DOI: 10.34616/151201

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 45–76

Adw. Oskar Grajewski
ORCID: 0009-0009-7968-5543

Mateusz Jakubik
Uniwersytet Jagielloński w Krakowie
Wydział Prawa i Administracji
ORCID: 0000-0002-8992-7309

Wybrane zagadnienia dotyczące roli sygnalistów[1] i kanałów zgłaszania w kontekście rozwoju technologii cyfrowych oraz zmian prawodawczych, a także związanych z tym wyzwań i perspektyw[2]

Streszczenie

Niniejsza praca skupia się na ewolucji roli sygnalistów w erze cyfrowej oraz na analizie wpływu nowoczesnych technologii, takich jak sztuczna inteligencja (AI), *blockchain*, *big data* oraz internet rzeczy (IoT), na skuteczność i bezpieczeństwo kanałów zgłaszania naruszeń. Celem pracy jest ocena, w jaki sposób technologie te mogą zrewolucjonizować proces zgłaszania nieprawidłowości, a także jakie wyzwania i możliwości wiążą się z ich integracją w kontekście współczesnych zmian prawodawczych, ze szczególnym uwzględnieniem dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii oraz Ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów. Metodologia badawcza obejmuje przeglądy literatury oraz analizę regulacji prawnych. Kluczowe ustalenia wskazują, że technologie cyfrowe mogą znacznie podnieść poziom bezpieczeństwa, anonimowości oraz efektywności systemów zgłaszania, lecz jednocześnie stawiają przed prawodawcami i organizacjami poważne wyzwania, związane z zapewnieniem zgodności z przepisami, ochroną danych osobowych oraz transparentnością. Praca podkreśla, że istotnym aspektem w przyszłości ochrony sygnalistów będzie harmonizacja przepisów prawnych z dynamicznie rozwijającym się krajobrazem technologicznym oraz edukacja w zakresie nowych narzędzi zgłaszania. Implikacje badań sugerują konieczność elastycznego podejścia do regulacji prawnych w ten sposób, aby

[1] W treści artykułu autorzy posługują się przeważnie terminem „sygnalista", będącym tłumaczeniem angielskiego wyrazu *whistleblower* (a także jego innej formy *whistle-blower*), jednakże we fragmentach poświęconych etymologii przedmiotowego terminu w obu formach, a także we fragmentach poświęconych tematom, w których zachodzą różnice w obrębie tych pojęć, wyrazy te wykorzystywane są równolegle w celu uwypuklenia uwag.

[2] Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autorów i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autorzy byli albo są powiązani.

zapewnić skuteczną ochronę sygnalistów w erze cyfrowej, oraz wskazują na potrzebę ciągłego monitorowania i adaptacji przepisów do nowych wyzwań technologicznych.

Słowa kluczowe

sygnaliści, ochrona sygnalistów, kanały zgłaszania naruszeń, technologie cyfrowe, sztuczna inteligencja (AI), *big data*, internet rzeczy (IoT), RODO

Uwagi wstępne

Celem niniejszej pracy jest zbadanie znaczenia, wyzwań i perspektyw związanych z rolą sygnalistów w erze cyfrowej oraz analiza, w jaki sposób technologie, takie jak AI, *big data* czy *blockchain*, mogą wpłynąć na skuteczność i bezpieczeństwo kanałów zgłaszania nieprawidłowości. Praca ta ma na celu również ocenę, jak zmiany prawodawcze, zwłaszcza dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (UE)[3] i ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów[4], dostosowują się do dynamicznie rozwijającego się krajobrazu technologicznego oraz prawodawczego i jakie implikacje niosą one dla przyszłości ochrony sygnalistów.

Artykuł ten nie aspiruje jednak do miana pracy propedeutycznej ani tym bardziej wyczerpującej temat sygnalistów i kanałów zgłaszania, co usiłowano zaznaczyć już w samym tytule. Choć powodów tego działania jest wiele, to dla dochowania zasady oględności można poprzestać na stwierdzeniu, iż problematyka ta w samym jej bieżącym zakresie jawi się jako nie mniej obszerna niż dotychczasowe dzieje zjawiska „sygnalistów" i godna jest wnikliwszych oraz z pewnością bardziej obszernych badań i analiz. W ich efekcie prawdopodobne byłoby, iż przy nagromadzeniu tak wielu zagadnień doczesnych ich ekspozycja odbyłaby się kosztem właśnie tego aspektu, któremu w niniejszej pracy pragną przyjrzeć się autorzy. Mowa tu o samym znaczeniu, wyzwaniach i perspektywach omawianego zjawiska, których natura nakazuje nam odnosić się do przyszłości, na co w dobie cyfrowej, gdy „wartość czasu" wykracza poza jego „kantowskie"[5] rozumienie jako *a priori* formę naszej zmysłowości[6], prawdopodobnie mało kto może sobie pozwolić. To hipotetyczne za-

[3] Dz. Urz. UE L 305/17 z 2019 r. (dalej: „dyrektywa 2019/1937" oraz „dyrektywa").

[4] Dz. U. z 2024 r. poz. 928 (dalej: „Ustawa o ochronie sygnalistów" oraz „u.o.s.").

[5] Chodzi o I. Kanta (ur. 22 kwietnia 1724 r., zm. 12 lutego 1804 r.), niemieckiego filozofa, profesora logiki i metafizyki na Uniwersytecie Albrechta w Królewcu, jednego z najwybitniejszych reprezentantów oświecenia, zob. I. Kant, [w:] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/Kant-Immanuel;3919929.html/ [dostęp: 30.08.2024].

[6] I. Kant, *Krytyka czystego rozumu*, tłum. R. Ingarden, Warszawa 1957, s. 79.

niechanie niosłoby za sobą niemałą szkodę, bowiem konsekwencją stale przez nas doświadczanego tempa rozwoju jest potrzeba podjęcia się zarówno indywidualnie, jak i zbiorowo wzmożonej pracy nad zrozumieniem możliwych przyszłych zmian w zakresie problematyki sygnalistów. Niezbędne w tym celu pozostaje także zrozumienie korelacji zjawiska sygnalistów z dalszym rozwojem rzutujących na ich aktywność technologii, a także wpływu sygnalistów na dotychczasowy sposób funkcjonowania społeczeństwa. Następstwem tych starań powinno być wypracowanie i wdrożenie odpowiednich mechanizmów oraz higieny korzystania z rozwijanych przez cywilizację technologii, a także zyskanie perspektywy i narzędzi do podejmowania działań prawodawczych, które zdołają dotrzymać kroku temu rozwojowi w wymiarze praktycznym, a nie jedynie postulatywnym, a to wszystko bynajmniej nie w celu zapewnienia sobie komfortu w miejscu, w którym aktualnie się znajdujemy, lecz w celu zachowania kontroli nad tym, dokąd zmierzamy.

Według poczynionych założeń nie można więc oczekiwać, aby w tak krótkiej formie publicystycznej przedstawić w sposób kompleksowy genezę bohaterów niniejszego tekstu, wszelkich możliwych kanałów zgłaszania, dorobku prawodawczego, doktrynalnego i jurydycznego, czemu z pewnością poświęcono już liczne publikacje oraz mnóstwo uwagi. Zamiast tego analizie poddane zostaną te zagadnienia, które zdają się obecnie dominować dyskurs nowych technologii w prawie. Dowodząc słuszności takiego działania, należy zwrócić uwagę na uzasadnione i nieodparte wrażenie autorów, iż w kontekście szybkiego rozwoju technologicznego i zmieniającego się otoczenia prawnego wzrasta także znaczenie problematyki sygnalistów, których rola ściśle wiąże się z tym dynamizmem i wpływa na nas jak jeszcze nigdy dotąd.

1. Ewolucja znaczenia „sygnalistów” i ich roli w kontekście technologii cyfrowych

Uprzedzając ewentualne uwagi, jakoby określanie sygnalistów mianem „bohaterów” stanowiło przejaw grandilokwencji, stwierdzić należy, iż zabieg ten, prócz waloru stylistycznego, umotywowany był także donioślejszą przyczyną. Zbyteczne byłoby pochylanie się nad kwestią ewentualnych osobistych korzyści, jakich mógłby potencjalnie doświadczyć sygnalista, lecz bez względu na to, chcąc wykazać, z jak istotną w tym przypadku mierzymy się materią, konieczne jest odnieść się do znaczenia roli sygnalistów i korzyści płynących z ich działalności w ujęciu powszechnym. Stając przed takim problemem, naturalne zdaje się postawienie najpierw pytania jeszcze bardziej ogólnego, a mianowicie: kim *de facto* są „sygnaliści”? Wiążąc

ładunek znaczeniowy omawianego pojęcia z samym terminem „sygnalista", można by poprzestać na przytoczeniu jedynie definicji tego pojęcia, jednakże w celu podkreślenia istoty zagadnienia konieczne zdaje się podjęcie próby dokonania jego egzegezy, co z kolei wymaga przytoczenia najpierw rysu historycznego.

W anglojęzycznych słownikach etymologicznych pochodzenie pojęcia *whistleblower* powiązano w sposób oczywisty z czynnością polegającą na dmuchaniu w gwizdek (ang. *blow the whistle*) i wskazano na jego występowanie w powszechnym obiegu co najmniej od XIX w., pierwotnie z łącznikiem jako *whistle-blower*, a następnie w zapisie łącznym *whistleblower*[7]. Jednakże jeszcze w XIX w. *whistleblower* nabrało bardziej specyficznego znaczenia, albowiem nie odnosiło się już tylko do osoby, która gwizdała w jakikolwiek sposób, lecz słowo to oznaczało również sędziego w zawodach sportowych[8]. Po tym jak pojęcia *whistleblower* zaczęto powszechnie stosować w odniesieniu do sędziego w zawodach sportowych, termin ten zaczął być także używany w znaczeniu zwrócenia uwagi publicznej na zdarzenie utrzymywane w tajemnicy[9]. Następnie zaś coraz częściej pojęcie *whistleblower* zaczęło być wiązane z ujawnianiem zdarzeń dotyczących naruszeń przepisów prawa, w tym także o charakterze przestępczym[10]. Z drugiej strony odnaleźć można także dowody wskazujące na to, iż metaforyczne znaczenie terminu *whistleblower* funkcjonowało już w drugiej połowie XIX w.[11]

W powszechnym obiegu ugruntował się także pogląd, iż pojęcie *whistleblower* w jego aktualnym znaczeniu zostało spopularyzowane w latach 60. i 70. XX w. przez dziennikarzy[12] i działaczy politycznych, takich jak R. Nader[13], amerykański

---

[7] *Whistleblower*, [w:] *Online Etymology Dictionary*, https://www.etymonline.com/search?q=whistleblower%20/ [dostęp: 30.08.2024].

[8] *Whistleblower*, [w:] *Merriam-Webster*, https://www.merriam-webster.com/wordplay/whistle-blower-blow-the-whistle-word-origins/ [dostęp: 30.08.2024], gdzie jako przykłady wskazano wybrane publikacje z czasopism: „The Huddersfield Chronicle and West Yorkshire Advertiser", Huddersfield 1890, „Jackson's Oxford Journal", Oxford 1894, „The Hampshire Advertiser", Southampton 1895.

[9] *Ibidem*, gdzie jako przykłady wskazano wybrane publikacje z czasopism: „San Francisco Chronicle", San Francisco 1929, „Richmond Times Dispatch", Richmond 1934.

[10] *Ibidem*, gdzie jako przykłady wskazano wybrane publikacje z czasopism: „Variety", City of New York 1963, „Asbury Park Press", Asbury Park 1966, „The Pittsburgh Press", Pittsburgh 1967.

[11] *Whistle-blower*, [w:] *Phrases Finder*, https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024], gdzie jako przykład wskazano wybrany artykuł z czasopisma: „Wisconsin's Janesville Gazette", Wisconsin 1883, w którym słowem *whistleblower* nazwano policjanta, który użył gwizdka, aby powiadomić obywateli o zamieszkach.

[12] *Whistleblower*, [w:] Wayback Machine, https://web.archive.org/web/20120429004210/http://www.wordor igins.org/index.php/site/whistleblower/ [dostęp: 30.08.2024].

