

สารบัญ

ภาค 1 : ความทั่วไปว่าด้วยคอมพิวเตอร์ อินเทอร์เน็ต ความผิด และสิทธิเสรีภาพ

บทที่ 1 ความเข้าใจพื้นฐานเกี่ยวกับเทคโนโลยีสารสนเทศ คอมพิวเตอร์ และ เครือข่ายคอมพิวเตอร์

1. คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ และยุคแห่งพัฒนาการทางเทคโนโลยีสารสนเทศ	1
1.1 คอมพิวเตอร์ และอินเทอร์เน็ต	1
1.2 วิวัฒนาการจาก PC Age ถึง Internet of Things	5
2. รูปแบบของบริการในเครือข่ายคอมพิวเตอร์ กับความผิดที่เกี่ยวข้อง	10
2.1 บริการจดหมายหรือไปรษณีย์อิเล็กทรอนิกส์ (E-Mail)	10
2.2 บริการเว็บไซต์ และการเชื่อมโยงเว็บไซต์เป็นเครือข่าย (Website and World Wide Web)	11
2.3 บริการเครื่องมือสืบค้นข้อมูล (Search Engine)	14
2.4 บริการโอนย้ายไฟล์ข้อมูล (File Transfer Protocol or FTP)	16
2.5 บริการแลกเปลี่ยนไฟล์ระหว่างเครื่องผู้ใช้งานโดยตรง (P2P File Sharing)	17
2.6 บริการแลกเปลี่ยนข้อมูลข่าวสาร กระดานข่าว หรือกระดานสนทนา (UseNet, Newsgroups, Chatrooms)	18
2.7 บริการส่งข้อความ หรือสนทนาโต้ตอบแบบทันทีทันใดหรือแบบ Real Time (Instant Messaging or IM)	20
2.8 บริการเก็บรักษาและบริหารจัดการข้อมูล (Cloud Service)	21
2.9 บริการพื้นที่ และเครื่องมือในการสร้างเนื้อหา และแบ่งปันข้อมูลด้วยตนเอง	23

บทที่ 2 การป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์และไซเบอร์:

ปัญหา อุปสรรค และการสร้างสมดุลกับสิทธิและเสรีภาพของประชาชน 27

1. หลักประกันสิทธิเสรีภาพของประชาชนในระบอบการปกครองแบบประชาธิปไตย 27
2. ปัญหา อุปสรรค และความท้าทายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ 36
 - 2.1 ขาดแคลนกฎหมายสารบัญญัติที่จะนำมาบังคับใช้กับอาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ 36
 - 2.2 ขาดเครื่องมือในทางวิธีบัญญัติ มีบุคลากรผู้เชี่ยวชาญไม่เพียงพอ มาตรการที่ใช้มีลักษณะละเมิดสิทธิและเสรีภาพประชาชนเกินไป 38
 - 2.3 ความอ่อนไหวและถูกปั่นป่วนได้ง่ายของพยานหลักฐานอิเล็กทรอนิกส์ กระบวนการรวบรวม และเก็บรักษาที่ไม่ได้มาตรฐาน 41
 - 2.4 ความเป็นนิรนาม และความไร้พรมแดน 42
 - 2.5 เหลือไม่แข็งแกร่ง หรือรายงานการกระทำผิดแก่เจ้าหน้าที่รัฐ 46
3. กฎหมาย และความร่วมมือระหว่างประเทศเพื่อการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ 49
 - 3.1 องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) 50
 - 3.2 กลุ่มประเทศอุตสาหกรรมชั้นนำของโลก (G8) 51
 - 3.3 สภายุโรป (The Council of Europe) 52
 - 3.4 สหภาพโทรคมนาคมระหว่างประเทศ (ITU) 53
 - 3.5 สหภาพยุโรป (European Union - EU) 54
 - 3.6 กลุ่มสันนิบาตแห่งรัฐอาหรับ (League of Arab States – LAS) 55
 - 3.7 กลุ่มเศรษฐกิจของรัฐแอฟริกาตะวันตก (ECOWAS) 56
 - 3.8 สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (ASEAN) 58

