

Cyberprzestępstwa przeciwko danym komputerowym i systemom informatycznym w kodeksie karnym - propozycje zmian

Przejdź do produktu na ksiegarnia.beck.pl

Spis treści

Wstęp	XI
Bibliografia	XVII
Wykaz skrótów	XXXV
Rozdział I. Konwencja RE o cyberprzestępczości otwarta do podpisu w Budapeszcie dnia 23.11.2001 r.	1
Rozdział II. Dyrektywa Parlamentu Europejskiego i Rady Nr 2013/40/UE z 12.8.2013 r. dotycząca ataków na systemy informatyczne	9
Rozdział III. Terminologia	15
§ 1. Dane komputerowe/informatyczne	15
§ 2. Dane dotyczące ruchu	16
§ 3. Dane telekomunikacyjne	22
§ 4. Dane osobowe	23
§ 5. Przetwarzanie danych	24
§ 6. Sieć telekomunikacyjna	25
§ 7. System komputerowy	30
§ 8. System informatyczny	31
§ 9. System teleinformatyczny	35
§ 10. Sieć teleinformatyczna	36
§ 11. System informacyjny	37
§ 12. Infrastruktura telekomunikacyjna	39
§ 13. System komputerowy, system informatyczny, system teleinformatyczny, sieć telekomunikacyjna, system informacyjny, sieć teleinformatyczna, infrastruktura telekomunikacyjna – próba podsumowania	40
§ 14. Nieuprawniony dostęp do całości lub części systemu informatycznego	42
§ 15. Cyberprzestrzeń	44
§ 16. Propozycje definicji	46
Rozdział IV. Rozdział XXXIII Kodeksu karnego – Przepisy przeciwko ochronie informacji	49
§ 1. Nieuprawniony dostęp do informacji i nieuprawniony dostęp do systemu informatycznego (hacking) – art. 267 § 1 i § 2 KK	49

§ 2. Nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych i programów komputerowych – art. 267 § 3 KK	62
§ 3. Odpowiedzialność karna za ujawnienie informacji uzyskanej w wyniku popełnienia przestępstwa z art. 267 § 1, § 2 lub § 3 KK – art. 267 § 4 KK	68
§ 4. Naruszenie integralności zapisu informacji na informatycznym nośniku danych – art. 268 KK	71
§ 5. Naruszenie integralności danych, utrudnianie dostępu do danych oraz zakłócanie ich przetwarzania – art. 268a i art. 269a KK	73
§ 6. Tzw. sabotaż informatyczny – art. 269 KK	81
§ 7. Stosunek art. 268a, art. 269 i art. 269a KK do art. 254a KK	84
§ 8. Tzw. bezprawne wykorzystanie urządzeń, programów i danych – art. 269b KK	85
§ 9. Kwestia zgodności polskiej regulacji z Konwencją o cyberprzestępczości oraz dyrektywą Nr 2013/40	100
Rozdział V. Problematyka typów kwalifikowanych (uwzględnienie okoliczności obciążających przewidzianych w dyrektywie Nr 2013/40)	
§ 1. Artykuł 9 ust. 3 dyrektywy Nr 2013/40	101
§ 2. Artykuł 9 ust. 4 dyrektywy Nr 2013/40	102
I. Spowodowanie znacznej szkody (art. 9 ust. 4 lit. a dyrektywy Nr 2013/40)	102
II. Popełnienie czynu w ramach organizacji przestępczej (art. 9 ust. 4 lit. b dyrektywy Nr 2013/40)	103
III. Popełnienie czynu przeciwko systemowi informatycznemu o charakterze infrastruktury krytycznej (art. 9 ust. 4 lit. c dyrektywy Nr 2013/40)	104
§ 3. Popełnienie czynu zabronionego określonego w art. 4 lub art. 5 dyrektywy Nr 2013/40 przy użyciu danych osobowych innej osoby w celu uzyskania zaufania osoby trzeciej	110
Rozdział VI. Tzw. przestępstwo kradzieży tożsamości (art. 190a § 2 KK) – propozycje zmian	
Rozdział VII. Nieumyślne przestępstwa przeciwko danym komputerowym i systemom informatycznym w ustawodawstwach innych państw	
§ 1. Uwagi wstępne	125
§ 2. Islandia	126
§ 3. Armenia	126
§ 4. Bułgaria	127
§ 5. Czechy	128
§ 6. Proponowane przepisy	128

Rozdział VIII. Cyberterroryzm	131
Rozdział IX. Niechciana poczta (spam)	139
Rozdział X. Naruszenia „ściśle osobistej” sfery życia prywatnego	145
§ 1. Stan obecny	145
§ 2. Niemcy	146
§ 3. Francja	148
§ 4. Finlandia	149
§ 5. Propozycja nowelizacji	149
Zakończenie	153
Załącznik	157
Indeks rzeczowy	199

[Przejdź do księgarni →](#)



ksiegarnia.beck.pl