

Alternatywne sposoby regulowania normatywnego kwestii organizacyjno-technicznych ochrony danych osobowych w systemach informatycznych: "soft law" versus "hard law"

dr Stefan Szyszko

Członek Stowarzyszenia Administratorów Bezpieczeństwa Informacji
Sekretarz Podkomisji PIU ds. Ochrony Danych i Standaryzacji
Informacji
Dyrektor Działu Zarządzania Informacją Ubezpieczeniową PIU

Warszawa, 28 marca 2010 r.

AGENDA

L.p.	Temat
1	Aktualny kształt legislacji dot. ochrony danych osobowych: lex generalis versus lex specialis, rola rozporządzeń wykonawczych
2.	Aktualna rola regulacji miękkich, ze szczególnym uwzględnieniem norm technicznych z obszaru bezpieczeństwa Informacji
3.	Czy prawo „twarde” ma w ogóle szansę nadążyć za przemianami społecznymi i gospodarczymi, wymuszonymi postępem informatyzacji? Casus bezradności w zderzeniu z serwisami społecznościowymi i wnioski stąd płynące.
4.	Jaki kształt prawa krajowego wynika z Dyrektywy 95/46/WE i czy w ogóle potrzebne są nam rozporządzenia wykonawcze do UODO w obszarze bezpieczeństwa technicznego systemów informacyjnych przetwarzających dane osobowe?
5.	Jeśli w ogóle zachować Rozporządzenie MSWiA w sprawie bezpieczeństwa systemów informatycznych, to w jakim kształcie i zakresie regulacji?
6.	Jak można dobrze wykorzystać prawo miękkie, nie doprowadzając do faktycznego obniżenia standardów ochrony?
7.	Zadania dla prawników w obszarze prawa informatycznego – jak mogą usprawnić tworzenie dobrego prawa w tym obszarze: PRIMUM NON NOCERE
8.	Dyskusja

Aktualny kształt legislacji dot. ochrony danych osobowych: lex generalis versus lex specialis, rola rozporządzeń wykonawczych /1

Lex generalis:

- UODO,
- Rozporządzenia wykonawcze do UODO – ze szczególnym uwzględnieniem Rozporządzenia MSWiA dot. bezpieczeństwa systemów informatycznych (RMSWiA)

Lex specialis:

- Regulacje ustawowe w poszczególnych obszarach gospodarczych i dziedzinowych administracji
 - W nich rzadko szczególne regulacje dot. ODO. Wyjątkiem są tu:
 - obszary co do zasady bazujące na technologiach informatycznych (np. prawo telekomunikacyjne, sprzedaż na odległość, etc.),
 - Regulacje dot. zasad gromadzenia i udostępniania danych w centralnych rejestrach referencyjnych
 - Obszar informacji niejawnych (tajemnicy państwowej)
 - Równie rzadko rozporządzenia wykonawcze, dot. szczególnego regulowania kwestii ochrony informacji

WĄTPLIWOŚĆ NATURY SYSTEMOWEJ: czy w takim krajobrazie legislacyjnym RMSWiA jest w ogóle potrzebne?

Konferencja SABI i PW: "Zabezpieczanie danych osobowych - aktualny stan prawny i rzeczywiste potrzeby", 28-03-2011

Aktualny kształt legislacji dot. ochrony danych osobowych: lex generalis versus lex specialis, rola rozporządzeń wykonawczych /2

