



Prof. dr hab. Jacek Gołaczyński

Uniwersytet Wrocławski

Recenzja rozprawy doktorskiej mgr Piotra Siemieniaka pt. „Ochrona danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych”

1. Uwagi ogólne.

Rozprawa doktorska przedstawiona do recenzji dotyczy ochrony danych osobowych, ale w czasie projektowania. Tematyka rozprawy doktorskiej jest doniosła jurydycznie i praktycznie. Nie ma bowiem wątpliwości, że obecnie powszechność usług cyfrowych ma wpływ na tworzenie gospodarki, której podstawą są informacje. Rozwój gospodarki jest bowiem zależny od usług świadczonych w chmurze obliczeniowej (*cloud computing*) jest postrzegane jako znak czasu. Doszło do nagromadzenia ogromnych ilości danych, które mogą być postrzegane jako dane nadmiarowe, ponieważ wcześniej jedynie część zgromadzonych danych była mogła być wykorzystywana w praktyce, ilość zapisanych danych rośnie w sposób wykładniczy. Jak wskazał autor, w 2020 roku ilość użytecznych danych osiągnie skalę 16 zettabajtów.

Autor wskazał we wstępie, że nowe technologie dają możliwość rozpoznawania twarzy, działania systemów RFID, czy rozwiązania z zakresu *Internet of Things*, mechanizmy sztucznej inteligencji czy różne rodzaje sposobów komunikacji, otwierają nowe możliwości związane z automatyzacją codziennych spraw lub poprawą komfortu życia.

Te zjawiska technologiczne powodują z kolei dostępność informacji o osobach fizycznych co może skutkować ich wykorzystywaniem, w celu uzyskania przewagi wobec osób, których dane są przetwarzane. Wykorzystuje się w tym celu rozwiązania służące do przeszukiwania danych, maszynowego uczenia, czy sztucznej inteligencji. Udostępnienie tych danych komukolwiek może doprowadzić, że ta jednostka poniesie stratę lub druga strona zyska określone korzyści. Budowanie przewagi względem drugiej strony może odbywać się przez łączenie informacji, które są niepowiązane treściowo, co daje możliwości jeszcze szerszej eksploracji danych osobowych oraz rozpoczęcia profilowania względem podmiotu danych. Autor zasadnie zauważa, że nie jest zagrożenie dla prywatności i danych osobowych, ale może prowadzić do

niepożądanych celów. Dlatego dane osobowe nie są sprzedawane w celu zysku, lecz są wykorzystywane w celu wpłynięcia na kogoś i przewidzenia zachowania danej jednostki.

Należy zauważyć, że powyższe zjawisko może prowadzić do różnych form dyskryminacji i ograniczeń, które będą miały wpływ na nasze codzienne życie. Wykorzystanie technologii zostało znacznie uproszczone w taki sposób, że coraz częściej nie jest potrzebna wiedza specjalistyczna, aby stworzyć system przetwarzający dane osobowe. Dużą popularność zyskują platformy typu *no-code* lub *low-code*, które w sposób wizualny umożliwiają stworzenie programów o określonym działaniu, co wiąże się z tym, że technologia może zostać wykorzystana w celach, które nie będą zgodne z obecnymi normami prawnymi oraz tymi, które są uznawane w społeczeństwie.

I dlatego, obecnie w pełni aktualnym zagadnieniem pozostaje wykorzystanie technologii w sposób odpowiedzialny (*responsible use*) i etyczny (*ethical use*). Wykorzystanie technologii oraz związanych z nim zagrożeń, wiąże się ochroną prywatności oraz ochroną danych osobowych jednostek. Stąd też niezwykle istotne są prawne instrumenty ochrony danych osobowych, które długofalowo pomogą zapobiegać występowaniu kolejnych zagrożeń. Realne zagrożenia dla prywatności i ochrony danych osobowych mogą się pojawiać już na etapie pomysłu na rozwiązanie, a nieprzewidziane przypadki użycia wytworzonej technologii doprowadzić do niechcianych konsekwencji.

