

สารบัญ

คำนำ

บทนำและโครงสร้างของหนังสือ 1

ภาค 1 ความผิดเกี่ยวกับการฉ้อโกงหลอกลวงและการปลอมแปลง

ทางคอมพิวเตอร์ 6

บทที่ 1 การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Computer-related fraud
หรือ Cyber fraud) 8

1.1 การจำแนกประเภทของการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ 9

1.2 เหตุผลของการกำหนดความผิดเฉพาะสำหรับการฉ้อโกงทางคอมพิวเตอร์ 12

1.3 ความผิดฐานฉ้อโกงตามกฎหมายอาญาเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ 15

1.4 การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ตามอนุสัญญาอาชญากรรมไซเบอร์ 17

1.5 แนวทางในการบัญญัติฐานความผิดเกี่ยวกับการฉ้อโกงหลอกลวง
ทางคอมพิวเตอร์ 19

1.5.1 แนวทางที่หนึ่ง ไม่กำหนดฐานความผิดเฉพาะสำหรับการฉ้อโกง

ทางคอมพิวเตอร์ 20

1.5.2 แนวทางที่สอง กำหนดฐานความผิดเฉพาะสำหรับการฉ้อโกง

ทางคอมพิวเตอร์แต่องค์ประกอบความผิดสะท้อนถึงการหลอกลวง

บุคคล 22

1.5.3 แนวทางที่สาม กำหนดฐานความผิดเฉพาะสำหรับการฉ้อโกง

ทางคอมพิวเตอร์ซึ่งมีองค์ประกอบความผิดเจาะจงสำหรับการกระทำ

ที่มีเป้าหมายต่อการทำงานหรือการประมวลผลโดยอัตโนมัติ 23

1.6 ความผิดฐานฉ้อโกงหลอกลวงทางคอมพิวเตอร์ ตามพ.ร.บ.คอมพิวเตอร์ 27

1.7 อธิบายมาตรา 14 (1) เปรียบเทียบกับความผิดฐานฉ้อโกง

ทางคอมพิวเตอร์ของต่างประเทศ โดยจำแนกตามองค์ประกอบ 28

1.7.1 องค์ประกอบส่วนการกระทำ 28

1.7.2 องค์ประกอบวัตถุแห่งการกระทำ 29

1.7.3 องค์ประกอบส่วนการกระทำต่อข้อมูลหรือระบบ 30

1.7.4 องค์ประกอบเจตนาพิเศษเกี่ยวกับการแสวงประโยชน์	31
1.7.5 องค์ประกอบด้านความเสียหายต่อทรัพย์สินของผู้อื่น	32
1.7.6 องค์ประกอบด้านขอบเขตความเสียหาย	32
1.7.7 องค์ประกอบเกี่ยวกับความจริงหรือเท็จของข้อมูล	33
1.7.8 ตารางสรุปเปรียบเทียบองค์ประกอบมาตรา 14 (1) กับความผิด ฐานฉ้อโกงทางคอมพิวเตอร์ของต่างประเทศ	35
1.7.9 ข้อวิพากษ์	39
1.8 อธิบายมาตรา 14 (1) เปรียบเทียบกับฐานความผิดฉ้อโกง ตามกฎหมายอาญา	40
1.9 อธิบายมาตรา 14 (1) โดยจำแนกตามประเภทของการฉ้อโกง หลอกลวงทางคอมพิวเตอร์	44
1.9.1 การฉ้อโกงทางคอมพิวเตอร์ที่มุ่งหลอกลวงบุคคล และการฉ้อโกง ทางคอมพิวเตอร์ที่มุ่งหลอกลวงระบบหรือโปรแกรมคอมพิวเตอร์	45
1.9.2 การหลอกลวงซอฟต์แวร์หรือโปรแกรมที่ใช้วิเคราะห์ข้อมูล (Analytics software)	50
1.9.3 การใช้วิธีการทางเทคนิคเพื่อส่งจดหมายหรือข้อความอิเล็กทรอนิกส์ ผ่านโปรแกรมหรือซอฟต์แวร์คัดกรอง (Filtering software)	51
1.9.4 การใช้มัลแวร์ที่มีลักษณะคล้ายกับการหลอกลวง	53
1.9.5 อาชญากรรมประเภท “Phishing” ซึ่งใช้วิธีการในลักษณะ ของการหลอกลวง	59
1.9.6 การใช้วิธีการทางเทคนิคเพื่อเพิ่มหรือสร้างปริมาณเข้าชมข้อมูล หรือการมีปฏิสัมพันธ์เนื้อหาข้อมูลคอมพิวเตอร์	60
1.9.7 การฉ้อโกงหลอกลวงในระบบการชำระเงินทางอิเล็กทรอนิกส์	73
1.9.7.1 การฉ้อโกงหลอกลวงที่เกี่ยวกับสินทรัพย์ดิจิทัล	73
1.9.7.2 การฉ้อโกงเกี่ยวกับการชำระเงินผ่านกระเป๋าเงิน อิเล็กทรอนิกส์ (E wallet หรือ Mobile wallet)	77
1.9.7.3 การฉ้อโกงที่เกี่ยวกับโปรแกรมประยุกต์ของธนาคาร (Mobile banking Application)	80
1.9.7.4 การฉ้อโกงหลอกลวงเกี่ยวกับการชำระเงินด้วย QR Code....	83
1.9.8 การฉ้อโกงที่เกี่ยวข้องกับเทคโนโลยีบล็อกเชน (Blockchain)	87
1.9.9 การฉ้อโกงที่เกี่ยวกับสัญญาแบบสมาร์ท (Smart contract)	89

