Prof. dr hab. Andrzej Wróbel
Instytut Nauk Prawnych
Polskiej Akademii Nauk
w Warszawie

Recenzja rozprawy doktorskiej
Pana mgr Marcina Rojszczaka
„Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji"
Warszawa 2018, ss. 398

I. Uwagi ogólne

Recenzowana rozprawa doktorska stanowi studium z dziedziny prawa międzynarodowego, prawa Unii Europejskiej i prawa polskiego, którego przedmiotem jest ochrona prawa do prywatności w związku z nowymi technikami/modelami przetwarzania danych na przykładzie *cloud computing, Big Data* i masowej inwigilacji.

Wybór zagadnienia naukowego będącego przedmiotem niniejszej rozprawy doktorskiej jest trafny i należycie uzasadniony (zob. *Wprowadzenie*). Nie ma bowiem wątpliwości, że problematyka zagrożeń prawa do prywatności wywołanych nowymi technikami przetwarzania danych osobowych w Cyberspace doczekała się wprawdzie licznych i obszernych opracowań naukowych, to jednak podjęcie się opracowania tego niezwykle złożonego zagadnienia prawnego w stanie prawnym po wejściu w życie RODO należy uznać za konieczne i uzasadnione.

Tytuł rozprawy jest sformułowany zasadniczo w sposób prawidłowy, chociaż użyte w nim terminy odbiegają od przyjętych konwencji językowych, a przez to mogą stwarzać ryzyko pewnych konfuzji. Pierwsze wiąże się ze zwrotem „ochrona prywatności", który nie uwzględnia aspektu podmiotowego, a mianowicie prawa do prywatności ujętego jako publiczne prawo podmiotowe (prawo konstytucyjne), będącego wszakże głównym

przedmiotem analiz rozprawy; nie jest też jasne, czy ochrona prywatności obejmuje problemy związane z treścią i granicami tego prawa podmiotowego czy również instrumenty prawne przysługujące osobie w razie bezprawnego naruszenia prawa do prywatności, np. droga sądowa. Autor wydaje się rozumieć to pojęcie szeroko, bowiem analizuje nie tylko treść prawa do prywatności/prawa do ochrony danych osobowych, ale także zagadnienie właściwej jurysdykcji czy instytucjonalnych aspektów nadzoru nad przetwarzaniem danych osobowych. Dalej, w tytule rozprawy pojawia się zwrot „prawo międzynarodowe", który ma utrwalone znaczenie i z pewnością nie obejmuje swoim zakresem prawa Unii Europejskiej jako „*new legal order*"; tymczasem głównym przedmiotem analiz dogmatycznych rozprawy pozostaje prawo Unii Europejskiej, w tym zwłaszcza nieobowiązująca dyrektywa 95/46 WE i rozporządzenie 2016/679. Wreszcie, rozprawa nie obejmuje swoim zakresem wszystkich zagrożeń wynikających z wszystkich nowych technik przetwarzania informacji, lecz tylko niektóre z tych zagrożeń wynikających jedynie z dwóch technik/modeli przetwarzania, a *cloud computing* i *Big Data*, przy czym raczej przetwarzania danych osobowych niż przetwarzania „informacji."

Autor recenzowanej rozprawy wypowiada się wyraźnie odnośnie do przyjętych w rozprawie metod badawczych, które określa jako metoda formalno-dogmatyczna, uzupełniona metodą prawno-porównawczą oraz historyczno-porównawczą (s. 15). Lektura rozprawy skłania wszakże do wniosku, że zawarte w niej analizy dogmatyczno-prawne zdecydowanie przeważają nad innymi typami analiz, co z jednej strony czyni rozprawę niewątpliwie mniej atrakcyjną intelektualnie, z drugiej zaś opartą na solidnej podstawie normatywnej, którą tworzą przepisy prawa unijnego, „klasycznego" prawa międzynarodowego i prawa polskiego, co z kolei podkreśla kompleksowość i wielostronność odnośnych analiz naukowych. Za trafny uważam wybór prawa USA jako punktu odniesienia analiz komparatystycznych, chociaż wypada zauważyć, że prawo kanadyjskie przewiduje trzecią alternatywę ochrony danych osobowych, w porównaniu z amerykańskim *industry self-regulating approach* i bardziej restrykcyjną regulacją unijną (zob. *Personal Information Protection and Electronics Documents Act*).

