PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS nr 487 • 2017

Polityka ekonomiczna

ISSN 1899-3192
e-ISSN 2392-0041

Paweł Kocoń
Uniwersytet Ekonomiczny w Katowicach
e-mail: pawel.kocon@ue.katowice.pl

BUDOWA ŚWIADOMOŚCI INFORMACJI NIEJAWNYCH WŚRÓD PRACOWNIKÓW SĄDÓW

BUILDING AWARENESS OF CLASSIFIED INFORMATION AMONG COURT EMPLOYEES

DOI: 10.15611/pn.2017.487.14
JEL Classification: H8

Streszczenie: Każda organizacja ma swoje sfery jawności i strefę tajemnicy. Nie inaczej jest z sądami, które zgodnie z prawem są depozytariuszami informacji niejawnych. Zarządzanie informacją obejmuje specyficzne dla klasycznych funkcji zarządzania sekwencje, takie jak planowanie, organizowanie, decydowanie, motywowanie i kontrolowanie. Prawidłowe wypełnianie tych funkcji wymaga świadomości przedmiotu zarządzania, jakim w tym wypadku są informacje niejawne. Uprzytomnienie sobie przez pracowników, czym są informacje niejawne, jaki jest ich podział, a także jak je chronić, jest warunkiem *sine qua non* właściwego utajnienia informacji. Innymi słowy, by chronić informacje, należy mieć wiedzę, które informacje chronić i w jaki sposób to robić. Utajnienie jest konieczne dla prawidłowej pracy sądów – utrzymania tajemnicy śledztwa, intymności ofiar i świadków.

Słowa kluczowe: informacje niejawne, informacje tajne, informacje zastrzeżone, informacje ściśle tajne, gryf tajności.

Summary: Every organization has its sphere of publicity and a secret zone. It is not different with the courts which are required by law to be depositaries of classified information. Information Management includes the classic management-specific sequences such as planning, organizing, deciding, motivating and controlling. Correct fulfilling of these functions requires the awareness of the subject of management,whichin in this case is classified information. Making employees realize what classified information is, what their division is and how to protect it is a sine qua non condition of proper making information confident. In other words, to protect information,the knowledge which information to protect and how to do it is needed. Conficence is necessary for the courts to function properly, to maintain the secret of the investigation, the intimacy of victims and of the witnesses.

Keywords: classified information, confidential information, proprietary information, highly confidential information, confidentiality.

1. Wstęp

Zachowanie tajemnicy zarówno przez kierownictwo, jak i szeregowy personel wymaga jasnego i klarownego systemu klasyfikującego informacje jako tajne lub jawne, a także szeregującego dostęp do tych pierwszych. Pomimo coraz doskonalszych technologii zabezpieczeń, uwzględniających także ludzkie niedbalstwo czy wręcz bezmyślność, niemożliwe jest wyeliminowanie tzw. czynnika ludzkiego.

Nie jest prawdą, że ludzie stanowią „najsłabsze ogniwo" systemu informacji niejawnych. To ludzie wytwarzają, rozpowszechniają i utajniają informacje, to ludzie wydobywają tajemnice na światło dzienne zarówno celem zysku, jak i „pro publico bono". Stąd też budowanie świadomości, czym jest informacja niejawna, jak ją chronić, kto ma do niej dostęp i wreszcie jakie warunki pozwalają na jej ujawnienie, jest kluczowe dla funkcjonowania organizacji.

Nie inaczej jest w przypadku władzy sądowniczej. Sądy są depozytariuszami różnorodnych informacji niejawnych, dotyczących nie tylko osób uczestniczących w postępowaniach karnych lub cywilnych, ale także danych osobowych pracowników sądów, danych osób ukaranych czy uniewinnionych. Wszystko to winno być pieczołowicie zabezpieczane. Informacje niejawne są kluczowe dla przeprowadzanych spraw sądowych, chociaż na etapie sprawy sądowej większość informacji jest udostępniana stronom, z wyjątkiem ściśle określonych przypadków związanych z danymi świadków postępowania czy wyłączeniem jego jawności.

Złamanie tajemnicy sądu kończy się nie tylko zakłóceniem jego pracy, lecz także – co ważniejsze – naruszeniem zaufania społecznego do instytucji państwowych w ogóle.

Przedstawione wyniki badań są pokłosiem programu badawczego „Zarządzanie informacją i komunikowanie się w organizacjach publicznych" – kierownikiem projektu była dr hab. Agata Austen. Metodyka badań opierała się na kwestionariuszu ankiety rozdanym 109 pracownikom sądów.

