Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# PANEL POSTEROWY

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

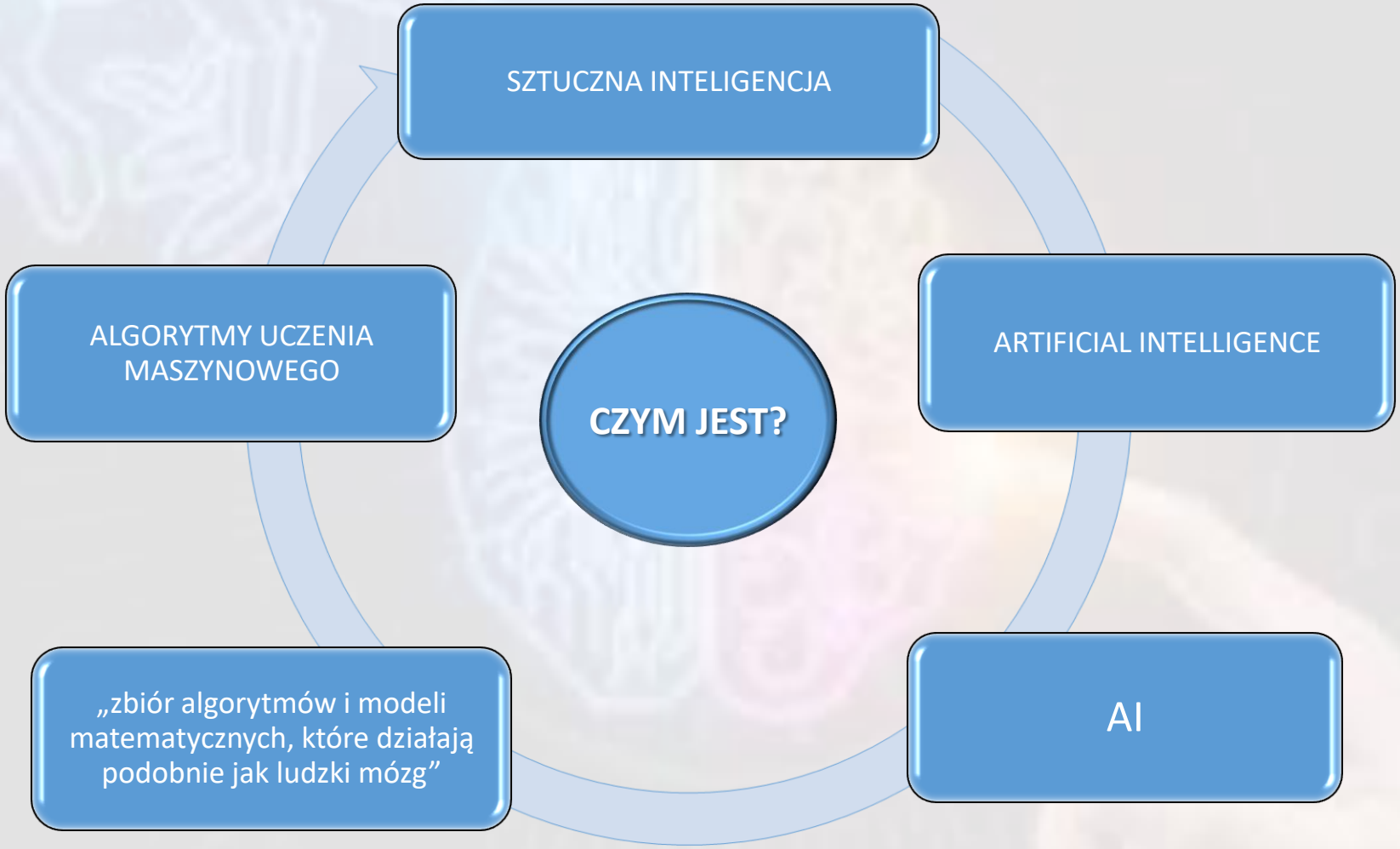
***w systemie bezpieczeństwa informacyjnego***

# Sztuczna inteligencja a bezpieczeństwo informacyjne

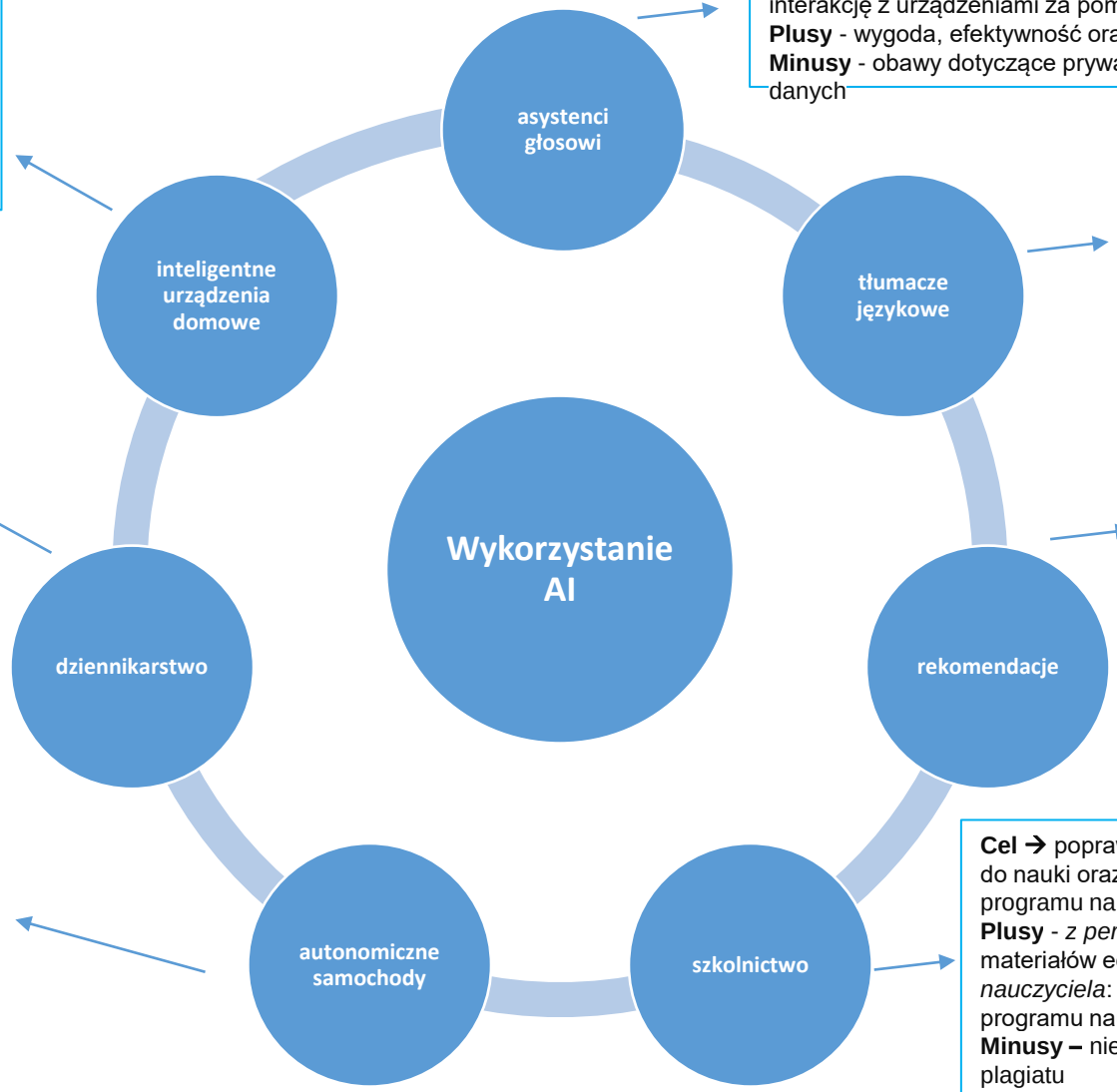
Adriana Dróżdż, adriana.drozdz@uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

Adriana Dróżdż



Adriana Dróżdż




**Cel** → automatyzacja codziennych zadań w domu, takich jak m.in. sterowanie oświetleniem, ogrzewaniem czy monitorowanie bezpieczeństwa
**Plusy** - wygoda, oszczędność czasu i energii, a także potencjał zwiększenia efektywności i komfortu życia
**Minusy** - obawy dotyczące prywatności, bezpieczeństwa danych oraz potencjalne zależności od technologii, której awaria może zakłócić codzienne funkcjonowanie

**Cel** → zastosowanie w wielu dziedzinach, umożliwiając interakcję z urządzeniami za pomocą głosu
**Plusy** - wygoda, efektywność oraz personalizacja usług
**Minusy** - obawy dotyczące prywatności i bezpieczeństwa danych

**Cel** → szybkie i skuteczne tłumaczenie tekstów między różnymi językami
**Plusy** - ułatwiają komunikację między ludźmi o różnych językach oraz wspierają globalną wymianę informacji i kulturę
**Minusy** - błędy w tłumaczeniach oraz braki w interpretacji kontekstu, co może prowadzić do nieporozumień

**Cel** → automatyzacja procesów pisania artykułów, analizę danych, personalizację treści oraz fakt-checking
**Plusy** - szybsze tworzenie treści, lepsze wykorzystanie danych oraz poprawę efektywności
**Minusy** - obawy o jakość informacji, utratę pracy dla dziennikarzy oraz potencjalne błędy w interpretacji danych przez algorytmy

**Cel** → rekomendacja produktów, filmów, muzyki oraz innych treści na podstawie analizy preferencji użytkowników i danych o ich zachowaniach
**Plusy** - pozwala użytkownikom odkrywać nowe treści i produkty, które mogą ich zainteresować, co z kolei może zwiększyć satysfakcję z użytkowania platform
**Minusy** - ryzyko filtracji informacji, utrata różnorodności w dostępie do treści, nadmierna personalizacja, brak przejrzystości (użytkownicy nie są w pełni świadomi, jakie czynniki wpływają na sugestie, co może budzić nieufność i obawy), wykorzystywanie algorytmów przez firmy do manipulowania zachowaniami użytkowników w celu zwiększenia zysków, co może prowadzić do wykorzystywania danych użytkowników w sposób nieetyczny

**Cel** → analiza danych z sensorów, planowania trasy oraz podejmowanie decyzji na drodze
**Plusy** - zwiększenie bezpieczeństwa na drodze poprzez eliminację ludzkich błędów, zmniejszenie liczby wypadków oraz optymalizacja przepływu ruchu
**Minusy** – redukcja miejsc pracy w sektorze transportu, wyzwania etyczne (zderzenie z innym pojazdem a potencjalne narażenie życia innych pasażerów), brak pewności co do niezawodności (awarie techniczne, błędy w działaniu algorytmów), potencjalne zagrożenia dla prywatności (gromadzenie danych o podróżach)

**Cel** → poprawa procesu nauczania poprzez spersonalizowane podejście do nauki oraz lepsze zrozumienie potrzeb uczniów i dostosowanie programu nauczania, wsparcie nauczycieli
**Plusy** - *z perspektywy ucznia*: ułatwienie dostępu do różnorodnych materiałów edukacyjnych, interaktywne narzędzia, *z perspektywy nauczyciela*: analiza danych dot. postępów uczniów, dostosowywanie programu nauczania, poprawienie efektywności nauczania
**Minusy –** niesamodzielne prace, co może prowadzić do przypadków plagiatu
i utraty autentyczności

Adriana Dróżdż

# Sztuczna inteligencja oferuje wiele korzyści, ale wiąże się także z wyzwaniami i ryzykiem, które wymagają uwagi i odpowiedniego zarządzania, aby wykorzystać jej potencjał w sposób korzystny dla społeczeństwa.

## PLUSY

**1.Automatyzacja i efektywność**: Sztuczna inteligencja może przyspieszyć i ułatwić wiele procesów, poprawiając wydajność i oszczędzając czas.

**2.Personalizacja**: Może dostosowywać się do indywidualnych preferencji i potrzeb użytkowników, zapewniając spersonalizowane doświadczenia.

**3.Postęp technologiczny:** Rozwój sztucznej inteligencji przynosi innowacje w różnych dziedzinach, takich jak medycyna, edukacja czy transport.

**4.Rozwiązanie problemów złożonych:** Sztuczna inteligencja może pomagać w rozwiązywaniu skomplikowanych problemów naukowych, technicznych i społecznych.

## MINUSY

**1.Prywatność i bezpieczeństwo danych:** Istnieją obawy dotyczące prywatności danych oraz ryzyka ich nadużyć lub wycieku.

**2.Bezrobocie:** Automatyzacja za pomocą sztucznej inteligencji może prowadzić do utraty miejsc pracy w niektórych sektorach.

**3.Uzależnienie od technologii:** Nadmierne poleganie na sztucznej inteligencji może prowadzić do utraty umiejętności ludzkich i zależności od technologii.

**4.Błędy i uprzedzenia**: Algorytmy sztucznej inteligencji mogą generować błędne lub uprzedzone wyniki, co może prowadzić do niesprawiedliwych decyzji i konsekwencji społecznych.

Adriana Dróżdż

## WPROWADZENIE

- Sztuczna inteligencja (SI) staje się integralną częścią dzisiejszego świata, znacząco wpływając na różne aspekty życia społecznego, gospodarczego i technologicznego. W obliczu tego dynamicznego postępu technologicznego, należy podkreślić pilną potrzebę zrozumienia oraz adaptacji do wyzwań i możliwości wynikających z integracji SI w różnych dziedzinach życia. Zrozumienie tego zjawiska wymaga holistycznego podejścia, uwzględniającego zarówno aspekty technologiczne, jak i społeczne, oraz konieczność świadomego zarządzania wpływem SI na społeczeństwo.

## BEZPIECZEŃSTWO INFORMACYJNE

- Jednym z obszarów, w którym SI ma coraz większe znaczenie, jest bezpieczeństwo informacyjne. Wraz z rosnącą ilością danych generowanych i przetwarzanych przez organizacje, wzrasta również potrzeba skutecznych narzędzi i strategii zapewniających ochronę tych danych przed zagrożeniami cybernetycznymi. W obliczu coraz bardziej zaawansowanych ataków cybernetycznych oraz coraz bardziej wyrafinowanych technik hakerów, kluczowym wyzwaniem staje się skuteczne wykorzystanie SI do wykrywania, zapobiegania i reagowania na zagrożenia w szybko zmieniającym się krajobrazie cyberbezpieczeństwa. W związku z tym konieczne jest nie tylko opracowanie nowoczesnych technologii, ale także ciągłe doskonalenie metod i procesów związanych z bezpieczeństwem informacyjnym, aby sprostać coraz bardziej wymagającym wyzwaniom.

Adriana Dróżdż

BEZPIECZEŃSTWO INFORMACYJNE

## Szanse wynikające z wykorzystania sztucznej inteligencji:

- Jedną z głównych szans wynikających z wykorzystania SI w bezpieczeństwie informacyjnym jest możliwość automatyzacji procesów zabezpieczeń. Algorytmy uczenia maszynowego mogą analizować ogromne ilości danych w czasie rzeczywistym, umożliwiając szybkie wykrywanie nieprawidłowości i podejrzanych zachowań w systemach informatycznych.
- Ponadto, SI może być wykorzystywana do ulepszania systemów wykrywania oszustw, poprzez identyfikację podejrzanych transakcji finansowych lub nieautoryzowanego dostępu do systemów.
- SI umożliwia także szybką analizę dużej ilości danych w celu identyfikacji wzorców i tendencji, co pomaga w szybkim reagowaniu na pojawiające się zagrożenia.

## Zagrożenia wynikające z wykorzystania sztucznej inteligencji:

- Jednym z głównych zagrożeń związanych z wykorzystaniem SI w bezpieczeństwie informacyjnym jest ryzyko ataków z wykorzystaniem tej samej technologii. Cyberprzestępcy mogą wykorzystywać algorytmy SI do generowania bardziej wyrafinowanych ataków, które są trudniejsze do wykrycia i zwalczania.
- Ponadto, istnieje ryzyko manipulacji danych, gdzie algorytmy SI mogą być wykorzystywane do wprowadzania błędnych informacji do systemów informatycznych, co może prowadzić do poważnych konsekwencji, takich jak utrata poufności danych czy fałszywe interpretacje danych.
- SI może także prowadzić do nadmiernego zbierania i analizy danych, co rodzi obawy dotyczące prywatności i nadużyć danych.

## KONKLUZJE

- Istotnym jest na wskazanie potencjału SI do poprawy skuteczności systemów zabezpieczeń, jednocześnie podkreślając konieczność świadomego zarządzania ryzykiem związanym z jej wykorzystaniem.
- Należy pamiętać, że generowane dane z wykorzystaniem SI mogą być nieprawdziwe, a ich celem potencjalnie jest usatysfakcjonowanie odbiorcy faktem uzyskania odpowiedzi na postawione pytanie zamiast nieudzielenia odpowiedzi, z uwagi na brak rzetelnych informacji.
- Warto zauważyć, że choć korzystanie z systemów SI może być korzystne, ich użytkowanie może również niesie ze sobą pewne niebezpieczeństwa oraz skutki uboczne, w tym takie, które mogą być trudne do przewidzenia, rozpoznania lub oceny (np. wpływ na demokrację, sprawiedliwość i równość lub efekty na ludzki umysł).
- Niezbędne są dalsze badania nad metodami wykorzystania SI w celu zwiększenia odporności systemów informatycznych na zagrożenia cybernetyczne, przy jednoczesnym uwzględnieniu etycznych i prawnych aspektów związanych z prywatnością danych.
- Kluczowym aspektem w stosowaniu systemów sztucznej inteligencji jest zaangażowanie społeczeństwa poprzez edukację i uczestnictwo w szkoleniach. Ma to na celu zapewnienie, że wszyscy użytkownicy SI posiadają pełną wiedzę na temat rzetelnej sztucznej inteligencji oraz są świadomi różnorodnych zagrożeń i możliwości związanych z jej użyciem. Niewiedza i brak świadomości mogą prowadzić do rozpowszechniania dezinformacji, co stwarza ryzyko dla społeczeństwa. Niestety, nie każdy będzie zdeterminowany w poszukiwaniu prawdziwych informacji, a niektórzy mogą łatwo dać się zwieść przez fałszywe treści generowane przez sztuczną inteligencję, które obejmują nie tylko fałszywe cytaty i obrazy, ale także manipulacyjne artykuły mające na celu wywołanie chaosu w społeczeństwie. W związku z tym konieczne jest podkreślenie znaczenia edukacji i świadomości społecznej w kontekście sztucznej inteligencji.

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Ochrona praw autorskich jak element bezpieczeństwa informacyjnego

Petro Beizel,
pb88470@stud.uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Wprowadzenie

- W dzisiejszym społeczeństwie informacyjnym, gdzie treści cyfrowe są łatwo dostępne i łatwo reprodukowalne, ochrona praw autorskich staje się niezwykle istotnym elementem bezpieczeństwa informacyjnego. Prawa autorskie stanowią fundament dla zachęcania do tworzenia nowych treści oraz zapewniają sprawiedliwe wynagrodzenie dla twórców za ich pracę intelektualną. Jednakże, w erze cyfrowej, ich egzekwowanie staje się coraz bardziej skomplikowane ze względu na łatwość kopiowania i dystrybucji treści w internecie.
- W tej prezentacji przyjrzymy się bliżej istocie praw autorskich, ich ewolucji w kontekście cyfrowym oraz wyzwaniom, jakie stawiają przed nami nowe technologie. Dowiemy się, jakie narzędzia i strategie można zastosować, aby skutecznie chronić prawa autorskie w świecie zdominowanym przez przepływ informacji. Ochrona praw autorskich nie tylko chroni interesy twórców, ale także wpływa na kulturę organizacyjną, innowacyjność oraz rozwój gospodarczy.

