Przegląd Prawniczy Uniwersytetu Warszawskiego
ISSN 1644-0242
Rok XIX, nr 2/2020
DOI 10.26330/ppuw.2020.02.05

ORCID 0000-0002-4709-2788
*Marek Porzeżyński**

Glosa do wyroku Sądu Najwyższego z dnia 13 lutego 2019 r. o sygn. Akt III PK 13/18 – częściowo krytyczna

1. Wstęp

Bezpieczeństwo organizacji, bez względu na publiczny czy prywatny charakter oraz wielkość i zasięg działania, jest już w chwili obecnej w dużej mierze bezpośrednio związane z wprowadzonymi środkami bezpieczeństwa teleinformatycznego. Podyktowane jest to spostrzeżeniem, zgodnie z którym większość takich podmiotów funkcjonuje z wykorzystaniem sieci i musi w związku z tym wziąć pod uwagę ilość i rodzaj zagrożeń z niej płynących. O tym, że niezbędne jest wprowadzenie pewnego minimalnego poziomu cyberbezpieczeństwa mówi się od wielu lat, choć w ramach wprowadzanych aktualnie aktów prawnych ostatecznie zrezygnowano z ustalenia generalnego poziomu ochrony[1]. Ważne jest jednak, że stale wzrasta świadomość co do coraz większych zagrożeń płynących z cyberprzestrzeni, ich wpływu na działalność organizacji oraz niezbędności wprowadzenia rozwiązań zwiększających poziom odporności na te ryzyka. Aby jednak takie rozwiązania miały jakiekolwiek znaczenie, muszą być należycie wdrażane i wykorzystywane.

Powyższe powinno być możliwe do weryfikacji, a w przypadku stwierdzenia uchybień pracodawca powinien mieć możliwość odpowiedniej reakcji w zależności od okoliczności konkretnej sprawy. Niektórzy uczestnicy rynku są zobowiązani do wdrażania odpowiednich środków bezpieczeństwa na podstawie konkretnych aktów prawnych, o których mowa w dalszej części niniejszej glosy. Pozostali wprowadzają

* Wydział Administracji i Nauk Społecznych, Politechnika Warszawska, Pl. Politechniki 1, 00-661 Warszawa, e-mail: m.porzezynski@wp.pl.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1), z którą łączono początkowo nadzieję na wprowadzenie tego typu rozwiązań.

odpowiednie rozwiązania chociaż fragmentarycznie[2], co również wskazuje na zainteresowanie cyberbezpieczeństwem.

Czy zatem można wyciągnąć konsekwencje wobec pracownika świadomie naruszającego zasady bezpieczeństwa obowiązujące w danej organizacji? Odpowiedź na to pytanie wydaje się oczywista. Zasady te są wyznaczane w wielu przypadkach na podstawie obowiązku prawnego w celu zapewnienia bezpieczeństwa. Czy można wobec takiego pracownika zastosować kwalifikację uprawniającą do wypowiedzenia umowy o pracę z winy pracownika bez zachowania jego terminu i w jakich okolicznościach? W szczególności z odpowiedzią na takie pytanie mierzyły się sądy pierwszej i drugiej instancji, jak również Sąd Najwyższy w głosowanym wyroku.

Stan faktyczny sprawy dotyczył głównie bezpieczeństwa informacji pracodawcy. W opisie stanu faktycznego zaznaczono bowiem już na wstępie, że punktem centralnym sporu jest „ciężkie naruszenie przez powoda podstawowych obowiązków pracowniczych poprzez użycie 18 października 2014 r., podczas nocnej służby, prywatnego, nieautoryzowanego, mobilnego, elektronicznego nośnika typu Pen-Drive, w komputerze służbowym i skopiowanie na to urządzenie informacji objętych ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz informacji będących tajemnicą przedsiębiorcy zgodnie z ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji”[3]. Jednocześnie ustalono, że pracownik ten bez wątpienia miał świadomość swojego działania i jego możliwych konsekwencji, gdyż zapoznawał się z zapisami dokumentacji dotyczącymi zarządzania bezpieczeństwem informacji u pracodawcy, jak również zobowiązał się do postępowania zgodnie z nimi i ich przestrzegania. Jego czyn naruszył szereg postanowień wskazanej dokumentacji, które zostały wyliczone w analizowanym Wyroku.

---

[2] Trudno wyobrazić sobie chyba przedsiębiorcę, który do swojej pracy wykorzystuje komputer bez obowiązku logowania się hasłem, z nieaktualnym oprogramowaniem, czy bez jakiegokolwiek oprogramowania antywirusowego, a są to tylko przykłady najpopularniejszych środków mających wpływ na poziom bezpieczeństwa.

[3] Wyrok SN z dnia 13 lutego 2019 r., III PK 13/18 (Legalis) – dalej: Wyrok.

Powyższe pytania, chociaż zadawane w kontekście stanu faktycznego komentowanego Wyroku, dotyczą niezwykle ważnej kwestii – możliwości skutecznej egzekucji zasad bezpieczeństwa obowiązujących w danej organizacji. Bezsprzecznie bowiem, co również podkreślane jest w praktyce, wprowadzenie odpowiednich procedur bezpieczeństwa prowadzi do zmniejszenia kosztów obsługi ewentualnych incydentów[4] i zdecydowanie obniża ryzyko ich wystąpienia.

2. Stan faktyczny

Dnia 13 lutego 2019 r. Sąd Najwyższy rozpoznał skargę kasacyjną od wyroku Sądu Okręgowego – Sądu Pracy i Ubezpieczeń Społecznych w Lublinie z dnia 27 września 2017 r.[5] w wyniku czego uchylił zaskarżony wyrok i przekazał sprawę powrotnie do Sądu Okręgowego w Lublinie. Rzeczona sprawa może mieć duże znaczenie dla bezpieczeństwa informacji i zarządzania nim. Dotyczy bowiem osoby zwolnionej z pracy z powodu ciężkiego naruszenia obowiązków pracowniczych. Naruszeniem tym było pobranie na prywatny zewnętrzny nośnik danych (tzw. *pen-drive*) informacji z komputera służbowego.

Powód (były pracownik) podczas pełnienia nocnej służby wykorzystał swój prywatny *pen-drive* do skopiowania zdjęć z komputera służbowego. Przejmujący służbę kolejny pracownik, zorientowawszy się, że do komputera służbowego podłączony jest zewnętrzny nośnik danych, powiadomił o tym fakcie komendanta posterunku, na wniosek którego o całym zajściu został poinformowany komendant regionu. Z tego zajścia sporządzono notatki służbowe i wszczęto postępowanie wyjaśniające.