1.10 ประเด็นทางกฎหมายเกี่ยวกับการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ กับมาตรา 14 วรรคท้าย	92
1.11 การโจรกรรมข้อมูลเอกลักษณ์ (Identity theft) กับการฉ้อโกง หลอกลวงทางคอมพิวเตอร์	97
1.11.1 ลักษณะของพฤติกรรมและกฎหมายที่เกี่ยวข้องในภาพรวม	98
1.11.2 ขอบเขตความสัมพันธ์ระหว่างการโจรกรรมข้อมูลเอกลักษณ์ กับการฉ้อโกงทางคอมพิวเตอร์	100
1.11.3 การปรับใช้ความผิดฐานฉ้อโกงตามกฎหมายอาญากับ การโจรกรรมข้อมูลเอกลักษณ์ทางระบบคอมพิวเตอร์	101
1.11.4 การปรับใช้ความผิดฐานฉ้อโกงหลอกลวงทางคอมพิวเตอร์ตาม พ.ร.บ.คอมพิวเตอร์กับการโจรกรรมข้อมูลเอกลักษณ์ทางระบบ คอมพิวเตอร์	103
1.12 เปรียบเทียบความผิดฐานปลอมตัวออนไลน์ (Online impersonation) ตามกฎหมายสหรัฐอเมริกากับการฉ้อโกงทางคอมพิวเตอร์	109
บทที่ 2 อาชญากรรมคอมพิวเตอร์ประเภท “ฟิชซิง” (Phishing)	115
2.1 ความหมายและลักษณะของฟิชซิง (Phishing)	116
2.2 การจำแนกประเภทของฟิชซิง (Phishing)	118
2.3 แนวทางกำหนดความผิดสำหรับฟิชซิง (Phishing)	119
2.3.1 แนวทางที่หนึ่ง กำหนดความผิดเกี่ยวกับฟิชซิง โดยพิจารณาจากแง่มุม ของพฤติกรรมการฉ้อโกงข้อมูลคอมพิวเตอร์	120
2.3.2 แนวทางที่สอง กำหนดความผิดเกี่ยวกับฟิชซิง โดยพิจารณา จากแง่มุมของพฤติกรรมการปลอมแปลงทางคอมพิวเตอร์	122
2.3.3 แนวทางที่สาม กำหนดความผิดเกี่ยวกับฟิชซิง โดยพิจารณา จากแง่มุมของพฤติกรรมการฉ้อโกงหลอกลวงทางคอมพิวเตอร์	123
2.3.4 แนวทางที่สี่ กำหนดความผิดเฉพาะสำหรับฟิชซิง โดยมี องค์ประกอบที่เจาะจงถึงลักษณะพฤติกรรม	125
2.3.5 แนวทางที่ห้า ไม่กำหนดความผิดเกี่ยวกับฟิชซิง แต่ฐานความผิด เกี่ยวกับอาชญากรรมคอมพิวเตอร์อื่นหรือกฎหมายอื่นมาปรับใช้	126
2.3.6 แนวทางกำหนดความผิดฐานฟิชซิง ตามพ.ร.บ.คอมพิวเตอร์	128
2.4 การปรับใช้ฐานความผิดตามพ.ร.บ.คอมพิวเตอร์ กับฟิชซิง (Phishing)	129