[13] J.K. Devitt, *Speaking Up Safely Civil Society Guide To Whistleblowing: Middle East And North Africa Region*, „Transparency International" 2015, s. 5–7, http://www.jstor.org/stable/resrep20533/ [dostęp: 30.08.2024].

prawnik, wykładowca, aktywista polityczny i wielokrotny kandydat na prezydenta Stanów Zjednoczonych Ameryki, założyciel Public Citizen[14], będącej organizacją non profit, zajmującą się obroną praw konsumentów[15]. Pogląd ten wymusza dookreślenie aktualnego znaczenia słowa *whistleblower*, które w słownikach języka angielskiego opisywane jest jako „osoba donosząca na inną osobę lub ujawniająca publicznie korupcję, nieprawidłowości, problemy lub tajne informacje, zwłaszcza wewnątrz organizacji" (ang. *a person who informs on another or makes public disclosure of corruption, wrongdoing, problems, or secret information, especially within an organization*)[16] albo ogólniej jako „osoba, która ujawnia coś tajnego lub donosi o kimś innym" (ang. *one who reveals something covert or who informs against another*)[17]. Podobnie omawiany termin pisany w formie *whistle-blower* definiowany jest jako „osoba próbująca podnieść alarm w sprawie jakiegoś problemu i nagłaśniać go wewnątrz lub na zewnątrz swojej organizacji" (ang. *a person who tries to raise the alarm about a problem and publicizes it inside and/or outside of his/her organization*)[18]. Co ciekawe, w chwili powstawania niniejszego artykułu *Słownik języka polskiego PWN* definiuje „sygnalistę" jedynie jako „osobę nadającą i odbierającą sygnały za pomocą odpowiednich urządzeń"[19], tym samym pomijając zupełnie tak powszechne i omawiane obecnie rozumienie tego słowa. Podobnie, co jednak zdaje się bardziej zrozumiałe, znaczenia tego nie zawiera *Słownik języka polskiego* pod red. W. Doroszewskiego, w którym „sygnalista", to „ten, kto nadaje i gra sygnały (np. na statku, w kopalni) za pomocą odpowiednich urządzeń, jak dzwonki, lampy, syreny alarmowe itp." Interesujące nas znaczenie „sygnalisty"[20], oprócz tożsamego do opisanych powyżej, znaleźć można dopiero w internetowym słowniku języka polskiego, znajdującym się na witrynie sieciowej SJP[21], który redagowany jest

---

[14] *Ralph Nader*, https://achievement.org/achiever/ralph-nader/ [dostęp: 30.08.2024].

[15] *Nader Riders*, https://pophistorydig.com/topics/naders-raiders-1968-1974/ [dostęp: 30.08.2024].

[16] *Whistleblower*, [w:] *Oxford English Dictionary*, https://www.dictionary.com/browse/whistleblower/ [dostęp: 30.08.2024], tłum. własne.

[17] *Whistleblower*, [w:] *Meriiam-Webster*, https://www.merriam-webster.com/dictionary/whistleblower/ [dostęp: 30.08.2024], tłum. własne.

[18] *Whistle-blower*, [w:] *Phrase Finder*, https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024], tłum. własne.

[19] *Sygnalista*, [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/ [dostęp: 31.08.2024].

[20] *Sygnalista*, [w:] *Słownik języka polskiego*, red. W. Doroszewski, https://sjp.pwn.pl/doroszewski/sygnalista/ [dostęp: 31.08.2024].

[21] Zob. *SJP*, https://sjp.pl/, który to słownik powstał na bazie dawnego słownika do programu ispella, napisanego w 1971 r. przez R.E. Gorina i służącego do sprawdzania pisowni dla systemów uniksowych, a więc systemów operacyjnych rozwijanych od 1969 r. w Bell Labs przez UNIX System Laboratories.

obecnie przez hobbystów i udostępniany jest na otwartych licencjach[22], a w którym przyjęto, iż „sygnalista" to także „osoba zgłaszająca w dobrej wierze informacje o nieprawidłowościach w miejscu pracy"[23].

Odnosząc takie stwierdzenie do wspominanej wcześniej okoliczności wciąż ugruntowującego się znaczenia terminu „sygnalista", zrozumiała pozostaje aprobata doktryny wobec wprowadzenia na etapie prac nad projektem ustawy o ochronie sygnalistów zmiany terminologicznej i zastąpienia pojęcia „osoby dokonującej zgłoszenia lub ujawnienia publicznego" właśnie terminem „sygnalista"[24]. Choć przesadą byłoby określenie tego zabiegu postępowym, to odpowiada on dowiedzionemu faktowi utrwalenia się w praktyce jego angielskiego odpowiednika *whistleblower.* Z drugiej strony w doktrynie zwraca się także uwagę na okoliczność, iż w u.o.s. nie wprowadzono rozróżnienia pomiędzy pojęciem „osoby dokonującej zgłoszenia", nawet jeśli nie podlega ochronie, a „sygnalistą»[25], co prowadzi do powstania rozdźwięku pomiędzy powszechnym (potocznym) oraz ustawowym zakresem tego terminu.

Zakres podmiotowy ustawy, wskazujący na to, kto podlega ochronie jako sygnalista w sytuacji dokonania zgłoszenia lub ujawnienia publicznego, określony został w art. 4 u.o.s. i obejmuje każdą osobę dokonującą zgłoszenia lub ujawnienia, która informację o naruszeniu prawa pozyskuje w związku z pracą, przy czym związek ten rozumiany jest w sposób szeroki, albowiem obejmuje pracę, która potencjalnie miała nastąpić, lecz nie doszła do skutku, pracę trwającą oraz pracę, która była wykonywana w przeszłości. Przepis zawarty we wskazanym artykule zawiera także wyliczenie konkretnych osób objętych ochroną, lecz nie jest ono enumeratywne[26]. Co ciekawe, w art. 4 ust. 1 pkt 4 u.o.s. jako jeden z przykładów osób objętych ochroną wskazano przedsiębiorcę i jak zauważa się w doktrynie, sytuacja ta oznacza, że zgłoszenia lub ujawnienia publicznego może dokonać także kontrahent podmiotu prawnego, u którego miało dojść do naruszenia prawa[27].

Niezależnie od tego zauważyć należy, iż o ile sam termin *whistleblower* (a tym bardziej „sygnalista") w omawianym ujęciu posiada względnie krótką historię, o tyle rola, jaką potocznie przypisuje się osobie określanej tym terminem,

---

[22] *Ibidem*.

[23] *Sygnalista*, [w:] *SJP*, https://sjp.pl/sygnalista [dostęp: 31.08.2024].

[24] D. Tokarczyk, [w:] E. Rutkowska, D. Tokarczyk, *Ustawa o ochronie sygnalistów. Komentarz*, LEX/el. 2024, art. 4, https://sip.lex.pl/#/commentary/587977514/774954?keyword=Ustawa%20o%20ochronie%20sygnalist%C3%B3w.%20Komentarz&tocHit=1&cm=SFIRST/ [dostęp: 31.08.2024].

[25] *Ibidem*.

[26] *Ibidem*.

[27] *Ibidem*.

ma znacznie dłuższą historię. A. Stanger twierdzi, iż pierwszymi udokumentowanymi sygnalistami byli w 1777 r. amerykańscy marynarze, którzy w obliczu walki z Królestwem Wielkiej Brytanii podpisali 19 lutego 1777 r. na pokładzie jednostki USS Warren petycję do Kongresu Kontynentalnego, dokumentującą nadużycia ich dowódcy Eseka Hopkinsa[28]. Zdawać się może jednak, iż podejmowana w ten sposób próba określenia „pierwszych udokumentowanych sygnalistów" wyklucza bezzałożeniową metodę fenomenologiczną i zasadza się na problemie uprzedniego określenia swoistego minimum cech wymaganych do zakwalifikowania osoby jako „sygnalisty". Co stoi bowiem na przeszkodzie, aby bez tych założeń, świadomie narażając się na anachronizm, protoplastów współczesnych sygnalistów upatrywać w czasach znacznie odleglejszych? Chociażby pojawiający się w Starym Testamencie prorok Nathan odegrał kluczową rolę w historii króla Dawida i Batszeby, ponieważ gdy Dawid dopuścił się grzechu (zlecając zabójstwo Uriasza, aby poślubić jego żonę Batszebę), Nathan, świadomy tego czynu, skonfrontował Dawida z jego grzechem[29]. Nathan opowiedział przypowieść, która ujawniła niesprawiedliwość popełnioną przez króla, co z kolei doprowadziło do pokuty tego ostatniego[30]. Tak więc Nathan, podobnie jak sygnalista, podjął ryzyko, ujawniając nadużycie przez osobę będącą u szczytu władzy, a jego działania zmierzały do naprawienia niesprawiedliwości i przywrócenia moralnego porządku. Analogii tej zdaje się nie przeczyć okoliczność, iż panujący w Izraelu na przełomie XI i X w. p.n.e. ustrój polityczny niejako wymuszał, aby nieprawidłowość została zasygnalizowana przez tę samą osobę, która dopuściła się nieprawości, a więc przez króla (przy czym na potrzeby analogii akceptowalne są wątpliwości co do możliwości utożsamienia działania polegającego na „ujawnieniu naruszenia" z jego „uświadomieniem"). Zaznaczyć należy, iż prorok działał w środowisku, gdzie krytykowanie króla mogło prowadzić do represji, ale mimo to zdecydował się na ujawnienie prawdy, a jego odwaga przypomina współczesnych sygnalistów, którzy narażają się na zawodowe i osobiste konsekwencje w imię prawdy i sprawiedliwości. Współcześni sygnaliści również często stają w obliczu ryzyka utraty pracy, represji ze strony przełożonych, jednak mimo to decydują się na ujawnienie nieprawidłowości. Co więcej, celem Nathana nie było tylko oskarżenie Dawida, ale przede

[28] A. Stanger, *Whistleblowers: Honesty in America from Washington to Trump*, Harvard University Press, Cambridge 2019, s. 28.

[29] *Pismo Święte Starego i Nowego Testamentu*, Biblia Tysiąclecia, wyd. 5, Poznań 2000, 2 Sm 12, s. 1–15.

[30] *Ibidem*.

wszystkim doprowadzenie do pokuty i naprawienia krzywd. Jego działania były więc skierowane na przywrócenie sprawiedliwości, podobnie jak w przypadku sygnalistów, którzy działają zazwyczaj w celu ujawnienia prawdy i doprowadzenia do naprawienia szkód wyrządzonych przez działania niezgodne z prawem lub etyką (często w kontekście ochrony dobra publicznego).

W mitologii greckiej postacią, którą można uznać za protoplastę sygnalistów we współczesnym rozumieniu, jest Prometeusz, znany z tego, że sprzeciwił się woli Zeusa, dostarczając ludziom ogień, symbolizujący wiedzę, technologię i cywilizację. Tym samym Prometeusz ujawnił ludziom tajemnice, które były zastrzeżone dla bogów, działając wbrew zakazowi najwyższego autorytetu Zeusa[31]. Podobnie więc jak sygnaliści, którzy często sprzeciwiają się autorytetom w celu ujawnienia informacji ukrywanych przed społeczeństwem, Prometeusz podjął działanie, które miało na celu przyniesienie dobra publicznego, mimo że było to sprzeczne z interesami potężnych jednostek. Przekazanie ognia ludzkości było aktem, który miał na celu rozwój i dobrobyt całej rasy ludzkiej. W mitologii Prometeusz został surowo ukarany przez Zeusa za swoje działania, gdyż przykuto go do skały, gdzie codziennie orzeł kaukaski wyjadał mu wątrobę[32]. Kara ta stanowi niejako symbol represji, jakie mogą spotkać tych, którzy działają na przekór władzy. Podobnie jak Prometeusz współcześni sygnaliści często stają w obliczu poważnych konsekwencji, takich jak utrata pracy, procesy sądowe, a nawet zagrożenie dla życia, a to za swoje działania na rzecz dobra innych. Przykłady te ukazują, że chociaż idea sygnalizowania nieprawidłowości jest współczesnym terminem, jej moralne fundamenty sięgają znacznie głębiej, nawet do starożytności i są zakorzenione w tradycjach etycznych, religijnych, a także w mitach i legendach, które od wieków uczą nas o wartości odwagi, wiedzy i sprawiedliwości.