Z powyższego wyłania się problem wyważenia pomiędzy zabezpieczeniem informacji przed dostępem osób nieuprawnionych a łatwym i sprawnym dostępem osób uprawnionych do odczytu informacji niejawnych.

Problemem, jaki dostrzega autor, jest niewłaściwy rozdział informacji wśród pracowników bądź też niewłaściwe obchodzenie się z nimi przez nich. Może temu sprzyjać dysfunkcjonalna kultura organizacyjna i patologiczny klimat organizacji. Stąd też utajnienie informacji i budowanie jego świadomości zostały ukazane w kontekście zjawiska rozszczepienia informacyjnego – *decouplingu*. Zjawisko to rozumiane jest jako tworzenie i utrzymywanie luk między sformalizowaną polityką organizacji a jej rzeczywistymi działaniami [Meyer, Rowan 1977].

Podsumowując, powyższe problemy trudno opisać w jednym krótkim tekście. Stąd też celem artykułu jest naszkicowanie podstawowych zagadnień dotyczących informacji niejawnych i budowania świadomości ich znaczenia w sądach.

2. Informacje niejawne – definicje i rozróżnienia

Odnosząc się do źródłosłowu, za informację niejawną należy uznać takie znaczenia lub dane, które są ujawniane w sposób ograniczony.

Komisja Europejska wyróżnia poziomy utajnienia: *EU Top Secret*, *EU Secret*, *EU Confidential* i *EU Restricted* [Council Decisionof 23 September 2013]:

1. *EU Top Secret* to informacje i materiały, których nieuprawnione ujawnienie mogłoby spowodować wyjątkowo poważne uszczerbki dla podstawowych interesów Unii Europejskiej albo jednego lub więcej państw członkowskich.
2. *EU Secret* to informacje i materiały, których nieuprawnione ujawnienie mogłoby spowodować poważną szkodę dla podstawowych interesów Unii Europejskiej albo jednego lub więcej państw członkowskich.
3. *EU Confidential* to informacje lub materiały, których nieupoważnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej albo jednego lub więcej państw członkowskich.
4. *EU Restricted*: informacje lub materiały, których nieupoważnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub jednego lub więcej państw członkowskich.

Identyfikacja informacji niejawnych wymaga refleksji prawniczej. Przyporządkowanie informacji niejawnych jest regulowane ustawą o ochronie informacji niejawnych [Ustawa z 5 sierpnia 2010].

W art. 1 ust. 1 ustawy wyjaśniono pojęcie „informacje niejawne". W ujęciu tego przepisu za informacje niejawne uznano takie, „których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania" [Leciak 2011, s. 194].

Według Administratora Strony Agencji Bezpieczeństwa Wewnętrznego „informacje niejawne – jak jest napisane – mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności, muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności, a także chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie" [Administrator BIP ABW].

Jak napisał Michał Cyrankiewicz: „informacje niejawne klasyfikuje się według stopnia ich ochrony na: »zastrzeżone«, »poufne«, »tajne« oraz »ściśle tajne«. Informacje o najdonioślejszym dla państwa znaczeniu klasyfikuje się jako »ściśle tajne«. Te, których nieuprawnione ujawnienie spowodowałoby najmniejsze szkody, opatruje się klauzulą »zastrzeżone«. Informacje niejawne przetwarzane są przede wszyst-

kim przez organy administracji publicznej i obsługujące je urzędy" [Cyrankiewicz 2012].

Jak napisano na stronach firmy bezpieczneit.com, specjalizującej się w zabezpieczaniu informacji niejawnych: „Zgodnie z art. 5 ust. 4 ustawy informacjom niejawnym nadawana jest klauzula »zastrzeżone«, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej" [*Ochrona Informacji Niejawnych. Klauzula: Zastrzeżone*].

Mamy więc do czynienia z przedmiotowym zakresem utajnienia, a także z brakiem precyzji co do kwalifikacji tychże informacji.

Zgodnie z art. 5 ust. 3 ustawy informacjom niejawnym jest nadawana klauzula „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że [*Ochrona Informacji Niejawnych. Klauzula: Poufne*]:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Trudno odróżnić metodologię nadawania informacjom tytułu „poufne" i „zastrzeżone"; należałoby w tym miejscu zastosować pogłębioną analizę językową wyrażeń „mieć szkodliwy wpływ" i „utrudnić". Wydaje się, że sami autorzy ustawy takiej analizy nie przeprowadzili.