2.4.1 การปรับใช้ฐานความผิดที่เกี่ยวข้องเป็นรายมาตรา	130
2.4.1.1 การปรับใช้มาตรา 14 (1) กับฟิชซิง	130
2.4.1.2 การปรับใช้มาตรา 8 กับฟิชซิง	136
2.4.1.3 การปรับใช้ฐานความผิดมาตราอื่นกับฟิชซิง	139
2.4.2 อธิบายการปรับใช้ฐานความผิดตามชนิดหรือประเภทของฟิชซิง	139
2.5 ฟิชซิง (Phishing) กับอาชญากรรมคอมพิวเตอร์อื่น	142
บทที่ 3 อาชญากรรมคอมพิวเตอร์ประเภท “Scam”	147
3.1 ความหมายและลักษณะของ “Scam”	147
3.2 ความสัมพันธ์ของฐานความผิดตามพ.ร.บ.คอมพิวเตอร์ กับ “Scam”	149
3.3 อธิบายการปรับใช้มาตรา 14 (1) กับ “Scam”	151
3.4 อธิบายการปรับใช้กฎหมาย โดยจำแนกตามประเภทของ “Scam”	154
3.4.1 “Scam” เกี่ยวกับการซื้อขายสินค้าหรือบริการ	155
3.4.2 “Scam” เกี่ยวกับการเสนอโอกาสการลงทุน (Investment scam)....	157
3.4.3 “Scam” เกี่ยวกับการเสนอผลประโยชน์ในลักษณะได้เปล่า แต่มีเงื่อนไขต้องกระทำบางอย่าง	164
3.4.4 “Scam” เกี่ยวกับการจ้างแรงงาน (Recruitment scam, employment or job scam)	166
3.4.5 “Scam” เกี่ยวกับการอ้างหน้าที่หรือความรับผิดชอบทางกฎหมาย	167
3.4.6 “Scam” เกี่ยวกับการบริจาคหรือการกุศล (Charity scam)	170
3.4.7 “Scam” เกี่ยวกับความสัมพันธ์ระหว่างบุคคลในเชิงความรัก (Romance scam)	172
3.5 “Scam” ที่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยของระบบ และข้อมูลคอมพิวเตอร์	179
3.5.1 Security warning หรือ Security Alert Scam หรือ Free Security (การหลอกลวงโดยเสนอให้บริการตรวจสอบ ความปลอดภัยของระบบ หรือข้อมูลคอมพิวเตอร์)	180
3.5.2 Technical Support Scam (การแอบอ้างเป็นผู้ให้บริการ ทางเทคนิค)	181
3.6 Scam กับการปลอมแปลงทางคอมพิวเตอร์	185
3.7 Scam กับอาชญากรรมคอมพิวเตอร์อื่น	187