ภาค 2: อาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์

บทที่ 3 ความทั่วไปว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ 61

1. วิวัฒนาการของการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ 61
 - 1.1 การกระทำความผิดต่อสิทธิความเป็นส่วนตัว และข้อมูลส่วนบุคคล 61
 - 1.2 ความผิดเกี่ยวกับคอมพิวเตอร์ในฐานะอาชญากรรมเศรษฐกิจ 63
 - 1.3 การกระทำความผิดที่อาศัยความสามารถ และศักยภาพของเครือข่ายคอมพิวเตอร์ 65
2. ความหมาย และลักษณะทั่วไปของอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ 69
3. ประเภทของอาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ 73
 - 3.1 การจำแนกโดยอาศัย “บทบาท” ของคอมพิวเตอร์ 73
 - 3.2 การจำแนกตามอนุสัญญาอาชญากรรมไซเบอร์ (Convention on Cybercrime) 75
 - 3.3 การจำแนกโดยพิจารณาจากเป้าหมาย หรือวัตถุประสงค์แห่งการกระทำ 77
 - 3.4 การจำแนกประเภท แบบอื่น ๆ 78
4. อาชญาวិทยา กับอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ 79
 - 4.1 ทฤษฎีทางสังคมวิทยา (Sociological Theories) 82
 - 4.2 ทฤษฎีทางอาชญาวิทยา (Criminological Theories) 86
 - 4.3 เหยื่อวิทยา (Victimology) 90
 - 4.4 อาชญาวิทยาไซเบอร์ (Cyber Criminology) 93

บทที่ 4 รูปแบบอาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ กรณีศึกษาที่น่าสนใจ และกฎหมายที่เกี่ยวข้อง 99

1. การกระทำความผิดต่อระบบ และ/หรือข้อมูลคอมพิวเตอร์ 100
 - 1.1 การละเมิดความลับของระบบ และ/หรือข้อมูลคอมพิวเตอร์ 100
 - 1.1.1 การเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized Computer Access) 100
 - 1.1.1.1 กฎหมาย และมาตรการในต่างประเทศ 108

1.1.1.2	การเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจตาม กฎหมายไทย	112
1.1.2	การเข้าถึง สอดส่อง และโจรกรรมข้อมูลคอมพิวเตอร์	115
1.1.2.1	การโจรกรรมข้อมูลที่บ้านที่กอยู่ในระบบคอมพิวเตอร์ หรือ ระบบสารสนเทศ	116
1.1.2.2	การดักจับข้อมูลคอมพิวเตอร์ในระหว่างการรับส่ง (Data Intercepted)	123
1.1.2.3	การสอดแนมข้อมูลคอมพิวเตอร์ผ่านโปรแกรมสอดแนม	131
1.2	การทำลายความครบถ้วนสมบูรณ์ และความพร้อมในการใช้งานระบบ และ/หรือข้อมูลคอมพิวเตอร์	134
1.2.1	การก่อวินาศกรรมคอมพิวเตอร์ (Computer Sabotage) หรือการ รบกวนการทำงานของระบบคอมพิวเตอร์ (System Interference)	134
1.2.1.1	การก่อวินาศกรรมคอมพิวเตอร์ หรือรบกวนระบบโดยใช้ โปรแกรมอันตราย	135
1.2.1.2	การโจมตีระบบคอมพิวเตอร์ หรือระบบสารสนเทศเพื่อให้ ปฏิเสธการทำงาน (Denial of Service and Distributed Denial of Service Attack)	138
1.2.1.3	กฎหมาย และมาตรการในต่างประเทศ	141
1.2.1.4	การก่อวินาศกรรม หรือรบกวนระบบคอมพิวเตอร์ตาม กฎหมายไทย	144
1.2.2	การรบกวน หรือทำลายข้อมูลคอมพิวเตอร์ (Data Interference and Destruction)	145
1.2.2.1	กฎหมาย และมาตรการในต่างประเทศ	146
1.2.2.2	การรบกวน หรือทำลายข้อมูลคอมพิวเตอร์ตาม กฎหมายไทย	150
1.3	การกระทำความผิดต่อระบบ หรือข้อมูลคอมพิวเตอร์โดยมี วัตถุประสงค์อื่น	151
1.3.1	การฉ้อโกงคอมพิวเตอร์ (Computer Fraud)	151

