

ความรับผิดชอบทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต



นายเชิดพันธุ์ อุปนิสากร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สาขาวิชานิติศาสตร์ ภาควิชานิติศาสตร์

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2542

ISBN 974-334-686-4

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

CRIMINAL LIABILITY OF HACKERS

Mr.Cherdpun Ubanisakorn

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Law

Department of Law

Faculty of Law

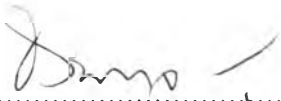
Chulalongkorn University

Academic Year 1999

ISBN 974-334-686-4

หัวข้อวิทยานิพนธ์ ความรับผิดชอบทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต
โดย นายเชิดพันธุ์ อุปนิสากร
ภาควิชา นิติศาสตร์
อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ

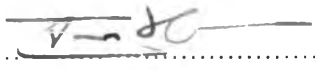
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่ง
ของการศึกษาตามหลักสูตรปริญญาโทบริหารธุรกิจ

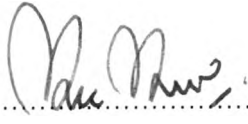

..... คณบดีคณะนิติศาสตร์
(รองศาสตราจารย์ ชงทอง จันทรางศุ)

คณะกรรมการสอบวิทยานิพนธ์


..... ประธานกรรมการ
(อาจารย์อิทธิพล ศรีเสาวลักษณ์)


..... อาจารย์ที่ปรึกษา
(รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ)


..... กรรมการ
(อาจารย์ ดร.จิรนิติ หะวานนท์)


..... กรรมการ
(อาจารย์ ดร.กิตติพงษ์ กิตยารักษ์)

บทคัดย่อวิทยานิพนธ์

เชิดพันธุ์ อุปนิสากร : ความรับผิดทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต. (Criminal liability of Hackers) อ. ที่ปรึกษา : รองศาสตราจารย์ ดร.อภิรัตน์ เพ็ชรศิริ, ๑๔๕ หน้า. ISBN ๙๗๔-๓๓๔-๖๘๖-๕.

การวิจัยครั้งนี้มีจุดมุ่งหมายเพื่อที่จะศึกษาหาคำนิยามของบุคคลที่ถูกเรียกว่าแฮกเกอร์ และหาคำตอบว่า รัฐควรจะมีนโยบายทางอาญาสำหรับบุคคลผู้นี้เช่นไร อีกทั้งหาแนวทางในการป้องกันการเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตโดยทั่วไป

ผลการวิจัยพบว่า ในปัจจุบันมีการใช้คำว่าแฮกเกอร์อย่างแพร่หลาย โดยไม่ทราบความหมายที่แน่นอน อีกทั้งเป็นคำในภาษาต่างประเทศ ดังนั้นในการกำหนดคำนิยามในภาษาไทยเพื่อผลในทางนิติศาสตร์ จึงเห็นควรสร้างความชัดเจนโดยกำหนดคำนิยามตามลักษณะของการกระทำอันได้แก่กิจกรรมเจาะระบบคอมพิวเตอร์ ดังนั้นในทางนิตินัยแฮกเกอร์จึงหมายถึง ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

สำหรับนโยบายทางอาญาสำหรับผู้เจาะระบบคอมพิวเตอร์นั้น สามารถแยกพิจารณาได้เป็น ๔ ประการ คือ ประการแรก มาตรการทางอาญาควรกำหนดขึ้นเพื่อลดหรือจำกัดแรงจูงใจในการกระทำของผู้เจาะระบบคอมพิวเตอร์ ประการที่สอง ควรบัญญัติกฎหมายเป็นพิเศษเนื่องจากพบว่ากฎหมายที่มีอยู่ในปัจจุบันไม่สามารถรองรับกับผู้กระทำความผิดได้ ประการที่สาม ควรกำหนดวิธีการลงโทษและระดับของโทษตามลักษณะของแรงจูงใจ ประการที่สี่ ควรสร้างความร่วมมือและเพิ่มประสิทธิภาพของหน่วยงานต่างๆในกระบวนการยุติธรรม