บทที่ 4 การปลอมแปลงทางคอมพิวเตอร์ (Computer-related forgery)	190
4.1 ความผิดฐานปลอมแปลงทางคอมพิวเตอร์ (Computer-related forgery) ตามอนุสัญญาอาชญากรรมไซเบอร์	191
4.2 เหตุผลของการกำหนดความผิดเฉพาะสำหรับการปลอมแปลง ทางคอมพิวเตอร์	192
4.3 แนวทางการบัญญัติความผิดฐานการปลอมแปลงทางคอมพิวเตอร์	196
4.3.1 แนวทางที่หนึ่ง กำหนดฐานความผิดเฉพาะสำหรับการ ปลอมแปลงทางคอมพิวเตอร์	196
4.3.2 แนวทางที่สอง ไม่กำหนดฐานความผิดเฉพาะสำหรับ การปลอมแปลงทางคอมพิวเตอร์แต่ปรับใช้กฎหมายอื่น	199
4.4 อธิบายองค์ประกอบและประเด็นทางกฎหมายของมาตรา 14 (1) ที่เกี่ยวกับการปลอมแปลงทางคอมพิวเตอร์	201
4.4.1 ประเด็นการบัญญัติความผิดฐานปลอมแปลงทางคอมพิวเตอร์ รวมกับความผิดฐานฉ้อโกงหลอกลวงทางคอมพิวเตอร์	201
4.4.2 เจตนารมณ์และคุณธรรมทางกฎหมายของความผิดฐาน ปลอมแปลงทางคอมพิวเตอร์	202
4.4.3 องค์ประกอบส่วนการกระทำ	204
4.4.4 การกระทำเกี่ยวกับการปลอมแปลง ที่ใกล้เคียงกับฐานความผิดอื่น....	207
4.4.5 ความแท้จริงของข้อมูลในแง่ผู้สร้างกับความจริงหรือเท็จ ของข้อมูลในแง่เนื้อหา	208
4.4.6 เป้าหมายของการกระทำ	210
4.4.7 องค์ประกอบเจตนาพิเศษ	211
4.4.8 การพิจารณาหรือกระทำทางกฎหมายกับข้อมูลปลอม เสมือนข้อมูลจริง	212
4.4.9 การหลอกลวงที่มุ่งต่อความเข้าใจผิดของมนุษย์กับการหลอกลวง ที่มุ่งต่อการประมวลผลโดยอัตโนมัติของระบบคอมพิวเตอร์	213
4.4.10 องค์ประกอบเกี่ยวกับขอบเขตผลกระทบ	216
4.4.11 ตารางเปรียบเทียบองค์ประกอบความผิดมาตรา 14 (1) กับความผิดฐานปลอมแปลงทางคอมพิวเตอร์ ตามกฎหมายต่างประเทศ	216

4.5 อธิบายการปรับใช้กฎหมายโดยจำแนกตามขั้นตอนของพฤติกรรม	
การปลอมแปลงทางคอมพิวเตอร์	218
4.5.1 ขั้นตอนที่หนึ่ง การได้มาซึ่งข้อมูล เพื่อนำมาทำข้อมูล	
คอมพิวเตอร์ปลอม	219
4.5.2 ขั้นตอนที่สอง การทำปลอมขึ้นซึ่งข้อมูลคอมพิวเตอร์	220
4.5.3 ขั้นตอนที่สาม การใช้ข้อมูลคอมพิวเตอร์ปลอม	221
4.6 อาชญากรรมเกี่ยวกับบัตรอิเล็กทรอนิกส์ในสภาพแวดล้อมดิจิทัล	222
4.6.1 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามกฎหมายอาญา	223
4.6.2 อธิบายการปรับใช้กฎหมายโดยจำแนกประเภทของพฤติกรรม	
การทำผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์	224
4.6.2.1 พฤติกรรมที่หนึ่ง การลักับัตรของผู้อื่นและ	
นำไปซื้อสินค้าหรือบริการ	225
4.6.2.2 พฤติกรรมที่สอง ทำบัตรอิเล็กทรอนิกส์ปลอมและ	
นำไปขายหรือนำไปใช้	227
4.6.2.3 พฤติกรรมที่สาม การนำข้อมูลระบุตัวตนของผู้อื่น	
ไปสมัครใช้งานบัตรและนำบัตรไปใช้	232
4.6.2.4 พฤติกรรมที่สี่ การได้มาและใช้บัตรอิเล็กทรอนิกส์	
ที่อยู่ในรูปของข้อมูลคอมพิวเตอร์โดยกระทำทั้งหมด	
ทางระบบคอมพิวเตอร์	236
4.7 การปลอมแปลงทางคอมพิวเตอร์กับอาชญากรรมอื่น	241
4.7.1 การปลอมแปลงทางคอมพิวเตอร์กับฟิชซิง (Phishing)	
และ “Pharming”	241
4.7.2 การปลอมแปลงทางคอมพิวเตอร์กับการโจรกรรมข้อมูลเอกลักษณ์ ...	243
4.7.3 การปลอมแปลงทางคอมพิวเตอร์กับความผิดอาญาอื่น	244
4.7.4 การปลอมแปลงทางคอมพิวเตอร์กับข้อโกงหลอกลวง	
ทางคอมพิวเตอร์	245
ภาค 2 ความผิดเกี่ยวกับสแปม (Spam)	248
บทที่ 5 บททั่วไปและหลักกฎหมายเกี่ยวกับสแปม	250
5.1 ความหมายของสแปม	250
5.2 โครงสร้างทางกายวิภาคของสแปม (Anatomy of spam)	254

