Fundusze Europejskie

„Cyberbezpieczeństwo w zamówieniach publicznych”

Warszawa, 3 kwietnia 2025 r.

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Fundusze Europejskie

Aktualne trendy rozwoju cyberprzestępczości

Adam Klawikowski

prokurator delegowany do Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Fundusze Europejskie

Cechy specyficzne cyberprzestępczości

1.

Efekt asymetrii – o efekcie asymetrii decyduje takie postępowanie cyberprzestępców, które pozwala na uzyskanie rezultatów niewspółmiernie większych od poniesionych nakładów:

- **jednym działaniem** mogą osiągnąć niewspółmiernie **wiele rezultatów/skutków**,
- mogą działać bezpośrednio lub za pomocą **zautomatyzowanych systemów** lub oprogramowania,
- przestępstwa w cyberprzestrzeni mogą dotyczyć **bezpieczeństwa systemów** teleinformatycznych lub bezpieczeństwa **danych**.

Fundusze Europejskie

Cechy specyficzne cyberprzestępczości

2.

Anonimowość - w cyberprzestępczości to możliwość **ukrycia tożsamości** podczas popełniania przestępstw w sieci.

Anonimowość **utrudnia ściganie cyberprzestępców**, ale także może zachęcać do tego rodzaju działalności.