# Prawa autorskie: Podstawy

Prawa autorskie stanowią podstawowy fundament ochrony własności intelektualnej, zapewniając autorom kontrolę nad wykorzystaniem ich twórczości oraz możliwość uzyskania korzyści finansowych z jej eksploatacji. Kluczowe aspekty praw autorskich:

- Historia i geneza praw autorskich: Prawa autorskie mają długą historię, sięgającą czasów starożytnych, kiedy to rzemieślnicy i artyści otrzymywali ochronę swoich dzieł poprzez przywileje królewskie. Obecnie prawo autorskie jest regulowane przez międzynarodowe umowy i krajowe przepisy, które określają prawa i obowiązki autorów oraz korzystających z ich dzieł.
- Zakres ochrony praw autorskich: Prawa autorskie obejmują szeroki zakres dzieł twórczych, takich jak literatura, muzyka, filmy, fotografie, programy komputerowe oraz inne wytwory o charakterze artystycznym i intelektualnym. Chronią one nie tylko sam fakt tworzenia dzieła, ale również sposób jego wyrażenia oraz wszelkie przekształcenia i reprodukcje.
- Prawa autorskie a własność intelektualna: Prawa autorskie są częścią szerszego spektrum własności intelektualnej, które obejmuje także patenty, znaki towarowe i wzory przemysłowe. W odróżnieniu od niektórych innych form własności intelektualnej, prawa autorskie nie wymagają rejestracji - wystarczy, że dzieło zostanie wyrażone w jakiejkolwiek formie materialnej.

## Wyzwania dla praw autorskich w erze cyfrowej

- W erze cyfrowej prawa autorskie stoją przed wieloma wyzwaniami. Jednym z głównych problemów jest łatwość kopiowania i dystrybucji treści, co prowadzi do rozpowszechniania piractwa oraz trudności w identyfikacji i ściganiu piratów. To z kolei wpływa na tradycyjne modele biznesowe, zmuszając twórców do poszukiwania nowych sposobów zarabiania na swoich dziełach. Jednakże, istnieje również dyskusja na temat równowagi między ochroną praw autorskich a swobodnym dostępem do wiedzy i kultury. Rozwój technologii cyfrowych, takich jak sztuczna inteligencja czy blockchain, dodatkowo komplikuje krajobraz, otwierając zarówno nowe możliwości naruszania, jak i ochrony praw autorskich. Wobec tych wyzwań konieczne jest ciągłe doskonalenie prawa autorskiego oraz opracowanie innowacyjnych rozwiązań, które umożliwią zachowanie równowagi między interesami twórców a potrzebami społeczeństwa.

# Implementacja ochrony praw autorskich w praktyce

Wdrożenie skutecznej ochrony praw autorskich wymaga zastosowania różnorodnych strategii i narzędzi, aby zapewnić ochronę twórców oraz ich dzieł. Kluczowe aspekty implementacji ochrony praw autorskich:

- Polityki korporacyjne dotyczące praw autorskich: Opracowanie jasnych i precyzyjnych polityk dotyczących praw autorskich, które określają prawa i obowiązki pracowników w zakresie korzystania z chronionych materiałów.
- Edukacja pracowników: Organizacja szkoleń i spotkań, aby zwiększyć świadomość pracowników na temat praw autorskich i konsekwencji ich naruszeń.
- Umowy licencyjne i prawa autorskie: Wykorzystanie umów licencyjnych do uregulowania sposobu wykorzystania dzieł przez inne podmioty.
- Monitorowanie i egzekwowanie praw autorskich: Regularne monitorowanie sieci w celu wykrywania naruszeń praw autorskich oraz podejmowanie działań egzekwujących te prawa, takich jak wysyłanie powiadomień o naruszeniach czy dochodzenie prawne.
- Współpraca z instytucjami i organizacjami: Współpraca z instytucjami rządowymi, organizacjami pozarządowymi oraz organizacjami zbiorowego zarządzania prawami autorskimi w celu wzmocnienia ochrony praw autorskich i zwalczania piractwa.

# Wpływ technologii na ochronę praw autorskich

Rozwój technologii odgrywa kluczową rolę w transformacji sposobów, w jakie ochrona praw autorskich jest zarządzana i egzekwowana. Główne sposoby, w jakie technologie wpływają na ochronę praw autorskich:

- Blockchain: Technologia blockchain oferuje potencjalnie rewolucyjne rozwiązania w zakresie śledzenia i zarządzania prawami autorskimi. Dzięki niezmienności i decentralizacji, blockchain może być wykorzystywany do tworzenia zdecentralizowanych rejestrów praw autorskich, umożliwiając twórcom skuteczną identyfikację i zarządzanie swoimi dziełami.
- Sztuczna inteligencja (AI): AI może być wykorzystywana do automatycznego wykrywania naruszeń praw autorskich poprzez analizę treści cyfrowych i porównywanie ich z bazami danych chronionych dzieł. Systemy AI mogą również wspomagać w identyfikacji podobieństw między dziełami oraz w śledzeniu ich dystrybucji w sieci.
- Technologie Digital Rights Management (DRM): Systemy DRM są stosowane do zabezpieczania treści cyfrowych przed nieuprawnionym kopiowaniem i rozpowszechnianiem. Za pomocą DRM twórcy mogą kontrolować dostęp do swoich dzieł oraz określać warunki ich wykorzystania przez użytkowników.
- Wodze cyfrowe: Wodze cyfrowe są niewidocznymi znakami umieszczanymi w treściach cyfrowych, które pozwalają na identyfikację ich źródła oraz śledzenie ich drogi dystrybucji w sieci. Wodze cyfrowe mogą być stosowane do ochrony praw autorskich poprzez umożliwienie szybkiego wykrywania i ścigania naruszeń.
- Rozproszone sieci i inteligentne kontrakty: Rozproszone sieci, takie jak Ethereum, umożliwiają stosowanie inteligentnych kontraktów do automatycznego wykonywania umów licencyjnych i regulowania płatności za korzystanie z dzieł autorskich. To zapewnia przejrzystość i pewność prawnych transakcji, zmniejszając ryzyko sporów i nieporozumień.

## Studium przypadków

Przyjrzyjmy się kilku konkretnym przykładom naruszeń praw autorskich oraz środków podejmowanych w celu ich egzekwowania:

- Naruszenie praw autorskich na platformie internetowej: W 2022 roku firma produkująca oprogramowanie do edycji grafiki zauważyła, że na jednej z popularnych platform udostępniane są nielegalne kopie ich produktu. Wspólnie z zespołem prawnym firma przeprowadziła dochodzenie i wysłała powiadomienia prawne do osób udostępniających nielegalne kopie. Ponadto, firma wdrożyła technologiczne środki ochronne, aby uniemożliwić dalsze naruszenia praw autorskich.
- Piractwo filmowe: W 2023 roku wytwórnia filmowa zauważyła, że ich najnowszy film został nielegalnie udostępniony na wielu stronach internetowych jeszcze przed oficjalną premierą. Wspólnie z zespołem prawnym wytwórnia przeprowadziła intensywne działania monitorujące w celu wykrycia wszystkich nielegalnych kopii filmu i wysłała powiadomienia prawne do stron hostingowych. Dodatkowo, wytwórnia zainwestowała w kampanię edukacyjną, aby zwiększyć świadomość społeczeństwa na temat szkodliwości piractwa.
- Naruszenie praw autorskich na platformie społecznościowej: W 2024 roku artysta muzyczny zauważył, że jego utwory są używane bez zgody w popularnych filmach opublikowanych na platformie społecznościowej. Artysta skontaktował się z platformą i zgłosił naruszenia, a także zaczął śledzić i dokumentować przypadki nielegalnego wykorzystania jego muzyki. Wspólnie z zespołem prawnym artysta zaczął podejmować działania prawne przeciwko osobom naruszającym jego prawa autorskie.
- Studia przypadków pokazują, jak firmy i twórcy mogą skutecznie bronić swoich praw autorskich poprzez połączenie działań prawnych, technologicznych i edukacyjnych. Jednakże, walka z naruszeniami praw autorskich wymaga systematycznych działań oraz zaangażowania różnych zasobów, aby skutecznie egzekwować prawo i chronić interesy twórców.

# Podsumowanie i wnioski

Ochrona praw autorskich w erze cyfrowej stawia przed nami liczne wyzwania, ale również otwiera nowe możliwości dzięki rozwojowi technologicznemu. Kluczowe wnioski wynikające z analizy ochrony praw autorskich to:

- Ważność świadomości i edukacji: Świadomość praw autorskich wśród twórców, firm i społeczeństwa jest kluczowa dla skutecznej ochrony dzieł twórczych. Edukacja na temat praw autorskich oraz konsekwencji ich naruszeń powinna być kontynuowana i poszerzana.
- Konieczność dostosowania się do zmieniającego się krajobrazu technologicznego: Dynamiczny rozwój technologii wymaga ciągłej adaptacji strategii ochrony praw autorskich. Nowe technologie, takie jak blockchain, sztuczna inteligencja czy technologie DRM, mogą być wykorzystywane do skutecznej ochrony praw autorskich.
- Współpraca i partnerskie podejście: Walka z naruszeniami praw autorskich wymaga współpracy między twórcami, firmami, instytucjami rządowymi i organizacjami pozarządowymi. Tylko poprzez wspólną pracę i wymianę wiedzy można skutecznie zwalczać piractwo i inne formy naruszeń praw autorskich.
- Równowaga między ochroną a dostępem: Istnieje konieczność zachowania równowagi między ochroną praw autorskich a zapewnieniem społeczeństwu dostępu do kultury i wiedzy. Wprowadzanie środków ochronnych nie powinno ograniczać swobody przepływu informacji ani hamować innowacji.
- Innowacja i ciągłe doskonalenie: Ochrona praw autorskich wymaga ciągłego monitorowania zmian w technologiach i przepisach prawnych oraz dostosowywania strategii do zmieniających się warunków. Innowacyjne podejścia i technologie mogą być kluczowe dla skutecznej ochrony praw autorskich w erze cyfrowej.

Podsumowując, ochrona praw autorskich stanowi fundamentalny element bezpieczeństwa informacyjnego w erze cyfrowej. Działania podejmowane w celu skutecznej ochrony praw autorskich mają znaczący wpływ nie tylko na interesy twórców, ale także na rozwój kultury, innowacji i gospodarki jako całości. Dlatego też, dążenie do skutecznej ochrony praw autorskich wymaga wspólnych wysiłków wszystkich zainteresowanych stron oraz ciągłego doskonalenia strategii i narzędzi.

# Pytania:

- Jakie są najważniejsze zagrożenia dla praw autorskich w erze cyfrowej i jak wpływają one na bezpieczeństwo informacyjne?
- W jaki sposób ochrona praw autorskich może być integrowana z ogólnym systemem bezpieczeństwa informacyjnego organizacji?
- Jakie są skuteczne strategie i narzędzia, które można zastosować w celu ochrony praw autorskich i zapewnienia bezpieczeństwa informacyjnego w organizacji?

# Literatura:


- Bartyzel, Jarosław. "Prawo autorskie w XXI wieku." Wydawnictwo Wolters Kluwer, Warszawa, 2018. (dostęp: 02.05.2024)
- Błeszyńska, Irena, i in. "Prawo autorskie: podręcznik akademicki." Wydawnictwo C.H. Beck, Warszawa, 2017. (dostęp: 02.05.2024)
- Samuelson, Pamela. "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised." Berkeley Technology Law Journal 18, no. 2 (2003): 519-560. (dostęp: 02.05.2024)
- Vaidhyanathan, Siva. "Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity." NYU Press, 2003. (dostęp: 02.05.2024)
- Brzeziński, Jacek. "Ochrona praw autorskich w Internecie." Wydawnictwo C.H. Beck, Warszawa, 2014. (dostęp: 02.05.2024)
- Von Hippel, Eric. "Democratizing Innovation." MIT Press, 2005. (dostęp: 02.05.2024)
- Radoszewski, Tadeusz. "Prawo autorskie: zagadnienia podstawowe." Wydawnictwo Wolters Kluwer, Warszawa, 2019. (dostęp: 02.05.2024)
- Sowiński, Roman. "Prawo autorskie w Polsce i w Unii Europejskiej: komentarz." Wydawnictwo Wolters Kluwer, Warszawa, 2020. (dostęp: 02.05.2024)
- Tarapacka, Barbara, i in. "Prawo autorskie i pokrewne: kodeks, komentarz." Wydawnictwo Wolters Kluwer, Warszawa, 2019. (dostęp: 02.05.2024)

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

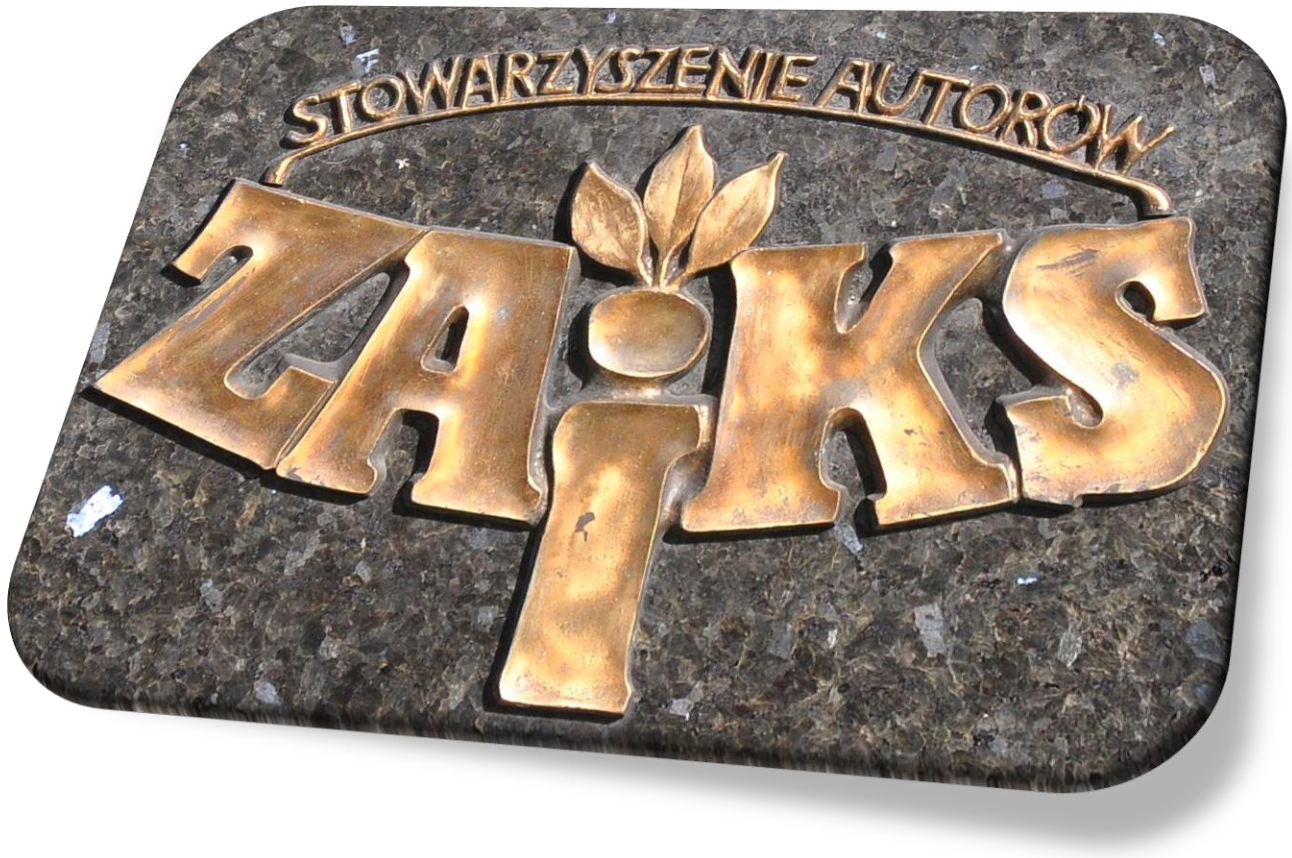
# ZAiKS jako instytucja praw autorskich

Marcin Kasprzak, mk88410@stud.uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

**Związek Autorów i Kompozytorów Scenicznych (ZAiKS)** – to polska organizacja zbiorowego zarządzania prawami autorskimi twórców. Instytucja ta jest zrzeszeniem osób fizycznych, twórców, których twórczość jest przedmiotem prawa autorskiego. Od 1918 roku, ma formę prawną stowarzyszenia i posiada osobowość prawną. Działa na tle ustawy z dnia 7 kwietnia 1989 r. *Prawo o stowarzyszeniach* (Dz. U. 1989 Nr 20 poz. 104) oraz ustawy z dnia 15 czerwca 2018 r. *o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi* (Dz. U. 2018 poz. 1293).

Funkcjonowanie ZAiKS-u reguluje statut uchwalony przez jego członków. Zasięg działania tej instytucji obejmuje obszar Rzeczypospolitej Polskiej, a jego siedzibą jest Warszawa. Członkowie ZAiKS-u wybierają spośród siebie władze Stowarzyszenia: **radę, zarząd i jego prezydium, komisję rewizyjną i sąd koleżeński.**



Marcin Kasprzak


W marcu 1918 roku **Julian Tuwim, Jan Brzechwa, Antoni Słonimski, Anda Kitschman** oraz kilkunastu innych autorów teatralnych i kabaretowych zawiązali pierwszą w Polsce organizację, która miała ochraniać prawa autorskie twórców. W tamtym momencie, na czele ZAiKS-u stanął dziennikarz, człowiek teatru i literatury **Stanisław Ossorya-Brochowski**. Od ponad 100 lat stowarzyszenie to jest zarządzane przez twórców i dla twórców.

Członkami ZAiKS-u są przedstawiciele wielu dziedzin twórczości (muzyki poważnej i rozrywkowej, poezji, prozy, dramatu, tekstów piosenek, scenariuszy, choreografii, fotografii, grafiki i innych sztuk plastycznych, a także nauki, publicystyki i architektury). Obecnie wciąż przybywają kolejne sekcje dla twórców, których dzieła przekraczają dawne granice i podziały.

**Głównymi celami statutowymi ZAiKS-u są:**

- ochrona praw autorskich, w szczególności:

a) zbiorowe zarządzanie prawami autorskimi,

b) działanie na rzecz rozwoju twórczości, doskonalenie jej ochrony, zwłaszcza w związku z rozwojem nowych technik,

c) działalność socjalna na rzecz jego członków.

Marcin Kasprzak

## Partnerzy ZAiKSU:

→**CISAC** (*Międzynarodowa Konfederacja Stowarzyszeń Autorów i Kompozytorów*) pracuje na rzecz współpracy między organizacjami zbiorowego zarządzania na świecie, dba o standardy ich działania oraz jednorodną i sprawną ochronę praw autorskich. Konfederacja powstała w 1926 roku, a ZAiKS był jednym z jej założycieli;

→**GESAC** (*Europejskie Zrzeszenie Stowarzyszeń Autorów i Kompozytorów*) pracuje nad wzmocnieniem prawa autorskiego w Unii Europejskiej;

→**BIEM** (*Międzynarodowe Biuro Stowarzyszeń Zarządzających Prawami do Nagrań i Reprodukcji Mechanicznej*) doskonali zarządzanie prawami w zakresie nagrań i reprodukcji mechanicznej.

## Partnerzy w Polsce:

- **SFP** *Stowarzyszenie Filmowców Polskich*;
- **STOART** *Związek Stowarzyszeń Artystów Wykonawców*;
- **SAWP** *Stowarzyszenie Artystów Wykonawców Utworów Muzycznych i Słowno-Muzycznych*;
- **ZPAV** *Związek Producentów Audio-Video*;
- **ZASP** *Związek Artystów Scen Polskich*;
- **ZPAF** *Związek Polskich Artystów Fotografików*;
- **ZPAP** *Związek Polskich Artystów Plastyków*;
- **STL** *Stowarzyszenie Twórców Ludowych*;
- **KOPIPOL** *Stowarzyszenie Zbiorowego Zarządzania Prawami Autorskimi Twórców Dzieł Naukowych i Technicznych*;
- *Stowarzyszenie Dziennikarzy i Wydawców* **REPROPOL**;
- *Stowarzyszenie Autorów i Wydawców* **COPYRIGHT POLSKA**.

