Głos Prawa **The Voice of Law**

Przegląd Prawniczy Allerhanda
2019 – t. 2 – nr 2 (4), poz. 23
ISSN 2657-7984

Allerhand Law Review
2019 – Vol. 2 – No. 2 (4), item 23
e-ISSN 2657-800X

Konrad Zawodziński*

WHISTLEBLOWING W INSTYTUCJACH FINANSOWYCH I W SEKTORZE NIEFINANSOWYM JAKO OBSZAR KONWERGENCJI WYMOGÓW I WYZWAŃ COMPLIANCE ORAZ WSPÓLNEGO POSZUKIWANIA ROZWIĄZAŃ

Celem artykułu jest przedstawienie whistleblowingu jako jednego z obszarów postępującej konwergencji regulacyjnej między instytucjami finansowymi i przedsiębiorstwami spoza sektora finansowego oraz identyfikacja wyzwań pojawiających się na tle dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii. W tekście podjęto próbę rozwiązania niektórych z trudności, w szczególności w odniesieniu do zgłoszeń nieprawidłowości dokonywanych w złej wierze. Rozważaniom tym towarzyszą bardziej ogólne uwagi dotyczące *compliance*, oparte o „cykl życia normy prawnej".

Pojęcia kluczowe: *whistleblowing*, sygnalista, *compliance*, dyrektywa o ochronie sygnalistów, harmonizacja, konwergencja regulacyjna, zarządzanie ryzykiem, zwolnienie dyscyplinarne, postępowanie wyjaśniające

* Konrad Zawodziński, członek-założyciel Sekcji Przeciwdziałania Korupcji w Biznesie i Compliance Instytutu Allerhanda, doktorant w Kolegium Prawa Akademii im. Leona Koźmińskiego, adwokat (Izba Adwokacka w Warszawie); ORCID: 0000-0002-5420-5656. Artykuł został przedstawiony podczas konferencji naukowej VI Kongresu FinReg 2019.

1. Uwagi wprowadzające

Bezpowrotnie minęły czasy, kiedy w dyskusji na temat whistleblowingu i whistleblowerów w Polsce zastanawiano się nad najbardziej adekwatnym odpowiednikiem tego określenia oraz znaczeniem pojęcia. Wydaje się, że praktyka gospodarcza, wespół ze środowiskiem akademickim, twórcami projektów aktów prawnych lub podwalin tychże, utorowały posługiwanie się oryginalnym sformułowaniem[1] obok takich polskich wyrażeń jak „(anonimowe) zgłaszanie (raportowanie, sygnalizowanie) nieprawidłowości" i „sygnalista". Pochopne byłoby jednak przyjęcie, że rozumienie wypracowane przez praktyków wolne jest od kontrowersji, a temat – wyczerpująco zbadany. Z pewnością jeden z dylematów dotyczy odejścia od „stonowanego" komunikowania nadużyć wobec przedsiębiorstwa lub organów władzy na rzecz nagłośnienia nieprawidłowości w środkach masowego przekazu.

Pożegnać przyszło też poszukiwanie polskiego odpowiednika „*compliance*" i definicji tego pojęcia[2]. Niewolne od kontrowersji, choć nie razi czytelnika w brzmieniu angielskim, zwykło się je tłumaczyć na język polski jako „zarządzanie zgodnością" lub „zarządzanie ryzykiem braku zgodności", co na marginesie może zawężać rozumienie „*compliance*" do jego procesowego wymiaru. Refleksja nad „*compliance*" przyniosła ze sobą także rozpowszechnienie się siatki pojęciowej zarówno autonomicznej, jak i zaczerpniętej z zarządzania ryzykiem. Przykładem pierwszego jest określenie „standard zgodności", rozumiane jako norma, do przestrzegania której organizacja zobowiązuje się dobrowolnie (w drodze autoregulacji, samoograniczania się, poprzez np. kodeks dobrych praktyk) lub jest zobowiązana (normy prawne i inne zewnętrzne standardy zgodności). Drugie ilustruje np. właściciel ryzyka, rozumiany jako kierujący jednostką, z której działalnością związane jest ryzyko braku zgodności. Oczywiście centralne pojęcie „ryzyka braku zgodności", obejmującego zwłaszcza ryzyka prawne, także nawiązuje do zarządzania ryzykiem[3].

---

[1] Prekursorskie opracowanie: W. Rogowski, *Whistleblowing: bohaterstwo, zdrada czy interes?,* „Przegląd Corporate Governance" 2007, nr 1 (9), s. 23-41; zob. także: A. Wojciechowska-Nowak, *Założenia do ustawy o ochronie osób sygnalizujących nieprawidłowości w środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych?,* Fundacja Batorego, Warszawa 2012, http://www.batory.org.pl/upload/files/Programy%20operacyjne/Przeciw%20Korupcji/zalozenia-do-ustawy-o-ochronie-sygnalistow.pdf (dostęp: 15 listopada 2019) r.; *Jawność i jej ograniczenia. T. II. Podstawy aksjologiczne,* red. Z. Cieślak, G. Szpor, Legalis 2013, rozdział 2, § 3, pkt II.8 *Ujawnianie nadużyć (whistleblowing);* O. C. Ferrel, J. Frædrich, L. Ferrell, *Business Ethics. Ethical decision making and cases, Mason 2013,* s. 191; A. Lewicka-Strzałecka, *Instytucjonalizacja whistleblowingu w firmie jako wyzwanie etyczne,* „Diametros" 2014, nr 41, s. 77-98; A. Piskorz-Szpytka, P. Szpytka, *Whistleblowing jako element systemu compliance,* [w:] *Compliance w wybranych podmiotach nadzorowanych rynku finansowego. Aspekty praktyczne,* red. P. Eleryk, A. Piskorz-Szpytka, P. Szpytka, LEX 2019.

[2] B. Makowicz, *Compliance w przedsiębiorstwie,* Warszawa 2011, s. 15-19.

[3] O dwoistej naturze ryzyka prawnego piszą m.in. K. Anderson, J. Black, *Legal risks and risks for lawyers,* Londyn 2013, s. 2-4, http://www.lse.ac.uk/law/people/academic-staff/julia-black/Documents/black9.pdf (dostęp: 15 listopada 2019 r.), zwracając celnie uwagę, że ryzyko to może obejmo-

Niewątpliwie postępujące zaawansowanie rozwiązań występujących w biznesie w zakresie whistleblowingu nie jest przeszkodą dla usystematyzowania refleksji na temat. Dzieje się tak nie tyle z uwagi na nieobecność tego rodzaju rozważań w polskim piśmiennictwie przez pewien czas, lecz także ze względu na istotne zmiany prawne w tym zakresie. W niniejszym artykule podjęto próbę zidentyfikowania pojawiających się wyzwań dla przedsiębiorstw, koncentrując się na problematyce wewnątrzorganizacyjnej, nie zaś kształtowaniu relacji z organami władzy czy tzw. ujawnieniem publicznym.

Proponuje się przy tym spojrzenie na *whistleblowing* jako jeden z elementów holistycznego i koherentnego systemu zarządzania ryzykiem braku zgodności (*compliance*), który z kolei podlega procesowi wielowymiarowej uniwersalizacji, między innymi wskutek konwergencji regulacyjnej, obserwowanej między instytucjami finansowymi oraz sektorem niefinansowym, zwłaszcza energetyką. Jak zauważono w piśmiennictwie, „System *Compliance* należy zatem budować w oparciu o konkretne wartości społeczne, dostrzeżone i odpowiednio wdrożone także na poziomie mikroekonomicznym. Na koniec należy jednoznacznie stwierdzić, że dobry system *Compliance* w przedsiębiorstwie nie zadziała bez wsparcia odpowiednich reguł etycznych”[4].

2. Wielowymiarowa uniwersalizacja zarządzania ryzykiem braku zgodności

Początki funkcji *compliance* powszechnie wiąże się z sektorem finansowym[5], choć niektórzy autorzy upatrują ich przed pojawieniem się wytycznych Komitetu Bazylejskiego, w przeciwdziałaniu naruszeniom prawa konkurencji w dużych przedsiębiorstwa amerykańskich[6]. Bez potrzeby zreferowania dynamicznego rozwoju zarządzania ryzykiem braku zgodności, można zgodzić się, że *compliance* z czasem zaczęło upowszechniać się w innych dziedzinach gospodarki. Upowszechnienie *compliance* doprowadziło do poszukiwania uniwersalnych modeli zarządzania ryzykiem zgodności. Uniwersalne trendy przejawiają się w wymiarze

wać zarówno ryzyko, którego źródło tkwi poza sferą prawną, natomiast materializuje się ono w tej sferze (np. w postaci sankcji ze strony organów władzy), jak i odwrotnie – ryzyko wynikające z przepisów prawnych, które ma swoje pozaprawne implikacje (np. stanowi przeszkodę w działalności operacyjnej). Wydaje się, że skutki ziszczenia się ryzyka braku zgodności, tradycyjnie wiązane m.in. ze sferą finansową, reputacyjną (wizerunkową) i operacyjną, konsumują tę dystynkcję (por. P. Hopkin, *Fundamentals of Risk Management. Understanding, evaluating and implementing effective risk management*, Londyn 2014, s. 21-25).

[4] B. Makowicz, *Compliance...*, s. 146; B. Makowicz, *Metody efektywnego kształtowania systemów compliance – Wprowadzenie*, „Monitor Prawniczy” 2013, nr 23 – dodatek specjalny, s. 1.

[5] P. Szpytka, *Geneza i rozwój compliance*, [w:] *Compliance w wybranych...*, red. P. Eleryk, A. Piskorz-Szpytka, P. Szpytka.

[6] B. Jagura, *Rozwój w ujęciu historycznym*, [w:] *idem, Rola organów spółki kapitałowej w realizacji funkcji compliance*, LEX 2017.

metodycznym, organizacyjnym (funkcjonalnym), procesowym i materialnym[7]. Przykładowo, przejawem uniwersalizacji metodycznej *compliance* jest oparcie tej funkcji na ekspozycji na ryzyko *(risk-based approach)* oraz wyodrębnienie wyspecjalizowanych jednostek *compliance* i funkcji *compliance officer*.

Poszukiwanie uniwersalnych rozwiązań organizacyjnych zakłada normalizację funkcji przy jednoczesnym rozproszeniu i skoordynowaniu osób odpowiedzialnych za zarządzanie ryzykami braku zgodności (swoistych liderów merytorycznych w organizacji, odpowiedzialnych za zarządzanie różnymi obszarami ryzyk braku zgodności) bądź ich skoncentrowaniu w jednej jednostce. Pierwsze z rozwiązań w większym stopniu sprosta potrzebom organizacji o wielobranżowej działalności i wielooddziałowej strukturze, drugie wydaje się bardziej adekwatne dla przedsiębiorstwa skoncentrowanego na określonym sektorze.