Dowodząc przemożnego wpływu tego zagadnienia na otaczającą nas rzeczywistość, można posłużyć się przykładem W.M. Felta, amerykańskiego prawnika i byłego zastępcy dyrektora Federalnego Biura Śledczego w Stanach Zjednoczonych Ameryki (FBI), który w maju 2005 r. ujawnił, iż w trakcie afery Watergate to on był źródłem informacji zwanym „Głębokie Gardło”[33], a więc ujawnił nielegalne działania administracji R. Nixona skierowane przeciwko jego przeciwnikom politycznym, co doprowadziło do ustąpienia tego polityka ze stanowiska prezydenta

[31] K. Kumaniecki, *Mitologia Greków i Rzymian*, Warszawa 1988, s. 45–48.

[32] *Ibidem*.

[33] J.D. O’Connor, *I’m the Guy They Called Deep Throat*, „Vanity Fair”, https://www.vanityfair.com/news/politics/2005/07/deepthroat200507?printable=true&currentPage=all/ [dostęp: 30.08.2024].

Stanów Zjednoczonych Ameryki[34]. Nie sposób także pominąć jako przykład sprawy E.J. Snowdena, byłego pracownika CIA i zleceniobiorcę firm Dell oraz Booz Allen Hamilton, który ujawnił kilkaset tysięcy poufnych, tajnych i ściśle tajnych dokumentów amerykańskiej wewnętrznej agencji wywiadowczej National Security Agency (NSA), co określono jako największy wyciek tajnych informacji w historii USA[35] (w tym m.in. informacje o programie PRISM, pozwalającym masowo podsłuchiwać rozmowy Amerykanów i obywateli innych krajów[36]). Symptomatyczna zdaje się już sama liczba możliwych do przytoczenia przypadków sygnalizowania nieprawidłowości, a to chociażby z ostatniej dekady, takich jak sprawy H. Wilkinsona[37], *Lux Leaks*[38], *Panama Papers*[39], *Novartis*[40] czy chociażby (wciąż tak nieodległy) przypadek L. Wenlianga, który był chińskim lekarzem pracującym w szpitalu w Wuhan, w prowincji Hubei i stał się znany jako sygnalista, który na początku pandemii COVID-19 próbował ostrzec swoich kolegów i władze chińskie o wybuchu nowego, groźnego wirusa przypominającego SARS, czego następstwem było upomnienie go przez chińskie władze[41].

Wśród polskich przykładów znanych sygnalistów wymienić należy przede wszystkim niezwykle doniosły historycznie przypadek J. Karskiego, polskiego kuriera i dyplomaty, który podczas II wojny światowej odegrał kluczową rolę jako sygnalista, kiedy to jako członek polskiego ruchu oporu na własne oczy zobaczył okrucieństwa Holocaustu, odwiedzając getto warszawskie i obóz przejściowy w Izbicy (zidentyfikowany przezeń mylnie jako obóz zagłady w Bełżcu), a zebrane przy tej

---

[34] R. Perlstein, *Watergate scandal*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/event/Watergate-Scandal/ [dostęp: 30.08.2024].

[35] M. Ray, *Edward Snowden*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/biography/Edward-Snowden/ [dostęp: 30.08.2024].

[36] *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program – The Washington Post*, „Washington Post", https://www.washingtonpost.com/ [dostęp: 30.08.2024].

[37] M. Todd, *Danske Bank Whistleblower Testifies at European Parliament*, Whistleblower Network News, https://whistleblowerprotection.eu/blog/danske-bank-whistleblower-testifies-at-european-parliament/ [dostęp: 30.08.2024].

[38] F. Shiel, *European court reverses course to rule in favor of LuxLeaks whistleblower*, https://www.icij.org/investigations/luxembourg-leaks/european-court-reverses-course-to-rule-in-favor-of-luxleaks-whistleblower/ [dostęp: 30.08.2024].

[39] M. Hudson, *The Panama Papers: Exposing the Rogue Offshore Finance Industry*, https://www.icij.org/investigations/panama-papers/ [dostęp: 30.08.2024].

[40] *United States Files Complaint Against Novartis Pharmaceuticals Corp. for Allegedly Paying Kickbacks to Doctors in Exchange for Prescribing Its Drugs*, https://www.justice.gov/opa/pr/united-states-files-complaint-against-novartis-pharmaceuticals-corp-allegedly-paying/ [dostęp: 30.08.2024].

[41] *Coronavirus kills Chinese whistleblower ophthalmologist, American Academy of Ophthalmology*, https://www.aao.org/education/headline/coronavirus-kills-chinese-whistleblower-ophthalmol/ [dostęp: 30.08.2024].

okazji informacje przekazał aliantom, osobiście informując o stwierdzonym procederze prezydenta Stanów Zjednoczonych Ameryki F.D. Roosevelta[42]. Mimo wysiłków J. Karskiego jego informacje nie wywołały natychmiastowej reakcji państw, które wspólnie przeciwstawiły się blokowi państw Osi, co nadaje staraniom J. Karskiego jako sygnalisty szczególnego tragizmu[43]. Wśród bardziej aktualnych przykładów można wspomnieć o mjr. M. Ratajczyku, który informował o możliwości złamania procedur wewnętrznych dotyczących izolacji chorych w zakładzie karnym w Garbalinie, gdzie w ciągu zaledwie kilku dni doszło do zakażenia się przez 82 osoby chorobą COVID-19, co miało się spotkać z naciskiem przełożonych na ograniczenie badania przypadków zakażeń[44].

W świetle przytoczonych dotychczas przykładów nie sposób kwestionować faktu, iż znaczenie działań sygnalistów, niezależnie od przyjętego zakresu tego pojęcia i wtórującego temu dziejowemu dorobkowi, pozostaje nieocenione. Znaczenie to zostało także dostrzeżone przez ustawodawcę europejskiego, czemu dano wyraz literalnie w treści dyrektywy 2019/1937, gdzie wskazano, że „zgłaszając naruszenia prawa Unii, które są szkodliwe dla interesu publicznego, osoby takie działają jako sygnaliści i tym samym odgrywają kluczową rolę w ujawnianiu takich naruszeń i zapobieganiu im oraz w ochronie dobra społecznego”[45]. Konstatacja ta przenosi nas z kolei do zagadnienia ewolucji roli „sygnalistów” w kontekście technologii cyfrowych, gdzie konieczne zdaje się odwołanie do truizmu, iż tym, co w istocie czyni rolę sygnalistów kluczową przy ujawnianiu i zapobieganiu naruszeń, a także stanowi zasadniczy element wspomnianego już minimum cech wymaganych do zakwalifikowania osoby jako „sygnalisty”, pozostaje „informacja”. Znalazło to odzwierciedlenie w dyrektywie 2019/1937 poprzez stwierdzenie, że „osoby pracujące dla organizacji publicznej lub prywatnej, lub utrzymujące kontakt z taką organizacją w związku ze swoją działalnością zawodową niejednokrotnie jako pierwsze dowiadują się o zagrożeniach, lub szkodach dla interesu publicznego, do jakich dochodzi w tym kontekście”[46]. *Prima facie* zdawać się może, iż tak błahe stwierdzenie nie może stanowić żadnego wkładu do dyskursu w zakresie omawianej tematyki, lecz w sposób przejrzysty obrazuje ono zarzewie ewolucji roli sygnalisty w kontekście

[42] J. Jankowski, J. Karski, *Raport tajnego emisariusza*, Kraków 2019, s. 222.

[43] A. Becker, *Messengers of Disaster: Raphael Lemkin, Jan Karski, and Others*, „Journal of Holocaust Studies” 2017, s. 114.

[44] *Epidemia w więzieniu? „Winny” sygnalista*, https://www.rp.pl/sluzby/art8644921-epidemia-w-wiezieniu-winny-sygnalista/ [dostęp: 30.08.2024].

[45] Zob. Preambuła dyrektywy 2019/1937 motyw 1.

[46] *Ibidem*.

technologii cyfrowych, albowiem o ile rola ta już w przeszłości istotnie oddziaływała na społeczeństwo, o tyle w dobie społeczeństwa informacyjnego oddziaływanie to ulega zasadniczej intensyfikacji.

Warto w tym miejscu przypomnieć, że pojęcie „społeczeństwo informacyjne" odnosi się do idei, iż informacja staje się centralnym zasobem, decydującym o rozwoju gospodarczym, społecznym i kulturalnym. Już w latach 60. XX w. japońscy badacze dostrzegli, że w wyniku postępu technologicznego i rosnącego znaczenia technologii informacyjnych społeczeństwo zaczyna ewoluować w kierunku, w którym informacja staje się kluczowym czynnikiem produkcji, obok pracy i kapitału[47]. Zrozumienie tej zmiany pozwala na lepsze uchwycenie roli sygnalistów w nowym, cyfrowym ekosystemie, gdzie sygnalista nie jest już jedynie osobą przekazującą istotne informacje na temat naruszeń, lecz staje się on także istotnym elementem obiegu informacji, której wartość nieustannie wzrasta. Informacja, będąca trzonem gospodarki opartej na wiedzy, zyskuje szczególną wagę w erze cyfrowej, gdzie dostęp do niej oraz jej właściwe zarządzanie mogą decydować o sukcesie lub porażce zarówno jednostek, jak i całych organizacji. Technologie cyfrowe, takie jak AI, *blockchain* czy *big data*, które rozwijały się równolegle z koncepcją społeczeństwa informacyjnego, przynoszą nowe wyzwania i możliwości w zakresie ochrony sygnalistów, ponieważ z jednej strony umożliwiają lepsze zabezpieczenie zgłoszeń oraz potencjalne zachowanie anonimowości, a z drugiej stawiają przed nami wyzwania związane z bezpieczeństwem danych, ich niezmiennością oraz odpowiedzialnością za decyzje podejmowane przez systemy algorytmiczne. W erze cyfrowej rola sygnalistów, choć zasadniczo opiera się na tych samych zasadach, to zyskuje jednak nowe, nieznane dotąd wymiary. O ile w przeszłości zakres działań sygnalistów ulegał zasadniczemu zawężeniu i to od czynników zewnętrznych zależała skala wpływu przekazywanych przez nich informacji, o tyle w dobie globalnych sieci informacyjnych sygnaliści samodzielnie mogą działać na skalę międzynarodową, przekazując informacje, które *per se* mogą wpłynąć na decyzje polityczne, gospodarcze, a nawet społeczne na całym świecie. Jednocześnie jednak rosnąca rola informacji w gospodarce stawia ich w jeszcze bardziej niebezpiecznej pozycji, narażając na represje zarówno ze strony organizacji, jak i rządów, co z kolei wymaga stosowania równie zaawansowanych środków ochrony, których tempo rozwoju musi co najmniej dorównywać tempu rozwoju technologii informa-

[47] K.J. Fietkiewicz, *The Development of Information Society in Japan: A Case Study of 21 Metropolitan Areas*, 2019, s. 3–5.

cyjnych. Dlatego tak ważne jest, aby prawo nadążało za omawianymi zmianami, oferując skuteczną ochronę i wsparcie dla tych, którzy decydują się ujawnić informacje na temat nieprawidłowości.

Podsumowując, ewolucja roli sygnalistów w erze cyfrowej odzwierciedla głębsze zmiany w strukturze społeczeństwa informacyjnego. W miarę jak informacja staje się centralnym zasobem naszej epoki, rośnie także znaczenie sygnalistów, którzy chronią jej integralność i przejrzystość. W tym kontekście sygnaliści nie tylko ujawniają naruszenia, ale również odgrywają kluczową rolę w kształtowaniu społeczeństwa przyszłości, w którym informacja jest nie tylko cennym zasobem, ale także narzędziem służącym do budowania bardziej sprawiedliwego i przejrzystego świata.