## Literatura:

1. Ustawa z dnia 7 kwietnia 1989 r. *Prawo o stowarzyszeniach* (Dz. U. 1989 Nr 20 poz. 104);
2. Ustawa z dnia 15 czerwca 2018 r. *o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi* (Dz. U. 2018 poz. 1293);
3. Wykład dr hab. Włodzimierza Fehlera prof. uczelni z dnia 24 kwietnia 2024 roku pt.: *Przywłaszczanie cudzego dorobku intelektualnego i twórczego*;
4. https://zaiks.org.pl/ (28.04.2024)

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Pojęcie, znaczenie i rodzaje tajemnic

Maksymilian Strzyżewski, maks.strzyzewski@protonmail.ch

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Definicja tajemnic

- Dane lub informacje, których ujawnienie osobom nieuprawnionym jest zakazane ze względu na normy prawne lub inne normy społeczne. Przykładowe tajemnice:
- Tajemnice chronione prawem, w tym:
  - Informacje poufne
  - Tajemnice zawodowe
- Tajemnice religijne (mistyczne)
- Świadkowie chronieni prawem
- Tajemnica danych osobowych
- Tajność wyborów

# Znaczenie tajemnic

- Istnienie tajemnic, niezależnie od ich rodzaju, pozwala zachować bezpieczeństwo wrażliwych danych.
- Istnienie tajemnic prywatnych zapewnia komfort życia, gdyż niektóre informacje nie powinny być dostępne dla osób niepowołanych.
- Tajemnice zawodowe zapewniają bezpieczeństwo firm i ich usługobiorców, a także mogą stanowić środek przeciwko nieuczciwej konkurencji.
- Prawna ochrona informacji niejawnych jest niezbędna do zachowania bezpieczeństwa i stabilności państwa. Zdobywanie informacji niejawnych jest szpiegostwem, któremu przeciwdziałają organy kontrwywiadu.

# Rodzaje tajemnic w polskim prawie

- Tajemnica zawodowa:
  - Ogólne pojęcie tajemnic ściśle związane z wykonywaniem określonych zawodów bądź prowadzeniem działalności gospodarczej. Określa ją szereg aktów prawnych.
- Informacja niejawna:
  - Dane, których nieuprawnione ujawnienie byłoby szkodliwe lub niekorzystne dla Rzeczpospolitej Polskiej.
  - Określone są w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
  - Zostały podzielone na cztery kategorie: ściśle tajne, tajne, poufne i zastrzeżone

Informacje z klauzulą „**ściśle tajne**” to informacje, który ujawnienie mogłoby:

- Zagrozić niepodległości, suwerenności lub integralności Rzeczpospolitej Polskiej
- Zagrozić bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu kraju
- Osłabić potencjał obronny RP
- Zagrozić sojuszom międzynarodowym, których członkiem jest RP
- Doprowadzić do identyfikacji funkcjonariuszy wywiadu lub kontrwywiadu, wykonujących czynności operacyjne
- Zagrozić zdrowiu lub życiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze oraz świadków koronnych i członków ich rodzin

Informacje z klauzulą „**tajne**” to informacje, który ujawnienie mogłoby:

- Uniemożliwić ochronę suwerenności państwa lub porządku konstytucyjnego
- Pogorszyć relacje Polski z innymi krajami
- Zakłócić funkcjonowanie Sił Zbrojnych
- Utrudnić czynności operacyjno-rozpoznawcze w interesie państwa lub ściganie sprawców zbrodni
- Wywołać znaczne straty ekonomiczne państwa
- Zakłócić funkcjonowanie wymiaru sprawiedliwości

Informacje z klauzulą „**poufne**” to informacje, który ujawnienie mogłoby:

- Utrudnić prowadzenie polityki zagranicznej
- Utrudnić realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych
- Zakłócić porządek publiczny lub zagrozić bezpieczeństwu obywateli
- Utrudnić wykonywanie zadań służbom odpowiedzialnym za ochronę bezpieczeństwa i porządku publicznego, ściganie sprawców przestępstw i przestępstw skarbowych
- Zagrozić stabilności systemu finansowego państwa
- Wpłynąć niekorzystnie na funkcjonowanie gospodarki narodowej

Informacje z klauzulą „**zastrzeżone**” to informacje, który ujawnienie mogłoby mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

# Wybrane przykłady tajemnic zawodowych

# Tajemnica skarbowa

- Podstawa prawna: art. 293 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa
- § 1. Indywidualne dane zawarte w deklaracji oraz innych dokumentach składanych przez podatników, płatników lub inkasentów objęte są tajemnicą skarbową.
- § 2. Przepis § 1 stosuje się również do danych zawartych w:
  - informacjach podatkowych przekazywanych organom podatkowym przez podmioty inne niż wymienione w § 1,
  - aktach dokumentujących czynności sprawdzające,
  - aktach postępowania podatkowego, kontroli podatkowej oraz aktach spraw karnych skarbowych,
  - informacjach uzyskanych przez organy podatkowe z banków oraz ze źródeł innych niż wymienione w § 1 lub w pkt 1 i 2.

# Tajemnica dziennikarska

- Podstawa prawna: art. 15 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe
- Dziennikarz ma obowiązek zachowania w tajemnicy:
  - danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych,
  - wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

# Tajemnica przedsiębiorstwa

- Podstawa prawna: art. 11 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji
- Tajemnicą przedsiębiorstwa są informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności

# Tajemnica adwokacka

- Podstawa prawna: art. 6 ustawy z 26 maja 1982 r. Prawo o adwokaturze
- 1. Adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej.
- 2. Obowiązek zachowania tajemnicy zawodowej nie może być ograniczony w czasie.
- 3. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.

# Tajemnica prokuratorska

- Podstawa prawna: art. 102 ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze
- § 1. Prokurator jest obowiązany zachować w tajemnicy okoliczności sprawy, o których w postępowaniu przygotowawczym, a także poza jawną rozprawą sądową, powziął wiadomość ze względu na swoje stanowisko prokuratora.
- § 2. Obowiązek zachowania tajemnicy trwa także po ustaniu stosunku służbowego.
- § 3. Obowiązek zachowania tajemnicy ustaje, gdy prokurator składa zeznania jako świadek w postępowaniu przygotowawczym lub przed sądem, chyba że ujawnienie tajemnicy zagraża dobru Państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W takich przypadkach od obowiązku zachowania tajemnicy może zwolnić prokuratora Prokurator Krajowy, a Prokuratora Krajowego – Prokurator Generalny.

# Tajemnica komornika sądowego

- Podstawa prawna:  art. 27 ustawy z dnia 22 marca 2018 r. o komornikach sądowych
- 1. Komornik jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na wykonywane czynności.
- 2. Obowiązek, o którym mowa w ust. 1, trwa także po odwołaniu komornika z zajmowanego stanowiska albo wygaśnięciu powołania na stanowisko komornika z mocy prawa.
- 3. Obowiązek, o którym mowa w ust. 1, ustaje, gdy komornik składa zeznanie jako świadek lub strona przed sądem lub prokuratorem, chyba że ujawnienie tajemnicy zagraża dobru państwa. W tym przypadku od obowiązku może zwolnić komornika Minister Sprawiedliwości.

# Tajemnica lekarska

- Podstawa prawna: art. 40 ustawy z dnia 5 grudnia 1996 r. o zawodzie lekarza
- Lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu.

# Tajemnica spowiedzi

- Podstawa kanoniczna: kan. 983 Kodeksu Prawa Kanonicznego
  - § 1. Tajemnica sakramentalna jest nienaruszalna; dlatego nie wolno spowiednikowi słowami lub w jakikolwiek inny sposób i dla jakiejkolwiek przyczyny w czymkolwiek zdradzić penitenta.
  - § 2. Obowiązek zachowania tajemnicy ma także tłumacz, jeśli występuje, jak również wszyscy inni, którzy w jakikolwiek sposób zdobyli ze spowiedzi wiadomości o grzechach.
- Tajemnica spowiedzi jest chroniona przez polskie prawo. Następujące akty prawne dają możliwość odmówienia składania zeznań lub wyłączają duchownych z tej czynności, jeśli ich zeznania byłyby naruszeniem tajemnicy spowiedzi:
  - Art. 178 pkt 2 kodeksu postępowania karnego
  - Art. 261 § 2 kodeksu postępowania cywilnego
  - Art. 82 pkt 3 kodeksu postępowania administracyjnego
  - Art. 195 pkt 3 Ordynacji podatkowej.

## Bibliografia


- Kodeks Prawa Kanonicznego 1983, www.episkopat.pl, [dostęp:19.04.2024]
- Ustawa z dnia 14 czerwca 1960r. Kodeks postępowania administracyjnego
- Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji
- Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego
- Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze
- Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe
- Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze
- Ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji
- Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa
- Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
- Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Cenzura jako instrument polityki bezpieczeństwa informacyjnego

Wojciech Januszewski, wj88413@stud.uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Polityka bezpieczeństwa informacyjnego

„Celowa i zorganizowana działalność danego podmiotu (państwa, korporacji, organizacji, instytucji itp.) ukierunkowana na tworzenie i utrzymywanie w optymalnym jakościowo kształcie własnych zasobów informacyjnych i mechanizmów ich użytkowania połączona z efektywną ochroną przed destrukcyjnym oddziaływaniem podmiotów konkurencyjnych, nieprzyjaznych czy wrogich.”

Cenzura - każde ograniczenie wolności słowa, niezależnie od podmiotu, który go dokonuje.

Cenzurę można określić mianem prawdy selektywnej. Jest to zjawisko odmienne od kłamstwa, bowiem kłamstwo wprowadza w błąd poprzez kreowanie fałszywych faktów. Natomiast prawda selektywna jest bardziej subtelna, polega na manipulowaniu kontekstem informacji oraz odpowiednio dobranymi i uporządkowanymi prawdami cząstkowymi.

Cenzura prewencyjna (uprzednia) oznacza ingerowanie w informację przed jej upowszechnieniem.

Cenzura post facto obejmuje działania podejmowane po opublikowaniu informacji.

Pewne formy nadzoru i kontroli, w tym m.in. w postaci cenzury, także prewencyjnej, są obecne w krajach powszechnie uważanych za nowoczesne i demokratyczne. Zapewnienie bezpieczeństwa obywatelom wymaga monitorowania Internetu przez organy państwowe. Jest to konieczne chociażby ze względu na występujące tam przestępstwa przeciwko porządkowi publicznemu (np. publiczne propagowanie faszyzmu, nawoływanie do nienawiści), obyczajowości czy moralności.

W państwach demokratycznych największe możliwości ograniczania treści prezentowanych w mediach zapewniają uregulowania dotyczące tajemnicy państwowej.

Kryterium sposobu dokonywania cenzury pozwala wyodrębnić cenzurę bezpośrednią i pośrednią. W pierwszym przypadku mamy do czynienia z jawną ingerencją w treść przekazu lub z jego blokowaniem. W przypadku cenzury pośredniej na przekaz wpływa się za pomocą miękkich technik oddziaływania – przykładem mogłoby być subsydiowanie prasy.

W państwach totalitarnych, cenzura była (i nadal jest) szczególnie surowa. Władze kontrolują niemal wszystkie aspekty życia publicznego, a media są państwowe lub pod ich ścisłą kontrolą. Każda forma opozycji lub krytyki jest surowo tłumiona, a obywatele narażeni są na represje za wyrażanie niezgodnych z oficjalną linią poglądów.

W państwach totalitarnych i autorytarnych często dochodzi do cenzurowania przez władzę treści zawartych w Internecie. Cenzura państwowa przybiera postać ingerencji bezpośredniej lub pośredniej – z wykorzystaniem różnorodnych sankcji, może mieć charakter prewencyjny lub post facto.

Najczęściej przejawia się w następujących formach:

– techniczne utrudnianie dostępu do sieci polegające na całkowitym bądź częściowym jej zablokowaniu,

– penalizowanie korzystania z określonych internetowych kanałów przekazu bądź usług i/lub wprowadzanie zakazu udostępniania pewnych treści,

– tworzenie administracyjnych, finansowych oraz polityczno-społecznych barier dostępu do Internetu, np. poprzez wymóg rejestracji treści zamieszczanych w sieci, zawyżanie cen dostępu do Internetu czy hakowanie stron internetowych, a następnie blokowanie/ kasowanie ich zawartości oraz zastraszanie aktywnych użytkowników

## Bibliografia

1. Fehler W., *O pojęciu bezpieczeństwa informacyjnego, [w:] Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce–Warszawa, 2016.
2. Krzewniak D., *Nadzór i kontrola internetu jako instrument polityki bezpieczeństwa informacyjnego współczesnych państw*, Uniwersytet w Siedlcach, 2021.
3. Mider D., Borówka O., *Internet – medium bez cenzury?*, Uniwersytet Warszawski, 2012.
4. Rajczyk R., *Instrumenty polityki bezpieczeństwa informacyjnego Białorusi*, Uniwersytet Śląski, 2024.

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Rola mediów społecznościowych w sytuacjach kryzysowych

Mahinbonu Isaeva

mahinbonu.isaeva@gmail.com

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Rola mediów społecznościowych w sytuacjach kryzysowych

Mahinbonu Isaeva

- Media społecznościowe odgrywają istotną rolę w sytuacjach kryzysowych, zarówno podczas naturalnych katastrof, jak i w sytuacjach kryzysowych.
- Pozwalają na szybką wymianę informacji między społecznościami, co może być istotne zwłaszcza w przypadku ewakuacji czy przemieszczania się ludzi w wyniku kryzysu.

- Ludzie znajdujący się na miejscu zdarzeń często stają się pierwszymi świadkami kryzysu. Dzięki mediom społecznościowym mają możliwość relacjonowania sytuacji w czasie rzeczywistym, co pozwala dostarczać cenne informacje zarówno lokalnym społecznościom, jak i służbom ratowniczym oraz organizacjom humanitarnym.
- Platformy społecznościowe pełnią również istotną rolę w szybkim rozpowszechnianiu informacji edukacyjnych, które uczą, jak bezpiecznie reagować na daną sytuację, jak korzystać z dostępnych zasobów oraz jak unikać niebezpieczeństw.

# Rola mediów społecznościowych w sytuacjach kryzysowych

Mahinbonu Isaeva

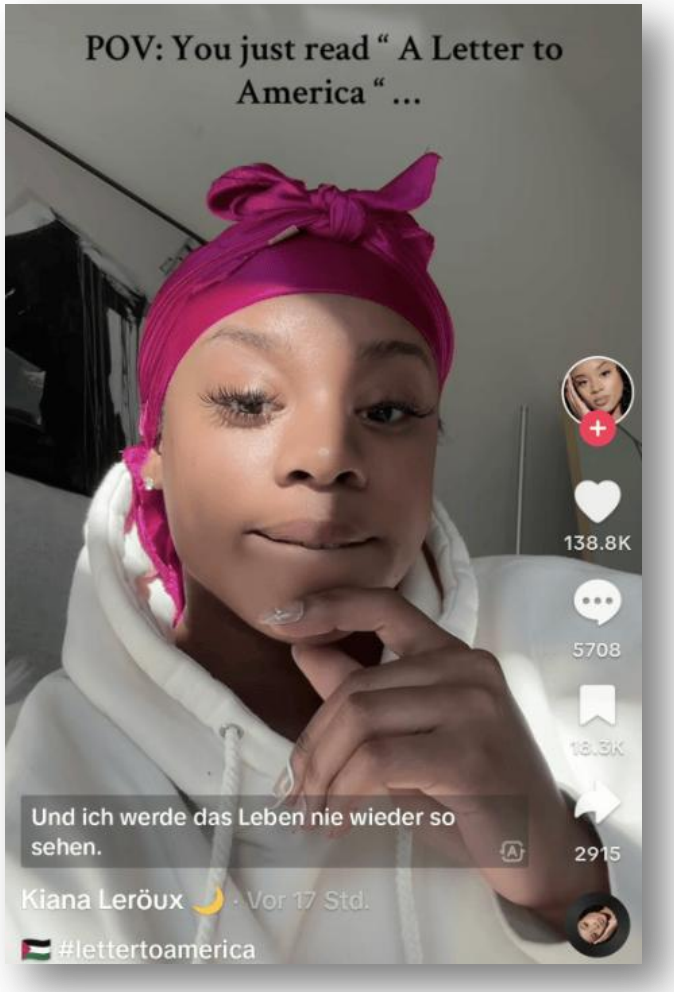
- W czasach kryzysowych często pojawia się dezinformacja, co może skutkować rozprzestrzenianiem się chaosu i dezorientacją społeczeństwa.

- Media społecznościowe pełnią jednak kluczową rolę, umożliwiając szybkie sprostowanie fałszywych informacji i przeciwdziałanie rozprzestrzenianiu się nieprawdziwych treści.

- Nadmiar informacji na platformach społecznościowych może prowadzić do zjawiska zwanego przeładowaniem informacyjnym, co sprawia, że użytkownicy mają trudności z odróżnieniem istotnych informacji od tych mniej ważnych. To może znacząco wpływać na efektywność komunikacji w krytycznych momentach.

- Dodatkowo, zarządzanie treściami niestandardowymi na mediach społecznościowych stanowi kolejne wyzwanie. Platformy te mogą nieumyślnie stać się miejscem dla szkodliwych treści, takich jak mowa nienawiści, fałszywe ogłoszenia o pomocy czy nieodpowiednie treści w kontekście kryzysowym. Efektywne moderowanie i filtrowanie treści jest kluczowe, aby zapewnić, że media społecznościowe służą jako wsparcie, a nie jako źródło dodatkowych problemów w trudnych sytuacjach.

- Jednym z negatywnych przykładów jest sytuacja, w której usprawiedliwienie Osamy bin Ladena dla ataków z 11 września stało się szeroko rozpowszechnione na platformie TikTok podczas konfliktu między Izraelem a Hamasem.
- TikTok usunął hashtag #lettertoamerica ze swojej funkcji wyszukiwania, po tym jak filmy dotyczące "Listu do Ameryki" bin Ladena z 2002 roku zdobyły popularność na platformie i były ponownie przesyłane. Niektórzy użytkownicy mediów społecznościowych sugerowali, że dokument założyciela Al-Kaidy oferuje alternatywne spojrzenie na zaangażowanie USA w konflikty na Bliskim Wschodzie.

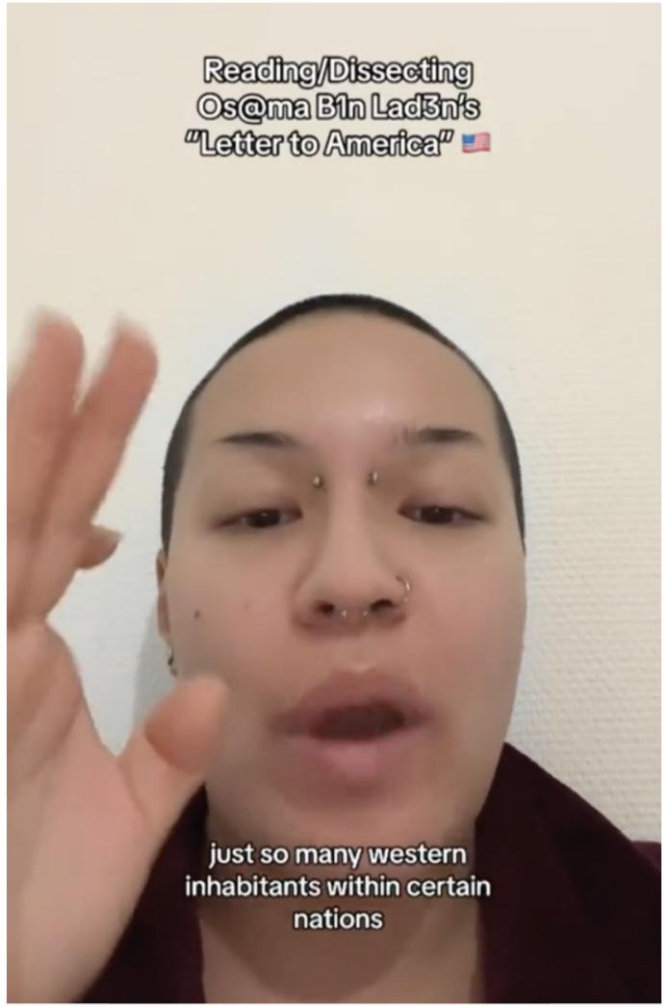


- Przez cały tydzień użytkownicy TikTok udostępniali link do transkrypcji listu bin Ladena, który został napisany przez The Guardian po atakach terrorystycznych z 11 września 2001 roku, w których zginęło prawie 3000 osób w Stanach Zjednoczonych.
- Bin Laden próbował manipulować faktami i emocjami, aby uzasadnić działania Al-Kaidy, które w rzeczywistości były motywowane radykalną ideologią i dążeniem do przemocy. List zawiera antysemicki język i homofobiczną retorykę.