นอกจากนี้ในส่วนการป้องกันการเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ได้เสนอแนวทางในการกำหนดให้เป็นความผิดสำเร็จเมื่อมีการแรกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เพื่อเป็นมาตรการแรกในการป้องกันการกระทำความผิดใดๆที่อาจจะเกิดขึ้น ภายหลังจากการเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และพบว่าเมื่อพิจารณาแนวทางดังกล่าวประกอบกับทฤษฎีทางกฎหมายอาญา สามารถเป็นทางเลือกหนึ่งในการที่จะนำไปใช้กับการกระทำความผิดต่อระบบคอมพิวเตอร์ในอนาคต

ภาควิชานิติศาสตร์.....
สาขาวิชานิติศาสตร์.....
ปีการศึกษา ๒๕๔๒

ลายมือชื่อนิสิต
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

AN ABSTRACT

3970470434 : MAJOR LAW

KEY WORD: Hacker / Computer / / /

CHERDPUN UBANISAKOUN : CRIMINAL LIABILITY OF HACKERS. (CRIMINAL LIABILITY OF HACKERS) THESIS ADVISOR : ASSOCIATE PROFESSOR APIRAT PETCHSIRI,S.J.D., THESIS COADVISOR :, 145 pp. ISBN 974-334-686-4.

The aim of this research is to define the word "hacker" and to go on to suggest taking legal proceedings on behalf of the government ,putting forward some guidelines in the prevention of illegal computer system access.

The findings reveal that the word "hacker" is widely used without a clear definition in the Thai Language. It is a foreign word,defining the word is legally beneficial. By law a hacker is somebody who illegally gains access to a computer system.

Four legal policies are suggested. First of all, criminal penalties should be prescribed to dissuade hackers. Secondly, a special provision is needed because the current law does not lead to criminal proceedings. Thirdly, the type and degree of punishment should be based on the offender's motives. Lastly, the cooperation and the efficient working of the various parts of the organization in judicial administration should be supported.

In order to prevent computer system breakdown and any resulting offence, illegal access to a computer system should be considered an offence. In conclusion, this suggestions together with the proposed four guidelines is suggested as an alternative means to cope with computer crime

ภาควิชานิติศาสตร์.....
สาขาวิชานิติศาสตร์.....
ปีการศึกษา 2542

ลายมือชื่อนิติสด
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้จะไม่สามารถสำเร็จลุล่วงไปได้ถ้าปราศจากความเมตตาและความช่วยเหลือจากผู้มีพระคุณดังต่อไปนี้

อาจารย์อภิรัตน์ เพ็ชรศิริ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ช่วยผลักดันให้ผู้เขียนฝ่าฟันอุปสรรคและปัญหาต่างๆ ได้อย่างไม่ย่อท้อตั้งแต่เริ่มต้นทำวิทยานิพนธ์ อีกทั้งให้เวลาแก่ผู้เขียนในการซักถามเมื่อมีปัญหาเสมอมาแม้ท่านจะมีภาระหน้าที่หลายประการซึ่งต้องรับผิดชอบ

อาจารย์ ดร.จิรนิติ หะวานนท์ เลขาธิการศาลฎีกา ที่ท่านทำให้ผู้เขียนเห็นแบบอย่างและตระหนักว่าผู้ที่มีจิตวิญญาณของความเป็นอาจารย์โดยแท้จริงมีลักษณะอย่างไร

อาจารย์ ดร.กิตติพงษ์ กิตยารักษ์ ผู้อำนวยการสถาบันกฎหมายอาญา ที่ท่านได้ให้ความสนใจไต่ถามความคืบหน้าและช่วยให้คำแนะนำที่เป็นประโยชน์อย่างมากในด้านกฎหมายอาญา

อาจารย์อิทธิพล ศรีเสาวลักษณ์ ประธานกรรมการสอบวิทยานิพนธ์ ซึ่งได้สละเวลามาเป็นประธานกรรมการและให้คำแนะนำในการสอบวิทยานิพนธ์

ขอขอบพระคุณอาจารย์ภาคีวิชาทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ทั้งในตำราและนอกตำราเรียน อันเป็นประสบการณ์ที่ดีตลอดระยะเวลาที่ศึกษาอยู่ จนกระทั่งสำเร็จการศึกษา

ขอขอบพระคุณสำหรับมิตรไมตรี ความห่วงใย กำลังใจ และความรู้สึที่ดีๆ ที่ได้รับจากเพื่อนๆ ทุกคนในรุ่น ๓๙

