Kodeks karny

Rozdział XXXIII

Przestępstwa przeciwko ochronie informacji

Wykład, 1 rok informatyki algorytmicznej WPPT

Mirosław Kutyłowski 2020

Cel prawa karnego (w państwach prawa):

- **Zestaw reguł odstraszający od negatywnych zachowań**
- **Wymaganie: prosta i jednoznaczna procedura decyzyjna – dla sądu i dla obywatela**

trade-off pomiędzy prostotą a precyzją

- **Optymalizacja niekoniecznie daje rezultaty zgodne z poczuciem sprawiedliwości**

Cel (w państwach totalitarnych):

- **reżim arbitralnie określa zasady i sankcje ex post**
- **środek: niejasne i arbitralne przepisy**

Przykład efektywnej regulacji:

sytuacja: wypadek drogowy, konieczność ustalenia sprawcy

czynnik: wpływ alkoholu

algorytm: o ile uczestnicy są pod wpływem alkoholu, to uczestnik mający wyższy poziom alkoholu uznawany jest jako winny

efekt: kierowca powstrzymuje się od spożycia alkoholu wiedząc że jak ktoś inny w niego wjedzie, to będzie za cudzy błąd odpowiadał karnie

Przykład efektywnej regulacji (Niemcy):

aproksymacja: nie jest zawsze prawdą, że osoba o wyższym stężeniu alkoholu faktycznie spowodowała wypadek

możliwe nadużycia: widząc pijanego kierowcę spowodować z nim stłuczkę

ale: koszty postępowania sądowego są minimalne, efekt odstraszający jest bardzo silny, nie ma możliwości tuszowania winy osób „wyżej postawionych”

Inny przykład (Australia):

sytuacja: postępowanie rozwodowe, podział majątku

zwykle: długa i niezwykle kosztowna walka obciążająca system sądownictwa, duże koszty społeczne

algorytm australijski podziału wspólnego majątku:

1) osoba A określa cenę x dla składnika majątku M
2) osoba B ma wybór:
   a) przejmuje całe M i płaci osobie A sumę x/2 , albo
   b) dostaje sumę x/2 od osoby A

Efekt: **osoba A wyznaczając cenę x dla składnika majątku M traci o ile**

- **cena x jest niższa od rzeczywistej wartości**
- **cena x jest wyższa od rzeczywistej wartości**

Więc: **nieuczciwe lub złośliwe postępowanie obraca się natychmiast przeciwko autorowi**

Podział majątku może być przeprowadzony online i zautomatyzowany

Przykład - Kradzież tożsamości

Art. 275. § 1. **Kto posługuje się dokumentem stwierdzającym tożsamość innej osoby** albo jej prawa majątkowe lub dokument taki kradnie lub go przywłaszcza, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.**

§ 2. Tej samej karze podlega, kto bezprawnie przewozi, przenosi lub przesyła za granicę dokument stwierdzający tożsamość innej osoby albo jej prawa majątkowe.

Przykład – kredyty na fałszowane dowody osobiste

sytuacja:

- Serwisy online umożliwiające zakup sfałszowanego dokumentu: wystarczy wpisać dane, opłacić (kilkaset zł) .. i dokument przychodzi kurierem
- Dobra jakość wykonania: wystarczająca do wzięcia kredytu „chwilówki” czy zwykłej inspekcji przez niespecjalistę
- Zgodnie z decyzją UODO: firma kredytowa nie ma nawet prawa skopiować dokumentu który okazano

Przykład – kredyty na fałszowane dowody osobiste

Realna groźba:

- **osoba znająca Twoje podstawowe dane (PESEL itp.) może wyrobić sobie dość wiarygodny dokument i wziąć kredyt**
- **kredytu się nie wyprzesz (chyba że np. możesz udowodnić że w tym czasie byłeś na Nowej Zelandii...)**

(Banki są świadome groźby i ostrożne ale co z „kredytami na dowód” w budkach koło Dworca?)

