บทที่ 4

วิเคราะห์ปัญหาทางกฎหมายที่เกี่ยวกับการชำระหนี้เป็นตัวเงิน

จากกรณีที่ผู้เขียนได้ศึกษาวิวัฒนาการความเป็นมา และกฎหมายที่เกี่ยวข้องของการทำธุรกรรมเกี่ยวกับการชำระเงิน ผ่านทางสื่ออิเล็กทรอนิกส์ รวมตลอดถึงได้ศึกษาค้นคว้ามาตรการทางกฎหมายทั้งในประเทศไทยและต่างประเทศ เช่น อังกฤษ และฝรั่งเศส ที่สามารถนำมาเปรียบเทียบปรับใช้เพื่อให้เป็นแนวทางในการแก้ไขปัญหา ของการทำธุรกรรมการชำระหนี้ทางอิเล็กทรอนิกส์ในระบบต่างๆ ซึ่งมีประเด็นที่สามารถจำแนกแยกวิเคราะห์ ประเด็นปัญหาที่สำคัญๆ ที่ควรได้รับการศึกษา ดังนี้

1. ปัญหาเครื่องหรือระบบคอมพิวเตอร์เกิดความบกพร่อง
(Malfunction of the System)

หากเกิดความเสียหายขึ้นมาใครจะเป็นผู้รับผิดชอบ เพราะปัญหาเรื่องความบกพร่องเป็นเรื่องทางเทคนิคที่ละเอียดอ่อน ยากที่ผู้บริโภคจะทำความเข้าใจได้ง่าย อีกทั้งยังไม่มีกฎหมายใดที่บัญญัติเกี่ยวกับเรื่องความบกพร่องของระบบคอมพิวเตอร์มาบังคับใช้ในการตัดสินปัญหา จากการศึกษาผู้เขียนเห็นว่าควรจะมีการนำประมวลกฎหมายแพ่งและพาณิชย์ของไทยมาปรับใช้เป็นแนวทางในการแก้ไขปัญหาดังกล่าว ในกรณีประเด็นที่มีการทำธุรกรรมการชำระหนี้ค่าสินค้าและบริการผ่านทางสื่ออิเล็กทรอนิกส์ แล้วเกิดความบกพร่องของระบบไม่ว่าจะเป็นการบกพร่องของระบบคอมพิวเตอร์ หรือระบบเครือข่ายอินเตอร์เน็ต รวมตลอดถึงความบกพร่องของเจ้าหน้าที่ที่ให้บริการการรับชำระเงิน เช่น เจ้าหน้าที่ของธนาคารหรือเจ้าหน้าที่ของสถานที่รับชำระเงินรายย่อยต่างๆ ที่มิใช่ธนาคาร และความเสียหายได้เกิดกับตัวผู้ใช้บริการ ซึ่งถือว่าเป็นผู้บริโภคที่ได้รับความเสียหายโดยตรง จากการที่ไม่สามารถปฏิบัติการชำระหนี้ได้ ลูกหนี้อาจจะถูกฟ้องร้องเรียกค่าเสียหาย โดยถือว่าลูกหนี้ผิดนัดการชำระหนี้

กรณีปัญหาดังกล่าวที่เกิดขึ้นจะเห็นได้ว่าผู้บริโภคมิได้รู้ถึงเหตุการณ์ความบกพร่องของระบบผู้ให้บริการในการชำระเงิน ทั้งที่ผู้บริโภคในฐานะของลูกหนี้ในการซื้อขายสินค้าและบริการมีเจตนาที่จะปฏิบัติตามข้อตกลงของสัญญา และเมื่อมีความเสียหายเกิดขึ้นรัฐก็ควรเข้ามาตัดสิน

ปัญหาเพื่อลดความขัดแย้งให้เกิดความเป็นธรรมกับทั้งสองฝ่าย แต่เนื่องจากประเทศไทยยังไม่มีกฎหมายแม่แบบที่จะเข้ามาควบคุมดูแลในเรื่องนี้ ผู้เขียนจึงเห็นว่ามีความจำเป็นที่จะต้องเอากฎหมายแพ่งและพาณิชย์ของไทย เรื่องการชำระหนี้ของลูกหนี้เข้ามาปรับใช้แก้ไขปัญหา เพราะเป็นเรื่องของการชำระหนี้ต่างตอบแทนทางการค้าและบริการ

จากประเด็นปัญหาจะเห็นได้ว่าความเสียหายที่เกิดขึ้นมิได้เกิดจากตัวลูกหนี้แต่อย่างใดแต่เกิดจากความบกพร่องของตัวผู้ให้บริการการชำระเงิน โดยเฉพาะธนาคารลูกหนี้จะเอาเหตุความบกพร่องของสถาบันการเงินขึ้นเป็นข้ออ้างว่าการชำระหนี้เป็นพ้นวิสัย ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 219 วรรคหนึ่ง มีหลักเกณฑ์ว่า ถ้าการชำระหนี้กลายเป็นพ้นวิสัย เพราะพฤติการณ์อันใดอันหนึ่ง ซึ่งเกิดขึ้นภายหลังที่ได้ก่อหนี้และซึ่งลูกหนี้ไม่ต้องรับผิดชอบลูกหนี้เป็นอันหลุดพ้นจากการชำระหนี้ อ้างถึงเป็นข้อแก้ตัวเพื่อมิต้องชำระค่าเสียหายได้หรือไม่ ถ้าพิจารณาแล้วเห็นว่าเป็นพ้นวิสัยลูกหนี้ก็ไม่ต้องชำระหนี้