Dodatkowym elementem, na który warto zwrócić uwagę, jest fakt, że pracownik przejmujący służbę w celu dokonania oględzin przenośnego nośnika danych sprawdził jego zawartość. W wyniku powyższego stwierdził, że na nośniku znajdują się pliki odpowiadające zawartości jednego z dysków komputera służbowego. To z kolei spowodowało, że zainicjowano postępowanie wyjaśniające w celu weryfikacji, czy doszło

[4] K. Prislan, I. Bernik, *Risk Management with ISO 27000 standards in Information Security, Advances in E-Activities, Information Security and Privacy*, ISPACT 2010, s. 63.

[5] Wyrok SO w Lublinie z dnia 27 września 2017 r., VIII Pa 50/17 (niepubl.).

do naruszenia polegającego na użyciu nieautoryzowanego przenośnego nośnika danych i jeszcze raz dokonano komisyjnych oględzin jego zawartości. W opinii autora niezwykle ważnym elementem stanu faktycznego jest to, że w pierwszym kroku oględzin zweryfikowano bezpieczeństwo nośnika danych[6]. Po sprawdzeniu jego zawartości przy użyciu oprogramowania antywirusowego stwierdzono, że znajdują się na nim wirusy. W wyniku oględzin ustalono, że „na pendrivach znajdowały się fotografie z pokazu psa służbowego, akcji bezpieczny przejazd oraz wzory dokumentów wykorzystywanych w służbie", jak również „foldery, w których zdaniem komisji znajdowały się dokumenty służbowe zawierające dane osobowe"[7].

W szczególności należy podkreślić, że u pracodawcy opracowano i wdrożono dokument „Polityka Bezpieczeństwa Teleinformatycznego", który częstokroć występuje w przedsiębiorstwach i wskazuje na określone procedury postępowania w ramach organizacji celem zachowania odpowiedniego poziomu cyberbezpieczeństwa. W tym konkretnym dokumencie wprost zabroniono wykorzystywania prywatnych komputerów oraz innych nośników informatycznych do celów służbowych, co miało miejsce w analizowanym stanie faktycznym.

Po przeprowadzeniu postępowania wyjaśniającego i dokonaniu powyższych ustaleń, podjęto decyzję o obniżeniu o 70% premii powoda za miesiąc, w którym dokonał naruszenia. Ponadto, w miesiącu kolejnym pracodawca rozwiązał z powodem umowę o pracę bez wypowiedzenia z winy pracownika. Powodem dla takiego wypowiedzenia były dokonane ustalenia.

Podczas postępowania toczącego się przed sądem rejonowym oraz dla potwierdzenia wniosków z postępowania wyjaśniającego u pracodawcy, zlecono wykonanie opinii biegłemu z zakresu informatyki. Co ważne, jeszcze przed zwolnieniem powoda z pracy, podjęto decyzję o „przeinstalowaniu systemu operacyjnego" komputera, do którego *pen-drive* był

[6] W opisie stanu faktycznego wskazano, że łącznie były spięte trzy przenośne nośniki danych *pen-drive*. Jednakże z uwagi na fakt, że jeden z nich pozostał podłączony do komputera służbowego i nie ma wątpliwości w związku z tym, że doszło do jego użycia, autor koncentruje się jedynie na tym elemencie.

[7] Uzasadnienie Wyroku, s. 3.

podłączony. Jak wskazano w uzasadnieniu, powyższe skutkowało usunięciem plików z dysku tego komputera. Zaznaczenia w tym kontekście wymaga, że samo przeinstalowanie systemu operacyjnego nie mogło wywołać takich skutków. Musiało dojść do sformatowania dysku lub innego rodzaju ingerencji w dane oprócz wskazanego czynu. Nie zmienia to jednak faktu, że biegły nie mógł udzielić rzeczowych odpowiedzi na wiele z postawionych pytań[8], na przykład czy doszło do pobrania plików we wskazanej dacie. Biegły mógł jednak poczynić ogólne uwagi, zgodnie z którymi wskazał, że nie było możliwe skopiowanie całej zawartości dysku rzeczonego komputera na nośniki danych powoda, gdyż nie mają one łącznie wystarczającej pojemności. Wziąwszy jednak pod uwagę, że pliki już się nie znajdowały na dysku badanym przez biegłego, mógł on wyjść z powyższego założenia jedynie poprzez porównanie wielkości tego dysku z łączną wielkością przenośnych nośników danych[9]. W rezultacie, sąd rejonowy uznał, że powodowi nie można przypisać czynów wskazanych w uzasadnieniu rozwiązania umowy o pracę.

Wydaje się, że na podstawie uzasadnienia omawianego Wyroku można wywnioskować, że zasadnicze znaczenie dla oceny sądu rejonowego miała opinia biegłego. Biegły wskazał, że nie zachowano środków zabezpieczających elementy podlegające oględzinom przed modyfikacjami, co już samo w sobie nie pozwala na pewność poczynionych ustaleń[10]. Dodatkowymi okolicznościami w tym stanie faktycznym było wskazanie przez powoda, że nośniki danych były przez niego pożyczane m.in. osobie, która pełniła po nim służbę i dokonała zgłoszenia, iż jeden z nich był podpięty do komputera służbowego.

W opinii sądu rejonowego brak było zatem dowodów wskazujących na winę powoda w zakresie kopiowania dokumentów służbowych, która uzasadniałaby rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika. Z uwagi na fakt, że w opinii sądu rejonowego nie udowodniono

[8] Biegły nie mógł udzielić odpowiedzi na 8 z 14 zadanych mu pytań.

[9] Jest to przypuszczenie autora oparte o stan faktyczny wskazany w uzasadnieniu Wyroku.

[10] Co ciekawe biegły stwierdził, że „nie można wykluczyć, iż po zabezpieczeniu nośników były dokonywane modyfikacje, co do treści i daty kopiowania" jednocześnie przyznając, że „nie znalazł przesłanek, które wskazywałyby, iż takie działania były podejmowane".

kopiowania danych przez powoda, brak było możliwości wypowiedzenia umowy o pracę bez zachowania terminu wypowiedzenia, nawet jeśli działanie pracownika naruszało postanowienia polityki bezpieczeństwa teleinformatycznego pracodawcy.