1.3.2	การกรรโชกทางคอมพิวเตอร์และไซเบอร์ (Computer- or Cyber Extortion)	158
2.	การกระทำความผิดบนอินเทอร์เน็ต	163
2.1	การเผยแพร่ข้อมูลที่มีเนื้อหาผิดกฎหมายบนอินเทอร์เน็ต	164
2.1.1	เนื้อหาอันมีลักษณะลามกอนาจาร	164
2.1.1.1	กฎหมาย และมาตรการในต่างประเทศ	167
2.1.1.2	การเผยแพร่ภาพลามกอนาจารตามกฎหมายไทย	182
2.1.2	เนื้อหาสร้างความเกลียดชัง (Hate Speech)	185
2.1.2.1	กฎหมาย และมาตรการในต่างประเทศ	190
2.1.2.2	Hate Speech กับกฎหมายไทย	200
2.1.3	เนื้อหาที่ขัดต่อความมั่นคงแห่งรัฐ หรือความสงบเรียบร้อยของประชาชน	203
2.1.3.1	กฎหมาย และมาตรการในต่างประเทศ	205
2.1.3.2	ความมั่นคงแห่งรัฐ และความสงบเรียบร้อยของประชาชนตามกฎหมายไทย	213
2.1.4	เนื้อหาหมิ่นประมาท หรือดูหมิ่นบุคคลอื่น	217
2.1.4.1	กฎหมาย และมาตรการในต่างประเทศ	218
2.1.4.2	ความผิดต่อเกียรติยศชื่อเสียงตามกฎหมายไทย	224
2.2	อาชญากรรมความรุนแรงบนอินเทอร์เน็ต (Violent Crime on the Internet)	228
2.2.1	พฤติกรรมก่อความรุนแรงบนอินเทอร์เน็ต	229
2.2.1.1	Cyberbullying	229
2.2.1.2	Cyberstalking	232
2.2.1.3	Cyber Harassment	234
2.2.1.4	Sextortion	235
2.2.1.5	Revenge Porn/ Nonconsensual Pornography	236
2.2.2	ความแตกต่างระหว่างการกระทำในโลกออนไลน์กับโลกทางกายภาพ	236
2.2.3	กฎหมาย และมาตรการในต่างประเทศ	240

2.2.4	การกลั่นแกล้งและการตามรังควานไซเบอร์ กับกฎหมายไทย	253
2.2.4.1	การเผยแพร่ หรือส่งต่อข้อความหรือข้อมูลที่ทำให้เหยื่อ ถูกดูหมิ่น เกลียดชัง เสียชื่อเสียง	257
2.2.4.2	การส่งข้อความดูถูกเหยียดหยามเหยื่อเป็นการ เฉพาะตัว	259
2.2.4.3	การส่งข้อความคุกคามหรือข่มขู่ให้เกิดความหวาดกลัว	261
2.2.4.4	การล่วงละเมิดพื้นที่ หรือข้อมูลส่วนบุคคล	263
2.2.4.5	ประกาศ โฆษณา หรือเชิญชวนให้บุคคลอื่นช่วยส่งต่อข้อมูลที่ ทำให้เหยื่อเสียหาย หรือให้ติดตามคุกคามเหยื่อต่อไป	263
2.3	การส่งข้อความรบกวน หรือจดหมายอิเล็กทรอนิกส์ไม่พึงประสงค์ (Spamming)	264
2.3.1	กฎหมาย และมาตรการในต่างประเทศ	267
2.3.2	Spamming กับกฎหมายไทย	274
2.4	การหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลด้านการเงิน และนำไปใช้โดยมิชอบ (Phishing/ Pharming)	281
2.4.1	กฎหมาย และมาตรการในต่างประเทศ	284
2.4.2	Phishing กับกฎหมายไทย	291
2.5	การสวมรอย หรือแอบอ้างเป็นบุคคลอื่นออนไลน์ (Online Impersonation)	295
2.5.1	กฎหมาย และมาตรการในต่างประเทศ	299
2.5.2	Online Impersonation กับกฎหมายไทย	303
2.6	การพนันออนไลน์ (Online or Internet Gambling)	307
2.6.1	กฎหมาย และมาตรการในต่างประเทศ	311
2.6.2	Online Gambling กับกฎหมายไทย	316
3.	การละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์ และผลงานสร้างสรรค์ บนอินเทอร์เน็ต	321
3.1	การละเมิดลิขสิทธิ์ผลงานสร้างสรรค์ที่เผยแพร่บนอินเทอร์เน็ต	323
3.1.1	ลักษณะการเผยแพร่ผลงานสร้างสรรค์ กับความคุ้มครอง ตามกฎหมาย	324