Uniwersalizacja w wymiarze procesowym sprowadza się do pytania, jakie strumienie czynności i jakie działania podejmuje się w ramach systemu zarządzania ryzykami braku zgodności. Obok prób normalizacji podjętych przez m.in. ISO, toczy się dyskusja na temat współzależności *compliance* i innych funkcji w przedsiębiorstwie. Nie opowiadając się jednoznacznie ani za metodycznym podejściem *Risk Management Institute*, ani optyką COSO, można zgodzić się, że *compliance*, obok audytu i zarządzania ryzykiem, plasuje się pośród funkcji *assurance*. Ze względu na procesową przydatność, w organizacji prowadzącej złożoną sektorowo działalność, warto rozważyć podejście oparte na zdecentralizowanym, lecz skoordynowanym systemie uwzględniającym dynamikę zmian w otoczeniu prawno-regulacyjnym, określoną jako cykl życia normy prawnej.

Proponowane pojęcie „cyklu życia normy prawnej" wzorowane jest na cyklu życia produktu i przedsiębiorstwa oraz zespołu (Bruce Tuckman i Mary Jensen), wypracowanych w naukach o zarządzaniu. Obejmuje ono:

- *forming* – monitorowanie zmian w prawodawstwie, orzecznictwie i praktyce decyzyjnej, ocenę oddziaływania zmian na przedsiębiorstwo, zgłaszanie uwag do projektów, przedstawianie opinii *amicus curiae*, udział w wysłuchaniach publicznych, rzecznictwo interesów;
- *storming* – dyskusję nad niezbędnymi środkami służącymi zarządzaniu ryzykiem braku zgodności wynikającym ze zmia-

[7] Ch. Roquilly, Ch. Collard, *De la conformité réglementaire à la performance: pour une approche multidimensionnelle du risque juridique*, Centre de Recherche Legal EDHEC Business School, https://www.edhec.edu/sites/www.edhec-portail.pprod.net/files/publications/pdf/com.univ.collaboratif.utils.LectureFichiergw%3FID_FICHIER%3D1328885973394jpg (dostęp: 15 listopada 2019 r.); B. Jagura, *Przyczyny i kierunki rozwoju compliance*, [w:] *idem, Rola organów...*

ny i alokacja w przedsiębiorstwie odpowiedzialności za ich wdrożenie, stosowanie i przegląd;
- *norming* – wdrażanie zmian w otoczeniu prawnym (prawodawczych lub w praktyce stosowania prawa) w organizacji i tworzenie środków służących zarządzeniu ryzykiem braku zgodności, obejmujących ukształtowanie procesu decyzyjnego w sposób pozwalający na świadome określenie m.in. apetytu na ryzyko i warunków akceptacji określonego poziomu ryzyka, ustalanie standardów i rozwijanie praktyki stosowania ustanowionych środków służących zarządzaniu ryzykiem braku zgodności;
- *performing* – stosowanie wdrożonych środków, pozwalające na osiągnięcie pożądanego poziomu tolerowanego ryzyka braku zgodności.

Podejmowane czynności korespondują z wieloma funkcjami występującymi w organizacji i obejmują w szczególności komunikację wewnętrzną i zewnętrzną oraz szkolenia. Jednym z takich mechanizmów będzie niewątpliwie konsultowanie, przyjmowanie i promulgowanie legislacji wewnętrznej[8] oraz zgłaszanie nieprawidłowości, prowadzenie postępowań wyjaśniających, audytów i kontroli zgodności[9].

Uniwersalizacja w wymiarze materialnym dotyczyć będzie standardów zgodności, dla których punktem wyjścia, kluczowym dla ustalenia spójnej misji i wizji, jest wprowadzenie w przedsiębiorstwie kodeksu etyki lub podobnego dokumentu kierunkowego[10]. W wielu obszarach, np. konfliktu interesów, towarzyszyć będą mu regulacje wykonawcze, np. dotyczące wyłączenia określonych osób od prowadzenia niektórych spraw. Niewątpliwie do takich regulacji zaliczyć należy politykę antykorupcyjną i prezentową, normującą w szczególności zasady przyjmowania i wręczania prezentów, prowadzenie rejestru korzyści oraz uwrażliwiającą na szersze implikacje przejawów „gościnności", zwłaszcza podatkowe i prawnokarne.

Uniwersalizacja przejawia się zarówno w zmianach legislacyjnych, jak i wypracowaniu standardów pozaprawnych. Pośród rozwiązań prawodawczych należy odnotować zarówno sektorowe (np. obowiązek ustanowienia inspektorów ds. zgodności i przygotowania programów zgodności w przedsiębiorstwach energetycznych spełniających funkcję operatora infrastruktury, do której należy zapewnić tzw. dostęp stron trzecich, na niedyskryminacyjnych zasadach), jak i mające bardziej gene-

[8] T. Braun, *Postulaty porządkujące – propozycja modelowego ujęcia norm compliance*, [w:] *idem, Unormowania compliance w korporacjach*, LEX 2017.

[9] B. Jagura, *Odgraniczenie terminologiczne compliance od pojęć pokrewnych i innych jednostek*, [w:] *idem, Rola organów...*

[10] C. Meckenstock, *Struktura i wdrażanie systemów "compliance" – wprowadzenie praktyczne*, „Monitor Prawniczy" 2013, nr 23 – dodatek specjalny, s. 6-8.

ralny charakter. Przykładem tych drugich jest wzrost znaczenia rad nadzorczych i wyodrębnionych z nich wyspecjalizowanych gremiów, komitetów audytu. Przedmiotem zainteresowania komitetów audytu, oprócz badania sprawozdań finansowych i zagadnień z tym związanych (jak rekomendacje dotyczące wyboru firmy audytorskiej, rola w zapewnieniu jej niezależności), samej funkcji audytu i kontroli wewnętrznej, jest właśnie *compliance.*

Jednostkami zainteresowania publicznego są natomiast nie tylko instytucje finansowe, lecz również spółki publiczne jako emitenci papierów wartości dopuszczonych do obrotu na rynku regulowanym (art. 2 pkt 9 lit. a ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym). Wiodące pod względem kapitalizacji spółki giełdowe w Polsce reprezentują – abstrahując od banków i zakładów ubezpieczeń – przede wszystkim sektor paliwowo-energetyczny (Polskie Górnictwo Naftowe i Gazownictwo, Polska Grupa Energetyczna, Lotos, Orlen, Tauron) i telekomunikacyjny (Orange).

Mówiąc z kolei o rozwiązaniach pozaustawodawczych, należy pamiętać o standardach „branżowych" dla *compliance*, np. normy ISO powstały zarówno dla zarządzania ryzykiem (ISO 31000:2009 i jej polski odpowiednik PN-ISO 31000:2012), jak i – na wzór tychże – dla zarządzania ryzykiem braku zgodności (ISO 19600) oraz dla przeciwdziałania korupcji (ISO 37001). Zrozumiałą presję na wdrożenie tego rodzaju rozwiązań w przedsiębiorstwie wywierać będzie rozwój przepisów o odpowiedzialności podmiotów zbiorowych i próby wykazania należytej staranności oraz zaadresowania braku winy w organizacji.

3. Konwergencja regulacyjna sektorów gospodarki

Konwergencja regulacyjna jest wielopoziomowym procesem, zróżnicowanym pod względem przyczyn oraz przejawów, rozumianym tutaj w płaszczyźnie horyzontalnej źródeł prawa, jako postępująca zbieżność regulacji działalności w różnych sektorach gospodarki[11]. Do jego przyczyn zaliczyć można zmiany w otoczeniu prawno-regulacyjnym (presję ustawodawczą) oraz upowszechniającą się praktykę biznesową, niekiedy presję komercyjną.

Wśród pierwszej grupy czynników należy wspomnieć pierwotne, wynikające ze stanowionego prawa, oraz wtórne, będące następstwem jego stosowania (wszczęcia przeciwko przedsiębiorcy postępowania lub zakończenia go decyzją wymierzającą karę lub zobowiązującą do określonego zachowania). Na uwzględnienie zasługują

[11] Por. M. Raczyński, *Implikacje konwergencji w branżach ICT dla polityki regulacyjnej*, http://mikroekonomia.net/system/publication_files/249/original/17.pdf?1314948750 (dostęp: 15 listopada 2019 r.).

tutaj dwa projekty ustaw, które w Sejmie poprzedniej kadencji nie zostały uchwalone, tj. ustawa o jawności życia publicznego (projekt zarzucono na etapie prac rządowych) oraz ustawa o odpowiedzialności karnej podmiotów zbiorowych za czyny zabronione pod groźbą kary. Ich szersze omówienie wykracza poza ramy niniejszego tekstu, niewątpliwie zwróciły one uwagę na znaczenie funkcji *compliance* w organizacji[12] oraz zintensyfikowały debatę wśród praktyków na temat skutecznych środków zarządzania ryzykiem baku zgodności. Pierwszy z nich przewidywał, obok innych wątpliwych rozwiązań (m.in. jawnego rejestru wszystkich zawieranych przez dany podmiot umów), rygorystyczny model ochrony sygnalisty oraz kary za pozorny lub nieskuteczny system *compliance*. Rozwiązania proponowane w tej ustawie budziły wiele wątpliwości, m.in. co do ich proporcjonalności, określoności (w przypadku norm karnych) czy zgodności z regułą *ne bis in idem*. W drugim z projektów również uwzględniono znaczenie kanałów zgłaszania nieprawidłowości i potraktowano zbagatelizowanie sygnałów od whistleblowerów jako okoliczność obciążającą, uzasadniającą surowsze ukaranie przedsiębiorcy.

Do drugiej grupy uwarunkowań należy zaliczyć w szczególności upowszechnienie się badania kontrahentów (CDD/KYC od ang. *client due diligence*, *know your client*) przed zawarciem umowy oraz wprowadzanie zapewnień kontraktowych dotyczących poprawności i aktualności wskazań zawartych w formularzu KYC. Coraz częściej w umowach występują także deklaracje o podzielaniu określonych wartości w biznesie, postanowienia uprawniające do wyznaczenia audytora celem zbadania ksiąg kontrahenta w razie podejrzeń dotyczących zgodności jego działalności z prawem (zwłaszcza podejrzeń naruszeń przepisów korupcyjnych, sankcji ekonomicznych lub regulacji dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu), czy wiążące się z określonym naruszeniem prawa umowne uprawnienie do zakończenia współpracy.

