนดฐานความผิดอื่นๆไว้ในอนุสัญญาฉบับนี้ด้วย ซึ่งขอกล่าวไว้โดยสรุป ได้แก่ ความผิดอันเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิเกี่ยวเนื่อง(Offences related to infringements of copyright and related

rights)[82] ที่มุ่งเอาผิดกับการละเมิดทรัพย์สินทางปัญญา, ความผิดฐานพยายามและช่วยเหลือหรือสนับสนุน(Attempt and aiding or abetting)[83] ที่มุ่งเอาผิดกับผู้พยายามกระทำความผิด หรือผู้ช่วยเหลือหรือสนับสนุนการกระทำผิดอื่นตามอนุสัญญานี้ นอกจากนี้ยังกำหนดให้นิติบุคคลร่วมรับผิดกับผู้กระทำผิดที่เป็นบุคคลธรรมดา[84] โดยแต่ละรัฐจะต้องบัญญัติกฎหมายให้มีประสิทธิภาพ ได้สัดส่วนและมีสภาพบังคับที่เหมาะสม โดยพิจารณาการจำกัดเสรีภาพอย่างเหมาะสม[85]

การจำแนกลักษณะการบัญญัติกฎหมายในต่างประเทศ

การบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ในต่างประเทศสามารถจำแนกได้เป็น 3 ลักษณะคือ[86]

1. การแก้ไขประมวลกฎหมายอาญา อาทิ ประเทศเยอรมัน แคนาดา ออสเตรเลีย อิตาลี สวิตเซอร์แลนด์ เดนมาร์ค ญี่ปุ่น

2. การบัญญัติเป็นกฎหมายเฉพาะ อาทิ ประเทศอังกฤษ สิงคโปร์ มาเลเซีย จีน อิสราเอล

3. บัญญัติรวมอยู่ในกฎหมายเทคโนโลยีสารสนเทศอื่นๆ อาทิ ประเทศฟิลิปปินส์ อินเดีย

---

[82] The Council of Europe Convention on Cybercrime : Article 10 – Offences related to infringements of copyright and related rights

[83] The Council of Europe Convention on Cybercrime : Article 11 – Attempt and aiding or abetting

[84] The Council of Europe Convention on Cybercrime : Article 12 – Corporate liability

[85] The Council of Europe Convention on Cybercrime : Article 13 – Sanctions and measures

[86] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "คำถามที่พบบ่อย เกี่ยวกับร่างพรบ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์", http://wiki.nectec.or.th.

ตารางที่ 2.2 กฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ในต่างประเทศ[87]

ออสเตรเลีย	ประมวลกฎหมายอาญา : Part VIA - Offences Relating To Computers and Copyrights Act.
บราซิล	กฎหมายลำดับที่ 9,983 (แก้ไขประมวลกฎหมายอาญา ปีค.ศ.2000)
แคนาดา	แก้ไขประมวลกฎหมายอาญา
ชิลี	Law Relative to Information/Computer Crimes.
จีน	Computer Information Network and Internet Security, Protection and Management Regulations.
สาธารณรัฐเช็ก	ประมวลกฎหมายอาญา : §152 -Infringement of copyright § 182 - Impairing and endangering the operation of public utility facilities § 249 - Unauthorized use of other people's articles § 257a - Damaging and misusing records in information stores § 250- Fraud §150 - Infringing trademark rights §151 - Infringing industrial rights §152 - Infringing copyright.
เดนมาร์ก	Legislation Electronic crime and data crime. กำหนดฐานความผิดเกี่ยวกับ Access, copyright infringements, appropriation of information (trade secrets, hacking etc.), offences in respect of electronic means of payment, forgery of electronic documents, and computer vandalism.
สาธารณรัฐเอสโตเนีย	Legislation Computer and Work Place Related Crimes.
อินเดีย	Information Technology Act,2000.
สิงคโปร์	Computer Misuse Act
ญี่ปุ่น	Unauthorized Computer Access Law,2000.

[87] http://www.mcconnellinternational.com/services/Updatedlaws.htm.

มาเลเซีย	The Computer Crime Act ,1997.
มอริเชียส	Information Technology Act 1998. Section 4: Criminal Code Amended. 369A. Computer Misuse. Tele- communications Act 1998. Copyright Act 1997.
เปรู	แก้ไขประมวลกฎหมายอาญา
ฟิลิปปินส์	Electronic Commerce Act.
โปแลนด์	แก้ไขประมวลกฎหมายอาญา, 1997. Personal Data Protection Act, 1997.
สเปน	แก้ไขประมวลกฎหมายอาญา
ตุรกี	แก้ไขประมวลกฎหมายอาญา
สหราชอาณาจักร	Computer Misuse Act, 1990. Data Protection Acts, 1994 & 1998. Telecommunications (Fraud) Act, 1997. Copyright, Designs and Patents Act, 1998.
สหรัฐอเมริกา	18 USC §1029 Fraud and Related Activity in Connection with Access §1030 Fraud and Related Activity in Connection with Computers §1362 Communication Lines, Stations, or Systems §2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited, §2701 Unlawful Access to Stored Communications §2702 Disclosure of Contents §2703 Requirements for Governmental Access, and No Electronic Theft Act .

