Prawo karne materialne

To po prostu wszystkie przepisy, które stanowią katalog przestępstw oraz kar, które grożą za ich popełnienie. Zawiera także zasady odpowiedzialności karnej.

Funkcje prawa karnego:

1. ochronna — ochrona dóbr przed zamachem na nie
2. afirmacyjno-motywacyjna — mamy sankcje oraz wytyczne co do dóbr chronionych
3. gwarancyjna — określone są przestępstwa i kary za nie przewidziane oraz jakie są zasady odpowiedzialności. Chodzi o zagwarantowanie, aby nikt niewinny nie został pociągnięty do odpowiedzialności.
4. prewencyjno-wychowawcza — prawo karne działa na sprawcę (prewencja indywidualna) oraz na społeczeństwo (prewencja społeczna)
5. sprawiedliwościowa — zaspokaja społeczne poczucie sprawiedliwości

Zasady prawa karnego:

1. odpowiedzialności karnej za czyn (za działanie lub zaniechanie działania)
2. winy (tylko, z popełnienia czynu można postawić zarzut)
3. odpowiedzialności indywidualnej i osobistej
4. zasada humanitaryzmu
5. Nullum crimen sine lege – nie ma przestępstwa bez ustawy
    a. nullum crimen sine lege scripts – prawo pisane, zawarte w ustawie
    b. nullum crimen sine lege certa – maksymalna dokładność opisu przestępstwa
    c. nullum poena sine lege – nie ma kary bez ustawy; musi być ściśle kara określona i przewidziana
    d. zakaz analogii na niekorzyść oskarżonego

Kryminologia – bada przestępstwo, przestępcę i społeczną reakcję na to przestępstwo, w sposób niezależny od aktualnych uregulowań prawnych.

Wyróżniamy dwa kierunki: biologiczny i psychospołeczny oraz socjologiczny. Pierwszy wiąże genezę przestępstwa z cechami psychofizycznymi człowieka albo z interakcją procesów psychicznych i społecznych. Kierunek socjologiczny natomiast wiąże przestępstwo i przestępczość jako zjawisko masowe ze zjawiskami i procesami społecznymi (ekonomicznymi, kulturowymi, itp.)

Dostarczając wiedzy socjologicznej i psychologicznej, kryminologia pozwala na poszukiwanie najlepszych form prawnej regulacji, zwłaszcza zaś wpływa na optymalizację prawnych środków zwalczania przestępstw.

Kryminalistyka – nauka o sposobach i metodach wykrywania przestępstw i ich sprawców oraz uzyskiwania środków dowodowych na potrzeby postępowania karnego. Także nauka o wykrywaniu istnienia związku między osobami i zdarzeniami.

Kryminalistyka:

- taktyka kryminalistyczna – wykorzystuje wiedzę psychologiczną (np. taktyka przesłuchania podejrzanego, świadka)

- technika kryminalistyczna – wykorzystuje zdobycze różnych nauk (chemii, fizyki, itp.)

Jej zadaniem jest opracowanie techniczno-taktycznych środków zapobiegania przestępczości.

Wiktymologia – nauka o ofiarach przestępstw.

Wiktymologia kryminalna – wiktymologia ograniczona do problematyki ofiar przestępstw i innych naruszeń praw człowieka.

Przedmiot badań:

- dynamika, struktura i uwarunkowanie zjawiska pokrzywdzenia (wiktymizacji)

- rola ofiary w genezie przestępstwa

- problematyka ochrony interesów ofiar przestępstw i innych pogwałceń praw człowieka – w tym indemnizacji

indemnizacja = naprawienie szkody wyrządzonej ofierze.

1985 r. Deklaracja ONZ o Podstawowych Prawach Ofiar Przestępstw i Nadużyć Władzy.

Dowód elektroniczny

Polskie prawo nie posiada tzw. legalnej (czyli oficjalnej / urzędowej) definicji dowodów elektronicznych.

Dowody elektroniczne można interpretować dwojako:

- jako dokumenty na podstawie art. 114 § 14 KK (zgodnie z którym *dokumentem jest każdy przedmiot lub inne zapisany nośnik informacji z którym związane jest określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne*),

- jako dowody “inne” z swego charakteru, nie mieszczących się w tradycyjnym podziale na dowody rzeczowe oraz osobowe.