Motywacja komercyjna zbieżna jest niekiedy z uwarunkowaniami prawnymi. Przykładem takiej sytuacji będzie internacjonalizacji działalności, np. poprzez wejście na rynek amerykański i podleganie pod wymogi *Dodd Frank Act, Sarbanes-Oxley Act i Federal Sentencing Guidelines for Organisations*[13] w zakresie whistleblowingu lub intensyfikację wymiany handlowej z kontrahentami ze Stanów

[12] A. Maćkowiak, T. Wiciak, *Standardy compliance drogą do unikania odpowiedzialności. Refleksje po IX. Polsko-Niemieckim Forum Compliance*, „Monitor Prawniczy" 2018, nr 24, s. 1323-1327; A. Krawczyk, A. Gisman, *Criminal compliance jako środek zapobiegania odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary*, „Monitor Prawa Handlowego" 2015, nr 1, s. 7-12.

[13] T. M. Dworkin, *SOX and Whistleblowing*, „Michigan Law Review" 2007, nr 105 (8), s. 1757-1780, Z. Rezæe, *Sarbanes-Oxley requirements and the implementation of US corporate governance controls – an overview for non-US companies*, [w:] *Legal Risk Management, Governance and Compliance*, red. S. Weinstein, Ch. Wild, Londyn 2013, s. 145-164.

Zjednoczonych, którzy na etapie przedkontraktowym i w samych umowach często wprowadzają postanowienia dotyczące *compliance*. Oczywiście rozwiązania ochronne dla whistleblowerów występują także na innych rynkach, np. brytyjskim (*Public Interest Disclosure Act*).

Zbieżne okazują się także wymogi dotyczące kwestii procesowych i proceduralnych, formalne standardy zgodności, na przykład standardy zgodności dotyczące whistleblowingu, o których obszerniej mowa dalej, czy wymagające ustanowienia określonych wewnętrznych polityk i procedur (np. przepisy o rewizji finansowej dotyczące zakupu usług nieaudytorskich od audytorów czy przepisy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu). Przykładem konwergencji materialnych standardów zgodności o randze prawodawczej są np. rozporządzenia służące przeciwdziałaniu nadużyciom na rynkach finansowych oraz na rynkach energetycznych: rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (Dz.Urz.UE L 173 z 12 czerwca 2014 r., s. 1-61; tzw. MAR) oraz – wzorowane na poprzedzającej MAR dyrektywie MAD – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1227/2011 z dnia 25 października 2011 r. w sprawie integralności i przejrzystości hurtowego rynku energii (Dz.Urz.UE L 326 z 8 grudnia 2011 r., s. 1-16; tzw. REMIT). Obie regulacje w szczególności instytucjonalizują kategorię informacji cenotwórczych (zwanych odpowiednio – poufnymi i wewnętrznymi) i określają zasady postępowania z nimi oraz wprowadzają zakaz manipulacji i usiłowania manipulacji, z którego wynikają jednocześnie zasady postępowania z informacjami mogącymi mieć wpływ dla integralności obrotu (informacje o planowanych zachowaniach na giełdzie, sposobie zabezpieczenia portfela, itd.). Rozwiązaniom tym towarzyszą także obowiązki sprawozdawcze i denuncjacyjne po stronie podmiotów profesjonalnych.

4. Standardy zgodności w zakresie whistleblowingu

Przykładu zbieżności standardów zgodności o charakterze pozaustawodawczym dostarczają np. wspomniana norma ISO dla zwalczania korupcji. Wymaga ona m.in. wprowadzenia mechanizmu anonimowego raportowania nieprawidłowości. Zbieżność ta wykracza resztą poza normy pozaprawne[14]. Systemu whistleblowingu wymagają również m.in.:

- art. 3b ustawy z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym (t.j. Dz.U. 2019, poz. 1871 ze zm.), m.in. wobec

[14] Por. A.-M. Weber-Elżanowska, *Normatywny charakter systemów compliance,* [w:] *Efektywność zarządzania i nadzoru w spółce handlowej. W poszukiwaniu optymalnego modelu ustroju spółki,* red. K. Bilewska, LEX 2018.

funduszy inwestycyjnych, izb rozliczeniowych i rozrachunkowych oraz giełd towarowych i towarowych domów maklerskich, a także niektórych przedsiębiorstw energetycznych;
- art. 9 ust. 1, 2a i 2b ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz.U. 2018, poz. 2187 ze zm.), z którym wiąże się § 45 i n. rozporządzenia Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz.U. 2017, poz. 637);
- art. 53 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz.U. 2019, poz. 1115 ze zm.), z którym wiąże się rozporządzenie Ministra Finansów z dnia 16 maja 2018 r. w sprawie odbierania zgłoszeń naruszeń przepisów z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018, poz. 959).

Ustawą z dnia 16 października 2019 r. o zmianie ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz niektórych innych ustaw (Dz.U. 2019, poz. 2217) rozszerzono krąg podmiotów zobowiązanych do ustanowienia systemu whistleblowingowego o:
- emitentów, na których na mocy art. 97d ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (t.j. Dz.U. 2019, poz. 623 ze zm.) nałożono obowiązek posiadania procedury anonimowego zgłaszania przez pracowników wskazanemu członkowi zarządu, a w szczególnych przypadkach – radzie nadzorczej, naruszeń prawa oraz procedur i standardów etycznych;
- spółki prowadzące rynek regulowany, na które stosownie do art. 25e ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz.U. 2018, poz. 2286 ze zm.) nałożono obowiązek posiadania procedury anonimowego zgłaszania wskazanemu członkowi zarządu, a w szczególnych przypadkach – radzie nadzorczej, naruszeń przepisów prawa oraz procedur i standardów etycznych obowiązujących w spółce prowadzącej rynek regulowany;
- podmioty świadczące usługi w zakresie udostępniania informacji o transakcjach, na które na podstawie art. 131m ww. ustawy o obrocie instrumentami finansowymi nałożono obowiązek posiadania procedury anonimowego zgłaszania wskazanemu członkowi zarządu, a w szczególnych przypadkach – radzie nadzorczej, naruszeń przepisów prawa oraz procedur i standardów etycznych obowiązujących

w podmiocie świadczącym usługi w zakresie udostępniania informacji o transakcjach.

Dodatkowo, obowiązek ustanowienia efektywnego systemu zarządzania ryzykiem braku zgodności wywodzić można z nakazu starannego prowadzenia spraw spółki z uwzględnieniem zawodowego charakteru kierownictwa[15]. Każdorazowo jednak podmiotom gospodarczym pozostawiono szerokie spektrum uznania, pozwalając na dostosowanie mechanizmów przyjmowanych w wykonaniu obowiązku o charakterze formalnym do specyfiki organizacji.

Problem ochrony sygnalistów został odnotowany w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.Urz.UE L 157 z 15 czerwca 2016 r., s. 1-18; dalej: dyrektywa o ochronie tajemnicy przedsiębiorstwa), która zarówno w preambule (np. pkt 20) oraz art. 5 lit. b wyraża dążenie, że środki ogólne, procedury i środki prawne nie powinny ograniczać możliwości sygnalizowania nieprawidłowości – pod warunkiem, że pozwany działał w celu ochrony ogólnego interesu publicznego.

Niebagatelną rolę w upowszechnieniu programów ochrony sygnalistów i samej praktyki whistleblowingu odegra niewątpliwie również dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii (DZ.Urz.UE L 305 z 26 listopada 2019 r., s. 17-56; dalej: dyrektywa o ochronie sygnalistów). Zakres przedmiotowy dyrektywy jest bardzo szeroki i dotyczy naruszeń w takich dziedzinach jak zamówienia publiczne; usługi, produkty i rynki finansowe oraz zapobieganie praniu pieniędzy i finansowaniu terroryzmu; bezpieczeństwo produktów; bezpieczeństwo transportu; ochrona środowiska; ochrona radiologiczna i bezpieczeństwo jądrowe; bezpieczeństwo żywności i pasz, zdrowie i dobrostan zwierząt; zdrowie publiczne; ochrona konsumentów; ochrona prywatności i danych osobowych oraz bezpieczeństwo sieci i systemów informacyjnych, a także naruszeń mających wpływ na interesy finansowe Unii oraz naruszeń dotyczących rynku wewnętrznego, o którym mowa w art. 26 ust. 2 TFUE, w tym naruszeń zasad konkurencji i pomocy państwa.

Zakres podmiotowy dyrektywy o ochronie sygnalistów jest dwoisty, pośród adresatów obowiązków wyróżnić należy podmioty publiczne oraz przedsiębiorstwa. Przedsiębiorstwa kwalifikowane są

[15] U. Schneider, *Compliance als Aufgabe der Unternehmensleitung*, „Zeitschrift für Wirtschaftsrecht und Insolvenzpraxis" 2003, nr 15, s. 645; J. Bürkle, *Compliance als Aufgabe des Vorstands der AG – Die Sicht des LG München I*, „Corporate Compliance Zeitschrift" 2015, nr 2, s. 52-55.

jako zobowiązane do wdrożenia kanałów raportowania nieprawidłowości i prowadzenia postępowań wyjaśniających na podstawie kryterium liczby pracowników oraz wykonywanej działalności. Z wyjątkiem określonych sektorów gospodarki (m.in. instytucji finansowych), obowiązek aktualizuje się wobec przedsiębiorstw zatrudniających przynajmniej 50 osób. Przewidziane jest wyłączenie spod niego małych jednostek samorządu terytorialnego, zatrudniających mniej niż 50 urzędników lub zamieszkałych przez mniej niż 10 000 mieszkańców. Dodatkowo, szeroko zarysowano zakres osób korzystających z ochrony, a także szeroko stypizowano niedozwolone działania odwetowe.

Ochronie podlegają nie tylko pracownicy zatrudnieni na umowę o pracę, lecz także kandydaci do pracy czy osoby zatrudnione w oparciu o umowy cywilnoprawne. Spośród szerokiego katalogu niedozwolonych retorsji, obejmującego m.in. zwolnienie z pracy, nieprzedłużenie zatrudnienia czasowego, pomijanie w ramach podnoszenia kwalifikacji czy przy awansach, wydaje się, że zakres ochrony zależny będzie w praktyce od specyficznych uwarunkowań sygnalisty. Ochrona ma bowiem tutaj wymiar negatywny (obowiązku zaniechania) i nie wymaga ustanowienia pozytywnych zachęt czy preferencji. Ma ona na celu neutralizację ewentualnych negatywnych reakcji poprzez przywrócenie stanu niezakłóconego funkcjonowania, przynajmniej takiego, jakby zgłoszenie nie zostało przez daną osobę dokonane.