Autor zauważa, że właściwe planowanie, projektowanie i zarządzanie projektami zarówno w sektorze publicznym, jak i prywatnym pomagają w odniesieniu sukcesu. Tematyka ochrony danych osobowych podczas projektowania została już dostrzeżona przez Ann Cavoukian, która opracowała koncepcję ochrony prywatności w fazie projektowania-*privacy by design*. Model *privacy by design* miał na celu wsparcie twórców procesów i systemów przetwarzania danych osobowych w rozwiązywaniu tego, aby ochrona prywatności była włączana w projekt w odniesieniu do całego cyklu życia danych, przy czym model ten wspierał podmioty projektujące systemy teleinformatyczne w rozwiązywaniu konfliktów wartości.

Istotne znaczenie miało przyjęcie modelu *privacy by design*, i zaimplementowanie go w zmodyfikowanej formie pod postacią *data protection by design* oraz *data protection by default* w przepisach ogólnego rozporządzenia o ochronie danych.

Koncepcja modelu *privacy by design* stała się częścią systemu prawnego Unii Europejskiej, którego zasięg w obszarze ochrony danych osobowych wykracza poza jej granice. W związku z tym, że *data protection by design* stał się częścią systemu prawnego Unii Europejskiej szczególnie istotne jest głębokie zrozumienie wpływu tej instytucji prawnej na podmioty, względem których regulacje dotyczące ochrony danych osobowych mają zastosowanie. Stąd też, tytułowe zagadnienie prawne, jest szczególnie doniosłe jurystycznie, ponieważ wymaga analizy z perspektywy prawa unijnego, ale ma też duże znaczenie dla gospodarki opartej na informacji.

Należy wskazać, że tematyka ochrony danych w fazie projektowania nie była jeszcze przedmiotem analizy w polskiej doktrynie, i także w literaturze zagranicznej, gdzie raczej analizuje się koncepcję *privacy by design* i co za tym idzie jest oderwana od problematyki *data protection by design* w systemie prawa Unii Europejskiej. Nadto publikacje w tym zakresie nie mają charakteru monograficznego i zwykle dotyczą jedynie pewnego aspektu. Trzeba podkreślić, że przyjęta koncepcja - model *data protection by design* nie ogranicza się jedynie do aspektów do prawnych, ale także uwzględnia kontekst norm i standardów w zakresie ochrony prywatności i bezpieczeństwa oraz perspektywę związaną z wytwarzaniem oprogramowania, czyli *Systems Development Life Cycle*. Prawidłowo także autor zastosował w dokonywanych analizach także aspektów technologicznych. Przeprowadzenie analizy związanej z instytucją prawną ochrony danych w fazie projektowania jest szczególnie istotne ze względu na to, że dochodzi do degradacji prywatności oraz ochrony danych osobowych, przez co jednostki mają coraz mniejszy wpływ na to, jakie informacje o nich pozostaną prywatne, a jakie informacje pozostaną swego rodzaju „własnością” innych podmiotów.

Autor prawidłowo postawił sobie pytanie badawcze, czy model ochrony danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych może wpłynąć na podniesienie poziomu ochrony prywatności i danych osobowych jednostek w dobie dynamicznego rozwoju technologicznego i funkcjonowania *data-driven economy*.

Szczegółowe tezy badawcze, rozwijane w poszczególnych rozdziałach także zostały określone prawidłowo i dotyczyły zagadnień: czy istnieje jednoznaczna metoda oceny prawidłowości implementacji przez administratorów danych dla modelu ochrony

danych w fazie projektowania? Czy rozwiązania prawne w obszarze ochrony danych osobowych skutecznie uzupełniają model ochrony danych w fazie projektowania, aby zmaksymalizować jego efektywność jako instrumentu prawnego, czy model ochrony danych w fazie projektowania jest potrzebny w systemie prawnym UE, czy działania organów ochrony danych są wystarczające, aby stosowanie modelu ochrony danych w fazie projektowania było skuteczne, czy model ochrony danych osobowych ma wpływ na ochronę praw i wolności osób fizycznych oraz czy model ochrony danych w fazie projektowania jest skutecznym instrumentem prawnym ochrony danych osobowych?