2. Rewolucja w zakresie ochrony sygnalistów i kanałów zgłaszania oraz towarzyszące im wyzwania prawodawcze w erze cyfrowej

Rewolucja cyfrowa, której jesteśmy świadkami, znacząco wpłynęła na niemal wszystkie aspekty życia społecznego i gospodarczego, w tym na oczekiwania wobec tego, w jaki sposób rewolucji tej sprosta prawo. O ile więc w kontekście ochrony sygnalistów osoby zgłaszające naruszenia doświadczają zarówno nowych możliwości, jak i wyzwań, o tyle po stronie ustawodawcy rozwój technologii cyfrowych sprowadza się przede wszystkim do wyzwań, z jakimi musi się zmierzyć. W odpowiedzi na te zmiany, zarówno na poziomie unijnym, jak i krajowym, wprowadzane są nowe regulacje, które mają na celu ochronę osób zgłaszających nieprawidłowości, i choć prawo chroniące sygnalistów jest stosunkowo nowym zjawiskiem w systemach prawnych na świecie, to idea ochrony tych, którzy odważają się zgłaszać naruszenia prawa, ma już swoje korzenie w poprzednich wiekach. W Stanach Zjednoczonych Ameryki namiastka przepisów z zakresu ochrony sygnalistów znalazła formalne odzwierciedlenie już w XVIII w., a to wraz z uchwaleniem ustawy *False Claims Act* w 1863 r.[48], która miała na celu walkę z korupcją i nadużyciami w czasie wojny secesyjnej. *False Claims Act* nie tylko chroniła sygnalistów, ale również oferowała im odszkodowania za ujawnienie nieprawidłowości, co miało na celu zachęcanie do zgłaszania przypadków oszustw. Kolejny wiek przyniósł dalszy rozwój ochrony prawnej sygnalistów w USA, którego owocami były m.in. takie

[48] *The False Claims Act*, https://www.justice.gov/civil/false-claims-act/ [dostęp: 30.08.2024].

ustawy, jak: *Lloyd–La Follette Act* z dnia 24 sierpnia 1912 r.[49], *Solid Waste Disposal Act* z dnia 20 października 1965 r.[50], czy *Whistleblower Protection Act* z dnia 10 kwietnia 1998 r.[51] W Europie prawo chroniące sygnalistów miało dotychczas wymiar epizodyczny[52] i zaczęło zyskiwać na znaczeniu w latach 90., czego przykładem jest *Public Interest Disclosure Act*, który wszedł w życie w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej 2 lipca 1998 r.[53]

W Polsce ochrona sygnalistów, jako formalne zagadnienie prawne, zaczęła zyskiwać na znaczeniu stosunkowo późno. W czasach Polskiej Rzeczpospolitej Ludowej (RPL) system prawny był ściśle kontrolowany przez władze komunistyczne, co sprawiało, że formalne mechanizmy ochrony sygnalistów (w przedmiotowym znaczeniu, które należy odróżnić od zjawiska denuncjacji władzom PRL) były ograniczone. Po upadku komunizmu w 1989 r. Polska weszła na ścieżkę transformacji ustrojowej, jednak formalna ochrona sygnalistów jako osobna kategoria i zagadnienie prawne nadal nie występowała. Współczesny rozwój prawa chroniącego sygnalistów w Polsce jest ściśle związany ze wdrażaniem dyrektywy 2019/1937, która stała się podstawą dla u.o.s. i była kluczowym krokiem w ustanowieniu nowoczesnych mechanizmów ochrony sygnalistów w Polsce.

Nie będzie chyba przesadą stwierdzenie, że dyrektywa 2019/1937 stanowi podwalinę dla próby uporania się z jednym z najbardziej aktualnych wyzwań Unii Europejskiej (UE), jakim jest problem ochrony sygnalistów. W czasach dynamicznych zmian technologicznych, globalizacji oraz rosnącej świadomości społecznej konieczność wprowadzenia jednolitych standardów ochrony dla osób zgłaszających naruszenia prawa stała się nieodzownym elementem wzmocnienia rządów prawa i demokracji w państwach członkowskich UE. Prace nad dyrektywą 2019/1937

---

[49] *Lloyd-La Follette Act of 1912*, https://whistleblower.house.gov/resources/all-resources/committee-jurisdiction-tool/whistleblowing-executive-branch-employee/lloyd-la-follette-act-1912/ [dostęp: 30.08.2024].

[50] *Filing Whistleblower Complaints Under the Solid Waste Disposal Act*, https://www.osha.gov/sites/default/files/publications/OSHA3815.pdf/ [dostęp: 30.08.2024].

[51] *Whistleblower Protections – Rights Of Employees [5 U.s.c. §2302 (B)(8)]*, https://www.americorps.gov/sites/default/files/document/2021_08_27_Whistleblower_Rights_Employees_OGC.pdf/ [dostęp: 30.08.2024].

[52] D. Huseynova, K. Piperigos, *Justice for justice: Protecting whistleblowers in the EU protection of whistleblowers – the why and the how*, http://transparency.eu/wp-content/uploads/2018/04/WB_Transparency-Group-CoE-17-18.pdf, *cit. per* B. Baran, 1. *Wprowadzenie*, [w:] B. Baran, M. Ożóg (red.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Warszawa 2021.

[53] *Guidance Whistleblowing and the Public Interest Disclosure Act 1998 (c.23) (accessible version)*, https://www.gov.uk/government/publications/whistleblowing-and-the-public-interest-disclosure-act-1998-c23/whistleblowing-and-the-public-interest- disclosure-act-1998-c23-accessible-version/ [dostęp: 30.08.2024].

zostały zainicjowane w odpowiedzi na rosnące zapotrzebowanie na jednolite standardy ochrony sygnalistów w UE, ponieważ wcześniejsze regulacje w tym zakresie były fragmentaryczne i różniły się w zależności od państwa członkowskiego. Niektóre kraje wprowadziły już wcześniej kompleksowe przepisy chroniące sygnalistów, podczas gdy inne państwa członkowskie miały jedynie ograniczone ramy prawne, które nie gwarantowały pełnej ochrony przed działaniami odwetowymi[54]. Dyrektywa 2019/1937 powstała więc z myślą o zniwelowaniu tych różnic.

Celem dyrektywy 2019/1937 jest przede wszystkim ustanowienie minimalnych standardów ochrony sygnalistów w całej UE i w tym celu zobowiązuje ona państwa członkowskie do wprowadzenia przepisów krajowych, które będą chronić osoby zgłaszające naruszenia prawa UE przed działaniami odwetowymi oraz zapewnią im dostęp do skutecznych mechanizmów zgłaszania nieprawidłowości. Dyrektywa 2019/1937 obejmuje szeroki zakres naruszeń, które mogą być zgłaszane przez sygnalistów. Zgodnie z art. 2 ust. 1 dyrektywy 2019/1937 ma ona zastosowanie do zgłoszeń dotyczących naruszeń przepisów UE w takich dziedzinach jak: zamówienia publiczne, usługi finansowe, bezpieczeństwo produktów, ochrona środowiska, ochrona zdrowia publicznego, ochrona konsumentów, ochrona prywatności i danych osobowych oraz bezpieczeństwo sieci i systemów informatycznych. Jednym z najważniejszych postanowień dyrektywy 2019/1937 jest obowiązek wprowadzenia przez państwa członkowskie UE efektywnych i bezpiecznych mechanizmów zgłaszania naruszeń prawa[55]. Art. 7 dyrektywy 2019/1937 zobowiązuje państwa członkowskie do zapewnienia, że osoby mające wiedzę o naruszeniach będą mogły je zgłaszać zarówno wewnętrznie, jak i zewnętrznie. Wewnętrzne kanały zgłaszania (art. 8 dyrektywy 2019/1937) muszą być dostępne dla wszystkich pracowników oraz innych osób związanych zawodowo z organizacją, np. kontrahentów czy stażystów. Pracodawcy mają obowiązek ustanowienia wewnętrznych procedur, które umożliwią sygnalistom zgłaszanie naruszeń w sposób poufny i zabezpieczający przed ujawnieniem ich tożsamości. Zewnętrzne kanały zgłaszania (art. 10 dyrektywy 2019/1937) powinny być ustanowione przez odpowiednie organy publiczne, które będą przyjmować zgłoszenia dotyczące naruszeń prawa UE. Te organy muszą także zapewnić, że informacje zgłaszane przez sygnalistów będą chronione i że sygnaliści nie będą narażeni na żadne formy represji z tego tytułu. Dyrektywa 2019/1937 wprowadza także bezwzględny zakaz działań odwetowych wobec sygnalistów (art. 19 dyrekty-

[54] J. Murszewski, *Problemy implementacji dyrektywy 2019/1937 do polskiego porządku prawnego*, [w:] B. Baran, M. Ożóg (red.), *op. cit*.

[55] *Ibidem*.

wy 2019/1937). Działania te mogą obejmować różnorodne formy represji, od zwolnienia z pracy, przez degradację, po subtelniejsze formy nacisku, jak np. pogorszenie warunków pracy czy odmowa awansu. Dyrektywa 2019/1937 wymaga, aby państwa członkowskie UE wprowadziły przepisy gwarantujące ochronę sygnalistów przed takimi działaniami, a także umożliwiły im dochodzenie swoich praw w przypadku, gdyby doszło do naruszenia tych przepisów. Nakłada ona także na państwa członkowskie UE obowiązek zapewnienia, że tożsamość sygnalistów będzie chroniona na każdym etapie procesu zgłaszania i rozpatrywania naruszeń. Poufność danych sygnalistów ma kluczowe znaczenie dla skuteczności mechanizmów zgłaszania, ponieważ obawa przed ujawnieniem tożsamości może skutecznie zniechęcać do zgłaszania nieprawidłowości (art. 16 dyrektywy 2019/1937). Zgodnie z art. 17 dyrektywy 2019/1937 państwa członkowskie UE muszą również wprowadzić odpowiednie środki ochrony danych osobowych sygnalistów, zgodnie z ogólnymi przepisami o ochronie danych, takimi jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Ochrona ta obejmuje zarówno dane osobowe sygnalistów, jak i wszelkie informacje, które mogłyby prowadzić do ich identyfikacji.

Proces implementacji dyrektywy 2019/1937 w państwach członkowskich UE napotkał liczne wyzwania. W Polsce prace nad implementacją dyrektywy 2019/1937 rozpoczęły się dopiero pod koniec 2021 r., co spowodowało znaczące opóźnienia względem harmonogramu narzuconego przez dyrektywę 2019/1937. Ostatecznie wejście w życie przepisów u.o.s. przypadło na dzień 25 września 2024 r. i regulują one szeroki zakres kwestii związanych z ochroną osób zgłaszających naruszenia prawa. Ustawa ta, zgodnie z art. 1 u.o.s., reguluje m.in. warunki objęcia ochroną sygnalistów, środki ochrony przed działaniami odwetowymi, zasady ustalania wewnętrznych procedur zgłaszania naruszeń oraz zadania Rzecznika Praw Obywatelskich w tym zakresie. Ustawa o ochronie sygnalistów definiuje także pojęcia kluczowe dla jej stosowania, takie jak „działanie odwetowe", „informacja o naruszeniu prawa" czy „kontekst związany z pracą" (art. 2 u.o.s.). Ustawa wprowadza obowiązek ustanowienia przez pracodawców wewnętrznych procedur zgłaszania naruszeń, które muszą być zgodne z wymogami określonymi w ustawie. Zgodnie z art. 8 u.o.s. procedury te muszą być transparentne, dostępne i zapewniać poufność zgłoszeń. Pracodawcy są zobowiązani do informowania pracowników o dostępnych kanałach zgłaszania oraz o przysługujących im prawach. W kontekście zgłoszeń zewnętrznych art. 10 u.o.s. nakłada obowiązek przyjmowania takich zgłoszeń przez odpowiednie organy publiczne, które są zobowiązane do ich rozpatrywania w sposób bezstronny i rzetelny. Ustawa o ochronie sygnalistów przewiduje także możliwość dokonania tzw. ujaw-

nienia publicznego, które może nastąpić, jeśli zgłoszenie wewnętrzne lub zewnętrzne nie przyniosło oczekiwanego rezultatu, a naruszenie prawa stanowi bezpośrednie zagrożenie dla interesu publicznego (art. 51 u.o.s.). Kluczowym elementem ustawy są przepisy dotyczące ochrony sygnalistów przed działaniami odwetowymi. Art. 11 u.o.s. wprowadza zakaz podejmowania jakichkolwiek działań odwetowych wobec sygnalistów, a także prób lub groźby zastosowania takich działań. Sygnaliści, którzy doświadczą działań odwetowych, mają prawo do odszkodowania, którego wysokość nie może być niższa niż przeciętne miesięczne wynagrodzenie w gospodarce narodowej (art. 14 u.o.s.). Ustawa przewiduje także możliwość zadośćuczynienia za szkody niematerialne, takie jak naruszenie dóbr osobistych sygnalisty.