จากหลักกฎหมายดังกล่าว จำต้องวินิจฉัยอีกต่อไปว่าการกระทำแค่ไหนที่ถือว่าเป็นพ้นวิสัย จากที่ผู้เขียนได้ศึกษากฎหมายทั้งในประเทศและต่างประเทศที่เกี่ยวกับเรื่องนี้ จะอ้างว่าเป็นพ้นวิสัยได้ ความบกพร่องนั้นต้องเกิดจากเหตุสุดวิสัยเท่านั้น ซึ่งตามกฎหมายแพ่งและพาณิชย์ของไทยมีบัญญัติไว้ในมาตรา 8 มีหลักว่า เหตุสุดวิสัย หมายถึง เหตุใดๆ อันเกิดขึ้นก็ดี จะทำให้ผลพิบัติก็ดีเป็นเหตุที่ไม่อาจป้องกันได้ หรือเป็นสิ่งที่คาดหมายไม่ได้ว่าจะเกิดขึ้น ซึ่งถ้าหากนำกฎหมายของไทยมาเทียบเคียงกับการศึกษา จากกฎหมายต่างประเทศไม่ว่าจะเป็นฝรั่งเศส หรืออังกฤษ จะให้ความหมายของคำว่าเหตุสุดวิสัยไว้ในความหมายเดียวกันว่าเหตุสุดวิสัย จะต้องเกิดจากเหตุการณ์ที่ไม่อาจคาดหมายได้ ในเหตุการณ์ที่อาจเกิดขึ้นหรืออาจป้องกันหรือหลีกเลี่ยงได้ เพราะฉะนั้น ความเสียหายที่เกิดขึ้นจากความบกพร่องที่จะทำให้การชำระหนี้ของลูกหนี้เป็นพ้นวิสัย ต้องเป็นความบกพร่องที่เกิดจากเหตุสุดวิสัย ในความหมายที่กล่าวมาข้างต้นเท่านั้น ซึ่งถือว่าเป็นเหตุการณ์ที่เข้ามาขัดขวางการปฏิบัติการชำระหนี้ของลูกหนี้ อายุความสะดุดหยุดลงจนกว่าสาเหตุที่เป็นอุปสรรคที่ไม่สามารถชำระหนี้ได้จะหมดไป เช่น ความบกพร่องของระบบคอมพิวเตอร์ที่ทำให้ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้ อาจเกิดจากความบกพร่องของระบบต่างๆ ที่สำคัญๆ ในปัญหาการชำระหนี้ ดังนี้

1.1 ระบบเครือข่ายอินเตอร์เน็ตล่ม (Internet Network)

1.2 ไวรัสคอมพิวเตอร์ (Virus Computer)

1.3 แฮกเกอร์ (Hacker)

1.1 ระบบเครือข่ายอินเตอร์เน็ตล่ม

ระบบเครือข่ายอินเตอร์เน็ต เป็นระบบเครือข่ายขนาดใหญ่ที่เชื่อมโยงเครือข่ายต่างๆ ทั่วโลกเข้าด้วยกัน กล่าวได้ว่า โครงสร้างของเครือข่ายอินเตอร์เน็ต คือ ต้นแบบของโครงสร้างแบบกระจายที่ครอบคลุมโยงใยไปทั่วโลก มีการใช้อินเตอร์เน็ต ติดต่อสื่อสารถึงกันอย่างแพร่หลาย การขยายตัวเพิ่มขึ้นอย่างรวดเร็ว จนกระทั่งกลายเป็นระบบเครือข่ายที่สำคัญสำหรับภาคธุรกิจ และประชาชนทุกคนในโลก ซึ่งนำมาสู่โอกาสทางธุรกิจต่างๆ ในกรณีที่มีการตกลงในการชำระหนี้ของลูกหนี้ ข้อตกลงในสัญญาที่ได้มีการปฏิบัติกันทางการค้าขายสินค้าและบริการ ผ่านทางสื่ออิเล็กทรอนิกส์และในขณะเดียวกัน ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้ ปรากฏว่าการชำระหนี้ผ่านทางธนาคารหรือสถาบันการเงินที่ให้บริการการชำระเงิน ในขณะทำธุรกรรมการชำระหนี้ผ่านทางสื่ออิเล็กทรอนิกส์ ระบบเครือข่ายเกิดล่มขัดข้องทั่วโลก จึงเป็นสาเหตุหนึ่งที่ทำให้ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้สำเร็จ จึงมีความเสียหายเกิดขึ้น ลูกหนี้อาจได้ชื่อว่าผิดนักการชำระหนี้ และต้องรับผิดชอบในความเสียหายที่เกิดขึ้น

จากประเด็นปัญหาดังกล่าวต้องพิจารณาต่อไปว่าการที่ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้นั้น ซึ่งเกิดจากระบบเครือข่ายล่ม ลูกหนี้สามารถเอาเหตุดังกล่าว นำขึ้นมาเป็นข้อแก้ตัวให้ลูกหนี้พ้นผิด จากการไม่ปฏิบัติการชำระหนี้ได้หรือไม่ ซึ่งการที่ลูกหนี้จะยกข้อแก้ตัวให้ตัวเองพ้นความรับผิดได้นั้น ลูกหนี้สามารถอ้างเหตุการณ์ที่เกิดขึ้นมาเป็นพ้นวิสัยที่ทำให้ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้ซึ่งทำให้ลูกหนี้ไม่ต้องชำระหนี้ตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 219 วรรคหนึ่ง การที่จะถือว่าเหตุการณ์ระบบเครือข่ายอินเตอร์เน็ตล่ม ถือว่าเป็นการพ้นวิสัยนั้นต้องพิจารณาอีกต่อไปว่าการล่มของเครือข่ายเกิดจากเหตุการณ์ที่ไม่อาจคาดหมายได้หรือป้องกันได้หรือไม่ ซึ่งจากการที่ได้ศึกษากฎหมายต่างประเทศไม่ว่าจะเป็นฝรั่งเศส หรืออังกฤษ โดยนำมาเทียบเคียงกับกฎหมายไทย พิจารณาจากระบบเครือข่ายอินเตอร์เน็ตล่ม ทำให้ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้นั้น ถือเป็นเหตุการณ์ที่เกิดจากระบบเครือข่ายที่โยงใยกันทั่วโลก เกิดขัดข้องซึ่งลูกหนี้ไม่สามารถที่จะคาดหมายได้หรือหลีกเลี่ยงที่จะป้องกันได้ ถือว่าเป็นเหตุสุดวิสัย ซึ่งตามกฎหมายแพ่งและพาณิชย์ของไทยบัญญัติไว้ในมาตรา 8 ว่าเหตุสุดวิสัย หมายถึงเหตุใดๆ อันเกิดขึ้นก็ดี จะทำให้ผลพิบัติก็ดี เป็นเหตุที่ไม่อาจป้องกันได้ หรือเป็นสิ่งที่คาดหมายไม่ได้ว่าจะเกิดขึ้น เมื่อพิจารณาว่าระบบเครือข่ายอินเตอร์เน็ตล่มเกิดจากเหตุการณ์ที่คาดหมายมาไม่ได้หรือป้องกันได้ ลูกหนี้ก็สามารถยกเอาเหตุสุดวิสัย ขึ้นเป็นข้ออ้างว่าการชำระหนี้ของลูกหนี้เป็นพ้นวิสัยตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 219 วรรคหนึ่ง ทำให้ลูกหนี้หลุดพ้นจากการชำระหนี้