Fundusze Europejskie

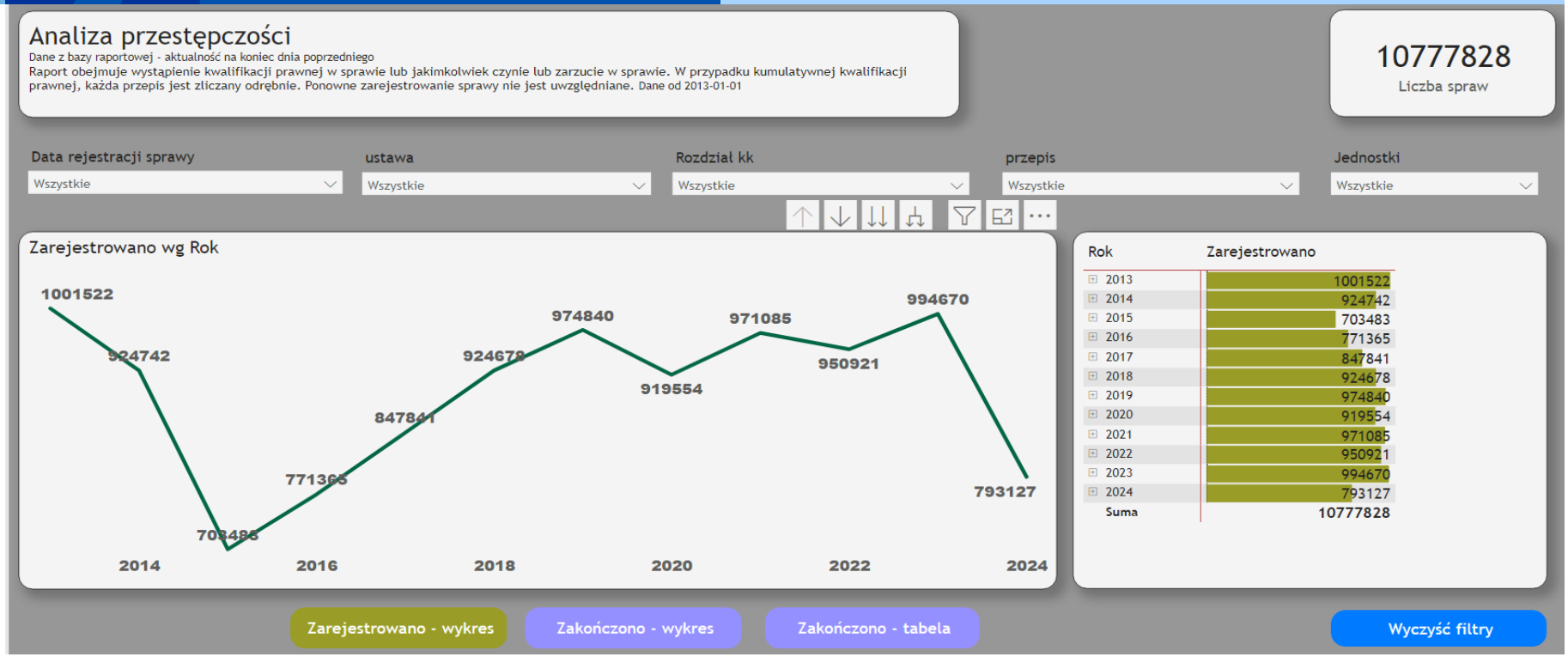
Cechy specyficzne cyberprzestępczości

3.

Transgraniczność - cyberprzestępczość często wykazuje cechy transgraniczne, co sprawia, że jest szczególnie **trudna do zwalczania** i wymaga **współpracy międzynarodowej** w dziedzinie prawa.

Fundusze Europejskie

Przestępczość w liczbach



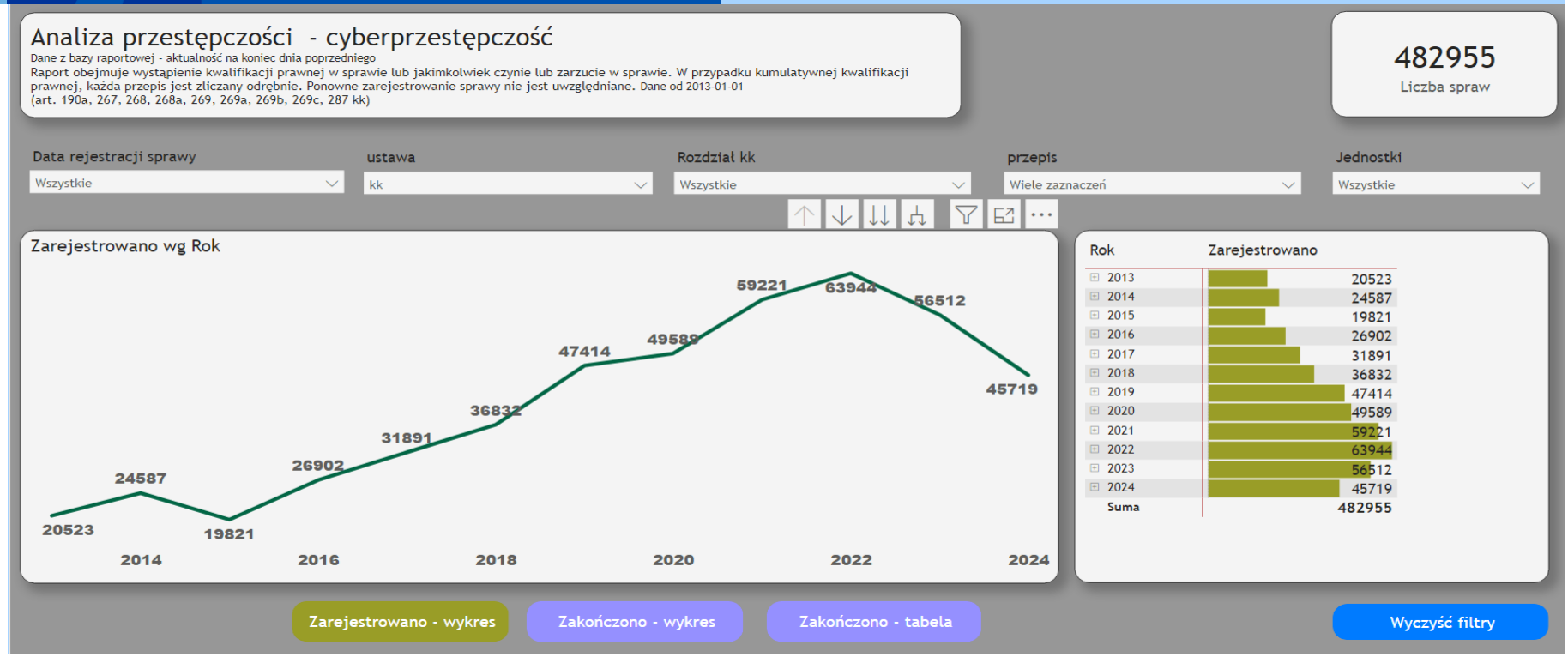
Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Fundusze Europejskie