Już na pierwszy rzut oka samo wyliczenie kwestii objętych ustawą o ochronie sygnalistów wskazuje na stosunkowo szerokie uregulowanie tej problematyki, lecz w kontekście rosnącej liczby regulacji dotyczących ochrony danych osobowych oraz ochrony sygnalistów widoczny staje się brak pełnej harmonizacji między kluczowymi aktami prawnymi UE i Rzeczpospolitej Polskiej (RP). 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, RODO)[56], ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[57] oraz ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów stawiają przed praktykami prawa i przedsiębiorstwami wyzwania, które mogą prowadzić do poważnych problemów z interpretacją i wdrażaniem odpowiednich procedur. Celem RODO jest zapewnienie wysokiego poziomu ochrony danych osobowych oraz ujednolicenie przepisów dotyczących ich przetwarzania na poziomie UE. Z drugiej strony u.o.s. wdraża do polskiego porządku prawnego dyrektywę 2019/1937, której celem jest ochrona osób zgłaszających naruszenia prawa, tzw. sygnalistów. Podczas gdy RODO koncentruje się na ochronie prywatności i danych osobowych, u.o.s. ma na celu zapewnienie bezpieczeństwa i ochrony osobom, które ujawniają nieprawidłowości, często narażając się na działania odwetowe. W praktyce oba te akty prawne mogą się wzajemnie przenikać, co prowadzi do licznych wyzwań związanych z ich wdrażaniem. Jednym z kluczowych punktów styku pomiędzy RODO a u.o.s. jest przetwarzanie danych osobowych w ramach systemów zgłoszeń. Przepisy u.o.s. wymagają, aby organizacje ustanowiły procedury umożli-

[56] Dz. Urz. UE L 119 z 2016 r. (dalej: „RODO").
[57] Dz. U. z 2019 r. poz. 1781 (dalej: „u.o.d.o.").

wiające zgłaszanie naruszeń prawa, które mogą zawierać dane osobowe, zarówno sygnalistów, jak i osób, których dotyczy zgłoszenie. Jak stanowi art. 5 RODO, przetwarzanie danych osobowych powinno być zgodne z zasadami legalności, rzetelności i przejrzystości, a także ograniczone do niezbędnego minimum. Jednak art. 4 ust. 3 u.o.s. pozwala na przetwarzanie danych osobowych w zakresie niezbędnym do realizacji celów zgłoszenia bez konieczności informowania osoby, której dane dotyczą, o ich przetwarzaniu, co w normalnych warunkach byłoby wymagane przez RODO, a to zgodnie z art. 13 i 14 RODO. Takie odstępstwo ma na celu ochronę sygnalistów i osób zaangażowanych w proces zgłaszania przed potencjalnymi działaniami odwetowymi. Mimo że takie rozwiązanie jest uzasadnione z punktu widzenia ochrony sygnalistów, może prowadzić do konfliktów z zasadami ochrony danych osobowych ustanowionymi przez RODO.

Co więcej, zgodnie z art. 14 RODO administrator danych osobowych jest zobowiązany do poinformowania osoby, której dane dotyczą, o przetwarzaniu jej danych, co stanowi kluczowy element zapewniający transparentność przetwarzania danych osobowych. W kontekście u.o.s. ten obowiązek informacyjny może jednak kolidować z potrzebą zapewnienia anonimowości i bezpieczeństwa sygnalistom. Co prawda w art. 14 ust. 5 lit. b RODO przewidziano możliwość wyłączenia obowiązku informacyjnego, jeśli jego realizacja mogłaby uniemożliwić lub poważnie utrudnić osiągnięcie celów przetwarzania danych. W praktyce oznacza to, że organizacje korzystające z przepisów u.o.s. mogą nie być zobowiązane do informowania osób, których dane dotyczą, o ich przetwarzaniu, jeśli mogłoby to narazić sygnalistę na działania odwetowe, jednakże brak jednoznaczności w stosowaniu tych przepisów może prowadzić do niepewności prawa. Przykładowo, jeśli zgłoszenie dotyczy poważnych naruszeń, takich jak korupcja, przestępstwa finansowe czy mobbing, organizacja musi balansować między obowiązkiem ochrony danych osobowych a potrzebą zapewnienia bezpieczeństwa sygnalistom. W praktyce decyzje te mogą prowadzić do różnic interpretacyjnych i potencjalnych naruszeń przepisów RODO.

Kolejnym aspektem, który wymaga uwagi, jest przetwarzanie danych wrażliwych, takich jak informacje o stanie zdrowia, orientacji seksualnej czy przynależności do związków zawodowych, które mogą być częścią zgłoszenia sygnalisty. Art. 9 ust. 1 RODO generalnie zakazuje przetwarzania takich danych, chyba że spełnione są określone warunki, jak np. wyraźna zgoda osoby, której dane dotyczą, lub jeśli przetwarzanie jest niezbędne do ochrony interesów publicznych. Natomiast u.o.s. nie precyzuje jednoznacznie, w jaki sposób takie dane powinny być przetwarzane w kontekście zgłoszeń. W praktyce oznacza to, że administratorzy

danych muszą podejmować *ad hoc* decyzje, które mogą nie być zgodne z wymogami RODO. Może to prowadzić do sytuacji, w których dane wrażliwe są przetwarzane w sposób, który narusza przepisy RODO, co z kolei może skutkować nałożeniem kar na organizację. Kolejnym wyzwaniem jest rozbieżność terminologiczna i proceduralna pomiędzy RODO a ustawą o ochronie sygnalistów. Przykładowo podczas gdy RODO posługuje się pojęciami takimi jak „administrator danych", „podmiot przetwarzający" czy „osoba, której dane dotyczą", u.o.s. wprowadza swoje pojęcia, takie jak „sygnalista" czy „zgłoszenie". Takie różnice, mimo że z perspektywy każdego z tych aktów z osobna zdawać się mogą zasadne, to mogą prowadzić do nieporozumień w interpretacji przepisów oraz trudności w ich praktycznym zastosowaniu. Co więcej, u.o.s. wprowadza specyficzne procedury zgłoszeń, które mogą kolidować z obowiązkami wynikającymi z RODO. Przykładowo art. 6 ust. 1 u.o.s. przewiduje, że zgłoszenia powinny być przyjmowane i rozpatrywane w sposób zapewniający maksymalną poufność, jednakże RODO wymaga, aby przetwarzanie danych osobowych odbywało się w sposób przejrzysty i zrozumiały dla osób, których dane dotyczą (art. 12 RODO). Te dwie zasady mogą być trudne do pogodzenia w praktyce, co już obecnie prowadzi do dylematów, jak zapewnić zgodność z obiema regulacjami.

Brak pełnej harmonizacji między tymi aktami prawnymi może prowadzić do różnic interpretacyjnych na poziomie krajowym i europejskim, bowiem państwa członkowskie UE mają możliwość dostosowania swoich przepisów krajowych do wymogów zarówno RODO, jak i dyrektywy 2019/1937, a różnice te mogą prowadzić do niejasności i niejednolitości w stosowaniu prawa. Brak harmonizacji pomiędzy RODO a u.o.s. stawia natomiast szereg poważnych wyzwań przed praktykami, a wiążące się z nimi ewentualne konsekwencje mogą mieć wymiar nie tylko prawny, lecz także finansowy. W tej sytuacji w celu minimalizacji ryzyka organizacje już obecnie powinny podejmować działania mające na celu zapewnienie zgodności z obiema regulacjami.

Konfrontując wskazane prawodawcze trudności w zakresie implementacji i harmonizacji przepisów z problematyką rozwoju technologii cyfrowych, stwierdzić należy, iż te spowodowały prawdziwą rewolucję w obszarze kanałów zgłaszania naruszeń. Tradycyjne formy zgłaszania, takie jak bezpośrednie raportowanie przełożonym czy korzystanie z linii telefonicznych, coraz częściej ustępują miejsca bardziej zaawansowanym technologicznie systemom, które oferują wyższy poziom anonimowości, bezpieczeństwa i efektywności. Nowoczesne kanały zgłaszania wykorzystują takie technologie jak AI, *blockchain*, a także różnorodne aplikacje mo-

bilne i internetowe, które wspierają sygnalistów w zgłaszaniu naruszeń w sposób bezpieczny i dyskretny. Tradycyjne kanały zgłaszania naruszeń miały istotne ograniczenia, w tym chociażby były narażone na brak poufności, co z kolei potęgowało ryzyko represji sygnalistów, a tym samym rzutowało także na problemy z efektywnością i czasem reakcji przy zgłaszaniu nieprawidłowości. Ponadto w wielu przypadkach sygnaliści nie mieli pewności, czy ich zgłoszenie dotrze do właściwych osób i czy zostanie potraktowane w sposób należyty. Technologie cyfrowe umożliwiają poprawę jakości i bezpieczeństwa kanałów zgłaszania, czego przykładem mogą być chociażby anonimowe platformy internetowe (takie jak GlobaLeaks[58], SecureDrop[59], Falcony[60], Navex[61] czy BKMS System[62]), aplikacje mobilne z funkcjami szyfrowania (takie jak Signal[63], Tella[64], Haven[65] czy Orbot[66]) oraz narzędzia do zgłaszania oparte na *blockchain* (takich jak Diss-co[67] czy FixNix[68]), które pokazują, jak technologia może zrewolucjonizować proces zgłaszania naruszeń.

Jednym z bardziej innowacyjnych zastosowań technologii w kontekście zgłaszania naruszeń jest wykorzystanie AI (jak chociażby w przypadku produktu SpeakUp[69]), która pozwala analizować zgłoszenia, identyfikować wzorce sugerujące naruszenia oraz wspierać organizacje w szybszym i dokładniejszym reagowaniu na zgłoszenia. AI może także wspierać sygnalistów poprzez automatyzację procesów, takich jak wstępna ocena zgłoszenia czy filtrowanie informacji, co pozwala na bardziej efektywne zarządzanie zgłoszeniami w organizacjach. Jednakże zastosowanie AI pociąga za sobą także pewne wyzwania, które muszą być starannie zarządzane, aby unikać potencjalnych zagrożeń związanych z błędami algorytmów, dyskryminacją, a także naruszeniami prywatności i bezpieczeństwa. W tym kontekście kluczowe znaczenie mają normy, takie jak norma BS ISO/IEC 42001:2023[70] oraz regulacje, np. rozporządzenie Parlamentu Europejskiego i Rady

---

[58] Globaleaks, https://www.globaleaks.org/ [dostęp: 30.08.2024].
[59] Securedrop, https://securedrop.org/ [dostęp: 30.08.2024].
[60] Falcony, https://www.falcony.io/ [dostęp: 30.08.2024].
[61] Navex, https://www.navex.com/ [dostęp: 30.08.2024].
[62] EQS Group System BKMS, https://www.eqs.bkms-system.com/ [dostęp: 30.08.2024].
[63] Signal, https://signal.org/pl/ [dostęp: 30.08.2024].
[64] Tella, https://tella-app.org/ [dostęp: 30.08.2024].
[65] Guardianproject, Haven, https://guardianproject.github.io/haven/ [dostęp: 30.08.2024].
[66] Guardianproject, Orbot, https://orbot.app/en/ [dostęp: 30.08.2024].
[67] DISS-CO, https://diss-co.tech/ [dostęp: 30.08.2024].
[68] Fixnix, https://www.fixnix.co/ [dostęp: 30.08.2024].
[69] SpeakUp, https://www.speakup.com/ [dostęp: 30.08.2024].
[70] *ISO/IEC 42001:2023, Artificial Intelligence Management Systems – Requirements*, https://www.iso.org/standard/81230.html/ [dostęp: 30.08.2024].

(UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (tzw. akt w sprawie sztucznej inteligencji, AI Act)[71], które określają zasady i wymogi dotyczące projektowania, wdrażania oraz monitorowania systemów AI. Algorytmy AI muszą być starannie zaprojektowane, aby uniknąć błędów, które mogą prowadzić do fałszywych oskarżeń lub ignorowania ważnych zgłoszeń. Według standardu ISO/IEC 42001:2023 organizacje muszą wdrożyć kompleksowy proces zarządzania ryzykiem, który obejmuje ocenę wpływu AI na różne aspekty działalności, w tym ryzyko związane z błędami algorytmicznymi i ich konsekwencjami. Ponadto zgodnie z klauzulą A.2.4 BS ISO/IEC 42001 organizacje powinny regularnie przeglądać i aktualizować politykę AI, aby zapewnić jej ciągłą adekwatność i skuteczność w świetle zmieniających się technologii i wymagań biznesowych.