1.2 ไวรัสคอมพิวเตอร์ (มหาวิทยาลัยเกษตรศาสตร์, ออนไลน์, ม.ป.ป)

ไวรัส คือโปรแกรมชนิดหนึ่งที่มีความสามารถในการสำเนาตัวเองเข้าไปติดอยู่ในระบบคอมพิวเตอร์ได้และถ้ามีโอกาสก็สามารถแทรกเข้าไประบาดในระบบคอมพิวเตอร์อื่นๆ ซึ่งอาจเกิดจากการนำเอาดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปใช้อีกเครื่องหนึ่ง หรืออาจผ่านระบบเครือข่ายหรือระบบสื่อสารข้อมูลไวรัสก็อาจแพร่ระบาดได้เช่นกัน

การที่คอมพิวเตอร์ใดติดไวรัสหมายถึงว่าไวรัสได้เข้าไปฝังตัวอยู่ในหน่วยความจำได้นั้นจะต้องมีการถูกเรียกให้ทำงานได้นั้น ยังขึ้นอยู่กับประเภทของไวรัส แต่ละตัวปกติผู้ใช้มักจะไม่รู้ตัวว่าได้ทำการปลุกคอมพิวเตอร์ไวรัสขึ้นมาทำงานแล้ว

จุดประสงค์ของการทำงานของไวรัสแต่ละตัวขึ้นอยู่กับตัวผู้เขียนโปรแกรมไวรัสนั้น เช่น อาจสร้างไวรัสให้ไปทำลายโปรแกรมหรือข้อมูลอื่นๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือแสดงข้อความวิ่งไปมาบนหน้าจอเป็นต้น

1.2.1 ประเภทของไวรัส

1) บูตเซกเตอร์ไวรัส (Boot Sector Viruses / Boot Infector Viruses)

คือไวรัสที่เก็บตัวเองอยู่ในบูตเซกเตอร์ของดิสก์ การใช้งานของบูตเซกเตอร์ คือ เมื่อเครื่องคอมพิวเตอร์เริ่มทำงานขึ้นมาตอนแรก เครื่องจะเข้าไปอ่านบูตเซกเตอร์ โดยบูตเซกเตอร์จะมีโปรแกรมเล็กๆ ไว้ใช้ในการเรียกระบบ ปฏิบัติการขึ้นมาทำงานอีกทีหนึ่ง บูตเซกเตอร์ไวรัสจะเข้าไปแทนที่โปรแกรมดังกล่าว และไวรัสประเภทนี้ถ้าไปติดอยู่ในฮาร์ดดิสก์ โดยทั่วไปจะเข้าไปอยู่บริเวณที่เรียกว่า มาสเตอร์บูตเซกเตอร์หรือพาร์ทิชั่นเทเบิ้ล (Master Boot Sector / Partition Table) ของฮาร์ดดิสก์นั้น

ถ้าบูตเซกเตอร์ของดิสก์ใดมีไวรัสประเภทนี้ติดอยู่ ทุกๆ ครั้งที่บูตเครื่องขึ้นมาโดยพยายามเรียก ดอสจากดิสก์นี้ตัวโปรแกรมไวรัสจะทำงานก่อนและจะเข้าไปฝังตัวอยู่ในหน่วยความจำเพื่อเตรียมพร้อมที่จะทำงานตามที่ได้ถูกโปรแกรมมาแล้ว ตัวไวรัสจึงค่อยไปเรียกดอสให้ขึ้นมาทำงานต่อไป ทำให้เหมือนไม่มีอะไรเกิดขึ้น

2) โปรแกรมไวรัสหรือไฟล์อินเทคเตอร์ (Program Viruses / File Intector Viruses) เป็นไวรัสอีกประเภทหนึ่งที่จะติดอยู่กับโปรแกรม ซึ่งปกติก็คือไฟล์ที่มีนามสกุลเป็น .COM หรือ .EXE และบางไวรัสสามารถเข้าไปติดอยู่ในโปรแกรมที่มีนามสกุลเป็น .SYS และโปรแกรมประเภท โอเวอร์เลย์โปรแกรม (Overlay Programs) ได้ด้วย โปรแกรมโอเวอร์เลย์ปกติจะเป็นไฟล์ที่มีนามสกุลที่ขึ้นต้นด้วย OV วิธีการที่ไวรัสใช้เพื่อที่จะเข้าไปติดโปรแกรมมีอยู่สองวิธี คือ การแทรกตัวเองเข้าไปอยู่ในโปรแกรมผลก็คือ หลังจากที่โปรแกรมนั้นติดไวรัสแล้ว ขนาดของโปรแกรมจะ