W wyniku apelacji złożonej przez pozwanego sprawa trafiła do rozpatrzenia przez sąd okręgowy. Sąd ten w uzasadnieniu oddalenia apelacji stwierdził, że sąd rejonowy prawidłowo przeprowadził postępowanie dowodowe i dokonał właściwych ustaleń w zakresie stanu faktycznego, który poddał trafnej ocenie prawnej. Z zeznań świadków wynika, że użyto prywatnego przenośnego nośnika danych, natomiast nie można potwierdzić, że tego dnia doszło do skopiowania danych pracodawcy. Pozostałe ustalenia sądu okręgowego są, co do zasady, powtórzeniem i uznaniem ustaleń dokonanych przez sąd pierwszej instancji.

Co niezmiernie ważne, w wyrokach sądów obu instancji podkreślono, że u pozwanego funkcjonowała polityka w zakresie bezpieczeństwa teleinformatycznego, w którym to dokumencie wprost zabroniono wykorzystywania prywatnych nośników danych dla celów służbowych. W związku z tym w obu przypadkach dokonano oceny, że samo użycie takiego nośnika, choć stanowi naruszenie obowiązków pracowniczych, nie powinno być automatycznie uznawane za ciężkie.

Pozwany w skardze kasacyjnej zarzucił rażące naruszenie przepisów prawa procesowego w wyniku nierozpoznania istoty sprawy apelacyjnej, co miało znaczący wpływ na wynik sprawy oraz pozbawiało faktycznie pozwanego prawa do rozpoznania jego stanowiska i podniesionych w postępowaniu apelacyjnym zarzutów. Ponadto, pozwany wskazał na brak wszechstronności w ocenie materiału dowodowego sprawy polegający na pominięciu zeznań świadków[11] oraz okoliczności, że powód,

[11] Z których wynika, że powód dnia 18 października 2014 r. skopiował i przetrzymywał na prywatnym nośniku danych (*pendrive*) informacje objęte ustawą o ochronie danych osobowych oraz informacje będące tajemnicą pozwanego przedsiębiorcy – podczas gdy z zebranego w sprawie materiału dowodowego (zeznań świadków, dowodów z opinii biegłego oraz wyjaśnień samego powoda) bezsprzecznie wynika, że powód przetrzymywał na wymienionym nośniku wskazane wyżej dane, a ponadto – z wyjaśnień samego powoda wynika wprost, iż dnia 18 października 2014 r. kopiował na prywatny nośnik danych dane z komputera służbowego, należącego do pozwanego, co zupełnie pominął sąd rozpoznający sprawę.

pomimo iż miał wiedzę o procedurach obowiązujących u pozwanego[12], co najmniej kilkukrotnie dopuścił się naruszeń nałożonych na niego obowiązków poprzez kopiowanie i przetrzymywanie na prywatnych nośnikach danych informacji stanowiących tajemnice przedsiębiorstwa pracodawcy. Zarzucono również, że możliwość określenia daty zapisania plików na nośnikach danych nie ma znaczenia dla oceny, czy postępowanie powoda stanowiło ciężkie naruszenie podstawowych obowiązków pracowniczych, jak również pominięcie twierdzeń powoda, zgodnie z którymi korzystał on niejednokrotnie z prywatnych nośników danych, w tym w dacie, której dotyczy przedmiotowa sprawa.

Oprócz powyższego zarzucono również obrazę przepisów prawa procesowego, która ostatecznie była przyczyną uchylenia zaskarżonego wyroku przez Sąd Najwyższy. Przedmiotem rozważań w niniejszej glosie będą jednak wyłącznie te kwestie postępowania kasacyjnego, które odnoszą się do prawa materialnego i stanowią mniejszość wywodu Sądu Najwyższego. W pierwszej kolejności odesłano do opinii biegłego, która, za stwierdzeniem poczynionym przez Sąd Najwyższy, może być pomocna w ustaleniu faktów, ale ich nie zastępuje[13]. Zauważono również, że „zarzut choć ujęty w koniunkcji, czyli jako użycie prywatnego pendriva i skopiowanie plików, może być rozdzielany na poszczególne zachowania”[14]. Zdaniem Sądu Najwyższego zasadne jest zatem pytanie, czy samo użycie prywatnego nośnika danych może uzasadniać rozwiązanie pracy bez zachowania terminu wypowiedzenia. Z drugiej jednak strony zważono, że podstawowe znaczenie w tym przypadku ma treść zarzutu wskazanego w piśmie rozwiązującym umowę o pracę. Spowodowane jest to faktem, że podane tam uzasadnienie wskazuje na zakres ustaleń faktycznych i ocen materialnoprawnych, które muszą być dokonane w przedmiotowej sprawie. Stąd w ocenie Sądu Najwyższego należałoby wymagać ustalenia, czy na nośnikach danych znajdowały się pliki skopiowane z komputera służbowego. Ponieważ takich ustaleń nie dokonano, Sąd Najwyższy wskazał, że postępowanie apelacyjne nie spełniło swej funkcji, a ocena zarzutów

[12] Wykazano odbyte szkolenia w tym zakresie.

[13] Uzasadnienie Wyroku, s. 12.

[14] Tamże, s. 14.

materialnych skargi jest możliwa w sytuacji, gdy jest osadzona w ustaleniach stanu faktycznego, czego w tym przypadku zabrakło.

3. Kwalifikacja naruszenia obowiązków pracowniczych

Abstrahując od elementów procesowych, które były poruszane przez sądy poszczególnych instancji, w niniejszym stanie faktycznym zasadniczą kwestią sporną niezbędną do rozważenia była możliwość rozwiązania umowy z pracownikiem z jego winy bez zachowania terminu wypowiedzenia na podstawie art. 52 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy[15]. Zgodnie ze wskazanym artykułem, pracodawca może rozwiązać w ten sposób umowę o pracę jedynie w przypadku[16]:

1) ciężkiego naruszenia podstawowych obowiązków pracowniczych;
2) popełnienia przez pracownika w czasie trwania umowy o pracę przestępstwa, które uniemożliwia dalsze zatrudnianie go na zajmowanym stanowisku, jeżeli przestępstwo jest oczywiste lub zostało stwierdzone prawomocnym wyrokiem;
3) zawinionej przez pracownika utraty uprawnień koniecznych do wykonywania pracy na zajmowanym stanowisku.

W niniejszym stanie faktycznym przyczyną rozwiązania przekazaną pracownikowi było ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu art. 52 ust. 1 KP. W doktrynie wskazuje się, że sytuacje, w których powyższa kwalifikacja prawna znajduje zastosowanie, należą do wyjątkowych i powinny być stosowane z dużą ostrożnością, a ciężar dowodu w tym przypadku spoczywa na pracodawcy[17]. Oznacza to, że pracodawca chcący skorzystać z możliwości wskazanej w cytowanym przepisie, powinien poczynić kroki umożliwiające późniejszą ochronę swoich interesów w razie negowania tego faktu przez zwalnianego pracownika w ramach postępowania sądowego[18].