Dowód elektroniczny w największym uproszczeniu jest informacją zapisaną na nośniku elektronicznym np. na dysku twardego komputera, w pamięci telefonu etc. Może on przybierać postać dokumentów komputerowych (maile, smsy, zdjęcia, teksty tworzone w wordzie) jak i danych cyfrowych (tzw. logów komputerowych) np. ukazujących historię logowania z danego IP komputera na dany serwer.

Dowodem elektronicznym będą zarówno tzw. logi cyfrowe pokazujące że o godzinie 12:05 z komputera o nr IP 2324 wysłano e-mail, jak i sama treść e-maila. Będa to też pliki znalezione w komputerze (fotografie, dokumenty tekstowe etc.) oraz informacje dostarczane przez komputer o procesach na nim prowadzonych (np. historia odwiedzanych witryn internetowych).

Nośnik to dla dowodów niematerialnych w postaci informacji to Corpus mechanicum. Są to dowody elektroniczne. Cechy szczególne to:

- specyficzna forma

- łatwość modyfikacji

- łatwość kopiowania

- nietrwałość

specjalne środki do ich gromadzenia, uzyskiwania oraz prezentacji w postępowaniu.

Computer Forensic zajmuje się metodami zabezpieczania i badania dowodów w sposób gwarantujący integralność oraz autentyczność. **Informatyka śledcza** pozwala odtworzyć kolejność działań na komputerze lub innym urządzeniu elektronicznym użytkownika w czasie.

Komputer może być obiektem przestępstwa, przedmiotem przestępstwa lub narzędziem przestępstwa.

System informatyczny

Pojęcie pojawiło się w art. 267 kk i występuje także w innych przepisach. Pomimo ujednolicenia terminologii informatycznej i wprowadzenia do ustaw terminu „system teleinformatyczny" ustawodawca posłużył się innym określeniem, nie zdefiniowanym ustawowo.

Definicję „system informatyczny" można natomiast znaleźć w art. 1 Konwencji o cyberprzestępczości. Zgodnie z nią jest to każde urządzenie lub grupa wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych. Ta definicja zasadniczo zgadza się z definicją „systemu teleinformatycznego"14, z tą różnicą, że nie obejmuje funkcji wysyłania i odbierania danych. Podobnego zdania jest A. Baworowski, który twierdzi, że pojęcie „system teleinformatyczny" jest szersze od pojęcia „system informatyczny", gdyż system teleinformatyczny oprócz przetwarzania i przechowywania danych będzie służył także do ich

przesyłania i odbierania. Jak zauważa, każdy system teleinformatyczny jest systemem informatycznym, lecz nie każdy system informatyczny jest systemem teleinformatycznym.

Hacking

art. 267 § 1 i 2 kk => hacking w wąskim ujęciu: przedmiotem ochrony jest informacja.

W klasycznym rozumieniu hacking to wtargnięcie do obcego systemu komputerowego nie w celu manipulacji, sabotażu ub szpiegostwa, ale dla satysfakcji i uzyskania informacji dot. środków zabezpieczenia.

W potocznym rozumieniu, termin wiąże się z prawem karnym, jednak pen testy nie zawsze są legalne.

cracking – włamanie do komputerów w celu uzyskania określonych korzyści

phreaking – wyszukiwanie luk w systemach telekomunikacyjnych

Karze podlega uzyskanie bez uprawnienia dostępu do systemu informatycznego lub jego części, nawet bez złamania jakiegokolwiek zabezpieczenia zainstalowanego w komputerze użytkownika lub zabezpieczenia systemowego.

System: w praktyce przyjmuje się, że jest to zespół współpracujących elementów sprzętowych i programowych, które służą do wprowadzania, przetwarzania i odczytywania informacji wykorzystujących binarną postać danych.

W zależności od ustaleń, można rozważać odpowiedzialność z art. 267 § 2 kk w przypadku uzyskania fizycznego dostępu do komputera i korzystania z niego przez osobę nieuprawnioną lub po ustaleniu, że doszło do wprowadzenia do komputera oprogramowania, które umożliwia przejęcie zdalnej kontroli.

W zależności od ustaleń, można rozważać odpowiedzialność z art. 267 § 1 kk w przypadku dostępu do poczty poprzez uzyskanie hasła do poczty, korzystając np. z procedury podpowiedzi.

Nielegalny podsłuch

art. 267 § 3 kk

Do podsłuchu może posłużyć każde urządzenie służące do rejestracji obrazu i dźwięku. Gdy rozpatruje się przestępstwa komputerowe, będzie to specjalistyczne oprogramowanie służące do nieuprawnionego pozyskania informacji. Używanie ich należy wiązać z procesem komunikowania się użytkowników komputera za pomocą Internetu.