„Dokumenty kolekcjonerskie”

trick:

tak zdefiniować produkt i jego przeznaczenie aby wyślizgnąć się z odpowiedzialności karnej

Przepis karny ma postać:

jeśli A to kara X

strategia przestępców: sprawić by zdanie A nie było spełnione

„Dokumenty kolekcjonerskie” - sytuacja do 2019

Co mogą mogły zrobić organy ścigania po wykryciu „dziupli” z tysiącami fałszywych dokumentów tożsamości.

Przyłapana osoba twierdzi, że jest kolekcjonerem i nie są to dokumenty tożsamosci, ale dokumenty kolekcjonerskie

Art. 270.

§1. Kto, **w celu użycia za autentyczny**, **podrabia lub przerabia** dokument **lub takiego dokumentu jako autentycznego używa**, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3miesięcy do lat 5.

Sąd jest bezsilny: trzebaby wykazać cel niekolekcjonerski lub przyłapać na próbie wyłudzenia kredytu

Art. 275. § 1. **Kto posługuje się dokumentem stwierdzającym tożsamość innej osoby** albo jej prawa majątkowe lub dokument taki kradnie lub go przywłaszcza, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.**

§ 2. Tej samej karze podlega, kto bezprawnie przewozi, przenosi lub przesyła za granicę dokument stwierdzający tożsamość innej osoby albo jej prawa majątkowe.

Policja jest bezsilna: tylko złapanie w momencie wyłudzania kredytu daje możliwość postawienia oskarżenia

Łatka – Ustawa z dnia 22.11.2018r. o dokumentach publicznych:

Art.58. Kto wytwarza, oferuje, zbywa lub przechowuje w celu zbycia replikę dokumentu publicznego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Faktyczny Efekt:

- **Scenariusz bezpieczny dla przestępcy: oferować działając np. w Holandii, fałszywy dokument wysłać bezpośrednio do klienta**
- **Co więcej: eliminacja konkurencji ze strony lokalnych polskich fałszerzy**

Zasady ogólne prawa karnego

Art. 1.

§ 1. Odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. ***(prawo nie działa wstecz)***

§ 2. Nie stanowi przestępstwa czyn zabroniony, którego społeczna szkodliwość jest znikoma.

§ 3. Nie popełnia przestępstwa sprawca czynu zabronionego, jeżeli nie można mu przypisać winy w czasie czynu. ***(np. osoby chore psychicznie)***

Art. 3.

Kary oraz inne środki przewidziane w tym kodeksie stosuje się z uwzględnieniem zasad humanitaryzmu, w szczególności z poszanowaniem godności człowieka.

Kar nie stosuje się „dla przykładu”.

Realia: tradycja kulturowa linczu, populizm polityków

Art. 4.

§ 1. Jeżeli w czasie orzekania obowiązuje ustawa inna niż w czasie popełnienia przestępstwa, stosuje się ustawę nową, jednakże należy stosować ustawę obowiązującą poprzednio, jeżeli jest względniejsza dla sprawcy.

– w momencie popełnienia czynu można oszacować wysokość kary

Art. 5.

Ustawę karną polską stosuje się do sprawcy, który popełnił czyn zabroniony na terytorium Rzeczypospolitej Polskiej, jak również na polskim statku wodnym lub powietrznym, chyba że umowa międzynarodowa, której Rzeczpospolita Polska jest stroną, stanowi inaczej.

– określenie miejsca może być kluczowe w przestępstwach dokonywanych w Internecie. Przepisy karne w różnych krajach (nawet UE) są bardzo różne

Art. 6. § 1. Czyn zabroniony uważa się za popełniony w czasie, w którym sprawca działał lub zaniechał działania, do którego był obowiązany.

§ 2. Czyn zabroniony uważa się za popełniony w miejscu, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, albo gdzie skutek stanowiący znamię czynu zabronionego nastąpił lub według zamiaru sprawcy miał nastąpić.

Aby dokonać cyberataku w Polsce i uniknąć odpowiedzialności nie wystarczy wyjechać z kraju.

Art. 9.

§ 1. Czyn zabroniony popełniony jest umyślnie, jeżeli sprawca ma zamiar jego popełnienia, to jest chce go popełnić albo przewidując możliwość jego popełnienia, na to się godzi.