ใหญ่ขึ้น หรืออาจมีการสำเนาตัวเองเข้าไปทับส่วนของโปรแกรมที่มีอยู่เดิมดังนั้น ขนาดของโปรแกรมจะไม่เปลี่ยนและยากที่จะซ่อมให้กลับเป็นดังเดิม

การทำงานของไวรัส โดยทั่วไป คือ เมื่อมีการเรียกโปรแกรมที่ติดไวรัส ส่วนของไวรัสจะทำงานก่อนและจะถือโอกาสนี้ฝังตัวเข้าไปอยู่ในหน่วยความจำทันทีแล้วจึงค่อยให้โปรแกรมนั้นทำงานตามปกติต่อไป เมื่อไวรัสเข้าไปฝังตัวอยู่ในหน่วยความจำแล้ว หลังจากนี้ถ้ามีการเรียกโปรแกรมอื่นๆ ขึ้นมาทำงานต่อ ตัวไวรัสก็จะสำเนาตัวเองเข้าไปในโปรแกรมอื่นๆ ที่อยู่ในดิสก์เพื่อทำสำเนาตัวเองลงไปทันทีแล้วจึงค่อยให้โปรแกรมที่ถูกเรียกนั้นทำงานตามปกติต่อไป

3) ม้าโทรจัน (Trojan Horse) เป็นโปรแกรมที่ถูกเขียนขึ้นมาให้ทำตัวเหมือนว่าเป็นโปรแกรมธรรมดาทั่วๆ ไป เพื่อหลอกล่อผู้ใช้ให้ทำการเรียกขึ้นมาทำงาน แต่เมื่อถูกเรียกขึ้นมาแล้วก็จะเริ่มทำลายตามที่โปรแกรมมาทันที ม้าโทรจันบางตัวถูกเขียนขึ้นมาใหม่ทั้งชุด โดยคนเขียนจะทำการตั้งชื่อโปรแกรมพร้อมทั้งชื่อรุ่นและคำอธิบายการใช้งานที่ดูสมจริง เพื่อหลอกให้คนที่จะเรียกใช้ตายใจ

จุดประสงค์ของคนเขียนม้าโทรจันอาจจะเช่นเดียวกับคนเขียนไวรัส คือ เข้าไปทำอันตรายต่อข้อมูลที่มีอยู่ในเครื่อง หรืออาจมีจุดประสงค์เพื่อที่จะล้างเอาความลับของระบบคอมพิวเตอร์

ม้าโทรจันนี้อาจจะถือว่าไม่ใช่ไวรัส เพราะเป็นโปรแกรมที่ถูกเขียนขึ้นมาโดดๆ และจะไม่มีการเข้าไปติดในโปรแกรมอื่นเพื่อสำเนาตัวเอง แต่จะใช้ความรู้เท่าไม่ถึงการณ์ของผู้ใช้เป็นตัวแพร่ระบาดซอฟต์แวร์ที่มีม้าโทรจันอยู่ในนั้นและนับว่าเป็นหนึ่งในประเภทของโปรแกรม ที่มีอันตรายสูง เพราะยากที่จะตรวจสอบและสร้างขึ้นมาได้ง่าย ซึ่งอาจใช้แค่แบตซ์ไฟล์ก็สามารถโปรแกรมประเภทม้าโทรจันได้

โพลีมอร์ฟิกไวรัส

4) โพลีมอร์พิกค์ไวรัส (Polymorphic Viruses) เป็นชื่อที่ใช้ในการเรียกไวรัสที่มีความสามารถในการแปรเปลี่ยนตัวเอง ได้เมื่อมีการสร้างสำเนาตัวเองเกิดขึ้น ซึ่งอาจได้หลายร้อยรูปแบบ ผลก็คือ ทำให้ไวรัสเหล่านี้ยากต่อการถูกตรวจจับ โดยโปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกนอย่างเดียว ไวรัสใหม่ๆ ปัจจุบันที่มีความสามารถนี้เริ่มมีจำนวนเพิ่มมากขึ้นเรื่อยๆ

5) สทีลต์ไวรัส (Stealth Viruses) เป็นชื่อเรียกไวรัสที่มีความสามารถในการพรางตัวต่อการตรวจจับได้ เช่น ไฟล์อินเฟกเตอร์ ไวรัสประเภทที่ไปติดโปรแกรมใดแล้วจะทำให้ขนาดของโปรแกรมนั้นใหญ่ขึ้น ถ้าโปรแกรมไวรัสนั้นเป็นแบบสทีลต์ไวรัส จะไม่สามารถตรวจดูขนาดที่แท้จริง ของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัวไวรัสจะเข้าไปควบคุมดอส เมื่อมีการใช้คำสั่ง Dir

หรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ดอสก็จะแสดงขนาดเหมือนเดิม ทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น

1. อาการของเครื่องที่ติดไวรัส

สามารถสังเกตการณ์ทำงานของเครื่องคอมพิวเตอร์ถ้ามีอาการดังต่อไปนี้อาจเป็นไปได้ว่ามีไวรัสเข้าไปติดอยู่ในเครื่องแล้ว อาการที่ว่านั้นได้แก่

1) ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
2) ขนาดของโปรแกรมใหญ่ขึ้น
3) วันเวลาของโปรแกรมเปลี่ยนไป
4) ข้อความที่ปกติไม่ค่อยได้เห็นกลับถูกแสดงขึ้นมาบ่อยๆ
5) เกิดอักษรหรือข้อความประหลาดบนหน้าจอ
6) เครื่องส่งเสียงออกทางลำโพงโดยไม่ได้เกิดจากโปรแกรมที่ใช้อยู่
7) แป้นพิมพ์ทำงานผิดปกติหรือไม่ทำงานเลย
8) ขนาดของหน่วยความจำที่เหลือลดน้อยกว่าปกติ โดยหาเหตุผลไม่ได้
9) ไฟล์แสดงสถานะการทำงานของดิสก์ติดค้างนานกว่าที่เคยเป็น
10) ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ๆ ก็หายไป
11) เครื่องทำงานช้าลง
12) เครื่องบูตตัวเองโดยไม่ได้สั่ง
13) ระบบหยุดทำงนโดยไม่ทราบสาเหตุ
14) เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นโดยมีการรายงานว่าจำนวนเซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้นกว่าแต่ก่อนโดยที่ยังไม่ได้ใช้โปรแกรมใดเข้าไปตรวจหาเลย

2. การตรวจหาไวรัสหรือการสแกน

โปรแกรมตรวจหาไวรัสที่ใช้วิธีสแกน (Scanning) เรียกว่า สแกนเนอร์ (Scanner) โดยจะมีการดึงเอาโปรแกรมบางส่วนของตัวไวรัสมาเก็บไว้เป็นฐานข้อมูล ส่วนที่ดึงมานั้นเราเรียกว่า ไวรัสซิกเนเจอร์ (Virus Signature) และเมื่อสแกนเนอร์ถูกเรียกขึ้นมาทำงานก็จะเข้าตรวจหาไวรัสในหน่วยความจำ บูตเซกเตอร์และไฟล์โดยใช้ไวรัสซิกเนเจอร์ที่มีอยู่

ข้อดีของวิธีการนี้ก็คือ เราสามารถตรวจสอบซอฟแวร์ที่มาใหม่ได้ทันที่เลยว่าติดไวรัสหรือไม่ เพื่อป้องกันไม่ให้ไวรัสถูกเรียกขึ้นมาทำงานตั้งแต่เริ่มแรก แต่วิธีนี้มีจุดอ่อนอยู่หลายข้อ คือ

(1) ฐานข้อมูลที่เก็บไวรัสซิกเนเจอร์จะต้องทันสมัยอยู่เสมอ และครอบคลุมไวรัส

ทุกตัวมากที่สุดเท่าที่จะทำได้

(2) เพราะสแกนเนอร์จะไม่สามารถตรวจจับไวรัสที่ยังไม่มีซิกเนเจอร์ของไวรัสนั้นเก็บในฐานข้อมูลได้

(3) ยากที่จะตรวจจับไวรัสประเภทโพลีมอร์ฟิก เนื่องจากไวรัสประเภทนี้เปลี่ยน-แปลงตัวเองได้ จึงทำให้ไวรัสซิกเนเจอร์ที่ใช้สามารถนำมาตรวจสอบได้ก่อนที่ไวรัสจะเปลี่ยนตัวเองเท่านั้น

(4) ถ้ามีไวรัสประเภทสทีลต์ไวรัสติดอยู่ในเครื่อง ตัวสแกนเนอร์อาจจะไม่สามารถตรวจหาไวรัสนี้ได้ ทั้งนี้ขึ้นอยู่กับความฉลาดและเทคนิคที่ใช้ของตัวไวรัสและของตัวสแกนเนอร์เองว่าใครเก่งกว่า เนื่องจากไวรัสมีตัวใหม่ๆ ออกมาอยู่เสมอ ผู้ใช้จึงจำเป็นจะต้องหาสแกนเนอร์ตัวที่ใหม่ที่สุดมาใช้

(5) มีไวรัสบางตัวจะเข้าไปติดในโปรแกรมทันทีที่โปรแกรมนั้นถูกอ่าน และถ้าสมมติว่าสแกนเนอร์ที่ใช้ไม่สามารถตรวจจับได้ และถ้าเครื่องมีไวรัสติดอยู่ เมื่อมีการเรียกสแกนเนอร์ขึ้นมาทำงาน สแกนเนอร์จะเข้าไปอ่านโปรแกรมทีละโปรแกรม เพื่อตรวจสอบ ผลก็คือจะทำให้ไวรัสตัวนี้เข้าไปติดอยู่ในโปรแกรมทุกตัวที่ถูกสแกนเนอร์นั้นอ่านได้

(6) สแกนเนอร์รายงานผิดพลาดได้ คือ ไวรัสซิกเนเจอร์ที่ใช้บังเอิญไปตรงกับที่มีอยู่ในโปรแกรมธรรมดาที่มาได้ติดไวรัส ซึ่งมักจะเกิดขึ้นในกรณีที่ไวรัสซิกเนเจอร์ ที่ใช้มีขนาดสั้นไปก็จะทำให้โปรแกรมดังกล่าวใช้งานไม่ได้อีกต่อไป

จากการทำความเข้าใจปัญหาไวรัสคอมพิวเตอร์ซึ่งเกิดขึ้นทำให้การชำระหนี้ทางสื่ออิเล็กทรอนิกส์ไม่สามารถที่จะทำได้ จากการศึกษาจะเห็นได้ว่าการเกิดไวรัสคอมพิวเตอร์เป็นเหตุการณ์ที่ผู้ให้บริการสามารถที่จะหาทางป้องกันไม่ให้ระบบทางอิเล็กทรอนิกส์ของตนติดไวรัสได้ ซึ่งมีวิธีป้องกันดังที่กล่าวมาแล้วข้างต้น กรณี เช่นนี้ไม่ถือว่าการที่คอมพิวเตอร์ติดไวรัสไม่เป็นการพ้นวิสัยที่ลูกหนี้จะอ้าง เพื่อให้ไม่ต้องชำระหนี้ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 219 วรรคหนึ่งได้ อีกทั้งการติดไวรัส ก็ยังไม่ถือว่าเป็นเหตุสุดวิสัยอีกด้วย เมื่อพิจารณาเทียบเคียงกฎหมายไทย และกฎหมายต่างประเทศเรื่องเหตุสุดวิสัย

1.3 แฮกเกอร์ (ทีเอสคอมพิวเตอร์, ออนไลน์, ม.ป.ป.)