Główne problemy z RMSWiA

- Metody uwierzytelnienia:
 - życie poszło bokiem – statyczne hasła to najłabszy środek
 - Bez litości dla użytkownika – jak zapamiętać ~10 różnych loginów i haseł, okresowo zmienianych w różnym czasie?
 - Efekt:
 - lepsze wrogiem dobrego: WSZYSCY TE IDENTYFIKATORY GDZIEŚ ZAPISUJĄ !!!
 - Kreowanie pewnej fikcji bezpieczeństwa
 - Tworzenie konstrukcji niezrozumiałym i budzących intelektualny sprzeciw: w wielu systemach po solidnej analizie ryzyka uznano by reżim wymuszania okresowej zmiany haseł za zbędny
 - To są rozwiązania z czasów, kiedy człowiek miał do czynienia z 1 systemem IT z DO: w pracy, a dziś ma ich przeciętnie 7-10, w pracy i w domu
- W czasach powszechnego usieciowienia kategoryzacja poziomów zabezpieczeń jest nieadekwatna do faktycznych podatności i ryzyk bezpieczeństwa

Aktualny kształt legislacji dot. ochrony danych osobowych: lex generalis versus lex specialis, rola rozporządzeń wykonawczych /3

Główne problemy z RMSWiA - c.d.

- Usiłuje regulować kwestie, których w obecnym stanie rozwoju technologii informatycznych w prawie „twardym” uregulować się nie da: np. co to jest OBSZAR PRZETWARZANIA DANYCH (poza jasnym przypadkiem centrum danych, serwerowni, etc.) – a może to wszędzie, gdziekolwiek znajdzie się „operator” AD / „procesora” z urządzeniem mobilnym?
- Nie różnicuje w adekwatny sposób wymagań na tworzenie dokumentacji stricte technicznej, co w czasach „komodytyzacji” informatyki rodzi wymagania absurdalne:
 - Czy konsument energii elektrycznej musi wiedzieć, jakie są przepływy w sieciach energetycznych?
 - Czy podpisując kontrakt outsourcingowy na dostarczanie usług przetwarzania danych (nie mam serwerów, oprogramowania, kupuję usługę bezpiecznego przetwarzania moich danych) dalej muszę wiedzieć, jak jest ono technicznie realizowane, jakie są przepływy danych na poziomie technicznych zabezpieczeń?

Aktualna rola regulacji miękkich, ze szczególnym uwzględnieniem norm technicznych z obszaru bezpieczeństwa Informacji /1

Punkt wyjścia:

- Bezpieczeństwo jest wyłącznie składnikiem zarządzania różnymi kategoriami ryzyk: biznesowych (specyficznych dla branży), operacyjnych, reputacyjnych, etc.
- Wszelka ODO w dużej organizacji jest składnikiem SZBI (Systemu Zarządzania Bezpieczeństwem Informacji),
- SZBI jest częścią składową systemu zarządzania ryzykiem

Co z tego wynika:

- Obszar ten jest w większości wyzwaniem techniczno-organizacyjnym, a nie prawnym
- Jak się popełni regulacje niezrozumiałe dla IT (**TO SĄ INŻYNIEROWIE, A NIE PRAKTYCY, LUDZIE Z 3-5 LETNIM CURRICULUM AKADEMICKIM MYŚLENIA ALGORYTMICZNEGO**), to na pewno nie poprawi się FAKTYCZNEGO STANU BEZPIECZEŃSTWA
- W rzeczywistości technicznej mamy dostępną szeroką paletę rozwiązań,
- Główne jej cechy:
 - **ZROZUMIAŁA I ZGODNA Z INTUICJĄ INŻYNIERSKĄ TERMINOLOGIA**
 - **STABILNOŚĆ – ZASADNICZE PODEJŚCIE Z BS-7799 NIE ULEGŁO ZMIANIE OD 1995 R.**

Aktualna rola regulacji miękkich, ze szczególnym uwzględnieniem norm technicznych z obszaru bezpieczeństwa Informacji /2

Główne problemy:

- Brak tradycji odwoływania się w procesach stanowienia prawa do krajowych norm technicznych – to się bardzo powoli, ale jednak zmienia
- Brak wypracowanych rozwiązań określania skutków prawnych stosowania zaleceń z tych norm płynących
 - tam gdzie chciałoby się z tych norm skorzystać w celu określenia tego skutku
 - Co do zasady, **normy są regulacjami „miękkimi”, bez takiego skutku automatycznie wywodzonego**
- Brak tradycji wydawania zaleceń i rekomendacji przez organy nadzoru
 - Przydałoby się trochę więcej podejścia w stylu brytyjskich guide books
- Brak tradycji autoryzowania przez GIODO zaleceń i rekomendacji branżowych
- **Sytuacji nie ułatwia PKN:**
 - dostęp do norm technicznych jest kosztowny – papierowa kopia normy kosztuje kilkaset PLN
 - Przydałaby się inna postawa państwa, promująca używanie utrwalonych standardów i obniżająca koszty ich stosowania
 - **Korzystanie ze standardów jest elementem składowym postulowanego „taniego państwa”**

Czy prawo „twarde” ma w ogóle szansę nadążyć za przemianami społecznymi i gospodarczymi, wymuszonymi postępem informatyzacji?

Moja odpowiedź: **raczej chyba NIE**

Dlaczego: bo całkowicie rozbieżne są cykle zmian w obu obszarach:

- Zmiana ustawy: średnio 5-7 lat , zmiana rozporządzenia: 2-4 lata (i to jest dobre, po prawo „twarde” ma być stabilne w państwie prawa)
 - Czas pracy nad zmianą ustawy: średnio 2 – 4 lata (najczęściej zaraz po uchwaleniu prawa, przystępuje się do „łatania dziur”)
- Rewolucja technologiczna w IT ze skutkami społecznymi: średnio co max. 5 lat

Efekt: kiedy już uchwali się nowe „twarde prawo”, najczęściej zderza się ono z rzeczywistością techniczną i – co jeszcze ważniejsze nowo wykreowaną SPOŁECZNA – do obsługi której nie jest dostosowane

W takim świecie znacznie lepiej dają sobie radę systemy prawne oparte na ***common law***

Casus bezradności w zderzeniu z serwisami społecznościowymi i wnioski stąd płynące:

- Skoro „prawo twarde” nie nadąża i nadążyć nie ma szans ze względów systemowych, może w całych obszarach w ogóle zrezygnować z niego, na rzecz zaleceń i rekomendacji branżowych i wydawanych przez właściwe organa nadzoru?

Jaki kształt prawa krajowego wynika z Dyrektywy 95/46/WE

Czy w ogóle potrzebne są nam rozporządzenia wykonawcze do UODO w obszarze bezpieczeństwa technicznego systemów informacyjnych przetwarzających dane osobowe?

- Czas pracy nad zmianą ustawy: średnio 2 – 4 lata (najczęściej zaraz po uchwaleniu prawa, przystępuje się do „łatania dziur”)
- Rewolucja technologiczna w IT: średnio co 5 lat

Efekt: kiedy już uchwali się nowe „twarde prawo”, najczęściej zderza się ono z rzeczywistością techniczną i – co jeszcze ważniejsze – nowo wykreowaną SPOŁECZNA – do obsługi której nie jest dostosowane

W takim świecie znacznie lepiej dają sobie radę systemy prawne oparte na *common law*

Casus bezradności w zderzeniu z serwisami społecznościowymi i wnioski stąd płynące:

- Skoro „prawo twarde” nie nadąża i nadążać nie ma szans ze względów systemowych, może w całych obszarach w ogóle zrezygnować z niego, na rzecz zaleceń i rekomendacji wydawanych przez właściwe organa nadzoru?

Jeśli w ogóle zachować Rozporządzenie MSWiA w sprawie bezpieczeństwa systemów informatycznych, to w jakim kształcie i zakresie regulacji?