§ 2. Czyn zabroniony popełniony jest nieumyślnie, jeżeli sprawca nie mając zamiaru jego popełnienia, popełnia go jednak na skutek niezachowania ostrożności wymaganej w danych okolicznościach, mimo że możliwość popełnienia tego czynu przewidywał albo mógł przewidzieć.

(np. kierowca jadący 100km/h w terenie zabudowanym, który potrącił pieszego)

– istotne rozróżnienie, bo wysokości kar są inne

Art. 9.

§ 3. Sprawca ponosi surowszą odpowiedzialność, którą ustawa uzależnia od określonego następstwa czynu zabronionego, jeżeli następstwo to przewidywał albo mógł przewidzieć.

Art. 10.

§ 1. Na zasadach określonych w tym kodeksie odpowiada ten, kto popełnia czyn zabroniony po ukończeniu 17 lat.

– dlatego przestępcy komputerowi wynajmują małoletnich (podobnie jak dilerzy)

Art. 11.

§ 1. Ten sam czyn może stanowić tylko jedno przestępstwo.

§ 2. Jeżeli czyn wyczerpuje znamiona określone w dwóch albo więcej przepisach ustawy karnej, sąd skazuje za jedno przestępstwo na podstawie wszystkich zbiegających się przepisów.

§ 3. W wypadku określonym w § 2 sąd wymierza karę na podstawie przepisu przewidującego karę najsurowszą, co nie stoi na przeszkodzie orzeczeniu innych środków przewidzianych w ustawie na podstawie wszystkich zbiegających się przepisów.

– inaczej niż w USA

Art. 13.

§ 1. Odpowiada za usiłowanie, kto w zamiarze popełnienia czynu zabronionego swoim zachowaniem bezpośrednio zmierza do jego dokonania, które jednak nie następuje.

§ 2. Usiłowanie zachodzi także wtedy, gdy sprawca nie uświadamia sobie, że dokonanie jest niemożliwe ze względu na brak przedmiotu nadającego się do popełnienia na nim czynu zabronionego lub ze względu na użycie środka nie nadającego się do popełnienia czynu zabronionego.

– włamanie do systemu nie musi się udać by zostać za nie skazanym. Nawet gdy włamanie nie może się technicznie udać...

Art. 14.

§ 1. Sąd wymierza karę za usiłowanie w granicach zagrożenia przewidzianego dla danego przestępstwa.

– tak więc nie można liczyć że nieudane włamanie skończy się mniejszą karą

Art. 15.

§ 1. Nie podlega karze za usiłowanie, kto dobrowolnie odstąpił od dokonania lub zapobiegł skutkowi stanowiącemu znamię czynu zabronionego.

§ 2. Sąd może zastosować nadzwyczajne złagodzenie kary w stosunku do sprawcy, który dobrowolnie starał się zapobiec skutkowi stanowiącemu znamię czynu zabronionego.

– jeśli przypadkiem uruchomimy jakiś malware, to lepiej go unieruchomić

Art. 16.

§ 1. **§ 1. Przygotowanie zachodzi tylko wtedy, gdy sprawca w celu popełnienia czynu zabronionego podejmuje czynności mające stworzyć warunki do przedsięwzięcia czynu zmierzającego bezpośrednio do jego dokonania, w szczególności w tymże celu wchodzi w porozumienie z inną osobą, uzyskuje lub przysposabia środki, zbiera informacje lub sporządza plan działania.**

§ 2. Przygotowanie jest karalne tylko wtedy, gdy ustawa tak stanowi.

– w informatyce trzeba uważać by nie zostać posądzonym o przygotowanie

Art. 18.

§ 1. Odpowiada za sprawstwo nie tylko ten, kto wykonuje czyn zabroniony sam albo wspólnie i w porozumieniu z inną osobą, ale także ten, kto kieruje wykonaniem czynu zabronionego przez inną osobę lub wykorzystując uzależnienie innej osoby od siebie, poleca jej wykonanie takiego czynu.

§ 2. Odpowiada za podżeganie, kto chcąc, aby inna osoba dokonała czynu zabronionego, nakłania ją do tego.