---

[15] Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2019 r., poz. 1040) – dalej: KP.

[16] *Kodeks pracy. Komentarz*, red. W. Muszalski, K. Walczak, Warszawa 2019, *Komentarz do art. 52*, p. I 1.

[17] Tamże.

[18] Pracownik, z którym rozwiązano umowę o pracę bez wypowiedzenia z naruszeniem wskazanych przepisów może zwrócić się do sądu z roszczeniem o przywrócenie do pracy albo o odszkodowanie na podstawie art. 56 KP.

Podkreślenia wymaga, że ustawodawca przewidział w treści wskazanego przepisu, że naruszenie obowiązków pracowniczych uzasadniające wypowiedzenie umowy o pracę w tym trybie musi być zakwalifikowane jako ciężkie. Naruszenie obowiązków pracowniczych może być uznane za ciężkie, jeżeli pracownikowi można przypisać winę umyślną lub rażące niedbalstwo[19]. Bezwzględnie należy się zgodzić z poglądem wyrażonym w doktrynie, zgodnie z którym naruszenie i jego kwalifikacja mogą być oceniane jedynie w odniesieniu do konkretnego przypadku, jako że w różnych stanach faktycznych różne zachowania mogą być oceniane jako naruszające interes pracodawcy[20]. Co więcej, w doktrynie wskazuje się, że pracodawca ma w takich przypadkach możliwość różnego ukształtowania swojego zachowania względem pracownika – może mu wymierzyć karę porządkową lub wypowiedzieć umowę o pracę jeżeli uzna, że „zaistniałe okoliczności dowodzą faktu nieprzydatności pracownika do pracy na zajmowanym stanowisku"[21].

Aby dokonać powyższej oceny, należy uwzględnić sytuację pracownika - jego stanowisko i zakres obowiązków, jak również charakterystykę naruszenia i stopień zagrożenia interesów pracodawcy. Co do zasady wszystkie wskazane czynniki składają się na stan faktyczny danej sprawy. Bez wątpienia inne będą zobowiązania osób pracujących na stanowiskach, na których możliwość naruszenia interesu pracodawcy w wyniku ich działania będzie ograniczona, a jeszcze inne na wysokich stanowiskach uprawniających do dostępu do wewnętrznych informacji, w tym stanowiących tajemnicę przedsiębiorstwa.

4. Uwagi wstępne do głosowanego wyroku

W głosowanym Wyroku, jak również wyrokach sądów niższych instancji wielokrotnie odwoływano się do problematyki kwalifikacji prawnej[22] postępowania pracownika. W Wyroku podkreślono, że „powstaje pytanie czy

[19] Wyrok SN z dnia 21 lipca 1999 r., I PKN 169/99 (OSNP 2000, nr 20, poz. 746).

[20] *Kodeks*…, red. W. Muszalski, K. Walczak, p. II 1.

[21] Tamże, p. A. I 4.

[22] Tj. wagi czynu, którego dopuścił się pracownik.

samo użycie prywatnego pendrive nie uzasadniało rozwiązania umowy bez wypowiedzenia". Wiele miejsca we wskazanych wyrokach poświęcono analizie, czy pozwany dopuścił się ściągnięcia na swój prywatny przenośny nośnik jakichkolwiek plików z komputera służbowego. Choć wynika to z zeznań świadków, jak również z doniesień dotyczących wcześniejszego postępowania sprawdzającego przeprowadzonego u pracodawcy, opinia sporządzona przez biegłego w zakresie informatyki nie przesądzała, czy do tego doszło z uwagi na sformatowanie wskazanych nośników, jak również komputera.

Sąd Najwyższy podkreślił, że uzasadnienie wypowiedzenia umowy o pracę obejmujące zarówno nieautoryzowane podłączenie prywatnego przenośnego nośnika danych, jak i ściągnięcie plików objętych tajemnicą pracodawcy, wskazuje na zakres niezbędnych ustaleń faktycznych, które są konieczne do ustalenia. Jednocześnie nieuzasadniona wydaje się ocena przyczyn wypowiedzenia dokonywana bez rozważenia podanych wypowiedzeniu elementów składających się na odrębne zachowania pracownika. Powyższe znajduje również uzasadnienie we wcześniejszym orzecznictwie Sądu Najwyższego, zgodnie z którym pracodawca rozwiązując z pracownikiem umowę o pracę w analizowanym trybie może podać większą liczbę zarzutów, ale nie wszystkie muszą zostać pozytywnie zweryfikowane dla potwierdzenia zaistnienia przesłanki wypowiedzenia[23]. W związku z powyższym w opinii autora, w pierwszej kolejności należy rozważyć, czy już samo podłączenie prywatnego przenośnego nośnika danych do komputera służbowego w tym stanie faktycznym mogło uzasadniać wypowiedzenie umowy o pracę bez zachowania terminu wypowiedzenia z winy pracownika. Dopiero negatywna odpowiedź na to pytanie uzasadniałaby położenie nacisku na ustalenie, czy doszło do ściągnięcia plików objętych tajemnicą przedsiębiorstwa i inne okoliczności towarzyszące.

Niewątpliwe jest również, co było przedmiotem analizy w orzecznictwie i doktrynie, że trzy elementy składają się na ciężkie naruszenie podstawowych obowiązków pracowniczych. Należą do nich: bezprawność

[23] Wyrok SN z dnia 12 lipca 2017 r., III PK 115/16 (niepubl.) [w:] *Kodeks*…, red. K. Walczak, W. Muszalski, p. A. II 11.

zachowania, naruszenie albo zagrożenie interesów pracodawcy i zawinienie[24].

