WHY PERSONAL DATA PROTECTION FAILS

Mirosław Kutyłowski

Prawo do bezpieczeństwa cyfrowego

Prawo do bezpieczeństwa powinno być praktowane zawsze jako jedno z podstawowych praw człowieka.

Bezpieczeństwo w świecie cyfrowym jest coraz ważniejszym komponentem.

Towards a Right not to Be Deceived?
Prawo-do-bycia-nieoszukiwanym?

- **Urbano Reviglio, 2020**
- **fundamentalnie I notorycznie łamane obecnie**

- **brak odpowiedzialności**
- **wolność słowa realizowana jako wolność oszukiwania**

- **konsekwencje dla bezpieczeństwa w cyberprzestrzeni**

Ochrona danych osobowych to element cyberbezpieczeństwa

- kradzież tożsamości
- tworzenie fikcyjnych tożsamości
- wywiad gospodarczy (i nie tylko)

Bezpieczeństwo poprzez eliminację

RODO ogranicza zasięg problemu poprzez eliminację danych i dostępu do nich

- **podejście takie jak w przypadku marihuany:**

-- zabronione używanie z wyjątkiem reglamentowanych przypadków

-- zabroniona produkcja poza reglamentowanymi przypadkami

Prohibicja okazuje się mało skuteczna a czasami spycha obrót w podziemie.

Podejście alternatywne

Nie zabronić przetwarzania ale obciążyć odpowiedzialnością za konsekwencje przetwarzania

Czasem bardziej skuteczne – przykład: reklamy leków przez lekarzy

-- w Polsce nielegalne ale obchodzone

-- na Tajwanie legalne, ale odpowiedzialność za fałszywe informacje

Ochrona danych osobowych – USA, CHRL

Początkowo niechęć do ograniczeń

Kierunek zmian:

Chiny: rozdział 4 w prawie o bezpieczeństwie cybernetycznym (ostre wymagania)

USA: poziom stanowy, coraz bardziej kompleksowe I pragmatyczne rozwiązania w Kalifornii

Paradygmaty RODO

zgodność z prawem, rzetelność i przejrzystość

przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą

Rzeczywistość:

- niejasne zasady, obfuskacja
- brak możliwości sprawdzenia kto przetwarza
- …

Paradygmaty RODO

ograniczenie celu

zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych ***nie jest*** *uznawane … za niezgodne z pierwotnymi celami*

Rzeczywistość:

- w kulturze praktyka zbierania danych I wykorzystania w innym celu,
- brak wsparcia technicznego do identyfikacji celów (systemy obiegu dokumentów)
- furtka interesu publicznego I badań naukowych
- …

Paradygmaty RODO

minimalizacja danych

adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane

Rzeczywistość:

- pobieranie i zbieranie na zapas
- brak świadomości odpowiedzialności za dane

Paradygmaty RODO

prawidłowość

prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane

Rzeczywistość:

- brak procedur
- problem uwierzytelniania
- uaktualnianie w archiwach
- uaktualnianie kopii u storn trzecich
- …

Paradygmaty RODO

ograniczenie przechowywania

przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą

Paradygmaty RODO

ograniczenie przechowywania

Rzeczywistość:

- techniki pseudonimizacji I anonimizacji – brak systemowego wsparcia technicznego
- zawodna skuteczność anonimizacji
- furtka, enigmatyczne *zagwarantowanie praw I wolności*

Paradygmaty RODO

integralność i poufność

przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

Rzeczywistość:

- notoryczny brak zabezpieczeń
- prowizoryczne systemy ochrony dostępu
- …

Paradygmaty RODO

rozliczalność

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie
(m.in.: privacy-by design)

Rzeczywistość:

- traktowana formalnie – dokumenty takie jak polityka ochrony danych bez związku z rzeczywistością i krytycznymi problemami (cut-and-paste z internetu)

- brak podstawowych narzędzi – np. identyfikacji osób fizycznych

Odpowiedzialność

Kary administracyjne:

- drakońskie dla podmiotów niepublicznych
- max 100tys. dla podmiotów publicznych

Odpowiedzialność wobec ofiary:

- jedynie cywilno-prawna

Zaprojektowane jako model nacisku państwa na koncerny technologiczne przy założeniu że organy kontrolne działają na rzecz obywateli

Przykład innego podejścia: prawa pasażerów linii lotniczych

Problemy interpretacyjne

- *„dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);*
- *możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;*

Problemy interpretacyjne – kiedy dane są “osobowe”?

relative approach:

to co podmiot przetwarzający wie

global approach:

to co globalnie wiadomo

Problemy interpretacyjne – kiedy dane są “osobowe”?

Problemem jest przypadek rozstrzygnięcia “to nie są dane osobowe”

relative approach:

prowadzi do iluzoryczności ochrony przez RODO

global approach:

technicznie niewykonalne

- brak dostepu do informacji
- brak możliwości rozstrzygania w czasie rzeczywistym

Problemy interpretacyjne: prawo-do-bycia-zapomnianym?

Przykład: nierzetelna praktyka lekarska, oceny pacjentów w serwisie typu JakiLekarz

kolizje:

- prawo do bycia zapomnianym z RODO (lekarz prowadzący praktykę pod imieniem i nazwiskiem jako osoba fizyczna)

- prawo do zdrowia

- Prawo do niezniszczenia danych osobowych: *"ja, Jan Kowalski, doznałem szkód na zdrowiu wskutek …"*

Kolizja praw do danych osobowych

Rekord medyczny:
Alicja Kowalska ma symptomy X tak samo jak jej brat.

Z kontekstu wynika że Jan Kowalski, jedyny brat Alicji Kowalskiej ma symptom X.

Kto jest “data subject” dla tego rekordu?