– zlecając włamanie pracownikowi dalej odpowiadamy.

§ 3. Odpowiada za pomocnictwo, kto w zamiarze, aby inna osoba dokonała czynu zabronionego, swoim zachowaniem ułatwia jego popełnienie, w szczególności dostarczając narzędzie, środek przewozu, udzielając rady lub informacji; odpowiada za pomocnictwo także ten, kto wbrew prawnemu, szczególnemu obowiązkowi niedopuszczenia do popełnienia czynu zabronionego swoim zaniechaniem ułatwia innej osobie jego popełnienie

– tworząc narzędzia informatyczne trzeba uważać by nie odpowiadać za pomocnictwo. Narzędzia muszą mieć jednoznacznie legalny zakres użycia.

Art. 23.

§ 1. Nie popełnia przestępstwa, kto w obronie koniecznej odpiera bezpośredni, bezprawny zamach na jakiekolwiek dobro chronione prawem.

§ 2. W razie przekroczenia granic obrony koniecznej, w szczególności gdy sprawca zastosował sposób obrony niewspółmierny do niebezpieczeństwa zamachu, sąd może zastosować nadzwyczajne złagodzenie kary, a nawet odstąpić od jej wymierzenia.

– dotyczy również cyberataków

Art. 26.

§ 1. Nie popełnia przestępstwa, kto działa w celu uchylenia bezpośredniego niebezpieczeństwa grożącego jakiemukolwiek dobru chronionemu prawem, jeżeli niebezpieczeństwa nie można inaczej uniknąć, a dobro poświęcone przedstawia wartość niższą od dobra ratowanego.

– odpieranie cyberataku może być również atakiem..

Art. 27.

§ 1. Nie popełnia przestępstwa, kto działa w celu przeprowadzenia eksperymentu poznawczego, medycznego, technicznego lub ekonomicznego, jeżeli spodziewana korzyść ma istotne znaczenie poznawcze, medyczne lub gospodarcze, a oczekiwanie jej osiągnięcia, celowość oraz sposób przeprowadzenia eksperymentu są zasadne w świetle aktualnego stanu wiedzy.

§ 2. Eksperyment jest niedopuszczalny bez zgody uczestnika …

– wiele czynności informatycznych daje się zakwalifikować jako eksperyment poznawczy

Art. 28.

§ 1. Nie popełnia umyślnie czynu zabronionego, kto pozostaje w błędzie co do okoliczności stanowiącej jego znamię.

§ 2. …

Art. 32. Karami są:

1) grzywna;

2) ograniczenie wolności;

3) pozbawienie wolności;

4) 25 lat pozbawienia wolności;

5) dożywotnie pozbawienie wolności.

W istocie dochodzą jeszcze środki zapobiegawcze i teraupetyczne – czasem bardziej dolegliwe niż kary.

Art. 39. Środkami karnymi są:

1) pozbawienie praw publicznych;

2) zakaz zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej;

…

– zakaz działalności zawodowej jest istotnym zagrożeniem

Art. 44.

§ 1. Sąd orzeka przepadek przedmiotów pochodzących bezpośrednio z przestępstwa.

§ 2. Sąd może orzec, a w wypadkach wskazanych w ustawie orzeka, przepadek przedmiotów, które służyły lub były przeznaczone do popełnienia przestępstwa.

§ 3. Jeżeli orzeczenie przepadku określonego w § 2 byłoby niewspółmierne do wagi popełnionego czynu, sąd zamiast przepadku może orzec nawiązkę na rzecz Skarbu Państwa.

– co jeśli pracownik dokona przestępstwa korzystając z firmowego sprzętu?

Art. 53.

§ 1. Sąd wymierza karę według swojego uznania, w granicach przewidzianych przez ustawę, bacząc, by jej dolegliwość nie przekraczała stopnia winy, uwzględniając stopień społecznej szkodliwości czynu oraz biorąc pod uwagę cele zapobiegawcze i wychowawcze, które ma osiągnąć w stosunku do skazanego, a także potrzeby w zakresie kształtowania świadomości prawnej społeczeństwa.