ตารางที่ 2.3 แสดงการเปรียบเทียบกฎหมายของประเทศต่างๆ[88]

ประเทศ	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network sabotage	Unauthorized Access	Virus Dissemination	Aidding& Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
ออสเตรเลีย	✔	✔	✔	✔		✔			✔	✔
บราซิล		✔			✔	✔		✔		
แคนาดา	✔	✔	✔	✔	✔	✔	✔			✔
ชิลี	✔	✔	✔	✔	✔					
จีน		✔		✔			✔			
สาธารณรัฐเช็ก		✔	✔		✔	✔				✔
เดนมาร์ก		✔		✔						✔
สาธารณรัฐเอสโตเนีย		✔	✔	✔	✔	✔	✔	✔		✔
อินเดีย		✔	✔	✔	✔	✔	✔	✔		✔
ญี่ปุ่น	✔	✔	✔	✔	✔	✔		✔	✔	✔
มาเลเซีย		✔				✔		✔		✔
มอริเชียส	✔	✔		✔	✔	✔	✔	✔	✔	

[88] McConnell International,Cyber Crimes ...and Punishment?Archaic Laws Treaten Global Information. http://www.mcconellinternational.com

เปรู	✔	✔	✔	✔	✔	✔				✔
ฟิลิปปินส์	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
โปแลนด์		✔	✔	✔				✔		
สเปน	✔	✔	✔					✔		✔
ตุรกี		✔	✔	✔	✔		✔	✔	✔	✔
สหราช อาณาจักร		✔		✔	✔	✔		✔		
สหรัฐอเมริกา	✔	✔	✔	✔	✔	✔	✔	✔		✔

<u>คำอธิบายข้อมูลตามตาราง</u>

Data Interception : การดักข้อมูลคอมพิวเตอร์ในการส่งข้อมูล

Data Modification : การแก้ไข,การทำลายหรือลบข้อมูล

Data Theft : การเอาไปหรือทำสำเนา,โดยไม่คำนึงว่าได้รับการคุ้มครองตามกฎหมายอื่นหรือไม่ เช่น กฎหมายลิขสิทธิ์,ความลับทางการค้าและกฎหมายอื่นๆ

Network Interference : การสร้างอุปสรรคหรือขัดขวางผู้อื่นในการเข้าสู่เครือข่าย,ตัวอย่างของการกระทำผิดประเภทนี้เช่น การโจมตีแบบDos(Denial of service),การสร้างข้อมูลให้ท่วมเว็บไซต์หรือท่วมระบบของผู้ให้บริการอินเทอร์เน็ตโดยวิธีการFlood(การเข้าถึงเป้าหมายซ้ำแล้วซ้ำเล่าเพื่อที่จะทำให้เกินความสามารถในการจุของเป้าหมายนั้น (overload))

Network sabotage : การดัดแปลงหรือทำลายระบบหรือเครือข่าย

Unauthorized Access : การ"Cracking"หรือ"Hacking"เพื่อเข้าสู่ข้อมูลหรือระบบ

Virus Dissemination : การเผยแพร่Softwareสำหรับทำลายข้อมูลหรือระบบ

Aidding & Abetting Cyber Crimes : การช่วยเหลือหรือสนับสนุนการกระทำผิดอาชญากรรมคอมพิวเตอร์

Computer-Related Forgery : การแก้ไขข้อมูลโดยเจตนานำเสนอข้อมูลนั้นอย่างข้อมูลที่แท้จริง

Computer-Related Fraud : การแก้ไขข้อมูลโดยเจตนาที่จะได้มาซึ่งผลประโยชน์ทางเศรษฐกิจจากการกระทำที่มิชอบ

2.4.2 กฎหมายสารบัญญัติของประเทศไทย

กฎหมายอาญามีเอกลักษณ์ที่แตกต่างจากกฎหมายอื่นๆ เช่น กฎหมายแพ่ง เนื่องจากกฎหมายอาญามีผลกระทบต่อชีวิต ร่างกาย เสรีภาพ และทรัพย์ของประชาชน หลักการสำคัญประการหนึ่งของกฎหมายอาญา คือ หลัก "ไม่มีความผิด ไม่มีโทษ หากไม่มีกฎหมาย" ซึ่งมาจากหลักในภาษาลาตินที่ว่า "Nullum crimem nulla poena sine lege"แปลเป็นภาษาอังกฤษว่า "No crime nor punishment with out law"หรือในภาษาอังกฤษเรียกหลักนี้ว่า "Priciple of legality"[89] ในประเทศไทยบัญญัติหลักการนี้ไว้ใน ประมวลกฎหมายอาญามาตรา 2 *"บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการ อันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนด โทษไว้และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย..."* ซึ่งหลักการนี้เป็นหลักการสากลอันเป็นที่ยอมรับกันในนานาอารยประเทศซึ่งแยกพิจารณาได้ ดังนี้

1) ผู้กระทำไม่ต้องรับผิดในทางอาญาหากการกระทำนั้นไม่มีกฎหมายบัญญัติในขณะกระทำว่าเป็นความผิดและกำหนดโทษไว้

2) กฎหมายอาญาจะย้อนหลังให้ผลร้ายมิได้

3) ถ้อยคำในกฎหมายอาญาจะต้องบัญญัติให้ชัดเจนแน่นอนปราศจากความคลุมเครือ

4) กฎหมายอาญาต้องตีความโดยเคร่งครัด

เนื่องจากการลงโทษทางอาญาแก่ผู้กระทำผิดจะต้องใช้กฎหมายที่บัญญัติไว้ในขณะกระทำความผิด ดังนั้น ในขณะที่ยังไม่มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงจำเป็นต้องใช้ประมวลกฎหมายอาญาและกฎหมายอื่นที่มีโทษทางอาญามาปรับใช้แก่กรณีเท่าที่ปรับใช้ได้[90] เนื่องมาจากหลักการข้างต้นที่ว่า "ผู้กระทำไม่ต้องรับผิดในทางอาญาหากการกระทำนั้นไม่มีกฎหมายบัญญัติในขณะกระทำว่าเป็นความผิดและกำหนดโทษไว้"และ "กฎหมายอาญาต้องตีความโดยเคร่งครัด" ดังที่ได้กล่าวมาแล้วข้างต้น ดังนั้น

---

[89] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค1,พิมพ์ครั้งที่ 4(กรุงเทพ: หจก.จิรรัชการพิมพ์, 2549), หน้า16-17.

[90] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "คำถามที่พบบ่อย เกี่ยวกับร่าง พรบ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์", http://wiki.nectec.or.th.