Podsumowując uznać należy, że zakreślony w rozprawie doktorskiej problem badawczy, zawarty w tytule oraz w poszczególnych rozdziałach, a dotyczący ochrony danych osobowych w trakcie projektowania, uwzględniający model oceny ochrony danych osobowych i prywatności, z uwzględnieniem także kontekstu pozaprawnego, w szczególności technologicznego i etycznego jest nowatorski. Nie był przedmiotem całościowej analizy zarówno w polskiej, jak i zagranicznej literaturze prawniczej. Monografia doktorska przedstawiona o recenzji będzie wypełniała zatem istniejąca w doktrynie lukę.

2. Systematyka rozprawy doktorskiej.

W rozdziale I pt. Prawo do prywatności a prawo do ochrony danych osobowych Autor omówił zagadnienia historyczne dotyczące ochrony prywatności, a które wiążą się z rozwojem technologii, także związku pomiędzy technologią a prawem do prywatności. Rozdział ten zawiera także opis i ocenę prawnych unormowań w zakresie prywatności w prawie polskim, prawie międzynarodowym oraz prawie Unii Europejskiej. Autor omówił także rozwój historyczny ochrony danych osobowych w prawie międzynarodowym, prawie Unii Europejskiej oraz w prawie polskim. Szczególnie ciekawe było rozważania o relacji pomiędzy pojęciem prawo do prywatności a prawem do ochrony danych osobowych.

W rozdziale II pt. Ochrona danych osobowych w fazie projektowania autor przedstawił z perspektywy historycznej różne modele *privacy by design* oraz *data protection by design*, a następnie dokonał oceny ze względu na ewentualne podobieństwa i różnice między modelem *privacy by design* a *data protection by design*. Porównanie to miało istotne znaczenie dla odróżnienia występujących w zakresie

ochrony danych osobowych w fazie projektowania modeli. Następnie autor omówił rozwiązania dotyczące *Privacy-Enhancing Technologies* oraz niektóre rozwiązania *Privacy-Invading Technologies*, oczywiście ograniczając rozważania do tytułowej dla rozprawy tematyki ochrony danych w fazie projektowania. Autor starał się w ten sposób udzielić odpowiedzi na pytanie, czy modele *privacy by design* oraz *data protection by design* są tożsame.

W rozdziale III pt. Zapewnienie zgodności z regulacjami w zakresie ochrony danych osobowych w kontekście *data protection by design* oraz *data protection by default* autor ocenił relacji między modelem ochrony danych w fazie projektowania a ogólnym rozporządzeniem o ochronie danych z uwzględnieniem *Systems Development Life-Cycle*, tak, aby odnieść model ochrony danych w fazie projektowania do faz produkcji systemów ICT. Celem autora było ustalenie czy art. 25 RODO jest potrzebny jako obowiązująca regulacja w przepisach ogólnego rozporządzenia o ochronie danych oraz jak należy postrzegać art. 25 RODO w ujęciu praktycznym.

W rozdziale IV pt. Normy i standardy bezpieczeństwa informacji oraz ochrony danych osobowych w kontekście ochrony danych w fazie projektowania autor dokonał analizy modelu ochrony danych w fazie projektowania w stosunku do mechanizmów certyfikacji, powszechnie stosowanych norm i standardów bezpieczeństwa oraz modeli oceny dojrzałości (z perspektywy technologicznej). Przedmiotem analizy był model ochrony danych w fazie projektowania odnośnie do regulacji prawnych standaryzacji i certyfikacji, przy ocenie, czy ten model ma wpływ na wartości analizowanych instytucji prawnych i zapewnienie ochrony danych w fazie projektowania. Autor zajął się także analizą pozaprawnych standardów oraz mechanizmów certyfikacji w kontekście ich oddziaływania na możliwość wykazania zgodności z wymaganiami art. 25 RODO.