Art. 53.

§ 2. Wymierzając karę, sąd uwzględnia w szczególności motywację i sposób zachowania się sprawcy, popełnienie przestępstwa wspólnie z nieletnim, rodzaj i stopień naruszenia ciążących na sprawcy obowiązków, rodzaj i rozmiar ujemnych następstw przestępstwa, właściwości i warunki osobiste sprawcy, sposób życia przed popełnieniem przestępstwa i zachowanie się po jego popełnieniu, a zwłaszcza staranie o naprawienie szkody lub zadośćuczynienie w innej formie społecznemu poczuciu sprawiedliwości, a także zachowanie się pokrzywdzonego.

Art. 57a.63) § 1. Skazując za występek o charakterze chuligańskim, sąd wymierza karę przewidzianą za przypisane sprawcy przestępstwo w wysokości nie niższej od dolnej granicy ustawowego zagrożenia zwiększonego o połowę.

– uwaga, „zwykłe przestępstwo” jest dużo mniej ryzykowne. Niektóre rodzaje ataków mogą być uznane za chuligaństwo

Występkiem o charakterze chuligańskim jest występek polegający na zamachu na wolność, na cześć lub nietykalność cielesną, na bezpieczeństwo powszechne, na działalność instytucji państwowych lub samorządu terytorialnego, na porządek publiczny, albo na umyślnym niszczeniu, uszkodzeniu lub czynieniu niezdatną do użytku cudzej rzeczy, jeżeli sprawca działa publicznie i bez powodu albo z oczywiście błahego powodu, okazując przez to rażące lekceważenie porządku prawnego.

Sąd stosuje nadzwyczajne złagodzenie kary, a nawet może warunkowo zawiesić jej wykonanie w stosunku do sprawcy współdziałającego z innymi osobami w popełnieniu przestępstwa, jeżeli ujawni on wobec organu powołanego do ścigania przestępstw informacje dotyczące osób uczestniczących w popełnieniu przestępstwa oraz istotne okoliczności jego popełnienia.

– „wsypanie wspólników”

4. Na wniosek prokuratora sąd może zastosować nadzwyczajne złagodzenie kary, a nawet warunkowo zawiesić jej wykonanie w stosunku do sprawcy przestępstwa, który, niezależnie od wyjaśnień złożonych w swojej sprawie, ujawnił przed organem ścigania i przedstawił istotne okoliczności, nieznane dotychczas temu organowi, przestępstwa zagrożonego karą powyżej 5 lat pozbawienia wolności.

– ***niebezpieczeństwo obciążenia fikcyjnymi zarzutami przez przestępcę usiłującego złagodzić swoją karę***

Kodeks karny

Rozdział XXXIII

Przestępstwa przeciwko ochronie informacji

Ważne dla informatyków!

Art. 265.

§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje stanowiące tajemnicę państwową podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

– ostrożnie w przypadku realizacji zadań dla podmiotów publicznych

Art. 165.

§ 1. Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach:

4) zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych,

… podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Jeżeli sprawca działa nieumyślnie … do lat 3.

Art. 265.

§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 266.

§ 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

– uważać na przestrzeganie umów NDA

Art. 266.

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację stanowiącą tajemnicę służbową lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes podlega karze pozbawienia wolności do lat 3.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Art. 267.

§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenia podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

– *dotyczy również komunikacji elektronicznej: emaili, komunikatorów, ...*

Art. 267.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

– zakładanie snifferów jest z tego powodu karalne!

Art. 268.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

– ***kary za manipulacje informacji i za jej usuwanie***

Art. 268.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

– wyższe kary gdy chodzi o straty gospodarcze (niższe kary z poprzedniego art. np. gdy komuś zniszczymy prywatne zdjęcia z wakacji)

Art. 268a.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

– z tego art. kary za zniszczenie danych umożliwiających logowanie, za ransomware,...

Art. 269.

§ 1. Kto **niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.**

– ***włamania do sieci wojska, policji, itp. są szczególnie złym pomysłem!***

Art. 269.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a.