กฎหมายกฎหมายสารบัญญัติที่กำหนดโทษเกี่ยวกับความผิดที่กระทำบนอินเทอร์เน็ตในช่วงก่อนที่จะบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 คือ

1) ประมวลกฎหมายอาญา

2) กฎหมายอื่นที่มีโทษทางอาญา เช่น พระราชบัญญัติความลับทางการค้า พ.ศ. 2545 พระราชบัญญัติลิขสิทธิ์ พ.ศ.2537 เป็นต้น

อย่างไรก็ดีการใช้ประมวลกฎหมายอาญาและกฎหมายอื่นที่มีโทษทางอาญามาปรับใช้กับการกระทำความผิดบนอินเทอร์เน็ตอาจมีข้อจำกัด เพราะกฎหมายอาญามุ่งเน้นที่จะคุ้มครองทรัพย์ที่มีรูปร่าง (Tangible Object) โดยมิได้มุ่งเน้นที่จะคุ้มครองข้อมูลที่เป็นวัตถุไม่มีรูปร่าง (Intangoble Object) ซึ่งมีคำพิพากษาฎีกาของไทยที่แสดงให้เห็นว่าการนำประมวลกฎหมายอาญามาปรับใช้อาจเกิดปัญหาเพราะประมวลกฎหมายอาญาไม่คุ้มครองข้อมูลที่เป็นวัตถุไม่มีรูปร่าง (Intangoble Object) จึงไม่สามารถลงโทษผู้กระทำความผิดในฐานลักทรัพย์ได้ เพราะข้อมูลไม่ถือเป็นทรัพย์[91]

การนำกฎหมายอาญามาปรับใช้ยังมีปัญหาว่าจะสามารถนำฐานความผิดเกี่ยวกับเอกสาร มาตีความให้รวมถึงข้อมูลคอมพิวเตอร์ได้หรือไม่ เพราะตามประมวลกฎหมายอาญา มาตรา 1(7) "เอกสาร" หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นจะเป็นโดย วิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น หากเป็นข้อมูลที่มีการPrint out ออกมาย่อมถือว่าเป็นเอกสารได้ แต่กรณีนี้เป็นปัญหาว่าเอกสารจะหมายรวมถึงข้อมูลที่เก็บอยู่ในระบบคอมพิวเตอร์ด้วยหรือไม่ หากมีการปลอมแปลงข้อมูลในระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต นอกจากนี้

---

[91] คำพิพากษาฎีกาที่ 5161/2547 "ข้อมูล ตามพจนานุกรมให้ความหมายว่า ข้อเท็จจริง หรือ สิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ ส่วนข้อเท็จจริง หมายความว่า ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่จริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง ดังนั้น ข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูล โดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อ ป.พ.พ. มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์"

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์บางประเภท เช่น ความผิดฐานการเข้าถึงคอมพิวเตอร์โดยมิชอบ(Illegal access) ก็ไม่อาจปรับเข้ากับความผิดฐานบุกรุกได้ จึงมีแนวคิดว่าควรมีกฎหมายใหม่ที่ไม่กระทบต่อโครงสร้างประมวลกฎหมายอาญา เพียงแต่กฎหมายที่ได้บัญญัติใหม่นี้จะต้องช่วยอุดช่องว่างของประมวลกฎหมายอาญาที่ไม่ได้กำหนดฐานความผิดที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ไว้เป็นการเฉพาะ

สาเหตุสำคัญที่ประเทศไทยเลือกใช้การออกกฎหมายเฉพาะในลักษณะพระราชบัญญัติแทนการแก้ไขประมวลกฎหมายอาญาเพราะการแก้ไขประมวลกฎหมายอาญาทำได้ยาก จำเป็นต้องใช้เวลานาน จึงอาจไม่ทันต่อการกระทำผิดในรูปแบบใหม่ อีกทั้งการดำเนินคดีกับผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ จำเป็นต้องมีกฎหมายวิธีพิจารณาเป็นพิเศษเพื่อให้เกิดความคล่องตัวในการดำเนินคดีกับผู้กระทำความผิดได้อย่างทันท่วงทีและจำเป็นต้องมีการบัญญัติกฎหมายให้อำนาจหน้าที่กับเจ้าพนักงานเป็นพิเศษด้วย จึงเป็นการยากและใช้เวลานานในการแก้ไขประมวลกฎหมายอาญาและประมวลกฎหมายวิธีพิจารณาความอาญาไปพร้อมๆกัน

ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

พระราชบัญญัติฉบับนี้ ในขณะอยู่ในชั้นร่างเคยใช้ชื่อว่า "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ..." แต่ด้วยเหตุที่ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์มิได้มีแต่บทบัญญัติว่าด้วยอาชญากรรมคอมพิวเตอร์ทั้งหมด แต่ยังมีบทบัญญัติความผิดบางประการที่มิใช่อาชญากรรมทางคอมพิวเตอร์โดยแท้ เช่น ความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารเด็ก (Child pornography) หรือการตัดต่อภาพผู้อื่นให้ได้รับความเสียหายด้วย ตลอดจนมีบทบัญญัติเอาผิดกับพนักงานเจ้าหน้าที่ที่ใช้อำนาจเกินของเขตด้วย ในการพิจารณาของคณะกรรมการกฤษฎีกา จึงได้แก้ไขชื่อเป็น"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ..."[92] เพื่อให้ครอบคลุมทั้งกรณีที่คอมพิวเตอร์ถูกใช้

---

[92] "บันทึกการประชุมคณะกรรมการกฤษฎีกา(คณะพิเศษ) เรื่องร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ... ครั้งที่1/2547" 16 มกราคม 2547

เป็นเครื่องมือ(A tool) เป็นเป้าหมาย(A target) หรือ เป็นพื้นที่ในการกระทำผิดด้วย(A place of criminal activities)[93]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดฐานความผิดเกี่ยวกับ การกระทำผิดเกี่ยวกับการรักษาความลับ (Confidential)ความครบถ้วน (Integrity) ความปลอดภัย (Security)และความพร้อมหรือเสถียรภาพในการใช้งาน (Availability)ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ และการเผยแพร่ข้อมูลที่ไม่เหมาะสมในระบบคอมพิวเตอร์ ดังที่ปรากฏในกำหนดฐานความผิดต่างๆตามพระราชบัญญัติดังกล่าว ดังต่อไปนี้[94]

1.) **การเข้าถึงโดยมิชอบ**(Illegal access/Unauthorized access) **(มาตรา 5, 6 และ7)**[95]

การกระทำความผิดฐานเข้าถึงโดยมิชอบหรือโดยไม่มีอำนาจหรือโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมายนี้ อาจเกิดขึ้นหลายวิธี เช่น การเจาะระบบ (hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) ซึ่งการกระทำเช่นว่านี้เป็นการขัดขวางการใช้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยชอบของบุคคลอื่น อันอาจทำให้เกิดการ

---

[93] สุนทร เปลี่ยนสี, "แนวความคิด หลักการและสาระสำคัญของร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์," วารสารกฎหมายปกครอง เล่ม24,ตอน2: หน้า102-103.

