Ryzyko jako zjawisko subiektywne. Włączenie kognitywistki do koncepcji ryzyka w europejskim prawie ochrony danych osobowych

Coraz więcej europejskich regulacji prawnych, zwłaszcza w obszarze nowych technologii, opiera się na stosowaniu tzw. podejścia opartego na ryzyku. Ma ono na celu zapewnienie odpowiedniego poziomu zabezpieczeń dla czynności o różnym poziomie ryzyka. Przykładem może być ryzyko wycieku danych wynikające z ataku hakerskiego z wykorzystaniem programów generujących olbrzymie liczby różnych rodzajów haseł (tzw. *bruteforce*). Ponieważ zazwyczaj w naszych skrzynkach mamy dużo ważnych dokumentów i tajemnic, nieuprawniony dostęp do tych informacji byłby dla nas bardzo dotkliwy. Jednocześnie liczba takich ataków jest bardzo duża. W związku z tym widzimy, że ryzyko włamania na skrzynkę jest wysokie. W takiej sytuacji powinniśmy zabezpieczyć swoją skrzynkę co najmniej dobrym hasłem (ostatnie rekomendacje to co najmniej 12 znaków, w tym litery wielkie i małe, cyfry oraz znaki specjalne). Z drugiej strony nie ma potrzeby aby równie wysoki poziom zabezpieczeń stosować w odniesieniu do konta na demowej wersji aplikacji internetowej, której funkcjonalności chcieliśmy tylko sprawdzić. Chodzi zatem o zabezpieczenie odpowiednie do ryzyka, ale tylko w odniesieniu do tego, co rzeczywiście wymaga zabezpieczenia. Dzięki temu możemy skoncentrować nasze zasoby na tym, co rzeczywiście tego potrzebuje. W tym celu powinniśmy przeprowadzić ocenę ryzyka. Podany przykład dotyczy zwykłych użytkowników nowych technologii, jednak analogiczne wymogi (choć oczywiście w odpowiednio większej skali i złożonym zakresie) nakłada na przedsiębiorców przetwarzających dane osobowe Rozporządzenie o Ochronie Danych Osobowych (RODO).

Pomysł zakładający dostosowywanie zabezpieczeń do poziomu ryzyka, w oparciu o wyniki jego analizy, jest teoretycznie bardzo dobry, jednak z czasem praktyka pokazała, że przeprowadzenie oceny ryzyka nie jest dla wszystkich takie łatwe. Poza tym, zarówno samo ryzyko jak i jego analiza mają charakter bardzo subiektywny. Przedsiębiorca (administrator danych) może ocenić ryzyko jakiegoś zdarzenia jako niskie, ale kontroler z organu nadzorczego arbitralnie może stwierdzić, że w tym przypadku ryzyko jest wysokie i w związku z tym nakłada karę na administratora za niezastosowanie odpowiednich środków zabezpieczających.

W ramach tego badania chcemy skupić się na subiektywności procesu szacowania ryzyka; zobaczyć jakie psychologiczne mechanizmy mają wpływ na proces szacowania ryzyka i zastanowić się, jak możemy poprawić naszą praktykę prawniczą, aby proces szacowania był bardziej rzetelny a kontroli nie tak arbitralny.

Badanie nasze prowadzimy na przykładzie analizy ryzyka wykonywanej w ramach oceny skutków dla ochrony danych wymaganej w RODO, ale wyniki badań będą mogły być wykorzystywane również w innych obszarach prawa, np. prawa dotyczącego sztucznej inteligencji albo cyberbezpieczeństwa.