W zakresie uznania winy pracownika w rzeczonym stanie faktycznym nie ma większych wątpliwości, że pracownik posłużył się prywatnym przenośnym nośnikiem danych na służbowym komputerze w sposób umyślny. Pracownik musiał co najmniej świadomie godzić się na możliwość wyrządzenia szkody pracodawcy poprzez swoje zachowanie. W orzeczeniach wielokrotnie podkreślano, że wewnętrzne regulacje prawne zabraniały tego typu działań z uwagi na bezpieczeństwo, ochronę danych osobowych oraz informacji przedsiębiorstwa. Pracownik ten, co wynika z uzasadnienia Wyroku, był zaznajomiony z wewnętrznymi procedurami pracodawcy, jak również odbywał szkolenia w zakresie zasad bezpieczeństwa. Co ważne, pracownik sam wskazywał, że nieraz posługiwał się prywatnym nośnikiem danych w celach służbowych. Z uwagi na brak dostępu do pełnego materiału tej sprawy, jedynie dla porządku wywodu, należy dodać, że nawet w przypadku niezakwalifikowania powyższego czynu jako wynikającego z winy umyślnej, czyn ten może być zakwalifikowany jako wynikający z rażącego niedbalstwa, która to kwalifikacja również umożliwia skorzystanie z wypowiedzenia umowy o pracę w omawianym trybie. Rażące niedbalstwo jest definiowane jako rażące niedołożenie staranności wymaganej od pracownika i może się przejawiać w zachowaniu lekkomyślnym, które ma miejsce, gdy pracownik przewiduje, że swoim zachowaniem uchybi obowiązkowi, ale bezpodstawnie przypuszcza, że do tego nie dojdzie.

5. Ocena stopnia naruszenia

Do znaczących wyzwań w przedmiotowym stanie faktycznym należy nie tylko ocena naruszenia podstawowych obowiązków pracownika przez powoda, ale również ocena stopnia tego naruszenia. Jest tak dlatego, że pracodawca może wypowiedzieć umowę o pracę bez zachowania odpowiedniego terminu z winy pracownika, jeżeli dane naruszenie zostało uznane za ciężkie. Ocena rodzaju i stopnia winy pracownika powinna

[24] Wina umyślna lub rażące niedbalstwo. Zob. wyrok SN z dnia 22 marca 2016 r., I PK 94/15 (Legalis).

być dokonana w stosunku do naruszenia podstawowych obowiązków pracowniczych, jak i z uwzględnieniem zagrożenia lub naruszenia interesów pracodawcy[25]. Działanie pracownika musi prowadzić do powstania co najmniej zagrożenia istotną szkodą w mieniu pracodawcy. Szkoda taka nie musi się zatem ostatecznie wystąpić, aby analizowana kwalifikacja była możliwa. Co więcej, wystarczy, że w świetle obiektywnie istniejących okoliczności, powstało potencjalne zagrożenie dla niezakłóconego funkcjonowania zakładu pracodawcy[26].

Jednym z rodzajów naruszeń wskazywanych w doktrynie jest tzw. naruszenie dbałości przez pracownika przejawiające się w braku dbania o powierzone mienie pracodawcy. Innym niezbędnym do rozważenia w przedmiotowym stanie faktycznym jest naruszenie porządku i dyscypliny pracy, które może się przejawiać na przykład w naruszeniu zasad bezpieczeństwa zakładu pracy. Wydaje się, że oba powyższe rodzaje naruszeń realizują się w ramach ustalonego przez sądy stanu faktycznego. Pracownik zaznajomiony z wymaganiami bezpieczeństwa swojego pracodawcy i posiadający w tym zakresie odpowiednie przeszkolenie, wielokrotnie podejmował decyzję o podłączeniu prywatnego przenośnego nośnika danych (bez autoryzacji) do komputera służbowego.

Całości stanu faktycznego dopełnia szczególny rodzaj podmiotu, jakim jest pracodawca w omawianej sprawie. Powód-pracownik był bowiem zatrudniony na stanowisku „starszego przodownika Straży (…)"[27] w jednostce należącej do kategorii organów ścigania[28]. Ustalenie to, nawet bez dogłębnej analizy zakresu obowiązków powoda, pozwala na uznanie wyższego niż przeciętny poziomu zobowiązania do zachowania wymagań bezpieczeństwa przez pracowników, z uwagi na szczególny rodzaj wykonywanych zadań oraz możliwy dostęp do dokumentacji

---

[25] Tak np. wyrok SN z dnia 19 sierpnia 1999 r., I PKN 188/99, (OSNAPiUS 2000, nr 22, poz. 818). *Kodeks…*, red. K. Walczak, W. Muszalski, p. B. I 35.

[26] *Kodeks pracy. Komentarz*, red. K.W. Baran, *Komentarz do art. 52*, LEX.

[27] Uzasadnienie Wyroku, s. 2.

[28] W samej treści Wyroku dokonano zmian uniemożliwiających jednoznaczne wskazanie konkretnego podmiotu. Pozostały jednak elementy takie jak „komendant posterunku", czy „komendant Komendy Regionalnej" wskazujące na powyższe.

zawierającej informacje nieprzeznaczone do rozpowszechniania lub ustawowo objęte poufnością.

Naruszenie zasad dbałości o mienie zakładu pracy stanowi ciężkie naruszenie podstawowego obowiązku pracownika[29]. Do stwierdzenia ciężkiego naruszenia obowiązków wystarczy ustalenie, że zaistniało zagrożenie wystąpieniem istotnej szkody. W analizowanym przez sądy stanie faktycznym, wskazane zagrożenie przejawiało się w możliwym dostępie osób trzecich do informacji dostępnych na komputerze służbowym, w wyniku możliwego zainfekowania tego komputera lub późniejszego dostępu do niezabezpieczonego przenośnego nośnika danych[30]. Powyższe zostało dodatkowo uprawdopodobnione w ramach postępowania sprawdzającego (przeprowadzonego przez pracodawcę przed rozwiązaniem umowy o pracę z winy pracownika), w wyniku którego stwierdzono, że badane nośniki danych są zainfekowane złośliwym oprogramowaniem. Jednakże, nawet w przypadku braku ustalenia, że nośniki zostały zainfekowane, samo naruszenie wewnętrznych przepisów dotyczących korzystania ze sprzętu komputerowego było niezgodne z wdrożonymi przez pracodawcę zasadami bezpieczeństwa. Postępowanie niezgodne z takimi zasadami może prowadzić do zainfekowania komputera służbowego lub sieci komputerowej pracodawcy złośliwym oprogramowaniem, a w konsekwencji prowadzić do nieautoryzowanego dostępu do informacji, w tym danych, które są przechowywane w tej sieci.