Cyberprzestępczość w liczbach



Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

Fundusze Europejskie

Rodzaje ataków na bazy danych :

Ransomware

1

- to **złośliwe oprogramowanie**, które **blokuje dostęp** do danych lub systemu komputerowego i **żąda okupu** za ich przywrócenie.

Wektor ataku:
a) **Szyfruje dane** na urządzeniu
b) **Blokuje dostęp** do komputera lub urządzenia mobilnego,
c) **Żąda okupu** za odzyskanie kontroli nad zaatakowanym urządzeniem lub plikami

Fundusze Europejskie

Rodzaje ataków na bazy danych :

2

Ataki DDoS

- Ataki DDoS („**Distributed Denial of Service**”) stanowią trzecią najczęstszą formę cyberataków,
- Ataki te **uniemożliwiają działanie systemu,**
- Współczesne ataki DDoS potrafią **generować ruch** sieciowy przekraczający **1 Tbps.**

Fundusze Europejskie

Rodzaje ataków na bazy danych :

3

Malware

- **Złośliwe oprogramowanie** mające na celu uszkodzenia komputera bądź zniszczenia zapisanych na nim informacji,
- Malware **obejmuje wszystkie rodzaje** złośliwego oprogramowania.

Nieudostępnienie dokumentacji oraz kodów źródłowych systemu np. w toku postępowania o udzielenie zamówienia publicznego

Fundusze Europejskie

1. Jawność kodów źródłowych w bardzo dużym stopniu **zwiększa ryzyko przeprowadzania ataków** na taki system, który jest szczególnie istotny z punktu widzenia działalności danego podmiotu, niejednokrotnie bezpieczeństwa państwa oraz interesu prywatnego wszystkich osób, podlegających rejestracji w takim systemie,
2. W systemie gromadzone są dane dotyczące **dużej ilości obywateli**, w tym **dane wrażliwe**.
3. Każdy system podmiotu publicznego jest **szczególnie narażony na ataki podmiotów zainteresowanych zakłóceniem jego działania**, ujawnieniem danych w nim zgromadzonych lub manipulacją treściami przechowanymi w systemie.

Fundusze Europejskie

Konsekwencje włamania do systemu

1.

naruszenie dostępności i **ciągłości działania** systemu

2.

naruszenie **poufności danych**

3.

naruszenie **integralności danych**

4.

godzi w **bezpieczeństwo publiczne** oraz **osób**, których dane mogłyby zostać ujawnione

Fundusze Europejskie

Inne rodzaje cyberprzestępstw:

4. Fałszywe sklepy internetowe - za pośrednictwem łudząco podobnych do oficjalnych stron internetowych sklepów lub nowych podmiotów, przestępcy oferują produkty po bardzo atrakcyjnych cenach, po dokonaniu płatności za towary, kontakt z klientem się urywa, zaś strona internetowa najczęściej przestaje działać.

5. Oszustwa inwestycyjne - za pośrednictwem reklam w intrenecie lub mediach społecznościowych lub specjalnie do tego przygotowanych stron internetowych oraz socjotechniki, oferowane są usługi w produkty inwestycyjne, po transferze środków pieniężnych przez potencjalnego inwestora/pokrzywdzonego w celu dokonania inwestycji, przestępcy przestają się z nim kontaktować.