- Osoby na platformie cytujące list zachęcały ludzi do jego przeczytania, mówiąc, że pomogło im to lepiej zrozumieć interwencje USA na Bliskim Wschodzie i wojnę między Izraelem a Hamasem.

- Wykorzystywanie wypowiedzi Osamy bin Ladena w dyskusjach o amerykańskiej polityce zagranicznej może doprowadzić glorifikacji postaci związanej z ekstremizmem.

- Przedstawiona sytuacja jest przykładem tego, jak terroryści mogą próbować wykorzystywać publiczne oświadczenia do prowadzenia swojej narracji i rekrutacji, jednocześnie dążąc do usprawiedliwienia swoich przestępczych działań w oczach międzynarodowej opinii publicznej.



- Traktowanie mediów społecznościowych jako głównego źródła informacji może prowadzić do znaczących wyzwań związanych z krytycznym przetwarzaniem informacji. Brak świadomości o działaniu algorytmów filtrujących treści, łatwy dostęp do informacji, a także manipulacje treściami dezinformacyjnymi i wpływy społecznościowe, często przyczyniają się do tego zjawiska. W efekcie, użytkownicy mogą być narażeni na jednostronne przekazy i mogą przyjmować przekonania bez odpowiedniej weryfikacji faktów.
- Aby zminimalizować te ryzyka, niezbędne jest promowanie edukacji medialnej oraz rozwijanie umiejętności krytycznego myślenia. Takie działania są kluczowe dla zwiększenia kompetencji medialnych w społeczeństwie, co umożliwi bardziej świadome i odpowiedzialne korzystanie z platform cyfrowych.

- **Bibliografia**


- https://www.timesofisrael.com/bin-ladens-antisemitic-letter-to-america-goes-viral-on-tiktok-amid-israel-hamas-war/?__cf_chl_tk=.smZwN63nrbJNm0_7PeEZtdMw2Z1HqiDeotlqDUJOHg-1714473426-0.0.1.1-1791 (dostęp 26.04.2024)

- https://www.euronews.com/2023/11/17/tiktok-takes-down-videos-promoting-osama-bin-ladens-letter-to-america-after-text-went-vira (dostęp 17.04.2024)

- Opgenhaffe, M. (2023). Combatting disinformation with crisis communication. Wydawnictwo De Gruyter

- Stasiuk-Krajewska, K., & Wenzel, M. (Red.). (2024). Dezinformacja w czasach kryzysu. Toruń: Wydawnictwo Adam Marszałek

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Organizacja obiegu dokumentów niejawnych w jednostce organizacyjnej

Konrad Cyran, kc88846@stud.uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Ochrona informacji niejawnych

Podstawą prawną ochrony informacji niejawnych w Polsce jest Ustawa z 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228) wraz z aktami wykonawczymi. W myśl ustawy informacją niejawną jest każda informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczpospolitej Polskiej. Informacje niejawne podlegają ochronie już w trakcie ich opracowywania.

# System ochrony informacji niejawnych

System ochrony informacji niejawnych stanowią:

- Przepisy i reguły z zakresu ochrony informacji niejawnych (ustawa, rozporządzenia, zarządzenia, decyzje, dyrektywy, instrukcje, procedury, wytyczne);
- Struktury organizacyjne (Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego oraz pion ochrony) powiązane ze sobą relacjami (kierowania) w taki sposób, że stanowią one całość zdolną do zapewnienia ochrony informacji niejawnych;
- Środki bezpieczeństwa fizycznego służące do ochrony informacji niejawnych (strefy ochronne, systemy alarmowe, sejfy, drzwi, niszczarki do dokumentów, oprogramowanie).

# Organizacja obiegu dokumentów niejawnych

Organizacja obiegu i ochrony informacji niejawnych oparta jest na kilku podstawowych zasadach, do których przestrzegania są zobowiązani adresaci ustawy (Dz.U. 2010, nr 182, poz. 1228). Najważniejsze są zapisane w art. 8 ustawy stanowiącym, że informacje niejawne, którym nadano określoną klauzulę tajności:

- Mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
- Muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;
- Muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

# Organizacja obiegu dokumentów niejawnych

ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych, oraz proces organizacji obiegu dokumentów niejawnych w jednostkach organizacyjnych:

- prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
- realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
- prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;
- zapewniają ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;
- prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

# W procesie obiegu dokumentów niejawnych można wyróżnić trzy zasadnicze etapy:

- Przygotowanie do przedsięwzięcia.
- Fizyczne zabezpieczenie przebiegu przedsięwzięcia.
- Czynności wykonywane po zakończeniu przedsięwzięcia.

# Etap pierwszy – przygotowanie do przedsięwzięcia

Etap pierwszy zawiera przedsięwzięcia myślowo - organizacyjne ukierunkowane na właściwe przygotowanie odprawy, rozmów czy narady. Wbrew pozorom jest to niezwykle istotny albo też najistotniejszy element całego procesu. Zła czy błędna ocena sytuacji, nieadekwatnie dobrane środki, miejsce czy uczestnicy mogą doprowadzić do utraty, zagubienia lub dotarcia informacji niejawnych do osoby lub osób nieuprawnionych. Konsekwencje mogą być jeszcze gorsze gdy informacja ta dotrze do osób, przed którymi miała być chroniona. Kolejny aspekt zaniedbań to mogące nastąpić reperkusje wynikające z zapisów ustawowych od postępowania wyjaśniającego począwszy po wynik postępowania kontrolnego w stosunku do organizatorów i winnych zaniedbań. Jeżeli nieprawidłowości dotyczyć będą informacji o klauzuli „Tajne” i „Ściśle Tajne”, to winni zaniedbań podlegać będą ocenie prokuratury. Dlatego też efekt tych działań obejmujący ten etap musi być dokładnie przemyślany i gruntownie przeanalizowany.

# Etap pierwszy – przygotowanie do przedsięwzięcia

Podczas etapu pierwszego należy odpowiedzieć na kilka zasadniczych pytań:

- Jakie informacje będziemy przedstawiać (dyskutować, prezentować)?;
- Komu będziemy je prezentować (adresaci)?;
- W jaki sposób będziemy przetwarzać informacje?;
- Czy posiadamy warunki do ich bezpiecznej prezentacji?;

# Etap drugi – fizyczne zabezpieczenie przebiegu przedsięwzięcia

Etap zabezpieczenia fizycznego dzieli się na trzy części:

- Wprowadzenie (część organizacyjna).
- Przebieg (tok).
- Część końcowa.

# Etap drugi – fizyczne zabezpieczenie przebiegu przedsięwzięcia

Wprowadzenie (część organizacyjna):

W części pierwszej prowadzący lub osoba przez niego upoważniona np. pełnomocnik do spraw ochrony informacji niejawnych dokonuje sprawdzenia przybycia właściwych osób (zgodnie z wcześniej zgłoszonymi osobami na listach) uprawnień osób biorących udział w przedsięwzięciu (wcześniej deklarowanych) tj.: posiadanie stosownych poświadczeń bezpieczeństwa oraz zaświadczeń o przeszkoleniu w zakresie ochrony informacji niejawnych. Następnie informuje (przypomina) o konieczności zdeponowania urządzeń mających możliwość nagrywania oraz o klauzuli przetwarzanych informacji. Jednocześnie informuje, że w tym pomieszczeniu podczas realizacji tego przedsięwzięcia nie ma możliwości przetwarzania informacji o wyższych klauzulach.

# Etap drugi – fizyczne zabezpieczenie przebiegu przedsięwzięcia

Przebieg (tok):

W części drugiej podczas trwania danego przedsięwzięcia należy pamiętać, że jeżeli będziemy zapoznawali jej uczestników z dokumentami niejawnymi o klauzuli „tajne” i „ściśle tajne” to bezwzględnie należy dopilnować aby wszyscy uczestnicy potwierdzili ten fakt w kartach zapoznania się z dokumentem. Natomiast przy dokumentach niejawnych o klauzuli „poufne” i „zastrzeżone” nie ma tego formalnego wymogu ale na podstawie wspomnianej wcześniej listy obecności będziemy dysponowali wiedzą kto został z tymi informacjami zapoznany.

# Etap drugi – fizyczne zabezpieczenie przebiegu przedsięwzięcia

Część końcowa:

W części końcowej w zależności od specyfiki i wagi danego przedsięwzięcia można np. przypomnieć uczestnikom o art. 4 ustawy i o konieczności zachowania dotychczas pozyskanych informacji w całkowitej dyskrecji lub tylko w gronie biorących w niej udział. Można określić również sposób dystrybucji materiałów niejawnych i ewentualny termin następnego spotkania oraz nakreślić zadania w celu przygotowania się do niego uczestników. Po opuszczeniu przez wszystkich miejsca, w którym odbywało się przedsięwzięcie należy dokonać szczegółowego sprawdzenia pomieszczenia pod kątem pozostawienia materiałów niejawnych.

# Etap trzeci – Czynności wykonywane po zakończeniu przedsięwzięcia

Po zakończeniu zebrania uczestnicy zdają dokumenty niejawne do kancelarii jednostki organizującej zebranie, celem przesłania ich do jednostki uczestnikom zebrania lub zniszczenia. Dokumenty mogą być wydane uczestnikom zebrania, jeżeli są upoważnieni do zebrania ich z sobą. Przewodniczący zebrania w porozumieniu z jego organizatorem ustala sposób dokumentowania wiadomości omawianych lub przekazywanych w czasie zebrania albo określa wiadomości, których dokumentować nie wolno. Wiadomości omawiane lub przekazywane w czasie zebrania mogą być zapisywane tylko w notatnikach (zeszytach pracy) przygotowanych i wydanych uczestnikom przez kancelarię jednostki organizującej zebranie lub przez kancelarie jednostki macierzystej. Wiadomości niejawne omawiane lub przekazywane na zebraniu mogą stenografować lub zapisywać na taśmie magnetofonowej tylko osoby mające upoważnienia.

# Podsumowanie

Organizacja obiegu dokumentów niejawnych w jednostce organizacyjnej to kluczowy element zapewnienia bezpieczeństwa informacji oraz ochrony poufności danych. Poprzez odpowiednie procedury, klasyfikację, oznakowanie, rejestrację, zabezpieczenie i kontrolę obiegu dokumentów niejawnych można skutecznie zapobiegać nieuprawnionemu dostępowi do poufnych informacji oraz minimalizować ryzyko ich ujawnienia. Wprowadzenie i przestrzeganie tych procedur stanowi fundamentalny element bezpieczeństwa w każdej jednostce organizacyjnej.

# Bibliografia


- Napiórkowski J, Stanik J., *Zastosowanie technologii RFID do zarządzania obiegiem dokumentów niejawnych.* „Ekonomiczne Problemy Usług", 2017.
- Topolewski S., *System ochrony informacji niejawnych,* (w:) *Ochrona informacji niejawnych. Teoria i praktyka,* red. M. Kubiak, S. Topolewski, Siedlce 2013.
- Topolewski S., Załoga R., *Organizacja ochrony informacji niejawnych w czasie narad, odpraw, konferencji i rozmów,* Siedlce 2014.
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, (Dz.U. 2010, nr 182, poz. 1228).

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

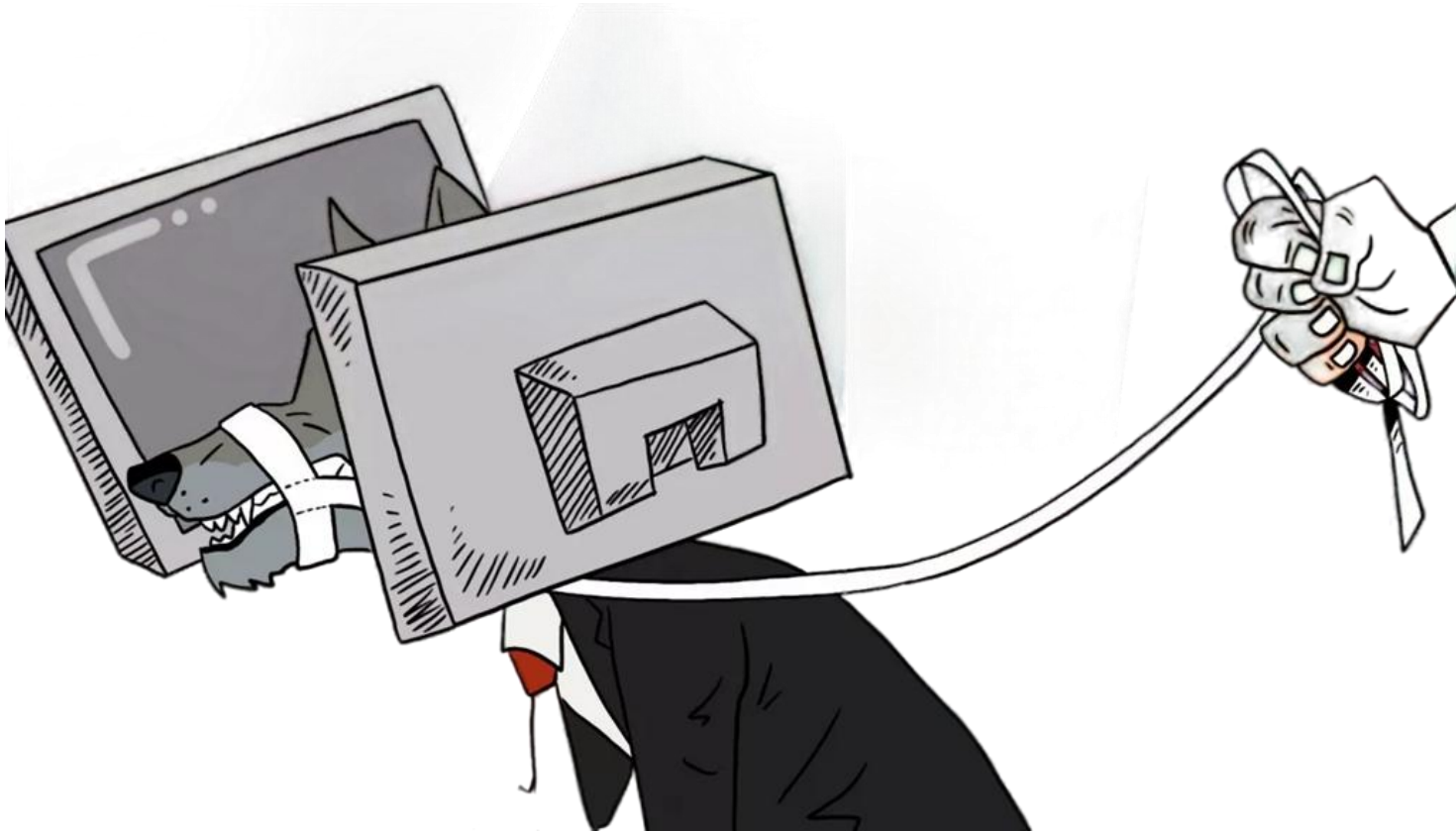
***w systemie bezpieczeństwa informacyjnego***

# Propaganda jako zagrożenie informacyjne

Yana Likhtarovich, lixtarovichy21@gmail.com

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

Ogólnopolska Konferencja Naukowa
z cyklu ***Bezpieczeństwo informacyjne*** na temat:
***Informacje niejawne i prawnie chronione***
***w systemie bezpieczeństwa informacyjnego***



# Cel i znaczenie bezpieczeństwa informacyjnego

K. Liedel: „**Bezpieczeństwo informacyjne** bardzo często rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania".

**Głównym celem** bezpieczeństwa informacyjnego jest zabezpieczenie informacji przed wszelkimi zagrożeniami, takimi jak cyberatak, manipulacja informacją, utrata danych czy działania szkodliwe. Obejmuje to nie tylko ochronę systemów komputerowych, ale również procesów, ludzi i danych, które są kluczowe dla funkcjonowania organizacji czy społeczeństwa.

**Znaczenie** bezpieczeństwa informacyjnego:

1. *Ochrona Wartościowych Informacji*
2. *Zapewnienie Spójności Komunikacji*
3. *Zabezpieczenie Przed Atakami Cybernetycznymi*
4. *Utrzymanie Zaufania Społecznego*

Yana Likhtarovich

# Propaganda

**Propaganda** (łac. prōpāgāre – rozszerzać, rozciągać, krzewić) – celowe działanie zmierzające do ukształtowania określonych poglądów i zachowań zbiorowości ludzkiej lub jednostki.

# Rozróżnienie między informacją a propagandą

**Informacja** to obiektywny przekaz faktów, danych lub wydarzeń bez wprowadzania subiektywnych opinii. Jej celem jest dostarczenie rzetelnej wiedzy.

Natomiast **propaganda** to celowe użycie przekazu w celu manipulacji i kształtowania opinii, często oparte na subiektywnych przekonaniach. Propaganda dąży do wprowadzenia odbiorcy w błąd, promowania określonych ideologii lub uzyskania poparcia dla konkretnej sprawy, często kosztem obiektywności i uczciwości. Różnice obejmują cel, obiektywność, źródło informacji, etykę komunikacji oraz stosowanie języka i sztuki perswazji.

# Propaganda ma długą historię, sięgającą starożytności, ale zyskała szczególne znaczenie w czasach nowożytnych i XX wieku

**Antyczne Imperia:** Już starożytne imperia, takie jak Rzym czy Persja, używały propagandy w formie posągów, zabytków i inskrypcji do promowania swojej potęgi i zasług.

**Rewolucja Przemysłowa:** Wraz z rozwojem druku w XV wieku, propagandę zaczęto masowo produkować, co umożliwiło szerokie jej rozpowszechnienie.

**I wojna światowa:** Ta wojna była punktem zwrotnym dla propagandy, z intensywnym wykorzystaniem plakatów, prasy i filmów, aby kształtować opinię publiczną i mobilizować społeczeństwo.

**II wojna światowa:** Propaganda osiągnęła apogeum podczas II wojny światowej, gdzie wszystkie strony konfliktu intensywnie ją wykorzystywały do manipulowania informacjami, kontrolowania narracji i budowania morale.

**Zimna wojna:** Konflikt między blokami kapitalistycznym a komunistycznym toczył się również na polu propagandy. Telewizja, radio i gazety były narzędziami walki o wpływy.

**Era Internetu:** Wraz z rozwojem internetu i mediów społecznościowych, propaganda stała się bardziej dostępna, globalna i skomplikowana. Dezinformacja i manipulacje są teraz powszechne w cyfrowym środowisku.

# Propagandę można kwalifikować jako białą, szarą lub czarną:

**Biała propaganda** - rodzaj propagandy, który podaje prawdziwe źródło pochodzenia informacji. Przykładem takich działań może być wystąpienie prominentnych członków rządu w telewizji, *exposé premiera* czy *plakat nawołujący* do walki w obronie ojczyzny.

**Szara propaganda** - rodzaj propagandy, która charakteryzuje się tym, że źródło jej pochodzenia jest dla odbiorcy nieznane i może się on jedynie domyślać jej pochodzenia. Przykładem takich działań są działania brytyjskiego Komitetu Propagandy Podziemnej (Underground Propaganda Committee, UPC) w czasie II wojny światowej polegające na rozprzestrzenianiu plotek o rzekomej nowej brytyjskiej broni umożliwiającej podpalenie morza.

**Czarna propaganda** - forma propagandy, która ma sprawiać wrażenie, że została stworzona przez tych, których ma zdyskredytować.

Przykładem takich działań w czasie II wojny światowej były fałszerstwa niemieckich pism urzędowych dokonywane przez polski ruch oporu (Akcja N) czy niemiecka ulotka napisana w języku polskim w czasie powstania warszawskiego z rzekomym „rozkazem" generała Tadeusza Bora-Komorowskiego. [5]

# 1. Osłabianie obiektywności informacji

Osłabianie obiektywności informacji jest jednym z kluczowych mechanizmów stosowanych w propagandzie. Obejmuje to celowe wprowadzanie w błąd, manipulowanie faktami i kierowanie przekazu w taki sposób, aby podważać rzetelność informacji. Główne metody osłabiania obiektywności informacji w kontekście propagandy:

**lektywne Przedstawianie Faktów:** Propaganda często wybiera jedynie te fakty, które pasują do określonej narracji, pomijając lub zniekształcając pozostałe. Poprzez selektywne przedstawianie faktów, tworzy się subiektywny obraz sytuacji.