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

– tutaj ataki nie na przetwarzenie konkretnych informacji ale na cała infrastrukturę, np. poprzez DDoS

Art. 269b.

§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 2, art. 268a § 1 albo § 2 w związku z §1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

– przykład nieudolnej regulacji – serwisy podpowiadające hasła wg art. 269b to działalność przestępcza

Art. 269c.

Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

– można naciągnąć art 269c aby podpowiadanie haseł zalegalizować

Art. 270.

§ 1. Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto wypełnia blankiet, zaopatrzony cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo takiego dokumentu

§ 3. Kto czyni przygotowania do przestępstwa określonego w § 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

– szczególnie ważne, gdy dokumenty mają postać elektroniczną, gdy można podszyć się pod nadawcę emaila

Art. 270a.

§ 1. Kto, w celu użycia za autentyczną, podrabia lub przerabia fakturę w zakresie okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym lub takiej faktury jako autentycznej używa, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

…

– uwaga: faktury nie muszą być zabezpieczone elektornicznie i ich przerabianie jest trywialne pod wzgledem technicznym

Art. 271.

§ 1. 4 Funkcjonariusz publiczny lub inna osoba uprawniona do wystawienia dokumentu, która poświadcza w nim nieprawdę co do okoliczności mającej znaczenie prawne, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Przypadek: oskarżenie recenzenta

Art. 272.

§ Kto wyłudza poświadczenie nieprawdy przez podstępne wprowadzenie w błąd funkcjonariusza publicznego lub innej osoby upoważnionej do wystawienia dokumentu, podlega karze pozbawienia wolności do lat 3.

– ***dotyczy np. uzyskania zaświadczenia z Dziekanatu itp. Nie można się zasłaniać tym, że to Dziekan poświadczył nieprawdę***

Art. 273.

§ Kto używa dokumentu określonego w art. 271 lub 272, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

– ***kary za posługiwanie się zaświadczeniami z nieprawdziwą treścią***

Art. 276.

Kto niszczy, uszkadza, czyni bezużytecznym, ukrywa lub usuwa dokument, którym nie ma prawa wyłącznie rozporządzać, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art. 277a.

§ 1. Kto dopuszcza się przestępstwa określonego w art. 270a § 1 albo art. 271a § 1 wobec faktury lub faktur, zawierających kwotę należności ogółem, której wartość lub łączna wartość jest większa niż dziesięciokrotność kwoty określającej mienie wielkiej wartości,

podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności.

– pisząc oprogramowanie finansowo-księgowe dla firm trzeba bardzo uważać. Błąd może okazać się zbrodnią z punktu widzenia prawa.

Art. 278.

§ 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej.

– nie ściągać żadnego programu, który nie jest opatrzony licencją. To może być pułapka!

Art. 287.

§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

– porównać z art. 269a (zadanie domowe).

Art. 282.

Kto, w celu osiągnięcia korzyści majątkowej, przemocą, groźbą zamachu na życie lub zdrowie albo gwałtownego zamachu na mienie, doprowadza inną osobę do rozporządzenia mieniem własnym lub cudzym albo do zaprzestania działalności gospodarczej,

podlega karze pozbawienia wolności od roku do lat 10.

Przykład: ransomware

Art. 291.

§ 1. Kto rzecz uzyskaną za pomocą czynu zabronionego nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 292.

§ 1. Kto rzecz, o której na podstawie towarzyszących okoliczności powinien i może przypuszczać, że została uzyskana za pomocą czynu zabronionego, nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art. 293.

§ 1. Przepisy art. 291 i 292 stosuje się odpowiednio do programu komputerowego.

– problem dla dostarczycieli przestrzeni dyskowej, chmury itp.

Ustawa o Policji

Art. 15.

1. Policjanci wykonując czynności, o których mowa w art. 14, mają prawo:

6) żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i jednostki obowiązane są, w zakresie swojego działania, do udzielenia tej pomocy, w zakresie obowiązujących przepisów prawa,

7) zwracania się o niezbędną pomoc do innych jednostek gospodarczych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa, w inny sposób.

Art. 20c.