Fundusze Europejskie

6. Oszustwo typu „Business Email Compromise”

1. Przestępca kieruje wiadomość e-mail do **zespołu płatności** w danym podmiocie, podając się za **kontrahenta, dostawcę, wierzyciela**, a nawet **członka dyrekcji**. Odbiorca może odnieść wrażenie, że pisze do niego przedstawiciel podmiotu z prośbą o **pilną płatność**, albo dostawca podaje **nowy numer rachunku**, na który należy dokonywać dalszych przelewów. Często odbiorca jest proszony poprzez wiadomość e-mail o **nieomawianie tej sprawy** z innymi osobami.

2. Ponieważ e-mail nadawcy jest **bardzo podobny** do znanego adresu, ten rodzaj oszustwa często pozostaje niezauważony, dopóki nie dojdzie do transferu środków pieniężnych i weryfikacji danych kontaktowych. Cyberprzestępcy mogą również **włamać się na prawdziwe konto** poczty elektronicznej.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Fundusze Europejskie

źródło: Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) (**ARTIFICIAL INTELLIGENCE ACT**) – **art. 3**

1) „system AI” oznacza **system maszynowy**, który został zaprojektowany do działania z różnym **poziomem autonomii** po jego wdrożeniu oraz który może wykazywać **zdolność adaptacji** po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – **wnioskuje**, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne;

AI

Fundusze Europejskie

Rozważając cyberprzestępczość w kontekście sztucznej inteligencji, należy wziąć pod uwagę następujące kwestie:

1. Sztuczna inteligencja może być wykorzystywana jako **narzędzie w rękach sprawców** czyli jako **środek wspomagający cyberprzestępczość i ułatwiający popełnienie przestępstw,**

2. Sztuczna inteligencja może być również wykorzystywana do:

- **poprawy cyberbezpieczeństwa** (filtrowanie ruchu),
- **przeciwdziałania cyberprzestępczości** (zautomatyzowana analiza kryminalistyczna).

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

AI

Fundusze Europejskie

W przypadku bezpośredniego **wykorzystywania systemu sztucznej inteligencji w celu popełnienia czynu zabronionego** odpowiedzialność winien ponieść **sprawca czynu**, zgodnie z treścią art. 1 § 1 k.k.

Art. 1. § 1. k.k. Odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia.

Problem pojawia się w przypadku wyrządzenia szkody, np. nieumyślnie lub wyłącznie przez **autonomiczny system**, który podlega bądź nie podlega czyjejś kontroli.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

A I

Fundusze Europejskie

Gardocki L., Prawo karne, C.H. Beck 2019, s. 51-55, 60-63, Królikowski M., Zawłocki R. (red.), Kodeks karny. Część ogólna. Tom I. Komentarz do art. 1-31, C.H. Beck, 2017, s. 202-208, 221-225.

Pojęcie czynu, które w polskim prawie karnym jest pojęciem fundamentalnym i oznacza **zachowanie człowieka**, które może podlegać **ocenie prawnej** i **ewentualnej odpowiedzialności karnej**.

Zgodnie z kodeksem karnym, aby dane zachowanie zostało uznane za czyn, musi spełniać następujące warunki:

1. **musi być zachowaniem człowieka** - tylko osoba fizyczna może popełnić czyn w rozumieniu prawa karnego.
2. **musi być zachowaniem zewnętrznym** - sama myśl, postanowienie lub wewnętrzne przeżycie nie stanowi czynu.
3. musi być **zachowaniem** dowolnym (**zależnym od woli człowieka**) - zachowania niezależne od woli, takie jak odruchy lub czynności podejmowane pod wpływem przymusu fizycznego, nie są czynami.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

A I

Fundusze Europejskie

Art. 9. k.k. [Strona podmiotowa czynu. Umyślność i nieumyślność]

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

AI

Fundusze Europejskie

https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

1. **Złośliwe oprogramowanie AI – tworzenie malware.**

Wykorzystanie sztucznej inteligencji do **poprawy skuteczności** złośliwego oprogramowania.