**Manipulacja Statystykami:** Celowe manipulowanie danymi statystycznymi, takie jak wybór konkretnych okresów czasu, ukrywanie pewnych danych lub prezentowanie ich w sposób mylący, może prowadzić do fałszywego przekazu.

**Użycie Emocji:** Propaganda często stara się wywoływać silne emocje u odbiorcy, co może zaciemniać obiektywny sposób postrzegania informacji. Wykorzystanie emocji może odwrócić uwagę od faktów na rzecz subiektywnego odczucia.

**Tworzenie Fałszywych Kontekstów:** Przekazywane informacje mogą być umieszczane w kontekstach, które podważają ich prawdziwość lub zmieniają ich znaczenie. Tworzenie fałszywych kontekstów jest skutecznym narzędziem manipulacji.

**Ataki na Wiarygodność Źródeł:** Propaganda może próbować dyskredytować wiarygodność źródeł informacji poprzez ataki personalne, zarzuty o stronniczość lub twierdzenia o ukrytych interesach.

**Rozprzestrzenianie Teorii Spiskowych:** Propaganda może aktywnie promować teorie spiskowe lub dezinformację, co wprowadza zamęt w informacjach i sprawia, że trudniej jest odróżnić prawdziwe informacje od fałszywych.

# 2. Manipulowanie percepcją odbiorcy

Manipulowanie percepcją odbiorcy to kluczowy element propagandy, który ma na celu kształtowanie opinii, postaw, i reakcji społeczeństwa. Kilka głównych technik wykorzystywanych w manipulowaniu percepcją:

**Użycie Języka i Słownictwa:** Propaganda często stosuje język, który pobudza emocje i wywołuje konkretne skojarzenia. Słowa mające silne konotacje emocjonalne mogą wpływać na odbiór informacji.

**Obrazowanie i Symbolika:** Wykorzystywanie grafiki, zdjęć czy symboli, które mogą wywołać określone emocje lub skojarzenia, ma znaczący wpływ na percepcję odbiorcy.

**Manipulacja Obrazem Czasu:** Umieszczanie informacji w określonym kontekście czasowym, takim jak wybór konkretnych momentów zdarzeń, może wprowadzać w błąd i zmieniać percepcję ich znaczenia.

**Kreowanie Fałszywych Narracji:** Propaganda buduje swoje narracje, które niekoniecznie odzwierciedlają rzeczywistość. Poprzez kreowanie specyficznych historii lub wydarzeń, próbuje ukształtować postrzeganie odbiorcy.

**Powtarzanie i Zasada Równoczesności:** Częste powtarzanie określonych informacji może wpłynąć na ich akceptację przez odbiorcę. Zasada równoczesności polega na jednoczesnym prezentowaniu kilku informacji, co utrudnia krytyczną analizę.

**Zastosowanie Autorytetów:** Propaganda często odwołuje się do postaci uważanych za autorytety, aby wzmocnić swoje argumenty. Wykorzystanie opinii specjalistów czy popularnych postaci publicznych wpływa na percepcję treści.

**Tworzenie Sztucznych Kontrowersji:** Celowe wywoływanie kontrowersji wokół określonych tematów ma na celu zwrócenie uwagi i skupienie się na wybranych

## 3. Naruszanie bezpieczeństwa informacyjnego jednostek i społeczeństw

Naruszanie bezpieczeństwa informacyjnego jednostek i społeczeństw to kompleksowy problem, który może mieć poważne konsekwencje na wielu poziomach. Główny aspekty związanych z tym zagrożeniem:

**Manipulacja Opinią Publiczną:** Propaganda i dezinformacja mogą wprowadzać w błąd opinię publiczną, wpływając na zdolność społeczeństwa do podejmowania świadomych decyzji.

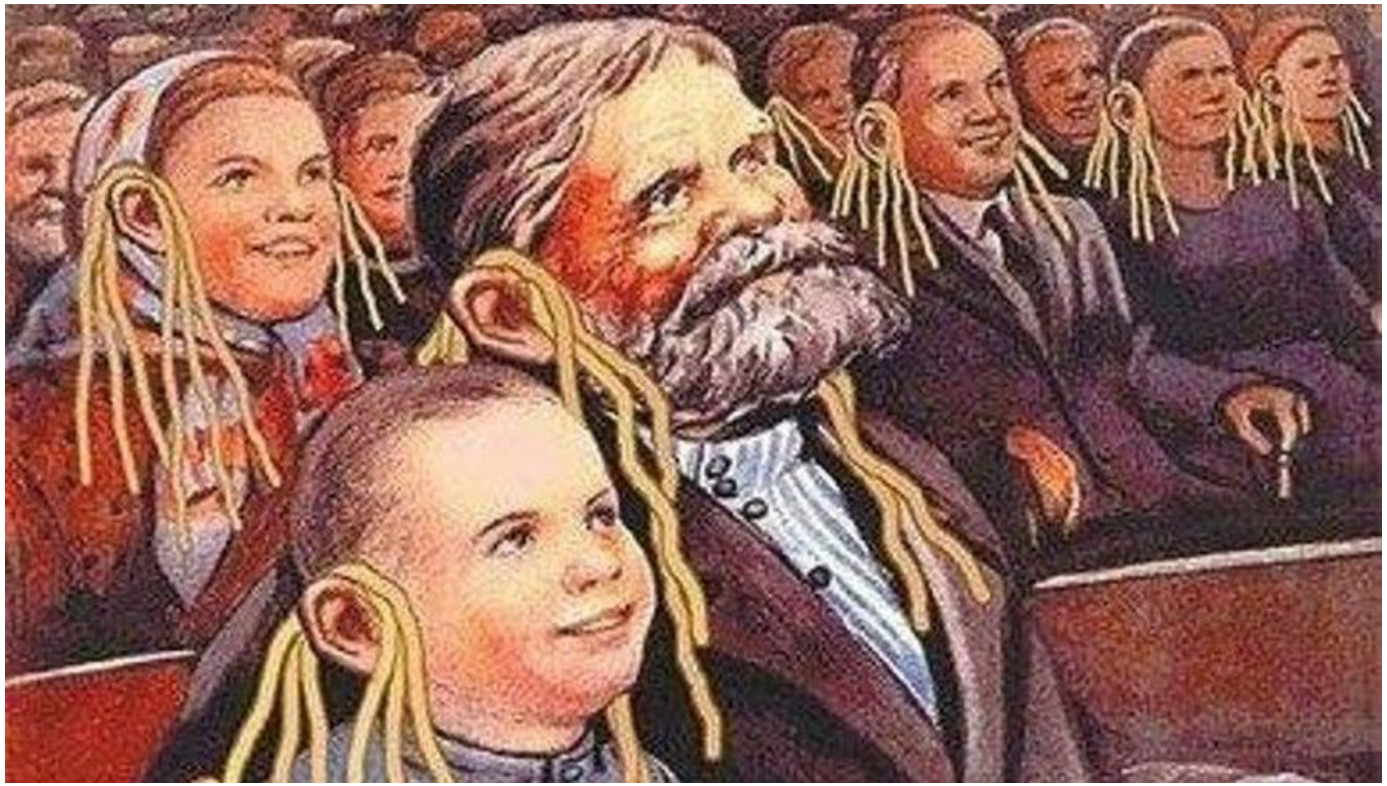
**Polaryzacja Społeczeństwa:** Propaganda może pogłębiać podziały społeczne, wywołując konflikty i zwiększając napięcia.

**Zagrożenia dla Bezpieczeństwa Cybernetycznego:** Ataki cybernetyczne, takie jak phishing czy ransomware, stanowią zagrożenie dla bezpieczeństwa informacyjnego jednostek i społeczeństw.

**Zniekształcanie Rzeczywistości:** Propaganda celowo zniekształca fakty, wprowadzając w błąd jednostki i społeczeństwo co do rzeczywistości zdarzeń czy działań politycznych.

**Utrata Zaufania do Instytucji:** Ciągłe narażanie społeczeństwa na dezinformację może prowadzić do utraty zaufania do instytucji, takich jak media czy rząd.

Ogólnopolska Konferencja Naukowa
z cyklu ***Bezpieczeństwo informacyjne*** na temat:
***Informacje niejawne i prawnie chronione***
***w systemie bezpieczeństwa informacyjnego***



## Wybory Prezydenckie w USA (2016):

- **Opis:** Rosnące zainteresowanie sprawą ingerencji Rosji w amerykańskie wybory prezydenckie.
- **Wpływ:** Kampanie dezinformacyjne miały na celu wprowadzenie zamętu, podsycanie podziałów społecznych i wpływanie na wynik wyborów.

## Brexit (2016):

- **Opis:** Kampania przed referendum ws. Brexitu.
- **Wpływ:** Wzrost dezinformacji dotyczącej konsekwencji wyjścia z UE, co wpłynęło na wybór wielu wyborców.

## Pandemia COVID-19 (2020-2021):

- **Opis:** Rozprzestrzenianie się dezinformacji dotyczącej pochodzenia, leczenia i skutków pandemii.
- **Wpływ:** Dezinformacja przyczyniła się do nieporozumień, oporu wobec środków bezpieczeństwa, a także podważania rzetelności informacji naukowej.

## Atak na Kliniki Wielkiej Brytanii (2017):

- **Opis:** Ransomware WannaCry zaatakował brytyjskie kliniki.
- **Wpływ:** Atak doprowadził do zakłócenia świadczenia opieki zdrowotnej, podkreślając zagrożenia związane z bezpieczeństwem cybernetycznym.

## Protesty w Hongkongu (2019):

Ogólnopolska Konferencja Naukowa
z cyklu ***Bezpieczeństwo informacyjne*** na temat:
***Informacje niejawne i prawnie chronione***
***w systemie bezpieczeństwa informacyjnego***

Wpływ propagandy na społeczeństwo i politykę jest istotnym zagadnieniem, które może kształtować opinie publiczną, wpływać na decyzje polityczne i kształtować społeczeństwo. Kluczowe aspekty tego wpływu:

## Kształtowanie Opinii Publicznej:

- Propaganda ma zdolność kształtowania opinii publicznej poprzez kontrolowanie przekazu i manipulację informacjami.
- Może wpływać na postrzeganie konkretnych wydarzeń, postaci politycznych czy ideologii.

## Podważanie Rzetelności Informacji:

- Propaganda często wprowadza zamęt w dostarczaniu rzetelnych informacji, co sprawia, że trudniej jest odróżnić prawdę od fałszu.
- Podważanie obiektywności mediów może prowadzić do utraty zaufania do instytucji informacyjnych.

## Manipulacja Emocjami:

- Propaganda często opiera się na manipulacji emocjami, wywoływaniu strachu, gniewu czy radości, aby wpłynąć na reakcje społeczeństwa.

## Podział Społeczeństwa:

- Poprzez podkreślanie istniejących podziałów lub tworzenie nowych, propaganda może prowadzić do polarizacji społeczeństwa.
- Podziały te mogą utrudniać dialog, współpracę i efektywne funkcjonowanie demokratycznego społeczeństwa.

## Wpływ na Wybory i Decyzje Polityczne:

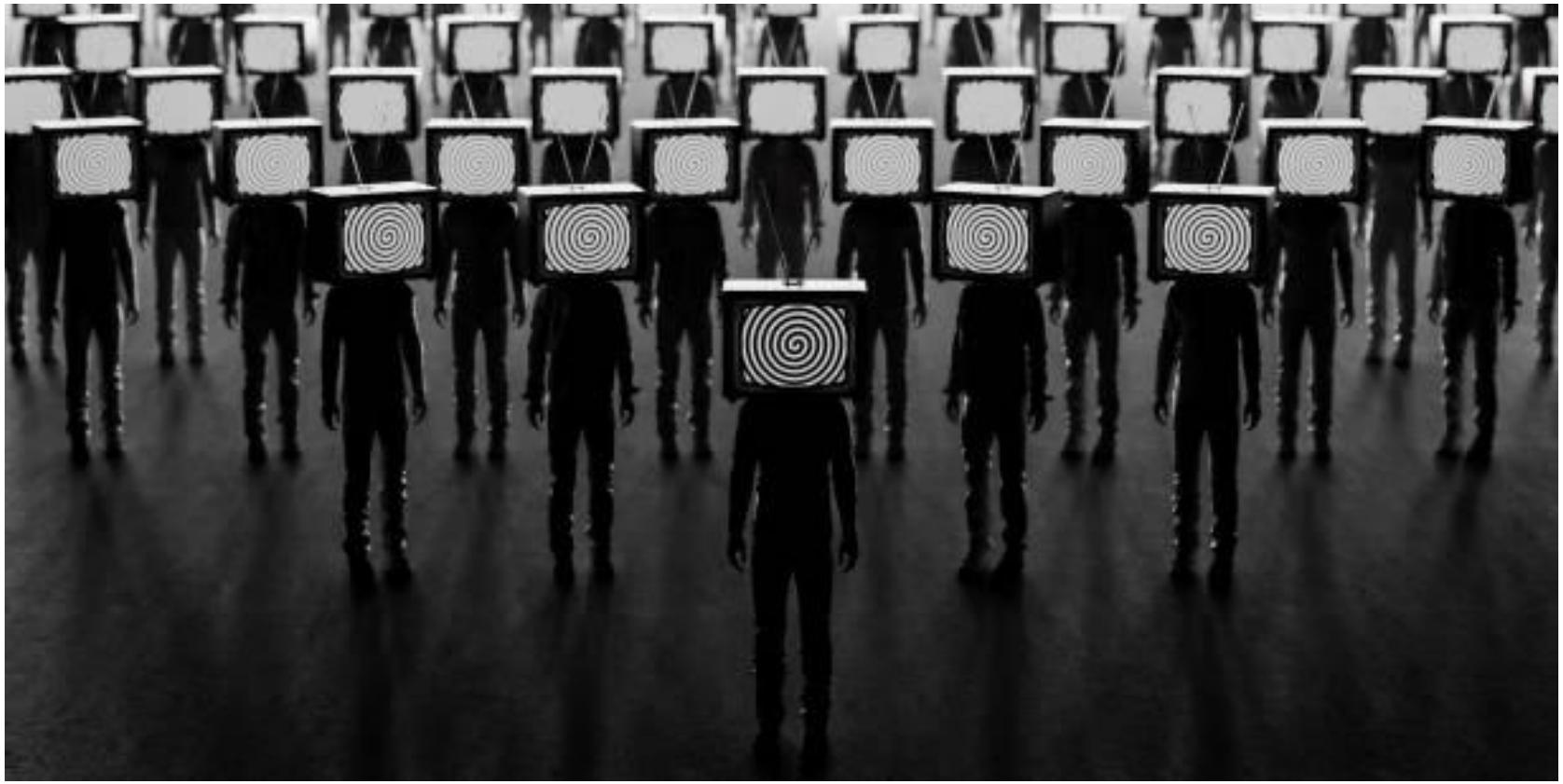
- Propaganda często jest używana w okresach wyborczych do wpływania na wyniki głosowania.
- Może także wpływać na decyzje polityczne, kształtując agendę publiczną i priorytety rządu.

## Osłabianie Krytycznego Myślenia:

- Propaganda może ograniczać zdolność społeczeństwa do krytycznej analizy informacji, prowadząc do przyjmowania przekazów bez głębszego zastanowienia.
- Osłabia to zdolność społeczeństwa do efektywnego uczestnictwa w procesach demokratycznych.

## Dezinformacja w Sferze Międzynarodowej:

Ogólnopolska Konferencja Naukowa
z cyklu ***Bezpieczeństwo informacyjne*** na temat:
***Informacje niejawne i prawnie chronione***
***w systemie bezpieczeństwa informacyjnego***



## Edukacja Społeczeństwa:

- **Rozwijanie Umiejętności Krytycznego Myślenia:** Włączenie edukacji medialnej do programów nauczania, które uczą ludzi analizy treści, identyfikacji dezinformacji i oceny źródeł informacji.
- **Świadomość Zagrożeń:** Edukowanie społeczeństwa na temat technik propagandy, metod manipulacji informacyjnej i zagrożeń związanych z dezinformacją.

## Współpraca Z Mediami:

- **Promowanie Standardów Etycznych:** Wspieranie mediów w przestrzeganiu wysokich standardów etycznych, rzetelności informacji i transparentności.
- **Zwiększanie Społecznej Odpowiedzialności Mediów:** Zachęcanie mediów do informowania społeczeństwa o próbach manipulacji oraz do aktywnego przeciwdziałania dezinformacji.

## Działania Rządowe:

- **Kreowanie Skutecznych Przepisów:** Tworzenie i egzekwowanie przepisów dotyczących dezinformacji i propagandy w celu karania ich autorów.
- **Transparentność Polityczna:** Zapewnianie transparentności działań polityków, aby ograniczyć

## Wsparcie Organizacji Społecznych:

- **Promowanie Faktu-Checkingu:** Wsparcie i promowanie organizacji zajmujących się faktu-checkingiem, które śledzą i korygują dezinformację.
- **Kampanie Edukacyjne:** Organizowanie kampanii edukacyjnych, które podnoszą świadomość społeczeństwa na temat technik propagandowych i skutków dezinformacji.

## Rozwój Narzędzi Technologicznych:

- **Technologie Analizy Treści:** Inwestowanie w rozwój technologii umożliwiających analizę treści w celu identyfikacji fałszywych informacji.
- **Algorytmy Przeciwdziałające Manipulacji:** Tworzenie i stosowanie algorytmów, które pomagają wykrywać i ograniczać rozprzestrzenianie się dezinformacji.

## Wzmacnianie Społeczeństwa Obywatelskiego:

- **Inicjatywy Społeczeństwa Obywatelskiego:** Wspieranie działań społeczeństwa obywatelskiego w zakresie monitorowania, raportowania i przeciwdziałania propagandzie.
- **Przeciwdziałanie Ekstremizmowi Online:** Działania na rzecz ograniczenia wpływu treści ekstremistycznych i manipulacyjnych w przestrzeni internetowej.

W zakończeniu rozważań na temat "Propaganda jako zagrożenie informacyjne" warto podkreślić, że świadomość mechanizmów propagandy oraz skuteczne przeciwdziałanie temu zagrożeniu są kluczowe dla zachowania zdrowego społeczeństwa. W erze powszechnego dostępu do informacji i rosnącej roli mediów społecznościowych, edukacja, współpraca z mediami, i rozwijanie umiejętności krytycznego myślenia stają się niezbędne. Przemiany w dziedzinie technologii wymagają także ciągłego rozwoju narzędzi analizy treści oraz algorytmów przeciwdziałających manipulacji informacyjnej. Tylko poprzez wspólną mobilizację społeczeństwa, mediów, rządu, i organizacji społecznych możemy skutecznie bronić się przed wpływami propagandy i chronić integralność informacyjną naszego społeczeństwa.

# Bibliografia

1. K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008
2. W. Fehler, *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021
3. Ł. Olejnik , *Propaganda. Od dezinformacji i wpływu do operacji i wojny informacyjnej*, Warszawa 2024
4. E.L.Bernays, *Propaganda*, Wrocław 2022

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Przestępczość internetowa

Katsiaryna Vysotskaya, katerinavysockaya@gmai.com

Centralna Bibliateka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Przestępczość internetowa

Katsiaryna Vysotskaya

Rewolucja informacyjna, jest wynikiem szybkiego rozwoju i powszechności światowej sieci (tzw. efekt informatyczny), przyczyniła się do znaczącej transformacji współczesnego społeczeństwa. Zmiany te objęły zarówno styl życia jednostek, jak i funkcjonowanie całych społeczności, wywołując zróżnicowane efekty socjologiczno-psychologiczne. Ponadto, rewolucja informacyjna zredefiniowała rolę państwa, generując znaczące implikacje polityczno-prawne.

# Przestępczość internetowa

Katsiaryna Vysotskaya

W sieci internetowej obserwuje się występowanie szeregu zjawisk o charakterze niezwykle groźnym, które stanowią zagrożenie dla praw i wolności jednostki. Te zjawiska często naruszają prywatność, godność, dobre imię oraz cześć jednostek, a także są skierowane przeciwko integralności środków przekazu. Ich istota polega na nieuprawnionym dostępie do informacji. Dla sprawcy tych przestępstw, internet jest jedynie narzędziem lub środkiem służącym do popełnienia czynu zabronionego.