Podstawowa teza rozprawy, sformułowana we *Wprowadzeniu*, to twierdzenie, że „istniejące regulacje prawne – w szczególności prawnomiędzynarodowe – nie zapewniają skutecznej ochrony przed zagrożeniami dla prywatności wynikającymi z nowoczesnych technik przetwarzania danych"(s. 13); teza ta jest następnie konkretyzowana i rozwijana w

Części 2. rozprawy: *OCHRONA PRYWATNOŚCI W DOBIE SPOŁECZEŃSTWA INFORMACYJNEGO – WYBRANE ZAGADNIENIA.* Niewątpliwie wytycza ona kierunek rozważań, którym podporządkowana jest struktura rozprawy. Z tego punktu widzenia przedstawienie tej tezy już we *Wprowadzeniu* było jak najbardziej celowe i uzasadnione. Problem trafności i racjonalności zasadniczej tezy rozprawy o nieskuteczności prawa międzynarodowego w zakresie ochrony (prawa do) prywatności w sferze nowych technik przetwarzania danych oraz jej uzasadnienia będzie przedmiotem dalszych uwag.

Recenzowana rozprawa jest napisana pragmatycznie jasnym, prostym i komunikatywnym językiem.

Rozprawa doktorska została przygotowana według stanu prawnego na 26 marca 2018 r., nie zaś, jak pisze się na s. 17, „na dzień 26 marca 2017 roku."

Struktura rozprawy doktorskiej Pana mgra Marcina Rojszczaka jest zbudowana poprawnie, z pewnymi wszakże zastrzeżeniami, o których niżej. Autor podzielił rozprawę na dwie części: Można w niej wyróżnić dwie zasadnicze części: *(CZĘŚĆ 1. OCHRONA PRYWATNOŚCI: HISTORIA, TERAŹNIEJSZOŚĆ I PRZYSZŁOŚĆ,* na którą składają się rozdziały 1. Prywatność i cyberprzestrzeń – zagadnienia podstawowe, 2. Prawnomiędzynarodowe i konstytucyjne źródła norm w obszarze ochrony prywatności, 3. Ewolucja zasad ochrony danych osobowych, 4. Prawo UE jako narzędzie podnoszenia standardów w obszarze prywatności w cyberprzestrzeni, 5. Uregulowania szczegółowe w prawie polskim; CZĘŚĆ 2. *OCHRONA PRYWATNOŚCI W DOBIE SPOŁECZEŃSTWA INFORMACYJNEGO – WYBRANE ZAGADNIENIA,* którą tworzy rozdział 6. Przetwarzanie danych w modelu chmury obliczeniowej, 7. Analizy dużych zbiorów danych (Big Data), 8. Prywatność a bezpieczeństwo publiczne – podstawy prawne prowadzenia programów masowej inwigilacji obywateli ; rozprawę zamykają *Wnioski końcowe*, które zawierają rekapitulację zasadniczych tez i wniosków rozprawy. Niewątpliwie część pierwsza rozprawy ma charakter wprowadzający do rozważań zawartych w części drugiej, w której prowadzone są analizy i formułowane wnioski zasadniczej – z punktu widzenia celów i założeń rozprawy – natury, a mianowicie dotyczące oceny rozwiązań prawnych dotyczących nowych technik przetwarzania danych w kontekście zapewnienia skuteczności prawa do ochrony prywatności/prawa do ochrony danych osobowych. Mając na uwadze tę kwalifikację wyróżnionych części rozprawy, należy stwierdzić, że Część 1 rozprawy (251 stron) jest

nieproporcjonalnie rozbudowana w stosunku do Części 2 (136 stron), a nadto zbyt wiele miejsca w Części 1 poświęcono nieobowiązującej dyrektywie 95/46 WE.

Biorąc pod rozwagę powyższe należy stwierdzić, iż konstrukcja recenzowanej rozprawy i zasadnicze elementy jej treści zasługują na ocenę pozytywną.

II. Układ rozprawy i struktura podziału jej treści

W Części 1. rozprawy, mającej w istocie charakter deskryptywny, opisano normatywne i nienormatywne relacje między prywatnością a cyberprzestrzenią (Rozdział 1), podstawy prawne prawa do prywatności i jego ochrony (Rozdział 2), ewolucję podstaw prawnych i zasad ochrony danych osobowych w klasycznym prawie międzynarodowym (Rozdział 3), prawie Unii Europejskiej (Rozdział 4) i prawie polskim (Rozdział 5).

W Rozdziale 1 przedstawiono rozmaite koncepcje prywatności, jednakże w sposób nieusystematyzowany i wybiórczy; pełna i metodyczna realizacja tego zamierzenia badawczego wymagałaby odrębnej monografii, tym bardziej że uwzględnia się nie tylko perspektywę prawną, ale i pozaprawną, w tym socjologiczną. Niewątpliwie na aprobatę zasługuje pogląd, że prawo do prywatności jako prawo człowieka jest prawem podmiotowym publicznym, mającym swoje źródło w godności człowieka (s. 28), aczkolwiek Autorem przedstawionej charakterystyki praw człowieka nie jest K. Motyka, lecz Robert Alexy (*Die Institutionalisierung der Menschenrechte im demokratischen Verfassungsstaat*; w: *Philosophie der Menschenrechte*, Frankfurt am Main 1998, s. 244 i nast.). Trafne jest także stanowisko, że ochrona prywatności jest pojęciem zdecydowanie szerszym niż ochrona danych osobowych (s. 31), jednakże należało szerzej uzasadnić tę słuszną tezę, niż uczyniono to w rozprawie, tym bardziej że prywatność jest pojęciem notorycznie wieloznacznym (np. w piśmiennictwie amerykańskim wyróżnia się: prywatność w sensie fizycznym jako odosobnienie, bezpieczeństwo, integralność cielesna; prywatność w sensie informacyjnym jako poufność, ochrona danych, tajemnica lub anonimowość, w szczególności korespondencji, prywatność w sensie decyzyjnym jako wolność, wybór lub autonomia w procesie podejmowania decyzji o płci, prawach reprodukcyjnych, małżeństwie, rodzinie i opiece zdrowotnej, prywatność w sensie wspólnotowym jako prawo jednostek do przynależności do wyłącznie prywatnych zrzeszeń i politycznych ugrupowań (A.L. Allen,

Constitutional Law and Privacy, w: *A Companion to Philosophy of Law and Legal Theory*, Singapore 2010, s. 147). Omawiając problemy prawne cyberprzestrzeni Autor formułuje tezę (s. 41), że „(Z) perspektywy obszaru badawczego niniejszej pracy, istotniejszym zagadnieniem niż kwestia nadzoru nad technicznym funkcjonowaniem Internetu, jest problem określania prawa właściwego do regulacji zdarzeń, mających miejsce w cyberprzestrzeni." Wprawdzie oba zagadnienia mieszczą się w szeroko pojmowanej sferze enforcement, lecz istotnie skuteczność norm dotyczących cyberprzestrzeni zależy w dużej mierze od skonstruowania spójnego systemu norm prawnomiędzynarodowych (ochronnych i regulacyjnych), standaryzujących przetwarzanie danych na płaszczyźnie międzynarodowej (s. 46). Rozdział 1 zakończony jest uwagą, którą należało wyeksponować we Wprowadzeniu, a mianowicie, że w rozprawie nie będą analizowane „aspekty identyfikacji i penalizacji cyberprzestępstw, ale (...) prawne mechanizmy prowadzące do ochrony sfery prywatności przed zagrożeniami związanymi z rozwojem nowych sposobów przetwarzania danych."

W Rozdziale 2 opisano podstawy prawne prawa do prywatności i jego ochrony zawarte w deklaracjach i paktach ONZ, EKPCZ, KPP i polskich przepisach konstytucyjnych oraz podjęto próbę zrekonstruowania treści tego prawa. W podsumowaniu tych analiz deskryptywnych Autor formułuje tezę o prawie do prywatności jako prawa nierozerwalnie związanego z godnością człowieka, o podobnym ukształtowaniu treści prawa do prywatności w systemie prawnym ONZ, EKPCz, KPP i Konstytucji RP, o przeważnie negatywnej strukturze obowiązku władzy publicznej z pewna koncesją na rzecz obowiązków pozytywnych, o zasadniczych różnicach między wyróżnionymi systemami prawnymi w zakresie instytucjonalnego usytuowania organu kontrolnego (sądu) oraz wpływu norm prawnych na dochodzenie roszczeń przed sądami krajowymi (s. 97). W związku z tym Autor nie ogranicza się do rekonstrukcji prawa do prywatności w rozumieniu np. MPPOP, lecz poświęca uwagę także spornej kwestii miejsca tego Paktu w systemie źródeł prawa RP, w tym problemowi pierwszeństwa umów międzynarodowych na gruncie Konstytucji RP (pkt 2.2.3). Autor poprawnie rekonstruuje elementy treści prawa do prywatności, zawarte implicite w art. 8 EKPCz, w tym w związku z ochroną danych osobowych. Pomija jednak ważny element tego prawa, którym jest prawo jednostki do pełnej informacji np. o zagrożeniach dla zdrowia (sprawa Roche). Ważna jest konkluzja, ze ochrona danych osobowych ma podstawowe znaczenie dla gwarancji przewidzianych w art. 8 (s. 65). Problem miejsca Konwencji w systemie prawnym RP został potraktowany niezwykle oszczędnie. Autor powołuje się na wyrok SN w sprawie I PZ 5/07, gdy tymczasem w tej kwestiach wypowiedział się obszernie

Sąd Najwyższy w wyroku z dnia 28 listopada 2008 r. V CSK 271/08: po pierwsze – „Konwencja o ochronie praw człowieka stanowi część polskiego porządku prawnego, została bowiem przez Rzeczpospolitą Polską ratyfikowana za uprzednią zgodą wyrażoną w ustawie (zob. art. 1 ustawy z dnia 2 października 1992 r. o ratyfikacji Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, Dz. U. Nr 85, poz. 427 oraz oświadczenie rządowe z dnia 7 kwietnia 1993 r., Dz. U. Nr 61, poz. 285). Postanowienia Konwencji mogą zatem stanowić nie tylko wskazówkę interpretacyjną przy wykładni przepisów prawa wewnętrznego, ale i bezpośrednią podstawę rozstrzygnięć organów krajowych, jeżeli pozwala na to ich charakter. Konwencja o ochronie praw człowieka ma przy tym pierwszeństwo przed ustawą, jeżeli ustawy tej nie da się pogodzić z Konwencją (art. 91 ust. 2 Konstytucji).";- po drugie – „ostateczny wyrok Trybunału uwzględniający skargę wiąże państwo, przeciwko któremu została ona skierowana. Państwo to zatem nie może kwestionować stwierdzonego tym wyrokiem naruszenia praw gwarantowanych Konwencją. Odmienna wykładnia przekreślałoby zresztą sens utworzenia Europejskiego Trybunału Praw Człowieka, który ma zapewniać przestrzeganie zobowiązań wynikających z Konwencji i jej protokołów."- po trzecie – „Ostateczny wyrok Trybunału stwierdzający naruszenie praw człowieka oznacza, że państwo naruszyło swoje międzynarodowe zobowiązanie do ich przestrzegania. Stwierdzone nim naruszenie Konwencji wiąże przy tym wszystkie władze tego państwa, zarówno władzę ustawodawczą, jaki i wykonawczą oraz sądowniczą." Autor poprawnie rekonstruuje charakter prawny KPP i podstawowe zasady jej stosowania w krajowym porządku prawnym. Wydaje się jednak, ze mimo powściągliwości orzecznictwa i doktryny na temat relacji między art. 7 i 8 KPP, Autor powinien zająć jednoznaczne i szerzej umotywowane stanowisko (uzasadnione celami badawczymi rozprawy) niż uczynił to na s. 75 stwierdzając ogólnikowo, że „(R)ozgraniczenie gwarancji związanych z ochroną prywatności (art. 7) i ochroną danych osobowych (art. 8) wskazuje, że terminy te – w ocenie prawodawcy – są w pewnych obszarach rozłączne, co oznacza w szczególności, że nie każde naruszenie ochrony danych osobowych prowadzi do ingerencji w prawo do prywatności."; tym bardziej, ze także stanowisko polskiego Trybunału Konstytucyjnego w tej kwestii jest równie niejednoznaczne; Autor poświęca jednak niewiele miejsca temu centralnemu dla rozprawy zagadnieniu kolizji lub konkurencji prawa do prywatności i prawa do ochrony danych osobowych (zob. rozważania na s. 90-92); podzielam krytykę wyroku TK w sprawie K 33/08 przedstawioną na s. 95.

W Rozdziale 3 przedstawione kształtowanie się podstaw prawnych ochrony danych osobowych w aktach prawnych uniwersalnego i regionalnego prawa międzynarodowego, przy czym słusznie poświecono najwięcej miejsca analizie dogmatycznej Konwencji nr 108 Rady Europy z trafna oceną jej ograniczonego znaczenia w „faktycznym budowaniu jednolitej przestrzeni przetwarzania informacji" (s. 113) i interesującymi postulatami *de lege ferenda* (s. 124 i nast..) wzmocnienia skuteczności instrumentów prawno-międzynarodowych w tej dziedzinie.

Rozdział 4 zawiera opis kształtowania się podstaw prawnych ochrony danych osobowych w prawie Unii Europejskiej, zwłaszcza w prawie pochodnym (dyrektywa 95/46, dyrektywa 2002/58 i RODO). Opis ten i sposób ujęcia tej problematyki budzi jednak pewne zastrzeżenia: po pierwsze – Autor nie dostrzegł monograficznego opracowania tego zagadnienia, jakim jest książka M. Krzysztofka, *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014, w której rozważa się analogiczne zagadnienia, jak te poruszane w Rozdziale 4 recenzowanej rozprawy, po drugie – równoległe prowadzenie rozważań na tle poprzedniego stanu prawnego, tj. przed wejściem w życie RODO i obecnego stanu prawnego oraz dokonywanie porównań rozwiązań przyjętych w uchylonej dyrektywie z rozwiązaniami przyjętymi w RODO nie ma szerszego uzasadnienia z perspektywy celów i założeń rozprawy, po trzecie – stanowczo zbyt mało miejsca poświęcono analizie odnośnych postanowień dyrektywy 2002/58, którą Autor trafnie uznaje za „jeden z kluczowych elementów europejskiego modelu ochrony prywatności w cyberprzestrzeni" (s. 192), nie dostrzegając przy tym ważnego, interpretującego tę dyrektywę wyroku TSUE w sprawie C-203/15. Nie można także zgodzić się z poglądem, jakoby „(W) obszarze przetwarzania danych szczególnie wrażliwych przepisy rozporządzenia w większości powielają rozwiązania wprowadzone w dyrektywie 95/46." (por. odmienny pogląd M. Kuba, uwagi do art. 9, RODO. Ogólne rozporządzenie o ochronie danych. Komentarz. Redakcja naukowa E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 439. Autor nie zajmuje także własnego stanowiska w przedmiocie „wyraźnej zgody", pozostawiając to wykładni organów unijnych (s. 154). Mimo tych wątpliwości, ocena analiz zawartych w Rozdziale 4 jest ostatecznie pozytywna, zwłaszcza z uwagi na zdefiniowanie i usystematyzowanie obszarów regulacji ochronny danych osobowych, relewantnych z punktu widzenia celów i hipotez badawczych. Za ważne i inspirujące należy uznać rozważania dotyczące niezależności organu nadzoru (s. 177 i nast.) czy statusu organów regulacyjnych w ochronie danych osobowych/prywatności w obszarze

łączności elektronicznej (s. 184 i nast.), chociaż pomija się milczeniem ważny dla tego obszaru wyrok TSUE w sprawie C-424/15.

Rozdział 5 poświęcony jest analizie dogmatycznej przepisów prawa polskiego regulujących ochronę danych osobowych, przy czym Autor słusznie koncentruje rozważania wokół dwóch zagadnień prawnych, a mianowicie wpływowi RODO na zakres i przedmiot regulacji krajowej oraz ochronie danych osobowych w przepisach szczególnych. Odnośnie do pierwszego z tych zagadnień prawnych przyjmuje się trafnie, ze wejście w życie RODO nie oznacza pasywności prawodawcy polskiego. Autor identyfikuje te obszary ochrony danych osobowych, które mogą lub powinny być przedmiotem interwencji ustawodawczej, a mianowicie: „ obszary, dla których ogólne rozporządzenie nie stanowi wyłącznej regulacji krajowej; obszary regulowane przez przepisy krajowe stanowione w wykonaniu innych norm prawa UE (w szczególności – dyrektyw);obszary znajdujące się poza zakresem istniejących regulacji unijnych, w tym związane z dziedzinami wyłączonymi z prawa UE." (s. 218). Rozważania dotyczące projektowanej ustawy o ochronie danych mają charakter historyczny wobec uchwalenia ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000). Błędne jest nazywanie aktów wydawanych przez „prawodawcę krajowego" „aktami delegowanymi i wykonawczymi" (s. 217); nazwa ta jest zastrzeżona dla aktów Unii stanowionych na podstawie art. 290 i 291 TFUE.

Część 2. Rozprawy, stanowiąca część analityczną i ściśle związaną z tematem rozprawy, poświęcona jest trzem zagadnieniom, a mianowicie zagrożeniom dla prywatności wynikającym z przetwarzania danych w chmurze obliczeniowej (Rozdział 6), analiz Big Data (Rozdział 7) oraz masowej inwigilacji obywateli (Rozdział 8). Wybór tych zagrożeń dla prywatności i ochrony danych osobowych uważam za trafny.

Nie ma wątpliwości, ze usługi oferowane w formie Cloud Computing dają możliwość jednoczesnego dostępu wielu użytkowników do zasobów danych i informacji z każdego miejsca i w każdym momencie, co powoduje znaczne ryzyko dla prywatności i bezpieczeństwa danych osobowych. Wirtualizacja (pkt 6.3.5. rozprawy), ale także „wielodzierżawa" („współkorzystanie") i skalowalność to te cechy chmury obliczeniowej z którymi związane są „ potencjalnie negatywne konsekwencje dla poufności przetwarzanych informacji (s. 261). Autor trafnie ogranicza zakres analiz dogmatycznych do usług w modelu SaaS, koncentrując się na kryterium poufności (s. 259). Spośród licznych zagadnień

prawnych związanych z przetwarzaniem danych osobowych w chmurze obliczeniowej, wybiera do analiz dwa z nich, a mianowicie charakter prawny umowy o świadczenie usług/przetwarzania danych w chmurze i prawo właściwe dla tych umów. Zagadnienia te były rozważane w piśmiennictwie (np. E. Molenda-Kropielnicka, *Cloud Computing – zagadnienia prawne*, Prace z Prawa Własności Intelektualnej 2013, z. 119), do której Autor się nie odnosi), a ostatnio stały się (z wyjątkiem prawa właściwego) przedmiotem obszernej monografii A. Krasuskiego, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018. Zagadnienia te są niewątpliwie doniosłe dla ochrony prywatności i ochrony danych osobowych, lecz jedynie w fazie *enforcement*, a mianowicie w fazie dochodzenia roszczeń wynikłych z tytułu naruszenia prawa do prywatności i prawa do ochrony danych. Autor określa umowę o świadczenie usług w chmurze obliczeniowej jako umowę o przetwarzanie w chmurze, co jest niewłaściwe. Zresztą w tekście pkt6.4.2. częściej posługuje się prawidłowym określeniem tej umowy jako umowy o świadczenie usług. Z kolei omawiając „prawo właściwe i jurysdykcję dla umów przetwarzania w chmurze", koncentruje swoją uwagę na analizie rozporządzenia Rzym I, a zatem ustaleniu sądu i prawa właściwego dla umów w modelu *Cloud Computing*, pomija natomiast rozporządzenie Bruksela I. Interesująca i przekonująca jest natomiast krytyka unijnego podejścia do *Cloud Computing* (s. 282 i nast.).

W Rozdziale 7 przedstawiono podstawowe zagrożenia dla prywatności związane z analizą dużych zbiorów danych *Big Data*. Autor trafnie identyfikuje te zagrożenia na każdym z wyróżnionych czterech etapów *Big Data* ujętych jako proces obejmujący inne zjawiska niż tylko analiza danych (s. 295). Podejście to uważam za uzasadnione i otwierające nowe perspektywy badawcze. Pozwala to na formułowanie interesujących poznawczo wniosków, takich jak na przykład teza o ograniczonej skuteczności podstawowych technik ochrony danych osobowych (wrażliwych) takich jak anonimizacja czy pseudonimizacja danych (s. 297) w kontekście możliwości technicznych *Big Data*. Podzielić należy również stanowisko, ze wpływ na skuteczność ochrony danych osobowych/prywatności mogą mieć także różne źródła danych, które Autor starannie identyfikuje i opisuje (7.3.2.). Autor stawia postulat de lege ferenda szczególnej regulacji poświęconej *Big Data*, uzasadniając to wyłączeniem przetwarzania dużych zbiorów danych spod zakresu normowania RODO (s. 315).

Część 2 rozprawy zamyka Rozdział 8 poświęcony rozważaniom w przedmiocie masowej inwigilacji w kontekście ochrony prywatności i bezpieczeństwa publicznego, z wyłączeniem tzw. inwigilacji indywidualnej działalności penalizowanej (s. 326). Autor

prezentuje uzasadniony pogląd, ze szyfrowanie komunikacji i danych oraz VPN nie są skutecznym i adekwatnym narzędziem ochrony prywatności (s. 337). Autor starannie rekonstruuje europejski standard orzeczniczy w zakresie ochrony prywatności i danych osobowych w związku z masową inwigilacją i na tej podstawie dokonuje krytycznej analizy odnośnych przepisów prawa polskiego (s. 355 i nast.).