[94] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 21-33.

[95] มาตรา 5 "ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ"

มาตรา 6 "ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

มาตรา 7 "ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ"

เปลี่ยนแปลงแก้ไข หรือทำลายข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ได้ อีกทั้งความผิดฐานนี้ยังอาจเป็นที่มาของการกระทำความผิดฐานอื่นต่อไป เช่น การใช้คอมพิวเตอร์เพื่อฉ้อโกงหรือปลอมเอกสาร เป็นต้น

คำว่า "การเข้าถึง (access)" ในที่นี้ หมายความถึง การเข้าถึง ทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายรวมถึง การเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ และ"การเข้าถึง" ในที่นี้ยังหมายความถึง การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์

ส่วนวิธีการเข้าถึงนั้นไม่จำกัดว่าเป็นการเข้าถึงด้วยวิธีการใด ไม่ว่าจะเป็นการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน และยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าด้วยกัน นอกจากนี้ ยังหมายความรวมถึงการเข้าถึงโดยการติดต่อต่อสื่อสารแบบ ไร้สาย (Wireless communication) อีกด้วย[96]

"การเข้าถึง" ซึ่งถือว่าเป็นความผิดฐานนี้ จะต้องเป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบ (without right) ด้วย ซึ่งหมายความว่า หากผู้ทำการเข้าถึงนั้นเป็นบุคคลที่มีสิทธิเข้าถึงไม่ว่าด้วยถือสิทธิตามกฎหมายหรือได้รับอนุญาตจากเจ้าของระบบ ตัวอย่างเช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บ (Webmaster) ย่อมไม่เป็นความผิด อย่างไรก็ตาม หากผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้น ได้เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับอนุญาต ใน

---

[96] พรเพชร วิชิตชลชัย , คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ,(กรุงเทพ: สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม, 2550), หน้า 8.

กรณีนี้บุคคลดังกล่าวก็ย่อมต้องรับผิดเช่นเดียวกัน เพราะถือว่าเป็นการเข้าถึงโดยปราศจากอำนาจโดยชอบนั่นเอง ซึ่งตัวอย่างของกฎหมายที่ระบุถึงกรณีการเข้าถึงเกินกว่ากรณีที่ตนได้รับอนุญาตแล้วต้องรับผิดได้แก่ สหรัฐอเมริกา (Computer Fraud and Abuse Act 1986 18 U.S.C. Section 1030 (a)(1)-(3))

สาเหตุที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้การเข้าถึงระบบคอมพิวเตอร์หรือ ข้อมูลคอมพิวเตอร์จะต้องเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ เนื่องจากพิจารณาเห็นว่า การเข้าถึงหรือระบบหรือข้อมูลที่บุคคลผู้เป็นเจ้าของมิได้มีเจตนาหวงแหนหรือเจตนาป้องกันไว้ก็ไม่น่าที่จะกำหนดเป็นโทษทางอาญา[97]

ส่วนเหตุที่ไม่ระบุถึงมาตรการการป้องกันการเข้าถึงโดยเฉพาะว่าเป็นมาตรการชนิดใดชนิดหนึ่งเป็นการเฉพาะนั้น เนื่องมาจากมาตรการของแต่ละบุคคลหรือของแต่ละองค์กรนั้นมีมาตรการและระดับมาตรฐานในการป้องกันแตกต่างกัน นอกจากนี้ การที่ไม่ระบุมาตรการป้องกันการเข้าถึงโดยเฉพาะไว้ในกฎหมายก็ย่อมจะทำให้กฎหมายมีลักษณะยืดหยุ่นสอดคล้องกับแนวทางการบัญญัติกฎหมายเพื่อให้มีความเป็นกลางทางเทคโนโลยี (Technology Neutrality) ซึ่งจะทำให้สามารถปรับใช้กฎหมายได้แม้ว่าเทคโนโลยีจะเปลี่ยนแปลงไปมากน้อยเพียงใดก็ตาม

---

[97] สุนทร เปลี่ยนสี, "แนวความคิด หลักการและสาระสำคัญของร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์," วารสารกฎหมายปกครอง, หน้า 108.

2.) **การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (Illegal interception) (มาตรา 8)**[98]

พระราชบัญญัตินี้ตามมาตรา 8 บัญญัติฐานความผิดเกี่ยวกับการลักลอบดักข้อมูลโดยฝ่าฝืนกฎหมาย (Illegal interception) เนื่องจากมีวัตถุประสงค์เพื่อคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร (The right of privacy of data communication) ทำนองเดียวกับการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบเดิมที่ห้ามดักฟังหรือแอบบันทึกการสนทนาทางโทรศัพท์ ตัวอย่างของการกระทำผิดประเภทนี้ เช่น การใช้โปรแกรมจำพวก Spyware, Sniffer หรือ Trojan horse ในการลักลอบดูพฤติกรรมการใช้คอมพิวเตอร์ของผู้อื่น หรือการลักลอบดักเก็บข้อมูลจากแป้นพิมพ์คอมพิวเตอร์ของผู้อื่น เป็นต้น