ในปัจจุบัน “แฮกเกอร์” นั้น ใช้ใน 2 ความหมายหลัก คือ ความหมายในทางที่ดี และในทางที่ไม่ดีเท่าไรนัก ความหมายที่เป็นที่นิยมและพบบ่อยในสื่อนั้น มักจะไม่ดี โดยส่วนใหญ่จะใช้ในการกระทำทางอาชญากรรมทางคอมพิวเตอร์ ส่วนในทางที่ดี “แฮกเกอร์” ยังใช้ในลักษณะ

หมายถึง ความเป็นพวกพ้อง และยังหมายถึงกลุ่มของผู้ใช้คอมพิวเตอร์ โดยเฉพาะผู้ที่ใช้ความสามารถในระดับผู้เชี่ยวชาญทางด้านโปรแกรม

1.3.1 การถูกแฮ็ก (Hack) มี 3 วิธี

วิธีที่ 1 สนิฟเฟอร์ (Sniffer) คือโปรแกรมที่แฮ็กใช้จับแพคเก็จ (Package) ที่ส่งกันไปมาในอินเตอร์เน็ต

วิธีที่ 2 ฟรอนทัลแอทแทค (Frontal Attack) คือการโจมตีแบบตรงๆ ให้เซริฟเวอร์ล้ม

วิธีที่ 3 เอ็กซ์โพลติ้ง (Exploiting a Security Bug or Loophole) ระบบทุกระบบที่มีอยู่ตั้งแต่ตอนติดตั้งระบบเสร็จ ทันทีที่ติดตั้งเสร็จ ระบบจะหาความบกพร่อง ที่จะให้แฮ็คเกอร์เข้ามาในระบบในฐานะ ซุปเปอร์ยูสเซอร์ได้

1.3.2 วิธีป้องกันการถูก Hack

1) ผู้ดูแลระบบ (Sysadmin) จะต้องเลิกใช้เทลเน็ต และติดตั้งระบบความปลอดภัย (Secure Shell: SSH) เพื่อป้องกันสนิฟเฟอร์ดักจับพาสเวิร์ด (Password)

2) ผู้ดูแลระบบจะต้องติดตั้งเอสเอสแอล (SSL) เพื่อทำให้เว็บของตนให้บริการได้อย่างปลอดภัย ถ้ามีข้อมูลที่สำคัญมากๆ เช่น การรับข้อมูลบัตรเครดิต เป็นต้น

3) ผู้ใช้ต้องเลิกใช้เทลเน็ตเวบเบสเมล์ (Telnet Web Base Mail) ที่ไม่มีการล็อคอินแบบปลอดภัย (Secure Login) หรือป๊อปทรี (Pop3) เช่น เอาท์ลุค (Outlook) แล้วไปใช้ฮ็อตเมล์ (hotmail.com) หรือ ยะฮู (yahoo.com)แทน

4) ผู้ใช้ต้องเลิกใช้เอฟทีพีอัพโหลด (FTP Upload) แต่หันไปใช้ไฟล์แมเนจเจอร์ (File Manager) ที่เว็บมีให้ ต้องเลือกที่บริการการล็อคอินแบบปลอดภัย

จากการที่ผู้เขียนได้ทำการศึกษาถึงความหมายของแฮ็คเกอร์ วิเคราะห์ได้ว่า การที่ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้อันเนื่องมาจาก ระบบอิเล็กทรอนิกส์ในการชำระหนี้ถูกแฮ็คไม่ว่าจะเป็นวิธีใดๆ ก็ตาม ดังที่ได้กล่าวไว้ข้างต้น ทำให้ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้ แม้ว่าเหตุการณ์ที่เกิดขึ้นมิได้เกิดจากการกระทำของตัวลูกหนี้เองก็ตาม ซึ่งถือว่าเป็นเหตุการณ์ที่เกิดจากการกระทำจากบุคคลภายนอก ซึ่งจากการได้ศึกษาถึงเรื่องเหตุสุดวิสัยจากกฎหมายต่างประเทศต่างๆ จะเห็นได้ว่าเหตุการณ์ที่ทำให้ลูกหนี้ไม่สามารถปฏิบัติการชำระหนี้ได้ จะเกิดจากเหตุภายนอก ซึ่งมิได้เกิดจากการกระทำของลูกหนี้ก็ตาม แต่เหตุที่เกิดขึ้น ลูกหนี้ยังสามารถที่จะป้องกันไม่ให้เกิดเหตุการณ์นั้นได้ ซึ่งมีวิธีป้องกันแฮ็คดังที่ได้อธิบายไว้แล้ว ลูกหนี้จึงไม่สามารถนำเหตุที่เข้ามาขัดขวางไม่ให้ลูกหนี้ปฏิบัติการชำระหนี้ได้ นำมาเป็นข้ออ้างเพื่อให้การชำระหนี้เป็น

พ้นวิสัยตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 219 วรรคหนึ่ง ไม่ได้ ลูกหนี้ยังมีภาระ ที่ต้องปฏิบัติการชำระหนี้อยู่ต่อไป

2. ปัญหาในเรื่องการละเมิดสิทธิส่วนบุคคลโดยการนำข้อมูลส่วนตัวไปเปิดเผย หรือใช้ในทางที่ผิด