Wspomniana ustawa stanowi, że informacjom niejawnym jest nadawana klauzula „tajne", jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że [*Ochrona Informacji Niejawnych. Klauzula: Tajne*]:

1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;

4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;

5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;

6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Z kolei klauzula „ściśle tajne" nadawana jest, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że [*Ochrona Informacji Niejawnych. Klauzula: Ściśle tajne*]:

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;

2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;

3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;

4) osłabi gotowość obronną Rzeczypospolitej Polskiej;

5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;

6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;

7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych.

Wspomniana ustawa o informacjach niejawnych wprowadza kilka istotnych pojęć, m.in. [Bogusz 2012]:

1) rękojmia zachowania tajemnicy – stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego zdolność osoby do spełnienia ustawowych wymogów w celu zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem;

2) dokument – każda utrwalona informacja niejawna;

3) przetwarzanie informacji niejawnych – wszelkie operacje na informacjach niejawnych i związane z informacjami niejawnymi, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

4) zatrudnienie – powołanie, mianowanie lub wyznaczenie.

Klauzulę „ściśle tajne", „tajne", „poufne" i „zastrzeżone" całym aktom lub poszczególnym tomom zawierającym informacje niejawne w postępowaniu sądowym nadaje prezes sądu, a w postępowaniu przygotowawczym prokurator [Kuspiel 2013].

Dla sądu informacjami niejawnymi o różnym stopniu tajności są dane osobowe świadków, w tym świadków koronnych (w tym tzw. małych świadków koronnych), a także informacje w sprawach zagrażających bezpieczeństwu ekonomicznemu państwa. Wszystko to wymaga budowania świadomości wagi posiadanych informacji nie tylko wśród sędziów, lecz także wśród pozostałego personelu potencjalnie będącego depozytariuszami informacji niejawnych.

3. Wyniki badań w kontekście rozszczepienia organizacyjnego

Z informacjami niejawnymi silnie związane jest zjawisko *decouplingu*. Powyższa identyfikacja informacji niejawnych to stan *de iure*. Stan *de facto* nie jest dostępny prostemu oglądowi, można jednak wywnioskować go pośrednio poprzez analizę działań, np. szkoleniowych. W tym miejscu między innymi należy doszukiwać się zjawiska *decouplingu*. Należy podkreślić, że większość badanych pracowników sądów została przeszkolona w zakresie zarówno w zakresie tajemnicy służbowej, ustawy o danych osobowych, jak i o ochronie informacji niejawnych. Niestety tylko 64 pracowników ze 109 badanych albo nie wie, albo nie chce powiedzieć, o czym konkretnie było dane szkolenie. Podobne wartości odnotowujemy wśród badanego personelu kierowniczego: ze 117 badanych kierowników 111 odbyło inkryminowane szkolenia, a 71 z nich jest skłonnych dzielić się informacją, o czym było konkretne szkolenie. Zarówno pracownicy, jak i kierownicy odbyli szkolenia na temat ochrony danych osobowych, gdzie zasady ich ochrony są znane dla 60,2% pracowników, jak i 54,1% kierowników; 86,7% pracowników i 89,2% kierowników zostało przeszkolonych w zakresie tajemnicy służbowej.

Widać z powyższych danych, że dane osobowe i tajemnica służbowa są istotnymi dla badanych organizacji zbiorami informacji niejawnych. W kontekście zarządzania informacjami niejawnymi samo rozdzielenie informacji jest prawidłowe, ale patologią jest nieuzasadnione pomijanie grup pracowników w dostępie do informacji, do których są uprawnieni. Objęcie w badanych placówkach szkoleniami wszystkich grup pracowników świadczy o niewystępowaniu tego zjawiska.

Analizując zjawisko *decouplingu* (rozdzielenia), należy podkreślić, że jest ono niejako naturalnie obecne w praktykach organizacyjnych dotyczących utajniania. Przejawia się ono między innymi w niezgodności taktyk utajniania z jego strategiami oraz „pęknięciach" pomiędzy praktykami organizacji a jej politykami. Przejawem takiego pęknięcia jest tzw. tajemnica poliszynela.