Dyrektywa ta wprowadza również gradację trybów sygnalizowania nieprawidłowości, preferując komunikację wewnątrz organizacji, ewentualnie z właściwymi organami władzy, instytucjonalizując jednocześnie jednak, jako subsydiarne i wyjątkowe, lecz w pewnych przypadkach dopuszczalne, ujawnienie publiczne.

Istotną cechą zharmonizowanego systemu whistleblowingu i ochrony sygnalistów w skali wspólnego unijnego rynku jest – obok jego znacznej szerokości i głębokości – położenie nacisku na autonomię decyzyjną przedsiębiorstwa, które w oparciu o charakteryzującą jego działalność ekspozycję na ryzyko, zobowiązane jest wdrożyć odpowiednie mechanizmy, dostosowane do specyfiki jego działalności, oczywiście przy poszanowaniu standardów wynikających z dyrektywy i jej krajowej implementacji. Dyrektywa o ochronie sygnalistów zdaje się przy tym prowadzić do upodmiotowienia jednostek *compliance* jako naturalnych gospodarzy procedur whistleblowingowych.

Powyższe ma dwojakie implikacje. Po pierwsze, wskazuje to na wybór modelu harmonizacji niezupełnej, pozostawiającego margines uznania regulacyjnego państwom członkowskim w miejsce ustanowienie jednolitych rozwiązań w skali całej Unii. Po drugie, system wprowadzony dyrektywą o ochronie sygnalistów zakła-

da dwojakie środki wykonawcze: legislacyjne, stosowane przez państwa członkowskie na etapie wdrażania dyrektywy do krajowego porządku prawnego, i organizacyjne, stosowane przez przedsiębiorstwa. Przynajmniej w niektórych przypadkach będzie to świadczyło o pośrednim oddziaływaniu dyrektywy na stosunki prawne. Na tle wprowadzenia środków organizacyjnych pojawia się wiele pytań.

5. Operacjonalizacja standardów zgodności w zakresie whistleblowingu – problem anonimowości i (dez)anonomizacji

Whistleblowing niemal z definicji wiąże się z anonimowym zgłaszaniem nieprawidłowości, takie też wymogi wynikają zwykle ze standardów zgodności. Dla porządku należy zasygnalizować różnicę między anonimizacją danych osobowych a ich pseudonimizacją. Pierwsze pojęcie zdefiniowano kontekstowo w przepisach o ochronie danych osobowych i uchylonym art. 19 ust. 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną jako „usunięcie oznaczeń identyfikujących osobę". Definicja drugiego z nich wynika m.in. z art. 3 pkt 1 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (t.j. Dz.U. 2018, poz. 484 ze zm.) oraz art. 3 pkt 5 rozporządzenia Parlamentu 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, dalej: RODO; Dz.Urz.UE L 119 z 4 maja 2016, s. 1-88).

W świetle pkt 26 preambuły do RODO „[z]asady ochrony danych nie powinny (...) mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować", natomiast „[s]pseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej". Posiłkowo sięgając do Opinii Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych z dnia 10 kwietnia 2014 r. nr 05/2014 w sprawie technik anonimizacji[16], należy podkreślić, że „pseudonimizacja nie jest metodą anonimizacji. Technika ta ogranicza jedynie możliwość powiązania zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą, i w związ-

[16] https://techinfo.uodo.gov.pl/wp-content/uploads/2018/10/Opinia-5_2014-w-sprawie-technik-anonimizacji-z-dnia-10-kwietnia-2014-r.-wersja-.pdf (dostęp: 15 listopada 2019 r.).

ku z tym jest ona użytecznym środkiem bezpieczeństwa". Efektem procesu anonimizacji jest osiągnięcie stanu anonimowości.

Pojawia się zatem pytanie o wymiar anonimowości zgłoszeń, którą w niniejszym tekście rozróżnić należy ze względu na krąg osób, względem którego zgłoszenie pozostaje anonimowe. Rozgraniczyć należy:

- anonimowość względną, polegającą na tym, że zamieszczone w zgłoszeniu dane zgłaszającego są zastrzeżone do wiadomości wąskiego kręgu osób rozpatrujących zgłoszenie oraz
- anonimowość bezwzględną, która charakteryzować będzie takie zgłoszenia, które nie są opatrzone danymi indywidualizującymi sygnalistę.

W niektórych przypadkach, okoliczności faktyczne mogą sprawić, że zgłoszenia pozbawione imienia, nazwiska, stanowiska pracy i tego rodzaju danych, z uwagi na wąski krąg osób w skali organizacji posiadających wiedzę o danym procederze, będzie wskazywało na osobę whistleblowera. Wydaje się jednak, że zgłaszający musi godzić się z tym przy dokonywaniu zgłoszenia. Należy przy tym chronić tożsamość zgłaszającego, podobnie jak na ochronę zasługuje tożsamość osoby, której zgłoszenie dotyczy oraz innych osób pojawiających się w zgłoszeniu (por. pkt 76 preambuły do dyrektywy o ochronie sygnalistów).

Dodatkowo, pojawia się pytanie o możliwość następczej (dez)anonimizacji zgłoszenia. Chodzi w szczególności o przypadek, w którym sygnalista dokonuje zgłoszenia bez podawania swoich danych osobowych, jednak opatruje je indywidualizującym oznaczeniem niezawierającym danych osobowych, kodem, znanym wyłącznie jemu. Kod taki powinien być odpowiednio długim ciągiem znaków, zawierającym litery i cyfry, aby z racji liczby możliwych kombinacji zminimalizować ryzyko odgadnięcia go przez osoby postronne. Wydaje się, że mechanizm ten możliwy jest do zastosowania zwłaszcza w odniesieniu do zgłoszeń dokonywanych online, z których każde otrzymywałoby po złożeniu indywidualny numer. Ewentualny kod nie musiałby być przekazywany do jednostki *compliance*, rozpatrującej zgłoszenie, a jedynie służyć do autentykacji whistleblowera, który zdecyduje się na przejście z poziomu anonimizacji bezwzględnej na poziom anonimizacji względnej lub całkowitej dezanonimizacji. Takie – nieodwracalne i dobrowolne – zdezanonimozowanie z inicjatywy sygnalisty mogłoby prowadzić do przekształcenia się zgłoszenia pierwotnie anonimowego w następczo spseudonimizowane. O dylemacie dezanonimizacji niedobrowolnej wzmianka znajdzie się w dalszej części tekstu.

W powyższych rozważaniach nieuchronnie pojawił się problem kanału raportowania nadużyć. Dla porządku należy wskazać na następujące możliwości przekazania zgłoszeń:

- zgłoszenia w formie pisemnej, przesyłane listownie na adres jednostki *compliance*, podany do wiadomości na stronie internetowej przedsiębiorstwa, przy czym warto uwrażliwić nadawców, aby zgłoszenia zamieszczać w dwóch kopertach, drugą (wewnętrzną) adresując imiennie do osoby dokonującej wstępnej kontroli zgłoszeń lub do jednostki *compliance* oraz wyraźnie opatrując adnotacją „do rąk własnych", aby pracownicy wewnętrznych służb doręczeniowych, biura podawczego czy sekretariatu nie uzyskali przypadkowo wglądu do potencjalnie wrażliwych treści;
- zgłoszenia w formie pisemnej, składane do przeznaczonych w tym celu nieprzezroczystych skrzynek oddawczych, zlokalizowanych w miejscach, do których dostęp nie wymaga wylegitymowania się czy odbicia przepustki lub które nie są nagrywane przy pomoc kamer przemysłowych;
- zgłoszenie w formie elektronicznej, przy pomocy wiadomości e-mail na przeznaczoną do tego skrzynkę funkcyjną bądź z wykorzystaniem dedykowanej funkcjonalności;
- zgłoszenia telefoniczne, za pośrednictwem „gorącej linii", dostępnej w określone dni tygodnia w określonych godzinach, z wyłączoną identyfikacją numeru dzwoniącego (połączeń przychodzących); zgodnie z art. 18 ust. 2 dyrektywy o ochronie sygnalistów nagranie rozmowy lub jej dokładna transkrypcja wymagają zgody sygnalisty, któremu na żądanie należy umożliwić zweryfikowanie transkrypcji i potwierdzenie poprawności poprzez jej podpisanie;
- za pomocą bezpośredniego spotkania zorganizowanego w rozsądnym terminie, zgodnie z art. 9 ust. 2 *in fine* dyrektywy o ochronie sygnalistów; zalecane jest przestrzeganie przy spotkaniu zasady dwóch par oczy i udokumentowanie przebiegu spotkania oraz umożliwienie sygnaliście potwierdzenia protokołu swoim podpisem.

W dobie rozwoju nowoczesnych technologii najbardziej celowe wydaje się elektroniczne przyjmowanie zgłoszeń z wykorzystaniem dedykowanej funkcjonalności. Ich niewątpliwą zaletę stanowi automatycznie generowane potwierdzenie wpływu zgłoszenia, możliwość nadania mu numeru, co realizuje jeden z wymogów wynikających z dyrektywy o ochronie sygnalistów. Dodatkowo, pozwala to sygnaliście na tzw. *tracking* – śledzenie dalszego toku zgłoszenia, w szczególności pod kątem podjęcia czynności w przewidzianym terminie (przeszkoda przed tzw. ujawnieniem publicznym), a w pewnych przypadkach – na dezanonimizację zgłoszenia przez whistleblowera. Na rynku istnieją wyspecjalizowane podmioty oferujące software przygotowany na potrzeby obsługi zgłoszeń whistleblowingowych. Ich usługi uzupełnia oferta kancelarii

prawnych, które na zlecenie podmiotu, którego zgłoszenie dotyczy, dokonują weryfikacji dokonanych zgłoszeń.

W przypadku podmiotów funkcjonujących w warunkach grup kapitałowych celowe może być ustanowienie jednolitego kanału zgłoszeń dla całego holdingu, zwłaszcza jeżeli za sprawą komunikacji marketingowej, stosowanych znaków towarowych i innych środków identyfikacji wizualnej, podmioty z danej grupy kapitałowej nie są odróżnialne od siebie w oczach interesariuszy zewnętrznych, a nie ma przeciwwskazań prawnych (np. naruszenie przejrzystości i integralności przetargów, obrotu giełdowego lub wymogów rozdziału określonych rodzajów działalności od siebie) lub organizacyjnych (np. funkcjonowanie na rozproszonych geograficznie rynkach pośród wielojęzycznej klienteli) do ujednolicenia systemu whistleblowingowego. Takie rozwiązanie może też pozwolić za zacieśnienie nadzoru właścicielskiego.