การดักข้อมูลในมาตรานี้ หมายถึง การดักข้อมูลโดยวิธีการทางเทคนิค (Technical means) เพื่อลักลอบดักฟัง (Listen) ตรวจสอบ (Monitoring) หรือติดตามเนื้อหาสาระของข่าวสาร (Surveillance) ที่สื่อสารถึงกันระหว่างบุคคล หรือเป็นการกระทำ เพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์ หรือการทำให้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลที่สื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ โดยไม่คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่ เพราะบางกรณีอาจใช้อุปกรณ์เช่นว่านั้นเพื่อบันทึกการสื่อสารข้อมูลที่ได้ส่งผ่านด้วยวิธีการแบบไร้สายก็ได้ เช่น การติดต่อผ่านทางโทรศัพท์เคลื่อนที่ การติดต่อโดยใช้เทคโนโลยีไร้สายประเภท Wireless LAN เป็นต้น ซึ่งนอกจากการใช้อุปกรณ์อิเล็กทรอนิกส์เพื่อบันทึกข้อมูลที่มีการส่งผ่านกันแล้ว ยังรวมถึงกรณีการใช้ซอฟต์แวร์ หรือรหัสผ่านต่างๆ เพื่อทำการแอบบันทึกข้อมูลที่ส่งผ่านถึงกันด้วย

อย่างไรก็ตาม การใช้วิธีการต่างๆ ที่ถือว่าเป็นการดักข้อมูลโดยวิธีการทางเทคนิคข้างต้นนั้น จะต้องเป็นการกระทำต่อ ข้อมูลคอมพิวเตอร์ที่มิใช่ข้อมูลที่ส่งผ่านโดยเปิดเผยให้สาธารณชนสามารถรับรู้ได้ (Non- public transmissions) หากเป็นข้อมูลที่มีไว้เพื่อ

---

[98] มาตรา 8 "ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ"

ประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ (Public transmissions) การดักข้อมูลเหล่านั้นย่อมไม่เป็นความผิด เนื่องจากการกระทำความผิดฐานนี้จำกัดเฉพาะแต่เพียงวิธีการส่งที่ผู้ส่งข้อมูลประสงค์จะส่งข้อมูลนั้นให้แก่บุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจงเท่านั้น แม้ว่าจะเป็นการข้อมูลผ่านทางเครือข่ายสาธารณะ เช่น การส่งผ่านทางอินเทอร์เน็ต เป็นต้น กล่าวคือไม่ว่าข้อมูลดังกล่าวจะเป็นข้อมูลที่เจ้าของข้อมูลหรือผู้ทำการส่งผ่านข้อมูลต้องการเก็บรักษาข้อมูลไว้เป็นความลับ อาทิ ความลับทางการค้า หรือเป็นข้อมูลที่รู้หรือเปิดเผยเป็นการทั่วไปของประชาชนก็ตาม ดังนั้น จึงอาจกล่าวได้ว่า มาตรานี้ไม่ได้มีประเด็นที่ต้องพิจารณาถึงเนื้อหาสาระของข้อมูลที่ส่งแต่อย่างใด หากแต่พิจารณาว่าผู้ส่งต้องการส่งเป็นความลับหรือไม่เป็นสำคัญ

องค์ประกอบสำคัญอีกประการหนึ่งของความผิดฐานนี้คือ จะต้องเป็นการดักข้อมูลโดยมิชอบ กล่าวคือ กระทำโดยเจตนาและปราศจากสิทธิ โดยชอบ (Without right) ที่ให้สามารถกระทำได้ ไม่ว่าสิทธิดังกล่าวจะเกิดขึ้นโดยผลของกฎหมายหรือข้อตกลง

ตัวอย่างของการดักข้อมูลที่ถือว่าเป็นการกระทำโดยชอบ ได้แก่

1) การดักข้อมูลนั้นเป็นการกระทำโดยชอบด้วยกฎหมายตามที่กฎหมายบัญญัติ เพื่อประโยชน์ด้านความมั่นคงหรือการสืบสวนการกระทำความผิดโดยหน่วยงานที่มีอำนาจสอบสวน ตัวอย่างเช่น การเข้าถึงข้อมูลที่อยู่ในระหว่างการสื่อสารโดยอาศัยอำนาจตามพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 (แก้ไข พ.ศ. 2545) มาตรา 14 จัตวา , พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46

2) การดักข้อมูลนั้นเป็นการกระทำโดยบุคคลที่มีอำนาจให้กระทำได้ โดยบุคคลดังกล่าวได้ปฏิบัติตามคำสั่งหรือโดยได้รับอนุญาตจากผู้มีส่วนเกี่ยวข้องกับการส่งข้อมูล และรวมถึงกรณีการได้รับอนุญาตให้ทำการดักข้อมูลเพื่อทดสอบระบบการรักษาความปลอดภัยด้วย เช่น การว่าจ้างให้ตรวจสอบข้อมูลใดๆก่อนส่งให้กับผู้ต้องการข้อมูล เพื่อตรวจสอบว่าข้อมูลคอมพิวเตอร์เหล่านั้นติดไวรัสหรือไม่

อนึ่ง หากพิจารณาลักษณะการกระทำความผิดฐานลักลอบดัก ข้อมูล และลักษณะการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือ ข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจนั้น จะเห็นได้ว่าค่อนข้างใกล้เคียงกันอย่างยิ่ง แต่ข้อที่ทำให้บทบัญญัติทั้งสามมาตรามี

ความแตกต่างกัน ก็คือ การกระทำความผิดฐานลักลอบดักข้อมูลเป็นการกระทำโดยมีมูลเหตุจูงใจเพื่อให้ได้ล่วงรู้ข้อมูลคอมพิวเตอร์ ส่วนการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจนั้น แม้กระทำโดยมิได้มีเจตนาต่อข้อมูลคอมพิวเตอร์หรือโปรแกรมหรือระบบคอมพิวเตอร์ใดโดยเฉพาะเจาะจง และแม้ไม่มีความเสียหายใดๆ เกิดขึ้น ผู้กระทำก็ต้องรับผิดในการกระทำดังกล่าว

3.) **การทำให้ข้อมูลคอมพิวเตอร์เสียหาย** (Data interference) **(มาตรา 9)**[99]

