

Dr hab. Andrzej Adamski, prof. UMK  
Katedra Prawa Karnego i Polityki Kryminalnej  
Wydział Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu,  
Kierownik Podyplomowych Studiów Problemów Przestępczości Komputerowej na Wydziale  
Prawa i Administracji UMK w Toruniu

**SZKOLENIE DLA SĘDZIÓW ORZEKAJĄCYCH W SPRAWACH KARNYCH**  
Będlewo k/ Poznania (7-8 stycznia 2008 r.)

**Wybrane zagadnienia z zakresu przestępstw przeciwko ochronie  
informacji oraz przestępstw popełnianych w cyberprzestrzeni**

**I. Przedmiot i cel szkolenia:**

1. Przestępstwa związane z wykorzystaniem technologii informacyjnych (komputery, telefony komórkowe, Internet, telewizja kablowa i satelitarna, karty płatnicze i bankomaty) stanowią jedną z najszybciej rozwijających się form przestępczości, która ze względu na swój „techniczny” charakter i szybkość z jaką ewoluuje, stwarza wiele problemów zarówno ustawodawcom (sfera kryminalizacji), jak i organom powołanym do ścigania przestępstw (stosowanie przepisów prawa, gromadzenie dowodów winy sprawców, współpraca międzynarodowa).
2. Członkostwo Polski w Unii Europejskiej wymaga nie tylko dostosowania polskiego ustawodawstwa karnego do europejskich standardów normatywnych w dziedzinie zwalczania cyberprzestępczości, lecz także przygotowania polskich prokuratorów i sędziów do prowadzenia postępowań karnych i świadczenia pomocy prawnej w sprawach o cyberprzestępstwa.<sup>1</sup>

---

<sup>1</sup> Czyny w zakresie cyberprzestępczości – oznaczają czyny przeciwko ochronie danych gromadzonych, przechowywanych, przetwarzanych lub przekazywanych w systemie informatycznym - wg definicji zawartej w rozporządzeniu Ministra Sprawiedliwości z 20 kwietnia 2004 r. w sprawie europejskiego nakazu aresztowania (Dz.U. Nr 73, poz .664; sprost. Nr 99, poz.1004)

3. W latach 2001-2004 do polskiego ustawodawstwa karnego (kodeksowego i pozakodeksowego) wprowadzono nowe typy cyberprzestępstw. W tym samym czasie rozpowszechniły się nowe techniki naruszania dóbr prawnych przy pomocy technologii informacyjnych (*dialery, p2p, skimming, spamming, phishing, spyware*). W konsekwencji - organy ścigania i wymiaru sprawiedliwości stanęły w obliczu nowych zadań i problemów związanych z koniecznością reagowania na nieznane wcześniej formy wiktyimizacji użytkowników Internetu i innych technologii informacyjnych. Wątpliwości dotyczące oceny prawnej incydentów, o których zawiadamiają osoby pokrzywdzone różnymi formami nadużyć internetowych i niewielka skuteczność prowadzonych w tych sprawach postępowań karnych mają na ogół wspólną przyczynę. Jest nią niedostateczny poziom wiedzy niezbędnej do podejmowania właściwych decyzji procesowych w sprawach z „elementem internetowym”.
4. Głównym celem planowanego szkolenia jest przedstawienie aktualnego zakresu kryminalizacji najbardziej typowych nadużyć związanych z technologią informacyjną i pomoc w rozpoznawaniu ich znamion ustawowych na tle uregulowań prawnych zawartych w kodeksie karnym i innych ustawach (prawo autorskie, ustawa o świadczeniu usług drogą elektroniczną, ustawa o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym). Scharakteryzowane zostaną również instrumenty prawa międzynarodowego i europejskiego w dziedzinie przeciwdziałania cyberprzestępczości.

## **II. Szczegółowy program szkolenia z zakresu cyberkryminologii i prawa karnego materialnego**

1. Cyberprzestępczość – charakterystyka zjawiska, skala i tendencje.
2. Międzynarodowe i europejskie standardy normatywne w dziedzinie przestępstw związanych z technologią informacyjną:
  - a. Konwencja Rady Europy o cyberprzestępczości z 2001 r.,

b. Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne [Dz.U.UE L 69/67].