Niejasny jest w tym kontekście art. 8 ust. 6 dyrektywy o ochronie sygnalistów, który dopuszcza, aby przedsiębiorstwa zatrudniające od 50 do 249 pracowników dzieliły się zasobami w zakresie przyjmowania zgłoszeń i wszelkich prowadzonych postępowań wyjaśniających. Przepis ten nie powinien być interpretowany jako wymóg internalizacji procesu obsługi zgłoszeń przez duże przedsiębiorstwa lub zakaz korzystania przez nie ze wspólnych zasobów z innymi podmiotami, na co wyraźnie wskazuje wcześniejszy ustęp tego przepisu, dopuszczający, aby kanały dokonywania zgłoszeń były zapewniane zewnętrznie przez osobę trzecią. Taką osobą trzecią może być w szczególności jednostka powiązana. Jego celem jest ustanowienie nienaruszalnych minimalnych gwarancji redukcji uciążliwości związanych z funkcjonowaniem systemu raportowania nieprawidłowości dla małych i średnich przedsiębiorstw.

Istotne kwestie, na które warto zwrócić uwagę przy podejmowaniu decyzji o wyborze gotowej funkcjonalności lub stworzeniu własnego kanału elektronicznego raportowania nieprawidłowości, obejmują:

- miejsce przechowywania przekazanych zgłoszeń, tzn. czy dostawca zewnętrzny udostępnia do tego swoje serwery, czy też zgłoszenia przechowywane są na serwerach przedsiębiorstwa lub wskazanego podmiotu trzeciego;
- zakres przewidzianego wglądu i możliwej ingerencji ze strony przedsiębiorstwa w dokonane zgłoszenia, w szczególności możliwość usunięcia zgłoszenia, poznania numeru IP komputera, z którego nadesłano zgłoszenie, itd.;
- powierzenie obsługi zgłoszeń podmiotowi trzeciemu oraz zakres ewentualnego outsourcingu.

Do czynników determinujących decyzję co do kształtu elektronicznego kanału zgłaszania nieprawidłowości zaliczyć należy

w pierwszej kolejności ochronę informacji. Dotyczy to w pierwszym rzędzie jakości ochrony przetwarzanych informacji przed bezprawnym ujawnieniem. Z perspektywy prawnej powierzenie obsługi zgłoszeń zewnętrznemu doradcy prawnemu, wykonującemu zawód adwokata lub radcy prawnego, zapewnia szeroki komfort przed ujawnieniem takich zgłoszeń zarówno wobec osób postronnych, jak i organów władzy. Możliwość tego rodzaju outsourcingu nie budzi wątpliwości na gruncie dyrektywy o ochronie sygnalistów (por. pkt 54 preambuły).

Tajemnica radcowska lub adwokacka stanowi prawnie doniosłą przeszkodę do ujawnienia informacji na żądanie organów władzy. Nie jest możliwe zwolnienie z niej w ramach postępowań cywilnych czy administracyjnych, w ramach których tajemnica zawodowa prawników zewnętrznych respektowana jest także przez Komisję Europejską jako organ ochrony konkurencji[17]. Dość przypomnieć, że na gruncie postępowania karnego tajemnica ta również podlega ochronie. Ewentualna dopuszczalność zwolnienia wykwalifikowanego prawnika w warunkach procesu karnego z obowiązku zachowania tajemnicy jest przedmiotem kontrowersji z perspektywy przepisów o ustroju adwokatury i zawodzie radcy prawnego, których roztrząsanie wykracza poza ramy niniejszego tekstu. Niewątpliwie istotnym ograniczeniem w dostępie do informacji chronionych tajemnicą radcowską lub adwokacką ze strony organów władzy towarzyszy jednocześnie wielowymiarowa ochrona przed nieuprawnionym udostępnieniem osobom trzecim czy też wyciekiem, w szczególności do środków masowego przekazu. Ochrona przed ujawnieniem następuje również – a może przede wszystkim – w sferze pozaprawnej, przykładowo poprzez wybór umiejscowienia informacji na określonych serwerach.

6. Operacjonalizacja standardów zgodności w zakresie whistleblowingu – podmiotowo-przedmiotowe ograniczenia dotyczące whistleblowera

Wątpliwości dotyczą także podmiotowo-przedmiotowej kwalifikacji osoby sygnalisty. Pierwsza dotyczy możliwości do-

[17] Por. I. Małobęcka-Szwast, *Compliance w zakresie prawa ochrony konkurencji jako wyzwanie dla organów spółki*, „Monitor Prawa Handlowego" 2018, nr 3, s. 25-32; M. Gac, *Programy zgodności z prawem konkurencji – efektywny mechanizm w tworzeniu europejskiej kultury compliance?*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2012, nr 2, s. 57-71. Na temat ochrony tajemnicy zawodowej (*legal professional privilege*) w sprawach z zakresu ochrony konkurencji zob. zwłaszcza B. Turno, A. Zawłocka-Turno, *Legal Professional Privilege and the Privilege Against Self-Incrimination in EU Competition Law after the Lisbon Treaty – Is It Time for a Substantial Change?*, „Yearbook of Antitrust and Regulatory Studies" 2012, nr 5 (6), s. 193-214; B. Turno, *Zagadnienie tajemnicy adwokackiej na gruncie prawa konkurencji*, [w:] *Aktualne problemy polskiego i europejskiego prawa ochrony konkurencji*, red. C. Banasiński, M. Kępiński, B. Popowska, T. Rabska, Warszawa 2006, s. 172-189; M. Bernatt, *Sprawiedliwość proceduralna w postępowaniu przed organem ochrony konkurencji*, Warszawa 2011, s. 229-235.

konywania zgłoszeń przez interesariuszy zewnętrznych. Zapewnienie takiej możliwości, zarówno z uwagi na uwarunkowania prawne, jak i względy celowości, nie powinno być kwestionowane, chociaż zwłaszcza w mniej dojrzałej fazie funkcjonowania systemu whistleblowingowego można liczyć się z napływem zgłoszeń o formie lub treści sprzecznej z przeznaczeniem takiego mechanizmu, w podobny sposób, w jaki wnoszeniu powództw towarzyszy element tzw. pieniactwa procesowego, nieobcy również tzw. skargom powszechnym, przewidzianym w dziale VIII Kodeksu postępowania administracyjnego, zatytułowanym „Skargi i wnioski".

Druga wątpliwość wiąże się z kręgiem interesariuszy wewnętrznych mogących dokonywać zgłoszeń. Niedopuszczalne wydaje się uzyskanie statusu sygnalisty przez członka wyższej kadry menedżerskiej, zwłaszcza w zakresie powierzonych mu do prowadzenia spraw (działalności kierowanej przez niego jednostki organizacyjnej). Odmienne podejście mogłoby prowadzić do czerpania przez dyrektora jednostki swoistych korzyści, wynikających z ochrony dla sygnalistów, ze sprzecznych ze standardami zgodności zachowań jego lub podległych mu pracowników. Jakkolwiek w pewnych przypadkach celowe może być zachęcanie pracowników do ujawnienia własnych nieumyślnych naruszeń, z rezerwą należy się odnieść do ochrony płynącej z dokonania zgłoszenia, które dotyczy zachowania samego zgłaszającego (por. pkt 9 dyrektywy o ochronie sygnalistów).

Niecelowe byłoby też traktowanie pracownika jednostki *compliance* lub audytu jako sygnalistę, bez uszczerbku jednakże dla gwarancji poszanowania ich niezależności, które jednak w większym stopniu powinny być nastawione na systemowe rozwiązania, a nie incydentalnie nabywane uprawnienia. Omówienie ich wykracza poza ramy niniejszego opracowania. Ze względu na m.in. deontologię zawodową, z bardzo dużą dozą ostrożności należy podejść do prób wcielenia się prawników wewnętrznych w rolę sygnalistów (por. postanowienie Sądu Najwyższego z 21 maja 2019 r., II DSI 66/18). Podobnie ostrożne podejście rozciąga się na lekarzy i personel medyczny (por. pkt 26 preambuły do dyrektywy o ochronie sygnalistów).

Trzecia wątpliwość daje się z kolei zawrzeć w pytaniu, czy zgłaszając naruszenie pracownicze, pracownik może stać się whistleblowerem, i czy przejawy aktywności w związku zawodowym pozwalają na nabycie takiego statusu. W praktyce, co zwłaszcza istotne dla oceny zgłoszeń dotyczących własnych prac zgłaszających, niekiedy oddziela się materię, która może być przedmiotem zgłoszeń nieprawidłowości (whistleblowingu) od tzw. *employment grievance*, obejmujących różnej natury roszczenia pracow-

nicze. Przykładu takiego podejścia dostarcza praktyka brytyjska[18]. Żądania dotyczące warunków zatrudnienia (pracy i płacy) nie powinny być przedmiotem zgłoszeń, gdyż dotyczą one nie tyle nieprawidłowości, co postulatów, względnie źródeł niezadowolenia załogi i – o ile nie powinny być bagatelizowane w dialogu społecznym – o tyle właściwym forum to ich załatwienia są w szczególności kolektywne regulacje podjęte w szczególności z udziałem organizacji związkowych reprezentujących pracowników wobec pracodawców. Nie powinny być one utożsamiane z whistleblowingiem, podobnie jak wystąpienia związków zawodowych do Państwowej Inspekcji Pracy nie powinny być rozpatrywane w tych kategoriach. Działacze związkowi korzystają bowiem ze szczególnego reżimu ochrony. Zbiorowe stosunki pracy powinny, ze względów przejrzystości, pozostać poza sferą whistleblowingu. Odnotować należy przy tym, że w uzasadnieniu do dyrektywy o ochronie sygnalistów wskazano, że „związki zawodowe mogą pełnić funkcję organów przyjmujących zgłoszenia sygnalistów lub informacje przez nich ujawniane i mają do odegrania kluczową rolę w udzielaniu porad i wsparcia (potencjalnym) sygnalistom"[19]. Umiejscowienie jednostki odpowiedzialnej za zgłoszenia nieprawidłowości w strukturze związku zawodowego, a zatem odrębnej od pracodawcy osoby prawnej, mającej nie zawsze zbieżne z nim dążenia, nie wydaje się rekomendowane i nie odpowiada uwagom na temat systemu zarządzania ryzykiem braku zgodności, poczynionym we wcześniejszej części tekstu.

W zgłoszeniach dotyczących pojedynczych naruszeń własnych praw pracowniczych (np. wątpliwości dotyczącej wysokości premii lub nagrody, żądania uregulowania roszczeń z tytułu godzin nadliczbowych), które oczywiście nie powinny prowadzić do retorsji ze strony zatrudniającego, interes prywatny zdaje się przeważać nad publicznym w stopniu, który uzasadnia nieobjęcie tego rodzaju sytuacji programami ochrony dla sygnalistów.