มาตรา 9 กำหนดขึ้นเพื่อให้ข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองเช่นเดียวกับทรัพย์ที่มีรูปร่าง (Tangible Object) โดยมีเจตนาที่จะก่อความเสียหายต่อประโยชน์ที่กฎหมายมุ่งประสงค์จะคุ้มครอง คือ ความครบถ้วนถูกต้องของข้อมูล (Integrity) และเสถียรภาพหรือความพร้อมในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้อย่างเป็นปกติ

ความผิดฐานนี้ถือเป็นความผิดสำคัญ เพราะเป็นพื้นฐานไปสู่การกระทำผิดฐานอื่นๆได้มากมาย เพราะการที่จะกระทำความผิดฐานอื่นๆได้ต้องอาศัยการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมข้อมูลคอมพิวเตอร์ที่เป็นเป้าหมายในการกระทำผิดก่อนทั้งสิ้น[100]

ฐานความผิดตามมาตรา 9 เป็นบทบัญญัติที่ลงโทษบุคคลซึ่งทำความเสียหาย หรือทำให้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์เสื่อมค่าหรือไร้ประโยชน์ รวมถึงการลบหรือทำลายข้อมูลคอมพิวเตอร์ หรือกระทำการใดๆ ให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์หรือใช้โปรแกรมคอมพิวเตอร์นั้นได้ รวมทั้งการเปลี่ยนแปลงข้อมูลใดๆ ด้วย

---

[99] มาตรา 9 "ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ"

[100] สุนทร เปลี่ยนสี, "แนวความคิด หลักการและสาระสำคัญของร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์," วารสารกฎหมายปกครอง, หน้า 109.

อย่างไรก็ตาม การกระทำซึ่งจะเป็นความผิดฐานรบกวนข้อมูลคอมพิวเตอร์นั้นจะต้องเป็นการกระทำโดยปราศจากสิทธิโดยชอบ (With out right) ให้สามารถกระทำได้ด้วย ดังนั้น หากเป็นการกระทำโดยบุคคลผู้มีสิทธิก็จะไม่เป็นการกระทำความผิดในฐานนี้ ตัวอย่างเช่น[101]

1) การทดสอบหรือรักษาความมั่นคงเพื่อความปลอดภัยของระบบคอมพิวเตอร์โดยบุคคลผู้ได้รับมอบอำนาจจากผู้เป็นเจ้าของระบบคอมพิวเตอร์ (Owner) หรือผู้ปฏิบัติการ (operator)

2) การปรับแก้ระบบปฏิบัติ (Operating system) ของคอมพิวเตอร์โดยผู้ปฏิบัติการ (operator) ก่อนติดตั้งซอฟต์แวร์ใหม่ๆ (ตัวอย่างเช่น การติดตั้งซอฟต์แวร์เพื่อการเชื่อมต่ออินเทอร์เน็ตซึ่งจะมีผลให้ระบบคอมพิวเตอร์ทำงานไม่เป็นปกติทั้งก่อนและหลังได้ติดตั้งโปรแกรม

3) การเปลี่ยนแปลงข้อมูลจราจรทางคอมพิวเตอร์(Traffic data) เพื่อประโยชน์ในการสื่อสารแบบไม่ระบุชื่อ ตัวอย่างเช่น การสื่อสารผ่านระบบ Anonymous remailer systems

4) การเปลี่ยนแปลงข้อมูลเพื่อการรักษาความลับและความปลอดภัยของการสื่อสาร อาทิ การเข้ารหัสข้อมูล (Encryption)

ตัวอย่างของการกระทำความผิดในฐานนี้ เช่น การปล่อยไวรัสคอมพิวเตอร์ และ รวมถึงโปรแกรมหรือคำสั่ง(Code)ใดๆที่ทำให้คอมพิวเตอร์ทำงานไม่ถูกต้องสมบูรณ์ เช่น โปรแกรมมุ่งประสงค์ร้าย(Malware) และ Logic bomb เป็นต้น

หากการกระทำตามมาตรา 9 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ของบุคคลทั่วไปหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์ที่มีความสำคัญตามมาตรา 12[102] ย่อมได้รับโทษหนักขึ้น

---

[101] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 30.

[102] มาตรา 12 "ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี"

4.) ความผิดฐานรบกวนการทำงานของระบบคอมพิวเตอร์(System interference) (มาตรา10)[103]

มาตรานี้มีวัตถุประสงค์เพื่อ คุ้มครองการทำงานของระบบคอมพิวเตอร์และระบบการติดต่อสื่อสารให้เป็นไปตามปกติ โดยกำหนดบทลงโทษสำหรับการรบกวนหรือขัดขวางการทำงานของระบบคอมพิวเตอร์ ซึ่งการรบกวนหรือขัดขวางหรือทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกตินั้น อาจเกิดขึ้นในขั้นตอนต่างๆ ตั้งแต่การป้อนข้อมูลเข้าไปในระบบหรือในการส่ง ทำลาย ลบ หรือเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งผลของการกระทำความผิดมาตรา 10 จะก่อให้เกิดความเสียหายที่ร้ายแรงหรือรุนแรงต่อการใช้ระบบดังกล่าวหรือต่อการติดต่อสื่อสารกับระบบอื่น

ตัวอย่างของการกระทำผิดฐานนี้ เช่น การทำให้คอมพิวเตอร์ปฏิเสธการทำงาน (Denial of service) หรือทำให้ระบบคอมพิวเตอร์ทำงานได้ช้าลงโดยการป้อนไวรัสคอมพิวเตอร์ หรือการรบกวนระบบของผู้รับข้อมูลคอมพิวเตอร์โดยวิธีการส่งอีเมล์จำนวนมากหรือส่งข้อความที่ไม่ต้องการ (Unsolicite e-mail)ไปยังผู้รับเพื่อให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้(Run out of memory)

หากการกระทำตามมาตรา 10 เป็นการกระทำต่อระบบคอมพิวเตอร์สำคัญตามที่กำหนดไว้ในมาตรา 12 ผู้กระทำผิดต้องรับโทษหนักขึ้นด้วย

5.) การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข(Spamming) (มาตรา11)[104]