W wyroku Sądu Okręgowego w Piotrkowie Trybunalskim w sprawie dotyczącej wykorzystania służbowego komputera z naruszeniem zasad bezpieczeństwa w postaci przechowywania na nim materiałów pornograficznych (co również mogło prowadzić do zainfekowania komputera lub sieci pracodawcy), sąd zważył, że „skoro zatem powód – jak wykazało postępowanie dowodowe – posiadał na swoim komputerze treści

[29] *Kodeks*…, red. K. Walczak, W. Muszalski

[30] L. Christou, *Unencrypted USB devices are putting more than 50% of businesses at risk of a data leak*, https://www.verdict.co.uk/usb-data-breach/, 02.12.2020; *Did you know that connecting a device via USB could be a serious security risk?*, https://www.netstar.co.uk/usb-security-risk/, 02.12.2020; C. Franklin Jr, *USB Drives Remain Critical Cyberthreat*, https://www.darkreading.com/threat-intelligence/usb-drives-remain-critical-cyberthreat/d/d-id/1332894, 02.12.2020.

niezwiązane z wykonywaną pracą i zajmowanym stanowiskiem tj. treści pornograficzne i miał tego świadomość, czym ciężko naruszył podstawowy obowiązek pracowniczy dbałości o dobro i mienie pracodawcy, co z kolei naruszało interesy pracodawcy, gdyż zagrażało bezpieczeństwu sieci informatycznej pracodawcy, to wskazane w oświadczeniu pracodawcy przyczyny rozwiązania stosunku pracy, prawidłowo Sąd Rejonowy uznał za prawdziwe i konkretne i jako takie uzasadniające rozwiązanie umowy o pracę bez wypowiedzenia w myśl art. 52 § 1 pkt 1 k.p."[31]. We wskazanym orzeczeniu podkreślono również, że nieprawidłowe użytkowanie komputera pracodawcy może powodować zagrożenie bezpieczeństwa informatycznego pracodawcy.

Zaznaczenia w kontekście rozpatrywanego stanu faktycznego wymaga, że problematyka bezpieczeństwa, w tym bezpieczeństwa sieciowego, stanowi ogromny problem i jest najprawdopodobniej jednym z największych wyzwań, przed którymi stoi społeczeństwo w XXI w. Z tego powodu nie dziwią kolejne rozwiązania prawne mające zapewnić bezpieczeństwo informacji[32], jak również pierwsze akty prawne dotyczące cyberbezpieczeństwa[33]. W celu zwiększenia poziomu bezpieczeństwa w organizacjach wprowadza się różne rozwiązania, które można podzielić najogólniej na środki techniczne i organizacyjne[34]. Do tych drugich należą szczególnie wewnętrzne procedury ustanowione w celu ochrony systemów informacyjnych. Aby zapewnić wyższy poziom bezpieczeństwa organizacji,

---

[31] Wyrok SO w Piotrkowie Trybunalskim z dnia 31 stycznia 2019 r., V Pa 81/18 (Legalis).

[32] 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.Urz. UE L 119, s. 1) – dalej: RODO.

[33] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1) i implementująca ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560) czy rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15).

[34] Taką kategoryzacją posługuje się ustawodawca chociażby w RODO.

wszyscy zainteresowani muszą być zaznajomieni ze wskazanymi procedurami oraz wdrożyć je w ramach swojej codziennej pracy.

Jednocześnie autor zwraca uwagę, że człowiek pozostaje najbardziej wadliwym elementem systemu cyberbezpieczeństwa. Wskazuje się, że błąd człowieka odpowiada za nawet 95% naruszeń bezpieczeństwa[35]. Pomimo że w zależności od przyjętego modelu badań lub ich mechanizmu wyniki mogą się różnić, błąd człowieka jest w tym przypadku zawsze na pierwszym miejscu. Oznacza to, że większości naruszeń dałoby się uniknąć, gdyby nie zachowanie poszczególnych osób. Z tego powodu wewnętrzne procedury cyberbezpieczeństwa oraz odpowiednie przeszkolenie pracowników należą do absolutnych podstaw bezpieczeństwa informacji w każdej organizacji, a w szczególności takiej, w której dochodzi do przetwarzania danych poufnych lub wrażliwych. Jednocześnie inne badania wskazują, że w przypadku znalezienia przenośnego nośnika danych, prawie połowa osób nie tylko podłącza je do swojego komputera, ale również otwiera co najmniej jeden plik na nim zapisany[36]. Statystyki te pokazują, że pozostawienie zainfekowanego przenośnego nośnika danych należy do jednej z najłatwiejszych, a zarazem najskuteczniejszych metod ataku[37]. Stąd ataków przy wykorzystaniu przenośnego nośnika danych typu *pen-drive* powstała niezliczona ilość[38], a bezpieczeństwo przenośnych nośników danych doczekało się badań naukowych[39].

---

[35] Tak w badaniu IBM Security Services 2014. Cyber Security Intelligence Index. Zob. *Analysis of cyber attack and incident data from IBM's worldwide security operations*, https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf, 18.01.2020.

[36] E. Bursztein, *Concerns about usb security are real: 48% of people do plug-in usb drives found in parking lots,* https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots/, 18.12.2020.

[37] Tak również C. Franklin Jr*, USB*…; G. Cluley, *Does dropping malicious USB sticks really work? Yes, worryingly well*…, https://www.tripwire.com/state-of-security/featured/does-dropping-malicious-usb-sticks-really-work-yes-worryingly-well/, 18.12.2020.

[38] Zobacz np. listę 29 różnych ataków wykorzystujących urządzenia podłączane do portu USB, https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/, 18.20.2020.

[39] Zob. H. Jeong [i in.], *Vulnerability analysis of secure USB flash drives, Memory Technology, Design and Testing*, IEEE, 2007, s. 61–64; D. Olenick, *Computers vulnerable to attack through USB ports, report*, https://www.scmagazine.com/home/security-news/vulnerabilities/computers-vulnerable-to-attack-through-usb-ports-report/, 20.12.2020.

Większość badań jednoznacznie wskazuje na brak bezpieczeństwa przenośnych nośników danych i potrzebę przywiązywania szczególnej wagi do ich wykorzystania. Już samo bowiem podłączenie zainfekowanego nośnika może spowodować zainfekowanie stacji roboczej lub całej sieci[40]. Ten rodzaj ataków jest nie tylko znany, ale również bardzo często wykorzystywany w ramach profesjonalnych akcji podejmowanych przez agencje wywiadowcze, o czym można było się dowiedzieć z upublicznionych informacji wewnętrznych CIA[41].