# Przestępczość internetowa

Katsiaryna Vysotskaya

W ostatnich latach zaobserwowano narastanie zagrożenia w postaci cyberterroryzmu, które stanowi poważne wyzwanie dla podstaw funkcjonowania demokratycznych państw oraz stabilności stosunków międzynarodowych. Niektóre działania cyberterrorystyczne bezpośrednio zagrażają bezpieczeństwu publicznemu poprzez atakowanie sił zbrojnych, organów bezpieczeństwa państwa oraz dążenie do wywołania paniki społecznej. Te incydenty mogą skutkować poważnymi konsekwencjami dla społeczeństwa i państwa jako całości.

Przestępczość internetowa manifestuje się w różnorodnych formach i objawia się poprzez szeroki wachlarz działań. Główne kategorie przestępczości internetowej:

- **Phishing (Oszustwa internetowe)**
- **Malware (Złośliwe oprogramowanie)**
- **Ataki hakerskie**
- **Ataki DDoS (Distributed Denial of Service)**
- **Kradzież tożsamości**
- **Handel dziećmi**
- **Naruszenie prywatności**
- **Oszustwa finansowe**
- **Nękanie onlin**
- **Cyberterroryzm**

- Phishing, jest formą oszustwa internetowego, opiera się na próbach pozyskania poufnych danych, takich jak hasła, numery kart kredytowych czy informacje osobiste, poprzez podszywanie się pod instytucje lub osoby oznaczone jako wiarygodne.

- Malware, czyli złośliwe oprogramowanie, obejmuje różnorodne rodzaje wirusów komputerowych, trojanów, robaków i inne formy, które są przeznaczone do infekowania systemów komputerowych i powodowania szkód. Szkody te mogą obejmować kradzież danych, zniszczenie plików oraz inne niepożądane działania.

Katsiaryna Vysotskaya

- Ataki hakerskie to próby nieautoryzowanego dostępu do systemów komputerowych, sieci lub stron internetowych w celu kradzieży, modyfikacji lub zniszczenia danych. Ich celem jest często uzyskanie poufnych informacji lub zakłócenie normalnego funkcjonowania systemu lub sieci.


- Ataki DDoS (rozproszone ataki odmowy usługi) polegają na przeciążeniu serwera lub sieci poprzez wysyłanie dużej liczby żądań, co prowadzi do niedostępności usług dla prawidłowych użytkowników. Ich celem jest sparaliżowanie działania systemu poprzez przeciążenie jego zasobów, uniemożliwiając tym samym dostęp do usług dla innych użytkowników.

Katsiaryna Vysotskaya

- Kradzież tożsamości to proceder polegający na pozyskiwaniu i wykorzystywaniu danych osobowych innej osoby bez jej zgody, w celu popełnienia przestępstw, często dotyczących oszustw finansowych.

- Handel pornografią dziecięcą, to nielegalna praktyka wykorzystująca internet do handlu pornografią dziecięcą lub do rekrutowania ofiar.

- Naruszenia prywatności to nielegalna praktyka polegająca na zbieraniu, przechowywaniu lub publikowaniu prywatnych informacji osób bez ich zgody.

- Oszustwa finansowe obejmują różnego rodzaju działania, takie jak kradzież kart kredytowych, fałszerstwa finansowe online oraz oszustwa związane z handlem elektronicznym.

Katsiaryna Vysotskaya

- Nękanie online polega na wykorzystywaniu internetu do nękania, szantażowania lub zastraszania innych osób.


- Cyberterroryzm to wykorzystywanie internetu w celu przeprowadzania aktów terroryzmu, które mogą obejmować ataki na infrastrukturę krytyczną lub inne formy destabilizacji społeczeństwa za pomocą działań online.

Departament Obrony Stanów Zjednoczonych zdefiniował cyberprzestrzeń jako współzależną i powiązaną sieć infrastrukturalną technologii informacyjnej, która obejmuje internet, sieci telekomunikacyjne, systemy komputerowe oraz systemy zarządzające procesami produkcji i kontroli w sektorach strategicznych dla bezpieczeństwa narodowego. Pojęcie "cyberprzestrzeni" jest stosowane jako synonim dla "sieci".

Literatura przedmiotu proponuje definicję "cyberprzestrzeni globalnej" jako systemu wymiany i przetwarzania informacji (danych), który działa zgodnie z formalnymi zasadami i przepisami prawnymi obowiązującymi na terytorium poszczególnych państw. Ten system funkcjonuje dzięki połączeniu zasobów technicznych zlokalizowanych na terytorium każdego z nich.

# System prawny wobec przestępstw w cyberprzestrzeni

W polskim systemie prawnym definicja cyberprzestrzeni została wprowadzona w Ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.

System prawny wobec przestępstw w cyberprzestrzeni różni się w zależności od państwa, jednak zazwyczaj obejmuje kilka kluczowych aspektów mających na celu zwalczanie przestępczości internetowej.

# Definicje i klasyfikacje przestępstw

System prawny musi precyzyjnie definiować różne rodzaje przestępstw internetowych, takie jak hakerstwo, phishing, ataki DDoS, kradzież tożsamości, pornografia dziecięca, cyberterroryzm itp. Klasyfikacja i definicje są istotne, aby organy ścigania mogły ścigać sprawców zgodnie z prawem.

# Jurysdykcja i współpraca międzynarodowa

W związku z globalnym charakterem przestępczości internetowej, system prawny powinien uwzględniać kwestie jurysdykcji oraz współpracy międzynarodowej. Wiele przypadków przestępczości internetowej obejmuje sprawców i ofiary z różnych krajów, co wymaga współpracy międzynarodowej w celu ścigania i wymierzania sprawiedliwości.

# Przepisy dotyczące ścigania

System prawny musi precyzyjnie określać uprawnienia i procedury dla organów ścigania w zakresie dochodzenia w sprawach przestępstw internetowych. W tym celu należy uwzględnić zdolność organów ścigania do zbierania elektronicznych dowodów, monitorowania działań w cyberprzestrzeni oraz współpracy z dostawcami usług internetowych. Dzięki klarownym przepisom prawnym organy ścigania mogą skutecznie prowadzić dochodzenia i ścigać sprawców przestępstw internetowych.

# Kary i sankcje

Przepisy prawne powinny dokładnie określać rodzaje kar i sankcji, jakie mogą być nałożone na sprawców przestępstw internetowych. W ramach tych przepisów przewidziane mogą być różnorodne kary, włączając w to grzywny, kary więzienia oraz konfiskatę mienia. Odpowiednie sankcje powinny być stosowane w zależności od charakteru i ciężkości popełnionego przestępstwa, aby zapewnić skuteczną ochronę praw i bezpieczeństwo w cyberprzestrzeni.

## Ochrona ofiar

System prawny powinien uwzględniać ochronę ofiar przestępstw internetowych, zapewniając im pełne prawa do prywatności, wsparcie psychologiczne oraz dostęp do innych środków pomocy. W ramach tych przepisów należy zapewnić ofiarom odpowiednie środki ochrony przed dalszymi atakami lub naruszeniami ich prywatności w cyberprzestrzeni.

## Bezpieczeństwo cyberprzestrzeni

System prawny winien uwzględniać regulacje dotyczące bezpieczeństwa cyberprzestrzeni, kładąc nacisk na wymaganie stosowania odpowiednich środków zabezpieczających dla systemów informatycznych i danych. Te działania są niezbędne dla zapewnienia integralności, poufności i dostępności danych w cyberprzestrzeni.

## Edukacja i prewencja

W ramach systemu prawnego można zastosować środki związane z edukacją społeczeństwa na temat zagrożeń w cyberprzestrzeni oraz prewencją przestępstw internetowych. Te środki mogą obejmować kampanie informacyjne, programy edukacyjne w szkołach i instytucjach publicznych, a także wsparcie finansowe dla organizacji pozarządowych i instytucji badawczych zajmujących się tematyką bezpieczeństwa w cyberprzestrzeni.

## Przepisy dotyczące prywatności

W kontekście przestępczości internetowej, system prawny musi równoważyć ochronę prywatności użytkowników z koniecznością zbierania danych w celu ścigania przestępstw. Jest to wyzwanie, które wymaga ustanowienia przepisów prawnych, które zapewnią użytkownikom internetu odpowiednią ochronę prywatności, jednocześnie umożliwiając organom ścigania dostęp do niezbędnych danych w celu dochodzenia w sprawach przestępstw internetowych.

# Przestępczość internetowa

Katsiaryna Vysotskaya

System prawny wobec przestępstw w cyberprzestrzeni musi być elastyczny i dostosowany do ciągłych zmian w charakterze zagrożeń oraz skomplikowanej struktury przestępczej w tej dziedzinie. Aktualizacja i dostosowywanie przepisów do dynamicznego środowiska cybernetycznego są kluczowe dla skutecznego zwalczania przestępczości internetowej. W tym kontekście konieczne jest ciągłe monitorowanie i analiza nowych technologii oraz metod stosowanych przez przestępców, aby zapewnić odpowiednie ramy prawne, które będą skuteczne w zwalczaniu różnorodnych form przestępczości internetowej.

# Ustawodawstwo wobec przestępstw w cyberprzestrzeni

Ustawodawstwo dotyczące przestępstw w cyberprzestrzeni obejmuje zbiór przepisów prawnych, które definiują różnorodne rodzaje działań uznawanych za przestępstwa internetowe oraz określają sankcje nakładane na sprawców. W kontekście przestępstw internetowych istnieją zarówno międzynarodowe akty prawne, które mają zastosowanie na poziomie globalnym, jak i przepisy państwowe, które regulują kwestie prawne w ramach danego kraju. Te regulacje obejmują zakres działań, takich jak cyberprzemoc, oszustwa internetowe, naruszenia prywatności, cyberterroryzm, pornografia dziecięca i wiele innych. Ustawodawstwo to jest kluczowe dla zapewnienia odpowiedniego ram prawnych w celu ścigania i karania sprawców przestępstw internetowych oraz ochrony praw ofiar.

# Międzynarodowe akty prawne

Kilka kluczowych międzynarodowych aktów prawnych dotyczących zwalczania cyberprzestępczości i współpracy międzynarodowej w ściganiu sprawców:

**Konwencja Rady Europy o Cyberprzestępczości (Budapesztańska Konwencja):**

Przyjęta w 2001 roku, konwencja ta jest pierwszym międzynarodowym instrumentem prawny obejmującym przestępstwa popełniane w Internecie. Określa standardy dotyczące definicji przestępstw internetowych, środków ścigania oraz współpracy międzynarodowej.

## Europejska Konwencja o Cyberprzestępczości (Konwencja z Budapesztu):

Konwencja ta, obejmuje obszerne postanowienia dotyczące przeciwdziałania cyberprzestępczości poprzez definicje konkretnych przestępstw internetowych, takich jak hakerstwo, oszustwa komputerowe, przestępstwa związane z pornografią dziecięcą itp. Ponadto nakłada na państwa członkowskie obowiązek dostosowania swoich praw i procedur karnych do celów konwencji oraz współpracy międzynarodowej w zakresie ścigania przestępstw internetowych.

## Międzynarodowa Konwencja o Zwalczaniu Przestępczości Komputerowej (Budapeszta 2.0):

Przyjęta w 2021 roku, jest to rozwinięcie poprzednich konwencji i stanowi próbę dostosowania prawa międzynarodowego do nowoczesnych wyzwań związanych z cyberprzestępczością.

## Inicjatywy ONZ:

Organizacja Narodów Zjednoczonych (ONZ) podejmuje inicjatywy mające na celu koordynację międzynarodowych wysiłków w zwalczaniu cyberprzestępczości. Jednym z owoców tych działań jest "Raport Sekretarza Generalnego ONZ o Cyberprzestępczości i Międzynarodowym Bezpieczeństwie", który stanowi dokument analizujący współczesne zagrożenia w cyberprzestrzeni oraz zalecenia dotyczące środków zapobiegawczych i działań przeciwdziałających.

## Dyrektywa Unii Europejskiej w sprawie Cyberbezpieczeństwa (NIS Directive):

Przyjęta w 2016 roku, ta dyrektywa nakłada obowiązki na państwa członkowskie w zakresie zwiększenia odporności krytycznej infrastruktury na cyberzagrożenia.

## Akt o Cyberprzestępczości (Cybercrime Act) Wspólnoty Karibskiej:

Przyjęty w 2018 roku przez Wspólnotę Karibską, ten akt ma na celu zwalczanie cyberprzestępczości w regionie Karaibów.

## Porozumienie o Wzajemnej Pomocy Prawnej w Sprawie Cyberprzestępczości (MLATs):

To umowy międzyrządowe, które umożliwiają krajom współpracę w dochodzeniach dotyczących cyberprzestępczości, wymieniając informacje i udzielając pomocy prawnej.

# Akty prawne w Polsce wobec przestępstw w cyberprzestrzeni

W Polsce ustawodawstwo dotyczące przestępstw w cyberprzestrzeni ewoluowało w odpowiedzi na rosnące wyzwania związane z cyberprzestępczością.

Kodeks Karny (KK):

Art. 267 KK:

Dotyczy nielegalnego dostępu do informacji informatycznej.

Art. 269 KK:

Obejmuje hakerstwo polegające na zakłócaniu funkcjonowania systemu informatycznego.

Art. 287 KK:

Kradzież danych informatycznych.

Art. 287a KK:

Nielegalne wprowadzanie programu komputerowego lub innego danych informatycznych.

**Ustawa o Ochronie Danych Osobowych (RODO):**

Ustawa ta reguluje zasady przetwarzania danych osobowych, a jej naruszenie może prowadzić do sankcji administracyjnych oraz konsekwencji karnych.

**Ustawa o Ochronie Systemów Informatycznych:**

Przepisy te regulują zagadnienia związane z bezpieczeństwem systemów informatycznych, w tym obowiązki operatorów systemów oraz reakcję na incydenty bezpieczeństwa.

**Ustawa o Krajowym Systemie Cyberbezpieczeństwa:**

Określa zasady funkcjonowania Krajowego Systemu Cyberbezpieczeństwa oraz obowiązki podmiotów zarządzających infrastrukturą krytyczną.

**Ustawa o Przeciwdziałaniu Przestępczości Informatycznej:**

Obejmuje kwestie związane z przeciwdziałaniem przestępczości informatycznej, w tym definicje przestępstw, procedury ścigania, kary oraz współpracę międzynarodową.

**Ustawa o Narodowym Centrum Cyberbezpieczeństwa:**

Określa zadania i kompetencje Narodowego Centrum Cyberbezpieczeństwa, które jest odpowiedzialne za koordynację działań w obszarze cyberbezpieczeństwa.

**Ustawa o Środkach Bezpieczeństwa Informacji:**

Reguluje kwestie związane z ochroną informacji niejawnych i wprowadza środki bezpieczeństwa w zakresie przetwarzania tych informacji.

**Ustawa o Zarządzaniu Kryzysowym:**

Określa zasady zarządzania kryzysowego, w tym reakcję na sytuacje kryzysowe w cyberprzestrzeni.

# Przestępczość internetowa

Katsiaryna Vysotskaya

Przestępczość internetowa przybiera różne formy i obejmuje szeroki zakres działań, takich jak oszustwa finansowe, nękanie online, kradzież tożsamości czy cyberterroryzm. Ustawodawstwo powinno precyzyjnie definiować, co jest uznawane za nielegalne w kontekście cyberprzestępczości, aby umożliwić skuteczne ściganie sprawców. Ponadto, zasady i mechanizmy współpracy międzynarodowej odgrywają istotną rolę w zwalczaniu przestępczości internetowej, w tym procedury ekstradycji sprawców między państwami.

# Bibliografia

Berdel-Dudzińska M., Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym, „Przegląd Prawa Publicznego" 2012, nr 2.

Bógdał-Brzezińska A., Gawrycki M.F., Cyberterroryzm i problem bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003.

Kosiński J., Cyberprzestępczość [w:] W. Jasiński, W. Mądrzejowski, K. Wiciak, (red.), Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne, Szczytno 2013.

Korcz, I. (2005). Internet a człowiek w kontekście globalizującego się świata. In M. Sokołowski (Ed.) Oblicza Internetu. Internet a globalne społeczeństwo informacyjne.[The faces of the Internet. The Internet and the global information socjety]. Elbląg: Instytut Informatyki Stosowanej PWSZ w Elblągu.Sokołowski, M. Furmanek (red.) Oblicza Internetu. Internet a globalne społeczeństwo informacyjne, Elbląg 2005.

Nowak A., Cyberprzestrzeń jako nowa jakość zagrożeń, „Zeszyty Naukowe Akademii Obrony Narodowej" 2013, nr 3.

https://www.gov.pl/web/gov/szukaj?query=Kodeks+Karny+art+267&category=kategoria&page=1&size=25 (data dostępu: 20/12/2023)

https://www.gov.pl/web/cyfryzacja/ustawa-o-krajowym-systemie-cyberbezpieczenstwa-weszla-w-zycie (data dostępu: 20/12/2023)

https://www.gov.pl/web/psse-gniezno/ustawa-o-ochronie-danych-osobowych (data dostępu: 20/12/2023)

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Kradzież tożsamości jako zagrożenie dla bezpieczeństwa informacyjnego

Adrian Kowalczyk, ak88415@stud.uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

Adrian Kowalczyk

- Czym jest kradzież tożsamości?

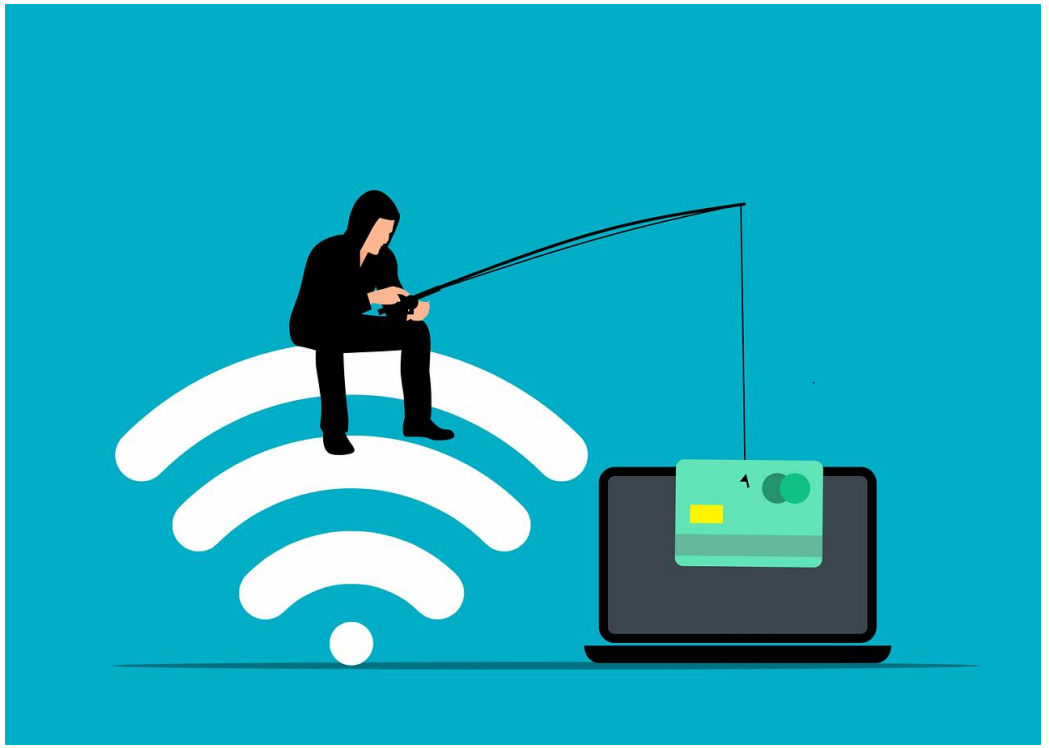
O kradzieży tożsamości mówimy w sytuacji, w której ktoś bezprawnie wejdzie w posiadanie danych osobowych innej osoby i wykorzysta je wbrew jej woli. Mówiąc wprost – podszywa się pod inną osobę, zazwyczaj w celu osiągnięcia korzyści majątkowej.