ความผิดตามมาตรานี้ประสงค์เอาผิดกับการกระทำที่ไม่ถึงกับทำให้เกิดการรบกวนการใช้งานคอมพิวเตอร์ได้ตามปกติตามมาตรา10 แต่เป็นเพียงการรบกวนการใช้งาน

---

[103] มาตรา 10 "ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ"

[104] มาตรา 11 "ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท"

คอมพิวเตอร์ของบุคคลโดยปกติสุข[105] เช่นการส่งอีเมล์จำนวนมากเต็มระบบทำให้เกิดความยุ่งยากต่อผู้อื่นในการใช้คอมพิวเตอร์ หรือ Spamming โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว ได้แก่การปกปิดหรือปลอมแปลงIP address และรวมถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบระบบข้อมูลจราจรทางคอมพิวเตอร์ได้

6.) การจำหน่ายหรือเผยแพร่ชุดคำสั่งที่ใช้เป็นเครื่องมือในการกระทำความผิด (Missuse of device) (มาตรา 13)[106]

ความมุ่งหมายของมาตรานี้ ต้องการเอาผิดกับผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อใช้เป็นเครื่องมือในการกระทำผิดตามร่างมาตรา5ถึงมาตรา11 โดยมุ่งเอาผิดกับผู้จำหน่ายหรือเผยแพร่ "ชุดคำสั่ง"เพื่อใช้กระทำความผิดเท่านั้น ไม่รวมถึง "อุปกรณ์" ซึ่งเดิม "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ..." ได้รวมถึง"อุปกรณ์"เพื่อใช้ในการกระทำความผิดด้วย ซึ่งตรงกับความผิดฐาน Misuse of device ของThe Council of Europe Convention on Cybercrime มาตรา 6 แต่ในชั้นคณะกรรมกฤษฎีกาได้ตัดหลักการดังกล่าวออก โดยกำหนดให้เป็นความผิดเฉพาะกรณีที่จำหน่าย หรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้น เพื่อเป็นเครื่องมือในการกระทำความผิด แต่ไม่รวมถึงอุปกรณ์ด้วย โดยคณะกรรมกฤษฎีกา ได้ให้เหตุผลไว้ดังนี้ *"... แก้ไขร่างมาตรานี้เดิม ซึ่งกำหนดความผิดฐานใช้อุปกรณ์โดยมิชอบเป็นความผิดฐานจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อใช้เป็นเครื่องมือในการกระทำความผิด เนื่องจากลักษณะของการกระทำความผิดดังกล่าว อาจส่งผลกระทบต่อนักเรียน นักศึกษา ที่มีความสนใจด้านคอมพิวเตอร์และทำการสะสมโปรแกรมไวรัสคอมพิวเตอร์ โดยมิได้มีเจตนากระทำผิดต้องรับโทษ จึงได้มีการแก้ไขหลักการในร่างมาตรานี้"*[107]

---

[105] พรเพชร วิชิตชลชัย , คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ,(กรุงเทพ: สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม, 2550), หน้า16.

[106] มาตรา 13 "ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

[107] "บันทึกประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ข้อ 3.2(11)"

สำหรับชุดคำสั่ง ที่ได้กล่าวไว้ในมาตรานี้ หมายถึงโปรแกรมคอมพิวเตอร์ที่ใช้ในการกระทำความผิด เช่น ไวรัสคอมพิวเตอร์ โดยชุดคำสั่งนั้นจะต้องจัดทำขึ้นโดยเฉพาะเพื่อใช้ในการกระทำความผิด(A tool in the commission of crime) เช่นการจำหน่ายโปรแกรมเพื่อใช้ในการกระทำความผิดเข้าถึงคอมพิวเตอร์โดยมิชอบ(Illegal access), การดักข้อมูลคอมพิวเตอร์ (Illegal interception),การรบกวนข้อมูลคอมพิวเตอร์(Data interference),การรบกวนระบบคอมพิวเตอร์(System interference) หากโปรแกรมนั้นเป็นโปรแกรมธรรมดา แต่ผู้กระทำผิดนำมาใช้กระทำความผิด ผู้จำหน่ายหรือเผยแพร่โปรแกรมธรรมดาย่อมไม่มีความผิด สำหรับการเผยแพร่นั้น หมายถึงการส่งข้อมูลที่ได้รับให้ผู้อื่นอีกทอดหนึ่ง (forward) หรือการสร้าง Hyperlinks เพื่อให้สามารถเข้าถึงชุดคำสั่งดังกล่าวโดยสะดวกด้วย

7.) การใช้ระบบคอมพิวเตอร์ทำความผิดอื่น (มาตรา 14)[108]

ความผิดตามมาตรา14 นี้ มีความแตกต่างจากฐานความผิดก่อนหน้านี้ เพราะมิใช่การกระทำความผิดต่อคอมพิวเตอร์โดยตรง แต่เป็นการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิดฐานอื่นๆ ซึ่งการกระทำความผิดเหล่านั้นอาจจะเป็นความผิดตามกฎหมายอื่นด้วย เช่นความผิดฐานฉ้อโกง หมิ่นประมาท ดูหมิ่น หรือเผยแพร่ภาพลามก เป็นต้น

ความผิดตามมาตรา14 มี 5 อนุมาตราจึงเปรียบเสมือนการบัญญัติความผิดขึ้นมาอีก 5 ฐานความผิด ได้แก่

---

[108] มาตรา "14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1)(2) (3) หรือ (4)"

7.1 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

7.2 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

7.3 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

7.4 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

7.5 เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1)(2) (3) หรือ (4)

8.) ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14(มาตรา15)[109]

ผู้ที่จะมีความผิดตามมาตรานี้ จะต้องเป็น"ผู้ให้บริการ" ซึ่งนิยามศัพท์ไว้ในมาตรา 3 โดยเจตนารมณ์ของกฎหมายกำหนดให้ผู้บริการมีหน้าที่จัดการลบข้อมูลที่ไม่เหมาะสมออกจากพื้นที่ของตนในทันที ที่รู้ถึงการกระทำผิดตามร่างมาตรา 14 หากมิได้ลบทันทีย่อมมีความผิดทางอาญา

---

[109] มาตรา 15 "ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14"