3.1.2 ปัญหาทางกฎหมายกับการละเมิดผลงานสร้างสรรค์ที่เผยแพร่บนอินเทอร์เน็ต	325
3.1.2.1 การดาวน์โหลดหรืออัปโหลดข้อมูลที่เป็นผลงานอันมีลิขสิทธิ์บนอินเทอร์เน็ต (Downloading or Uploading)	327
3.1.2.2 การแสดงผล และการบันทึกข้อมูลชั่วคราวในระบบคอมพิวเตอร์	328
3.1.2.2.1 Browsing	328
3.1.2.2.2 Local Caching และ Proxy Caching	328
3.1.2.2.3 Mirroring	329
3.1.2.2.4 มาตรการ และกรณีศึกษาที่น่าสนใจในไทยและต่างประเทศ	329
3.1.2.3 การเชื่อมโยง (Link) ผลงานลิขสิทธิ์บนอินเทอร์เน็ต	334
3.1.2.3.1 Hyperlink	334
3.1.2.3.2 Deep Link	334
3.1.2.3.3 Inline Link หรือ Hot Link	335
3.1.2.3.4 Framing	335
3.1.2.3.5 Search Engine	336
3.1.2.3.6 การฝังโค้ด หรือ Embed ไฟล์ข้อมูล	337
3.1.2.3.7 กฎหมาย และกรณีศึกษาที่น่าสนใจในต่างประเทศ	337
3.1.2.3.8 กฎหมาย และมาตรการในประเทศไทย	344
3.1.2.4 การแบ่งปันผลงานลิขสิทธิ์ผ่านโปรแกรมแบ่งปันไฟล์แบบ Peer to Peer (P2P File Sharing)	347
3.1.2.4.1 กฎหมาย และกรณีศึกษาที่น่าสนใจในต่างประเทศ	350
3.1.2.4.2 กฎหมาย และมาตรการในประเทศไทย	356
3.1.3 สัญญาอนุญาตให้ใช้ผลงานล่วงหน้า Creative Commons	358
3.2 การละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์	361
3.2.1 ลักษณะการคุ้มครองโปรแกรมคอมพิวเตอร์	362

3.2.1.1	การคุ้มครองโปรแกรมคอมพิวเตอร์ตามกฎหมาย	253
	ต่างประเทศ	363
3.2.1.2	การคุ้มครองโปรแกรมคอมพิวเตอร์ตามกฎหมายไทย	368
3.2.2	สัญญาอนุญาต กับปัญหาการคุ้มครองโปรแกรมคอมพิวเตอร์แบบ ปิดรหัสโปรแกรมต้นฉบับ (Close Source Software)	370
3.2.3	สัญญาอนุญาต กับโปรแกรมคอมพิวเตอร์แบบเปิดรหัสโปรแกรม ต้นฉบับ (Open Source Software)	373
4.	สงครามไซเบอร์/ อาชญากรรมไซเบอร์โดยรัฐ (Cyberwarfare/ State and State sponsored Cybercrime)	377
4.1	ปรากฏการณ์การโจมตีทางไซเบอร์ที่รัฐเป็นผู้กระทำหรือ สนับสนุน	381
4.1.1	ความขัดแย้งทางการเมือง: แทรกแซงการเมือง โจมตีโครงสร้าง พื้นฐาน รวบรวมข้อมูลอ่อนไหว	383
4.1.1.1	นักบไซเบอร์จีนผู้เริ่มต้น ขยับ และปฏิบัติการโจมตี	383
4.1.1.2	เกาหลีเหนือ - เกาหลีใต้คู่ขัดแย้งสองโลก	385
4.1.1.3	อินเดีย - ปากีสถาน คู่กัดที่พลัดกันรุกพลัดกันรับ	386
4.1.1.4	แอกเกอร์รัสเซียกับเทคนิคโจมตีขั้นสูง ชุ่มเยิบ ตรวจจับยาก	387
4.1.1.5	นักโจมตีไซเบอร์ตะวันออกกลางที่สร้างสรรค์ และหลอกลวง	390
4.1.1.6	สหรัฐอเมริกา ระหว่างตำรวจไซเบอร์โลกกับ อันทาลอนไลน์	392
4.1.1.7	สหภาพยุโรปกลุ่มประเทศผู้ตีที่มักตกเป็นเป้าโจมตี	393
4.1.2	คู่แข่งทางเศรษฐกิจ: สถาบันการเงิน ความลับทางการค้า ทรัพย์สินทางปัญญา และอุตสาหกรรมที่สำคัญ	394
4.1.3	การเมืองภายใน: สอดแนมข้อมูลส่วนบุคคล ความคิดและ พฤติกรรมของประชาชน ขัดขวาง ทำลายผู้เห็นต่าง	396
4.2	การโจมตีไซเบอร์โดยรัฐหรือที่รัฐสนับสนุน กับกฎหมายว่าด้วย อาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์	401

5. การก่อการร้ายไซเบอร์ (Cyberterrorism)	404
5.1 กฎหมาย และมาตรการในต่างประเทศ	414
5.2 การก่อการร้ายไซเบอร์ กับกฎหมายไทย	419
6. องค์กรอาชญากรรมไซเบอร์ (Cyber Organized Crime)	427