ขอขอบคุณ คุณวสันต์ เจนร่วมจิตที่ช่วยค้นคว้าข้อมูลทางคอมพิวเตอร์ และเจ้าหน้าที่งานรับฟัง ศาลฎีกาทุกท่านที่ให้การสนับสนุนและให้กำลังใจเสมอมา

เหนือสิ่งอื่นใด ผู้เขียนวิทยานิพนธ์ขอกราบขอบพระคุณ บิดา ซึ่งสนับสนุนในด้านการเงินและให้ความรัก ความห่วงใย แก่ผู้เขียนมาโดยตลอด

อนึ่ง หากมีความดีส่วนใดที่เกิดขึ้นจากเนื้อหาในวิทยานิพนธ์ฉบับนี้ และเป็นส่วนที่ทำให้เกิดผลบุญขึ้น ผู้เขียนใคร่ขออุทิศแด่ มารดาผู้ล่วงลับ ซึ่งไม่มีโอกาสได้เห็นความสำเร็จที่ท่านมีส่วนร่วม และเป็นผู้ให้กำลังใจแก่ผู้เขียนในยามเหนื่อยล้าเสมอมา สำหรับข้อบกพร่องทั้งหลายผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

เชิดพันธุ์ อุปนิสากร

สารบัญ

๗

หน้า

บทคัดย่อภาษาไทย	๖
บทคัดย่อภาษาอังกฤษ	๗
กิตติกรรมประกาศ	๘
สารบัญ	๗

บทที่

บทที่ ๑ บทนำ

๑.๑	ความเป็นมาและความสำคัญของปัญหา	๑
๑.๒	วัตถุประสงค์ของการวิจัย	๒
๑.๓	ประโยชน์ที่คาดว่าจะได้รับ	๒
๑.๔	วิธีดำเนินการวิจัย	๒
๑.๕	สมมุติฐานในการวิจัย	๓

บทที่ ๒ ความทั่วไปว่าด้วยแฮกเกอร์และการเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต

๑.	คำนิยาม	๔
๑.๑	แฮกเกอร์คือใคร	๔
๑.๒	สาเหตุที่ทำให้ คำนิยามของคำว่าแฮกเกอร์แตกต่างกัน	๖
๑.๓	กลุ่มของคำนิยาม	๖
๑.๓.๑	การให้คำนิยามโดยอาศัยความเห็น	๖
๑.๓.๒	การให้คำนิยามที่กำหนดโดยอาศัยเจตนาของ การกระทำ	๘
๑.๓.๓	การให้คำนิยามโดยอาศัยลักษณะของการกระทำ	๑๐
๑.๔	ผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต.....	๑๒
๑.๔.๑	ระบบคอมพิวเตอร์	๑๒
-	ระบบเครือข่าย	๑๔
-	อินเทอร์เน็ต	๑๔
๑.๔.๒	การเจาะระบบคอมพิวเตอร์	๑๕
๑.๔.๓	การกระทำโดยไม่มีอำนาจหรือไม่ได้รับอนุญาต	๑๘

สารบัญ (ต่อ)

๗

หน้า

๑.๔.๔	ความหมายของผู้เจาะระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต.....	๑๘
๒.	การเจาะระบบคอมพิวเตอร์ทำอะไร	๑๙
๒.๑	การเริ่มเจาะระบบคอมพิวเตอร์โดยทั่วไป	๒๐
๒.๒	เครื่องมือที่นำมาสนับสนุนการเจาะระบบคอมพิวเตอร์	๒๒
บทที่ ๓	การกำหนดความผิดทางอาญาต่อผู้เจาะระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต.....	๒๕
๑.	แนวคิดทั่วไปในการกำหนดความผิดทางอาญา	๒๕
๑.๑	ความหมายของกฎหมายอาญา	๒๕
๑.๒	มุมมองของการกระทำความผิดและกฎหมายอาญา	๒๖
๑.๒.๑	มุมมองทางด้านต้นกำเนิดของความคิด	๒๖
๑.๒.๒	มุมมองทางด้านแรงขับที่ไม่สามารถอธิบาย ได้ด้วยเหตุผล	๒๗
๑.๒.๓	มุมมองทางด้านประวัติศาสตร์	๒๘
๑.๒.๔	มุมมองด้านแก่นของจริยศาสตร์	๒๘
๑.๒.๕	มุมมองด้านจุดประสงค์ของกฎหมายอาญา	๒๙
	- การควบคุมการกระทำความผิด	๓๐
	- การควบคุมความมีศีลธรรม	๓๑
๑.๓	การกระทำใดสมควรกำหนดเป็นความผิดอาญา	๓๒
๒.	การกระทำของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตสมควร เป็นความผิดทางอาญาหรือไม่	๓๔
๒.๑	การเจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นการกระทำ ที่กระทบกระเทือนและก่อให้เกิดความเสียหายแก่สังคมหรือไม่ .	๓๔
๒.๒	เมื่อมีการกำหนดความรับผิดทางอาญาจะกระทบต่อ ความก้าวหน้าทางเทคโนโลยีในประเทศไทยหรือไม่	๔๔
๒.๓	การนำกฎหมายอาญามารองรับการกระทำของผู้เจาะระบบ คอมพิวเตอร์จะเป็นการใช้กฎหมายอาญาเพื่อหรือไม่	๔๖
๒.๔	การนำความรับผิดทางแพ่งมารองรับการกระทำของผู้เจาะ ระบบคอมพิวเตอร์เพียงพอหรือไม่	๔๘