Sztuczna inteligencja może być wykorzystywana do tworzenia złośliwego oprogramowania – takiego, które **nieustannie zmienia swój kod**, aby **uniknąć wykrycia**.

Oprogramowanie stworzone przez AI może być zaprojektowane tak, aby **modyfikować się w czasie rzeczywistym**, co sprawia, że tradycyjne środki bezpieczeństwa niemal nie są w stanie go zidentyfikować i zneutralizować.

AI

Fundusze Europejskie

https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

2. Phishing, jeden z typów ataków opartych o wiadomości e-mail lub SMS.

Zastosowanie sztucznej inteligencji, w tego typu cyberatakach polega na stworzeniu **wysoce przekonujących** wiadomości phishingowych.

Modele sztucznej inteligencji mogą tworzyć/generować wiadomości e-mail, które **naśladują** ton, styl, **język rzeczywistej komunikacji**.

Generowane w ten sposób wiadomości są często **pozbawione typowych błędów**, które umożliwiały wykrycie ataku phishingowego.

Zastosowanie sztucznej inteligencji znacznie utrudnia identyfikację takich zachowań jako oszustwa.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

AI

Fundusze Europejskie

https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

3. Generowanie fałszywych stron Internetowych.
4. Automatyzacja ataków socjotechnicznych.

Strony internetowe generowane przez sztuczną inteligencję oraz fałszywe recenzje produktów i usług mogą **wprowadzić w błąd** konsumentów, by zaufali oni i dokonali transakcji z podmiotami zarządzanymi przez przestępców.

5. Odgadywanie haseł wspomagane przez AI.

Dzięki wykorzystaniu sztucznej inteligencji istnieje możliwość prowadzenia tego rodzaju działań w sposób **bardziej ukierunkowany**, **szybszy** i **skuteczniejszy**, niż dotychczas.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

AI

Fundusze Europejskie

https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

6. Łamanie CAPTCHA (internetowy system identyfikacji użytkownika) **wspierane przez AI.**

Obrazy CAPTCHA są powszechnie używane na stronach internetowych, aby udaremnić próby użytkowników/przestępców, którzy próbują **nadużywać usługi sieciowe**, np. tworzenie nowych kont lub dodawanie nowych komentarzy lub odpowiedzi na forach internetowych.

Aktualnie opracowywane są systemy z wykorzystaniem sztucznej inteligencji, których zadaniem jest podjęcie **prób złamania obrazów CAPTCHA**, aby zautomatyzować nadużywanie usług sieciowych.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

A I

Fundusze Europejskie

W prawie karnym do **przestępstw komputerowych** zalicza się w szczególności czyny z :

- art. 267 § 1 i 2 k.k. – nielegalne uzyskanie informacji,
- art. 268 § 2 k.k. – niszczenie informacji,
- art. 268a k.k. – szkoda w bazach danych,
- art. 269 § 1 i 2 k.k. – sabotaż komputerowy,
- art. 269a k.k. – zakłócenie pracy sieci,
- art. 269b k.k. – bezprawne wykorzystanie programów i danych,
- a także art. 287 k.k., czyli oszustwo komputerowe.

Niemalże wszystkie dotyczą **automatycznego przetwarzania**, a także **naruszenia danych informatycznych**.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Fundusze Europejskie

DEEP FAKE

źródło: Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) (**ARTIFICIAL INTELLIGENCE ACT**) – **art. 3**

60) „deepfake” oznacza wygenerowane przez AI lub **zmanipulowane** przez AI **obrazy**, treści **dźwiękowe** lub treści **wideo**, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe;