Zapewnienie przejrzystości decyzji podejmowanych przez AI jest kluczowe, aby budować zaufanie i spełniać wymagania prawne. Przykładowo AI Act kładzie silny nacisk na konieczność projektowania systemów AI w sposób zapewniający ich przejrzystość[72] oraz nakłada na dostawców systemów AI obowiązek dostarczenia szczegółowej dokumentacji technicznej, która umożliwia zrozumienie sposobu działania algorytmów oraz umożliwia ocenę ich zgodności z wymaganiami prawnymi[73]. Dokumentacja ta powinna zawierać informacje o architekturze systemu, użytych danych, metodach testowania oraz procedurach walidacji, co pozwala na dokładne monitorowanie i kontrolę systemu w trakcie jego użytkowania. Kolejnym ważnym aspektem przy wykorzystaniu technologii AI jest zarządzanie ryzykiem i zgodność z etyką. Norma BS ISO/IEC 42001:2023 wskazuje, że organizacje muszą uwzględniać aspekty etyczne na każdym etapie cyklu życia systemu AI, od jego projektowania po wdrożenie i użytkowanie[74]. Systemy AI powinny być projektowane w sposób minimalizujący ryzyko dyskryminacji oraz zapewniający zgodność z przepisami dotyczącymi ochrony danych osobowych, takimi jak przepisy RODO. AI Act dodatkowo podkreśla konieczność nadzoru nad systemami AI tak, aby zapobiec potencjalnym naruszeniom praw człowieka i zapewnić ich zgodność z obowiązującymi standardami etycznymi oraz zapewniać przejrzystość działań, oraz chronić prawa i interesy wszystkich zainteresowanych stron[75].

---

[71] Dz. Urz. UE L 1689 z 2024 r. (dalej: „AI Act").
[72] Zob. art. 13 AI Act.
[73] Zob. art. 16 AI Act.
[74] Zob. B.6.1.2 oraz B.9.3. normy BS ISO/IEC 42001:2023.
[75] Zob. art. 14 AI Act.

Technologia *blockchain*, znana powszechnie przede wszystkim za sprawą fenomenu popularności kryptowalut, znalazła swoje zastosowanie również w kontekście ochrony sygnalistów. *Blockchain* oferuje zaawansowaną architekturę umożliwiającą tworzenie zdecentralizowanych rejestrów, które charakteryzują się niezmiennością oraz wysokim poziomem przejrzystości i bezpieczeństwa. Mechanizm działania *blockchain* opiera się na rozproszonej sieci komputerów (tzw. węzłów), z których każdy posiada kopię tego samego rejestru. Każda nowa transakcja, zgłoszenie czy wpis do tego rejestru muszą zostać zatwierdzone przez konsensus większości węzłów, co uniemożliwia jednostronne wprowadzanie zmian w danych, zapewniając ich integralność. Niezmienność danych w *blockchain* jest zapewniona przez algorytmy kryptograficzne, które tworzą unikalny identyfikator (ang. *hash*) dla każdej operacji. Gdy operacja (zapis) zostaje dodana do bloku, jest on kryptograficznie powiązany z poprzednim blokiem, tworząc w ten sposób łańcuch bloków (ang. *blockchain*). Zmiana któregokolwiek z wcześniejszych bloków wymagałaby zmodyfikowania wszystkich kolejnych bloków w łańcuchu oraz uzyskania zgody większości węzłów, co jest praktycznie niemożliwe do osiągnięcia bez wykrycia[76]. Dzięki *blockchain* sygnaliści mogą mieć pewność, że ich zgłoszenie nie zostanie zmanipulowane ani usunięte, co jest kluczowe dla zachowania zaufania do systemów zgłaszania. Pomimo licznych zalet *blockchain* niesie ze sobą także pewne wyzwania. Wdrożenie tej technologii wymaga znacznych zasobów[77], a także specjalistycznej wiedzy, co może być barierą dla mniejszych organizacji. Ponadto pojawiają się pytania dotyczące skalowalności i zgodności z przepisami o ochronie danych osobowych, zwłaszcza w kontekście unijnych przepisów RODO.

Mając na uwadze wskazane spostrzeżenia, nie będzie stanowić nadużycia stwierdzenie, że jednym z największych wyzwań w kontekście nowoczesnych kanałów zgłaszania naruszeń przez sygnalistów jest zapewnienie im bezpieczeństwa i anonimowości. Chociaż technologie cyfrowe oferują zaawansowane narzędzia szyfrowania i ochrony danych, nie eliminują one całkowicie ryzyka naruszeń prywatności. W erze cyfrowej, gdzie inwigilacja i gromadzenie danych są na porządku dziennym, sygnaliści mogą czuć się niepewnie, czy ich zgłoszenia rzeczywiście pozostaną anonimowe i bezpieczne. Oprócz technologii kluczowe znaczenie ma

[76] Z. Zheng *et al.*, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, [w:] *2017 IEEE 6th International Congress on Big Data, IEEE Computer Society*, 2017, s. 557–559.

[77] P. Sharma, R. Jindal, M. D. Borah, *A Review of Blockchain-Based Applications and Challenges*, [w:] *Wireless Personal Communications*, 2022, s. 1201–1243.

także kultura organizacyjna i odpowiednie szkolenie personelu odpowiedzialnego za obsługę zgłoszeń. Właściwe zarządzanie systemami zgłoszeń, a także regularne audyty bezpieczeństwa są niezbędne do zapewnienia, że sygnaliści będą mieli zaufanie do nowoczesnych kanałów zgłaszania. Szczególnie istotne pozostaje więc, aby technologie wykorzystywane w kanałach zgłaszania były zgodne z obowiązującymi przepisami prawa, w tym wspomnianymi już przepisami RODO, u.o.d.o., AI Act, dyrektywy 2019/1937 czy u.o.s., dlatego też wdrożenie systemów opartych na AI czy *blockchain* wymaga każdorazowo szczegółowej analizy prawnej, aby zapewnić zgodność z wymogami dotyczącymi ochrony danych, poufności oraz odpowiedzialności.

Rozwój technologii cyfrowych i ich integracja z systemami ochrony sygnalistów wymaga też ciągłej aktualizacji i harmonizacji przepisów prawnych. W miarę jak technologie takie jak AI i *blockchain* stają się coraz bardziej powszechne, konieczne jest dostosowanie przepisów prawnych, aby zapewnić ich skuteczność i zgodność z dynamicznie zmieniającym się otoczeniem technologicznym. W tym kontekście ustawodawcy muszą podejmować działania mające na celu stworzenie elastycznych ram prawnych, które będą mogły reagować na nowe wyzwania wynikające z postępu technologicznego. Harmonizacja przepisów na poziomie międzynarodowym jest również kluczowa, aby zapewnić spójność regulacji dotyczących ochrony sygnalistów w różnych jurysdykcjach. W dobie globalizacji sygnaliści mogą działać na różnych rynkach i w różnych systemach prawnych, co wymaga rozwijania i popularyzowania międzynarodowych standardów ochrony, które będą uwzględniać specyfikę cyfrowego środowiska. Przyszłość ochrony sygnalistów będzie więc zależała od zdolności ustawodawców do adaptacji przepisów prawnych do szybko zmieniającego się otoczenia technologicznego oraz od umiejętności organizacji w skutecznym wdrażaniu nowoczesnych systemów zgłaszania, które będą spełniać najwyższe standardy bezpieczeństwa i zgodności z przepisami. Z tej perspektywy szczególnie istotne jest także to, aby regulacje dotyczące ochrony sygnalistów nadążały za rozwojem technologicznym w ten sposób, aby na bieżąco chronić skutecznie sygnalistów w zmieniającym się otoczeniu technologicznym, co w obliczu zasadniczej dyferencji pomiędzy tempem rozwoju AI, liczonym w tygodniach i miesiącach a tempem implementacji prawodawstwa (czego przykładem może być wdrożenie u.o.s., która zgodnie z założeniami dyrektywy 2019/1937 powinna być wprowadzona przez kraje członkowskie UE do 17 grudnia 2021 r.) zdaje się pozostawać wciąż odległym ideałem.

3. Możliwości i perspektywy rozwoju problematyki

AI, która już teraz odgrywa kluczową rolę w wielu dziedzinach, ma potencjał, aby jeszcze bardziej zrewolucjonizować systemy zgłaszania naruszeń. Zaawansowane algorytmy AI mogą nie tylko analizować zgłoszenia i identyfikować potencjalne naruszenia, ale potencjalnie także przewidywać i zapobiegać przyszłym problemom na podstawie analizy wzorców danych. Takie podejście pozwoliłoby na bardziej proaktywne zarządzanie ryzykiem oraz szybsze i dokładniejsze reagowanie na zgłoszenia naruszeń. Jednakże wykorzystanie AI w kontekście ochrony sygnalistów stawia także wyzwania, zwłaszcza w zakresie transparentności i etyki. Algorytmy AI muszą być projektowane i wdrażane w sposób, który zapewnia uczciwość i równość, a także zgodność z przepisami prawa, w tym z zasadami ochrony danych osobowych. W sektorze publicznym AI może wspierać systemy zgłaszania naruszeń poprzez automatyzację procesów analizy zgłoszeń. Przykładowo chatbot zasilany AI może być wykorzystywany do automatycznego przyjmowania i wstępnej analizy zgłoszeń od pracowników i obywateli, co pozwoli na szybsze zidentyfikowanie kluczowych informacji i przekazanie ich do odpowiednich działów[78]. Takie rozwiązania nie tylko zwiększają efektywność, ale także redukują ryzyko błędów ludzkich. Systemy AI mogą analizować też treści zgłoszeń pod kątem słów kluczowych i tonacji, identyfikując potencjalnie krytyczne zgłoszenia, które wymagają natychmiastowej interwencji[79]. Tego typu analiza może być szczególnie użyteczna w dużych organizacjach, gdzie liczba zgłoszeń jest znaczna, a ręczne przetwarzanie wszystkich zgłoszeń byłoby nieefektywne, albo w organizacjach związanych z infrastrukturą krytyczną.

Technologia *blockchain*, znana z zapewnienia niezmienności i transparentności, ma ogromny potencjał w kontekście ochrony sygnalistów. Możliwość tworzenia niezmiennych rejestrów zgłoszeń może znacząco zwiększyć zaufanie do systemów zgłaszania naruszeń, zapewniając, że każde zgłoszenie zostanie odpowiednio zabezpieczone i pozostanie niezmienione. Systemy zgłaszania naruszeń mogą korzystać zarówno z publicznych, jak i prywatnych *blockchain*. Rejestry *blockchain* udostępniane za uprzednią zgodą (ang. *permissioned blockchain*) oferują większą

[78] Rynek komercyjny oferuje dostęp do takich rozwiązań, czego przykładem jest system UiPath, https://www.uipath.com/ [dostęp: 30.08.2024].

[79] H. Taherdoost, M. Madanchian, *Artificial Intelligence and Sentiment Analysis: A Review in Competitive Research*, https://doi.org/10.3390/computers12020037 [dostęp: 30.08.2024].

kontrolę nad tym, kto może uczestniczyć w sieci[80], co jest kluczowe w kontekście ochrony danych osobowych i poufności. Kontrakty inteligentne (ang. *smart contracts*) mogą automatyzować procesy związane ze zgłaszaniem naruszeń, takie jak przesyłanie zgłoszeń do odpowiednich organów, uruchamianie dochodzeń wewnętrznych czy powiadamianie sygnalistów o statusie ich zgłoszeń[81]. Z kolei wysoki poziom szyfrowania, w tym kryptografia asymetryczna (opierająca się na funkcjach jednokierunkowych, które da się łatwo wyliczyć w jedną stronę, ale bardzo trudno w drugą) i homomorficzna (będąca formą kryptografii klucza publicznego, która umożliwia komponowanie na zaszyfrowanych danych bez ich pierwszego deszyfrowania) pozwala na przyjęcie, że dane zgłaszających są chronione na każdym etapie przetwarzania[82]. W praktyce technologia *blockchain* może przykładowo ułatwić audyt i weryfikację procesów związanych ze zgłaszaniem, co jest kluczowe dla zapewnienia, że organizacje rzeczywiście realizują swoje zobowiązania w zakresie ochrony sygnalistów, może zapewnić anonimowość sygnalistów, chroniąc ich tożsamość przed ujawnieniem, co jest szczególnie ważne w przypadku zgłaszania nieprawidłowości w instytucjach rządowych. Użycie *blockchain* może zapewnić transparentność w procesach administracyjnych i medycznych, umożliwiając łatwiejsze monitorowanie zgłoszeń i ich przetwarzanie. Technologia *blockchain* może być stosowana do monitorowania aktywności w systemach IT i wykrywania anomalii, które mogą wskazywać na naruszenia. Jednakże, aby technologia *blockchain* mogła być w pełni wykorzystywana, konieczne jest przezwyciężenie kilku istotnych wyzwań. Po pierwsze, *blockchain* wymaga znacznych zasobów obliczeniowych i infrastrukturalnych, co może być barierą dla jego powszechnego wdrożenia. Ponadto technologia ta musi być zgodna z przepisami dotyczącymi ochrony danych osobowych, co w kontekście niezmienności danych może rodzić pewne problemy, np. w przypadku potrzeby usunięcia danych na żądanie osoby, której dotyczą.

Kolejnym obszarem, który ma potencjał do znacznego rozwoju, jest integracja systemów zgłaszania naruszeń z innymi technologiami cyfrowymi, takimi jak internet rzeczy (IoT). IoT to technologia, która umożliwia wzajemne połączenie i komu-

---

[80] M.J. Amiri, D. Agrawal, A. Abbadi, *Permissioned Blockchains: Properties, Techniques and Applications*, [w:] *SIGMOD '21: Proceedings of the 2021 International Conference on Management of Data*, 2021, s. 2813–2820.

[81] H. Taherdoost, *Smart Contracts in Blockchain Technology: A Critical Review*, [w:] *Information*, *2023*, https://www.mdpi.com/2078-2489/14/2/117/ [dostęp: 30.08.2024].

[82] C. Gentry, C.S. Halevi, *Homomorphic Encryption and its Applications. Cryptology ePrint Archive, Paper 2022/1602*, https://eprint.iacr.org/2022/1602.pdf/ [dostęp: 30.08.2024].

nikację różnorodnych urządzeń za pośrednictwem sieci internetowej[83]. W kontekście systemów zgłaszania naruszeń IoT może być wykorzystany do automatyzacji i monitorowania procesów, zwiększenia transparentności oraz poprawy ochrony sygnalistów. Możliwości te wynikają z właściwości IoT, takich jak ciągłe zbieranie danych, ich analiza w czasie rzeczywistym oraz zdolność do wykrywania anomalii w funkcjonowaniu systemów i procesów[84]. Integracja systemów zgłaszania naruszeń z IoT może przebiegać na kilku poziomach. Na poziomie operacyjnym IoT może monitorować działanie urządzeń i systemów w organizacji, zbierając dane, które mogą sugerować nieprawidłowości lub naruszenia. Przykładowo w systemach produkcyjnych IoT może monitorować zużycie energii przez maszyny, a nagłe i nieuzasadnione wzrosty zużycia mogą wskazywać na nieefektywne praktyki[85] czy nawet działania o charakterze przestępczym. Takie dane mogą być automatycznie przesyłane do systemu zgłaszania naruszeń, gdzie będą analizowane pod kątem potencjalnych nieprawidłowości. Na poziomie zarządzania IoT może wspierać sygnalistów poprzez anonimowe zbieranie dowodów na temat naruszeń, wykorzystując do tego np. czujniki dźwięku i obrazu, i tym samym dokumentowanie zdarzeń, które mogą później służyć jako dowody w procesie wewnętrznego dochodzenia. Jednym z kluczowych wyzwań związanych z integracją IoT z systemami zgłaszania naruszeń jest zapewnienie bezpieczeństwa danych. IoT, ze względu na swoją naturę, generuje ogromne ilości danych, które muszą być odpowiednio chronione przed nieautoryzowanym dostępem. W kontekście ochrony sygnalistów kluczowe jest zapewnienie, że dane dotyczące zgłaszania naruszeń są anonimowe i nie mogą zostać zidentyfikowane przez osoby niepowołane. Przykładem zastosowania IoT w systemach zgłaszania naruszeń może być monitorowanie zgodności z przepisami dotyczącymi ochrony środowiska. Czujniki IoT mogłyby być wykorzystywane do ciągłego monitorowania emisji zanieczyszczeń przez zakłady przemysłowe[86], przy czym byłyby one automatycznie przesyłane do systemu zgłaszania naruszeń, gdzie z kolei zostałyby porównywane z obowiązującymi normami prawnymi. W przypadku wykrycia przekroczenia dopuszczalnych poziomów system mógłby automatycznie wygene-

[83] *Internet Rzeczy (IoT) – Co to jest? Jak działa? Zastosowanie, przykłady*, https://cryps.pl/internet-rzeczy-iot-co-to-jest/ [dostęp: 30.08.2024].

[84] *Ibidem*.

[85] *Monitorowanie zużycia energii elektrycznej urządzeń przemysłowych – przykład wtryskarki FANUC. APA LAB*, https://apagroup.pl/apalab/jak-skutecznie-monitorowac-zuzycie-energii-elektrycznej-urzadzen-przemyslowych-przyklad-wtryskarki-fanuc/ [dostęp: 30.08.2024].

[86] *The Impact of Smart Sensors on Environmental Monitoring and Compliance*, https://fatfinger.io/the-impact-of-smart-sensors-on-environmental-monitoring-and-compliance/ [dostęp: 30.08.2024].

rować zgłoszenie naruszenia, co umożliwia szybkie podjęcie działań naprawczych. IoT może również zautomatyzować procesy zgłaszania naruszeń poprzez integrację z systemami ERP (ang. *Enterprise Resource Planning*) i CRM (ang. *Customer Relationship Management*). Przykładowo, w sektorze finansowym IoT mogłoby monitorować transakcje w czasie rzeczywistym i wykrywać anomalie, które mogłyby wskazywać na nieprawidłowości, takie jak pranie pieniędzy[87]. Takie podejście nie tylko prowadzi do zwiększenia efektywności systemów zgłaszania, ale także pozwala na szybkie reagowanie na potencjalne zagrożenia.

Innym jeszcze obszarem, którego rozwój rzutuje istotnie na omawianą problematykę, jest *big data*. Termin ten odnosi się do przetwarzania i analizy bardzo dużych zbiorów danych, które charakteryzują się dużą objętością, różnorodnością oraz szybkością napływu. W kontekście systemów zgłaszania naruszeń *big data* pozwala na integrację różnorodnych źródeł danych od wewnętrznych raportów pracowniczych, poprzez dane z monitoringu systemów IT, po publiczne bazy danych i media społecznościowe[88], a to celem zidentyfikowania wzorców, anomalii oraz potencjalnych zagrożeń. Przykładowo w przemyśle finansowym technologia *big data* może być wykorzystywana do monitorowania transakcji finansowych pod kątem prania pieniędzy oraz innych działań niezgodnych z prawem. Integracja systemów zgłaszania naruszeń z analizą danych pozwala na automatyczne wykrywanie podejrzanych transakcji na podstawie wzorców zachowań, które mogą wskazywać na działalność przestępczą. Systemy te mogą analizować setki tysięcy transakcji dziennie, identyfikując anomalie takie jak nietypowo duże przelewy, które następnie podlegają dalszej weryfikacji. Z kolei w sektorze opieki zdrowotnej *big data* może wspierać systemy zgłaszania naruszeń poprzez analizę danych pacjentów oraz danych operacyjnych szpitali w celu wykrywania potencjalnych nieprawidłowości, takich jak oszustwa związane z ubezpieczeniami zdrowotnymi, błędy medyczne czy naruszenia prywatności pacjentów. Na przykład analiza danych dotyczących przepisywania leków może ujawnić nieuzasadnione wzorce, takie jak nadmierne przepisywanie leków opioidowych, co może być wskazówką do złożenia zgłoszenia[89]. Natomiast

---

[87] *How Real-time Monitoring Changes the Game for Transaction Security*, https://www.flagright.com/post/how-real-time-monitoring-changes-the-game-for-transaction-security/ [dostęp: 30.08.2024].

[88] M.M. Alani, *Big data in cybersecurity: a survey of applications and future trends. Journal of Reliable Intelligent Environments*, „Journal of Reliable Intelligent Environments", https://www.researchgate.net/publication/348278146_Big_data_in_cybersecurity_a_survey_of_applications_and_future_trends [dostęp: 30.08.2024].

[89] P. Pandey, A. Saroliya, R. Kumar, *Analyses and Detection of Health Insurance Fraud Using Data Mining and Predictive Modeling Techniques*, [w:] *Advances in Intelligent Systems and Computing*, 2017, s. 41–49.

w administracji publicznej można wykorzystać *big data* do monitorowania zgodności z przepisami prawa i zapobiegania korupcji. Przykładem może być system zgłaszania naruszeń, który integruje dane z różnych źródeł, takich jak rejestry publiczne, przetargi czy audyty, aby wykrywać konflikty interesów, nieprawidłowości w zamówieniach publicznych czy inne działania korupcyjne[90].

W odpowiedzi na rozwój technologii cyfrowych ustawodawcy muszą być gotowi do dalszego rozwoju przepisów dotyczących ochrony sygnalistów, tak aby były one skuteczne w aktualnym środowisku technologicznym. Regulacje muszą uwzględniać specyfikę technologii takich jak AI i *blockchain* i tym samym chronić prawa osób korzystających z nowoczesnych systemów zgłaszania. Jednym z kluczowych aspektów przyszłych regulacji powinno być zapewnienie, że sygnaliści będą mieli dostęp do skutecznych mechanizmów ochrony niezależnie od technologii, z której korzystają. Ustawodawcy muszą również zadbać o to, aby regulacje były elastyczne i zdolne do adaptacji w obliczu przyszłych zmian technologicznych, co może wymagać regularnej aktualizacji przepisów oraz stworzenia mechanizmów monitorowania ich skuteczności, tylko bowiem w ten sposób można zapewnić, że ochrona sygnalistów pozostanie skuteczna i adekwatna do wyzwań, jakie stawia przed nami XXI w.

Wnioski

Zagadnienia związane z ochroną sygnalistów w erze cyfrowej są nie tylko aktualne, ale również niezwykle złożone. W miarę jak technologia rozwija się w coraz szybszym tempie, ustawodawcy, organizacje i sami sygnaliści zmuszeni są stawić czoła nowym wyzwaniom, które wymagają przemyślanych i zrównoważonych rozwiązań. Zaprezentowana w artykule pokrótce analiza wskazuje, że technologia cyfrowa, w szczególności AI i *blockchain*, ma potencjał do rewolucjonizowania systemów zgłaszania naruszeń. Dzięki zaawansowanym algorytmom AI możliwe jest automatyzowanie procesów zgłaszania i weryfikacji naruszeń, co zwiększa efektywność i dokładność tych procesów. *Blockchain* z kolei zapewnia niezmienność i przejrzystość zgłoszeń, co jest kluczowe dla budowania zaufania do systemów zgłaszania naruszeń. Jednakże wdrożenie tych technologii wiąże się z licznymi wyzwaniami. W szczególności kwestie odpowiedzialności prawnej za decyzje podejmowane przez systemy AI

[90] *Preventing Corruption in Procurement through Big Data*, https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2020/preventing-corruption-procurement-big-data.html [dostęp: 30.08.2024].

oraz zgodność z przepisami dotyczącymi ochrony danych osobowych pozostają nierozwiązane i wymagają dalszych badań oraz rozwoju regulacji. Dyrektywa 2019/1937 oraz u.o.s. stanowią znaczący krok naprzód w harmonizacji przepisów dotyczących ochrony sygnalistów w UE. Przepisy te nakładają na organizacje obowiązek wdrożenia skutecznych i bezpiecznych systemów zgłaszania, które muszą być zgodne z dynamicznie zmieniającym się środowiskiem technologicznym. W odpowiedzi na te regulacje organizacje muszą nie tylko dostosować swoje procedury, ale także zainwestować w nowe technologie, które wspierają ochronę sygnalistów.

Patrząc w przyszłość, nic nie wskazuje na to, aby tak dynamiczny rozwój technologii miał ulec spowolnieniu, a zatem również zmiany w zakresie ochrony sygnalistów muszą nadążyć za tą rewolucją. Technologie takie jak AI, *blockchain*, *big data* czy IoT będą odgrywać coraz większą rolę w kształtowaniu systemów zgłaszania i ochrony sygnalistów, jednakże kluczowe będzie zrównoważenie korzyści wynikających z tych technologii z wymogami prawnymi, etycznymi oraz potrzebą zapewnienia transparentności i odpowiedzialności, albowiem jak głosi stara rzymska paremia *non omne quod licet honestum est*[91].