๒.๕	การนำหลักทางจริยธรรมมาเป็นแนวทางในการกำหนด ความประพฤติของผู้เจาะระบบคอมพิวเตอร์จะ เพียงพอหรือไม่	๕๑
บทที่ ๔	นโยบายทางอาญาสำหรับผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต.....	๕๖
๑.	การป้องกันมิให้เกิดการกระทำความผิดโดยกำจัดมูลเหตุแห่ง อาชญากรรม	๕๗
๑.๑	ทฤษฎีทางอาชญาวิทยา	๕๘
๑.๑.๑	กลุ่มทฤษฎีที่กล่าวถึงสาเหตุอาชญากรรมทางชีววิทยา	๖๐
๑.๑.๒	กลุ่มทฤษฎีที่กล่าวถึงสาเหตุอาชญากรรมทางจิตวิทยา	๖๑
๑.๑.๓	กลุ่มทฤษฎีที่กล่าวถึงสาเหตุอาชญากรรมทางสังคมวิทยา	๖๒
๑.๒	แรงจูงใจของผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต	๖๕
๑.๒.๑	แรงจูงใจทางสังคม	๖๕
๑.๒.๒	แรงจูงใจทางเทคนิค	๖๖
๑.๒.๓	แรงจูงใจทางการเมือง	๖๖
๑.๒.๔	แรงจูงใจทางการเงิน	๖๖
๑.๒.๕	แรงจูงใจทางรัฐบาล	๖๖
๑.๓	แรงจูงใจกับแนวโน้มการกระทำผิดและทฤษฎีทางอาชญาวิทยา	
๑.๓.๑	กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์ ที่เกิดจากแรงจูงใจทางสังคม	๖๗
๑.๓.๒	กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์ ที่เกิดจากแรงจูงใจทางเทคนิค	๖๘
๑.๓.๓	กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์ ที่เกิดจากแรงจูงใจทางการเมือง	๖๘
๑.๓.๔	กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์ ที่เกิดจากแรงจูงใจทางการเงิน	๖๙
๑.๓.๕	กรณีการกระทำของผู้เจาะระบบคอมพิวเตอร์ ที่เกิดจากแรงจูงใจทางรัฐบาล	๖๙