Próba pseudonimizacji

Rekord medyczny:

Alicja Kowalska ma symptomy X tak samo jak jej brat.

Alicja Kowalska ma symptomy X tak samo jak osoba Y.

Osoba A ma symptomy X tak samo jak osoba Y.

Kolizja praw do danych osobowych

Rekord:

Alicja Kowalska ma symptomy X tak samo jak jej brat.

Żądanie Alicji Kowalskiej:

przechowuj ten record

Żądanie Jana Kowalskiego:

usuń ten rekord

Kolizja praw do danych osobowych

RODO napisane przy założeniu, że dla każdych danych istnieje jeden “data subject” – podmiot danych osobowych

Tak jest często ale nie zawsze

Wyzwania:

- Jak identyfikować podmiot(y) danych osobowych
- Jak rozstrzygać kolizje praw

Uprawnienia do przetwarzania

Przykład: weryfikacja podpisu elektronicznego

Wg definicji z RODO:

- weryfikacja JEST przetwarzaniem danych
- przetwarzanie jet dozwolone o ile jest zgoda podmiotu danych, istnieje interes prawny, obowiązek ustawowy, …
- Jeśli takiej zgody itp nie ma to przetwarzać nie wolno, istnienie dokumentu w obszarze publicznym nie wystarcza… -- zgoda musi być EXPLICITE

Uprawnienia do przetwarzania

Rozwiązanie techniczne: **signature validation token z zapisanymi explicite warunkami**

Przykład dla podpisu Schnorra and wiadomością *M przy* użyciu klucza *x* i token *d*:

- wybierz losowe *k* , *oblicz* $r := g^k$
- oblicz ~~$e := Hash(M,r)$~~ $e := Hash(M,r,d)$
- oblicz $s := k - ex \bmod q$

- Podpis to *(s,e)*

Spór o Prawo do anonimizacji

Czy mając dane osobowe można je "wyjąć spod rygorów RODO poprzez skuteczną anonimizację?

(anonimizacja = nie jest możliwe odtworzenie których osób dane dotyczą)

Motywacja: o ile dane są zanonimizowane to w żaden sposób ich przetwarzanie nie naruszy "praw I wolności" podmiotów danych

Ale: czynność anonimizowania podlega RODO dopóki dane jeszcze nie są zanonimizowane

Decyzja EDPS

Przypadek przetwarzania zanonimizowanych danych z nasłuchu szmuglerów imigrantów przez europejską agencję na Malcie

Decyzja:

Przetwarzanie narusza RODO, bo źródła przed anonimizacją zawierały dane osobowe

Czyli: brak prawa do anonimizacji I przetwarzania zanonimizowanych danych

Prawo do anonimizacji - konsekwencje

Zagrożenie dla europejskiego sektora AI

-- brak dostępu do legalnego inputu w wielu przypadkach

RODO a Sytuacje wyjątkowe

Wymiana danych COVID-19

-- brak rozwiązań, RODO pisane pod kątem "normalnej sytuacji"

-- w pierwszej fazie COVID Włochy wyłączyły to spod RODO, współpraca miedzypaństwowa kulała

-- kontrowersje wobec Contact Tracing Apps

Contact tracing

-- EU początkowo: rozwiązania niezgodne z RODO I elementarną ochroną danych

-- nacisk koncernów technologicznych z USA by zrobić to porządnie (osoba zagrożona kontaktem dowiaduje się o tym ale nie organy państwowe) i nie zaistalować narzędzi do totalnej inwigilacji

-- dostępny mechanizm Apple-Google

Realne konsekwencje

- zalew zgód do udzielenia przez użytkownika -- nikt tego nie czyta, zgody nawet wtedy gdy niepotrzebne
- język niezrozumiały dla użytkownika – niewielu jest w stanie zrozumieć
- bezużyteczne polityki ochrony danych -- pisane by nie było zarzutów że ich nie ma a nie by usunąć niebezpieczeństwa

Snowden: “GDPR is a paper tiger”

Czy faktycznie zostały wyłączone systemy stwarzające zagrożenia?

Czy system nadzoru funkcjonuje?

NIE: prasa w dniu 25.10.2021:

“Mirosław H., …, prowadził pojazd w stanie nietrzeźwości”

- identyfikowalne kogo informacja dotyczy
- RODO: brak zgody, brak interesu prawnego, brak obowiązku prawnego publikacji
- **Reakcja UODO: brak**

Niektóre wyzwania techniczne:

- **RODO z “prawem o bycie zapomnianym” a technologie distributed ledger**

- **RODO a usługi chmurowe i zasięg terytorialny:**
  - **wyroki Schrems oraz Schrems II**
  - **kontrowersje USA/Europa w zakresie dostępu agencji rządowych zwalczających przestępczość**
  - **stanowisko KE o ramowych warunkach przetwarzania, poprzednio Safe Harbour, …**

Przyszłość

- konieczna rewizja koncepcji prawnych
- wymagana współpraca pragmatycznych informatyków I pragmatycznych prawników -- ortodoksyjne podejście po którejkolwiek stronie doprowadzi do katastrofy
- konieczny rozwój narzędzi ochrony prywatności – zapewne jedynie *co-design* gwarantuje sukces
- inni (Ameryka, Azja, …) mogą efektywnie narzucić swoje rozwiązania

Pozytywny przykład

Komunikacja pomiędzy paszportem /dowodem osobistym a czytnikiem wg standard ICAO:

-osoba podsłuchująca nie jest w stanie odzyskać hasła ani tożsamości dokumentu tożsamości (tracing nie działa)

- **atakujący (czytnik) w trakcie jednej sesji może wypróbować jedno hasło (numer CAN) i je potwierdzić. Nic nie daje to na temat innych haseł**

- **wysoka odporność na ataki aktywne**

Dziękuję za uwagę