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Zgodnie z **art. 52 § 3** Rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji użytkownicy systemu sztucznej inteligencji *deep fake* są zobowiązani do **ujawniania w odpowiedni, terminowy, jasny i widoczny sposób, że treść została sztucznie wygenerowana lub zmanipulowana**, a także w miarę możliwości **imię i nazwisko osoby fizycznej lub prawnej, która ją wygenerowała lub zmanipulowała**. Ujawnianie oznacza umieszczenie w takim wytworze typu *deep fake* wyraźnej i widocznej dla odbiorcy **informacji**, że treść jest **nieautentyczna**.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Ogólnie należy przyjąć, że **deep fake** to technologia wykorzystująca sztuczną inteligencję do tworzenia lub edytowania treści wideo albo obrazu w celu pokazania czegoś, co nigdy się nie wydarzyło. (*N. Young, Deep Fake Technology: Complete Guide to Deepfakes, Politics and Social Media, New York 2019, s. 14.*)

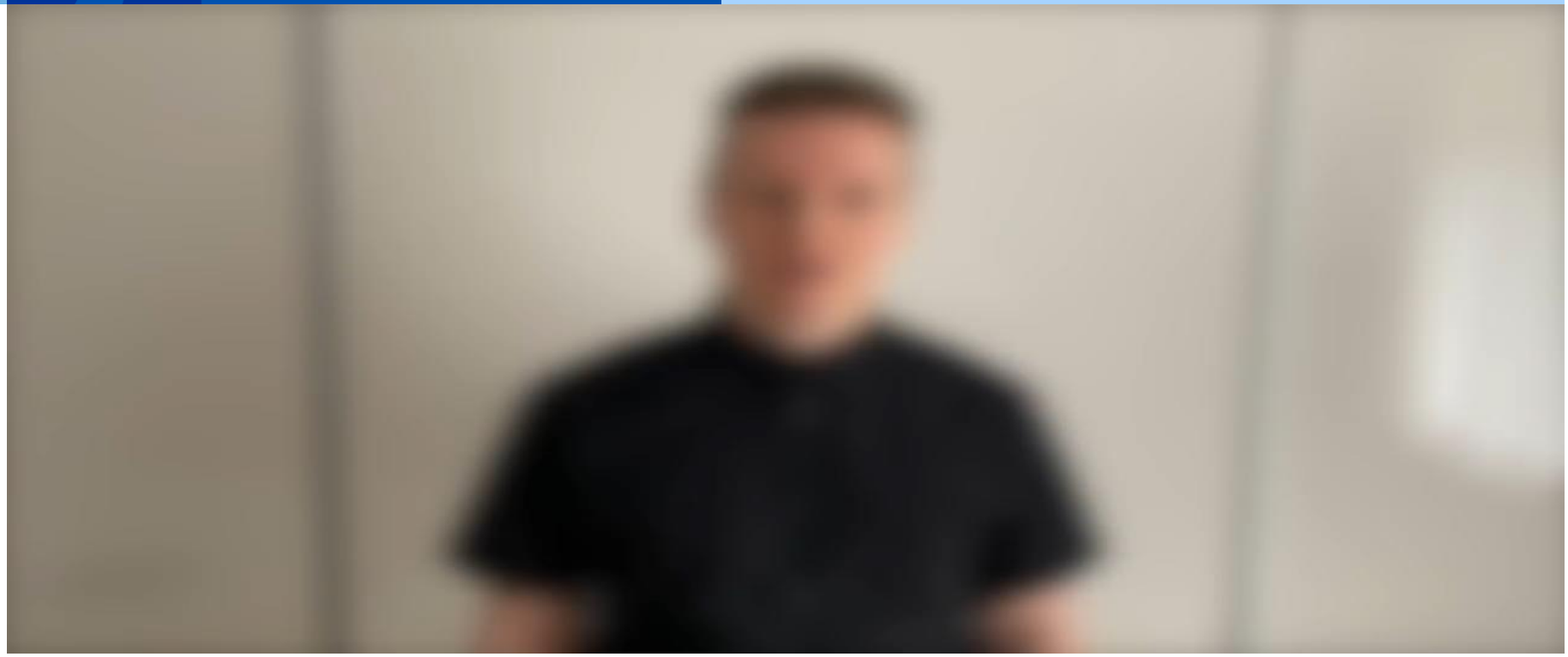
Postęp techniczny i technologiczny w ostatnich latach sprawił, że tworzenie deep fake'ów jest jeszcze łatwiejsze i szybsze, a otrzymane rezultaty bardziej realistyczne.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