4. Zakończenie

Niniejszy tekst ma charakter szkicu; trzeba przyznać, że odczuwalny jest brak na polskim rynku naukowym publikacji, które próbują zjawiska utajnienia osadzić w kontekście zarządczym. Stąd też nie tylko proste sprawdzenie, na ile szkoli się

w utrzymaniu tajemnicy pracowników sądów, ale też ukazanie zagrożeń związanych z nierównomiernym dostępem do informacji.

Zjawisko niepełnych i niejasnych informacji wypływających od menedżerów powoduje reakcję polegającą na aktywnym poszukiwaniu informacji przez interesariuszy. Owocuje to legalną formą zbierania informacji, jaką jest *intelligence*, a także szpiegostwem. Sądy z jednej strony obligowane są do zarówno utajniania, jak i ujawniania wielu informacji. Problem polega na jednoznacznej kwalifikacji informacji do tych dwu procedur. Organizacje publiczne mają obowiązek ustawowy chronienia informacji niejawnych, ustawodawca daje im względną swobodę w doborze metod i technik ochrony. Z drugiej strony organizacje publiczne, aby egzystować na labilnym rynku, muszą także zbierać informacje o swoim otoczeniu, co w rezultacie może owocować opracowaniem własnych form wywiadu gospodarczego, które zresztą spotkają się z reakcją obronną interesariuszy.

Nie inaczej jest z sądownictwem. To, że pracownicy sądów mają świadomość, jakie informacje nie powinny być upubliczniane, jest pierwszym krokiem do właściwego zabezpieczenia tego typu danych. Niestety zbadanie dalszych kroków takiego postępowania jest trudne i potencjalnie społecznie szkodliwe. Ujawnienie, w jaki sposób szkoli się pracowników, jest wskazówką dla osób, które chcą przejąć dla siebie treść utajnionych informacji.

Z drugiej strony brak jawności metodologii utajnienia informacji, jego uznaniowość jest polem do nadużyć. Reasumując, rysuje się ważne pole badawcze dla teorii i praktyki zarządzania publicznego.

Należy zauważyć, że przyjęta przez ustawodawcę koncepcja ochrony informacji niejawnych jest w istotnym stopniu ogólna i nieprecyzyjna. Wskazane wyżej definicje legalne są na tyle niejasne i ocenne, że ich jednolita interpretacja może okazać się w praktyce niemożliwa.

Trzeba także dodać, że artykuł ten nie rości sobie pretensji do pełnego lub choćby obszernego wyjaśnienia opisywanych zagadnień, jego zadaniem jest jedynie zasygnalizowanie problemu.

Literatura

Administrator BIP ABW, *Organizacja Ochrony Informacji Niejawnych*, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/organizacja-ochrony-in/145,organizacja-ochrony-informacji-niejawnych.html#1 (1.05.2017).

Bogusz A., 2012, *Nowe spojrzenie na ochronę informacji niejawnych*, http://www.zabezpieczenia.com.pl/ochrona-informacji/nowe-spojrzenie-na-ochron%C4%99-informacji-niejawnych (1.05.2017).

Council Decision of 23 September 2013 on the security rules for protecting EU classified information(2013/488/EU), Official Journal of the European Union, 15 October 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:EN:PDF (5.09.2015).

Cyrankiewicz M., 2012, *Kto może mieć dostęp do informacji niejawnych*, http://www.rp.pl/artykul/941574-Kto-moze-miec-dostep-do-informacji-niejawnych.html (2.05.2017).

Kuspiel D., 2013, *Materiały niejawne w postępowaniu karnym*, http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2013/07-08/16kuspiel.pdf (2.05.2017).

Leciak M., 2011, *Prawno karne aspekty nowej ustawy o ochronie informacji niejawnych*, Studia Iuridica Toruniensia, vol. 9, s. 192–214.

Meyer J.W., Rowan B., 1977, *Institutionalized organizations: formal structure as myth and ceremony*, American Journal of Sociology, vol. 83, s. 340–363.

Ochrona Informacji Niejawnych. Klauzula: Poufne, http://www.niejawne.info/klauzula-poufne/ (1.05.2017).

Ochrona Informacji Niejawnych. Klauzula: Ściśle tajne, http://www.niejawne.info/klauzula-scisle-tajne (1.05.2017).

Ochrona Informacji Niejawnych. Klauzula: Tajne, http://www.niejawne.info/klauzula-tajne (3.05.2017).

Ochrona Informacji Niejawnych. Klauzula: Zastrzeżone, http://www.niejawne.info/klauzula-zastrzezone (1.05.2017).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2016, poz. 1167.