Ryzyko, jakie wiąże się z wykorzystaniem nieautoryzowanego przenośnego nośnika danych, jest niewątpliwe. Często jednak zapomina się o nim w kontekście nieświadomego umożliwienia dostępu do informacji lub danych o charakterze poufnym, do którego może dojść, jeśli urządzenie jest zainfekowane lub jest na nim zainstalowanie złośliwe oprogramowanie. W niektórych badaniach podaje się, że nawet ¼ wszystkich przypadków rozprzestrzeniania się złośliwego oprogramowania dzieje się za pośrednictwem urządzeń przenośnych[42]. Dlatego nie powinno dziwić, że wiele organizacji stara się wykluczać m.in. powyższe ryzyka poprzez stosowanie odpowiednich środków organizacyjnych w rozumieniu art. 32 ust. 1 RODO, do których należy w szczególności stworzenie i wdrożenie odpowiedniej polityki wykorzystania przenośnych nośników danych[43]. Powyższe przekłada się na rzeczywiste działania, gdyż z badań wynika, że aż 64% organizacji posiada wdrożoną procedurę dotyczącą wykorzystania przenośnych nośników danych[44].

---

[40] Zob. historię jednego z największych ataków cybernetycznych Stuxnet. Zob. J. Talamantes, *USB Drop Attacs: The Danger of „Lost And Found" Thumb Drives*, https://www.redteamsecure.com/blog/usb-drop-attacks-the-danger-of-lost-and-found-thumb-drives/, 20.12.2020.

[41] B. Muqeet, *Wikileaks Reveals The CIA's Illegal PC Hacking via USB*, https://www.privacyend.com/wikileaks-reveals-cia-illegal-pc-hacking-via-usb/, 20.12.2020.

[42] Z. Ali, *How a USB could become security risk for your device*, https://www.hackread.com/how-your-usb-becomes-a-security-risk/, 20.12.2020.

[43] Obok równie standardowych polityk czystego biurka, pulpitu lub drukarki.

[44] *The State of USB Data Protection 2019*, https://www.apricorn.com/media/2019surveyinfographic.pdf, 20.12.2020.

6. Podsumowanie

Bezpieczeństwo informacji jest jednym z największych zagrożeń, przed którym stoją różnego rodzaju i poziomu organizacje na całym świecie[45]. Nie od dzisiaj wiadomo, że informacje posiadają wymierną wartość. O tym, że świadomość ryzyk wzrasta, mogą chociażby świadczyć wchodzące w życie akty prawne, które wprowadzają nowe wymogi w obszarze bezpieczeństwa informacji, w tym również danych osobowych, co zostało omówione przez autora. W ramach wspomnianych aktów nakłada się na odpowiednie jednostki obowiązek oceny występujących ryzyk i wdrożenie środków odpowiednich do ich zniwelowania. W większości przypadków dzieli się je na środki organizacyjne i techniczne[46]. Do pierwszej ze wskazanych grup należą w szczególności wdrożone wewnętrzne procedury działania w określonych przypadkach. Do takich przypadków może należeć wystąpienie określonego incydentu[47] lub np. postępowanie w przypadku potrzeby podłączenia przenośnego nośnika danych. Podkreślenia w tym kontekście wymaga, że zagrożenia wynikające z wykorzystywania nieautoryzowanego przenośnego nośnika danych są znaczące, o czym świadczyć może chociażby fakt, że jednostka US-CERT wydała raport dotyczący takich ryzyk i możliwości ich minimalizacji[48]. Wskazane wyżej procedury stanowią zatem wyznacznik zachowania przyczyniającego się do zdecydowanego obniżania poziomu ryzyk, na które narażone są różne organizacje.

W komentowanym Wyroku sądy różnych instancji podkreślały zasadność powództwa i brak wątpliwości co do pierwszego elementu czynu powoda – podłączenia nieautoryzowanych przenośnych nośników danych do służbowego komputera. Pomimo dowodów świadczących o tym, że na wskazanych nośnikach znajdowały się pliki pochodzące z tego

---

[45] Zob. mapę zagrożeń cyberprzestrzeni aktualizowaną w czasie rzeczywistym. Zob. *Live Cyber Threat Map*, https://threatmap.checkpoint.com/, 20.12.2020.

[46] Jak również we wskazanych aktach prawnych.

[47] Lub dokonanie oceny czy jest to incydent.

[48] P. Walters, *The Risks of Using Portable Devices*, US-CERT, United States Computer Emergency Readiness Team, https://www.us-cert.gov/sites/default/files/publications/RisksOfPortableDevices.pdf, 20.12.2020.

komputera, jak się wydaje, nie uznano tego elementu za jednoznacznie udowodniony[49]. Jednocześnie wskazano że „w przypadku udowodnienia powodowi zarzucanego mu zachowania, rozwiązanie umowy o pracę bez wypowiedzenia z jego winy byłoby uzasadnione"[50]. Jak wynika z powyższego, sądy wszystkich instancji doszły w niniejszym stanie faktycznym do wniosku, że udowodniono podłączenie nieautoryzowanego nośnika danych do komputera służbowego, co stanowi naruszenie obowiązków pracowniczych. Jednakże nie udowodniono ściągnięcia danych na wskazany nośnik, co uzasadniałoby kwalifikację jako istotnego naruszenia podstawowych obowiązków pracowniczych umożliwiającą rozwiązanie umowy o pracę bez zachowania terminu wypowiedzenia z winy pracownika.

Powyższe rozumowanie jest całkowicie racjonalne i uzasadnione w świetle orzecznictwa. Wydaje się, że pominięto w tym przypadku dynamiczny rozwój technologii i zmiany, również w obszarze prawnym, które miały miejsce w ostatnich latach. Jak zobrazowano przy wykorzystaniu licznych badań naukowych i pochodzących z nich statystyk, cyberbezpieczeństwo należy do kluczowych ryzyk, na które narażone są różnego rodzaju organizacje. Biorąc powyższe pod uwagę, to człowiek należy do największych czynników ryzykotwórczych. Dlatego jakiekolwiek działania w obszarze zarządzania ryzykiem powinny być poprzedzone wdrożeniem odpowiednich polityk i edukacją pracowników. Porównując bezpieczeństwo informacji w ramach danej organizacji do bezpieczeństwa budynku, należałoby wskazać, że wdrożenie nawet najbardziej zaawansowanych środków technicznych (na przykład alarmu czy monitoringu) może pozostać bez znaczenia dla bezpieczeństwa, w przypadku gdy podstawowe środki organizacyjne związane z bezpieczeństwem, jak na przykład zamykanie drzwi[51], nie są skutecznie zaimplementowane. Co więcej, takie sytuacje

[49] Sąd pierwszej instancji wskazał, że „nie ma jednoznacznych dowodów na przyjęcie, iż to powód dokonał skopiowania na swoje urządzenia informacji objętych ustawą o ochronie danych osobowych lub stanowiących tajemnicę przedsiębiorcy".

[50] Podkreślano również, że w świetle orzecznictwa niekwestionowane jest, że do ciężkich naruszeń podstawowych obowiązków pracowniczych należy skopiowanie informacji stanowiących tajemnicę przedsiębiorstwa lub objętych ochroną danych osobowych.

[51] Analogicznie do obowiązku ustawiania hasła i wylogowywania się.

mogą powodować obciążenie odpowiedzialnością z tytułu nieuprawnionego dostępu do określonych danych, również samą organizację, która ostatecznie nie zapewniła odpowiedniej ochrony swoich zasobów. Przykłady wyroków odnoszących się do podobnych zagadnień są coraz liczniejsze[52] i, jak się wydaje, kwestie zachowania cyberbezpieczeństwa będą przedmiotem jeszcze wielu dyskusji.

Wykorzystywanie przenośnych nośników danych, podobnie jak korzystanie z sieci Internet, samo w sobie może generować ryzyka dla organizacji. Jednak przy wdrożeniu kilku prostych zasad możliwe jest znaczące zminimalizowanie takich ryzyk[53]. Zasady te, jak również wskazówki i dobre praktyki, najczęściej są ubierane w ramy wewnętrznych procedur lub polityk obowiązujących w danym przedsiębiorstwie. Każdy pracownik jest zobowiązany do zapoznania się z nimi i ich akceptacji, a w większości przypadków przeprowadza się nawet cykliczne szkolenia[54]. W związku z powyższym, jak również wziąwszy pod uwagę wszelkie przedstawione raporty, statystyki i dane, w opinii autora należy uznać, że w zaprezentowanym stanie faktycznym już samo umieszczenie przez pracownika nieautoryzowanego prywatnego nośnika danych w porcie komputera służbowego jest umyślnym naruszeniem podstawowego obowiązku pracownika dbałości o dobro zakładu pracy i ochrony jego mienia[55]. Choć sytuacja ta jest wyjątkowa ze względu na specyficzny charakter pracodawcy w omawianym stanie faktycznym, to powyższa zasada powinna

---

[52] Zobacz np. wyrok Sądu Najwyższego Zjednoczonego Królestwa z dnia 1 kwietnia 2020 r., UKSC 2018/0213, *Various claimants przeciwko WM Morrison Supermarkets* ([2020] UKSC 12), w której były pracownik (audytor systemów IT) udostępnił dane osobowe ponad 100 tys. innych pracowników, a za odpowiedzialną uznano organizację pracodawcy, pomimo wdrożenia odpowiednich procedur wewnętrznych.

[53] *How to use a USB without the risk of data leaks*, https://www.pandasecurity.com/mediacenter/security/usb-without-the-risk-of-data-leaks/, 20.12.2020; C. Eckstein, *Preventing data leakage. A risk based approach for controlled use of the use of administrative and access privileges*, SANS 2015, s. 5 i n.; por. K. Lee [i in.], *A Study on a Secure USB Mechanism That Prevents the Exposure of Authentication Information for Smart Human Care Services*, JoS 2018.

[54] Należy mieć na uwadze, że samo wdrożenie procedur bez odpowiedniego przeszkolenia i zabezpieczenia może nie przynosić założonych skutków. Tak np. J. Wiele, *Pebkac revisited – Psychological and Mental Obstacles in the Way of Effective Awareness Campaigns* [w:] *ISSE2011 Securing Electronic Business Processes*, red. N. Pohlmann, H. Reimer, W. Schneider, s. 93.

[55] Art. 100 § 2 pkt 4 KP.

mieć zastosowanie w większości przypadków, w których dany pracownik posiada, co do zasady, nieograniczony dostęp do infrastruktury IT pracodawcy lub zakres informacji lub danych, do których ma dostęp jest na tyle szeroki, aby powyższe stanowiło istotne ryzyko. Ryzyko to może się zmaterializować chociażby w stratach finansowych[56], które stale i dynamicznie rosną, a odpowiednie procedury i przeszkolenie pracowników nadal jest oceniane jako najmniej dofinansowana aktywność w zakresie bezpieczeństwa cybernetycznego[57].

S t r e s z c z e n i e

Cyberbezpieczeństwo stanowi jedno z największych wyzwań dla współczesnej gospodarki. Coraz większe koszty związane z naruszeniami bezpieczeństwa cybernetycznego uzasadniają rosnące wraz z nimi budżety i środki przeznaczane na minimalizację ryzyk. W tym celu wprowadza się do organizacji środki organizacyjne i techniczne, które mają odpowiadać stwierdzonym ryzykom i uwzględniać aktualny stan techniki. Powyższe wynika z obowiązków prawnych, w tym przypadku z rozporządzenia 2016/679 z dnia 27 kwietnia 2016 r. (RODO). Statystyki bezsprzecznie wskazują, że działanie człowieka odpowiada za zdecydowaną większość przypadków nieuprawnionego dostępu do informacji. Stąd należy uznać, że odpowiednie wypełnianie procedur wewnętrznych jest jednym z podstawowych obowiązków pracowniczych, a ich naruszenie może prowadzić do powstania co najmniej zagrożenia istotną szkodą w mieniu pracodawcy.

Słowa kluczowe: cyberbezpieczeństwo, nośnik danych, ryzyko, *pen-drive*, procedura.

---

[56] Wydatkach związanych z wdrożeniem odpowiednich zabezpieczeń jak również ewentualnych kar lub kosztów działań zaradczych w przypadku wystąpienia incydentu.

[57] Accenture Security, *The Cost of Cybercrime, Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Protection*, 2019, s. 8 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50, 21.12.2020.

Commentary to the III PK 13/18 Supreme Court judgement of February 13, 2019 – partially critical

Summary

Cybersecurity is one of the biggest challenges facing the modern economy. The increasing costs of cyber security breaches justify the rising budgets and funds allocated to minimize the risks it entails. To this end, organizational and technical measures are introduced into organizations to meet these risks and take into account the state of the art. Such changes are also the result of legal obligations, such as those stemming from Regulation 2016/679 of 27 April 2016 ("GDPR"). Statistics clearly indicate that human action is responsible for the vast majority of unauthorized access to information. Accordingly, it should be recognized each employee's basic obligations include proper compliance with internal procedures and that the violation of such procedures may at least give rise to a threat of material damage to the employer's property.

Key words: cybersecurity, storage medium, risk, pen drive, procedure.

dr Marek Porzeżyński
Warsaw University of Technology
Faculty of Administration and Social Sciences
Pl. Politechniki 1, 00-661 Warsaw, Poland
e-mail: m.porzezynski@wp.pl