ภาค 3 : มาตรการอื่นเพื่อป้องกันและปราบปรามอาชญากรรม

คอมพิวเตอร์และอาชญากรรมไซเบอร์

นอกเหนือจากกฎหมายที่กำหนดความผิด

บทที่ 5 การกำหนดหน้าที่ และความรับผิดชอบแก่ผู้ให้บริการอินเทอร์เน็ต 439

1. แนวคิดและกฎหมายว่าด้วยการกำหนดหน้าที่ และความรับผิดชอบแก่ผู้ให้บริการอินเทอร์เน็ต	439
2. หน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลผู้ให้บริการ (Data Retention)	440
2.1 กฎหมาย และมาตรการในต่างประเทศ	441
2.2 หน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยผู้ให้บริการตามกฎหมายไทย	445
3. หน้าที่กำกับดูแล ปิดกั้นช่องทางการเข้าถึงเนื้อหาที่ผิดกฎหมาย	449
3.1 หน้าที่กำกับดูแลเนื้อหาผิดกฎหมาย และความรับผิดชอบของผู้ให้บริการในต่างประเทศ	449
3.2 หน้าที่จัดการเนื้อหาผิดกฎหมาย และความรับผิดชอบของผู้ให้บริการตามกฎหมายไทย	469
4. หน้าที่ลบข้อมูลส่วนบุคคลตามคำร้องขอของเจ้าของข้อมูลภายใต้แนวคิด “สิทธิที่จะถูกลืม” (Right to be Forgotten)	477
4.1 สิทธิที่จะถูกลืมในกฎหมายต่างประเทศ	485
4.2 สิทธิที่จะถูกลืมในกฎหมายไทย	488

บทที่ 6 การควบคุม สอดส่อง ปิดกั้นเนื้อหาบนอินเทอร์เน็ตโดยรัฐ 495

1. ข้อความคิด และรูปแบบในการควบคุม ปิดกั้นเนื้อหาบนอินเทอร์เน็ต	495
2. การควบคุม สอดส่อง ปิดกั้นเนื้อหาบนอินเทอร์เน็ตในต่างประเทศ	498

2.1	กฎหมาย มาตรการ และเทคนิควิธีการต่าง ๆ ในประเทศจีน	498
2.1.1	การควบคุมช่องทางการเข้าถึงอินเทอร์เน็ตของพลเมือง	500
2.1.2	การตรวจสอบ หรือจับตาดำเนินการบนอินเทอร์เน็ต ของพลเมือง	504
2.1.3	การควบคุมการเข้าถึงข้อมูลผ่านเครื่องมือสืบค้น (Search Engine)	506
2.1.4	การปิดเว็บไซต์ภายในประเทศที่มีเนื้อหาวิพากษ์ วิจารณ์รัฐบาล	508
2.1.5	การควบคุม Web 2.0 และเครือข่ายสังคมออนไลน์	509
2.2	มาตรการควบคุมเนื้อหา และปิดกั้นเว็บไซต์ในประเทศเยอรมนี	514
2.2.1	กฎหมายที่ให้อำนาจรัฐใช้มาตรการปิดกั้นเนื้อหา บนอินเทอร์เน็ต	516
2.2.2	ปรากฏการณ์ปิดกั้นการเข้าถึงเนื้อหาบนอินเทอร์เน็ต ในเยอรมนี	517
2.3	มาตรการควบคุมเนื้อหา และการปิดกั้นสื่อออนไลน์ ในประเทศอินเดีย	520
2.3.1	กฎหมายให้อำนาจรัฐใช้มาตรการปิดกั้นเนื้อหา บนอินเทอร์เน็ต	521
2.3.2	ปรากฏการณ์ปิดกั้นการเข้าถึงเนื้อหาบนอินเทอร์เน็ต ในประเทศอินเดีย	527
3	กฎหมาย และมาตรการควบคุม ลบเนื้อหา หรือปิดกั้นอินเทอร์เน็ต ในประเทศไทย	532
3.1	กฎหมายปิดกั้นเนื้อหาบนอินเทอร์เน็ตในสภาวะการณ์ปกติ	534
3.2	กฎหมายปิดกั้นเนื้อหาบนอินเทอร์เน็ตในสภาวะการณ์ไม่ปกติ	542
3.3	ปรากฏการณ์ และสถิติการปิดกั้นเว็บไซต์ในประเทศไทย	544

บรรณานุกรม

ดรชนี

ภาคผนวกดิจิทัล