W rozdziale V pt. Ocena i propozycja rozszerzenia modelu ochrony danych w fazie projektowania oraz ochrony danych jako wartości domyślnej model ochrony danych w fazie projektowania poddano ocenie w kluczowych obszarach jego stosowania oraz przedstawiono propozycję rozszerzonego podejścia do ochrony danych w fazie projektowania.

Podsumowując ocenę systematyki rozprawy doktorskiej należy wskazać, że jest

ona prawidłowa. Autor rozpoczął rozważania od zagadnień ogólnych i wprowadzających do rozważań zasadniczych. Omówił zatem pojęcie i różnice pomiędzy prawem do prywatności a prawem do ochrony danych osobowych. W rozdziale kolejnym zajął się już istotnym aspektem tematyki rozprawy doktorskiej, czyli ochrona danych w fazie projektowania, wskazując historyczny rozwój ochrony prywatności i danych osobowych w fazie projektowanie w prawie polskim, unijnym i międzynarodowym, a następnie także rozwinął przedmiotowe zagadnienia w perspektywie technologicznej (PETs) i (PIT).

Ciekawe były następne rozważania odnoszące się do zapewnienia zgodności z regulacjami w zakresie ochrony danych osobowych w kontekście *data protection by design* oraz *data protection by default*. Chodziło tu o ocenę planowania projektu, gdzie analizuje się i identyfikuje wymagania systemowe, następnie fazę projektowania systemu do przetwarzania danych osobowych, i działania operacyjne mając na celu monitorowanie i przetwarzanie danych osobowych. Ostatecznie autor omówił także zagadnienia związane z wpływem norm i standardów bezpieczeństwa informacji na zakres ochrony danych osobowych w kontekście ochrony danych w fazie projektowanie. Rozprawa kończy się omówieniem propozycji rozszerzenia modelu ochrony danych osobowych w fazie projektowania oraz ochrony danych jako wartości domyślnej. Mamy tu do czynienia zatem z opracowaniem w kompleksowym, oryginalnym, i temu służy przyjęta systematyka. Rozprawa zawiera także wstęp i zakończenia zawierające zebranie wniosków przedstawionych przez autora w poszczególnych rozdziałach pracy.

3. Pod względem metodologicznym rozprawa doktorska także została w sposób prawidłowy przygotowana. Autor zastosował metodę historyczną, metodę prawnoporównawczą oraz metodę dogmatycznoprawną. Wykorzystano także do analizy metodę aksjologiczną oraz teoretycznoprawną. Wybrane metody badawcze wykorzystano w celu przeprowadzenia analiz na wielu płaszczyznach z uwzględnieniem zagadnień o charakterze interdyscyplinarnym. (prawo prywatne, prawo publiczne, nowe technologie). Metodę dogmatycznoprawną Autor wykorzystał do analizy obowiązujących regulacji prawnych odnośnie do ochrony danych w fazie projektowania z uwzględnieniem orzecznictwa i literatury. Metoda historyczna była zastosowana dla oceny tendencji zdarzeń, które miały wpływ na powstanie i dalszy rozwój modelu ochrony prywatności w fazie projektowania oraz modelu ochrony

danych w fazie projektowania. Metodę porównawczą autor wykorzystał w celu poddania ocenie relacji wewnętrznych oraz zewnętrznych dla modelu ochrony danych w fazie projektowania. Chodziło o podobieństwa modeli *privacy by design* oraz *data protection by design*; oraz relacji wewnętrznych relacji modelu *data protection by design* z regulacjami zawartymi w przepisach prawa oraz zewnętrznych relacji modelu *data protection by design* z powszechnie stosowanymi standardami i dobrymi praktykami ochrony bezpieczeństwa lub ochrony prywatności.