Nie należy jednak zakładać, że praca nad ochroną sygnalistów kończy się na wprowadzeniu nowych przepisów. Jest to ciągły proces, który wymaga elastyczności, innowacyjności i współpracy na wielu poziomach. W obliczu szybkich zmian technologicznych i prawnych kluczowe jest, aby organizacje, ustawodawcy i sygnaliści pozostawali na bieżąco z najnowszymi trendami i rozwiązaniami, aby zapewnić skuteczną ochronę dla tych, którzy decydują się mówić prawdę w obliczu nadużyć i nieprawidłowości. Ostatecznie przyszłość ochrony sygnalistów w erze cyfrowej będzie zależała od naszej zdolności do adaptacji, innowacyjności oraz zaangażowania w tworzenie sprawiedliwego i transparentnego systemu, który będzie służył zarówno jednostkom, jak i społeczeństwu jako całości.

Bibliografia

Źródła

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305/17 z 2019 r.).

Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. z 2024 r. poz. 928).

[91] *Digesta Iustiniani*, D. 50.17.144 pr.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 12 lipca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Dz. Urz. UE L 1689 z 2024 r.).

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 (Dz. Urz. UE L 119 z 2016 r.).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Źródła internetowe

Alani M.M., *Big data in cybersecurity: a survey of applications and future trends. Journal of Reliable Intelligent Envi*ronments, „Journal of Reliable Intelligent Environments", https://www.researchgate.net/publication/348278146_Big_data_in_cybersecurity_a_survey_of_applications_and_future_trends [dostęp: 30.08.2024].

Coronavirus kills Chinese whistleblower ophthalmologist, American Academy of Ophthalmology, https://www.aao.org/education/headline/coronavirus-kills-chinese-whistleblower-ophthalmol/ [dostęp: 30.08.2024].

Epidemia w więzieniu? „Winny" sygnalista, https://www.rp.pl/sluzby/art8644921-epidemia-w-wiezieniu-winny-sygnalista/ [dostęp: 30.08.2024].

Filing Whistleblower Complaints Under the Solid Waste Disposal Act, https://www.osha.gov/sites/default/files/publications/OSHA3815.pdf/ [dostęp: 30.08.2024].

Gentry C., Halevi S., Hom*omorphic Encryption and its Applications. Cryptology ePrint Archive, Paper 2022/1602,* https://eprint.iacr.org/2022/1602.pdf/ [dostęp: 30.08.2024].

Guidance Whistleblowing and the Public Interest Disclosure Act 1998 (c.23) (accessible version), https://www.gov.uk/government/publications/whistleblowing-and-the-public-interest-disclosure-act-1998-c23/whistleblowing-and-the-public-interest-disclosure-act-1998-c23-accessible-version/ [dostęp: 30.08.2024].

How Real-time Monitoring Changes the Game for Transaction Security, https://www.flagright.com/post/how-real-time-monitoring-changes-the-game-for-transaction-security/ [dostęp: 30.08.2024].

Hudson M., *The Panama Papers: Exposing the Rogue Offshore Finance Industry*, https://www.icij.org/investigations/panama-papers/ [dostęp: 30.08.2024].

Internet Rzeczy (IoT) – Co to jest? Jak działa? Zastosowanie, przykłady, https://cryps.pl/internet-rzeczy-iot-co-to-jest/ [dostęp: 30.08.2024].

ISO/IEC 42001:2023, Artificial Intelligence Management Systems – Requirements, https://www.iso.org/standard/81230.html/ [dostęp: 30.08.2024].

Lloyd-La Follette Act of 1912, https://whistleblower.house.gov/resources/all-resources/committee-jurisdiction-tool/whistleblowing-executive-branch-employee/lloyd-la-follette-act-1912/ [dostęp: 30.08.2024].

Monitorowanie zużycia energii elektrycznej urządzeń przemysłowych – przykład wtryskarki FANUC. APA LAB, https://apagroup.pl/apalab/jak-skutecznie-monitorowac-zuzycie-energii-elektrycznej-urzadzen-przemyslowych-przyklad-wtryskarki-fanuc/ [dostęp: 30.08.2024].

Nader Riders, https://pophistorydig.com/topics/naders-raiders-1968-1974/ [dostęp: 30.08.2024].

O'Connor J.D., *I'm the Guy They Called Deep Throat*, „Vanity Fair", https://www.vanityfair.com/news/politics/2005/07/deepthroat200507?printable=true&currentPage=all/ [dostęp: 30.08.2024].

Pandey P., Saroliya A., Kumar R., *Analyses and Detection of Health Insurance Fraud Using Data Mining and Predictive Modeling Techniques,* [w:] *Advances in Intelligent Systems and Computing,* 2017, s. 41–49.

Perlstein R., *Watergate scandal*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/event/Watergate-Scandal/ [dostęp: 30.08.2024].

Preventing Corruption in Procurement through Big Data, https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2020/preventing-corruption-procurement-big-data.html [dostęp: 30.08.2024].

Ralph Nader, https://achievement.org/achiever/ralph-nader/ [dostęp: 30.08.2024 r.].

Ray M., *Edward Snowden*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/biography/Edward-Snowden/ [dostęp: 30.08.2024].

Shiel F., *European court reverses course to rule in favor of LuxLeaks whistleblower*, https://www.icij.org/investigations/luxembourg-leaks/european-court-reverses-course-to-rule-in-favor-of-luxleaks-whistleblower/ [dostęp: 30.08.2024].

Sygnalista, [w:] *Słownik języka polskiego*, red. W. Doroszewski, https://sjp.pwn.pl/doroszewski/sygnalista/ [dostęp: 31.08.2024].

Sygnalista, [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/ [dostęp: 31.08.2024].

Sygnalista, https://sjp.pl/ [dostęp: 30.08.2024].

Taherdoost H., Madanchian M., *Artificial Intelligence and Sentiment Analysis: A Review in Competitive Research,* https://doi.org/10.3390/computers12020037 [dostęp: 30.08.2024].

Taherdoost H., *Smart Contracts in Blockchain Technology: A Critical Review,* [w:] *Information, 2023,* https://www.mdpi.com/2078-2489/14/2/117/ [dostęp: 30.08.2024].

The False Claims Act, https://www.justice.gov/civil/false-claims-act/ [dostęp: 30.08.2024].

The Impact of Smart Sensors on Environmental Monitoring and Compliance, https://fatfinger.io/the-impact-of-smart-sensors-on-environmental-monitoring-and-compliance/ [dostęp: 30.08.2024 r.].

Todd M., *Danske Bank Whistleblower Testifies at European Parliament*, Whistleblower Network News, https://whistleblowerprotection.eu/blog/danske-bank-whistleblower-testifies-at-european-parliament/ [dostęp: 30.08.2024].

Tokarczyk D., [w:] E. Rutkowska, D. Tokarczyk, *Ustawa o ochronie sygnalistów. Komentarz*, LEX/el. 2024, art. 4., https://sip.lex.pl/#/commentary/587977514/774954?keyword=Ustawa%20o%20ochronie%20sygnalist%C3%B3w.%20Komentarz&tocHit=1&cm=SFIRST/ [dostęp: 31.08.2024].

United States Files Complaint Against Novartis Pharmaceuticals Corp. for Allegedly Paying Kickbacks to Doctors in Exchange for Prescribing Its Drugs, https://www.justice.gov/opa/pr/united-states-files-complaint-against-novartis-pharmaceuticals-corp-allegedly-paying/ [dostęp: 30.08.2024].

U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program – The Washington Post, „Washington Post", https://www.washingtonpost.com/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Online Etymology Dictionary,* https://www.etymonline.com/search?q=whistleblower%20/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Merriam-Webster,* https://www.merriam-webster.com/wordplay/whistle-blower-blow-the-whistle-word-origins/ [dostęp: 30.08.2024].

Whistle-blower, [w:] *Phrases Finder*, https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Word Origins*, http://www.wordorigins.org/index.php/site/whistleblower/, [w:] Wayback Machine, https://web.archive.org/web/20120429004210/http://www.wordorigins.org/index.php/site/whistleblower/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Oxford English Dictionary*, https://www.dictionary.com/browse/whistleblower/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Meriiam-Webster*, https://www.merriam-webster.com/dictionary/whistleblower/ [dostęp :30.08.2024].

Whistle-blower, [w:] *Phrase Finder,* https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024].

Whistleblower Protections – Rights Of Employees [5 U.s.c. §2302 (B)(8)], https://www.americorps.gov/sites/default/files/document/2021_08_27_Whistleblower_Rights_Employees_OGC.pdf/ [dostęp: 30.08.2024].

Globaleaks, https://www.globaleaks.org/ [dostęp: 30.08.2024].

Securedrop, https://securedrop.org/ [dostęp: 30.08.2024].

Falcony, https://www.falcony.io/ [dostęp: 30.08.2024].

Navex, https://www.navex.com/ [dostęp: 30.08.2024].

EQS Group System BKMS, https://www.eqs.bkms-system.com/ [dostęp: 30.08.2024].

Signal, https://signal.org/pl/ [dostęp: 30.08.2024].

Tella, https://tella-app.org/ [dostęp: 30.08.2024].

Guardianproject, Haven, https://guardianproject.github.io/haven/ [dostęp: 30.08.2024].

Guardianproject, Orbot, https://orbot.app/en/ [dostęp: 30.08.2024].

DISS-CO, https://diss-co.tech/ [dostęp: 30.08.2024].

Fixnix, https://www.fixnix.co/ [dostęp: 30.08.2024].

SpeakUp, https://www.speakup.com/ [dostęp: 30.08.2024].

Literatura

Amiri M.J., Agrawal D., Abbadi A., *Permissioned Blockchains: Properties, Techniques and Applications* [w:] *SIGMOD '21: Proceedings of the 2021 International Conference on Management of Data*, 2021.

Becker A., *Messengers of Disaster: Raphael Lemkin, Jan Karski, and Others*, „Journal of Holocaust Studies" 2017.

Devitt J.K., *Speaking Up Safely Civil Society Guide To Whistleblowing: Middle East And North Africa Region,* „Transparency International" 2015, http://www.jstor.org/stable/resrep20533/ [dostęp: 30.08.2024].

Digesta Iustiniani, D. 50.17.144 pr.

Fietkiewicz K.J., *The Development of Information Society in Japan: A Case Study of 21 Metropolitan Areas.* Proceedings of the Hawaii University International Conferences on Arts, Humanities, Social Sciences & Education, 2019.

Jankowski J., Karski J., *Raport tajnego emisariusza*, Kraków 2019.

Kant I., *Krytyka czystego rozumu*, tłum. R. Ingarden, Warszawa 1957.

Murszewski J., *Problemy implementacji dyrektywy 2019/1937 do polskiego porządku prawnego*, [w:] B. Baran, M. Ożóg (red.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Warszawa 2021.

Sharma P., Jindal R., Borah M.D., *A Review of Blockchain-Based Applications and Challenges,* [w:] *Wireless Personal Communications,* 2022.

Stanger A., *Whistleblowers: Honesty in America from Washington to Trump*, Cambridge 2019.

Zheng Z., Xie S., Dai H., Chen X., Wang H., *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, [w:] *2017 IEEE 6th International Congress on Big Data, IEEE Computer Society,* 2017.

Selected issues regarding the role of whistleblowers and reporting channels in the context of the development of digital technologies and legislative changes, as well as related challenges and prospects

Abstract

The article focuses on the evolution of the role of whistleblowers in the digital era and on the analysis of the impact of modern technologies, such as artificial intelligence (AI), blockchain, Big Data, and the Internet of Things (IoT), and on the effectiveness and security of reporting channels. The aim of the work is to assess how these technologies can revolutionize the process of reporting irregularities, as well as what challenges and opportunities are associated with their integration in the context of contemporary legislative changes, with particular emphasis on Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of EU law and the Polish Act of 14 June 2024 on the protection of whistleblowers. The research methodology includes a literature review and an analysis of legal regulations. Key findings indicate that digital technologies can significantly increase the level of security, anonymity and efficiency of reporting systems, although at the same time they pose challenges to legislators and organizations related to ensuring compliance with regulations, protection of personal data and transparency. The work emphasizes that an important aspect of the future of whistleblower protection will be the harmonization of legal regulations with the dynamically developing technological landscape and education in the field of new reporting tools. The implications of the research suggest the need for a flexible approach to legal regulations to ensure effective whistleblower protection in the digital era, and indicate the need for continuous monitoring and adaptation of regulations to new technological challenges.

Keywords

Whistleblowers, whistleblower protection, reporting channels, digital technologies, artificial intelligence (AI), big data, Internet of Things (IoT), data protection law