5.3 องค์ประกอบของ “สแปม”	256
5.4 การจำแนกประเภทของสแปมตามวัตถุประสงค์	257
5.5 ปัจจัยสนับสนุนและผลกระทบของสแปม	259
5.6 หลักกฎหมายเกี่ยวกับสแปมตามพ.ร.บ.คอมพิวเตอร์	663
5.7 หลักและองค์ประกอบของฐานความผิดที่ 1 (มาตรา 11 วรรคหนึ่ง)	265
5.7.1 องค์ประกอบ “ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์”	265
5.7.2 องค์ประกอบ “ปกปิดหรือปลอมแปลงแหล่งที่มา	
ของการส่งข้อมูล”	265
5.7.2.1 การปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งกับ	
“Email Spoofing”	266
5.7.2.2 การปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง	
กับปัจจัยด้านความจริงหรือเท็จ	267
5.7.2.3 แหล่งที่มาของการส่งกับความมีอยู่จริง	
ของบุคคลที่เกี่ยวข้อง	269
5.7.2.4 การใช้วิธีการทางเทคนิคเพื่อหลบเลี่ยงระบบคัดกรองสแปม	
(Spam filtering system)	269
5.7.2.5 การปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง	
กับการหลอกลวงหรือทำให้เข้าใจผิด	275
5.7.2.6 การส่งจดหมายอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์	
ที่ขัดแย้งกับข้อสัญญา	276
5.7.2.7 การปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง	
กับรางวัลลิงก์ไปยังยูอาร์แอลโดยมีการเปลี่ยนแปลง	
เกิดขึ้นกับยูอาร์แอล	276
5.7.2.8 ความสัมพันธ์ขององค์ประกอบ “ปกปิดหรือปลอมแปลง	
แหล่งที่มาของการส่ง” กับฐานความผิดอื่น	278
5.7.3 องค์ประกอบ มูลเหตุชักจูงใจหรือเจตนาพิเศษ	279
5.7.4 องค์ประกอบ “อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์	
ของบุคคลอื่นโดยปกติสุข”	280
5.7.5 ความสัมพันธ์ระหว่าง “รบกวนการทำงานของระบบคอมพิวเตอร์	
ของผู้อื่นโดยปกติสุข” กับ “ปกปิดหรือปลอมแปลงแหล่งที่มา	
ของการส่ง”	284

5.7.6 ความสัมพันธ์ของมาตรา 11 วรรคหนึ่ง กับการโจมตีระบบคอมพิวเตอร์ตามมาตรา 10	285
5.8 หลักและองค์ประกอบของฐานความผิดที่ 2 (มาตรา 11 วรรคสอง และวรรคสาม)	287
5.8.1 คำนิยามสำคัญขององค์ประกอบในฐานความผิดที่ 2	287
5.8.2 องค์ประกอบ “อันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูล”	290
5.8.2.1 กรณีที่ไม่ถือว่าก่อให้เกิดความเดือดร้อนรำคาญ : การจำแนกประเภทการส่งข้อมูล 3 กลุ่มที่ไม่ถือว่าเป็น การเดือดร้อนรำคาญตามประกาศกระทรวงฯ	293
5.8.2.2 กรณีที่ก่อให้เกิดความเดือดร้อนรำคาญ	301
5.8.3 องค์ประกอบ “ไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้ง ความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย”	302
บทที่ 6 อธิบายองค์ประกอบความผิดเกี่ยวกับสแปมเชิงเปรียบเทียบ	
กับกฎหมายต่างประเทศ	324
6.1 ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่อยู่ภายใต้กฎหมาย เกี่ยวกับสแปม	324
6.2 วัตถุประสงค์เชิงพาณิชย์ (Commercial purpose)	327
6.2.1 ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ที่มีวัตถุประสงค์ เชิงพาณิชย์	327
6.2.2 เกณฑ์การพิจารณาวัตถุประสงค์เชิงพาณิชย์ : เปรียบเทียบ กับมาตรา 11 วรรคสอง	332
6.2.3 ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ที่มีวัตถุประสงค์อื่น	336
6.2.4 ความผิดเกี่ยวกับสแปมที่มีองค์ประกอบกว้างกว่าการติดต่อ เพื่อการพาณิชย์	336
6.3 ความสัมพันธ์ระหว่างผู้ส่งและผู้รับ (Relationship)	337
6.4 ขอบเขตด้านระยะเวลาของความสัมพันธ์ทางธุรกรรม	344
6.5 องค์ประกอบเชิงปริมาณและความถี่ของข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์	346
6.6 วิธีการส่ง	350