3. Uwagi szczegółowe

Już na wstępie należy ocenić pozytywnie wywody merytoryczne zawarte w niniejszej rozprawie doktorskiej. Autor, na podstawie dokonanych analiz dochodzi do wniosku, że model ochrony danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych podlega ocenie wielowymiarowej, ponieważ jedynie takie podejście daje możliwość identyfikacji zastosowanie *data protection by design*, zapewniając rozwiązania korzystne dla każdej ze stron. Do oceny modelu ochrony danych w fazie projektowania należy, w ocenie autora uwzględnić, kontekst legislacyjny, kontekst stosowania modelu przez podmioty zobowiązane oraz perspektywę oceny tego modelu przez organy ochrony danych osobowych. Ocena tego modelu, jak prawidłowo wskazuje autor, winna także uwzględniać relację z modelem teoretycznym *privacy by design*, relację z normami i dobrymi praktykami w obszarze ochrony prywatności i bezpieczeństwa informacyjnego, relację z regulacjami dotyczącymi zatwierdzonych mechanizmów certyfikacji, relację względem innych norm występujących w RODO oraz ocenę pod względem implementacji z perspektywy podmiotu zobowiązanego.

Ostatecznie autor dochodzi do słusznego wniosku, że ocena skuteczności *data protection by design* jako instrumentu prawnego winna uwzględnić wpływ modelu ochrony danych w fazie projektowania na ochronę praw i wolności jednostki.

Autor zauważył, że istotnym zagadnieniem wpływającym na trudność stosowania art. 25 RODO, będzie brak dostępu do odpowiednich zasobów praktycznej wiedzy na temat ochrony danych w fazie projektowania i studium przypadków. W tym zakresie chodzi o wiedzę specjalistyczną administratorów danych, którzy mogą korzystać mogą z udostępnionych przez EROD wytycznych opracowanych przez niektóre

organy ochrony danych dokumentów, międzynarodowych norm i standardów technicznych oraz dokumentów wydanych przez ENISA.

Autor zauważył także, że model ochrony danych w fazie projektowania jest ograniczony przez zakres stosowania przepisów RODO, ale także i dyrektywy 2016/68

Należy także zaaprobować pogląd autora, że między *privacy by design* a *data protection by design* istnieją różnice w zakresie ich stosowania, mimo, że pierwszy stanowi jedynie teoretyczną koncepcją, a drugi jest już regulacją prawną. *Data protection by design* to koncepcja wywodząca się z *privacy by design*, czyli na modelu, który został opracowany w kanadyjskim systemie prawnym przez dr Ann Cavoukian, natomiast model *privacy by design* został uwzględniony w systemie prawnym Unii Europejskiej jako *data protection by design* oraz *data protection by default* w art. 25 RODO oraz art. 20 Dyrektywy Policyjnej. Autor słusznie jednak zwraca uwagę, że nie można tych pojęć zamiennie i że zastosowanie *data protection by design* wiąże się z wykorzystaniem „innych zasad gry” niż w przypadku *privacy by design*, co ma doniosły wpływ na praktykę ochrony danych osobowych.

Autor udzielił też odpowiedzi na pytanie, czy model *data protection by design* oraz *data protection by default* powinien funkcjonować w systemie prawnym? Autor uznaje, że model ochrony danych w fazie projektowania należy rozpatrywać zarówno z perspektywy inne regulacji mogących mieć podobne funkcje. Chodzi tu o realizację w systemie prawnym model ochrony danych w fazie projektowania poprzez promowanie ochrony danych już w fazie projektowania rozwiązań służących do przetwarzania danych osobowych. Obecna regulacja wpłynęła na to, że samo pojęcie *data protection by design* ma dodatkową wartość dodaną w postaci większej świadomości stron zobowiązanych do stosowania art. 25 RODO. Wskazany czynnik w postaci zwiększonej świadomości może bezpośrednio wpłynąć pozytywnie na prawa i wolności osób fizycznych.

Autor zauważa także, że model ochrony danych w fazie projektowania przyczynia się do „stworzenia gwarancji technologicznych i organizacyjnych”. Skuteczność ochrony prywatności oraz ochrony danych w fazie projektowania jest uzależniona od tego, czy zostaną zaimplementowane odpowiednie środki techniczne i organizacyjne, które pomagają ograniczać lub uniemożliwiać występowanie naruszeń prawa przez

samego administratora, a także przez strony trzecie. Ze względu na ochronę danych w fazie projektowania istotne są środki techniczne, których przykłady stosowania zostały podane w rozdziale II. Stosowanie *Privacy-Enhancing Technologies* podniosło złożoność technologiczną procesu przetwarzania danych osobowych. Poziomą złożoność technologiczną zwiększył jednocześnie zapotrzebowanie wśród administratorów danych na dodatkowe zasoby, np. ludzkie, technologiczne, finansowe, aby możliwe było zapewnienie zgodności z wymaganiami art. 25 RODO.