Zakres danych i ich bezprawne wykorzystanie, traktowane jako kradzież, może być bardzo różne. Niekiedy może być to nazwa użytkownika i hasło do forum internetowego, ale może to być również pełen zakres danych personalnych, które wykorzystane są do wyłudzenia kredytu.

# Metody kradzieży tożsamości

- Phishing

Jest to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.



# Metody kradzieży tożsamości

- Pharming

Polega na modyfikacji zawartości adresu www w celu przekierowania użytkownika na fałszywą stronę, mimo wpisania prawidłowego adresu strony. Ma to na celu przejęcie wpisywanych przez użytkownika do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych.

# Metody kradzieży tożsamości

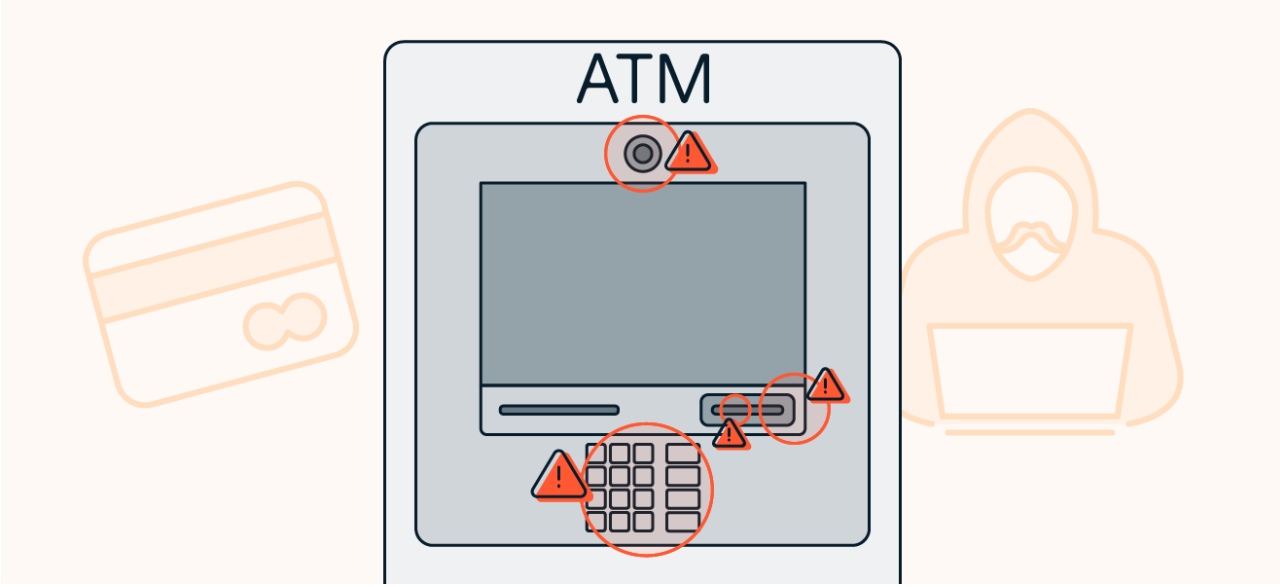
- Keylogging

Odnosi się do korzystania z oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika. Na ogół są spotykane w wersji programowej, rzadziej w sprzętowej.

# Metody kradzieży tożsamości

- Skimming

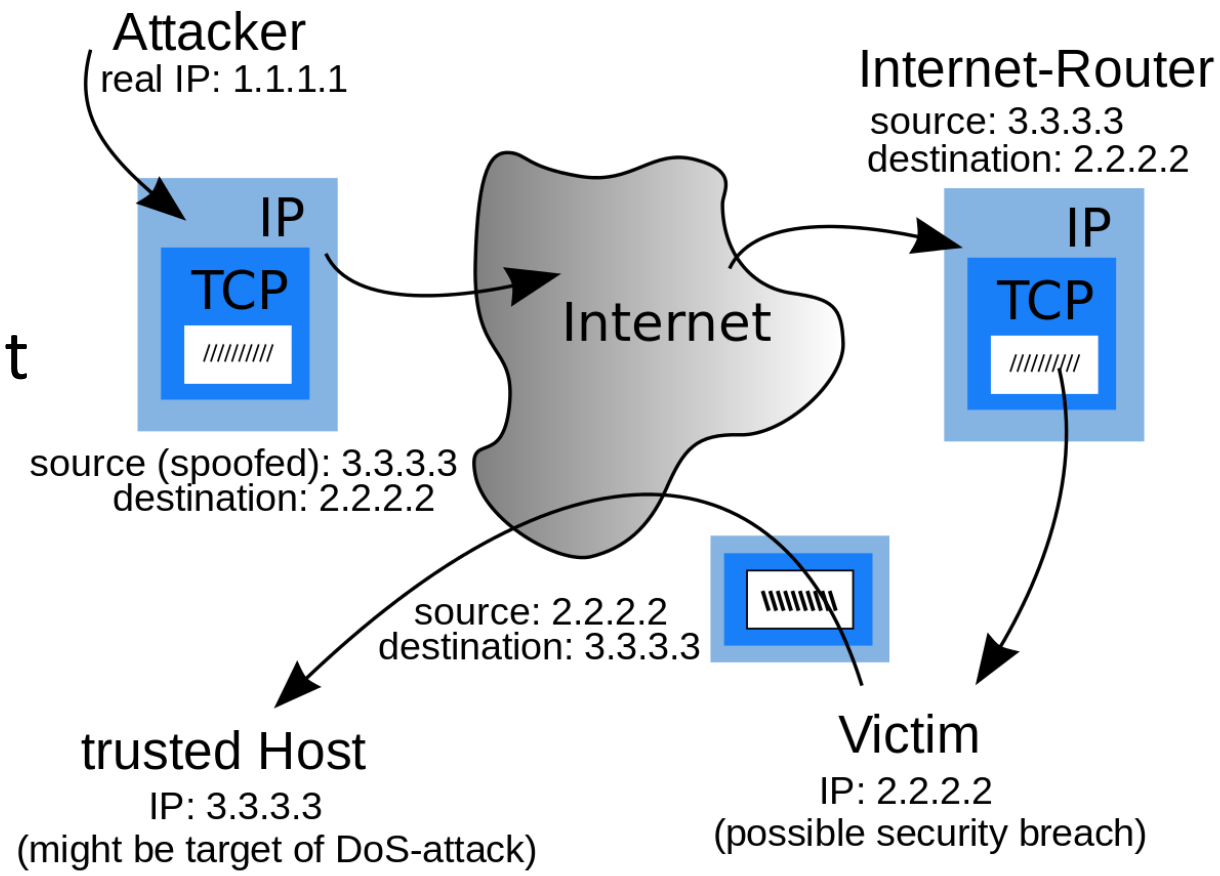
Jest to przestępstwo polegające na nielegalnym skopiowaniu zawartości paska magnetycznego karty płatniczej bez wiedzy jej posiadacza w celu wytworzenia kopii i wykonywania nieuprawnionych płatności za towary i usługi lub wypłat z bankomatów.



# Metody kradzieży tożsamości

- Spoofing

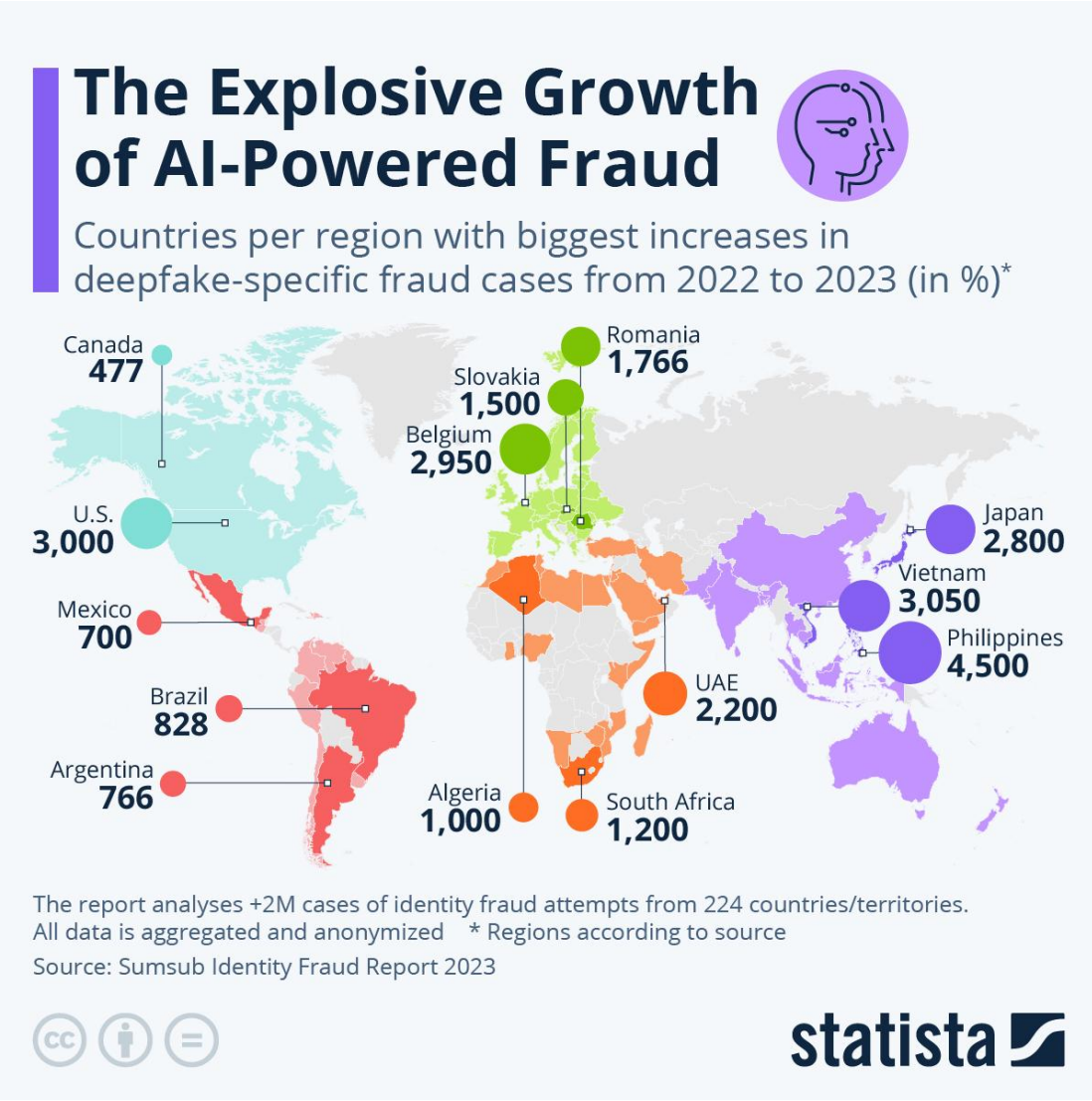
Grupa ataków na systemy teleinformatyczne, polegająca na podszywaniu się pod inny element tego systemu. Efekt ten osiągany jest poprzez umieszczanie w sieci preparowanych pakietów danych lub niepoprawne używanie protokołów.



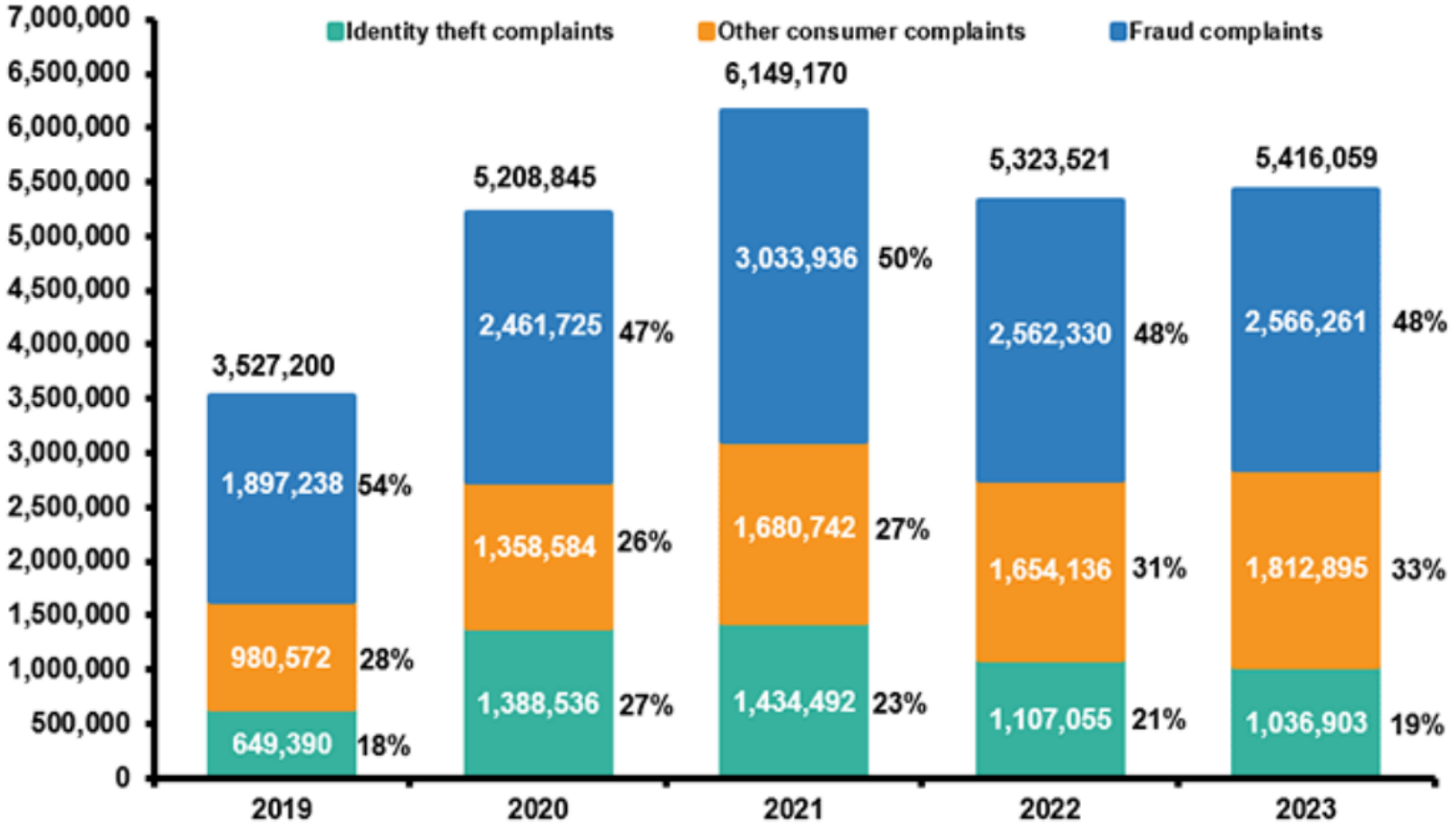
# Metody kradzieży tożsamości

- Deepfake

Jest to technika wykorzystująca sztuczną inteligencję do tworzenia fałszywych wideo, imitujących autentyczne nagrania. Niesie ze sobą poważne konsekwencje dla społeczeństwa, ponieważ wpływa na percepcję faktów i rzeczywistości.



# Raporty dotyczące kradzieży tożsamości i oszustw w latach 2019–2023 w Stanach Zjednoczonych



- Pięć najpopularniejszych rodzajów kradzieży tożsamości w USA, 2023

| Type of identity theft | Number of reports | Percent of total top five |
|---|---|---|
| Credit card fraud-new accounts | 381,122 | 42.0% |
| Miscellaneous identity theft (2) | 279,221 | 30.7 |
| Bank fraud-new accounts | 84,335 | 9.3 |
| Government benefits fraud-applied for/received | 82,419 | 9.1 |
| Loan fraud-business/personal loan | 81,342 | 9.0 |
| **Total, top five** | **908,439** | **100.0%** |

# Przykłady znanych przypadków kradzieży tożsamości

- Nicole McCabe

Wyobraź sobie, że zostałeś wrobiony w zabójstwo przywódcy Hamasu. To właśnie przydarzyło się Nicole McCabe, której tożsamość została rzekomo skradziona w 2010 roku przez izraelską agencję wywiadowczą Mossad i została użyta w zamachu na Mahmouda Al-Mabhouha w Dubaju. Nicole o zabójstwie usłyszała w radio i była zszokowana, gdy speaker wymienił jej nazwisko jako podejrzanej. Okazało się, że zabójcy wykradli jej tożsamości i dwóch innych Australijczyków oraz wielu osób z Wielkiej Brytanii, Irlandii, Francji i Niemiec. Na szczęście sprawa została szybko wyjaśniona przez władze i Nicole nie została oskarżona o współudział w zamachu.

# Przykłady znanych przypadków kradzieży tożsamości

- Phillip Cummings

Jednym z najsłynniejszych przypadków kradzieży tożsamości był przypadek Phillipa Cummingsa. 35-latek pracował w małej firmie programistycznej Teledata Communications od 1999 do 2000 roku i w tym czasie ukradł raporty kredytowe 33 tysięcy osób w całych Stanach Zjednoczonych. Cummings i jego wspólnik sprzedali te informacje przestępcom, którzy wyłudzili niemal 100 milionów dolarów.

# Przykłady znanych przypadków kradzieży tożsamości

- David Matthew Read

W 2018 roku 35-letni David Matthew Read podszył się pod aktorkę Demi Moore i zgłosił, że jej karta American Express została skradziona. Uzyskał jej numer SSN i inne dane osobowe on-line, a następnie udając osobistego asystenta przechwycił nową kartę w FedEx. Ze skradzioną kartą udał się na zakupy i wydał 169 tysięcy dolarów w luksusowych sklepach w Nowym Jorku. Został jednak zidentyfikowany za pomocą kamer monitoringu.

# Przykłady znanych przypadków kradzieży tożsamości

- Oszustwo deepfake i ogromny przelew

Na początku tego roku pracownik międzynarodowej firmy w Hongkongu otrzymał wiadomość z poleceniem wykonania przelewu. Autorem komunikatu miał być dyrektor finansowy firmy z siedzibą w Wielkiej Brytanii. Mężczyzna nie uwierzył w otrzymanego maila i początkowo przypuszczał, że ma do czynienia z oszustwem. Potem miała jednak miejsce wideo rozmowa z członkami zarządu, których wygląd oraz brzmienie głosu do złudzenia przypominały cechy prawdziwych osób na tych stanowiskach. Pracownik finalnie wykonał przelew w wysokości 200 milionów dolarów hongkońskich, co w przeliczeniu daje odpowiednio ok. 103 miliony złotych. Przestępców nie odnaleziono do teraz.

Bibliografia:


- https://www.statista.com/chart/31901/countries-per-region-with-biggest-increases-in-deepfake-specific-fraud-cases/
- https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
- https://forsal.pl/lifestyle/technologie/artykuly/9426806,rekordowy-przekret-na-deepfake-oszusci-ukradli-25-mln-dolarow.html
- https://forsal.pl/lifestyle/technologie/artykuly/9465305,jak-niebezpieczne-sa-deepfakes-i-inne-oszustwa-wykorzystujace-sztuczna.html
- https://qdpr.pl/manipulacja-i-kradziez-tozsamosci-ai-kontra-rzeczywistosc
- https://bezpiecznewybory.pl/baza-wiedzy/kradziez-danych-w-internecie
- https://ochronatozsamosci.pl/blog/5-zuchwalych-przypadkow-kradziezy-tozsamosci-o130gc3-one.html
- Mirski, A., Barcik, M., & Gawron, M. (2015). *Kradzież tożsamości w Internecie*.
- Protasowicki, I. (2016). *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci. Zeszyty Naukowe WSIZiA*, (4), 37.

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Szpiegostwo jako zagrożenie dla bezpieczeństwa informacyjnego państwa

Maciej Tyszkiewicz,
mt88416@stud.uws.edu.pl
Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

- Szpiegostwo to działalność polegająca na pozyskiwaniu wrażliwych i wartościowych informacji oraz przekazywaniu ich określonemu odbiorcy.

Można wyróżnić następujące rodzaje szpiegostwa mające wpływ na bezpieczeństwo informacyjne państwa:

- gospodarcze,
- przemysłowe,
- cyberszpiegostwo.

- Szpiegostwo gospodarcze prowadzi się w celu zdobycia informacji na temat rozwoju przemysłu zbrojeniowego oraz działalności naukowo-technicznej.

- Szpiegostwo przemysłowe prowadzone jest w celu uzyskania przewagi na określonych rynkach.

- Celem cyberszpiegów jest zdobycie informacji przechowywanych cyfrowo.

- Szpiegostwo niesie ze sobą poważne skutki, takie jak zagrożenie bezpieczeństwa państwa oraz uzyskanie przez inne państwo informacji na temat strategiczny.

- W celu ochrony przed szpiegostwem powinno się dokładnie sprawdzać ludzi  przed ich zatrudnieniem, przeprowadzać inspekcję na obecność urządzeń, których może używać szpieg, podrzucać fałszywe informację i zobaczyć, gdzie zostaną udostępnione.

- W Polsce wyspecjalizowanymi służbami przeciw zwalczaniu obcych wywiadów są Agencja Bezpieczeństwa Wewnętrznego (ABW)i Służba Kontrwywiadu Wojskowego (SKW).

- Grzelak M., Wpływ szpiegostwa internetowego na stosunki między USA a Chinami. *Bezpieczeństwo Narodowe*, (2), 2013
- Nyzio A.,O szpiegach, szpiegostwie i polskim kontrwywiadzie, 2023
- Żebrowski A., Zagrożenia i bezpieczeństwo przemysłu zbrojeniowego u progu XXI wieku (wybrane aspekty), 2016
- http://www.iniejawna.pl/pomoce/szpieg_2.html [dostęp 6.05.2024 r.].

Ogólnopolska Konferencja Naukowa z cyklu ***Bezpieczeństwo informacyjne***

na temat:

***Informacje niejawne i prawnie chronione***

***w systemie bezpieczeństwa informacyjnego***

# Stalking jako przestępstwo w sferze informacyjnej

Weronika Rechnio, wr88851@stud.uws.edu.pl

Centralna Biblioteka Wojskowa
Warszawa, 16-17 maja 2024 r.

# Początki stalkingu

Etymologia słowa „stalking" związana jest z pojęciem odnoszącym się do żargonu myśliwskiego. „To stalk" należy tłumaczyć jako skradanie się, chodzenie, skrywanie się, a są to określenia czynności wykonywanych przez kłusownika, który poluje na zwierzynę.

# Początki stalkingu

W 1989 roku po raz pierwszy użyto słowa „stalker” na określenie sprawcy prześladowania. Media informowały wówczas o przypadkach stalkingu dotyczących gwiazd showbiznesu, m.in. o zamordowaniu aktorki Rebecci Scheaffer przez chorego psychicznie fana. Kilka lat wcześniej ofiarą stalkera stał się John Lennon, który został zastrzelony przez swego „psychofana”. Sprawcami stalkingu w tamtym okresie byli przede wszystkim chorzy, posiadający pewne zaburzenia psychiczne, fani. Zaczęto wówczas postrzegać stalking jako zapowiedź przemocy, której sprawca może w przyszłości użyć wobec swojej ofiary.

# Czym jest stalking?

Według definicji, stalking to naprzykrzanie się, prześladowanie jakiejś osoby i naruszanie jej prywatności. Za stalking uznaje się również podszywanie się pod ofiarę i wykorzystywanie jej wizerunku oraz danych osobowych w celu wyrządzenia szkody osobistej lub majątkowej.

Zjawisko te obejmuje wiele różnych zachowań, m.in.: ciągłe wysyłanie e-maili i SMS-ów, wydzwanianie, pogróżki, śledzenie, nachodzenie ofiary w domu lub pracy, ciągłe obserwowanie, a nawet nachalne obdarowywanie prezentami. Warto jednak podkreślić, że za stalking uznaje się co najmniej kilkukrotne nękanie ofiary.

# Stalking w Internecie

Stalkerzy bardzo często wykorzystują narzędzia internetowe do swoich działań. Przykładem może być wysyłanie obraźliwych wiadomości lub maili z pogróżkami kilka razy dziennie. Obecnie, stalkerzy koncentrują się głównie na serwisach społecznościowych, gdzie wiele osób chętnie dzieli się informacjami na temat swojego życia osobistego. Dzięki czemu stalkerzy mogą bez problemu podszywać się pod swoją ofiarę, zakładając jej fałszywy profil na Facebooku lub Instagramie. Dodatkowo, takie konta wykorzystywane są przez przestępców internetowych do wysyłania niepokojących wiadomości.

Stalkerzy, obserwując działania swojej ofiary na serwisie społecznościowym, mogą zobaczyć co komentuje, czym się interesuje, do jakich wydarzeń dołącza i gdzie można ją spotkać. Jest to dla nich największe źródło informacji.

# Rodzaje stalkingu

Stalking można podzielić na trzy rodzaje, uwzględniając stopień zażyłości pomiędzy ofiarą a sprawcą:

1. **After – intimate – relationship – stalking** występuje najczęściej, gdyż sprawca i ofiara dobrze się znają: byli w przeszłości parą, kolegami, sąsiadami, przyjaciółmi.

2. **Acquaintance – Stalking**, występuje przy mniejszym stopniu zażyłości oraz znajomości. Ofiara i sprawca mogli kiedyś przypadkowo się poznać lub spotkać, lecz nie nawiązali bliższego kontaktu.

3. **Stranger – Stalking**, dotyka najczęściej ludzi sławnych, gdyż w tym przypadku ofiara nigdy nie poznała osobiście sprawcy.

# Rodzaje stalkingu

Podziału stalkingu można dokonać także ze względu na rodzaj czynności, które są podejmowane przez sprawcę. Wówczas za kryterium rozróżniające przyjmuje się zachowania stanowiące naruszenie przestrzeni prywatnej ofiary, z wykorzystaniem środków przekazu i kontaktu, w tym nowoczesnych technik informatycznych i telekomunikacyjnych, jak też podejmowanie działań wobec rodziny ofiary i jej przyjaciół. Zachowania stalkera mogą być zarówno bezpośrednie, gdy sprawca samodzielnie nęka swoją ofiarę, jak i pośrednie – przy korzystaniu z pomocy innych osób lub narzędzi, które pozwalają zachować anonimowość.

# Motywy stalkingu

1. Zaburzenia osobowości (graniczne i narcystyczne)
2. Nieprawidłowe relacje w rodzinie
3. Brak zaufania w społeczeństwie
4. Emancypacja kobiet

# 1. Zaburzenia osobowości (graniczne i narcystyczne)

Zaburzenia graniczne wiążą się z nadmiernym strachem przed porzuceniem. Stalkerzy posiadający ten typ zaburzeń mają przekonanie, iż same są ofiarami, choć to one prześladują inne osoby. Uzasadnieniem takiego zachowania sprawcy może być to, że osoby te posiadają niską samoocenę, a wszelkiego rodzaju odrzucenie przez innych ludzi powoduje u nich poczucie poniżenia. Chcąc zrekompensować sobie to uczucie za wszelką cenę dążą do przejęcia kontroli nad osobą, która ich odrzuciła.

Osoby z zaburzeniami narcystycznymi lubią kontrolować swoje życie, co przekłada się także na życie innych osób, np. partnerów. Wszelkie odrzucenie powoduje stan urojenia, gdyż osoby z narcystycznym zaburzeniem osobowości próbują przełożyć swój świat fantazji na świat rzeczywisty.

# 2. Nieprawidłowe relacje w rodzinie

Zjawisko to występuje u osób, które w dzieciństwie nie były otaczane właściwą opieką fizyczną oraz wsparciem emocjonalnym ze strony rodziców. Dziecko przystosowało się w związku z tym do świata, w którym zachowania opiekunów nie są przewidywalne i stabilne. W ten sposób wytworzyło swój własny świat, w którym jedynym celem było odzyskanie uwagi i zainteresowania rodziców. W późniejszym wieku, tym samym celom służyło manipulowanie rodzicami, m.in. poprzez szantaże, groźby i autodestrukcję. Działania sprawców stalkingu mogą wynikać także z sytuacji, w jakiej się znaleźli. Determinująco mogły zadziałać takie czynniki, jak: samotność, izolacja, a także dorastanie w środowisku patologicznym.

# 3. Brak zaufania w społeczeństwie

Z punktu widzenia socjologicznego, występowanie zjawiska stalkingu jest zarówno przyczyną, jak i skutkiem braku zaufania w społeczeństwie. Genezy stalkingu można upatrywać w konsekwencjach wzmożonej urbanizacji, która zmusiła ludzi do życia wśród nieznajomych. Egzystując w słabej integracji z najbliższym otoczeniem, jednostka staje się bardziej wrażliwa i podejrzliwa w stosunku do innych osób. W takiej sytuacji nieznani sąsiedzi są dużo częściej postrzegani jako potencjalne zagrożenie dla prywatności.

# 4. Emancypacja kobiet

Kolejną socjokulturową przyczynę występowania stalkingu wyjaśnia dość kontrowersyjny pogląd, pojawiający się w literaturze, który wiąże istnienie prześladowania kobiet z ich emancypacją. Zastąpienie dawnego systemu patriarchalnego swobodą decydowania kobiet o sobie mogło wywołać frustrację mężczyzn, którzy – nie mogąc pogodzić się z wyzwoleniem kobiet – chcą nadal mieć kontrolę nad ich życiem. Stąd też pojawiające się zachowania prześladowcze. Zatem emancypacja kobiet, a także ich wzmożona obecność w życiu publicznym, wiąże się z ich większą podatnością na bycie ofiarą niechcianego zalotnika.


Skutki stalkingu
Negatywne konsekwencje w sferze psychicznej oraz fizycznej
Problemy emocjonalne lub inne natury psychicznej
Obawa przed wyjściem z domu
Objawy agresji oraz rozkojarzenia
Zaburzenia łaknienia
Inne objawy fizjologiczne
Zmiana pracy lub jej utrata
Zmiana miejsca zamieszkania
Palenie papierosów
Spożywanie alkocholu
Zażywanie leków uspokajających lub branie narkotyków
0%
10%
20%
30%
40%
50%
60%
70%
80%

# Profil sprawców stalkingu

1. „Odrzucony” (rejected)
2. „Poszukiwacz intymności” (intimacy seeker)
3. Erotoman
4. „Nieudolny adorator” (incompetent suitor)
5. „Urażony” (resentful)
6. „Drapieżny” (predatory)

# 1. „Odrzucony” (rejected)

Jego działania podyktowane są tym, że druga strona chce zakończyć dany związek. Stalker początkowo próbuje załagodzić sytuację, dążąc do osiągnięcia porozumienia lub wymierzenia tej osobie „nieszkodliwej kary”. W większości przypadków natura związku pomiędzy stalkerem typu rejected a ofiarą opierała się na relacjach intymnych. Mógł to jednak być także inny rodzaj związku, w który odrzucony partner zainwestował pokłady emocjonalne. Stalker motywowany jest przez żal oraz uczucie niesprawiedliwości i upokorzenia. Sprawcom, którzy nie mogą pogodzić się z rozstaniem, stalking będzie zastępować związek i stworzy złudną nadzieję bliskości. Zazwyczaj „odrzuceni” stalkerzy sami siebie uważają za ofiarę, a prześladowanie dokonywane z ich strony tłumaczą jako prowokację. Należy dodać, iż „odrzuceni” stosują największe spectrum zachowań składających się na stalking, a determinacja uprzykrzenia życia eks-partnerowi będzie wyrażała się w zachowaniach naruszających prywatność ofiary: śledzenia jej, zbliżania się, wysyłania dużej liczby listów i sms-ów.

# 2. „Poszukiwacz intymności" (intimacy seeker)

Głównym celem tego typu stalkerów jest nawiązanie nowej bliskiej relacji lub podtrzymanie dawnej znajomości, istniejącej kiedyś pomiędzy ofiarą a sprawcą. W dążeniu do swego celu stalkerzy idealizują swoją ofiarę, przypisując jej cechy, które zdaniem sprawcy są najlepsze, choć nie zawsze zgodne z rzeczywistością. Dodatkowo „poszukiwacze intymności" są wytrwali w swoich dążeniach, gdyż nie zniechęca ich negatywna reakcja ofiary. Ten rodzaj stalkerów to często osoby samotne, pozbawione doświadczenia intymności. Zarówno sam akt stalkingu, jak i nadzieja na związek z ofiarą zdają się być swoistym lekiem na ich samotność. Należy zaznaczyć jednak, że nie wszystkie osoby samotne stają się prześladowcami, a zatem uczucie izolacji odczuwane przez jednostkę nie może być przyczyną objawiania się zachowań związanych ze stalkingiem. Niewątpliwie symptomem tego typu działań jest zaburzenie osobowości: stalker tworzy imaginację związku z osobą, która odrzuca jego starania. Związane jest to z interpretowaniem przez stalkera negatywnych reakcji ofiary jako reakcji pozytywnych i zachęcających do dalszego działania.

# 3. Erotoman

Erotoman jest zbliżony do poprzedniego profilu pod względem zachowania prezentowanego przez sprawcę. Wynika ono jednak bardziej z choroby psychicznej, np. schizofrenii, pewnego rodzaju manii, a nawet defektów mózgu. Erotoman uważa, że jego miłość do ofiary jest odwzajemniona. Ten rodzaj sprawców wybiera sobie na ofiarę najczęściej osoby atrakcyjne fizycznie i o wyższym statusie społecznym niż on sam. Niektórzy erotomani nie żyją wyobrażeniami czy imaginacją przeżytej relacji intymnej z osobą, ale dopiero jej poszukują, a przykładem tego jest stalker Jodie Foster. Warto dodać, że ci prześladowcy przejawiają determinację podobną do „odrzuconych", gdyż związek z ofiarą stanowi cel ich życia. Część z nich będzie zabiegać o uwagę ofiary na przestrzeni kilku, a nawet kilkunastu lat.

# 4. „Nieudolny adorator” (incompetent suitor)

„Nieudolny adorator” będący w rzeczywistości pseudoadoratorem, który zabiega o obiekt uczuć w nieodpowiedni sposób, co w konsekwencji daje efekt przeciwny do zamierzonego. Stalkerzy w tej grupie to często osoby ze słabymi zdolnościami w nawiązywaniu bliskich relacji. Kieruje nimi silne uczucie chęci stworzenia związku z osobą, którą uznali za interesującą, bez względu na jej uczucia. Przeświadczenie, że dana relacja im się należy, czyni ich niestrudzonymi w dążeniach. Ich preferowany sposób komunikacji to kontakt bezpośredni. Dodatkowo zauważono, że „nieudolnych adoratorów” można podzielić na dwie grupy: osoby widzące w nękaniu cel swego życia, bez względu na powzięte w tym zakresie środki oraz osoby zabiegające o zgodę ofiary na randkę czy intymne spotkanie

# 5. „Urażony” (resentful)

W działaniu tych stalkerów widoczna jest chęć zemsty na ofierze i wzbudzenie u niej maksymalnego strachu. Motywacja sprawcy do wyrządzenia krzywdy ofierze może wybiegać poza ramy nienawiści względem jednostki i odnosić się do nienawiści wobec systemu, korporacji, większej grupy. Nie będzie zatem dziwił fakt, że stalker posiadający tak wielką chęć zemsty nie dostrzega tego, że obarcza winą bezbronne osoby. W rzeczywistości jest odwrotnie, a mianowicie stalker widzi siebie jako ofiarę. „Urażeni” prześladowcy posługują się najczęściej groźbami, choć rzadko je spełniają – w obawie przed konsekwencjami prawnymi.

# 6. „Drapieżny” (predatory)

„Drapieżni” stalkerzyzgodnie z amerykańskimi badaniami stanowią 5% wszystkich stalkerów. Pomimo ich stosunkowo małej liczebności, to właśnie ich działania są najczęściej przedstawiane przez media. Motywem nękania są pobudki seksualne, a sam stalking jest sposobem na poczucie przewagi nad ofiarą. Stwierdza się również, że często nękanie daje stalkerowi satysfakcję seksualną, np. poczucie podniecenia podczas telefonowania do ofiary, a w niektórych wypadkach stalking może mieć charakter zapowiedzi ewentualnej napaści seksualnej. Większość „drapieżnych” stalkerów cierpi na zaburzenia seksualne oraz ma za sobą procesy o napaści seksualne.

# Prawne aspekty stalkingu

Na gruncie prawa polskiego, sposobem walki ze stalkingiem od 2011 r. jest art. 190a k.k., którego § 1 brzmi: *„Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do 3 lat”.* Został on wprowadzony ustawą z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny.

# Prawne aspekty stalkingu

Typem podstawowym przestępstwa stalkingu w art. 190a § 2 k.k. jest natomiast podszywanie się pod inną osobę, wykorzystanie jej wizerunku lub innych danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej. Zdaniem ustawodawcy konieczne było umieszczenie tego typu negatywnych zachowań w odrębnym paragrafie, ponieważ np. wykorzystanie danych osobowych może być działaniem jednorazowym, w odróżnieniu od wielokrotnego, uporczywego nękania. Sprawca stalkingu może wykorzystać cudzy wizerunek lub dane osobowe swojej ofiary, w celu jej prześladowania, co wiąże się z nieuprawnionym korzystaniem z nich.

# Prawne aspekty stalkingu

Przestępstwo przywłaszczenia tożsamości zagrożone jest taką samą karą jak przestępstwo z art. 190a § 1 k.k., a mianowicie karze pozbawienia wolności do 3 lat. Natomiast ustawowa różnica w wymiarze kary występuje w przypadku typu kwalifikowanego uregulowanego w art. 190a § 3 k.k., gdyż zagrożenie karą wynosi w tym przypadku od roku do 10 lat pozbawienia wolności. Ustawodawca przewidział takie granice sankcji, jeżeli następstwem czynu określonego w § 1 i § 2 jest targnięcie się pokrzywdzonego na własne życie. Uzasadnił to tym, że *„granice ustawowego zagrożenia zostały określone na tym poziomie dla zapewnienia pełnej spójności z innymi rozwiązaniami kodeksowymi, w szczególności do sankcji przewidzianej w art. 151 k.k., która za doprowadzenie do targnięcia się na własne życie za pośrednictwem namowy lub udzielenia pomocy przewiduje odpowiedzialność karną w granicach od 3 miesięcy do 5 lat pozbawienia wolności”*.

# Jak bronić się przed stalkingiem?

Jeśli padniesz ofiarą stalkera, powinieneś zebrać dowody i niezwłocznie zgłosić sprawę na policję. Gdy uda się namierzyć stalkera, skontaktuj się z prawnikiem, który pomoże ci udowodnić winę sprawcy.

# Jak uniknąć działania stalkera?

Przede wszystkim, nie podawaj swoich danych osobowych do publicznej informacji. Pamiętaj, że wszystko co umieszczasz w sieci na swój temat, może być wykorzystane przez takie osoby. Zadbaj także o odpowiednie zabezpieczenia swoich kont na serwisach społecznościowych. Większość z nich posiada możliwość zablokowania widoczności konta dla nieznanych osób. W razie jakichkolwiek niepokojących zachowań, poinformuj o wszystkim swoich najbliższych.

# Bibliografia


- Ustawa z dnia 6 czerwca 1997 r. – kodeks karny (Dz.U. Nr 88, poz. 553 ze zm.).
- Wielki słownik polsko-angielski, Oxford 2002.
- Mullen P., Pathe M., Purcell R., Stalkers and their victims, Cambridge University Press 2009.
- Chlebowska A., Nalewajko P., Stalking – zarys problemu oraz analiza rozwiązań ustawodawcy niemieckiego, austriackiego, polskiego, „Prokurator" 2010/2011, nr 4(44)/1(45).
- Gruszczyńska B., Marczewski M., Ostaszewski P., Siemaszko A., Woźniakowska–Fajst D., Stalking w Polsce. Rozmiary – Formy – Skutki, [w:] Stosowanie prawa. Księga jubileuszowa z okazji XX–lecia Instytutu Wymiaru Sprawiedliwości, Siemaszko A. (red.), Warszawa 2011.
- Pathe M., Surviving stalking, Cambridge 2002.
- https://informaticalegis.com/na-czym-polega-stalking-w-internecie-jak-bronic-sie-przed-stalkingiem-w-sieci/ (dostęp: 06.05.2024r.).