https://www.youtube.com/watch?v=mUfJOQKdtAk



Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Przechodząc do prawnego punktu widzenia, można wskazać, że deep fakes to informacje niezgodne z prawdą, tym samym ich karalność nastąpi wszędzie tam, gdzie **prawo karne penalizuje fałszowanie rzeczywistości** (*K. Mamak, Prawnokarne sposoby walki z fake newsami. RAPORT PROJEKTU SPOŁ-TECH,2020,s.34, file:///C:/Users/ASUS/OneDrive/Desktop/phd/DEEPFAKE/Raport_walka-zfake-newsami%20MAMAK.pdf (2.06.2023).*)

Przykładowe kwalifikacje prawne przestępstw: art. 286 § 1 k.k., art. 190a § 2 k.k., art. 224a k.k., art. 212 § 1 k.k., art. 216 § 1 k.k., art. 132 k.k. oraz art. 135 § 2 k.k.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 286 § 1 k.k. – oszustwo - skierowane na osobę, którą sprawca zamierza doprowadzić do niekorzystnego rozporządzenia mieniem, i może przybierać trojaką postać: wprowadzenia w błąd tej osoby, wyzyskania błędu tej osoby, wyzyskania niezdolności tej osoby do należytego pojmowania przedsiębranego działania.

Wprowadzenie w błąd może przejawiać się w **najrozmaitszych formach**: przykładem takiego zachowania może być również **wykorzystanie technologii deep fake** w reklamie przy oszustwach na pozagiełdowym rynku forex, w celu nakłonienia do zainwestowania posiadanych środków pieniężnych przez inwestora/pokrzywdzonego.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 190a § 2 k.k. – kradzież tożsamości - czyn ten polega na wykorzystaniu przy podszywaniu się pod inną osobę jej wizerunku, innych danych osobowych lub innych danych, za pomocą których jest publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej

W doktrynie przyjmuje się, iż **wizerunek** oznacza „dostrzegalne, fizyczne cechy człowieka, tworzące jego wygląd i pozwalające na identyfikację osoby wśród innych ludzi" *(E. Wojnicka, Prawo do wizerunku w ustawodawstwie polskim, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej" 1990, z. 56, s. 107.)*

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 190a § 2 k.k. – kradzież tożsamości

W szerokim znaczeniu „w tym pojęciu mieści się nie tylko obraz fizyczny (**obraz wizualny**), lecz również głos (**wizerunek dźwięczny**). Są nimi również objęte wszystkie elementy identyfikujące daną jednostkę jako konkretną osobę fizyczną" *(J. Sieńczyło-Chlabicz, Przedmiot, podmiot i charakter prawa do wizerunku, „Przegląd Ustawodawstwa Gospodarczego" 2003, nr 8, s. 20.)*

Podszywanie się pod inną osobę to **wprowadzenie w błąd** osób trzecich co do swojej tożsamości, **podawanie się za kogoś innego**. *(J. Lachowski, art. 190a [w:] Kodeks karny. Komentarz, red. V. Konarska-Wrzosek, LEX 2020, teza 9.)* Podszywanie się to podejmowanie **działań jako inna osoba** (*A. Zoll, art. 190a [w:] Kodeks karny. Część szczególna, t. II, cz. 1: Komentarz do art. 117–211a, red. W. Wróbel, A. Zoll, LEX 2017, teza 9.*

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 190a § 2 k.k. – kradzież tożsamości

Uzyskanie fałszywej tożsamości może mieć miejsce na trzy sposoby:

1)przez **stworzenie fikcyjnej tożsamości**;
2)przez **modyfikację swojej własnej tożsamości**;
3)przez **kradzież lub przywłaszczenie istniejącej wcześniej tożsamości**, co może być połączone z jej późniejszą modyfikacją.