Odmiennie wydają się prezentować zgłoszenia nadużyć typu mobbing, molestowanie (zwłaszcza molestowanie seksualne) lub dyskryminacja. Wynika to zwłaszcza z ich szczególnie wrażliwej materii, dotykającej życia intymnego pracownika lub przekładającej się na jego kondycję psychosomatyczną, społeczne odium niektórych sytuacji bądź przynależność do klasy chronionej, a także z osobistej dolegliwości procederu i ryzyka wtórnej wiktymizacji w toku postępowania dotyczącego nadużycia, czy to wewnątrzkorporacyj-

[18] https://www.gov.uk/whistleblowing (dostęp: 15 listopada 2019 r.); https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415175/bis-15-200-whistleblowing-guidance-for-employers-and-code-of-practice.pdf (dostęp: 15 listopada 2019 r.).

[19] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018PC0218&from=EN (dostęp: 15 listopada 2019 r.).

nego, czy też prowadzonego przez organ publiczny. Za celowe należy uznać objęcie takich zgłoszeń ochroną przewidzianą dla sygnalisty i traktowanie ich jako integralnej części whistleblowingu, przynajmniej w zakresie, w jakim obnażają one systemowe dysfunkcje, dotyczą większej liczby pracowników lub nie odnoszą się wyłącznie do osoby zgłaszającej.

7. Operacjonalizacja standardów zgodności w zakresie whistleblowingu – wybrane uwagi dotyczące postępowania ze zgłoszeniem

Wspomniany wcześniej model systemu zarządzania ryzykiem braku zgodności będzie miał swoje implikacje również z perspektywy obsługi zgłoszeń. O ile celowe jest skierowanie wszystkich zgłoszeń w jedno miejsce, do komórki organizacyjnej odpowiedzialnej za *compliance*, o tyle dalsze rozpatrywanie zgłoszeń może wykracza poza kompetencje takiej jednostki. Materia zgłoszeń, zwłaszcza w przedsiębiorstwie prowadzącym działalność w wielu sektorach gospodarki, cechować będzie się w praktyce złożonością i różnicowaniem wymagającym zaangażowania specjalistów z innych obszarów. Wsparcie to może dotyczyć zarówno pomocy w zbadaniu stanu faktycznego (np. przeprowadzenie audytu, skorzystanie z funkcji *forensic*), jak i merytorycznej pomocy w poszczególnych dziedzinach (np. z zakresu rachunkowości, prawa konkurencji czy przeciwdziałania korupcji). Naturalnymi partnerami dla jednostki *compliance* będą wówczas ustanowieni w organizacji pracownicy odpowiedzialni za zarządzanie ryzykiem braku zgodności w obszarach mających znaczenie dla sprawy.

Formuła współpracy będzie determinowana m.in. kulturą organizacyjną i zwyczajami panującymi w przedsiębiorstwie, a nawiązywać może do spotykanych w praktyce gremiów, wzorowanych na komitetach kredytowych czy inwestycyjnych bądź komisjach antymobbingowych. W zależności od rangi problemu oraz skutków naruszenia, rekomendacje mogą wymagać eskalowania na poziom zarządu przedsiębiorstwa. Aby nie zaburzyć proporcji raportowania zarządczego oraz uniknąć uśpienia czujności najwyższego szczebla kierownictwa organizacji, celowe wydaje się ustanowienie progu *de minimis* dla spraw załatwianych bez udziału zarządu, jeżeli możliwe jest wypracowanie konsensusu na niższym szczeblu. Specyficzna sytuacja dotyczyć będzie nieprawidłowości w funkcjonowaniu komórki merytorycznej, która w normalnym toku czynności udzielałaby wsparcia komórce *compliance*, kiedy to potencjalnie konieczne okaże się pozyskanie określonych kompetencji poza organizacją. Omówienie szczegółowego toku załatwienia sprawy oraz raportowania wyników (jednostkowych oraz zbiorczych, w tym komunikacji

z radą nadzorczą i komitetem audytu) wykracza poza ramy niniejszego opracowania.

Warto jednak sygnalizować jedno z istotnych ograniczeń prawnych. Wyobrażalną rekomendacją, w razie potwierdzenia się zgłoszenia nieprawidłowości, może być dyscyplinarne zwolnienie odpowiedzialnych za nadużycie pracowników, tzn. rozwiązanie umów o pracę bez wypowiedzenia. Zgodnie z art. 52 § 2 k.p. rozwiązanie umowy o pracę w takim trybie nie może nastąpić po upływie miesiąca od uzyskania przez pracodawcę wiadomości o okoliczności uzasadniającej rozwiązanie umowy. W orzecznictwie ukształtował się wyważony, choć dość korzystny dla przedsiębiorców, pogląd dotyczący rozpoczęcia biegu miesięcznego terminu. W szczególności należy zwrócić uwagę na wyrok SN z 6 grudnia 2018 r., II PK 233/17, zgodnie z którym „[b]ieg miesięcznego terminu określonego art. 52 § 2 k.p. rozpoczyna się dopiero od chwili, w której pracodawca uzyskał w dostatecznym stopniu wiarygodne informacje uzasadniające jego przekonanie, że pracownik dopuścił się czynu nagannego w stopniu usprawiedliwiającym niezwłoczne rozwiązanie z nim umowy o pracę, czyli od zakończenia – podjętego niezwłocznie i sprawnie przeprowadzonego – wewnętrznego postępowania sprawdzającego uzyskanie przez pracodawcę wiadomości o niewłaściwym zachowaniu pracownika. W razie trwałego naruszania obowiązków pracowniczych, termin z art. 52 § 2 k.p. rozpoczyna bieg dopiero od ostatniego ze zdarzeń składających się na to zachowanie. Przez trwałe naruszenie obowiązków rozumie się przy tym zachowanie o charakterze ciągłym, to jest zachowanie polegające na wykorzystywaniu tej samej sposobności, jednorodzajowe i mieszczące się w zwartym odcinku czasu". Wielokrotnie akcentowano, że chodzi tutaj o faktyczne powzięcie informacji przez pracodawcę (zob. wyrok SN z 10 maja 2018 r., II PK 76/17): „Termin rozwiązania umowy o pracę bez wypowiedzenia z winy pracownika (...) rozpoczyna bieg od faktycznego uzyskania przez pracodawcę wiadomości o ciężkim naruszeniu przez pracownika jego podstawowych obowiązków (np. od dnia sprawdzenia treści wiadomości wysłanych ze służbowego adresu poczty elektronicznej (...)), a nie od dnia, w którym pracodawca mógł taką wiadomość powziąć (np. od dnia, kiedy służby informatyczne pracodawcy dysponowały możliwością weryfikacji treści wysłanych wiadomości elektronicznych)". Jednocześnie zwrócono uwagę na potrzebę dołożenia staranności w przeprowadzeniu postępowania wewnątrzkorporacyjnego, nie tylko pod względem jego wnikliwości, lecz także szybkości (zob. wyrok SN z 22 marca 2016 r., II PK 37/15): „[pracodawca powinien podejmować] decyzję, która (...) musi być poprzedzona uzyskaniem wiadomości dostatecznie sprawdzonych. (...) Z drugiej strony nie powinno być zwłoki w sprawdzeniu tych in-

formacji. (...) Bieg terminu liczy się od zakończenia procesu sprawdzającego wiadomość. Gdy pracodawca ma możliwość sprawdzenia informacji o niewłaściwym postępowaniu pracownika, a tego nie czyni, to termin rozpoczyna bieg od powstania możliwości sprawdzenia informacji"). Powyższe oznacza, że wypracowanie i wdrożenie rekomendacji obejmujących zwolnienie pracownika w trybie dyscyplinarnym winno nastąpić w przeciągu miesiącu od ustalenia okoliczności naruszenia. Termin miesięczny nie służy limitowaniu czasu trwania samego postępowania wyjaśniającego (audytu)[20]. Ograniczenia w tym zakresie wynikają z art. 11 ust. 2 lit. d dyrektywy o ochronie sygnalistów, który wprowadza termin trzymiesięczny z możliwością przedłużenia do pół roku.

8. Potrzeba holistycznego *compliance* – wybrane kontrowersje funkcjonowania systemu whistleblowingowego w organizacji

Jak wspomniano wcześniej, system zarządzania ryzykiem braku zgodności wymaga, dla swojej spójności i odpowiedniej recepcji w organizacji, oparcia na kierunkowym dokumencie w postaci kodeksu etyki lub podobnym *compliance statement*. System whistleblowingowy stanowi jedno z narzędzi takiego systemu, źródło informacji o okolicznościach wymagających zainteresowania osób odpowiedzialnych za *compliance*. Tym bardziej rozważania o mechanizmach zgłaszania nieprawidłowości i programach ochrony sygnalistów wymagają refleksji o sytuacjach, w których pojawić mogą się wątpliwości natury aksjologicznej bądź kolizje porządków normatywnych.

W odniesieniu do zgłoszeń pochodzących od niektórych kategorii osób bądź dotyczących niektórych kwestii przedstawiono powyżej wątpliwości co do ich podleganiu programowi ochrony sygnalistów. Przypadków takich w rzeczywistości będzie znaczenie więcej. Dyskwalifikujące dla sygnalisty jest dokonanie zgłoszenia w złej wierze. Jak zauważono w piśmiennictwie, „Doceniając znaczenie *whistleblowing* jako systemu wczesnego ostrzegania o nieprawidłowościach w firmie należy podkreślić, że ochronie prawnej powinien podlegać jedynie pracownik działający w dobrej wierze i dysponujący informacjami, które uwiarygodniają, że wysuwane wobec pracodawcy zarzuty są prawdziwe. System działań, o którym mowa, polega bowiem na ujawnianiu faktów, a nie na szkalowaniu podmiotu zatrudniającego. Dlatego też projektując stosowne regulacje prawne należy dążyć nie tylko do ochrony wskazanej wyżej ka-

[20] Por. „Miesięczny termin z art. 52 § 2 k.p. nie jest przeznaczony na ustalanie przez pracodawcę, czy pracownik dopuścił się określonego czynu oraz jaki jest stopień jego naganności, lecz ma służyć zastanowieniu się i podjęciu decyzji przez pracodawcę, który wie, że określony czyn został popełniony oraz jakie są towarzyszące mu okoliczności" za: R. Sadlik, *Miesięczny termin na rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika*, „Służba Pracownicza" 2014, nr 5, s. 14-16.

tegorii pracowników, ale także uwzględnić ochronę interesu pracodawcy przed ujawnieniami w złej wierze"[21].

Niewątpliwie taka sytuacja mieć będzie miejsce, jeżeli sygnalista umyślnie zawarł w zgłoszeniu informacje nieprawdziwe, tzn. miał świadomość rozbieżności między treściami zawartymi w zgłoszeniu a stanem rzeczywistym. Doniosłe wydają się przy tym jedynie rozbieżności co do faktów, a nie ich ocen, w tym kwalifikacji prawnych. Zgłaszający nie dość, że nie będzie mógł wówczas korzystać z ochrony, to może narazić się na konsekwencje, które żadną miarą nie będą stanowić działań odwetowych, zakazanych na mocy art. 19 dyrektywy o ochronie sygnalistów (por. pkt 103 preambuły do dyrektywy). Należy jednak pamiętać o wynikającym z art. 7 k.c. domniemaniu dobrej wiary, które znajdzie zastosowanie również w stosunkach pracowniczych (art. 300 k.p.).

Bardziej problematyczne wydaje się nieujawnienie przez whistleblowera istotnych faktów. Za naganne uznać należy z pewnością przypadki, w których zaniechanie ujawnienia okoliczności było instrumentalnie nastawione na uzyskanie korzyści, czy to poprzez oddalenie podejrzeń od zgłaszającego, czy to skierowanie ich na osobę niewinną, np. potencjalnego konkurenta w walce o awans. Dodatkowo, pojawia się kwestia standardu staranności oczekiwanego od sygnalisty, tj. czy do stwierdzenia złej wiary wystarczy, że przy dołożeniu należytej staranności mógł on dowiedzieć się o odmiennym stanie rzeczywistym niż przedstawiony przez niego w zgłoszeniu, czy raczej z łatwością mógł to ustalić, a może też konieczne jest stwierdzenie, że miał świadomość istnienia rozbieżności. Wydaje się, że w razie wykazania przez przedsiębiorstwo, że zgłaszający z łatwością mógł się dowiedzieć, że jego zgłoszenie jest błędne lub wprowadzające w błąd, można uznać, że dokonano go w złej wierze; formułowanie wobec zgłaszającego wyższych oczekiwań prowadziłoby do podważeniu celu mechanizmu i późniejszego postępowania wyjaśniającego.

Za nadużycie mechanizmów zgłaszania nieprawidłowości, uzasadniające odmowę skorzystania z przewidzianej dla whistleblowerów ochrony, należałoby uznać również zgłoszenie „przeleżałej" nieprawidłowości lub zgłoszenie dokonane w celu uzyskania korzyści innej niż wynikająca z programu ochrony sygnalistów (równoważącej trudności związane ze zgłoszeniem), zwłaszcza zbudowania kapitału politycznego, wykorzystania swojego zgłoszenia w grze politycznej lub walce o wpływy korporacyjne.

W pierwszym przypadku, aby uniknąć zgłoszeń nastawionych wyłącznie na oddalenie groźby zwolnienia z pracy, celowe wydaje się wprowadzenie odpowiedniego terminu na dokonanie zgłoszeń

[21] W. Koczur, *Tajemnica pracodawcy (zakładowa)*, „Monitor Prawniczy" 2015, nr 7, s. 390.

od dnia wprowadzenia systemu whistleblowingowego w organizacji, a po jego wdrożeniu dopuszczanie zgłoszeń jedynie w określonym terminie od dnia zdarzenia oraz powzięcia przez pracownika wiedzy o nieprawidłowości. Tego rodzaju mechanizmom dyscyplinującym może towarzyszyć także składanie przez pracowników, zwłaszcza średniego i wyższego szczebla kadry menedżerskiej, okresowych oświadczeń o wystąpieniu określonego rodzaju nieprawidłowości. Oświadczenia takie, choć nie będą w realiach procesu sądowego zastępować dowodu z zeznań świadka, mogą być pomocne w kwestionowaniu ich wiarygodności, w razie niedającej się rozsądnie wyjaśnić rozbieżności między treścią oświadczenia pochodzącego z okresu zatrudnienia a złożonego po jego zakończeniu. Trudności czasowe obecne będą przynajmniej jeszcze w przynajmniej jednym przypadku. Wyobrażalne jest bowiem podjęcie decyzji o zwolnieniu pracownika przed dokonaniem przez niego zgłoszenia, przy czym doręczenie oświadczenia przez pracodawcę nastąpi po zaraportowaniu nieprawidłowości. Swoista luka może wynikać przykładowo z oczekiwania na konsultację zwolnienia danego zatrudnionego z organizacją związkową czy uzyskania zgody ze strony organu stanowiącego samorządu terytorialnego (w przypadku pracownika łączącego zatrudnienie z mandatem radnego).

Dla uniknięcia nieporozumień należy rozgraniczyć zwolnienia z pracy dokonane jako środki odwetowe, od takich, które znajdują merytoryczne uzasadnienie. Ochrona przewidziana dla sygnalistów nie ma bowiem charakteru bezwzględnego i skorzystanie z niej wymaga istnienia związku między dokonanym zgłoszeniem a określonym zachowaniem pracodawcy, przy czym związek ten wykazywalny jest także przy pomocy poszlak (domniemań faktycznych), a wykazanie odpowiednich podstaw do zakończenia zatrudnienia sygnalisty obciąża pracodawcę. Przykładowo, za zasadniczo dopuszczalne uznać należy przeprowadzenie zwolnień, którymi objęty zostałby whistleblower, w następstwie restrukturyzacji, zwłaszcza w związku ze zmianą przedmiotu lub skali działalności przedsiębiorstwa bądź jego modernizacją. Otwartą kwestią pozostaje umożliwienia sygnaliście przekwalifikowania lub przeprowadzenia outplacementu. Wydaje się to celowe w okresie krótko po zgłoszeniu lub wdrożeniu rekomendacji w następstwie postępowania wyjaśniającego, kiedy świadomość zaistniałej sytuacji na ryku pracy pozostaje stosunkowo „świeża". Nie należy też utożsamiać ze środkami odwetowym samodzielnej decyzji pracownika o rezygnacji z pracy lub zmianie miejsca jej świadczenia (przejście do innej jednostki organizacyjnej).

Problem whistleblowingu do mediów, mogącego być narzędziem zyskania popularności sygnalisty, staje się jeszcze bardziej realny w świetle dyrektywy o ochronie sygnalistów. Pomimo gradacji kana-

łów whistleblowingu nie jest wykluczone, że informacje o nieprawidłowościach trafią do środków masowego przekazu, także w zakresie dotyczącym przedsiębiorców. Co więcej, dyrektywa o ochronie sygnalistów zdaje się ograniczać możliwość uwzględniania motywacji sygnalisty przy rozpatrywaniu jego zgłoszenia w kategoriach nadużycia, wskazując w pkt 33 preambuły, że motywy osób dokonujących zgłoszenia, jakimi kierują się dokonując zgłoszenia, nie powinny mieć znaczenia przy podejmowaniu decyzji, czy powinny one otrzymać ochronę.

W tym kontekście należy pamiętać, że treść zgłoszeń obejmować będzie informacje prawnie chronione o różnym stopniu wrażliwości[22]. Tak długo, jak komunikacja ma charakter wewnątrzkorporacyjny lub kierowana jest do organu władzy, sytuacja jest nieco mniej problematyczna; w pierwszym przypadku przedsiębiorca ma instrumenty oraz (wynikający z dyrektywy o ochronie sygnalistów) obowiązek zapewnienia poufności zgłoszeń; na urzędnikach spoczywa natomiast obowiązek zachowania w poufności informacji, w posiadanie których weszli przy wykonywaniu funkcji publicznych, przy czym w zależności od organu i materii możemy mieć do czynienia z różnym reżimem prawnym (np. art. 24 ust. 2 pkt 4 ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych, t.j. Dz.U. 2019, poz. 1282; art. 17 ust. 2 pkt 5 ustawy z dnia 16 września 1982 r. o pracownikach urzędów państwowych, t.j. Dz.U. 2018, poz. 1915 ze zm.).

Niewątpliwie system whistleblowingowy nie ma na celu ujawnienia tajemnicy adwokackiej (radcowskiej, rzeczni-kowskiej, doradcy podatkowego) czy medycznej (art. 3 ust. 3 lit. b dyrektywy o ochronie sygnalistów). Niefrasobliwością byłoby również zawarcie w zgłoszeniu informacji niejawnych. Dyrektywa o ochronie sygnalistów nie ingeruje w kwestie bezpieczeństwa i obronności. Obieg informacji niejawnych winien następować zgodnie z obowiązującymi procedurami, dostosowanymi do klasy dokumentu, a zapewniana w ten sposób ochrona interesów państwa winna w razie potrzeby przeważyć nad zgłaszaniem nieprawidłowości. Dość przypomnieć, że nawet w procesie karnym przed organami państwowymi dokumenty niejawne przechowywane są w kancelarii tajnej, a dostęp do nich jest ograniczony, co ma swoje konsekwencje m.in. przy przeglądaniu akt i redagowaniu pism procesowych. Nie wydaje się jednocześnie, aby tego rodzaju przypadki miały istotne znaczenie dla rzeczywistości gospodarczej.

Dużo istotniejszą dla biznesu kategorią informacji prawnie chronionych jest tajemnica przedsiębiorstwa. Dyrektywa o ochronie sygnalistów koresponduje w tym zakresie z dyrektywą o ochronie

[22] Por. M. Derlacz-Wawrowska, *Whistleblowing a ochrona informacji poufnych pracodawcy,* [w:] *Prawo pracy. Refleksje i poszukiwania. Księga Jubileuszowa Profesora Jerzego Wratnego*, red. G. Uścińska, Warszawa 2013, s. 390 i n.

tajemnicy przedsiębiorstwa w ten sposób, że dopuszcza ujawnienie tajemnicy przedsiębiorstwa, traktując to jednak jako *ultima ratio* (por. pkt 36 i pkt 98 dyrektywy o ochronie sygnalistów). Ponownie najbardziej problematyczne będą tu przypadki ujawnienia publicznego.