4. Uwagi formalne.

Praca doktorska jest napisana poprawnie pod względem językowym, Nie obserwuje się tutaj błędów stylistycznych, interpunkcyjnych czy ortograficznych. Przypisy są bardzo bogate, co świadczy o gruntownym przygotowaniu autora, znajomości poglądów doktryny krajowej i co ważne, z uwagi na tematykę międzynarodową rozprawy, także zagranicznej. Na szczególne uznanie zasługuje, że autor wykorzystał orzecznictwo polskie, zagraniczne i trybunałów europejskich. Na uwagę zasługuje, że wykorzystanie dokumentów określających standardy techniczne bezpieczeństwa danych w fazie tworzenia projektów informatycznych, co uwzględnia także kontekst techniczny.

Należy też zaaprobować poglądy autora w zakresie obowiązków administratorów monitorowania i oceny ryzyka wyboru niektórych środków technicznych w postaci *Privacy-Enhancing Technologies* z tego powodu, że określone rozwiązania zwiększają ryzyko utraty danych osobowych lub nieumiejętne zastosowanie tych technologii zagwarantuje jedynie pozorną ochronę danych osobowych. Skuteczne wykorzystywanie z modelu ochrony danych w fazie projektowania wraz z prawidłowym zastosowaniem środków technicznych może przynieść potencjalną oszczędność czasu oraz zasobów finansowych związaną z tym, że wcześniej zaprojektowany system lub proces przetwarzania danych osobowych nie będzie wymagać kosztownego przeprojektowywania tego systemu lub procesu przetwarzania, aby osiągnąć stan zgodności z regulacjami dotyczącymi ochrony danych osobowych. Autor zauważa słusznie, że w opozycji do *Privacy-Enhancing Technologies* pozostaje *Privacy-Invasive Technologies*, wpływające negatywnie na prawo do prywatności lub prawo do ochrony danych osobowych jednostki (np. mechanizmy *dark patterns*). Wówczas rozwiązania z grupy *Privacy-Enhancing Technologies* mogą zapewnić

ochronę przed niechcianą ingerencją w prywatność. I dlatego, wniosek autora, że administratorzy danych zatem powinni projektować rozwiązania, które w miarę możliwości powinny ograniczyć.

Autor zajął się także samym procesem wdrożenia modelu ochrony danych w fazie projektowania. I tak, autor dokonał oceny tego wdrożenia przez umiejscowienie modelu ochrony danych w fazie projektowania w ramach *Systems Development Life Cycle*, co pozwoliło przybliżyć do tego modeli implementację art. 25 RODO. Autor podkreślił także

iteracyjność, która występuje w procesach wytwórczych systemów informatycznych. Zwykle nie jest możliwe zidentyfikowanie wszystkich wymagań oraz wszystkich problemów związanych z przetwarzaniem za pierwszym razem, ale podczas procesu testowania wymagań mogą pojawić się problemy techniczne oraz logiczne, które wywrą wpływ na prawa i wolności podmiotów danych. I dlatego, w ocenie autora model *data protection by design* w celu zapewnienia odpowiedniego poziomu ochrony danych powinien zostać wpisany w cykl rozwojowy środków technicznych organizacyjnych służących do przetwarzania danych osobowych. Model ochrony danych w fazie projektowania wymaga od administratora danych interdyscyplinarnego podejścia do problematyki ochrony danych osobowych, mając pod uwagę także cykl życia danych od momentu określania sposobów przetwarzania danych osobowych przez przetwarzanie i retencję danych osobowych aż do zakończenia przetwarzania danych osobowych.