9.) ตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพบุคคล(มาตรา16)[110]

มาตรา16 กำหนดให้การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ถือเป็นความผิด โดยมีองค์ประกอบคล้ายความผิดฐานหมิ่นประมาท แต่มีจุดแตกต่างตรงที่ และมาตรา 16 นี้ไม่ต้องการองค์ประกอบในส่วนของ "การใส่ความต่อบุคคลที่สาม" และได้เพิ่มคำว่า "ได้รับความอับอาย"เข้าไปด้วยซึ่งมีความหมายกว้างกว่า ความผิดฐานหมิ่นประมาท[111]

การใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่ได้กำหนดหลักการในการใช้กฎหมายดังกล่าวไว้ เพราะสามารถนำประมวลกฎหมายอาญามาปรับใช้ได้ ตามหลักการของประมวลกฎหมายอาญา มาตรา 17 ซึ่งกำหนดให้นำบทบัญญัติในภาค1 ของประมวลกฎหมายอาญามาใช้กับกฎหมายอื่นด้วย[112] ดังนั้น ในการใช้พระราชบัญญัตินี้จึงต้องนำหลักการของกฎหมายอาญามาปรับใช้ด้วย เช่น[113] หลักเจตนา (มาตรา59),การพยายามกระทำความผิด (มาตรา80),ตัวการผู้ใช้และผู้สนับสนุน(มาตรา83-89) เป็นต้น

---

[110] มาตรา 16 "ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ"

[111] พรเพชร วิชิตชลชัย , คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550, หน้า 27.

[112] มาตรา 17 " บทบัญญัติในภาค 1 แห่งประมวลกฎหมายนี้ ให้ใช้ในกรณีแห่งความผิดตามกฎหมายอื่นด้วย เว้นแต่กฎหมายนั้นๆจะบัญญัติไว้เป็นอย่างอื่น"

[113] สมาคมผู้ดูแลเว็บไทยร่วมกับหลายๆหน่วยงาน, "ร่วมวิพากษ์ร่าง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...." เอกสารประกอบการบรรยาย การเสวนารับฟังความคิดเห็น ครั้งที่ 1 โรงแรมดิเอมเมอรัล รัชดา กรุงเทพฯ 21 ธันวาคม 2549

ดังนั้น การพิจารณาความผิดตามพระราชบัญญัตินี้ จำเป็นต้องพิจารณาหลักการของประมวลกฎหมายอาญาประกอบด้วย เช่นการพิจารณาเจตนาภายในของผู้กระทำ หากเป็นการกระทำโดยสุจริต โดยมิได้มีเจตนาร้าย เช่น การแก้ไขข้อมูลคอมพิวเตอร์ที่เป็นประวัติคนไข้ให้ถูกต้องตรงความเป็นจริง โดยหากปล่อยไว้ ผู้ป่วยอาจได้รับอันตรายและการกระทำดังกล่าวไม่เกิดความเสียหายใดๆเกิดขึ้น ในทางตรงกันข้ามกลับเป็นคุณแก่ผู้ป่วย ไม่ถือว่าเป็นการกระทำโดยมิชอบ จึงไม่เป็นความผิดตามมาตรานี้[114]

นอกจากนี้ลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จะเกิดขึ้นโดยไม่มีเขตแดน(Borderless) จึงเป็นการยากที่จะกำหนดเขตอำนาจการใช้กฎหมาย ดังนั้นการพิจารณาความรับผิดทางอาญา จึงต้องพิจารณาตามประมวลกฎหมายอาญาประกอบด้วย ได้แก่ การกระทำส่วนหนึ่งส่วนใดในราชอาณาจักรหรือผลแห่งการกระทำเกิดขึ้นในราชอาณาจักร ตามมาตรา5[115] และการกระทำของตัวการ ผู้สนับสนุนหรือผู้ใช้ให้กระทำความผิดที่ได้ประทำนอกราชอาณาจักร ตามมาตรา6[116] แต่การใช้ประมวลกฎหมายอาญายังมีข้อจำกัด เพราะยังมีบางกรณีที่กฎหมายอาญาไม่สามารถใช้ได้ เช่น การเจาะข้อมูลคอมพิวเตอร์ของสถานทูตไทยในต่างประเทศ ในกรณีนี้แม้ว่าผู้เสียหายจะเป็นคนไทย แต่ไม่ก็ไม่สามารถนำประมวลกฎหมายอาญามาตรา 8 มาใช้ได้ เพราะมาตรา8 ใช้ได้เฉพาะฐานความผิดที่ระบุไว้ในมาตรานั้น เท่านั้น จึงได้บัญญัติเพื่อให้ครอบคลุมกรณีเหล่านี้ตามหลักการที่ปรากฏในมาตรา 17

---

[114] สุนทร เปลี่ยนสี, "แนวความคิด หลักการและสาระสำคัญของร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์," วารสารกฎหมายปกครอง เล่ม24,ตอน2 : หน้า 109.

[115] มาตรา 5 "ความผิดใดที่การกระทำแม้แต่ส่วนหนึ่งส่วนใดได้กระทำ ในราชอาณาจักรก็ดี ผลแห่งการกระทำเกิดในราชอาณาจักร โดยผู้กระทำ ประสงค์ให้ผลนั้นเกิดในราชอาณาจักร หรือโดยลักษณะแห่งการกระทำ ผลที่ เกิดขึ้นควรเกิดในราชอาณาจักร หรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดใน ราชอาณาจักรก็ดี ให้ถือว่าความผิดนั้นได้กระทำในราชอาณาจักร..."

[116] มาตรา 6 "ความผิดใดที่ได้กระทำในราชอาณาจักรหรือที่ประมวล กฎหมายนี้ถือว่าได้กระทำในราชอาณาจักร แม้การกระทำของผู้เป็นตัวการด้วยกัน ของผู้สนับสนุน หรือของผู้ใช้ให้กระทำความผิดนั้นจะได้กระทำนอกราชอาณาจักร ก็ให้ถือว่าตัวการ ผู้สนับสนุน หรือผู้ใช้ให้กระทำได้กระทำในราชอาณาจักร"