ความก้าวหน้าของเทคโนโลยีสารสนเทศ ทำให้เกิดรูปแบบใหม่ของการค้าที่เรียกว่า พาณิชย์อิเล็กทรอนิกส์ หมายถึง รูปแบบหรือแนวทางในการซื้อขายสินค้าข้อมูลและบริการผ่านระบบเครือข่ายคอมพิวเตอร์ สื่ออิเล็กทอนิกส์รวมทั้งการทำธุรกิจการค้าบนระบบอินเตอร์เน็ต ทำให้ผู้ซื้อ ผู้ขายติดต่อสั่งซื้อสินค้า บริการและชำระเงินได้สะดวกมากขึ้น แต่การติดต่อสื่อสารกันผ่านการพาณิชย์อิเล็กทรอนิกส์ ผู้ซื้อผู้ขายไม่ได้พบกันโดยตรง จึงไม่สามารถยืนยันตัวบุคคลได้รูปแบบการชำระเงินผ่านทางอินเตอร์เน็ตจึงเข้ามาช่วยในการยืนยันตัวบุคคลที่กำลังติดต่อด้วยว่ามีตัวตนจริง ข้อมูลที่ใช้เพื่อยืนยันความมีตัวตนนี้นอกจากจะมีความเชื่อมโยงไปยังบุคคลแล้วยังมีความเชื่อมโยงไปถึงจำนวนเงินของบุคคลนั้นๆ ด้วย ผู้ที่ได้ข้อมูลเหล่านี้ไปเปรียบเสมือนได้จำนวนเงินไปด้วย ข้อมูลอิเล็กทรอนิกส์เกี่ยวกับการเงินเหล่านี้ ได้แก่ หลายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต รหัสลูกค้า เป็นต้น ข้อมูลอิเล็กทรอนิกส์เกี่ยวกับการเงินนี้จะจัดทำขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์ซึ่งไม่สามารถมองเห็นได้ว่ามีข้อความว่าอย่างไร โดยจัดทำขึ้นในสื่ออิเล็กทรอนิกส์รูปแบบต่างๆ เช่น บัตรเครดิต ซึ่งในประเทศไทยก็เคยมีการแก้ไขข้อมูลอิเล็กทรอนิกส์และเอาเงินจำนวนที่แก้ไขในคอมพิวเตอร์ไป ซึ่งมีคำพิพากษาฎีกาไปแล้ว เรื่องนี้จำเลยเป็นพนักงานธนาคารมีการจัดเก็บข้อมูลและดำเนินธุรกิจด้วยคอมพิวเตอร์ ทำรายการถอนเงินที่ข้อมูลคอมพิวเตอร์แต่ไม่มีรายการถอนเงินในสมุดคู่ฝาก รายการทั้ง 2 แห่งแตกต่างกันเนื่องจากการทุจริต มีการลักลอบทำรายการถอนเงินอันเป็นเท็จในคอมพิวเตอร์และเอาเงินจำนวนนั้นไป โดยไม่ปรากฏการทำรายการถอนเงินดังกล่าวในสมุดคู่ฝาก เหตุที่พบการกระทำความผิดนี้ เนื่องจาก เจ้าของบัญชีมาติดต่อเพื่อขอลงรายการรับดอกเบี้ยตรวจพบความแตกต่างของรายการในสมุดคู่ฝากและในข้อมูลจากเครื่องคอมพิวเตอร์ที่เรียกมาได้ โดยสมุดคู่ฝากมีรายการฝากเงิน 1,100,000 บาท เมื่อวันที่ 7 เมษายน 2538 โดยยอดเงินคงเหลือไม่ได้เพิ่มขึ้นจากรายการเหนือขึ้นไป ซึ่งบันทึกเมื่อวันที่ 7 มีนาคม 2538 แสดงว่า ในระหว่าง 2 วันนั้นมีรายการถอนเงิน 1,100,000 บาท ที่ไม่ได้บันทึกในสมุด ในกรณีนี้ศาลพิพากษาว่าจำเลยมีความผิดฐานลักทรัพย์

ดังนั้น การนำข้อมูลอิเล็กทรอนิกส์ไปและหาประโยชน์โดยมิชอบด้วยกฎหมาย ไม่มีกฎหมายใดบัญญัติลงโทษผู้ที่นำข้อมูลไปใช้ไว้โดยเฉพาะ ผู้เขียนเห็นว่าควรมีการนำกฎหมายอาญา

แก้ไขเพิ่มเติม ฉบับที่ 17 พ.ศ.2547 มาบังคับใช้โดยอนุโลม ซึ่งมีบัญญัติไว้ในมาตรา 269/5 และมาตรา 269/6

ตามประมวลกฎหมายอาญา มาตรา 269/5 บัญญัติว่า ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชนต้องระวางโทษ

ตามประมวลกฎหมายอาญา มาตรา 269/6 บัญญัติว่า ผู้ใดมีไว้เพื่อนำออกใช้ ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 ในประการน่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชนต้องระวางโทษ

ตามประมวลกฎหมายอาญามาตรา 1 (14) (ข) บัญญัติว่า "บัตรอิเล็กทรอนิกส์" หมายความว่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชื่อทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้ผู้มีสิทธิใช้โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้

มาตรานี้เป็นความผิดกรณีที่ใช้บัตรอิเล็กทรอนิกส์โดยมิชอบ และบัตรนั้นจะต้องเป็นของผู้อื่น มิใช่บัตรของตนเองและบัตรนั้นต้องไม่ใช่บัตรอิเล็กทรอนิกส์ปลอม ถ้าเป็นบัตรอิเล็คทรอ-นิกส์ปลอมจะเป็นความผิดตามมาตรา 269/4