Zastosowanie keyloggera możliwe jest tylko w sytuacji umieszczenia go w podsłuchiwanym systemie komputerowym.

Sniffer służy do podsłuchu komputerowego. Jego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w badanej sieci. Może mieć legalne i nielegalne zastosowanie. Mogą mieć zastosowanie w diagnostyce problemów z funkcjonowaniem połączeń internetowych przez administratorów sieci, ale także służyć jako narzędzie informatyczne do podsłuchiwania innego użytkownika komputera. Żeby zastosować, narzędzie nie musi być zainstalowane na komputerze ofiary. Wystarczy, że będzie dostępne na komputerze sprawcy lub komputerze, do którego sprawca ma dostęp.

Keylogger: musi być zainstalowany na komputerze ofiary, umożliwia pozyskiwanie zrzutów z ekranu ofiary, przeanalizowane dane wysyłane są na maila sprawcy lub serwer FTP

Sniffer: (np. tcpdump, wireshark) może przechwytywać dane przepływające przez sieć, poprzez analizę danych sieciowych sprawca uzyskuje dostęp do komputera ofiary, do zastosowania wystarczy, że będzie zainstalowane na komputerze sprawcy

Nielegalny podsłuch:

- jest tylko umyślny, w bezpośrednim zamiarze pozyskania informacji,

- przestępstwo jest bezwzględnie wnioskowe

- indywidualnym przedmiotem ochrony jest poufność informacji

przedmiotem badania jest wyłącznie zakładanie i posługiwanie się oprogramowaniem w celu uzyskania informacji bez uprawnienia.

Naruszenie integralności komputerowego zapisu informacji:

- niszczenie istotnych informacji zapisanych na informatycznym nośniku danych,

- uszkodzenie informacji zapisanej na informatycznym nośniku danych,

- usunięcie istotnych informacji zapisanych na informatycznym nośniku danych,

- zmiana zapisu informacji,

- udaremnienie w inny sposób zapoznania się z istotną informacją zapisaną na informatycznym nośniku danych,

- utrudnianie w inny sposób zapoznania się z istotną informacją zapisaną na komputerowym nośniku danych.

Sankcje są przewidziane za typ kwalifikowany wyłącznie z uwagi na działanie przestępcze skierowane wobec informacji i miejsca jej zapisu w postaci nośnika komputerowego.

Przestępstwo z art. 268 ma charakter materialny. Skutkiem karalnym jest zniszczenie, uszkodzenie i inne zmiany przewidziane w tym przepisie. Ma charakter powszechny – dopuścić się go może każdy, kto nie ma uprawnienia do informacji. Może być popełnione zarówno przez działanie jak i zaniechanie. Działanie lub zaniechanie może objąć samą informację jak i jej nośnik. Ścigane na wniosek.

Dotyczy:

- bezprawnego usuwania plików,

- bezprawnej modyfikacji danych,

- uszkodzenia dzialania systemu informatycznego,

- zakłócenia jego funkcjonowania,

skutkujące niemożnością dostępu przez osoby uprawnione do informacji.

Najczęściej działanie następuje przez umieszczenie w systemie złośliwego oprogramowania.

Wniosek o ściganie może złożyć każdy, kto stwierdzi istnienie złośliwego oprogramowania. Warunkiem jest to, że rezultatem działania oprogramowania musi być wskazane w przepisach kk oddziaływanie na informację.

Sabotaż komputerowy

art. 269:

- zniszczenie,

- uszkodzenie,

- usunięcie,

- zmiana,

- zakłócenie automatycznego przetwarzania, gromadzenia, przekazywania danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego.

To też zniszczenie albo uszkodzenie urządzenia służącego do ich automatycznego przetwarzania, gromadzenia lub przekazywania.

Przedmiotem ochrony jest poufność, integralność i dostępność informacji. Można je popełnić z zamiarem bezpośrednim lub z ewentualnym w stosunku do:

- samych danych informatycznych oraz

- nośnika zawierającego te dane.

Karane jest logiczne (programowe) i fizyczne niszczenie wskazanych w przepisie danych. Nie ma znaczenia, czy te dane zostały utracone ani czy znajdowały się nadal w posiadaniu organu, zabezpieczone przez sporządzenie backupów w postaci kopii rezerwowej.

Informacja podlegająca ochronie musi mieć znaczenie dla podmiotów wskazanych w przepisie, oceniane obiektywnie. Sabotaż jest ścigany z urzędu.