Funkcjonowaniu systemu whistleblowingowego towarzyszy nieuchronnie przetwarzanie danych osobowych. Dyrektywa o ochronie sygnalistów odnosi się do tej materii w kilku miejscach, w szczególności umożliwiając ograniczenie – w drodze aktów prawnych – wykonywania niektórych praw do ochrony danych osobowych osób, których dotyczy zgłoszenie (por. pkt 84 preambuły) oraz odsyłając w art. 17 do generalnych zasad przetwarzania danych osobowych. Obszerne omówienie różnicowanych aspektów ochrony danych osobowych w kontekście whistleblowingu wymaga z pewnością odrębnego pogłębionego opracowania. Wypada jednak zwrócić uwagę na taki sposób wykonywania obowiązków wynikających z RODO, aby nie podważyły one fundamentów funkcjonowania systemu whistleblowingowego. Wśród postulatów w tym zakresie należy wymienić następujące. O ile nie mamy do czynienia ze zgłoszeniem w złej wierze, oczerniającym lub w inny sposób godzącym w dobra osobiste osoby objętej nim, ani ze zgłoszeniem dobrowolnie nieanonimowym, ujawnianie danych sygnalisty potencjalnemu naruszycielowi nie wydaje się celowe ani uzasadnione. Realizacja obowiązku informacyjnego winna być wobec niego odroczona do czasu przyjęcia i przystąpienia do wykonywania rekomendacji w następstwie postępowania wyjaśniającego. Niewyobrażalne jest także wykonanie prawa do bycia zapomnianym, chyba że mamy do czynienia ze zgłoszeniem w złej wierze, oczerniającym, a poszkodowany zgłoszeniem dobrowolnie żąda usunięcia jego danych. W przypadku zgłoszeń dotyczących pracowników pojawia się pytanie, czy w „generalnej" klauzuli informacyjnej przygotowanej przez pracodawcę nie byłoby wystarczające wskazanie, że ich dane mogą być przetwarzane także w zakresie whistleblowingu. Na pograniczu ochrony danych osobowych i ochrony dobrego imienia pozostaje ujawnienie lub doprowadzenie do ustalenia danych osobowych sygnalisty, który dokonał oczerniającego zgłoszenia w złej wierze, aby umożliwić ochronę praw osoby, której dobra osobiste zostały w ten sposób naruszone.

9. Podsumowanie

Whistleblowing, zwłaszcza w zharmonizowanym unijnym modelu wynikającym z dyrektywy o ochronie sygnalistów, jawi się jako kolejny obszar konwergencji regulacyjnej między rynkiem finansowym i energetycznym. Intensyfikujące się podobieństwa w obszarze wymogów *compliance* dostarczają jednocześnie coraz to nowych wy-

zwań dla systemów zarządzania ryzykiem braku zgodności, zwłaszcza w przedsiębiorstwach o złożonych procesach biznesowych.

Programy ochrony sygnalistów stanowią już obecnie część rzeczywistości gospodarczej, a zmiany w otoczeniu prawno-regulacyjnym jedynie przyczynią się do ich upowszechnienia i wzrostu znaczenia, czemu, jak można oczekiwać, towarzyszyć będzie rozwój jednostki *compliance*.

Oczekiwanie takie jest tym bardziej zrozumiałe, że harmonizacja whistleblowingu na wspólnym rynku ma charakter niezupełny, pozostawiając z jednej strony przestrzeń do przyjęcia uregulowań na szczeblu krajowym, z drugiej zaś strony potwierdzając znaczną autonomię decyzyjną po stronie przedsiębiorców we wprowadzeniu i stosowaniu systemów whistleblowingowych. Ustanowienie mechanizmów stanowi element starannego prowadzenia spraw danego przedsiębiorstwa i wymaga dostosowania do uwarunkowań danej organizacji.

Należy zadbać, aby *whistleblowing* stanowił jedno z ogniw systemu zarządzania ryzykiem braku zgodności, dla którego punktem wyjścia powinien być kodeks etyczny lub podobny dokument kierunkowy. Sama rola sygnalisty budzi pewne wątpliwości moralne, stąd jednoznaczne osadzenie zgłaszania nieprawidłowości w tego rodzaju manifeście korporacyjnym pozwoli na zapewnienie odpowiedniej wymowy komunikatu dla pracowników, tzw. *tone from the top*. Obok norm etycznych, system *compliance* winien integrować także uwarunkowania wynikające z przepisów o ochronie danych osobowych i prywatności, ochronie dóbr osobistych, informacji prawnie chronionych, itd.

Tego rodzaju holistyczne ujęcie nabiera szczególnego znaczenia w przypadku whistleblowingu. Procedura anonimowego raportowania nadużyć winna zapewniać zgłaszającym określony poziom ochrony przed działaniami odwetowymi, musi jednocześnie ważyć racje i interesy pracodawcy oraz potencjalnie objętych zgłoszeniem pracowników, przewidując nie tylko standardy uczciwego postępowania wyjaśniającego, lecz także obronę przed oczerniającymi zawiadomieniami. W konkretnych przypadkach może pojawić się potrzeba rozstrzygnięcia, czy zgłoszenia nie dokonano w złej wierze i czy nie jest konieczne podjęcie w związku z nim kroków prawnych.

Bibliografia

Anderson Karen, Black Julia, *Legal risks and risks for lawyers*, Londyn 2013, s. 2-4, http://www.lse.ac.uk/law/people/academic-staff/julia-black/Documents/black9.pdf

Bernatt Maciej, *Sprawiedliwość proceduralna w postępowaniu przed organem ochrony konkurencji*, Warszawa 2011.

Braun Tomasz, *Unormowania compliance w korporacjach*, LEX 2017.

Bürkle Jürgen, *Compliance als Aufgabe des Vorstands der AG – Die Sicht des LG München I*, „Corporate Compliance Zeitschrift" 2015, nr 2, s. 52-55.

Compliance w wybranych podmiotach nadzorowanych rynku finansowego. Aspekty praktyczne, red. Paweł Eleryk, Alicja Piskorz-Szpytka, Przemysław Szpytka, LEX 2019.

Derlacz-Wawrowska Marta, *Whistleblowing a ochrona informacji poufnych pracodawcy*, [w:] *Prawo pracy. Refleksje i poszukiwania. Księga Jubileuszowa Profesora Jerzego Wratnego*, red. Gertruda Uścińska, Warszawa 2013, s. 390-403.

Dworkin Terry Morehead, *SOX and Whistleblowing*, „Michigan Law Review" 2007, nr 105 (8), s. 1757-1780.

Efektywność zarządzania i nadzoru w spółce handlowej. W poszukiwaniu optymalnego modelu ustroju spółki, red. Katarzyna Bilewska, LEX 2018.

Ferrel O. C., Frædrich John, Ferrell Linda, *Business Ethics. Ethical decision making and cases*, Mason 2013.

Gac Maciej, *Programy zgodności z prawem konkurencji – efektywny mechanizm w tworzeniu europejskiej kultury compliance?*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2012, nr 2, s. 57-71.

Hopkin Paul, *Fundamentals of Risk Management. Understanding, evaluating and implementing effective risk management*, Londyn 2014.

Jagura Bartosz, *Rola organów spółki kapitałowej w realizacji funkcji compliance*, LEX 2017.

Jawność i jej ograniczenia. T. II. Podstawy aksjologiczne, red. Zbigniew Cieślak, Grażyna Szpor, Legalis 2013.

Koczur Wiesław, *Tajemnica pracodawcy (zakładowa)*, „Monitor Prawniczy" 2015, nr 7, s. 386-392.

Krawczyk Aleksandra, Gisman Aleksander, *Criminal compliance jako środek zapobiegania odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary*, „Monitor Prawa Handlowego" 2015, nr 1, s. 7-12.

Legal Risk Management, Governance and Compliance, red. Weinstein Stuart, Wild Charles, Londyn 2013.

Lewicka-Strzałecka Anna, *Instytucjonalizacja whistleblowingu w firmie jako wyzwanie etyczne*, „Diametros" 2014, nr 41, s. 77-98.

Maćkowiak Aleksandra, Wiciak Tomasz, *Standardy compliance drogą do unikania odpowiedzialności. Refleksje po IX. Polsko-Niemieckim Forum Compliance*, „Monitor Prawniczy" 2018, nr 24, s. 1323-1327.

Makowicz Bartosz, *Compliance w przedsiębiorstwie*, Warszawa 2011.

Makowicz Bartosz, *Metody efektywnego kształtowania systemów compliance – Wprowadzenie*, „Monitor Prawniczy" 2013, nr 23 – dodatek specjalny, s. 1-2.

Małobęcka-Szwast Iga, *Compliance w zakresie prawa ochrony konkurencji jako wyzwanie dla organów spółki*, „Monitor Prawa Handlowego" 2018, nr 3, s. 25-32.

Meckenstock Cordula, *Struktura i wdrażanie systemów "compliance" – wprowadzenie praktyczne*, „Monitor Prawniczy" 2013, nr 23 – dodatek specjalny, s. 6-8.

Raczyński Mirosław, *Implikacje konwergencji w branżach ICT dla polityki regulacyjnej*, http://mikroekonomia.net/system/publication_files/249/original/17.pdf?1314948750

Rogowski Wojciech, *Whistleblowing: bohaterstwo, zdrada czy interes?*, „Przegląd Corporate Governance" 2007, nr 1 (9), s. 23-41.

Roquilly Christophe, Collard Christophe, *De la conformité réglementaire à la performance: pour une approche multidimensionnelle du risque juridique*, Centre de Recherche Legal EDHEC Business School, https://www.edhec.edu/sites/www.edhec-portail.pprod.net/files/publications/pdf/com.univ.collaboratif.utils.LectureFichiergw%3FID_FICHIER%3D1328885973394jpg

Sadlik Ryszard, *Miesięczny termin na rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika*, „Służba Pracownicza" 2014, nr 5, s. 14-16.

Schneider Uwe, *Compliance als Aufgabe der Unternehmensleitung*, „Zeitschrift für Wirtschaftsrecht und Insolvenzpraxis" 2003, nr 15, s. 645-650.

Turno Bartosz, *Zagadnienie tajemnicy adwokackiej na gruncie prawa konkurencji*, [w:] *Aktualne problemy polskiego i europejskiego prawa ochrony konkurencji*, red. Cezary Banasiński, Marian Kępiński, Bożena Popowska, Teresa Rabska, Warszawa 2006, s. 172-189.

Turno Bartosz, Zawłocka-Turno Agata, *Legal Professional Privilege and the Privilege Against Self-Incrimination in EU Competition Law after the Lisbon Treaty – Is It Time for a Substantial Change?*, „Yearbook of Antitrust and Regulatory Studies" 2012, nr 5 (6), s. 193-214.

Wojciechowska-Nowak Anna, *Założenia do ustawy o ochronie osób sygnalizujących nieprawidłowości w środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych?*, Fundacja Batorego, Warszawa 2012, http://www.batory.org.pl/upload/files/Programy%20operacyjne/Przeciw%20Korupcji/zalozenia-do-ustawy-o-ochronie-sygnalistow.pdf