Więcej: A. Gryszczyńska, Kradzieże tożsamości w sprawach z zakresu cyberprzestępczości, [w:] Rocznik Bezpieczeństwa Morskiego, Przestępczość Teleinformatyczna 2019, red. J. Kosiński, G. Krasnodębski, Gdynia 2020, s. 207-227, ISSN 1898-3189

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 224a k.k. – wprowadzenie w błąd instytucji użyteczności publicznej – fałszywy alarm : przestępstwo to ma **charakter skutkowy** polegający na tym, iż w wyniku jego popełnienia instytucja wskazana w treści przedmiotowego przepisu podejmuje działania mające na celu uchylenie nieistniejącego w rzeczywistości zagrożenia *(M. Kulik, komentarz do art. 224a [w:] Kodeks karny. Komentarz aktualizowany, red. M. Mozgawa, Warszawa 2020, teza 5.)*

Przestępstwo z art. 224a k.k. sprawca może popełnić, wyłącznie działając **umyślnie z zamiarem bezpośrednim** *(J. Lachowski, komentarz do art. 224a [w:] Kodeks karny. Część szczególna. Komentarz, t. II: Art. 222–316, red. M. Królikowski, R. Zawłocki, Warszawa 2017, s. 56.)*

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 212 k.k. – zniesławienie - przestępstwo to, może obejmować więc różne rodzaje deep fake'ów, dotyczących **nie tylko osób fizycznych**, ale także **instytucji**. Deep fake w formie zniesławienia to informacja, która przypisuje ofierze negatywnie oceniane właściwości czy postępowanie, co może ją narazić na poniżenie w opinii publicznej czy utratę zaufania *(K. Mamak, Prawnokarne sposoby..., s. 22.)*

W przypadku przedstawienia konkretnej osoby czy instytucji w złym świetle, technologia deep fake może istotnie przyczynić się do **pogorszenia** lub **zniszczenia jej reputacji i renomy** oraz **wpłynąć negatywnie na jej funkcjonowanie** (w przypadku instytucji) jak też **odbiór społeczny**.

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

DEEPFAKE

Fundusze Europejskie

Art. 216 k.k. – zniewaga – przedmiotem ochrony jest cześć wewnętrzna (podmiotowa), czyli godność. Chroniona jest godność każdej osoby fizycznej, bez względu na jej płeć, wiek, status społeczny czy pochodzenie (Marek, Komentarz, s. 486).

Przykładem zachowania, które mogłoby wypełnić znamiona omawianego przepisu, jest **stworzenie filmu wideo**, na którym wykreowana postać z twarzą prawdziwej osoby zachowuje się w sposób **obiektywnie uznany społecznie za niewłaściwy**.

DEEPFAKE

Fundusze Europejskie

Art. 216 k.k. – zniewaga – formy:

W przypadku publicznego znieważenia grupy ludności lub poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości w grę wchodzi przepis **art. 257 k.k.**;
Jak również **art. 135 § 2 k.k.** (znieważenie Prezydenta RP),
art. 136 § 3 k.k. (znieważenie głowy obcego państwa).

Fundusze Europejskie

Przykłady wykorzystania technologii

DEEP FAKE

Przykład 1

źródło: https://cebrf.knf.gov.pl/deepfake

Fundusze Europejskie

Przykłady wykorzystania technologii

DEEP FAKE

Przykład 2

źródło: https://cebrf.knf.gov.pl/deepfake

Fundusze Europejskie
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

Fundusze Europejskie

Dziękuję

za uwagę.

Adam Klawikowski

Fundusze Europejskie

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską