L O D Z U N I V E R S I T Y O F T E C H N O L O G Y
No. 1(1)/2020 JOURNAL OF MANAGEMENT CHALLENGES, Vol. 01 2020

PIOTR SZEFLIŃSKI
Uczelniane Centrum Informatyczne
Politechnika Łódzka

STANDARDY DZIAŁANIA UCZELNI W ZAKRESIE OCHRONY WIEDZY I BEZPIECZEŃSTWA INFORMACJI

1. Wstęp

Problem ochrony, czy szerzej zarządzania wiedzą jako wartością dostrzega coraz więcej uczelni, choć jest to proces powolny. Niemałą wagę do tego zagadnienia przywiązuje od dawna literatura przedmiotu, zwracając przy tym uwagę na trudność zdefiniowania samego pojęcia wiedzy, związanych z nią pojęć, takich jak: dane, informacja czy mądrość i ich wzajemnych relacji. Dlatego w pierwszej części artykułu przedstawiony jest szerzej zarys problematyki zarządzania wiedzą, opracowany na podstawie dostępnej literatury.

Z drugiej strony otoczenie prawne stawia przed uczelniami coraz więcej i coraz bardziej skomplikowanych obowiązków z zakresu bezpieczeństwa informacji. Regulują one kwestie definiowania, inwentaryzowania, kategoryzowania, wartościowania i w końcu ochrony zasobów wiedzy i informacji. Niektóre z tych regulacji dotyczą wyłącznie uczelni, inne w sposób pośredni przenoszą się z aktów prawnych dotyczących podmiotów publicznych, a jeszcze inne z aktów prawa powszechnego. Druga część artykułu przedstawia uogólnione spostrzeżenia na temat zmieniającego się środowiska formalno-prawnego i tendencji, które można w tych zmianach zauważyć.

Dla określonego typu instytucji można podjąć próbę zdefiniowania odpowiadającego jej zbioru zasobu informacji, na podstawie którego instytucje tego typu kreują własne wartości. Dlatego, rozpatrując środowisko szkół wyższych, można wydzielić zasoby informacji, których interpretacja i kontekst są wspólne dla całej grupy i w podobny sposób zasoby tych informacji kształtują wiedzę uczelni. Artykuł w dalszych częściach przedstawia analizę standardów opisujących w sposób formalny ochronę informacji w uczelniach w czterech wybranych obszarach ochrony wiedzy i informacji.

2. Wiedza i zarządzanie wiedzą

Mimo, że termin „zarządzanie" jest dobrze i jednoznacznie rozumiany, to już termin „zarządzanie wiedzą" rozmywa tę ostrość postrzegania. A. Jashapara twierdzi wręcz, że „każdy rozumie ten termin jak chce" [1, s. 30]. Rozwijając tę myśl autor zauważa, że można wyodrębnić podejście do zarządzania wiedzą od strony systemów informatycznych, traktując je jako rozbudowane zarządzanie informacją lub od strony zarządzania zasobami ludzkimi. Inne spotykane w literaturze omówienie zagadnienia zarządzania wiedzą traktują je jako część zarządzania strategicznego lub też zarządzanie zmianą kulturową [1, s. 26]. Potwierdza to również K. Perechuda [2] zauważając, że wśród przedstawicieli klasycznego nurtu nauk zarządzania termin „zarządzanie wiedzą" wywołuje dysonans terminologiczny, gdyż według nich zarządzać można przedsiębiorstwem rozumianym obiektowo, złożonym z zasobów rzeczowych oraz zasobów ludzkich. J. Fazlagić definiuje cel zarządzania wiedzą jako „zapewnienie środowiska, które stwarza optymalne warunki do tworzenia, przesyłania i wykorzystania wiedzy" [3, s. 12]. Zarządzanie wiedzą nie jest więc klasycznym zarządzaniem zasobami, ale raczej sprzyjaniem pewnym procesom, które wiedzę tworzą, gromadzą i wykorzystują.

P. Drucker [4] zwraca uwagę na fakt, że wiedza już niedługo będzie podstawowym bogactwem społeczeństwa, a instytucje posługujące się nią, w tym uczelnie, muszą być zdolne do globalnej konkurencji. W tym aspekcie wiedza nabiera wyjątkowego znaczenia, jako zasób wymagający szczególnej ochrony. A. Jashapara zauważa, że już w 2000 r. raport KPMG wskazywał, że 38% największych przedsiębiorstw europejskich i amerykańskich ma za sobą wdrożenie przynajmniej jednej inicjatywy z zakresu zarządzania wiedzą [1, s. 31]. Autor zebrał też najpopularniejsze nazwy stanowisk związanych z zarządzeniem wiedzą, wśród których są, np. dyrektor ds. wiedzy, analityk ds. zarządzania wiedzą, kierownik działu wiedzy, czy administrator wiedzy [1, s. 32]. Prawie 20 lat po raporcie KPMG w instytucjach naukowych nie można często spotkać stanowisk czy działów zajmujących się zarządzaniem wiedzą. Być może wyjątkiem potwierdzającym tę regułę jest Dział Zarządzania Wiedzą funkcjonujący w Instytucie Medycyny Pracy im. J. Nofera w Łodzi [5].

Z ochroną wiedzy łączy się jeszcze pewien pozorny paradoks, na który zwraca uwagę B. Mikuła [6]. Polega on na wyróżnieniu (spośród opisanych sześciu) dwóch przeciwstawnych strategii zarządzania wiedzą: strategii protekcji wiedzy i strategii udostępniania wiedzy. Pierwsza jest niekiedy trudna do zrealizowania, gdyż wiedza ugruntowana jest zwykle dostępna w produktach lub usługach. Tym niemniej dla zbudowania i utrzymania przewagi konkurencyjnej ochrona wiedzy kluczowej może mieć niezwykle istotne znaczenie dla organizacji. Natomiast dzielenie się wiedzą z otoczeniem, zgodnie ze strategią udostępniania, może być łatwiejsze do zaimplementowania, a często stanowi element strategii kreacji

realizowanej przez organizację. Mimo swojej przeciwstawności, obie wymienione strategie mogą być jednocześnie w różnym stopniu implementowane przez tę samą organizację.

Paradoks ten jest szczególnie mocno widoczny w środowisku uczelni. Udostępnianie wiedzy jest główną misją uczelni, traktowaną również jako szersza misja społeczna, czy wręcz imperatyw, a realizacja tej misji jest głównym celem strategicznym uczelni. Jest to też wyraźnie umocowane w nieformalnej kulturze organizacyjnej szkoły wyższej. Tym trudniej jest realizować w środowisku uczelni strategię protekcji wiedzy. Oczywiście, obie te strategie odnoszą się implementacyjnie do różnych zasobów wiedzy, ale środowisko akademickie nie jest ani nauczone, ani przyzwyczajone do pracy w sformalizowanej poufności.

Subiektywny charakter wiedzy, jej indywidualne postrzeganie i wykorzystanie w środowisku konkretnej instytucji wydaje się czymś oczywistym. Indywidualna interpretacja rzeczywistości powoduje, że wiedza na temat określonego zjawiska będzie różna dla różnych osób [1, s. 34]. Nie da się jednak posiąść wiedzy bez poznania informacji. A. Jashapera przedstawia piramidę mądrości, w której szereguje wg złożoności pojęcia: dane – informacje – wiedza – mądrość – prawda [1, s. 35]. Wytworzenie unikalnej wiedzy jest możliwe w oparciu o unikalne dane. Chcąc zatem chronić wartość, jaką jest wiedza, należy chronić informacje, na podstawie których można zbudować wiedzę. J. Fazlagić [3, ss. 33-34], proponuje dość obszerne porównanie relacji między wiedzą a informacją, zwracając szczególną uwagę na kontekstowe znaczenie wiedzy, silne umocowanie jej w procesie myślowym i poznawczym i bardzo małą podatność na jej przekazanie w postaci dokumentów. Autor przeciwstawia wiedzy informację, która – będąc jej podstawą – jest niezmienna, obiektywna i nie zależy od kontekstu poznawczego, gdyż tak naprawdę jest „jedynie" zbiorem prze-tworzonych i uporządkowanych danych.

3. Standardy ochrony informacji w aktach prawnych

Zagadnienie tworzenia i ochrony wiedzy znalazło swoje ważne miejsce w aktach prawnych, które tworzą pewien obszar ustandaryzowanego postrzegania i opisu wiedzy oraz zadań, jakie stawia się przed instytucjami publicznymi, w tym szczególnie szkołami wyższymi. Swoje miejsce wśród nich zajmują również dokumenty Unii Europejskiej, np. Deklaracja EUA [7], która zwraca uwagę na silną rolę szkół wyższych w budowaniu, a nawet stawia je w roli głównych kreatorów europejskiego społeczeństwa wiedzy. Budowanie zasobów wiedzy przez uniwersytety jest istotne nie tylko z partykularnego punktu widzenia pojedynczej instytucji, ale również realizuje bardzo ważną misję społeczną, wychodzącą poza obszar narodowy, a nazywaną w tych dokumentach Europą Wiedzy [8].

Opisane w rozdziale 2 cechy informacji spowodowały zapewne, że legislatorzy oraz twórcy standardów – chcąc unormować i opisać warunki ochrony wiedzy – skupili się nie na niej samej, ale na jej nośniku, czyli informacji. Informację łatwiej obiektywnie zdefiniować i zmaterializować, a co za tym idzie – łatwiej określić warunki jej ochrony. Mimo tego, trudne i mało uzasadnione jest chronienie informacji samej w sobie bez odniesienia do kontekstu jej wykorzystania, a więc do wartości, jaką może stanowić dla danej instytucji, zwłaszcza że ta sama informacja może być nośnikiem różnie wartej wiedzy dla różnych organizacji. Jako przykład można podać informację o kursach walut. Dla szkoły wyższej taka informacja ma wartość instrumentalną, wykorzystywaną do obsługi bieżących transakcji finansowych. Zmienność w czasie kursów walut nie jest źródłem wiedzy dla szkoły wyższej, a więc nie będzie stanowić o wartości jej zasobów. Inaczej sytuacja wygląda dla biura maklerskiego, dla którego tendencje zmian kursów stanowią jedną z podstawowych informacji decydujących o podejmowanych działaniach, a więc w konsekwencji o sukcesie funkcjonowania tej instytucji.

Na podstawie historycznej analizy można zaobserwować ewolucję rozumienia i opisu w aktach prawnych wartości, jaką jest i reprezentuje informacja. Widać to szczególnie wyraźnie choćby na przykładzie ochrony danych osobowych. Na przestrzeni lat postrzeganie wartości zasobu informacji w tych obszarach zmienia się ze zobiektywizowanego, enumeratywnego wręcz przypisania wartości szczegółowym informacjom w kierunku subiektywnej, zindywidualizowanej oceny wartości tego zasobu, przeprowadzanej w oparciu m.in. o analizę ryzyka. Konsekwencją tej zmiany jest trudniejsze wdrożenie uniwersalnych mechanizmów ochrony informacji, gdyż jej zabezpieczenie musi być zindywidualizowane. W obowiązującym do dnia 6.02.2019 r. Rozporządzeniu MSWiA [9] określa się dokładnie długość i zawartość hasła służącego do uwierzytelniania użytkowników, jako składające się z co najmniej ośmiu znaków, zawierające małe i wielkie litery oraz cyfry lub znaki specjalne. Ani w rozporządzeniu RODO, które weszło w życie 25.05.2018 r. [10], ani w jego krajowych aktach wykonawczych nie znajdziemy podobnego przepisu. Jest natomiast w art. 24 RODO wskazane, że administrator musi wdrożyć odpowiednie środki techniczne i organizacyjne, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia prawa o różnym prawdopodobieństwie i wadze. Oznacza to, że na administratorze spoczywa obowiązek doboru takich środków ochrony, które będą adekwatne do ocenionego ryzyka. To ważna tendencja w budowaniu środowiska prawnego wokół zarządzania wiedzą i informacją, gdyż uwzględnia jej kontekstowy charakter.

4. Ochrona własności intelektualnej

W przypadku ochrony własności intelektualnej analiza obowiązków uczelni jest stosunkowo prosta. Zarówno uchylona Ustawa o szkolnictwie wyższym z 2005 r. [11] w art. 86c, jak i nowa, tzw. Ustawa 2.0 [12] w art. 152 nakazują senatowi uczelni przyjąć regulamin zarządzania prawami autorskimi i prawami pokrewnymi oraz prawami własności przemysłowej i zasad komercjalizacji. Wuszczegółowieniu podana jest obowiązkowa zawartość regulaminu:

„a) prawa i obowiązki uczelni, pracowników, doktorantów i studentów w zakresie ochrony i korzystania z praw autorskich, praw pokrewnych i praw własności przemysłowej,
b) zasady wynagradzania twórców,
c) zasady i procedury komercjalizacji,
d) zasady korzystania z majątku uczelni, wykorzystywanego dokomercjalizacji, oraz świadczenia usług w zakresie działalności naukowej."

Co ciekawe, zawartość wskazanych artykułów różni się jedynie pojedynczymi słowami. Najistotniejszą zmianą jest zastosowanie w starym brzmieniu punktu d zamiast „usług w zakresie działalności naukowej" sformułowania „usług naukowo-badawczych". Legislator nie widział potrzeby, aby zmieniać obowiązujące od kilkunastu lat regulacje w tym zakresie, uznając je zapewne za wystarczające. Wskazane obowiązki są dość skromne w przeciwieństwie do przedmiotu zagadnienia. Można by postawić tezę, że i w tym obszarze zadziałała zasada indywidualnego relatywizmu, umożliwiająca każdej uczelni wprowadzenie zasad według własnej oceny ryzyka, własnej wyceny zasobów wiedzy, czy w końcu przyjętej strategii wskazującej, jakie informacje i jakimi narzędziami technicznymi i organizacyjnymi uczelnia chce chronić. Jednak już pobieżna analiza zagadnienia wskazuje, że pozornie skromne obligacje odsyłają uczelnie do kolejnych trzech ustaw, które regulują szczegółowo zakres oraz sposób ochrony i postępowania z tego typu informacjami:
– Ustawy o prawie autorskim i prawach pokrewnych [13],
– Ustawy Prawo własności przemysłowej [14],
– Ustawy o zwalczaniu nieuczciwej konkurencji [15].

Wdrażając ustawowe obowiązki oraz procedury przewidziane szczegółowymi przepisami dotyczącymi np. zgłaszania wynalazków, po stronie uczelni pozostaje mądre wyważenie balansu między prawami i interesem uczelni a prawami i interesem twórcy. Zadanie to komplikuje się szczególnie, gdy twórcą jest pracownik uczelni, a przedmiotem rozważań jest pracownicza własność intelektualna. Oprócz dylematu pogodzenia interesów uczelni i twórcy powstaje tu do rozstrzygnięcia kwestia zachowania poufności wyników badań, w szczególności w czasie procesu patentowego. Po stronie uczelni jest zapewnienie takich warunków technicznych i organizacyjnych, aby postępowanie patentowe mogło zostać

przeprowadzone skutecznie, z zachowaniem interesu gospodarczego uczelni i słusznych praw twórcy. W szczególnych przypadkach w opisane relacje może wejść jeszcze strona trzecia, np. przedsiębiorca zlecający prace badawcze wykonane w ramach pracy dyplomowej. Taka sytuacja wymaga jeszcze rozważniejszej oceny ryzyka, potencjalnie uzyskanych korzyści i zabezpieczenia praw i interesów wszystkich zaangażowanych stron [16].

5. Dane osobowe

Problem ochrony danych osobowych jest zagadnieniem bardzo szeroko rozpowszechnionym w ostatnim czasie. Przyczyniło się do tego wejście w życie 25.05.2018 r. tzw. Rozporządzenia RODO [10]. Rozporządzenie to nie traktuje szkół wyższych w sposób szczególny, ale nakłada na wszystkie instytucje szereg obowiązków, które również uczelni dotyczą. Jest to główny akt w naszym systemie prawnym regulujący kwestie ochrony informacji, jakimi są dane osobowe. Mimo pozornej szerokiej znajomości praw obywateli (studentów, pracowników) z jednej strony i obowiązków szkoły wyższej, która takie dane przetwarza z drugiej strony znalezienie reguł ochrony tych informacji nastręcza niemałych kłopotów. Już sama definicja „danych osobowych" umieszczona w art. 4 nie określa jednoznacznie co jest daną osobową: „dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej". Mimo że w dalszej części definicji wskazano wprost, że identyfikator w postaci imienia i nazwiska może być daną osobową, to w środowisku tak dużym, jak uczelnia, która zatrudnia kilka tysięcy pracowników i kształci kilkadziesiąt tysięcy studentów powtórzenie się zestawu imienia i nazwiska jest wręcz pewne. W bazie kadrowo-płacowej Politechniki Łódzkiej prawie 9% danych identyfikujących osoby to dublety, tzn. identyczne pary imię i nazwisko przypisane różnym osobom fizycznym [17]. W takiej sytuacji identyfikator w przysłowiowej postaci jan. kowalski nie musi być daną osobową, gdyż za jego pomocą możemy nie zidentyfikować konkretnej osoby fizycznej. W pkt. 4 preambuły do RODO wskazano, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym i należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw [10], co jeszcze bardziej relatywizuje postrzeganie obowiązków, jakie ten akt prawny nakłada na uczelnie.

Nie bez znaczenia jest wymóg, aby dobór środków technicznych do ochrony danych osobowych dobrać na podstawie wieloczynnikowej oceny ryzyka. Wymaga to uwzględnienia nie tylko elementów obiektywnych, takich jak ryzyko zniszczenia czy utraty danych, ale także czynników relatywnych, takich jak np.: stan wiedzy technicznej, kontekst, cele przetwarzania danych oraz wagę i prawdopodobieństwo naruszenia praw [10, art. 32, pkt. 1].

Głębsza analiza kontekstowego podejścia do zagadnienia ochrony danych osobowych reprezentowanego w rozporządzeniu RODO całkowicie nie współgra z potocznym rozumieniem ochrony danych osobowych. To drugie cały czas rozumie się jako problem, że nie można głośno mówić, np. o studentach, wymieniając ich z imienia i nazwiska lub należy zmieniać co 30 dni hasło w systemie obsługującym dane osobowe. W rzeczywistości jednak RODO realizuje postulaty dotyczące relatywnej i subiektywnej wartości wiedzy, którą należy chronić adekwatnie do jej wartości, wyznaczonej w procesie np. oceny ryzyka. Oczywiście w przypadku ochrony danych osobowych w uczelni podstawowym ryzykiem jest narażenie się na przekroczenie prawa i związane z tym sankcje finansowe, opisane w art. 83 RODO. Sankcje te są tym dotkliwsze, że ustalone jako adekwatne do warunków europejskich, a nie polskich (do 20 mln EUR). Innym ważnym ryzykiem może być utrata wizerunku instytucji, ale najbardziej związanym z substancją przedmiotu jest oczywiście ryzyko tzw. „wycieku danych" i wykorzystania ich w sposób niezgodny z pierwotnym celem ich przetwarzania.

Mimo ogólnego podejścia do opisu obowiązków, jakie uczelnie muszą wypełnić w związku z RODO, daje się jednak wyszczególnić podstawowe obligacje, które uczelnia powinna spełnić, aby zapewnić bezpieczeństwo informacji w zakresie ochrony danych osobowych. Do najważniejszych należy zaliczyć [18]:

- powołanie Inspektora Ochrony Danych;
- identyfikacja obszarów przetwarzania danych osobowych uwzględniająca cel wynikający z obowiązków prawnych lub zadań realizowanych przez uczelnię, zakres przetwarzania danych adekwatny do zdefiniowanych celów i realizujący zasadę minimalizacji zakresu zbieranych danych, sposób zbierania i udostępniania danych, grupy osób przetwarzające dane, procesy przetwarzana danych w uczeni (wewnętrzny przepływ i udostępnienie danych) i w relacjach z innymi podmiotami, z uwzględnieniem szczególnych kategorii danych osobowych:
  szczególne zwrócenie uwagi na profilowanie użytkowników (wykorzystanie danych osobowych do przypisania określonej osobie pewnych cech) i ocena jego dopuszczalności;
  wykonanie oceny skutków naruszenia ochrony danych w stosunku do obszarów przetwarzania danych, w tym w szczególności do systemów teleinformatycznych przetwarzających dane osobowe;
  dobór środków technicznych adekwatnych do ocenionego ryzyka, również na etapie projektowania i wdrażania systemów teleinformatycznych (poziom techniczny) i procedur (poziom organizacyjny);
- analiza procesów przetwarzania danych osobowych w systemach teleinformatycznych uwzgledniająca cechy, takie jak dostępność, poufność i integralność;

- zapewnienie realizacji obowiązku informacyjnego w stosunku do osób, których dane dotyczą;
- założenie i prowadzenie rejestru czynności przetwarzania danych osobowych;
- założenie i prowadzenie rejestru upoważnień do przetwarzania danych osobowych;
- dostosowanie umów powierzenia przetwarzania danych do nowych regulacji.

Ciekawą informacją jest również to, że w obecnych przepisach nie ma obowiązku tworzenia tzw. polityki bezpieczeństwa informacji oraz instrukcji przetwarzania danych osobowych w systemach teleinformatycznych. Jest to duże zaskoczenie, gdyż 20 lat obowiązywania dotychczasowych przepisów [19] nauczyło uczelnie stosowania tych reguł.

6. Bezpieczeństwo IT

Bezpieczeństwo IT lub bezpieczeństwo systemów komputerowych jest dość dobrze reprezentowane w normach i przepisach prawa. Jedno z omawianych we wstępie podejść do zarządzania wiedzą dzieli je na zarządzanie systemami informatycznymi i zarządzaniem zasobami ludzkimi [1, s. 30]. Wyodrębnienie zarządzania systemami informatycznymi jako jedną z dwóch części zarządzania wiedzą uzasadnia się o tyle, że przetwarzanie „informacji", na której zbudowana jest wiedza, jest kwintesencją funkcjonowania systemów informatycznych. Warto może przy tym zaznaczyć, że zagadnienie zarządzania informacją jest w nauce obecne od bardzo dawna. Jej początki powstały w czasach, gdy znane nam dziś systemy komputerowe istniały tylko w teoretycznych rozważaniach jako maszyny matematyczne. Wprowadzenie pojęcia „teorii informacji" przypisuje się C.E. Shannonowi za sprawą jego publikacji z 1948 r. pt. *Matematyczna teoria komunikacji* [20] – dlatego w obecnych czasach jest to już zagadnienie dość dobrze ustandaryzowane.

Jednym z podstawowych dokumentów dotyczących zarządzania informacją jest zespół norm z grupy 27000. Warto powołać się na trzy z nich:

- PN-EN ISO/IEC 27000 Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia [21],
- PN-EN ISO/IEC 27001:2017-06 Systemy zarządzania bezpieczeństwem informacji. Wymagania [22],
- PN-EN ISO/IEC 27002:2017-06 Praktyczne zasady zabezpieczenia informacji [23].
-

Normy te określają wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji. Obejmują również terminologię i wymagania odnośnie szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji dostosowanych do potrzeb organizacji i środowiska, w którym funkcjonuje organizacja. Wymogi określone w normach są ogólne i mają zastosowanie do wszystkich organizacji, które chcą je wdrożyć, niezależnie od typu, wielkości i charakteru [24].

Cała grupa norm 27000 jest niezwykle przydatna przy planowaniu i tworzeniu systemów zarządzania informacją i jej bezpieczeństwem. Metodologia w nich wskazana wprowadza podejście procesowe do zarządzania informacją oraz cykl ciągłego doskonalenia PDCA. To również te normy opisują bezpieczeństwo informacji jego trzema najważniejszymi atrybutami: poufność, dostępność, integralność. Normy są dokumentami ogólnymi, dlatego można je stosować w każdej organizacji, implementując te elementy, które są adekwatne do środowiska funkcjonowania tej organizacji i zostały wybrane na podstawie ogólnego podejścia do zarządzania ryzykiem. Normy można traktować jako punkt wyjścia do opracowania zaleceń uwzględniających specyfikę organizacji. Nie wszystkie zabezpieczenia i zalecenia podane w normie mogą mieć zastosowanie. Ponadto mogą być wprowadzone dodatkowe mechanizmy i zalecenia nieuwzględnione w normie.

Wspomniane normy nie są dokumentami, które uczelnie są zobligowane wdrożyć. Są jednak o tyle znaczące, że wiele aktów prawnych stosuje opisane w normach podejście do bezpieczeństwa informacji lub wręcz przywołuje je w sposób bezpośredni. Ponieważ dodatkowo normy podają kompletne wymagania do stworzenia i wdrożenia polityki bezpieczeństwa informacji, trudno sobie wyobrazić, aby jakakolwiek uczelnia, zajmując się tą problematyką, mogła te publikacje pominąć.

Jednym z aktów prawnych obowiązujących uczelnie publiczne jest Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) [25]. Samo rozporządzenie dotyczy podmiotów świadczących drogą elektroniczną usługi w ramach realizacji zadań publicznych i odnosi się głównie do jednostek administracji publicznej. Warto jednak zwrócić uwagę na § 19-21 KRI, opisujące wymagania systemu zarządzania bezpieczeństwem informacji, jakie podmioty publiczne, w tym uczelnie publiczne, są zobligowane wdrożyć. Cały proces opisany jest wieloelementowo i obejmuje opracowanie, ustanowienie, wdrożenie, eksploatację, monitorowanie, przegląd, utrzymanie i doskonalenie tego systemu przy zapewnieniu poufności, dostępności i integralności informacji. Uczelnie zobowiązane są wykonać analizę ryzyka, zapewnić odpowiedni do wymagań poziom bezpieczeństwa oraz przeprowadzać coroczne audyty. Znamienny jest fakt, że wdrożenie w organizacji normy [22] pozwala uznać wymagania omawianego rozporządzenia jako spełnione.

KRI nakłada, również na uczelnie, wymagania w zakresie dostępności dla osób niepełnosprawnych dotyczące prezentacji zasobów informacji w systemach teleinformatycznych. Wymagania te obejmują zapewnienie, aby strony informacyjne uczelni spełniły zasady określone w tzw. Web Content Accessibility Guidelines (WCAG 2.0) dla systemów teleinformatycznych. Wymagania opisane są dość ogólnie i bez doświadczenia trudno ocenić ich spełnienie, ale na szczęście funkcjonują dostępne w Internecie narzędzia, które taką ocenę dla stron WWW przeprowadzają. Ich przykładem może być A. Checker [26].

Stosunkowo młodym aktem prawnym dotyczącym bezpieczeństwa informatycznego jest ustawa o Krajowym Systemie Cyberbezpieczeństwa, uchwalona w lipcu 2018 roku [27]. Określa ona m.in. zadania i obowiązki podmiotów wchodzących w skład tego systemu, w tym również uczelni publicznych. Wśród tych zadań należy wyszczególnić obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz obowiązek zgłaszania i obsługi „incydentu w podmiocie publicznym". Obowiązki te nie wydają się nad wymiar skomplikowane, ale mają przypisany do siebie wyraźny reżim czasowy, np. na zgłoszenie incydentu, czyli zdarzenia, które powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego uczelnia ma tylko 24 godziny od jego wykrycia. Incydenty muszą być zgłoszone do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego, którym dla uczelni jest CSIRT NASK. Dodatkowo uczenia musi posiadać system zarządzania incydentami, co wymaga niemałego zaangażowania organizacyjnego.

7. Informacje niejawne

Informacje niejawne zajmują dość szczególne miejsce wśród wszystkich innych chronionych informacji, gdyż zasady obowiązujące przy ich przetwarzaniu mają pierwszeństwo przed regulacjami dotyczącymi innych tajemnic chronionych prawem. Wynika to z faktu, że terminem „informacje niejawne" określa się w Ustawie [28] informacje, których ujawnienie spowoduje lub może spowodować szkodę dla Rzeczypospolitej Polskiej. Szkoda ta może dotyczyć niepodległości Polski, suwerenności kraju, integralności jego granic, jego obronności, porządku wewnętrznego lub konstytucyjnego, zagrozić sojuszom lub pozycji międzynarodowej RP, czy zakłócić funkcjonowanie Sił Zbrojnych RP [28, art. 5]. Katalog przedstawionych w ustawie zagrożeń jest dużo szerszy. Większości z nich jednak nie można odnieść do codziennego życia uczelni, dlatego pracownicy i studenci uczelni nie mają częstego kontaktu z informacją niejawną. Przypadki, kiedy ma to miejsce mogą być związane z realizacją przez szkoły wyższe specjalistycznych badań zleconych z zakresu np. obronności, nowych technologii stosowanych w celach specjalnych lub szeroko rozumianego bezpieczeństwa publicznego.

Informacje niejawne są klasyfikowane wg zasad opisanych w ustawie poprzez nadanie im właściwych klauzul bezpieczeństwa, z których najwyższą jest klauzula „ściśle tajne". Dla informacji oznaczonych tą klauzulą stosuje się najbardziej skomplikowane stopnie zabezpieczenia, a dostęp do nich jest związany z największymi ograniczeniami. Kolejne klauzule wg ważności to „tajne", „poufne" i „zastrzeżone".

Dostęp do informacji niejawnych, oznaczonych nawet najniższą klauzulą, związany jest z wyjątkowymi rygorami. Pierwszy z nich dotyczy bezpieczeństwa osobowego. Dla jego zapewnienia każda osoba mająca mieć dostęp do informacji niejawnych musi się poddać procedurze sprawdzającej, gdyż tylko osoba „dająca rękojmię zachowania tajemnicy" może uzyskać dostęp do informacji niejawnych. Dostęp taki wiąże się również z odbyciem specjalnego szkolenia z zakresu ochrony informacji niejawnych. Drugie poważne ograniczenie związane jest z organizacją w uczelni stref ochronnych, w których mogą być przetwarzane informacje niejawne. Związane jest to z utrzymaniem w uczelniach kancelarii tajnych lub kancelarii niejawnych, obowiązkiem powołania pełnomocnika ds. ochrony informacji niejawnych i przygotowaniem rozbudowanej dokumentacji opisującej wdrożone procedury, opracowane na podstawie analizy ryzyka. Nie do pominięcia jest również wymóg polegający na dopuszczalności przetwarzania informacji niejawnych w formie elektronicznej wyłącznie w systemach teleinformatycznych posiadających specjalną akredytację. Jest to znaczące utrudnienie dla osób zajmujących się informacją niejawną i jej przetwarzaniem. Po pierwsze, z powodu skomplikowanego przygotowania, a po drugie z tego powodu, że systemy te zlokalizowane muszą być w strefach ochronnych, co w praktyce oznacza umieszczenie ich w kancelarii tajnej. Wszystkie dokumenty i opracowania muszą być zatem tworzone nie w zaciszu pokoi pracowników naukowych, ale właśnie w kancelarii tajnej.

W warunkach uczelni wyższej wymóg zachowania bezpieczeństwa informacji niejawnej najczęściej zgłasza kontrahent z obszaru obronności lub strona umowy projektowej, którą jest któreś z tzw. siłowych ministerstw, czy też Narodowe Centrum Badań i Rozwoju, które dla tych instytucji realizuje badania.

Przy analizie obszaru przetwarzania informacji niejawnych wato zwrócić uwagę na dwa aspekty. Pierwszy związany jest z ewolucją podejścia do ochrony informacji niejawnej w polskim systemie prawnym. Obecnie obowiązująca ustawa o ochronie informacji niejawnych [28] weszła w życie w 2010 roku, uchylając poprzednią jej wersję z roku 1999 [29]. Wersja ta definiowała informacje niejawne przez enumeratywne wskazanie typów informacji, którym można nadać określoną klauzulę. I tak lista dla informacji „ściśle tajnych" obejmowała 29 pozycji, a dla klauzuli „tajne" 59 typów informacji. Przy czym szczegółowość tych pozycji była dość duża, gdyż wskazywała np. konkretne plany operacyjne, strukturę rodzajów sił zbrojnych, lokalizację stanowisk dowodzenia itp. Nadawanie klauzuli tajności

odbywało się zgodnie z tym wykazem. Zupełnie inne podejście reprezentuje obecnie obowiązująca ustawa. Osoba nadająca klauzulę tajności „ściśle tajne" musi sama, w oparciu o swoją najlepszą wiedzę rozstrzygnąć, czy nieuprawnione ujawnienie informacji, które mają być chronione, spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej. Analizę przeprowadza się w jednym z ogólnie opisanych obszarów funkcjonowania RP, takich jak gotowość obronna RP, bezpieczeństwo wewnętrze i inne na podobnym poziomie abstrakcji. Trudności dodaje fakt, że dla klauzuli „tajne" kryterium jest sformułowanie „wyrządzenie poważnej szkody dla RP". Różnica między opisanymi kryteriami tkwi w obecności lub nie przysłówka „wyjątkowo". Dla informacji klasyfikowanych jako „poufne" kryterium jest jeszcze bardziej osłabione, gdyż wskazanie dotyczy po prostu „szkody dla RP". Zdumiewająco nieostre granice między określeniami poszczególnymi klauzul wskazują na niezwykle nowoczesne podejście do zarządzania informacją. Jest to tym bardziej zaskakujące, że dotyczy – wydawałoby się – jednej z najbardziej zachowawczych i skostniałych dziedzin przetwarzania informacji. Wyjaśnienie tej swoistej rewolucji można znaleźć w rządowym uzasadnieniu do obecnej ustawy [30]. Autorzy zwracają uwagę, że istotą projektu nowej ustawy o ochronie informacji niejawnych jest unormowanie systemu ich ochrony jako maksymalnie efektywnego zarówno w sferze krajowej, jak i zagranicznej, przy jednoczesnej prostocie i elastyczności funkcjonowania. Wcześniej stosowane rozwiązania powodowały z jednej strony wymóg nadawania klauzul tajności olbrzymiej liczbie informacji, w wielu przypadkach niewymagających ochrony, a także częste zawyżanie klauzul bez merytorycznego uzasadnienia. Jak widać, automatyzm stosowania pozornie prostego przepisu (załącznik ze szczegółową listą spraw podlegających klauzulowaniu) powodował efekt odwrotny do zamierzonego.

Inną ważną przyczyną modyfikacji podejścia do klauzulowania, wskazaną w tym samym uzasadnieniu [30], była ogromna zmiana, jaka zaszła w obszarze obronności RP na przestrzeni 10 lat obowiązywania poprzedniej ustawy (1999-2010). To przecież w tym czasie Polska przystąpiła na NATO i Unii Europejskiej i sposób postrzegania spraw obronności, bezpieczeństwa, wymiany informacji z nowymi partnerami wymusił podejście dużo bardziej elastyczne i relatywistyczne.

Drugi aspekt, warty zwrócenia uwagi, dotyczy dużego podobieństwa stosowanych metod podejścia do informacji niejawnych i zapewnienia ich bezpieczeństwa do metodologii opisanej normami z grupy 27000. Najważniejsze cechy bezpieczeństwa informacji niejawnych przetwarzanych w systemach teleinformatycznych opisane są trzema atrybutami: poufność, integralność i dostępność [28, art. 49], czyli dokładnie tymi samymi, które wskazuje norma 27002 [23]. Dodatkowo, zapewnienie wymienionych atrybutów dla informacji niejawnych realizuje się w oparciu o zarządzanie ryzykiem, co jest polecane do stosowania również przez normę. Co prawda, sama ustawa w art. 49 tylko ogólnie wskazuje te wymagania,

ale akt wykonawczy do niej [31] szczegółowo implementuje reguły postępowania z ryzykiem opisanym w normie.

Z informacją niejawną uczelnia nie musi mieć wiele wspólnego w sensie ilościowym. Jakościowo natomiast wdrożenie zasad ich ochrony nie powinno stanowić dużego problemu mentalnego, gdyż wymaga zastosowania znanej z norm metodologii podejścia do wartości informacji opartej o wiedzę, dotycząca subiektywnego znaczenia tej informacji w konkretnym kontekście jej wykorzystania.

8. Podsumowanie

Wszystkie opisane powyżej obszary ochrony informacji i wiedzy powinny być ze sobą spójne i zebrane w ogólną politykę bezpieczeństwa informacji, traktowaną jako ustrukturyzowany dokument odnoszący się indywidualnie do wybranych obszarów zidentyfikowanych jako najważniejsze aktywa uczelni [22]. Powyższe przeglądowe opracowanie może stanowić pomoc przy uwzględnieniu najistotniejszych dla danej uczelni zasobów, które powinny być chronione. Trzeba jednak mieć na względzie fakt, że niniejsze opracowanie bazuje przede wszystkim na analizie wymogów formalno-prawnych i nie uwzględnia oceny aktywów i ich wartości z punktu widzenia misji i celów każdej z uczelni oraz, że –z powodu ograniczeń tej publikacji – jest tylko wyborem niektórych zagadnień.

W wymaganiach opisanych dla wybranych obszarów funkcjonowania uczelni można znaleźć zaawansowane metody ochrony informacji, oparte o wspólne pierwiastki, których spoiwem ze strony czysto formalnej mogą być normy z grupy 27000 [21], [22], [23].

Patrząc jednak szerzej –zarówno na omawiane normy, jak i na opisane w artykule obszary – można stwierdzić, że w gruncie rzeczy realizują one implementację postulatów naukowych dotyczących zarządzania wiedzą. Bez względu na to, czy rozważamy ochronę danych osobowych, czy ochronę własności intelektualnej, czy nawet ochronę informacji niejawnych, zawsze przy realizacji strategii protekcji wiedzy należy głęboko rozważyć indywidualny jej kontekst i relatywistyczne podejście do wartości informacji pod kątem wytworzenia z niej cennej dla uczelni wiedzy.

Literatura

[1] Jashapara A., (2014), *Zarządzanie wiedzą*, Polskie Wydawnictwo Ekonomiczne, Warszawa.
[2] Perechuda K. (red.), (2005), *Zarządzanie wiedzą w przedsiębiorstwie*, PWN Warszawa.
[3] Fazlagić J., (2014), *Innowacyjne zarządzane wiedzą*, Difin Warszawa.

[4] Drucker P., *Przyszłe społeczeństwo*, „Przegląd Polityczny" 2003, Gdańsk, nr 62/63 s. 109-133.
[5] http://www.imp.lodz.pl/home_pl/o_instytucie/structure/dzial_zarzadzania_wiedza/, (dostęp: 03.2019).
[6] Mikuła B., *Geneza, przesłanki i istota zarządzania wiedzą*, [w:] Perechuda K. (red.) (2005) *Zarządzanie wiedzą w przedsiębiorstwie*, PWN, Warszawa.
[7] Deklaracja European University Association „Silne Uniwersytety dla Silnej Europy", Glasgow 15.04.2005, https://eua.eu/downloads/publications/glasgow%20declaration%20%20strong%20universities%20for%20a%20strong%20europe%202005%20pl.pdf, (dostęp: 03.2019).
[8] The role of the universities in the Europe of knowledge, Communication from the Commission, Bruxelles, 2003, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52003DC0058, (dostęp: 03.2019).
[9] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r., nr 100, poz. 1024 – nie obowiązuje.
[10] Rozporządzenie Parlamentu Europejskiego 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), Dz.U.UE.L.2016.119.1
[11] Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym, Dz.U. z 2017 r., poz. 2183 – nie obowiązuje.
[12] Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, Dz.U. z 2018 r., poz.1668.
[13] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U. z 2018 r., poz. 1191.
[14] Ustawa z dnia 30 czerwca 2000 r. Prawo własności przemysłowej, Dz.U. z 2017 r., poz. 776.
[15] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 2018 r, poz. 419.
[16] Uchwała Nr 3/2015 Senatu Politechniki Łódzkiej z dnia 25 lutego 2015 r. Regulamin zarządzania prawami własności intelektualnej oraz zasad komercjalizacji wyników badań naukowych i prac rozwojowych w Politechnice Łódzkiej.
[17] Kwerenda z bazy DODARP PŁ 03.2019.
[18] Starzak S., Wójtowicz W., Rozporządzenie_PE_i_RE_2016-679, Konferencja Kanclerzy, Kwestorów i Dyrektorów Finansowych Polskich Uczelni Technicznych, Politechnika Koszalińska, 10-12 maja 2017.
[19] USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2016 r., poz. 922 – nie obowiązuje.
[20] Mazur M., *Społeczne znaczenie cybernetyki*, [w:] „Nowe Drogi" 1980, nr 5, s. 152-163.

[21] Polska norma PN-EN ISO/IEC 27000:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, PKN, Warszawa 2018.
[22] Polska norma PN-EN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN Warszawa 2018.
[23] Polska norma PN-EN ISO/IEC 27002:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczenia informacji, PKN, Warszawa 2018.
[24] Polski Komitet Normalizacji, opis zakresu normy PN-EN ISO/IEC 27001:2017-06 http://pkn.pl, (dostęp 03.2019).
[25] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2017 r., poz. 2247.
[26] https://achecker.ca/checker/index.php, (dostęp: 03.2019).
[27] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560.
[28] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. z 2018 r., poz. 412.
[29] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz.U. z 2005 r., nr 196, poz. 1631 – nie obowiązuje.
[30] Rządowy projekt ustawy o ochronie informacji niejawnych oraz o zmianie niektórych ustaw, VI.2791 z dn.16.02.2010 r.
[31] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz.U. z 2011 r., nr 159, poz. 948.