6.7 การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยการใช้สคริปต์ (Script)	351
6.8 “ลักษณะที่ทำให้เข้าใจผิด” ในส่วนประกอบต่างๆ ของข้อมูล คอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์	353
6.8.1 จำแนกลักษณะที่ทำให้เกิดความเข้าใจผิด ตามโครงสร้าง ทางกายวิภาคของสแปม (Anatomy of spam)	354
6.8.2 กลไกทางกฎหมายเกี่ยวกับลักษณะที่ทำให้เข้าใจผิดของสแปม	356
6.8.2.1 กลไกที่หนึ่ง ควบคุมการใช้วิธีการทางเทคนิค ซึ่งทำให้เกิดความเข้าใจผิดในแหล่งที่มาของการส่ง	357
6.8.2.2 กลไกที่สอง ควบคุมการใช้ข้อมูลส่วนหัว ที่ทำให้เข้าใจผิด.....	364
6.8.2.3 กลไกที่สาม กำหนดหน้าที่ให้ผู้ส่งจดหมายหรือข้อความ อิเล็กทรอนิกส์ต้องระบุเนื้อหาหรือรายละเอียดบางประการ เพื่อป้องกันไม่ให้ผู้รับเกิดความเข้าใจผิด.....	373
6.8.2.4 กลไกที่สี่ การควบคุม “เนื้อหา” ข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ที่ก่อให้เกิดเข้าใจผิด เป็นเท็จ หรือหลอกลวง	379
6.8.3 ความสัมพันธ์ระหว่างมาตรา 14 และมาตรา 11 ในกรณีสแปมมีเนื้อหาข้อมูลที่ทำให้เข้าใจผิดหรือเป็นเท็จ	383
6.8.4 การกระทำที่มุ่งต่อความเข้าใจผิดของระบบคอมพิวเตอร์ กับการกระทำที่มุ่งต่อความเข้าใจผิดของ “บุคคล” ผู้รับข้อมูล	384
6.9 หลักความยินยอม และหลัก “Opt-in” - “Opt-out”	386
6.9.1 หลัก “Opt-in” - “Opt-out” ตามกฎหมายสแปม ของต่างประเทศ	388
6.9.2 หลัก “ความยินยอม” และหลัก “Opt-in” - “Opt out” ตาม พ.ร.บ.คอมพิวเตอร์	393
6.9.3 หลัก “Opt-in” ชั้นเดียว และ “Opt-in” สองชั้น	393
6.9.4 หลัก “Opt-out” สองชั้น ตามพ.ร.บ.คอมพิวเตอร์	395
6.9.5 “Opt-in Spam” และการกำหนดกฎหมายแบบผสมทั้งหลัก “Opt-in” และ “Opt-out”	402
6.9.6 หลักการกำหนดให้ข้อมูลเกี่ยวกับผู้ส่ง และข้อมูลและวิธีการ สำหรับบอกเลิก	405