- Regulować tylko te aspekty, które uznamy za odporne na zmiany technologiczne i społeczne – może uda się nam w miarę dobrze przewidzieć je
- Zasadniczo zmienić całą konstrukcję, aby była zrozumiała dla nie-prawników:
- Punkty wyjścia:
 - W odniesieniu do danych: PUFNOŚĆ, INTEGRALNOŚĆ, DOSTĘPNOŚĆ
 - W odniesieniu do działań ludzi i systemów: ROZLICZALNOŚĆ (w szczególności NIEZAPRZECZALNOŚĆ)
 - Analiza ryzyka jako podstawa do zastosowania adekwatnych środków ochrony:
 - Jak ma być dokumentowana
 - Jak ma być powiązana z w/w desygnatami
- Wprowadzenie kategoryzacji podmiotów w celu wskazania, jaki poziom szczegółowości dokumentacji systemu zabezpieczeń ma być wdrożony
- Przywrócenie obowiązku szkoleń okresowych
- Odesłanie w kwestiach szczegółowych do zaleceń GIODO, publikowanych na jego stronie WWW, oraz branżowych pozytywnie zaopiniowanych przez GIODO, jako przykładowych rozwiązań

Regulacja powinna zatrzymać się na tym poziomie – bez operowanie szczegółami typu konstrukcja bezpiecznego hasła

Jak można dobrze wykorzystać prawo miękkie, nie doprowadzając do faktycznego obniżenia standardów ochrony?

- **GIODO – wzorem nadzoru hiszpańskiego, który wydał ich kilkadziesiąt – mógłby wydawać własne ZALECENIA / REKOMENDACJE:**
 - Nadążać będą one za zmianami technologicznymi i społecznymi, bo można je będzie w właściwym tempie zmieniać
 - Formuła mogłaby przypominać brytyjskie *guide books*
 - Dobre początki już są na stronie WWW GIODO, brak jest systemowego umocowania – co wynika z zastosowania się do nich dla przetwarzających DO
 - Terminologia powinna być w całości wywodzona z utrwalonej terminologii w obszarze SZBI, zarządzania ciągłością działania i analizy ryzyka (branżowego, oraz ryzyk operacyjnych)
- **GIODO mógłby autoryzować branżowe rekomendacje z obszarów w/w - we właściwym sobie zakresie, dot. ODO**
 - Bez elementu przymusu – chętni mogliby do GIODO o weryfikację wystąpić
- **Kontynuacja już rozpoczętej przez GIODO współpracy nad tworzeniem BRANŻOWYCH KODEKSÓW DOBRYCH PRAKTYK PRZETWARZANIA DO**
- **Powiązanie z RZĄDOWYM PROGRAMEM OCHRONY CYBERPRZESTRZENI RP:**
 - On z zasady będzie miał charakter zaleceń
 - Oferować będzie szereg rozwiązań, obejmujących również DO

Zadania dla prawników w obszarze prawa informatycznego – jak mogą usprawnić tworzenie dobrego prawa w tym obszarze: **PRIMUM NON NOCERE**

- **Znalezienie sensownych powiązań pomiędzy:**
 - Zaleceniami / rekomendacjami GODO, oraz branżowymi przez GODO autoryzowanymi
 - Przepisami prawa „twardego”
- **Skoncentrowanie się w prawie „twardym” na przypadkach, kiedy podmiot danych faktycznie doznaje uszczerbku**
- **W tym zakresie obecne przepisy prawa cywilnego i karnego wydają się być wystarczające**
 - Jedyne czego w nich brakuje, to pomocy w ustalaniu stanu faktycznego (że naruszenie faktycznie nastąpiło i kto jest za nie odpowiedzialny)
 - **Jest to obszar tzw. INFORMATYKI ŚLEDZCZEJ, znacznie szerszy niż kwestie ODO i jako taki powinien być odrębnie regulowany, obejmując swoim zasięgiem również ODO**
- **Powstrzymanie się przed tworzeniem regulacji:**
 - nadmiarowych,
 - Operujących ad hoc tworzonymi neologizmami i skrótami myślowymi, zamiast terminologią utrwaloną i powszechnie zrozumiałą w obszarze zarządzania systemami bezpieczeństwa i analizy ryzyka

Dziękuję za uwagę

PYTANIA I ODPOWIEDZI