Zasadnie autor zauważył, że zapewnienie zgodności z art. 25 RODO w całym cyklu życia danych osobowych wymaga od administratora danych zapewnienia odpowiedniej synergii z innymi regulacjami dotyczącymi przetwarzania danych osobowych. Dopiero wówczas stosowanie art. 25 RODO łącznie z innymi instrumentami prawnymi w ramach *Systems Development Life Cycle* prowadzi do maksymalizacji potencjału tej regulacji. Podmioty zobowiązane również powinny uwzględniać cechy charakterystyczne przetwarzania danych osobowych, aby eliminować lub ograniczać ryzyka związane z nieplanowanym przetwarzaniem.

Analizy problematyki zagadnienia *data protection by design* oraz *data protection by default* pozwala wskazać na istotne wady, które łącznie ograniczają możliwości

wykorzystania tej instytucji jako bardziej skutecznego modelu prawnej ochrony danych osobowych. Maksymalizacja efektywności oddziaływania instytucji *data protection by design* z art. 25 RODO oraz samego podejścia *design* jest możliwa przez połączenie tych dwóch grup działań. Według autora, proponowanym rozwiązaniem, które dotyczy modelu *data protection by design* oraz *data protection by default*, jest przeprowadzenie zmian i aktywności o charakterze prawnym i pozaprawnym łącznie składające się na trzy kluczowe obszary, które mogą zwiększyć jego efektywność jako instrumentu prawnej ochrony danych osobowych. Obejmują one obszar ochrony praw podstawowych w fazie projektowania, obszar ochrony prywatności i ochrony danych w fazie projektowania w systemie prawa oraz obszar dotyczący edukacji i standaryzacji ochrony prywatności i ochrony danych w fazie projektowania. Autor zauważył, że obowiązek wykorzystania modelu *data protection by design* jest ograniczony wyłącznie do obszaru ochrony danych osobowych, co w przypadku wszelkich urządzeń i rozwiązań, które nie przetwarzają informacji będących danymi osobowymi, powoduje węższy zakres stosowania tej regulacji i prowadzi do pominięcia podejścia *data protection by design* dla wielu rozwiązań technologicznych.

W ocenie autor, i pogląd ten należy ocenić pozytywnie, wpływ na podnoszenie skuteczności i rozliczalność prawnego instrumentu, jakim jest model ochrony danych w fazie projektowania, mają normy w obszarze ochrony prywatności, bezpieczeństwa informacyjnego, jakości i ciągłości działania. Chodzi tu, o normy, standardy i zestawy dobrych praktyk, czyli NIST Privacy Framework, NIST Cybersecurity Framework, SOC 2 Type 1 lub Type 2, normy z serii ISO 27001, a także normy ISO 29100 i ISO 29151. Są stosowane przez administratorów danych oraz podmioty przetwarzające, aby wykazać określony poziom jakości w obszarze przetwarzania danych osobowych oraz w sposób pośredni wykazać postępowanie podmiotu ukierunkowane na zgodność z art. 25 RODO. W przypadku niektórych z nich istnieje możliwość certyfikacji przez niezależne podmioty certyfikujące.

Są to zagadnienia merytoryczne, które wskazano jedynie przykładowo. Autor bowiem wypowiada się co do wszystkich zagadnień badawczych, które wskazał we wstępie i udziela na nie przekonującej odpowiedzi wraz z pełnym uzasadnieniem. Na uwagę zasługują wnioski zawarte w rozdziale V rozprawy, że zachodzi konieczność rozszerzenia modelu ochrony danych osobowych w fazie projektowania oraz ochrony danych jako wartości domyślnej.

5. Uwagi końcowe

Mając na uwadze powyższe uwagi, jak widać bardzo pozytywne, uważam, że przedstawiona od recenzji rozprawa doktorska mgr Piotra Siemieniaka pt. „Ochrona danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych” spełnia wszystkie kryteria przewidziane w art. ustawy z 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce i stanowi podstawę do dalszych etapów przewodu doktorskiego i stanowi podstawę do dalszych etapów w przewodzie doktorskim.

Prof. dr hab. Jacek Gołaczyński

Wrocław, 6.02.2023r.

