Postęp technologiczny powinien przekładać się na funkcjonowanie jednostki w społeczeństwie oraz ułatwiać jej kontakty z organami publicznymi. Nowe technologie muszą być wykorzystywane proporcjonalnie do celu założeń. Ich stosowanie wymaga uregulowania prawnego. W tym samym ujawnia się pozytywny aspekt jurydyzacji. Proporcjonalność użytych środków to tzw. arystotelesowski „złoty środek" zapewniający równowagę i adekwatność w uwzględnianiu spraw obywatela przez państwo[1]. Przepisy prawne dotyczące przetwarzania danych osobowych potrzebują szczególnie rzetelnej i efektywnej regulacji w demokratycznym porządku prawnym, inaczej mogłyby być skierowane przeciwko obywatelowi. Doszłoby do naruszenia prawa do prywatności z art. 47 Konstytucja RP, art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, a także art. 2 Traktatu o Unii Europejskiej. Prawo ma gwarantować bezpieczeństwo, na co wskazywała już nowożytna myśl prawnicza[2].

Uważam, że uczelnia ma prawo do przetwarzania danych osobowych studenta w celu weryfikacji jego tożsamości, by przeprowadzić test zdalnie. Aby z tego prawa skorzystać, musi mieć podstawę do działania. Zgodnie z zasadą legalizmu z art. 7 Konstytucji RP organy działają na podstawie i w granicach prawa. Musi istnieć podstawa prawna do działań organów w porządku demokratycznego państwa prawnego (art. 2 Konstytucji RP)[3]. Obie zasady krzyżują się i chronią prawa jednostki. Miał rację Ronald Dworkin w książce „Biorąc prawa poważnie" określając zasady jako ważne i doniosłe w systemie prawa, ponieważ wyznaczają kierunek ich stosowania, akcentując jednocześnie ich autorytet w systemie prawnym[4].

Uczelnia jest organem administracji w znaczeniu funkcjonalnym[5]. Jej działanie musi wynikać z przestrzegania przepisów prawa. Zgodnie z wyrokiem NSA z dnia 21 kwietnia 2020 r., II OSK 1042/19: „każde działanie organu (…) musi mieć oparcie w obowiązującym prawie. Działanie na podstawie i w granicach prawa to działanie organu, który na podstawie przepisu prawa jest właściwy, i którego działanie oparte jest na przepisie prawa, który daje umocowanie do jego podjęcia[6]."

---

[1] Jeanne Hersch, *Wielcy myśliciele Zachodu. Dzieje filozoficznego zdziwienia*, Warszawa 2001, s.45.
[2] Roman Tokarczyk, *Filozofia prawa*, Lublin 2005, str. 107-109.
[3] *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2008, s. 6.
[4] Ronald Dworkin, *Biorąc prawa poważnie*, Wydawnictwo Naukowe PWN 1998, s. 64 i s.80.
[5] Zbigniew R. Kmiecik, *Postępowanie administracyjne, postępowanie egzekucyjne w administracji i postępowanie sądowo-administracyjne*, Warszawa 2017, s. 71-72.
[6] Wyrok NSA z dnia 21 kwietnia 2020 r., II OSK 1042/19.

Przetwarzanie danych osobowych przez uczelnię powinno odpowiadać celowi. Regulacje rozporządzenia PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w art. 5 ust. 1 pkt c) określa adekwatność przetwarzania danych osobowych do celu, tzw. „minimalizacja danych”[7]. Art. 288 Traktatu o funkcjonowaniu Unii Europejskiej wskazuje, iż rozporządzenie unijne ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowane[8]. Przepisy rozporządzenia mają bezpośrednią skuteczność i są bezpośrednio stosowane w państwie członkowskim. Zgodnie z art. 9 ust. 2 w związku z ust. 1 wskazanego rozporządzenia PE i RADY (UE) z dnia 27 kwietnia 2016 r. o ochronie danych osobowych przetwarzanie danych biometrycznych znajduje podstawę prawną w przypadku wyrażenia zgody osoby, której dane dotyczą[9]. Student może zgodzić się na pobranie jego danych biometrycznych w celu przystąpienia do egzaminu zdalnego poprzez zeskanowanie tęczówki oka. Zgodnie z art. 60 k.c. wola osoby dokonującej złożenia oświadczenia woli może być dokonana przez każde zachowanie, które ujawnia jej wolę dostatecznie. Złożenie oświadczenia woli w postaci maila jest zgodne z art. 60 k.c.[10]. Jest to forma dokumentowa w rozumieniu art. 77^2 k.c.[11].

Uczelnia jest podmiotem, który przetwarza dane osobowe, a więc ich administratorem zgodnie z art. 4 pkt 7) rozporządzenia PE i RADY (UE) o ochronie danych osobowych. W związku z tym nałożone są na nią obowiązki dotyczące administrowania danymi. Artykuł 24 rozporządzenia unijnego wskazuje, iż administrator musi wdrożyć środki, które zapewnią od strony technicznej i organizacyjnej przetwarzanie danych zgodnie z rozporządzeniem. Przy wykonywaniu powyższych czynności uwzględnione powinny być cel, zakres przetwarzania danych, a także uwzględnione ryzyko. Dyspozycja z artykułu 25 ust. 1 rozporządzenia dokładnie określa, by przetwarzane były wyłącznie te dane osobowe, które są niezbędne do wykonania konkretnego celu. Zgodnie z powyższym uzyskane dane z tęczówki oka zostałyby użyte wyłącznie w przypadku określenia tożsamości studenta. Cel byłby zgodny i dookreślony.

---

[7] Rozporządzenie PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, (Dz.U.UE.L.2016.119.1), art. art. 5 ust. 1 pkt c).
[8] Traktat o funkcjonowaniu Unii Europejskiej (Dz.U.2004.90.864/2).
[9] Rozporządzenie PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r., art. 9 ust. 1 i ust. 2.
[10] Ustawa z dnia 23 kwietnia 1964 r. *kodeks cywilny*, (Dz.U.2020.1740 t.j.), art. 60.
[11] Ibidem, art. 77^2.

Uczelnia A w celu prawidłowego przetwarzania danych musi ocenić istnienie ryzyka naruszenia praw i wolności podmiotów, których dane przetwarza. Obowiązkowe przy ocenie jest podjęcie zapobiegania i zaradzeniu naruszenia w postaci wdrożenia mechanizmów bezpieczeństwa (art. 35 ust. 7 rozporządzenia unijnego o ochronie danych osobowych)[12].

Posiadanie przez uczelnię zapisu numerycznego, tzw. „klucza" porównującego dane z tęczówki oka wskazują na działanie uczelni A w ramach przepisów prawa (art. 32 ust. 1 pkt a rozporządzenia o ochronie danych osobowych)[13], a także środki podjęte przez uczelnię A umożliwiają zapobieganiu wystąpienia ryzyka naruszenia danych osobowych (art. 24 ust. 1 rozporządzenia o ochronie danych osobowych)[14]. Pseudonimizacja (art. 4 pkt 5 rozporządzenia o ochronie danych osobowych) oznacza przetworzenie danych w taki sposób, by nie można było już ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji[15]. Uczelnia A nie przechowywałaby zapisu obrazu ani danych biometrycznych, tym samym wypełnia funkcję prewencyjną, przeciwdziałałaby potencjalnemu naruszeniu przetwarzania danych osobowych studenta. Gwarantuje bezpieczeństwo poprzez posiadanie zaszyfrowanego „klucza" porównującego dane z tęczówki oka z ciągiem numerycznym. Tym samym prawdopodobieństwo naruszenia przetwarzania danych biometrycznych jest znikome. Uczelnia A stawia na maksymalne zabezpieczenie danych, gdyż rezygnuje z przetrzymywania zapisu cech biometrycznych, posiadając jedynie „klucz" w celu weryfikacji. Na zapewnienie bezpieczeństwa przetwarzania danych wskazuje w orzeczeniu WSA w Warszawie z dnia 3 września 2020 r., II SA/Wa 2559/19: „W myśl art. 32 ust. 2 RODO, administrator oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych."[16] Uczelnia A tym samym uwzględnia indywidualne dobro studenta, przestrzegając przepisów rozporządzenia. Cel działania zapewnia bezpieczeństwo danych poprzez techniczne i organizacyjne przygotowanie w związku z podjętym innowacyjnym rozwiązaniem. Wypełnia wymogi proporcjonalnego działania w odniesieniu do celu, w zgodzie ze standardami demokratycznego państwa prawnego.

---

[12] Rozporządzenie PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r., art. 35 ust. 7.
[13] Ibidem, art. 32 ust. 1.
[14] Ibidem, art. 24 ust. 1.
[15] Ibidem, art. 4 pkt 5.
[16] Wyrok WSA w Warszawie z dnia 3 września 2020 r., II SA/Wa 2559/19.

Jeżeli uczelnia A nie wprowadziłaby stosownych zabezpieczeń technicznych i środków ochrony danych, a wystąpiłoby wysokie ryzyko naruszenia praw i wolności konkretnej osoby, musiałaby wykonać dyspozycję z art. 34 ust. 1 rozporządzenia o ochronie danych osobowych i zawiadomić osobę, której dane dotyczą[17]. W przypadku naruszenia przetwarzania danych osobowych studenta, uczelnia A miałaby obowiązek poinformowania jego o zaistniałym przypadku naruszenia. Ponadto musiałaby zgłosić problem właściwemu organowi nadzorczemu zgodnie z art. 33 wskazanego rozporządzenia[18]. Organem nadzorczym w rozumieniu art. 34 ust. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych[19].

Warto zauważyć, iż ochronę danych osobowych wzmacniają regulacje zawarte w art. 37 rozporządzenia o ochronie danych osobowych[20] i art. 8 ustawy o ochronie danych osobowych poprzez wskazanie na obligatoryjność wyznaczenia inspektora ochrony danych osobowych[21]. Inspektor monitoruje przestrzeganie rozporządzenia unijnego, informuje o obowiązkach administratora wynikających z przepisów rozporządzenia. Dzięki temu podmiot administrujący jest stale monitorowany w swoich działaniach, co służy zapobieganiu naruszenia prawa.

Uczelnia A proponuje rozwiązane innowacyjne, a jednocześnie w zgodzie ze standardami demokratycznego państwa prawa. Nowe technologie wymagają nowych przepisów prawa. Przywołane regulacje prawne pokazują, iż w demokratycznym społeczeństwie istnieje możliwość zastosowania dorobku cywilizacyjnego w zgodzie z ochroną praw obywatela. Ważna jest proporcjonalność, cel, zapewnienie bezpieczeństwa przetwarzanych danych. Pobrane cechy biometryczne oka mogą wywoływać u niejednego obywatela poczucie obawy przed instrumentalnym wykorzystaniem tych danych. Jednakże rozporządzenie PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych osobowych, a także ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych gwarantują maksymalną ochronę.

Inaczej rzecz ma się w Chińskiej Republice Ludowej, gdzie innowacyjne technologie służą kontroli społeczeństwa; ich zastosowanie odbiega od respektowania prywatności obywateli.

---

[17] Rozporządzenie PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r., art. 34 ust. 1
[18] Ibidem, art. 33.
[19] Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 r. poz. 1781. t.j.), art. 34 ust. 1 i 2.
[20] Rozporządzenie PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r., art. 37.
[21] Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, art. 8.

Funkcjonowanie systemu chińskiego w pełnym świetle obrazuje znaczenie paremii prawniczej *dura lex, sed lex*, a „państwowy aparat bezpieczeństwa zagląda obywatelowi przez ramię”[22]. Wzmacnianiu potencjału państwa ma służyć permanentna kontrola społeczeństwa przy wykorzystaniu innowacyjności: „big data i sztuczna inteligencja pozwolą zbudować silniejsze Chiny”[23]. Pozyskiwane dane obywateli za pomocą nowoczesnych rozwiązań przy zastosowaniu kamer do monitoringu (w 2016 r. było ich 176 mln, w 2020 r. już 600 mln)[24], skanowaniu twarzy na ulicach, w urzędach, prywatnych firmach, stosowanie algorytmów w celu identyfikacji poszczególnych osób[25], nie zapewnia ochrony danych osobowych, gdyż są one instrumentalnie traktowane przez władze chińskie. Pozwalają szczegółowo zidentyfikować osobę: „korzystając z naszych kamer, możemy dowiedzieć się w jakim wieku są klienci, czy są wysportowani, jakie marki ubrań noszą”[26]. Władze chińskie przy wykorzystaniu innowacyjnych rozwiązań technologicznych naruszają dane osobowe jednostek. Upublicznienie ich stosują m.in. jako sankcję za nieprzestrzeganie przepisów: „policja w Jinan i Shenzen piętnuje pieszych za przechodzenie na czerwonym świetle – ich twarze ukazują się w czasie rzeczywistym na ekranach na poboczu ulicy razem z nazwiskiem, adresem i numerem dowodu osobistego”[27].

Kwestia ochrony danych osobowych w różnych reżimach politycznych jest uregulowana w sposób odmienny. Regulacja może służyć jednostce albo być skierowana przeciwko niej. Założenia prawodawcy demokratycznego ukazują, jak tworzyć przepisy, by zapewnić zastosowanie nowoczesnych rozwiązań w sposób przyjazny prawom obywatela, chroniąc jego dane osobowe. Przepisy tak skonstruowane ukazują racjonalność i poszanowanie dorobku demokratycznego państwa prawa. Przeciwieństwem tego są konstrukcje prawne, które nie respektują ochrony danych obywateli. Przepisy reżimu chińskiego przypominają Austinowską formę definicji reguły jako rozkazu suwerena[28]. Tylko demokratyczny porządek prawny daje możliwość poszanowania i ochronę danych osobowych. Przetwarzanie danych przez uczelnię A jest zgodne z rozporządzeniem PE i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. i gwarantuje zaufanie jednostki do państwa.

[22] Kai Strittmatter, Chiny 5.0. Jak powstaje cyfrowa dyktatura, Warszawa 2020, s. 229.
[23] Kai Strittmatter, *Chiny 5.0. (...),* s. 211.
[24] Ibidem, s. 225.
[25] Ibidem, s.221.
[26] Ibidem, s. 220.
[27] Ibidem, s. 237.
[28] Ronald Dworkin, Biorąc prawa poważnie, Wydawnictwo Naukowe PWN 1998, s. 48-49.