1. Dane identyfikujące abonenta, zakończenia sieci lub urządzenia telekomunikacyjnego, między którymi wykonano połączenie oraz dane dotyczące uzyskania lub próby uzyskania połączenia między określonymi urządzeniami telekomunikacyjnymi lub zakończeniami sieci, a także okoliczności i rodzaj wykonywanego połączenia, mogą być ujawnione Policji oraz przetwarzane przez Policję - wyłącznie w celu zapobiegania lub wykrywania przestępstw.

2. Ujawnienie danych, o których mowa w ust. 1, następuje na:

1) pisemny wniosek Komendanta Głównego Policji lub komendanta wojewódzkiego

2) ustne żądanie policjanta posiadającego pisemne upoważnienie osób, o których mowa w pkt 1.

– telekomunikacja, śledzenie telefonów komórkowych

TRANSGRANICZNE ZASADY

Art. 109. **Ustawę karną polską stosuje się do obywatela polskiego, który popełnił przestępstwo za granicą.**

Art. 110. § 1. Ustawę karną polską stosuje się do cudzoziemca, który popełnił za granicą czyn zabroniony

skierowany przeciwko interesom Rzeczypospolitej Polskiej,

obywatela polskiego,

polskiej osoby prawnej

lub polskiej jednostki organizacyjnej niemającej osobowości prawnej

oraz do cudzoziemca, który popełnił za granicą przestępstwo o charakterze terrorystycznym.

§ 2. Ustawę karną polską stosuje się w razie popełnienia przez cudzoziemca za granicą czynu zabronionego innego niż wymieniony w § 1,

jeżeli czyn zabroniony jest w ustawie karnej polskiej zagrożony karą przekraczającą 2 lata pozbawienia wolności,

a sprawca przebywa na terytorium Rzeczypospolitej Polskiej i nie postanowiono go wydać.

Art. 111. § 1. Warunkiem odpowiedzialności za czyn popełniony za granicą jest uznanie takiego czynu za przestępstwo również przez ustawę obowiązującą w miejscu jego popełnienia.

§ 2. Jeżeli zachodzą różnice między ustawą polską, a ustawą obowiązującą w miejscu popełnienia czynu, stosując ustawę polską, sąd może uwzględnić te różnice na korzyść sprawcy.

§ 3. Warunek przewidziany w § 1 nie ma zastosowania do polskiego funkcjonariusza publicznego, który pełniąc służbę za granicą popełnił tam przestępstwo w związku z wykonywaniem swoich funkcji, ani do osoby, która popełniła przestępstwo w miejscu nie podlegającym żadnej władzy państwowej.

Art. 112. Niezależnie od przepisów obowiązujących w miejscu popełnienia czynu zabronionego, ustawę karną polską stosuje się do obywatela polskiego oraz cudzoziemca w razie popełnienia:

1) przestępstwa przeciwko bezpieczeństwu wewnętrznemu lub zewnętrznemu Rzeczypospolitej Polskiej,

2) przestępstwa przeciwko polskim urzędom lub funkcjonariuszom publicznym,

3) przestępstwa przeciwko istotnym polskim interesom gospodarczym,

4) przestępstwa fałszywych zeznań złożonych wobec urzędu polskiego,

5) przestępstwa, z którego została osiągnięta, chociażby pośrednio, korzyść majątkowa na terytorium Rzeczypospolitej Polskiej.

– czyli bardzo często można zastosować

Kodeks wykroczeń

Art. 107. Kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 1500 złotych albo karze nagany.

– ***spam nigeryjski, hejt,...***

Kodeks wykroczeń

Art. 66. § 1. Kto, chcąc wywołać niepotrzebną czynność, fałszywą informacją lub w inny sposób wprowadza w błąd instytucję użyteczności publicznej albo organ ochrony bezpieczeństwa, porządku publicznego lub zdrowia, podlega karze aresztu, ograniczenia wolności albo grzywny do 1500 zł.

§ 2. Jeżeli wykroczenie spowodowało niepotrzebną czynność, można orzec nawiązkę do wysokości 1000 złotych.

– można karać „żartownisiów”