6.9.7	หน้าที่จัดให้ระบบหรือกลไกสำหรับบอกเลิกอยู่ในสภาพใช้ได้ และข้อยกเว้นกรณีปัญหาทางเทคนิค	407
6.9.8	ข้อกำหนดในสัญญาเกี่ยวกับการรับข้อความอิเล็กทรอนิกส์ และหลักความยินยอม	409
6.9.9	ความยินยอมที่เกี่ยวข้องกับความสัมพันธ์ลักษณะต่าง ๆ ระหว่างผู้ส่งและผู้รับ	412
บทที่ 7	ประเด็นทางกฎหมายเกี่ยวกับสแปม	414
7.1	หน้าที่และความรับผิดชอบของผู้ให้บริการเกี่ยวกับสแปม	414
7.1.1	ขอบเขตความหมายของผู้ให้บริการที่เกี่ยวข้องกับสแปม	414
7.1.2	จำแนกความรับผิดชอบของผู้ให้บริการที่เกี่ยวข้องกับการส่งสแปม	416
7.2	การควบคุมสแปมตามพร.บ.คอมพิวเตอร์ คับการควบคุมสแปม โดยสมัครใจของผู้ให้บริการ	423
7.3	สแปมในสภาพแวดล้อมตลาดโปรแกรมประยุกต์ (Application Market หรือ App market)	426
7.3.1	สแปมในบริบทของตลาดโปรแกรมประยุกต์ กับฐานความผิดมาตรา 11	428
7.3.2	แนวทางปรับปรุงใช้มาตรา 11 กับพฤติกรรม “สแปม” ในบริบท ตลาดโปรแกรมประยุกต์	430
7.4	ความรับผิดชอบในกรณีผู้ประกอบธุรกิจบริการส่งข้อมูลโฆษณา หรือประชาสัมพันธ์	432
7.5	การส่งโฆษณาระหว่างผู้บริโภค โดยแรงจูงใจจากผู้ประกอบธุรกิจ	434
7.5.1	เปรียบเทียบกับกฎหมายสหรัฐอเมริกา กรณี “แผนการตลาด ที่ผู้บริโภคส่งต่อจดหมายอิเล็กทรอนิกส์ให้กับเพื่อน”	435
7.6	สแปมกับการส่งจดหมายอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์ ในเชิงพาณิชย์ที่อยู่ภายใต้กฎหมายเฉพาะ	437
7.6.1	สแปมกับการทวงถามหนี้ทางระบบคอมพิวเตอร์	437
7.6.2	สแปมกับการขายตรงและตลาดแบบตรงทางระบบคอมพิวเตอร์	441
7.6.3	สแปมกับการเสนอขายประกันภัยทางอิเล็กทรอนิกส์	445
7.7	สแปมกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562	450

7.8 แนวทางการบัญญัติกฎหมายเพื่อควบคุมสแปม	457
7.9 กฎหมายควบคุมสแปม ในกรอบเสรีภาพการแสดงความคิดเห็น	459
ภาค 3 ความผิดอื่นที่ส่งผลกระทบหลายมิติ	465
บทที่ 8 การก่อการร้ายไซเบอร์ (Cyber terrorism)	467
8.1 ความหมายทั่วไปของการก่อการร้ายไซเบอร์	468
8.2 การก่อการร้ายไซเบอร์กับอาชญากรรมคอมพิวเตอร์ (Cyberterrorism and Cybercrime)	469
8.3 การก่อการร้ายไซเบอร์กับสงครามไซเบอร์ (Cyber terrorism and Cyber warfare)	471
8.4 กฎหมายที่เกี่ยวข้องกับการก่อการร้ายไซเบอร์	471
8.4.1 ความผิดตามประมวลกฎหมายอาญา	471
8.4.2 ความผิดตามพ.ร.บ.คอมพิวเตอร์	473
8.4.3 กฎหมายเกี่ยวกับการป้องกันและปราบปรามการฉ้อโกง ทางการเงินแก่การก่อการร้าย	474
8.5 การจำแนกประเภทการก่อการร้ายตามความสัมพันธ์กับทรัพยากร คอมพิวเตอร์ และการปรับใช้กฎหมาย	476
8.5.1 การก่อการร้ายที่ไม่ได้กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ และไม่ส่งผลกระทบต่อคุณลักษณะด้านความปลอดภัยของระบบ หรือข้อมูลคอมพิวเตอร์	476
8.5.2 การก่อการร้ายที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์	477
8.5.3 การวางแผนและการเตรียมการก่อการร้าย	479
8.5.4 การขู่เข็ญจะก่อการร้าย (Terroristic threat)	482
8.5.4.1 การกำหนดความผิดฐานขู่เข็ญว่าจะก่อการร้าย กับการคุ้มครองเสรีภาพในการแสดงความคิดเห็น	484
8.5.5 การโฆษณาชวนเชื่อ การกระตุนยั่วยุหรือยุยงเกี่ยวกับ การก่อการร้ายและการรับสมัครสมาชิก	486
8.5.5.1 ความผิดตามกฎหมายอาญามาตรา 135/2 และ มาตรา 116 ที่กระทำทางระบบคอมพิวเตอร์	488
8.5.6 ครอบครองข้อมูลสำหรับใช้เพื่อการวางแผน เตรียม หรือกระทำการก่อการร้าย	489

