

อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่ร้ายแรงเป็นภัยต่อสังคมรูปแบบหนึ่ง ที่ก่อให้เกิดความเสียหายแก่ระบบเศรษฐกิจเป็นอย่างมาก แทบทุกประเทศต่างก็เล็งเห็นถึงอันตรายจากอาชญากรรมประเภทนี้ และผลกระทบที่เกิดขึ้นกับกฎหมายอาญาของประเทศต่างๆ ทั่วโลก เนื่องจากกฎหมายอาญาที่ใช้อยู่ไม่เพียงพอที่จะดำเนินคดีกับอาชญากรได้ จึงพยายามหามาตรการทางกฎหมายใหม่ๆ เพื่อค้นหาวิธีการป้องกันและปราบปราม สำหรับประเทศไทยเป็นประเทศหนึ่ง ที่เห็นความสำคัญของปัญหาดังกล่าวจึงมีการร่างกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้นเป็นกฎหมายเฉพาะ อย่างไรก็ตามสิ่งที่ควรคำนึงถึงควบคู่ไปกันไปด้วยคือต้องมีการปรับปรุงกฎหมายวิธีสบัญญัติให้ มีประสิทธิภาพด้วย โดยเฉพาะในการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ที่เป็นข้อมูลส่วนบุคคล

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 29 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักพื้นฐาน แต่ก็มีข้อยกเว้นที่ให้อำนาจอธิปไตยสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณีภายในขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล และรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจอธิปไตยกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้นรัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคลเกินความจำเป็น หรือตามอำเภอใจ โดยอ้าง “ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเห็นสมควรโดยเฉพาะข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำดังกล่าวถือเป็นการกระทำที่กระทบกระเทือนต่อสาระ

สำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัติดังกล่าวไม่สามารถใช้บังคับได้ ทั้งนี้ การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการจำเป็นสำหรับรัฐมาใช้แสวงหาพยานหลักฐานเพื่อมาดำเนินคดีกับอาชญากรที่ก่ออาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น จึงควรมีการบัญญัติกฎหมายขึ้นมาให้อำนาจ แก่เจ้าหน้าที่ของรัฐในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญของสิทธิในข้อมูลข่าวสารส่วนบุคคล

พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ มีลักษณะแตกต่างไปจากพยานหลักฐานทั่วๆ ไป กล่าวคือพยานหลักฐานประเภทนี้เป็นสิ่งที่ไม่มียุติวิธาน มองไม่เห็นด้วยตาเปล่า และอยู่ในรูปของคลื่นแม่เหล็กไฟฟ้า อาจถูกแก้ไขเปลี่ยนแปลง ลบ ทำลายได้ง่าย เจ้าหน้าที่ในกระบวนการยุติธรรมทั้งหลายจึงต้องประสบปัญหาในการดำเนินคดีกับผู้กระทำความผิด โดยเฉพาะพนักงานสอบสวนที่มีหน้าที่ในการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของจำเลย ผู้วิจัยได้ทำการศึกษาวิจัยปัญหาการรวบรวมพยานหลักฐานและการพิสูจน์พยานหลักฐานที่เป็นอิเล็กทรอนิกส์ และเป็นข้อมูลส่วนบุคคล ภายในกรอบของ 3 หัวข้อใหญ่ คือ หนึ่งลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ สองสิทธิส่วนบุคคล สามกระบวนการค้น และกระบวนการนำเสนอพยานหลักฐานต่อศาล ภายใต้สมมติฐานว่าการรวบรวมพยานหลักฐานเป็นการละเมิดสิทธิส่วนบุคคลที่ได้รับการคุ้มครองตามรัฐธรรมนูญและกฎหมายอาญาเจ้าหน้าที่ของรัฐสามารถกระทำได้เพียงใด ปัจจุบันมีกฎหมายฉบับใดให้อำนาจกระทำหรือไม่อย่างไร และควรจะทำอย่างไรเพื่อที่จะนำตัวผู้กระทำความผิดมาลงโทษให้ได้

ผลจากการศึกษาและวิเคราะห์ปัญหาทั้งในประเทศไทยและต่างประเทศ ตลอดจนศึกษาแนวทางแก้ไขปัญหามาจากต่างประเทศ โดยเฉพาะของประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น พบว่าการที่จะให้เจ้าหน้าที่ของรัฐเข้าถึงหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เร็ว และไม่เป็นการละเมิดสิทธิในข้อมูลข่าวสารส่วนบุคคลจะต้องมีกฎหมายให้อำนาจในการปฏิบัติงานได้ ควรมีองค์กรที่เป็นกลางเป็นผู้ให้อำนาจและตรวจสอบการใช้อำนาจ และควรมีหลักกฎหมายลักษณะพยานหลักฐานเกี่ยวกับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่ชัดเจนกว่านี้

Computer crime is a serious crime which is dangerous to society. It causes serious damage to the system of economy. Most countries realize the damage of this crime and its effect worldwide. Because of insufficient provisions of criminal law to be applied against the criminals who committed a computer crime, each country tries to find out new legal measures to fight such crime. Thailand is a country who recognizes the importance of this problem, and therefore, elaborates a draft legislation against computer crime. However, there should be an amendment on the criminal procedure legislation at the same time in order to enhance particularly the effectiveness of finding and collecting the evidence and the admissibility of the evidence which is a personal information in the case of computer crime.

The Constitution of the Kingdom of Thailand B.E. 2540 (1997), Article 29 recognizes, in principle, the civil rights and freedom of the people. Nevertheless in some case, the Constitution concedes that a restriction of civil rights and freedom can be made by law. For example, in article 37 of the Constitution, even if the Constitution recognizes the protection of right to privacy, the State has a power to do anything for the sake of public interest. Therefore, under such provision, the State may enact a law limiting the civil rights and freedom in information or allowing the state officials to search a personal information of any body at anytime, even if such information is kept in the computer.

Such operation affects the main principle of rights and freedom in private information and enters into conflict with the article 6 of the Constitution, the highest legislation of the country. As a result, the provision allowing such operation will be ineffective, even though

the access to a private information is a necessary measure for the State to use as a tool in finding evidence against the offender in computer crime, because of the non-functional actual measure. It is, therefore, suggested that an enactment of legislation be necessary to provide the state official with the power of accessing to the private information under the condition that such procedure must not effect the principle of right to privacy of personal information.

The evidence which is an electronic information differs from an ordinary evidence. It is transparent unseen object, figured in the form of electromagnetic wave that can be easily modified, deleted, destroyed. The officials in criminal justice administration have a difficult task in gathering an evidence against the offender, especially the inquiry official who has a duty to collect the evidence that can prove the guilt of offender.

In this thesis, the researcher made a study on the problems of collecting the evidence which is electronic information. The study divides in to three main topic. The first is the characters of electronic information evidence. The second is the right to privacy. The third is the procedure of search and bringing such evidence to the Court.

The research is done under the hypothesis that, in what circumstances, the collection of evidence which violates the right to privacy, protected by the Constitution and the criminal law, can be allowed and operated by the state official. Is there, nowadays, the legislation, that provide such a power to the state official ? And how the justice can bring the offender to the punishment?

The result came from the comparative study on the problem occurred in Thailand and the other countries such as U.S.A , England and Japan, can conclude that a rapid access of the state official to an electronic information which is not considered as a violation of right to privacy of personal information must be allowed by law. There should also be an independent organ who can permit and control such operation. Finally, there should be a more obvious rule of evidence relating to an electronic information evidence.