Ochrona danych osobowych

Wykład 1 rok informatyki algorytmicznej

Mirosław Kutyłowski 2022

Katedra Podstaw Informatyki

Przykład 1: przestępczość

zbiory danych wykorzystywane do optymalizacji działalności przestępczej:

- **typowanie ofiary**
- **maksymalizacja zysku**
- **minimalizacja ryzyka**

Przykład źródła danych: smart meter i charakterystyka zużycia prądu:

- **aktywność dobowa ofiary i jej sąsiadów**
- **wskazówki o życiu zawodowym**
- **wyznaczenie okresów, gdy brak będzie świadków**

Przykład 2: kradzież tożsamości

przestępstwa finansowe (kredyty na koszt ofiary, włamania na konta):

- **dane osobowe ofiary używane do uwierzytelniania wnioskodawcy**

- **działania ostrożnościowe kontrahentów (weryfikacja danych -np. znajomości historii kredytowej) jest nieskuteczna**

Przykład 3: wykorzystywanie konsumenta

profilowanie i agresywny marketing:

- **identyfikacja potencjalnych ofiar marketingu (np. osoby z demencją, osoby z uzależnieniemi) na podstawie danych osobowych,**

(reklama loterii dla osób uzależnionych od hazardu, reklama środków przeciwbólowych dla osób z problemami ortopedycznymi, reklamy alkoholu dla osób AA, ...)

Przykład 4: ubezpieczenia zdrowotne

Optymalizacja biznesowa firm ubezpieczeniowych:

- **przyjmowanie wyłącznie klientów zdrowych, którzy opłacą składki ale nie zachorują**

- **USA: firmy ubezpieczeniowe odmawiające przejęcia kosztów leczenia pod pretekstami winy ubezpieczonego – niezdrowego trybu życia**

ubezpieczenia mają wtedy sens, gdy nie są oparte na dyskryminacji ubezpieczonych

Przykład 5: szpiegostwo przemysłowe

Mnóstwo informacji o działaniach konkurencji można wydobyć informacji o aktywności pracowników – z pozoru nie związanych z życiem zawodowym:

- **aktywność zakupowa w sferze prywatnej mówi wiele o kondycji finansowej firmy,**
- **określone podróże mogą wskazywać na negocjacje biznesowe z określonymi kontrahentami,**
- **dane osobowe mogą pozwolić na wytypowanie pracownika konkurencji do przekupienia (kompromitujące dane, nałogi, …)**

Przykład 6: nękanie, hejt

Dostęp do danych osobowych daje znakomite narzędzia hejterom:

- **uprawdopodabnianie fake newsów poprzez mieszanie ich z informacjami prawdziwymi,**
- **uniemożliwienie ucieczki przed prześladowcami,**

Przykład 7: bezpieczeństwo publiczne

Dostęp do danych osobowych daje znakomite narzędzia terrorystom, działalności agenturalnej, mafii:

- **głęboka znajomość sieci znajomości, kontaktów, itp. pozwala infiltrować społeczeństwo:**

PRZYKŁAD: portal NaszaKlasa – zakupiony przez podmiot zagraniczny (rosyjski)

- **ułatwienie zastraszania np. przeciwników politycznych**

Tendencje:

USA: **tradycja otwartego dostępu do danych i braku ochrony danych osobowych, podejście zmienia się (Privacy Shield, ochrona danych osobowych w Kalifornii), ale niejednolicie (CLOUD Act z 2018)**

Niemcy: **po doświadczeniach z czasów nazistowskich i władzy Stasi w NRD bardzo silny opór przed dostępem do danych osobowych**

Chińska Republika Ludowa: **szybkie przejście do restrykcyjnej ochrony danych osobowych, ochrona szersza od europejskiej i stanowiąca filar cybersecurity**

Europa (stan przed RODO):

- **dane chronione do momentu opublikowania, potem bez ochrony**
- **konsekwencje karne za bezprawne ujawnienie**
- **brak technicznych i organizacyjnych wymagań bezpieczeństwa**

(„jak nie wdrożysz i wycieknie, to spotka Cię kara” – ale większość firm ryzykowała minimalizując koszty)

gdyby takie podejście stosować w budownictwie:

- **brak wymagań sporządzenia projektu technicznego mostu, prób obciążeniowych, ...**
- **… tylko kary w przypadku katastrofy budowlanej**

Stan w UE przed RODO:

- **ochrona nieskuteczna (anonimowo opublikowana informacja staje się niechroniona)**
- **powszechne łamanie zasad wpisanych w Dyrektywę UE (wyjątek: Niemcy, gdzie stosunkowo zaawansowana ochrona i świadomość społeczeństwa)**
- **niekompatybilności pomiędzy krajami**

Polska:

- **brak świadomości zagrożeń („po co chronić moje dane osobowe, przecież nic złego nie robię”)**
- **tradycja gromadzenia danych „na zapas”**
- **fasadowość ochrony (działania ograniczone do biurokracji, bez odniesienia do rzeczywistości)**