3. Zagadnienie locus delicti i zakresu jurysdykcji.

4. Analiza polskiego ustawodawstwa karnego:

3.1. Przesłępstwa przeciwko ochronie informacji : art. 267 – art. 269b kk.

3.1.1. haking (art. 267 § 1 kk)

3.1.2. nielegalne przechwytywanie informacji (art. 267§ 2 kk)

3.1.3. ingerencja w dane (art. 268 § 2, 268a, kk)

3.1.4. ingerencja w system (art. 268a i 269 kk)

3.1.5. narzędzia hakerskie (art. 269b kk)

3.2. Spamming (art. 24 ustawy o świadczeniu usług drogą elektroniczną).

3.3. Oszustwo komputerowe (art. 287 kk) i internetowe (art. 286 kk)

3.3.1. analiza znamion ustawowych i *modus operandi*

3.3.2. analiza kazuów:

3.3.2.1. oszustwo komputerowe w banku,

3.3.2.2. oszustwo na aukcji internetowej.

3.4. Wyłudzenie usług telekomunikacyjnych (art. 285 kk, art. 121 kw)

3.5. „Kradzież” sygnału płatnej telewizji (kablowej i satelitarnej) - przepisy karne ustawy z dnia 23 maja 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym.

3.6. Piractwo internetowe utworów prawnie chronionych:

3.6.1. programy komputerowe (art. 278 § 2 i art. 293 kk; art. 116-188 PrAut)

3.6.2. utwory muzyczne i filmy (art. 116-188 PrAut)

### 3.7. Przestępstwa związane z kartami płatniczymi.

3.7.1. Decyzja ramowa 2001/413/WSiSW z 28 maja 2001 w sprawie zwalczania oszustw i podrabiania bezgotówkowych środków płatniczych [ Dz.Urz. WE nr L 149, 02/06/2001].

3.7.2. Polska regulacja prawna i orzecznictwo SN.

### 3.8. Cyberpornografia z udziałem małoletnich

3.8.1. Ewolucja zjawiska i kontroli społecznej

3.8.2. Międzynarodowe i europejskie standardy karalności:

1. Konwencja NZ o Prawach Dziecka z 1989 r.
2. Protokół dodatkowy z 2000 r. do Konwencji o Prawach Dziecka dotyczący sprzedaży dzieci, prostytucji dziecięcej i pornografii dziecięcej.
3. Art. 9 konwencji Rady Europy z 2001 r. o Cyberprzestępczości
4. Decyzja ramowa Rady Unii Europejskiej 2004/68/WSiSW o zwalczaniu eksploatacji seksualnej dzieci i pornografii dziecięcej.
5. Konwencja Rady Europy z 2007 r. o ochronie dzieci przed seksualną eksploatacją i wykorzystywaniem.

3.8.3 Polskie ustawodawstwo karne.

3.8.3.1 Przedmiot wykonawczy przestępstw związanych z cyberpornografią dziecięcą

3.8.3.2 Pornografia wirtualna i symulowana

3.8.3.3 Internetowe usługi informacyjne a czynności wykonawcze - zagadnienie kwalifikacji prawnej na podstawie art. 202 kk

- i. rozpowszechnianie,
- ii. publiczne prezentowanie,
- iii. produkowanie,
- iv. utrwalanie,
- v. sprowadzanie,
- vi. przechowywanie,
- vii. posiadanie

#### 3.8.4 Karalność uwodzenia małoletnich przez sieć.

- 3.8.4.1 Konwencja Rady Europy z 2007 r. o ochronie dzieci przed seksualną eksploatacją i wykorzystywaniem
- 3.8.4.2 Prawo porównawcze
- 3.8.4.3 Projekt nowelizacji kk z 26.04.2007 r. (art. 199a i art. 255a kk)

#### 3.8.5 Ochrona małoletnich przed pornografią internetową ( art. 202 § 2 kk).

#### Literatura:

Andrzej Adamski, Prawo karne komputerowe, Wydawnictwo C.H. Beck, Warszawa 2000.

Andrzej Adamski, Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, TNOiK, Toruń 2001.

Andrzej Adamski, Karnoprawna ochrona dziecka w sieci Internet, *Prokuratura i Prawo* nr 9, 2003.

Andrzej Adamski, Retencja danych o ruchu telekomunikacyjnym - polskie rozwiązania i europejskie dylematy, *Przeгляд Prawa i Administracji*, t. LXII, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław, 2005.

Andrzej Adamski, Cyberprzestępczość - aspekty prawne i kryminologiczne, *Studia Prawnicze* 2005 nr 4 (167).

Andrzej Adamski, Harmonizacja prawa karnego państw Unii Europejskiej w dziedzinie przestępstw związanych z kartami płatniczymi, *Studia Prawnicze* 2006 nr 4.

Andrzej Adamski, Nowe ujęcie cyberprzestępstw w kodeksie karnym - ale czy lepsze?, *Prawo Teleinformatyczne* 2007 nr 3 (5).