๒.	วิธีการทางนิติบัญญัติเพื่อจะได้ผลในทางป้องกันและปราบปราม	
	การกระทำความผิด	๗๒
๒.๑	หลัก Legality	๗๒
๒.๒	ปัญหาในการปรับใช้ประมวลกฎหมายอาญาในปัจจุบัน	๗๓
	๒.๒.๑ กรณีการกระทำต่อข้อมูลและระบบคอมพิวเตอร์ที่เกิดขึ้น	
	ภายหลังจากการเจาะเข้าไปในระบบคอมพิวเตอร์โดย	
	ไม่ได้รับอนุญาตแล้ว	๗๓
	๒.๒.๒ กรณีการกระทำก่อนหรือขณะเจาะระบบคอมพิวเตอร์ ..	๗๖
	- การเตรียมกระทำความผิด	๗๗
	- การกระทำอย่างไรเป็นการลงมือเจาะระบบ	
	คอมพิวเตอร์	๗๙
	- การพยายามเจาะระบบคอมพิวเตอร์	๘๐
	๒.๒.๓ กรณีการแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต	๘๐
๓.	วิธีการบังคับเพื่อจะได้ผลในทางป้องกันอาชญากรรม	๘๑
๓.๑	วัตถุประสงค์ของการลงโทษ	๘๑
	๓.๑.๑ ทฤษฎีการลงโทษเพื่อเป็นการแก้แค้น	๘๒
	๓.๑.๒ ทฤษฎีการลงโทษเพื่อเป็นการข่มขู่	๘๓
	๓.๑.๓ ทฤษฎีการลงโทษเพื่อเป็นการฟื้นฟูผู้กระทำความผิด ..	๘๔
	๓.๑.๔ ทฤษฎีการลงโทษเพื่อชดเชยการกระทำ	๘๔
	๓.๑.๕ ทฤษฎีการลงโทษเพื่อตัดไม่ให้มีโอกาสกระทำ	
	ความผิดอีก	๘๔
๓.๒	การลงโทษผู้เจาะระบบคอมพิวเตอร์ที่คำนึงถึงความเหมาะสม	
	แต่ละบุคคลตามลักษณะแรงจูงใจ	๘๕
	๓.๒.๑ การลงโทษกรณีผู้กระทำโดยมีแรงจูงใจเพื่อต้องการ	
	ให้เป็นที่ยอมรับของสังคม	๘๕
	๓.๒.๒ การลงโทษกรณีผู้กระทำโดยมีแรงจูงใจทางเทคนิค	๘๘
	๓.๒.๓ การลงโทษกรณีผู้กระทำโดยมีแรงจูงใจทางการเงิน	
	การเมือง ทางรัฐบาล	๘๙

สารบัญ (ต่อ)

ฎ

หน้า

๔.	การประสานงานระหว่างสถาบันที่มีส่วนในการป้องกันอาชญากรรม	๙๐
๔.๑	ประเทศไทย	๙๑
๔.๒	สหรัฐอเมริกา	๙๐
๔.๒.๑	The U.S. Secret Service	๙๐
๔.๒.๒	NCCS	๙๓
๔.๒.๓	IPTF	๙๓
๔.๒.๔	FCIC	๙๔
๔.๒.๕	CERT	๙๔
๕	แนวทางในการกำหนดให้การแรกเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต เป็นความผิดอาญา	๙๘
๑.	เหตุผลในการใช้มาตรการทางอาญากับการแรกเข้าไปในระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต	๙๘
๒.	ลักษณะของบทบัญญัติว่าด้วยการแรกเข้าสู่ระบบคอมพิวเตอร์ โดยไม่มีอำนาจควรมีลักษณะอย่างไร	๙๘
๓.	องค์ประกอบความผิดฐานบุกรุกและการแรกเข้าสู่ระบบคอมพิวเตอร์ โดยไม่ได้รับอนุญาต	๑๐๑
๓.๑	การเข้าไป	๑๐๓
๓.๒	ทรัพย์สิน	๑๐๘
๓.๓	การได้รับอนุญาต	๑๑๐
๓.๔	ความเสียหาย	๑๑๑
	- ความเสียหายต่อสิทธิความเป็นส่วนตัว	๑๑๒
	- ผลกระทบหรือความเสียหายต่อสิทธิในทรัพย์สิน	๑๑๔
๓.๕	เจตนา	๑๑๕
	- ข้อยกเว้นกรณีที่บุคคลไม่จำเป็นต้องมีเจตนาที่ต้องรับผิด	๑๑๖
๓.	กฎหมายต่างประเทศ	๑๒๐
๓.๑	ประเทศสหรัฐอเมริกา	๑๒๑
๓.๒	ประเทศสาธารณรัฐประชาชนจีน	๑๒๗
๓.๓	ประเทศฟินแลนด์	๑๒๗
๓.๔	ประเทศกรีซ	๑๒๘

สารบัญ (ต่อ)

ฏ

หน้า

๓.๕	ประเทศไอร์แลนด์	๑๒๙
๓.๖	ประเทศอิตาลี	๑๒๙
๓.๗	ประเทศนอร์เวย์	๑๓๐
๓.๘	ประเทศสวีเดน	๑๓๐
บทที่ ๖. บทสรุปและเสนอแนะ		๑๓๒
รายการอ้างอิง		๑๓๙
ประวัติผู้วิจัย		๑๔๕