III. Wartość naukowa rozprawy

Recenzowana rozprawa doktorska poświęcona jest kilku powiązanym ze sobą merytorycznie i funkcjonalnie zagadnieniom prawnym, z których te opisane w Części 1. tworzą instytucjonalny kontekst dla szczegółowych zagadnień o bardziej analitycznym charakterze, badanych i krytycznie ocenianych w Części 2. Problemy zapewnienia ochrony prywatności i danych osobowych w związku ze zdefiniowanymi w rozprawie zagrożeniami wynikającymi z Cloud Computing, analiz Big Data i masowej inwigilacji, które uznaje się za zasadnicze i z trudem poddające się adekwatnej i skutecznej regulacji prawnej, są sytuowane na szerokiej płaszczyźnie normatywnej obejmującej prawo międzynarodowe, prawo europejskie i prawo polskie. Autor dostrzega konsekwencje wejścia w życie RODO dla tytułowej problematyki, ale także dla spójności prawa polskiego w tej dziedzinie. W zakresie optymalnego standardu normatywnego w tej dziedzinie wydaje się opowiadać za standardem europejskim, chociaż dostrzega też potrzebę ustanowienia jednolitych materialnych standardów prawnomiędzynarodowych. Mimo pewnych zastrzeżeń co do kompletności tez, analiz i wniosków oraz doboru literatury przedmiotu oraz w istocie deskryptywnego charakteru rozważań oceniam pozytywnie rekonstrukcję określonych przepisami prawa i orzecznictwa standardów ochrony prywatności i danych osobowych we wskazanych wyżej trzech poziomach normatywnych.

Część 2 rozprawy, poświęcona ochronie prywatności i danych osobowych w związku z nowymi technikami przetwarzania i analiz zawiera wiele interesujących hipotez badawczych, które podlegają krytycznej weryfikacji i falsyfikacji oraz uzasadnionej naukowo krytyce.

Twierdzenia zawarte w rozprawie są uporządkowane według jednolitej zasady merytorycznej, jaką jest teza o ograniczonej skuteczności obowiązujących przepisów

prawnych w ochronie prywatności i danych osobowych przed zagrożeniami wynikającymi z Cloud Computin, Big Data i masowej inwigilacji. Uzasadnianie twierdzeń dogmatycznych i pozadogmatycznych w prawoznawstwie polega na wskazywaniu argumentów skłaniających do uznania prawdziwości danego zdania. W związku z tym należy podkreślić, że zasadnicze tezy rozprawy są należycie uzasadnione. Autor w sposób konsekwentny przedstawia wiele argumentów różnej natury nakazujących uznać prawidłowość i poprawność zawartych w rozprawie hipotez, tez i wniosków.

Podsumowując pozytywne strony recenzowanej rozprawy należy podkreślić, że jest ona oparta na solidnym materiale źródłowym, zaś większość tez i wniosków jest niepodważalna, przekonująca i należycie uzasadniona. Wszystko to świadczy o tym, że Autor dobrze opanował naukowy warsztat badawczy, potwierdził swe uzdolnienia do twórczej pracy naukowej oraz zdolność samodzielnego rozwiązywania problemów naukowych z dziedziny prawa ochrony danych osobowych.

IV. Konkluzja

Recenzowana rozprawa doktorska stanowi oryginalne rozwiązanie przez jej Autora problemu naukowego z zakresu prawa ochrony danych osobowych . Merytoryczna zawartość rozprawy wykazuje, że Autor posiada ogólną wiedzę teoretyczną w tej dziedzinie prawa i umiejętność samodzielnego prowadzenia pracy naukowej nad zagadnieniem prawnym stanowiącym przedmiot tej rozprawy. W konkluzji stwierdzam, że rozprawa doktorska Pana magistra Marcina Rojszczaka spełnia wymagania, o których mowa w art. 13 ust. 1 ustawy z dnia 14 marca 2003 r. o tytule naukowym i stopniach naukowych oraz o stopniach i tytule w zakresie sztuki (tj. Dz.U. z 2017 r., poz. 1798).

Warszawa, dnia 16 lipca 2018 r.