หมายเลขบัตรเครดิต รวมทั้งวันหมดอายุของบัตรที่ปรากฏอยู่บนบัตรไม่ใช่ บัตรอิเล็กทรอนิกส์ ตามนิยามในมาตรา 1(14) (ก) (ค) และก็ไม่เข้าตาม (ข) เพราะเป็นข้อมูลหรือหมายเลขที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมีการออกเอกสารหรือวัตถุอื่นใดให้ด้วย กล่าวคือปรากฏอยู่บนบัตรเครดิตนั้นเอง ดังนั้นหากมีการนำเอาเฉพาะหมายเลขบัตรเครดิตของผู้อื่นไปใช้โดยมิชอบก็ไม่เป็นความผิดตามมาตรานี้ เพราะหมายเลขดังกล่าวไม่ใช่ บัตรอิเล็กทรอนิกส์

ในบรรดาบทบัญญัติที่เพิ่มขึ้นมาในหมวดนี้ บัตรอิเล็กทรอนิกส์ตาม (ข) สามารถนำมาใช้กับความผิดที่กำหนดในมาตรา 269/5 นี้ มาตราเดียว เนื่องจากบัตรอิเล็กทรอนิกส์ตาม (ข) นั้น โดยลักษณะข้องการใช้แล้วไม่สามารถจะปลอมกันได้ เพราะการใช้บัตรอิเล็กทรอนิกส์ตาม (ข) ผู้ใช้ต้องใช้บัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้กับระบบคอมพิวเตอร์ของผู้ออกบัตร ถ้าเป็นบัตรอิเล็กทรอนิกส์ปลอมก็จะใช้ไม่ได้ ก็จะมีแต่บัตรอิเล็กทรอนิกส์ที่แท้จริงเท่านั้นที่ใช้ได้ และการใช้บัตรอิเล็กทรอนิกส์ (ข) ของผู้อื่นโดยมิชอบ (ข) ซื้อสินค้าหรือบริการบนอินเตอร์เน็ต แล้วมีผู้ลักลอบเอาบัตรอิเล็กทรอนิกส์หรือรหัสของผู้มีสิทธ์ใช้ไปใช้

ส่วนบัตรอิเล็กทรอนิกส์ตาม (ค) หากเป็นการนำลักษณะเฉพาะตัวบุคคล เช่น ลายนิ้วมือของผู้อื่นไปใช้โดยมิชอบก็เป็นความผิดฐานนี้ด้วยดังที่ได้กล่าวมาแล้วในบทที่2ว่าบัตรอิเล็กทรอนิกส์ตาม (ค) ไม่ได้จำกัดเพียงลักษณะเฉพาะตัวของบุคคล เนื่องจากนิยามใช้คำว่า สิ่งอื่นใด ดังนั้น รหัสประจำตัวบุคคลก็อาจเป็นบัตรอิเล็กทรอนิกส์ตาม (ค) ของผู้อื่นไปใช้ก็จะเป็นความผิดฐานนี้ด้วย และเนื่องจากบัตรอิเล็กทรอนิกส์ตาม (ค) มีไว้เพื่อวัตถุประสงค์ในการระบุตัว

บุคคลที่เป็นเจ้าของ การนำบัตรอิเล็กทรอนิกส์ตาม (ค) ของผู้อื่นไปใช้อาจมีความผิดฐานฉ้อโกง โดยเฉพาะตนเป็นบุคคลอื่นได้อีกด้วยตามมาตรา 342 (1) แห่งประมวลกฎหมายอาญา

การกระทำความผิดตามมาตรานี้อาจเป็นความผิดฐานอื่นๆ อีกด้วย เช่น ลักทรัพย์ เช่น การลักบัตรเอทีเอ็ม ไปกดเงินจากเครื่องจ่ายเงิน นอกจากมีความผิดฐานลักทรัพย์ คือ ลักบัตรและลักเงิน และความผิดตามมาตรา 188 แล้ว ยังมีความผิดตามมาตรานี้อีกบทหนึ่งด้วย เพราะบัตรเอทีเอ็มก็คือบัตรอิเล็กทรอนิกส์ตามนิยามในมาตรา 1 (4) ที่เพิ่มเติมแก้ไขใหม่นี้

จากหลักกฎหมายดังกล่าวข้างต้นเป็นกรณีที่ใช้บัตรอิเล็กทรอนิกส์โดยมิชอบ และบัตรนั้นจะต้องเป็นของผู้อื่น มิใช่บัตรของตนเอง และบัตรนั้นต้องไม่ใช่บัตรอิเล็กทรอนิกส์ปลอม บทบัญญัติที่เพิ่มขึ้นมาในหมวดนี้บัตรอิเล็กทรอนิกส์ตามมาตรา (14) (ข) สามารถนำมาใช้กับความผิดที่กำหนดในมาตรา 269/5 นี้ มาตราเดียว เนื่องจากบัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) นั้นโดยลักษณะของการใช้กันแล้วไม่สามารถจะปลอมกันได้ เพราะการใช้บัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) ผู้ใช้ต้องใช้บัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้กับระบบคอมพิวเตอร์ ของผู้ออกบัตรถ้าเป็นบัตรอิเล็กทรอนิกส์ปลอมก็จะใช้ไม่ได้ ก็จะมีแต่บัตรอิเล็กทรอนิกส์ที่แท้จริงเท่านั้นที่ใช้ได้และการใช้บัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) ของผู้อื่นโดยมิชอบ เช่น การใช้บัตรอิเล็กทรอนิกส์ ตามมาตรา 1 (14) (ข) ที่ผู้ออกได้ออกให้ผู้มีสิทธิใช้ ใช้บัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) ซื้อสินค้าและบริการบนอินเตอร์เน็ต แล้วมีผู้ลักลอบเอาบัตรอิเล็กทรอนิกส์หรือรหัสของผู้มีสิทธิไปใช้ เพราะฉะนั้นผู้ที่นำข้อมูลทางอิเล็กทรอนิกส์ออกเปิดเผย จึงมีเพียงประมวลกฎหมายอาญา มาตรา 269/5 ที่จะเอาผิดกับผู้ที่นำข้อมูลออกเปิดเผยโดยทุจริต