8.5.7 การใช้ทรัพยากรคอมพิวเตอร์เพื่อสนับสนุนด้านการเงิน ฝึกอบรมและการอื่น	491
8.6 การก่อการร้ายไซเบอร์กับการเรียกร้องหรือรณรงค์โดยอาศัยทรัพยากร คอมพิวเตอร์ หรือ “Hacktivist”	496
8.7 การมีปฏิสัมพันธ์ในสื่อสังคมออนไลน์กับบุคคลหรือเนื้อหาเกี่ยวกับการ ก่อการร้าย	497
8.8 อธิบายการปรับใช้มาตรา 14 (2) และ มาตรา 14 (3) กับการสื่อสารข้อมูลเกี่ยวกับการก่อการร้าย	499
8.9 แนวทางการกำหนดความผิดสำหรับการก่อการร้ายไซเบอร์	502
บทที่ 9 การกรรโชกทรัพย์ไซเบอร์ (Cyber extortion)	507
9.1 องค์ประกอบ ลักษณะ และความหมายของการกรรโชกทรัพย์ไซเบอร์	507
9.2 ความผิดฐานกรรโชกทรัพย์ไซเบอร์ของต่างประเทศ	510
9.3 การจำแนกประเภทการกรรโชกทรัพย์ไซเบอร์และการปรับใช้กฎหมาย	511
9.3.1 การกรรโชกทรัพย์ไซเบอร์ที่เกี่ยวกับภัยคุกคาม ต่อความมั่นคงปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์	513
9.3.2 การกรรโชกทรัพย์ไซเบอร์ที่ไม่เกี่ยวกับภัยคุกคามต่อความมั่นคง ปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์	519
9.3.3 การกรรโชกทรัพย์ไซเบอร์ ที่มีลักษณะผสมของภัยคุกคาม ต่อระบบหรือข้อมูลคอมพิวเตอร์และภัยคุกคามในมิติอื่น	521
9.3.4 การกรรโชกทรัพย์ไซเบอร์โดยขู่ว่าจะสร้างเงื่อนไข อันอาจให้ผู้ถูกขู่ต้องมีความรับผิดชอบตามกฎหมาย	526
9.3.4.1 การกรรโชกทรัพย์ไซเบอร์โดยขู่จะสร้างเงื่อนไขอันอาจ ให้ผู้ถูกขู่ต้องมีความรับผิดชอบตามกฎหมายคุ้มครอง ข้อมูลส่วนบุคคล (Cyber Breach Extortion)	526
9.3.5 การกรรโชกทรัพย์ไซเบอร์โดยขู่ว่าจะกระทำความผิด ในนามของเหยื่อ	530
9.4 การกรรโชกทรัพย์ไซเบอร์กับฐานความผิดตามประมวลกฎหมายอาญา	533
9.4.1 การกรรโชกทรัพย์ไซเบอร์กับความผิดฐานกรรโชกทรัพย์	534
9.4.2 การกรรโชกทรัพย์ไซเบอร์กับความผิดฐานริดเอาทรัพย์สิน	535

9.4.2.1 การกรรโชกทรัพย์ไซเบอร์กับความผิดฐานรีดเอาทรัพย์ :	
กรณีจะเปิดเผยข้อมูลลับที่ไม่ชอบด้วยศีลธรรมอันดี	
ของประชาชน	537
9.4.2.2 การกรรโชกทรัพย์ไซเบอร์กับความผิดฐานรีดเอาทรัพย์ :	
กรณีที่เกี่ยวข้องกับข้อมูลส่วนบุคคลรั่วไหล	538
9.4.2.3 การกรรโชกทรัพย์ไซเบอร์กับความผิดฐานรีดเอาทรัพย์ :	
กรณีจะเปิดเผยข้อมูลที่กฎหมายกำหนดหน้าที่ให้เปิดเผย	539
9.4.3 การกรรโชกทรัพย์ไซเบอร์กับความผิดฐานเรียกค่าไถ่	540
9.5 ความสัมพันธ์ระหว่างการกรรโชกทรัพย์ไซเบอร์กับการกระทำความผิดอื่น	
ที่กระทบต่อความปลอดภัยของระบบหรือข้อมูล	541
9.6 การกรรโชกทรัพย์ไซเบอร์กับความผิดเกี่ยวกับเนื้อหา	
ตามพ.ร.บ.คอมพิวเตอร์	542
9.7 ตารางเปรียบเทียบการปรับใช้พ.ร.บ.คอมพิวเตอร์ และกฎหมายอาญา	
กับการกรรโชกทรัพย์ไซเบอร์	544
คำส่งท้าย	546
บรรณานุกรม	549

□ □ □

¹ Convention on Cybercrime, Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems