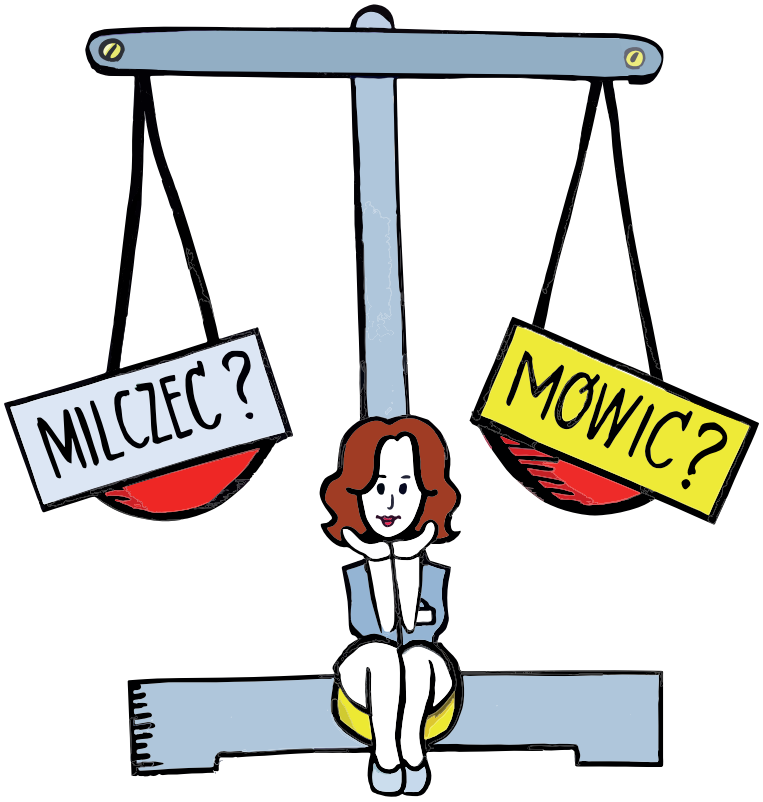
WIEM I POWIEM

OCHRONA SYGNALISTÓW I DZIENNIKARSKICH ŹRÓDEŁ INFORMACJI



PRAKTYCZNY PRZEWODNIK

DOROTA GŁOWACKA
ADAM PLOSZKA
MARCIN SZCZANIECKI

HELSIŃSKA FUNDACJA PRAW CZŁOWIEKA

Wydanie Przewodnika było możliwe dzięki wpłatom darczyńców, którzy wzięli udział w zbiórce internetowej zorganizowanej przez Helsińską Fundację Praw Człowieka w ramach akcji „Wiem i powiem".

Dziękujemy wszystkim osobom, które nas wsparły, w tym m.in.:

Marek Bryling, chaka, Maciej Chart-Olasiński, Piotr Choroś, Adam Czaplarski, Piotr Czejkowski, deejay1, Rafał Dembe, eudrag, Jan A. Hryniewiecki, jacpok, Piotr Jaworski, Krzysztof Kajetanowicz, Anna Kluj, Jakub Kozakoszczak, Karol Krzyczkowski, Karol Kwiatkowski, Łukasz Lasek, Sergiusz Lelakowski, Maja Łysienia, mmad, nocucco, Maciej Nowicki, Marek Antoni Nowicki, Joanna Rof, Dariusz Rybi, Marta Sikorska, Piotr Sołowij, Piotr Szotkowski, Hanna Szuleka, Piotrek T., Katarzyna Warecka, Zuzanna Warso, WMS, Karolina Wysocka, Izabela Żbikowska

Szczególne podziękowania za wsparcie i zaangażowanie w akcję chcielibyśmy przekazać prof. Wiktorowi Osiatyńskiemu.

Na przełomie 2015 i 2016 r. Helsińska Fundacja Praw Człowieka prowadziła akcję „**Wiem i powiem**". Celem akcji było zebranie funduszy na opublikowanie praktycznego przewodnika dla dziennikarzy i sygnalistów.

Oddając w Państwa ręce ten Przewodnik, chcielibyśmy serdecznie podziękować ponad ponad 220 osobom, które wsparły naszą akcję i dzięki którym wydanie tej publikacji było możliwe.

Autorzy: Dorota Głowacka, Adam Ploszka, Marcin Sczaniecki

Konsultacja merytoryczna: prof. dr hab. Ireneusz C. Kamiński

Koordynacja przygotowania i wydania Przewodnika: Małgorzata Szuleka

Opracowanie graficzne: Milena Moździerz

Koszty przygotowania i opublikowania Przewodnika zostały pokryte ze zbiórki funduszy w ramach akcji „Wiem i powiem". Akcję wsparło ponad 220 osób na łączną kwotę 19 509 zł. Autorzy serdecznie dziękują Małgorzacie Szulece, Marcie Boruckiej i Przemkowi Marciniakowi za przygotowanie i koordynację akcji „Wiem i powiem".

Publikacja bezpłatna, nieprzeznaczona do sprzedaży.

Publikacja jest dostępna także w formacie PDF na stronie internetowej Helsińskiej Fundacji Praw Człowieka: **www.hfhr.pl** oraz stronie programu HFPC Obserwatorium Wolności Mediów w Polsce: **www.obserwatorium.org**.

Stan prawny: marzec 2016 r.

ISBN 978-83-62245-55-0
Warszawa 2016

Wydawca
Helsińska Fundacja Praw Człowieka
00-018 Warszawa, ul. Zgoda 11,
www.hfhr.pl

Spis treści

Wstęp

W ramach kilku programów prawnych Helsińskiej Fundacji Praw Człowieka zostaliśmy skonfrontowani z nowym zagadnieniem tzw. demaskatorów czy też sygnalistów. To osoby, które w interesie ogólnym ujawniają znane im nieprawidłowości mające publiczne znaczenie w działaniach instytucji władzy lub innych podmiotów. Jednocześnie postępowanie sygnalistów naraża ich na zarzut złamania różnych reguł: prawa pracy (bo postępują „nielojalnie" wobec przełożonych i zatrudniającego ich podmiotu), kodeksów zawodowych (jeśli te nakazują rozstrzyganie zarzutów za pomocą „korporacyjnych procedur" i zabraniają „wynoszenia" sprawy poza własne środowisko), chroniących informacje poufne i tajemnice (gdy dochodzi do ich ujawnienia) czy dobre imię i cześć jednostki (gdy ujawniane informacje negatywnie wpływają na wizerunek pewnej osoby).

Sądy oraz inne organy stosujące prawo muszą znaleźć należytą równowagę między publicznymi racjami, które powodują podjęcie działań przez sygnalistów, a przepisami chroniącymi poszczególne interesy zbiorowe oraz indywidualne. Nawet jeśli ujawnianie nieprawidłowości, a tym bardziej nadużyć, służy ogólnemu dobru, sygnaliście nie zawsze wolno od razu zwrócić się do opinii publicznej. Również on działa w ramach pewnego rygoru prawnego i musi stopniować swoje postępowanie. Z drugiej strony koncentrowanie się przez sądy na przepisach prawa i egzekwowanie ich automatycznie przeciwko sygnaliście pomijać będzie obywatelski sens podjętych działań.

Do sygnalistów znajdzie zastosowanie pojęcie „publicznego kontrolera" (*public watchdog*). Ale dotychczas ta konstrukcja była używana przez krajowe i międzynarodowe sądy oraz organy do określania dziennikarzy (mediów) i organizacji pozarządowych. Powstaje więc pytanie, jak stworzone w takim kontekście reguły można „przenieść" na sygnalistów. Czasami da się to zrobić, innym razem będzie to niemożliwe. Zasadniczo jednak będziemy musieli stworzyć nowe reguły dostosowane do specyfiki sygnalistów.

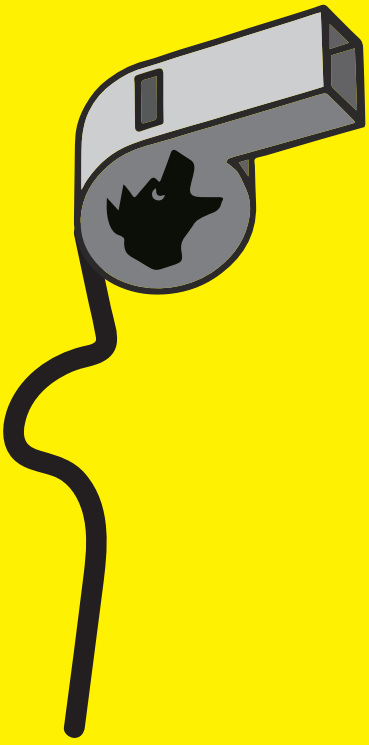
Niniejsze opracowanie ma charakter praktycznego przewodnika. Pokazuje, jakie narzędzia prawnicze już mamy i co jeszcze należy zrobić. W rozdziale I szkicujemy zjawisko sygnalistów i rekonstruujemy reguły prawne – krajowe i międzynarodowe – które mają do nich zastosowanie. Wskazujemy pomocne orzecznictwo, w tym Europejskiego Trybunału Praw Człowieka, który nie tylko miał już okazję wypowiedzieć się o sytuacji prawnej sygnalistów, ale ponadto uczynił to w sposób doniosły, bo jako Wielka Izba – największy skład orzekający. Identyfikujemy, jakie argumenty prawne ma do swojej dyspozycji sygnalista w poszczególnych postępowaniach.

Rozdział II to prezentacja regulacji oraz standardów prawnych dotyczących ochrony tajemnicy dziennikarskiej. Najmocniejszej ochronie podlega tożsamość informatora przekazującego dziennikarzom informacje mające publiczne znaczenie. Możliwość zwolnienia dziennikarza z tego aspektu tajemnicy zawodowej istnieje tylko w przypadku ścigania przez instytucje państwa sprawców najpoważniejszych przestępstw. W pozostałych sytuacjach do zwolnienia może dojść wtedy, jeśli wymaga tego ważny interes wymiaru sprawiedliwości i okoliczności objętej tajemnicą dziennikarską nie można ustalić w inny sposób. Co jednocześnie ważne, gwarancje przysługujące dziennikarzowi nie są tylko jego zawodowym przywilejem, ale i obowiązkiem prawnym. Nie może więc dojść do „samozwolnienia" się przez dziennikarza z zachowania tajemnicy. Zamykający Przewodnik rozdział III dotyczy nowego zjawiska „inwigilacji elektronicznej", a więc uzyskiwania przez instytucje państwa dostępu do treści wiadomości oraz rejestrów połączeń dokonywanych przez jednostkę. Regulacje dotyczące tego obszaru dopiero powstają, a te, które istnieją, okazują się niewystarczające, czego ilustracją jest powstanie programów masowej kontroli komunikacji telefonicznej oraz internetowej. Przedstawiamy ochronne standardy prawne obowiązujące w tym obszarze, które powstają w następstwie orzecznictwa konstytucyjnego i konwencyjnego. Wskazujemy ponadto, w jaki sposób można samemu zabezpieczyć się przed inwigilacją elektroniczną.

Zapraszamy do lektury.

Prof. dr hab. Ireneusz C. Kamiński

Rozdział I
Ochrona sygnalistów



Wprowadzenie

Osoby planujące w dobrej wierze ujawnić ważne dla opinii publicznej informacje o nieprawidłowościach lub korupcji, a więc tzw. sygnaliści, nazywani także demaskatorami, nie mogą liczyć na specjalną ochronę prawną, ponieważ taka w polskim systemie prawnym nie istnieje. Pozbawieni są zatem swego rodzaju tarczy, mogącej chronić ich przed atakami ze strony podmiotu, którego dotyczyły ujawnione informacje. Takie ataki są częstym następstwem ujawnienia nieprawidłowości i mogą przybrać m.in. postać postępowań sądowych.

Celem tego rozdziału Przewodnika jest opisanie, jakie działania prawne mogą spotkać sygnalistę w odwecie za ujawnienie przez niego informacji. Przybliżone zostaną również zasadnicze sposoby obrony przed tymi działaniami oraz argumenty, po które sygnalista może sięgnąć dla ochrony swoich praw. W rozdziale tym w szczególności zdefiniowane zostanie pojęcie sygnalisty, wyjaśnione zostaną powody, dla których warto chronić sygnalistów, ale także wskazane zostaną granice swobody wypowiedzi sygnalistów.

Należy w tym miejscu podkreślić, że rozdział ten, podobnie jak i cały Przewodnik, nie stanowi zachęty dla przyjmowania roli sygnalisty. Decyzja o zasygnalizowaniu nieprawidłowości może bowiem, obok zakładanej poprawy sytuacji, wiązać się z szeregiem negatywnych skutków w pracy, a także w życiu prywatnym. Powinna być zatem dobrze przemyślana, a lektura tego rozdziału pozwoli – mamy nadzieję – lepiej ocenić związane z nią ryzyko.

1. Kim są sygnaliści?

Sygnalista, określany zamiennie demaskatorem, donosicielem w dobrej wierze, ujawniaczem – to polskie tłumaczenia angielskiego terminu *whistleblower*: w dosłownym tłumaczeniu oznacza osobę dmuchającą w gwizdek. Co do zasady określenia tego używa się w stosunku do osoby, która ujawnia informacje na temat kwestii zagrażających interesowi publicznemu w kontekście stosunków pracowniczych, zarówno w sektorze prywatnym, jak i publicznym[1]. Sygnalista nie zawsze jednak musi być pracownikiem. Informacje o nieprawidłowościach czy korupcji może uzyskać, będąc związanym z danym miejscem w inny sposób, np. będąc zatrudnionym na umowie cywilnoprawnej bądź świadcząc usługi na rzecz jakiegoś podmiotu czy będąc żołnierzem lub agentem służb specjalnych. Kluczowymi elementami odróżniającymi sygnalistów od zwykłych

[1] Tak definiuje się to pojęcie w Rekomendacji Komitetu Ministrów Rady Europy CM/Rec (2014)7 dotyczącej ochrony sygnalistów z 30 kwietnia 2014 r.

donosicieli jest z jednej strony działanie w dobrej wierze, a nie np. w ramach zemsty, czy dla korzyści finansowej, z drugiej zaś to, że podejmowane przez nich działania są dokonywane w interesie publicznym.

Lekarz – sygnalista w interesie pacjentów

Jednym z najbardziej znanych polskich sygnalistów jest Tadeusz Pasierbiński, lekarz ginekolog, który działając w interesie publicznym i w dobrej wierze, jako szef regionalnej izby lekarskiej oraz radny powiatowy, ujawnił informację o z góry przesądzonym konkursie na ordynatora oddziału ginekologicznego jednego ze śląskich szpitali. Wybrany w wyniku „ustawionego" konkursu ordynator miał realizować zadanie wojewódzkiego konsultanta ds. ginekologii, polegające na otwarciu w szpitalu oddziału ginekologiczno-onkologicznego pomimo nieprzystosowania szpitala do wykonywania tego typu zabiegów leczniczych. Motywowany troską o dobro pacjentek T. Pasierbiński przekazał swoją wiedzę bezpośrednio władzom szpitala, właściwej Izbie Lekarskiej oraz na sesji Rady Powiatu. Pomimo ujawnienia tych informacji konkurs się odbył i doszło do zatrudnienia w szpitalu nowego ordynatora. W efekcie zaniedbań nowego ordynatora na oddziale doszło do kilku komplikacji zdrowotnych i zgonów, o czym sygnalista ponownie poinformował właściwe władze, co tym razem skutkowało zwolnieniem ordynatora.

Mimo to za swoje działania sygnalista został m.in. ukarany dyscyplinarnie (najpierw otrzymał upomnienie, a później został zwolniony z pracy) oraz oskarżony o zniesławienie w procesie przed sądem. Po wieloletniej batalii sądowej udało mu się wygrać wszystkie sprawy. Sąd przywrócił go do pracy w przychodni, w której pracował przed zwolnieniem[2].

2. Dlaczego warto chronić sygnalistów?

Rezolucja Zgromadzenia Parlamentarnego Rady Europy w sprawie ochrony demaskatorów wskazuje, że ochrona sygnalistów stanowi narzędzie do usprawnienia mechanizmów kontrolnych i walki z niegospodarnością oraz korupcją zarówno w sektorze publicznym, jak i prywatnym[3]. Sygnaliści działający w instytucjach publicznych

[2] Wyroki: Sądu Rejonowego w Mikołowie z dnia 9 grudnia 2004 r., sygn. akt IV P 763/04; Sądu Okręgowego w Katowicach z dnia 12 lipca 2005 r., sygn. akt IX Pa 245/05.

[3] Rezolucja Zgromadzenia Parlamentarnego Rady Europy w sprawie ochrony demaskatorów (dalej: ZPRE) nr 1729 z 29 kwietnia 2010 r.

to także ważny element mechanizmu demokratycznej kontroli państwa wykonywanej przez społeczeństwo. Gdyby nie działalność amerykańskiego sygnalisty Edwarda Snowdena pewnie do dziś nie wiedzielibyśmy o programach niezwykle szerokiej masowej inwigilacji środków komunikacji obywateli przez służby specjalne USA i innych państw.

Sygnalista ujawnia szkodliwość palenia tytoniu

Działania sygnalisty mogą mieć poważne skutki, czego dobrym przykładem są efekty ujawnienia informacji przez Jeffreya Wiganda, amerykańskiego naukowca pracującego dla przemysłu tytoniowego. Wigand ujawnił szkodliwość tytoniu zawartego w papierosach. Ujawnione przez niego informacje stanowiły podstawę procesów o milionowe odszkodowania. Historia ta została zekranizowana w filmie Michaela Manna *Insider* (*Informator*).

Warto uświadomić sobie, że dla firm i instytucji ochrona sygnalistów to przede wszystkim korzyści, a nie koszty. Doskonale wiedzą o tym przedsiębiorstwa międzynarodowe, które inwestują w wewnętrzne procedury umożliwiające funkcjonowanie sygnalistom. Uzyskanie informacji o potencjalnych nieprawidłowościach od człowieka znajdującego się wewnątrz danej organizacji pozwala na zapobiegnięcie negatywnym i często bardzo kosztownym skutkom takich informacji, gdy zostaną ujawnione na zewnątrz.

Nieuczciwy bankier

Jeden z oddziałów banku X od każdego posiadacza konta pobiera bezprawnie 10 groszy miesięcznie, które trafiają do kieszeni dyrektora tego oddziału. Posiadacze kont w większości nie mają o tym pojęcia. Jeden z szeregowych pracowników banku, korzystając z wewnętrznych kanałów sygnalizowania nieprawidłowości, informuje o tym centralę banku, która podejmuje działania naprawcze i zwraca pieniądze posiadaczom kont, dodatkowo wynagradzając za nadszarpnięcie zaufania. Dzięki temu bank został ochroniony przed późniejszym skandalem i utratą zaufania klientów.

Przekonanie o korzyściach płynących z ochrony sygnalistów zyskuje na znaczeniu także w sektorze publicznym, o czym świadczą np. pomysły wprowadzania programów nagradzania informatorów

wspomagających wykrywanie karteli, a więc zagrażających uczciwej konkurencji[4].

Choć prawo polskie nie zapewnia specjalnej ochrony prawnej sygnalistom, to jednak nakłada na każdego pewne obowiązki sygnalizacyjne. W tym miejscu warto wskazać dwa najważniejsze. Pierwszy to społeczny obowiązek poinformowania organów ścigania o podejrzeniu popełnienia przestępstwa wynikający z art. 304 § 1 Kodeksu postępowania karnego. Drugi to obowiązek pracownika dbania o dobro zakładu pracy, z którego ma wynikać obowiązek sygnalizowania dostrzeganych nieprawidłowości w funkcjonowaniu zakładu pracy (art. 100 § 2 pkt 4 Kodeksu Pracy[5]).

3. Kiedy należy chronić sygnalistów według Europejskiego Trybunału Praw Człowieka?

Pomimo braku specjalnej ochrony prawnej dla wyznaczenia standardu ochrony sygnalistów w Polsce szczególne znaczenie ma orzecznictwo Europejskiego Trybunału Praw Człowieka (dalej: ETPC, Trybunał). Trybunał Strasburski ustalił kryteria, które pozwalają dokonać oceny, czy daną osobę można uznać za sygnalistę[6]. Jeśli dana osoba spełni te kryteria, zdaniem ETPC nie powinna ona ponieść negatywnych konsekwencji swoich działań. Kryteria te są następujące:

1. Dostęp do innego skutecznego środka umożliwiającego właściwą reakcję na naruszenie prawa, które miało być ujawnione

Jak twierdzi ETPC, sygnalista, aby skorzystać z ochrony, powinien w pierwszej kolejności przekazać informacje o nieprawidłowościach przełożonemu lub innej właściwej władzy bądź organowi. Jeżeli taka sygnalizacja byłaby „w oczywisty sposób niepraktyczna" (ang. *clearly impracticable*), to informacja może zostać ostatecznie ujawniona opinii publicznej. Cytowana wyżej rezolucja ZPRE, do której odwołuje się często ETPC, stwierdza, że z zewnętrznej drogi

[4] J. Polański, *Programy nagradzania informatorów w prawie państw europejskich*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, nr 9 (3), s. 10-33.

[5] M. Wujczyk, *Podstawy whistleblowingu w polskim prawie pracy*, „Przegląd Sądowy" 2014, nr 6, s. 114-122.

[6] Kryteria te wynikają z fundamentalnego orzeczenia ETPC z dnia 12 lutego 2008 r. (Wielka Izba) w sprawie *Guja p. Mołdawii*, skarga nr 14277/04, które następnie zostały powtórzone w wyroku ETPC z 21 lipca 2011 r. w sprawie *Heinisch p. Niemcom*, skarga nr 28274/08. Omówienie i rozważania na temat wyroku w sprawie Guja: I.C. Kamiński, *Ograniczenia swobody wypowiedzi dopuszczalne w Europejskiej Konwencji Praw Człowieka. Analiza krytyczna*, Warszawa 2010, s. 240-243.

informowania o nieprawidłowościach można skorzystać, gdy nie istnieje wewnętrzna droga alarmowa, nie funkcjonuje ona prawidłowo albo jeśli nieracjonalne byłoby oczekiwać, że droga wewnętrzna będzie działać właściwie, biorąc pod uwagę naturę ujawnionego problemu.

Procedura „oczywiście niepraktyczna"

Duże przedsiębiorstwo wprowadziło procedurę informowania o nieprawidłowościach. Procedura ta polegała na odczytywaniu zgłaszanych zarzutów publicznie na zebraniu pracowników. Pozostali pracownicy, na podstawie treści i stylistyki, ze zgłoszenia mogli łatwo wywnioskować, kto jest jego autorem. Dodatkowo stawiane zarzuty nie były należycie wyjaśniane. Taka procedura mogłaby zostać uznana za „oczywiście niepraktyczną".

W praktyce informacje o nieprawidłowościach powinny w pierwszej kolejności trafiać do władz podmiotu, którego nieprawidłowości dotyczą. W tym celu należy skorzystać z wewnętrznych procedur informowania o nieprawidłowościach (jeżeli takowe istnieją). Jeżeli nieprawidłowości dotyczą szeroko rozumianej sfery prawa pracy, w dalszej kolejności można zwrócić się do Państwowej Inspekcji Pracy, która gwarantuje anonimowość autorowi zgłoszenia. W sytuacji zaś, gdy dostrzeżone braki dotyczą instytucji publicznych, kolejno należy powiadomić właściwą jednostkę nadrzędną, a w ostateczności odpowiednie ministerstwo, a także Najwyższą Izbę Kontroli. Dopiero po bezskutecznym wyczerpaniu wszystkich „nieinwazyjnych" sposobów zwrócenia uwagi na dostrzeżony problem o sprawie można powiadomić media i opinię publiczną.

List do ministra

Do powyższych wskazówek zastosował się P.S. Sygnalista ten podczas świadczenia pracy w spółce X powziął wątpliwości dotyczące rozliczeń finansowych między Pocztą Polską, na której zlecenie wydawany był tygodnik „Poczta Polska", a firmą X. Swoimi wątpliwościami podzielił się z wiceministrem infrastruktury w liście z 3 kwietnia 2008 r., w którym wskazał przypadki niegospodarności w spółce X, szkodzące zarówno samej spółce X, jak i jej właścicielowi – Poczcie Polskiej. Na początku lipca 2008 r. otrzymał odpowiedź od ministra z podziękowaniami za zainteresowanie sprawami poczty. Niedługo później został zwolniony z uwagi na utratę zaufania spółki do sygnalisty. Od zwolnienia odwołał się do sądu pracy, który uznał, że sygnalista, zwracając się z pismem do ministra infrastruktury, nie miał zamiaru

zaszkodzić spółce, a jedynie zmierzał do wyjaśnienia sprawy niegospodarności[7]. Sąd przyznał mu odszkodowanie[8].

2. Istnienie interesu publicznego związanego z ujawnieniem informacji

Kolejnym warunkiem stawianym przez ETPC sygnalistom jest to, by sygnalista działał w interesie publicznym, a więc nie w celu osobistym, np. chęci uzyskania awansu.

3. Autentyczność ujawnionych informacji i działanie w dobrej wierze

Dalej ETPC wymaga, by informacje, które ujawnia sygnalista, były autentyczne oraz by sygnalista działał w dobrej wierze, a nie np. kierowany chęcią zaszkodzenia instytucji, w której funkcjonowaniu dostrzega nieprawidłowości. Jak podkreśla się w rezolucji Zgromadzenia Parlamentarnego Rady Europy, „sygnalista powinien być uważany za działającego w dobrej wierze, gdy ma rozsądne powody do uznania, iż ujawniona informacja była prawdziwa, nawet jeśli następnie okaże się ona błędna, oraz pod warunkiem że nie działa w celach niezgodnych z prawem lub sprzecznych z etyką".

„Sygnalista" w złej wierze

Utrudnione będzie uznanie danej osoby za sygnalistę działającego w dobrej wierze i w interesie publicznym w przypadku, gdy informacje o nieprawidłowościach w funkcjonowaniu swojego zakładu pracy ujawnił on po zwolnieniu z pracy z innego powodu niż chęć nagłośnienia dostrzeganych nieprawidłowości – np. gdy do jego zwolnienia doszło w wyniku wykrycia, że nadużywa on alkoholu. Trudno byłoby także uznać daną osobę za sygnalistę zasługującego na ochronę, gdyby świadomie rozpowszechniała ona fałszywe informacje na temat rzekomych nadużyć.

4. Stosunek szkody do korzyści

Dalej ETPC wskazał, że ewentualna szkoda, jaka została poniesiona przez podmiot, w którego działaniu ujawniono nieprawidłowości, w związku z ujawnieniem informacji, nie przewyższa korzyści, jaka powstała w związku z ujawnieniem informacji.

[7] Wyrok Sądu w Warszawie z dnia 27 maja 2010 r., sygn. akt XXI PA 154/10.

[8] Wyrok Sądu Rejonowego dla Warszawy-Żoliborza z dnia 8 grudnia 2009 r., sygn. akt VII P 660/08, utrzymany w mocy przez wyrok sądu drugiej instancji.

Ważenie korzyści i szkód

Ujawnienie nieprawidłowości w funkcjonowaniu szpitala polegających na stosowaniu niewystarczających środków medycznych, zaniedbaniach opieki medycznej i innych, które zagrażają zdrowiu i życiu pacjentów, w sposób oczywisty przewyższa szkodę związaną z nadszarpnięciem reputacji danego szpitala w wyniku upublicznienia takiej informacji.

5. Proporcjonalny charakter sankcji wymierzonych sygnaliście

Wreszcie ostatnim kryterium ochrony sygnalistów jest proporcjonalność sankcji, jakie spotykają go ze strony pracodawcy w związku z ujawnieniem niewygodnej informacji. Zbyt surowe ukaranie sygnalisty, który np. nie skorzystał z drogi zewnętrznej sygnalizowania nieprawidłowości może zostać uznane za nieproporcjonalne. W jednym z wyroków ETPC uznał, że zwolnienie sygnalisty z pracy stanowiło zbyt surową sankcję, która miała nie tylko negatywne skutki dla skarżącego, ale mogła również w poważnym stopniu zniechęcić innych pracowników do informowania o dostrzeganych przez nich nieprawidłowościach.

Sygnalista korzysta z ochrony Europejskiego Trybunału Praw Człowieka, gdy spełnione są następujące wymogi:

- w pierwszej kolejności sygnalista skorzystał z innego skutecznego środka umożliwiającego właściwą reakcję na naruszenie, które miało być ujawnione (o ile środek taki istnieje);
- istnieje interes publiczny związany z ujawnieniem informacji;
- ujawnione informacje są autentyczne;
- działania sygnalisty wykonywane są w dobrej wierze;
- ewentualna szkoda, jaka została poniesiona w związku z ujawnieniem informacji, nie przewyższa korzyści, które powstały w wyniku działania sygnalisty;
- sankcje wymierzone sygnaliście mają charakter proporcjonalny.

Dla oceny przez ETPC działania sygnalisty i stwierdzenia, czy korzysta on z ochrony europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności[9] (dalej: EKPC, Konwencja), znaczenie ma także forma wypowiedzi, której używa demaskator, by zasygnalizować nieprawidłowości. Z ochrony konwencyjnej wyłączona będzie wypowiedź, która została wyrażona w wulgarnej, uwłaczającej godności

[9] Europejska Konwencja o ochronie praw człowieka i podstawowych wolności (Dz.U. z 1993 r. Nr 61 poz. 284 ze zm.).

formie[10]. Przekłada się to na zalecenie, by każdy sygnalista podejmował starania w celu maksymalnego powściągania emocji, gdy podejmuje się działalności sygnalizacyjnej.

Wyrok Europejskiego Trybunału Praw Człowieka w sprawie *Palomo Sanches i inni p. Hiszpanii*

Do takiego wniosku doszedł ETPC, rozpatrując skargę działaczy związkowych zwolnionych z pracy za opublikowanie karykatur i satyrycznych tekstów na temat dwóch innych pracowników i menadżera. W marcu 2002 r. w jednym z numerów gazetki zakładowej ukazał się artykuł skarżących na temat częściowo wygranego przez nich procesu przed sądem pracy w Barcelonie przeciwko ich pracodawcy o zapłatę zaległego wynagrodzenia. Na okładce gazetki zamieszczono karykaturę obrazującą dwóch pracowników – jak pisze Trybunał – „świadczących usługi seksualne" jednemu z menadżerów. Także artykuły wewnątrz gazetki w sposób wulgarny odnosiły się do dwójki pracowników. Wcześniej skarykaturowani pracownicy zeznawali w procesie pracowniczym na rzecz pracodawcy, przeciwko skarżącym. Gazeta została rozprowadzona wśród pracowników oraz powieszona na tablicy informacyjnej związku zawodowego. Skarżący zostali dyscyplinarnie zwolnieni z pracy pod zarzutem rażącego naruszenia godności i reputacji współpracowników oraz menadżera. Skarżący zaskarżyli decyzję pracodawcy do sądu jako bezpodstawne rozwiązanie stosunku zatrudnienia. Hiszpańskie sądy pracy nie dopatrzyły się jednak naruszenia praw pracowniczych i uznały zwolnienie za uzasadnione. Podobnie orzekł ETPC.

Jakie znaczenie mają standardy strasburskie w Polsce?

W postępowaniu przed polskimi sądami warto powołać się na orzecznictwo Europejskiego Trybunał Praw Człowieka, który wypracował kryteria pozwalające na ocenę, czy wypowiedź sygnalisty mieści się w granicach wolności słowa[11]. Orzecznictwo ETPC jest dla polskich sądów wiążące. Niezastosowanie się do niego naraża państwo polskie na odpowiedzialność odszkodowawczą. Innymi słowy, w sytuacji gdy dana wypowiedź będzie spełniać wskazane wyżej kryteria, a mimo to dojdzie do uznania sygnalisty

[10] Zob. w szczególności wyrok ETPC z 12 września 2011 r. w sprawie *Palomo Sanches i inni p. Hiszpanii*, skargi nr 28955/06, 28957/06, 28959/06 i 28964/06.

[11] Szerzej: A. Ploszka, *Ochrona demaskatorów (whistleblowers) w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Europejski Przegląd Sądowy" 2014, nr 4, s. 12-18.

za winnego zniesławienia lub za dopuszczającego się bezprawnego naruszenia dóbr osobistych bądź sąd pracy nie uzna jego racji, dojdzie wówczas do naruszenia europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Więcej informacji na temat postępowania przed Trybunałem znajduje się w dalszej części tego rozdziału.

4. Czy polskie prawo chroni w sposób szczególny sygnalistów?

W prawie polskim nie istnieją przepisy w sposób wyraźny regulujące status sygnalistów, choć standardy międzynarodowe nakładają na państwa obowiązek stworzenia ram prawnych dla działalności sygnalizacyjnej. Taki obowiązek wynika zarówno z ratyfikowanej przez Polskę Cywilnoprawnej konwencji Rady Europy o korupcji, orzecznictwa ETPC oraz szeregu aktów o charakterze prawnie niewiążącym (tzw. *soft law*). Tym samym Polska pozostaje jednym z krajów, w których nie istnieją odrębne regulacje dotyczące ochrony sygnalistów. Luka ta powinna być jak najszybciej wypełniona przez ustawodawcę. Na problem ten zwracał uwagę m.in. Rzecznik Praw Obywatelskich[12] czy Fundacja im. Stefana Batorego[13]. Apele tych instytucji nie przyniosły na razie skutku. Nie oznacza to jednak, że sygnaliści pozbawieni są jakichkolwiek instrumentów ochrony. Istnieją pewne przepisy, na których mogą się oprzeć, ale są rozrzucone po całym systemie prawa.

Skąd wynika obowiązek uregulowania statusu sygnalistów w Polsce?

1. Z art. 9 ratyfikowanej przez Polskę Cywilnoprawnej konwencji Rady Europy o korupcji z 1999 r.[14].
2. Z rezolucji Zgromadzenia Parlamentarnego Rady Europy w sprawie ochrony sygnalistów nr 1729 (2010).
3. Z rekomendacji Zgromadzenia Parlamentarnego Rady Europy nr 1916 (2010) pt. „Ochrona sygnalistów".

[12] Od kilku lat zwraca na to uwagę Rzecznik Praw Obywatelskich. Zob. wystąpienie Rzecznika Praw Obywatelskich z dnia 3 marca 2009 r. do Ministra Pracy i Polityki Społecznej (sygn. RPO-606960-III/09/RP/AF), także wystąpienie Rzecznika Praw Obywatelskich z dnia 18 grudnia 2015 r. do Ministra Pracy i Polityki Społecznej (II.7040.104.2015AF/LN).

[13] O potrzebie regulacji w tym zakresie wypowiada się także doktryna, zob.: M. Wujczyk, *Podstawy whistleblowingu w polskim prawie pracy*, „Przegląd Sądowy" 2014, nr 6, s. 114-122; A. Ploszka, *Ochrona demaskatorów (whistleblowers) w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Europejski Przegląd Sądowy" 2014, nr 4, s.12-18; A. Bodnar, A. Ploszka, *Europa uczy się ochrony sygnalistów. Dzięki Snowdenowi*, https://wszystkoconajwazniejsze.pl/adam-bodnar-adam-ploszka-europa-uczy-sie-ochrony-sygnalistow-dzieki-snowdenowi/ (dostęp: 15 marca 2016 r.).

[14] Dz.U. z 2004 r. Nr 244 poz. 2443.

4. Z rekomendacji Komitetu Ministrów CM/Rec (2014) dotyczącej ochrony sygnalistów.
5. Z raportu Specjalnego Sprawozdawcy ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi dotyczącego ochrony dziennikarskich źródeł informacji i praw sygnalistów (sygn. dokumentu A/70/361).

6. Z raportu Komitetu ds. Prawnych i Praw Człowieka Zgromadzenia Parlamentarnego Rady Europy „Wzmocnienie ochrony praw sygnalistów".

7. Z orzecznictwa ETPC w sprawie sygnalistów omówionego wyżej.

Jaki skutek mają te dokumenty na poziomie krajowym? Czy sygnalista może się na nie powołać w Polsce?

Poza wskazaną w punkcie 1 Cywilnoprawną konwencją Rady Europy o korupcji wskazane wyżej akty mają charakter tzw. prawa miękkiego. Oznacza to, że nie można z nich wyprowadzić konkretnego obowiązku, którego realizacji następnie można by domagać się na drodze sądowej. Niemniej stanowią one pewną wskazówkę interpretacyjną dla sądów i zapowiedź rozwoju prawa międzynarodowego w tym zakresie, a także wpływają na kształt standardu ochrony sygnalistów. Innymi słowy, powołanie się na te dokumenty stanowi dodatkowy argument przemawiający za koniecznością pochylenia się sądu nad problematyką szczególnego statusu sygnalisty. Powinny być one także uwzględniane przez ustawodawcę, aby w pełni realizować standardy międzynarodowe.

Procedowana właśnie w Unii Europejskiej Dyrektywa o tajemnicach handlowych może stanowić dodatkowe źródło obowiązku uregulowania statusu sygnalistów. Po jej przyjęciu niezapewnienie ochrony sygnalistom narażałoby Polskę na konsekwencje wynikające z nieprawidłowego implementowania prawa Unii Europejskiej. Należy jednocześnie zaznaczyć, że dyrektywa ta budzi pewne kontrowersje środowisk pozarządowych związane ze zbyt niskim poziomem ochrony sygnalistów[15].

Fundacja im. Stefana Batorego, działając od wielu lat na rzecz ochrony sygnalistów, opracowała „Założenia do

[15] Zob. szerzej kampanię organizacji X-net „Say no to the New laws on Trade Secrets #StopTradeSecrets" https://xnet-x.net/en/trade-secrets-trolls/ (dostęp: 15 marca 2016 r.).

ustawy o ochronie praw osób sygnalizujących nieprawidłowości środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych?"[16]. Założenia te nie stały się jednak przedmiotem prac parlamentarnych. Co więcej, kwestia uregulowania ochrony prawnej sygnalistów znajdowała się także w Rządowym programie przeciwdziałania korupcji na lata 2014-19, niemniej została z niego usunięta bez podania oficjalnego powodu.

5. Granice swobody wypowiedzi sygnalistów

Na działalność sygnalistów można patrzeć z różnych perspektyw[17]. Przyjmując za Europejskim Trybunałem Praw Człowieka perspektywę praw człowieka, każda wypowiedź sygnalisty, napisanie przez niego skargi, ulotki itp. będzie stanowiła korzystanie z wolności słowa, gwarantowanej przez art. 54 ust 1. Konstytucji RP[18] i art. 10 EKPC.

§

Konstytucja RP

Art. 54.1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji.

2. Cenzura prewencyjna środków społecznego przekazu oraz koncesjonowanie prasy są zakazane. Ustawa może wprowadzić obowiązek uprzedniego uzyskania koncesji na prowadzenie stacji radiowej lub telewizyjnej.

Konwencja o ochronie praw człowieka i podstawowych wolności

Art. 10.1. Każdy ma prawo do wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa państw do poddania procedurze zezwoleń przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych.
2. Korzystanie z tych wolności pociągających za sobą obo-

[16] A. Wojciechowska-Nowak, *Założenia do ustawy o ochronie praw osób sygnalizujących nieprawidłowości środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych?*, Fundacja Batorego, Warszawa 2012.

[17] Z perspektywy nauki o zarządzaniu zob.: W. Rogowski, *Whistleblowing: bohaterstwo, zdrada czy interes?*, „Przegląd Corporate Governance" 2007, nr 1, s. 23-41; I. Świątek-Barylska, *Whistleblowing w praktyce. Postawy i zachowania pracowników organizacji gospodarczych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2012, nr 249, s. 403–412.

[18] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. Nr 78 poz. 483 ze zm.).

wiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej.

Sygnaliści wobec braku wyraźnych regulacji prawnych mogą zatem powołać się na ogólne gwarancje swobody wypowiedzi. Należy jednak pamiętać, że wolność słowa nie ma charakteru absolutnego, podobnie jak większość konstytucyjnych praw i wolności, i może podlegać pewnym ograniczeniom (zob. art. 31 ust. 3 Konstytucji oraz art. 10 ust. 2 EKPC).

Granice wolności słowa sygnalistów wyznaczają w szczególności:

1. **Kodeks pracy**[19], który w art. 100 § 2 pkt 4 mówi o obowiązku dbania o dobre imię pracodawcy i zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
2. **Kodeks cywilny**[20], który w art. 23 i 24 zawiera regulację dotycząca ochrony dóbr osobistych chroniącą przed ich bezprawnym naruszaniem.
3. **Kodeks karny**[21], który w art. 212 określa przestępstwo zniesławienia chroniące cześć człowieka.
4. **Tajemnice prawnie chronione**, zawarte w ustawach zawodów regulowanych ustawowo, takie jak tajemnice adwokacka, dziennikarska, lekarska, tajemnica przedsiębiorstwa itd.
5. **Kodeksy etyczne** niektórych zawodów, a także pracodawców.
6. **Wewnętrzne regulacje** dotyczące sygnalizowania nieprawidłowości.

[19] Ustawa z dnia 26 czerwca 1974 r., – Kodeks Pracy (Dz.U. z 2014 r. poz. 1502 j.t.).

[20] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2014 r. poz. 121 j.t.).

[21] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88 poz. 553 ze zm).

6. Na czym polega obowiązek lojalności wobec pracodawcy?

Na sygnalistach-pracownikach ciąży szczególny obowiązek troski o dobre imię pracodawcy, który to obowiązek sygnalista musi brać pod uwagę, decydując się na ujawnienie jakiejkolwiek informacji dotyczącej pracodawcy. Obowiązek ten nie ma jednak charakteru bezwzględnego.

„Prawo do *whistleblowingu*" a obowiązek lojalności

Jak zauważył Sąd Najwyższy w jednym z wyroków:
„Pracownik ma prawo do dozwolonej, publicznej krytyki przełożonego (prawo do *whistleblowingu*, czyli ujawnienia nieprawidłowości w funkcjonowaniu jego zakładu pracy, polegających na różnego rodzaju aktach nierzetelności, nieuczciwości z udziałem pracodawcy lub jego przedstawicieli), gdy nie prowadzi to do naruszenia jego obowiązków pracowniczych polegających w szczególności na dbaniu o dobro zakładu pracy i zachowaniu w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę (obowiązek lojalności; nienaruszania interesów pracodawcy – art. 100 § 2 pkt 4 Kodeksu pracy), a także na przestrzeganiu zakładowych zasad współżycia społecznego (art. 100 § 2 pkt 6 Kodeksu pracy; pracownik nie może pochopnie, w sposób uzasadniony tylko względami subiektywnymi, formułować negatywnych opinii wobec pracodawcy lub jego przedstawicieli). Podkreślenia wymaga, że chodzi o obowiązki pracownicze, a więc obowiązki pracownika wobec pracodawcy, a nie wobec osób fizycznych reprezentujących pracodawcę.

«Dozwolona krytyka» musi cechować się rzeczowością, rzetelnością, adekwatnością do konkretnych okoliczności faktycznych oraz odpowiednią formą. Podstawową cechą dozwolonej krytyki jest «dobra wiara» pracownika, czyli jego subiektywne przekonanie, że opiera krytykę na faktach zgodnych z prawdą (przy dochowaniu należytej staranności w ich sprawdzeniu) oraz działa w usprawiedliwionym interesie pracodawcy"[22].

Dla wyznaczenia zakresu wolności słowa sygnalisty należy wziąć pod uwagę także orzecznictwo Trybunału Strasburskiego, które kształtuje sposób rozumienia praw człowieka w Polsce. W szczególności doprecyzowuje ono obowiązek lojalności, który nie w każdym zawodzie jest taki sam w stosunku do pracodawcy.

[22] Wyrok Sądu Najwyższego z dnia 28 sierpnia 2013 r., sygn. akt I PK 48/13.

W zawodach, w których obowiązek ten jest szczególnie silny, granice wolności słowa są węższe.

Najwyższego stopnia lojalności wymaga się od funkcjonariuszy służb mundurowych. Służba w formacjach mundurowych (np. w wojsku, policji czy też służbach specjalnych) wiąże się z obowiązkiem zachowania szczególnej lojalności wobec przełożonych oraz dbałości o dobre imię jednostki i dyscyplinę, bez której służby te nie mogą właściwie funkcjonować. Nie pozbawia to jednak funkcjonariuszy zupełnie prawa do krytyki i w pewnych sytuacjach także oni powinni być chronieni przed negatywnymi konsekwencjami za sygnalizowanie nieprawidłowości[23]. Wysokiego stopnia lojalności wymaga się ponadto od urzędników, w tym w szczególności służby cywilnej[24].

Niższego stopnia lojalności wymaga się natomiast np. od dziennikarzy, szczególnie mediów publicznych. Jak stwierdził ETPC, obowiązek lojalności pracowników wobec pracodawcy nie może mieć jednakowej mocy wiążącej w odniesieniu do dziennikarzy, ponieważ istotą tego zawodu jest wolność głoszenia informacji i opinii. Dziennikarze mają prawo, a nawet obowiązek, komentowania spraw o znaczeniu publicznym, w tym także tych odnoszących się do organizacji pracy czy funkcjonowania mediów realizujących misję publiczną[25].

Ochrona dziennikarzy-sygnalistów

Jedną ze spraw dziennikarzy-sygnalistów, którą zajmowała się HFPC, była sprawa red. J.W. Sprawa ta zaczęła się od krytyki przez red. J.W. ówczesnego prezesa publicznej rozgłośni radiowej, w której dziennikarz pracował. J.W. kwestionował kompetencje prezesa do prowadzenia rozgłośni oraz zarzucał mu, że został wybrany z klucza politycznego. W konsekwencji obniżyła się jakość audycji radia. W reakcji na krytykę prezes zaczął stopniowo ograniczać wymiar pracy dziennikarza, co bezpośrednio przekładało się na zmniejszenie jego wynagrodzenia. Ponadto prezes izolował dziennikarza i wyrażał o nim niepochlebne opinie przy innych pracownikach, a także kwestionował status pokrzywdzonego, jaki red. J.W. otrzymał od IPN. Wreszcie

[23] Wyrok ETPC z dnia 25 listopada 1997 r. w sprawie *Grigoriades p. Grecji*, skarga nr 24348/94); wyrok ETPC z dnia z 20 maja 1999 r. w sprawie *Rekvenyi p. Węgrom*, skarga nr 24348/94. Zob. także wyrok ETPC z dnia 8 stycznia 2013 r. w sprawie *Bucur i Toma p. Rumunii*, skarga nr 40238/02 – opisany w rozdziale III.

[24] Wyrok ETPC z dnia 2 lutego 2008 r. w sprawie *Guja p. Mołdawii*, skarga nr 14277/04.

[25] Wyrok ETPC z dnia 29 lutego 2000 r. w sprawie *Fuentes Bobo p. Hiszpanii*, skarga nr 39293/98; wyrok ETPC z dnia 16 lipca 2009 r. w sprawie *Wojtas-Kaleta p. Polsce*, skarga nr 20436/02.

dziennikarz został zwolniony, a gdy sąd uznał jego wypowiedzenie za bezpodstawne i nakazał przywrócenie go do pracy, prezes zwlekał z wykonaniem wyroku. W kolejnym procesie sąd nie miał wątpliwości, że działania prezesa spełniały przesłanki mobbingu i opierając się na art. 943 Kodeksu pracy przyznał dziennikarzowi 20 tys. zadośćuczynienia za rozstrój zdrowia[26].

7. Czy warto wprowadzać wewnętrzne regulacje dotyczące sygnalizowania nieprawidłowości? Kiedy stanowią one nadmierne ograniczenie wolności słowa?

Omówiony wyżej obowiązek lojalności pracowników wynikający z Kodeksu pracy (dalej: k.p.) może być doprecyzowany w regulaminie pracy czy też umowie o pracę. Ograniczenia wolności wypowiedzi wynikające z przepisów wewnętrznych nie mogą być jednak niezgodne z powszechnie obowiązującym prawem, w tym ze standardami ochrony wolności słowa. Przykładem niezgodnych z prawem regulacji wewnętrznych są przyjmowane przez niektórych pracodawców, w nieuzasadnionej obawie przed działalnością sygnalistów, specjalne regulacje wewnętrzne określane jako „klauzule kneblujące" (ang. *gagging clauses*), których celem jest uniemożliwienie działalności sygnalizacyjnej.

Zakaz wypowiedzi o pracodawcy w internecie

W aneksie do umów o pracę w jednej z miejskich spółek wykonującej zadania użyteczności publicznej w mieście W. zawarto następujący fragment: „Pracownik nie będzie składać publicznych oświadczeń, pisemnych lub ustnych, dotyczących Pracodawcy. Powyżej określony zakaz dotyczy także jakichkolwiek wypowiedzi i innych aktywności na forach internetowych portalach społecznościowych i innych tego typu serwisach sieciowych dotyczących Pracodawcy lub jego personelu". Taki zapis wprowadzono w związku z założeniem przez pracowników forum w internecie, na którym wymieniali komentarze o swoim pracodawcy.

Tak szeroki zakaz sprawił, że w praktyce jakiekolwiek kwestie związane z funkcjonowaniem spółki zostały w zasadzie wyłączone z debaty publicznej. Pracownik jest zobowiązany dbać o dobre imię pracodawcy, jednak nie można

[26] Wyrok Sądu Rejonowego w Łodzi z dnia 23 maja 2011 r., sygn. akt XP 263/09. Wyrok został utrzymany w mocy przez Sąd Okręgowy.

całkowicie pozbawiać go prawa do wyrażania poglądów związanych ze swoim miejscem pracy, a w pewnych sytuacjach także prawa do krytyki. Szczególnie gdy mamy do czynienia z miejską spółką, która wykonuje zadania publiczne.

„Klauzule kneblujące" mogą także ingerować w inne zagwarantowane konstytucyjnie wolności i prawa, w tym w szczególności w wolność zrzeszania się w związkach zawodowych poprzez uniemożliwienie przekazania jakichkolwiek informacji związkowi zawodowemu, który reprezentuje pracownika. W kontekście działalności związkowej ETPC w jednym z wyroków dotyczących działalności sygnalizacyjnej przypisał reprezentantom związków swoiste domniemanie dobrej wiary w działalności sygnalizacyjnej[27].

Interwencja HFPC na prośbę związku zawodowego

Pracownikom szpitala w S. zostało przedłożone do podpisu „Zobowiązanie Pracownika do zachowania Tajemnicy Zawodowej i Poufności". Dokument ten zakazywał pracownikom „rozpowszechnienia w jakiejkolwiek formie wszystkich dostępnych pracownikowi informacji dotyczących pracodawcy, podejmowanych przez pracodawcę czynności i zamierzonych działań, tak podejmowanych na zewnątrz, jak i w odniesieniu do zakładu pracy".

Na prośbę przedstawicieli związku HFPC skierowała do władz szpitala pismo interwencyjne, wskazując w nim na zbyt szeroki zakres zakazu wypowiedzi i jego potencjalną niezgodność z gwarancjami wolności słowa oraz wolnością zrzeszania się w związkach zawodowych. Wprowadzanie tak szerokich ograniczeń dla swobody wypowiedzi pracowników budzi tym większe wątpliwości, że w dokumencie nie wprowadzono jednocześnie żadnej wewnętrznej procedury pozwalającej im informować o nieprawidłowościach w funkcjonowaniu zakładu pracy w bezpieczny sposób, bez narażenia się na negatywne konsekwencje. Odpowiednia wewnętrzna procedura sygnalizowania dostrzeganych nieprawidłowości nie tylko chroniłaby interesy pracowników, ale sprzyjałaby również eliminowaniu nadużyć w miejscu pracy, zapewniając przy tym ochronę dobrego imienia spółki[28].

[27] Wyrok ETPC z dnia 19 lutego 2009 r. w sprawie *Marchenko p. Ukrainie*, skarga nr 4063/04.

[28] Zob. list HFPC z 17 grudnia 2015 r. do prezesa Wojewódzkiego Szpitala w S. http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4782:prawo-pielgniarek-i-poonych-do-sygnalizowania-o-nieprawidowociach&catid=47:aktualnosciprog&Itemid=66 (dostęp: 15 marca 2016 r.).

W sytuacji gdy wprowadza się obostrzenia dla wolności słowa, pracodawca powinien jednocześnie, dla równowagi, wprowadzić wewnętrzne procedury sygnalizowania nieprawidłowości, podobne do funkcjonujących obecnie procedur antymobbingowych.

Do wdrażania wewnętrznych procedur sygnalizowania nieprawidłowości pracodawców zachęca m.in. Transparency International[29], rekomendując, by tego typu procedury były bezpieczne (np. anonimowe), łatwo dostępne, gwarantowały rzetelne, niezależne i mieszczące się w rozsądnym czasie sprawdzenie zgłoszonych informacji. Ponadto procedury te powinny mieć wbudowany mechanizm monitorowania wyników danego zgłoszenia, a także ich funkcjonowania.

Wewnętrzne procedury a ustawa o ochronie danych osobowych

Wprowadzenie wewnętrznych procedur sygnalizowania nieprawidłowości wiąże się z koniecznością przestrzegania przez pracodawcę ustawy o ochronie danych osobowych[30]. W szczególności będą to obowiązki określone przez art. 23 ust.1 pkt 5, zgodnie z którym przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą[31].
W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę bezpośrednio po utrwaleniu zebranych danych m.in. o źródle danych. Z tego powodu niezwykle istotną gwarancją wewnętrznych procedur sygnalizowania nieprawidłowości powinna być możliwość anonimowego zgłoszenia nieprawidłowości. Z drugiej strony dla zagwarantowania anonimowości sygnalisty informacja administratora danych dla podmiotu danych powinna się sprowadzać jedynie do ogólnego wskazania źródła, którym jest wewnętrzny system sygnalizowania.

[29] Ang. *Internation Principles for Whistleblower Legislation Best practices for laws to protect whistleblowers and support whistleblowing in the public interest.* http://www.transparency.org/whatwedo/publication/international_principles_for_whistleblower_legislation (dostęp:15 marca 2016 r.).

[30] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r. poz. 2135 j.t.).

[31] P. Litwiński, *Korporacyjne systemy raportowania nadużyć (whistleblowing hotlines) a ochrona danych osobowy*ch [w:] A. Mednis (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013, s. 113-127.

Jak stworzyć skuteczną procedurę sygnalizowania wewnątrz organizacji?

Dużą popularność zyskały standardy opisujące wewnętrzne procedury sygnalizowania, wypracowane przez Międzynarodową Izbę Handlu[32] oraz amerykańską organizację pozarządową Government Accountability Project[33]. Standardy te mogą być pomocne w skonstruowaniu odpowiedniej procedury w miejscu pracy.

8. Na jakie negatywne konsekwencje może być narażony sygnalista?

Decyzja o zasygnalizowaniu nieprawidłowości może wiązać się z rozmaitymi konsekwencjami, zarówno prawnymi, jak i społecznymi. Sygnalista może spotkać się z ostracyzmem środowiskowym, współpracownicy mogą się od niego odwrócić, może zostać pozbawiony różnych dodatków do pensji, nagród i innych środków motywacyjnych, także stanowiących znaczną część wynagrodzenia. Może także zostać ukarany dyscyplinarnie: upomnieniem, naganą, a w skrajnych przypadkach nawet zwolnieniem z pracy. W przypadku gdy sygnalista jest pracownikiem, jego umowa o pracę może zostać wypowiedziana, może nastąpić rozwiązanie umowy o pracę bez wypowiedzenia lub może otrzymać wypowiedzenie zmieniające warunki pracy. W sytuacji gdy demaskator jest związany innym stosunkiem zatrudnienia niż stosunek pracy, jego związki z danym podmiotem mogą zostać zerwane, np. gdy jest mundurowym, może zostać zwolniony ze służby. Podmiot, w którego działaniu demaskator ujawnił nieprawidłowości, może wystąpić przeciwko niemu na drogę sądową, oskarżając go o zniesławienie czy też naruszenie dóbr osobistych. Zdarza się, że pracodawcy wykorzystują nie tylko jedno z przedstawionych narzędzi, ale kilka z nich jednocześnie.

Jedna sygnalistka i dwa procesy

W jednej ze spraw, w jakie była zaangażowana HFPC, lekarka zauważyła szereg nieprawidłowości w instytucie medycznym, w którym pracowała. O dostrzeżonych nieprawidłowościach poinformowała dyrekcję szpitala, odpowiedniego konsultanta wojewódzkiego, Ministerstwo Zdrowia i Najwyższą Izbę Kontroli. Gdy działania te nie

[32] http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/corporate--responsibility-and-anti-corruption/whistleblowing/ (dostęp: 15 marca 2016 r.).

[33] https://whistleblowingnetwork.org/other-resources/europe-and-international/international-best-practices-for-whistleblower-policies/ (dostęp: 15 marca 2016 r.).

przyniosły skutku, udzieliła wywiadu gazecie. Wywiad stał się bezpośrednią przyczyną jej zwolnienia ze szpitala, a także jednoczesnego oskarżenia o zniesławienie. Lekarka musiała równolegle zaangażować się w dwa procesy: przed sądem pracy oraz przed sądem karnym. Dodatkowo szpital wytoczył pozew o ochronę dóbr osobistych przeciwko dziennikarce, której sygnalistka udzieliła wywiadu.

W tym miejscu warto przypomnieć, że pracodawca nie dysponuje niczym nieograniczoną swobodą w sięganiu po sankcje wymierzane sygnaliście. W tym zakresie powinien kierować się zasadą proporcjonalności. Wielokrotnie zwracał na to uwagę m.in. Europejski Trybunał Praw Człowieka, który podkreśla, że zbyt surowa kara dla sygnalisty może doprowadzić do nieuzasadnionej ingerencji w wolność słowa (zobacz wyżej pkt 3). Dyrektywa proporcjonalności sankcji może stanowić ważny argument przed sądem pracy, przesądzającym np. o bezprawności zwolnienia pracownika.

Co więcej, zbyt ostra reakcja pracodawcy może wywołać tzw. efekt mrożący w stosunku do wszystkich pracowników, którzy w przyszłości mogą bać się wypowiadania jakiejkolwiek krytyki w obawie przed negatywnymi konsekwencjami.

9. Jak się bronić w sądzie?

9.1. Do kogo sygnalista może zwrócić się o pomoc i jak powinien przygotować się do obrony?

Mając powyższe na uwadze, w tym miejscu zamieszczamy podstawowe wskazówki, jak bronić się przed najczęściej spotykanymi w praktyce atakami na sygnalistów. Przed sądem można występować samodzielnie lub z profesjonalnym pełnomocnikiem (adwokatem, radcą prawnym), który zadba o interesy demaskatorów w toku postępowania. Z prawnikiem mającym doświadczenie w tego typu sprawach warto także skonsultować ewentualną decyzję o zasygnalizowaniu nieprawidłowości przed ich ujawnieniem, aby mieć jak największą świadomość związanego z tym ryzyka.

Do kogo można zwrócić się o pomoc?

Prawo przewiduje możliwość ustanowienia profesjonalnego pełnomocnika lub obrońcy z urzędu osobom, których nie stać na jego opłacenie. W postępowaniu przed sądami administracyjnymi zasady udzielania tzw. prawa pomocy regulują artykuły 140-263 ustawy Prawo o postępowaniu przed sądami administracyjnymi[34], w postępowaniu cywilnym – art. 117 Kodeksu postępowania cywilnego[35], w postępowaniu karnym – art. 78 Kodeksu postępowania karnego[36].

Jeszcze przed rozpoczęciem procedury sądowej (czyli zanim nastąpi np. wniesienie powództwa do sądu) istnieje możliwość skorzystania z bezpłatnej pomocy prawnej. Zasady jej udzielania określa ustawa z dnia 5 sierpnia 2015 r. o nieodpłatnej pomocy prawnej oraz edukacji prawnej[37].

Ze sprawą można także zgłosić się do organizacji pozarządowych działających na rzecz ochrony sygnalistów. Organizacja pozarządowa może wesprzeć demaskatora m.in. przez włączenie się w proces bądź obserwując jego przebieg.

W sytuacji gdy sygnalista jest pracownikiem, może się zwrócić do reprezentujących go związków zawodowych, które mają prawo wystąpić w obronie interesów pracownika.

Cechą wspólną opisanych niżej postępowań sądowych jest konieczność zgromadzenia przez sygnalistę materiału dowodowego, potwierdzającego ujawnione informacje. Będą to w szczególności wszelkiego rodzaju notatki służbowe, kopie e-maili, pisma zarówno do podmiotów zewnętrznych, jak i znajdujących się wewnątrz danej organizacji, zeznania świadków, które zgodzą się złożyć w sądzie. Warto przy tym pamiętać, że świadkowie, którzy zgodzili się zeznawać przed zasygnalizowaniem nieprawidłowości, mogą później się wycofać, np. w obawie przed utratą pracy.

[34] Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2012 r. poz. 270 j.t.).

[35] Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2014 r. poz. 101 j.t.).

[36] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 1997 r. Nr 89 poz. 555 ze zm.).

[37] Szczegóły i praktyczne wskazówki dotyczące korzystania z bezpłatnej pomocy prawnej dostępne są na specjalnej stronie Ministerstwa Sprawiedliwości: https://darmowapomocprawna.ms.gov.pl/pl/ (dostęp: 15 marca 2016 r.).

Gromadzenie odpowiednich dowodów jest także niezbędne z uwagi na fakt, że dostrzegane przez sygnalistów nieprawidłowości mogą stanowić przestępstwo. W przypadku zgłoszenia zawiadomienia o podejrzeniu popełnienia przestępstwa sygnalista musi uprawdopodobnić swoje zarzuty. W innym przypadku postępowanie karne zostanie umorzone, a odwołanie się sygnalisty od takiej decyzji często może być niemożliwe z uwagi na to, że nie jest on stroną w sprawie.

9.2. Jak się bronić w sądzie pracy?

Jak zostało wspomniane wcześniej, polskie prawo nie przewiduje specjalnych gwarancji dla sygnalistów-pracowników. Dlatego w wypadku wypowiedzenia umowy o pracę, rozwiązania umowy o pracę bez wypowiedzenia czy też wypowiedzenia zmieniającego warunki pracy sygnaliści mogą odwołać się, podobnie jak i inni pracownicy, do sądu pracy (zob. w szczególności art. 44 k.p.[38], art. 56 k.p. i następne). W zależności od rodzaju umowy o pracę oraz trybu jej rozwiązania pracownik może domagać się uznania wypowiedzenia za bezskuteczne, przywrócenia do pracy bądź odszkodowania. Pracownik-sygnalista może także powoływać na przepisy antymobbingowe (art. 94^3 k.p.) oraz przepisy o równym traktowaniu (art. 18^3 k.p.).

Co do zasady pracownik, kierując sprawę do sądu, nie wnosi opłaty. Zgodnie z art. 35 ustawy z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych, w przypadku spraw z zakresu prawa pracy pobiera się opłatę podstawową w kwocie 30 złotych wyłącznie od apelacji, zażalenia, skargi kasacyjnej i skargi o stwierdzenie niezgodności z prawem prawomocnego orzeczenia. Jednakże w sprawach, w których wartość przedmiotu sporu przewyższa kwotę 50 tys. złotych, pobiera się od wszystkich podlegających opłacie pism procesowych opłatę stosunkową.

Z powyższego przeglądu wynika, że pracownik-sygnalista jest chroniony przez przepisy prawa pracy. Jak wskazują jednak badania sędziów sądów pracy wykonane przez Fundację Batorego, przepisy te w praktyce nie zapewniają często należytej ochrony pracownikowi-sygnaliście[39]. Pracownik formalnie nie jest zwalniany z powodu sygnalizowania nieprawidłowości, ale zwykle jako przyczynę zwolnienia wskazuje się szereg jego innych niedociągnięć. W takiej sytuacji powinien on w sądzie pracy kwestionować wskazany w wypowiedzeniu umowy powód jej rozwiązania jako pozorny.

[38] Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2014 r. poz. 1502 j.t.).

[39] A. Wojciechowska-Nowak, *Ochrona prawna sygnalistów w doświadczeniu sędziów sądów pracy. Raport z badań*, Warszawa 2011, s. 95-97.

Sygnalista niesłusznie zwolniony

J.D., strażak przyzakładowej straży pożarnej, dowiedział się o nieprawidłowościach w funkcjonowaniu swojej jednostki, polegających na kradzieży paliwa dokonywanej przez zatrudnionych w jednostce strażaków oraz nadużywaniu przez nich alkoholu. O fakcie tym zawiadomił on prokuraturę, która jednak umorzyła postępowanie. W następstwie swoich działań strażak został zwolniony. Od zwolnienia odwołał się do sądu pracy, który w uzasadnieniu wyroku stwierdził, że „zaangażowana postawa powoda (sygnalisty), jak również zwracanie uwagi na niewłaściwe zachowanie pracowników w kontekście potwierdzonych wypadków świadczenia pracy pod wpływem alkoholu oraz sygnalizowanie podejrzenia niewłaściwego rozliczenia paliwa nie powinno prowadzić do postawienia pracownikowi zarzutu działania na niekorzyść spółki”[40]. Sprawa zakończyła się zasądzeniem sygnaliście odszkodowania[41].

9.3. Jak się bronić przed oskarżeniem o zniesławienie?

Sygnalista na podstawie art. 212 Kodeksu karnego (dalej: k.k.)[42] może zostać oskarżony o popełnienie przestępstwa zniesławienia, tj. pomówienia danej osoby czy podmiotu o postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności. Występek ten ściga się z oskarżenia prywatnego (tj. co do zasady pokrzywdzony sam wnosi akt oskarżenia i popiera go przed sądem, postępowanie odbywa się bez udziału prokuratora). Za jego popełnienie k.k. przewiduje karę grzywny albo karę ograniczenia wolności. W sytuacji gdy do pomówienia dochodzi za pośrednictwem środków masowego komunikowania się (w tym w internecie, np. na portalach Facebook czy Twitter), sprawcy grozi grzywna, kara ograniczenia wolności albo kara pozbawienia wolności do roku.

Statystyki wskazują, że sądy najczęściej sięgają po sankcję grzywny[43]. Warto jednak pamiętać, że w przypadku skazania nawet na najniższą karę znacznie bardziej dotkliwe mogą okazać się „skutki uboczne” takiego wyroku (przede wszystkim wpis do Krajowego Rejestru Karnego, uniemożliwiający często zatrudnienie na

[40] Historia opisana przez Fundację Batorego na stronie Sygnalista.pl, http://www.sygnalista.pl/ (dostęp: 15 marca 2016 r.).

[41] Wyrok Sądu Rejonowego w Kędzierzynie-Koźlu z dnia 13 września 2011 r., sygn. akt IV P 2/10.

[42] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88 poz. 553).

[43] Zob. D. Głowacka, *Praktyczny przewodnik po art. 212 k.k.*, Warszawa 2012, s. 21.

określonym stanowisku w sektorze publicznym, otrzymanie kredytu lub dotacji) czy też dolegliwości związane z samym prowadzeniem postępowania karnego. Chodzi przede wszystkim o obowiązek osobistego stawiennictwa na rozprawach, możliwość zastosowania przymusowego doprowadzenia na rozprawę w razie nieusprawiedliwionej nieobecności lub możliwość stosowania środków zapobiegawczych.

Obrona przed zarzutem zniesławienia powinna opierać się na wskazaniu spełnienia przesłanek uwalniających od odpowiedzialności karnej. Przesłanki te zostały uregulowane w art. 213 k.k. Ich wypełnienie sprawia, że osoba podnosząca określone zarzuty w istocie nie popełnia przestępstwa zniesławienia i wobec tego powinna zostać uniewinniona przez sąd. W skrócie rzecz ujmując, należy udowodnić prawdziwość zarzutów – w tym przypadku ujawnianych informacji – oraz, jeśli zarzut został podniesiony publicznie (np. w mediach, liście otwartym, internecie), należy wykazać, że służy obronie społecznie uzasadnionego interesu. Ta ostatnia przesłanka jest zbieżna z tym, że wymogiem objęcia sygnalistów ochroną jest działanie w interesie publicznym.

Przykładem sprawy, w której sygnalistce udało się obronić przed zarzutem zniesławienia, jest przytoczona wcześniej sprawa lekarki, ujawniającej w wywiadzie prasowym nieprawidłowości w funkcjonowaniu szpitala. Lekarka została uniewinniona od zarzutu zniesławienia przez sąd pierwszej instancji[44] (zob. pyt. 8).

Kodeks karny

§

Art. 213 § 1. Nie ma przestępstwa określonego w art. 212 § 1, jeżeli zarzut uczyniony niepublicznie jest prawdziwy.

§ 2. Nie popełnia przestępstwa określonego w art. 212 § 1 lub 2, kto publicznie podnosi lub rozgłasza prawdziwy zarzut:
1) dotyczący postępowania osoby pełniącej funkcję publiczną lub
2) służący obronie społecznie uzasadnionego interesu.

Jeżeli zarzut dotyczy życia prywatnego lub rodzinnego, dowód prawdy może być przeprowadzony tylko wtedy, gdy zarzut ma zapobiec niebezpieczeństwu dla życia lub zdrowia człowieka albo demoralizacji małoletniego.

[44] Wyrok Sądu Rejonowego dla Warszawy-Mokotowa w Warszawie z dnia 26 stycznia 2016 r., sygn. akt VIII K 161/14. W chwili oddawania Przewodnika do druku wyrok nie był jeszcze prawomocny.

W sytuacji gdy wypowiedź stanowiła opinię, a nie twierdzenie o faktach, nie trzeba dowodzić jej prawdziwości.

Krytyczne opinie o pracodawcy nie są zniesławieniem

HFPC zaangażowała się w sprawę niepełnosprawnego mężczyzny, który nazwał firmę swojego byłego pracodawcę na forum internetowym „polskim obozem pracy". Mężczyzna ten twierdził, że w firmie mającej status zakładu pracy chronionej dochodziło do naruszeń zasad bezpieczeństwa pracy. Nieprawidłowości te doprowadziły zdaniem oskarżonego do wypadku w firmie, na skutek którego ucierpiał, przez co podwyższono mu stopień niepełnosprawności i zalecono wykonywanie lżejszych prac w mniejszym wymiarze godzin. W konsekwencji firma rozwiązała z nim umowę o pracę. Za swoją późniejszą wypowiedź na forum internetowym mężczyzna został oskarżony o zniesławienie.

Sąd Rejonowy w Bydgoszczy wyrokiem z 3 lutego 2014 r. uniewinnił oskarżonego od popełnienia zarzucanego mu czynu, stwierdzając m.in., że tekst, który zamieścił na portalu, był sądem wartościującym (opinią), który nie mieścił się w zakresie art. 212 k.k.[45]

Bardziej rozbudowane informacje o obronie przed zarzutem zniesławienia, a także dodatkowe argumenty, które można podnieść przed sądem, zawiera przewodnik wydany przez Helsińską Fundację Praw Człowieka pt. „Praktyczny przewodnik po art. 212 k.k.". Publikacja ta dostępna jest na stronie programu Obserwatorium Wolności Mediów w Polsce HFPC[46].

[45] Wyrok Sądu Rejonowego w Bydgoszczy z dnia 3 lutego 2014 r., sygn. akt VI K 445/13/MK. Wyrok jest prawomocny. Na prośbę Helsińskiej Fundacji Praw Człowieka obrońcą pro bono oskarżonego był mec. Jakub Czarnecki z kancelarii Fiks Korpecki Czarnecki Adwokaci. HFPC obserwowała także postępowanie przed sądem.

[46] http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4479:praktyczny-przewodnik-po-art-212-kk-broszura-informacyjna&catid=51:publikacjerozne&Itemid=41 (dostęp: 15 marca 2016 r.).

9.4. Jak się bronić przed zarzutem naruszenia dóbr osobistych?

Cześć, dobre imię osoby fizycznej i innych podmiotów oraz inne wartości określane jako dobra osobiste podlegają na gruncie prawa polskiego ochronie także na podstawie przepisów Kodeksu cywilnego (dalej: k.c.)[47]. Zgodnie z art. 24 k.c. „ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne". W przypadku naruszenia dóbr osobistych można żądać usunięcia skutków naruszenia dóbr osobistych, np. przeprosin, a także zadośćuczynienia (art. 448 k.c.) lub odszkodowania w przypadku wystąpienia szkody majątkowej spowodowanej ujawnioną informacją.

W sytuacji gdy podmiot, w odniesieniu do którego zostały ujawnione informacje, zarzuca sygnaliście naruszenie jego dóbr osobistych, sygnalista powinien wykazać w postępowaniu przed sądem, że jego działanie było zgodne z prawem. Istnienie interesu społecznego uzasadniającego naruszenie czci (łączącego w sobie obronę społecznie uzasadnionego interesu, obronę uzasadnionego interesu publicznego lub prywatnego, cel społeczny działania itp.) może być uznane za okoliczność wyłączającą bezprawność naruszenia dóbr osobistych[48].

9.5. Jak się bronić przed zarzutem naruszenia zasad etyki?

W niektórych zawodach obowiązują kodeksy etyczne, które rozszerzają zakres obowiązków pracowniczych. Jeśli kodeks etyczny jest częścią regulaminu albo układu zbiorowego pracy, jego naruszenie może być nawet podstawą do rozwiązania stosunku pracy. W innych przypadkach kodeksy etyczne są podstawą odpowiedzialności zawodowej (dyscyplinarnej). Odpowiedzialność ta ma swoje granice, czego najlepszym przykładem są orzeczenia ETPC, w których uznał on za naruszenie wolności słowa dyscyplinarne zwolnienie z pracy lekarzy krytykujących swoich kolegów[49].

Sygnaliści i zasady etyki lekarskiej

Barbara Sosinowska była specjalistką z zakresu chorób płuc w szpitalu w Rudzie Śląskiej. Kilka lat temu (w 2004 r.) krytycznie oceniła decyzje swojej przełożonej dotyczące diagnoz i terapii pacjentów. Napisała w tej sprawie m.in.

[47] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2014 r. poz. 121 j.t.).

[48] A. Pązik, *Wyłączenie bezprawności naruszenia dobra osobistego na podstawie interesu społecznego*, Warszawa 2014, LEX el.

[49] Wyrok ETPC z dnia 18 października 2011 r. w sprawie *Sosinowska p. Polsce*, nr skargi 10247/09; wyrok ETPC z dnia 16 grudnia 2008 r. w sprawie *Frankowicz p. Polsce,* nr skargi 53025/99.

list do regionalnego konsultanta medycznego w dziedzinie chorób płuc. Przeciwko lekarce wszczęto postępowanie dyscyplinarne, zarzucając jej naruszenie zasad etyki zawodowej. Miało do tego dojść przez otwartą krytykę decyzji diagnostycznych i terapeutycznych przełożonej w obecności innych kolegów ze szpitala – tak uznały sądy lekarskie, skazując B. Sosinowską na karę nagany. Na tę decyzję lekarka wniosła skargę do ETPC.
Trybunał uznał, że doszło do naruszenia swobody wypowiedzi lekarki. Zdaniem Trybunału jej krytyka była merytoryczna, a działanie zmierzało do zwrócenia uwagi właściwych organów na poważną, w jej przekonaniu, dysfunkcję w pracy jej zwierzchniczki. Trybunał zauważył, że sądy lekarskie nie wzięły w ogóle pod uwagę, czy opinia lekarki była uzasadniona i wyrażona w dobrej wierze oraz czy zmierzała do ochrony interesu publicznego. Sądy dyscyplinarne skupiły się wyłącznie na fakcie skrytykowania innego lekarza, co Kodeks Etyki Lekarskiej uznawał za wykroczenie dyscyplinarne. Taka interpretacja, jak stwierdził Trybunał, rodzi ryzyko, że lekarze będą rezygnowali z udzielania pacjentom obiektywnych informacji o stanie ich zdrowia w obawie przed sankcjami dyscyplinarnymi.

9.6. Co grozi za ujawnienie tajemnicy zawodowej?

Na niektórych sygnalistach z uwagi na wykonywany przez nich zawód ciąży obowiązek zachowania w tajemnicy informacji uzyskiwanych przy okazji wykonywania zawodu. Są to np. takie zawody jak: lekarze, pielęgniarki, tłumacze przysięgli, detektywi czy celnicy. Obowiązek ten może wynikać z przepisów ustawy oraz przyjętego na siebie zobowiązania. Zgodnie z art. 266 k.k. ujawnienie lub wykorzystanie informacji, z którą sygnalista zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, pomimo ciążącego obowiązku stanowi przestępstwo zagrożone karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do lat 2.

W sytuacji gdy sygnalista jest funkcjonariuszem publicznym, ujawniającym osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega on karze pozbawienia wolności do lat 3.

Obrona przed zarzutem naruszenia tajemnicy zawodowej wymaga od sygnalisty przede wszystkim wykazania, że dana informacja nie była objęta tajemnicą zawodową.

Uwaga! Jak podkreślono w jednym z wyroków Sądu Najwyższego, w pewnych okolicznościach dopuszczalne jest opublikowanie przez dziennikarzy w interesie publicznym informacji objętych tajemnicą ustawowo strzeżoną, taką jak np. tajemnica skarbowa. Ujawnienie takich informacji przez osoby, na których ciąży obowiązek zachowania tej tajemnicy jest przestępstwem zgodnie z art. 306 § 1-2 ustawy Ordynacja podatkowa[50]. Katalog podmiotów zobowiązanych do zachowania tajemnicy skarbowej określa ordynacja podatkowa (są to np. urzędnicy skarbowi). Dziennikarze nie znajdują się jednak w gronie tych osób i w związku z tym nie mogą być sprawcami przestępstwa z art. 306 § 1-2 ordynacji podatkowej i zostać na tej podstawie pociągnięci do odpowiedzialności. Co więcej, opublikowanie w prasie informacji objętych tajemnicą skarbową, podjęte w obronie społecznie uzasadnionego interesu w konkretnych okolicznościach faktycznych, może wyłączać bezprawność takiej publikacji w przypadku procesu o ochronę dóbr osobistych przeciwko dziennikarzowi[51] (zob. więcej na temat tego wyroku w rozdziale II, pyt. 6).

10. Kiedy sygnalista może poskarżyć się do Europejskiego Trybunału Praw Człowieka?

W sytuacji gdy dana osoba spełnia wskazane wyżej warunki wypracowane przez orzecznictwo Trybunału Strasburskiego pozwalające na uznanie jej za sygnalistę, a mimo tego jej racje nie zostaną uznane przez polskie sądy, po uzyskaniu prawomocnego, ostatecznego wyroku sądu polskiego i spełnieniu innych wymogów określonych przez EKPC sygnalista może złożyć skargę do ETPC.

Kiedy sygnalista może wnieść skargę do Europejskiego Trybunału Praw Człowieka?[52]

1. Gdy jego wolność lub prawo zostało naruszone przez państwo-stronę Konwencji (skargi kierowane przeciwko osobom prywatnym, instytucjom państwowym czy fundacjom są uznawane za niedopuszczalne).
2. Gdy doszło do naruszenia prawa gwarantowanego przez Konwencję po wejściu w życie Konwencji w państwie-stronie (dla Polski jest to 1 maja 1993 r.).
3. Gdy skarżący wyczerpał krajowe środki odwoławcze.

[50] Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz.U. z 2012 r. poz. 749 ze zm.).

[51] Wyrok Sądu Najwyższego z dnia 27 listopada 2014 r., sygn. akt IV CSK 174/14.

[52] Zob. szerzej: *Praktyczny przewodnik w sprawie kryteriów dopuszczalności*, https://www.msz.gov.pl/resource/29734ee5-a2c2-4b2c-b09f-ce7f58b1fef3:JCR (dostęp: 15 marca 2016)

4. Jeżeli sprawa nie została poddana innej międzynarodowej procedurze (art. 35 ust. 2 Konwencji).
5. Gdy skarżący nie doznał znaczącego uszczerbku, chyba że poszanowanie praw człowieka w rozumieniu Konwencji i jej Protokołów wymaga rozpoznania przedmiotu skargi oraz pod warunkiem że żadna sprawa, która nie została należycie rozpatrzona przez sąd krajowy, nie może być odrzucona na tej podstawie.

Skargę należy złożyć w ciągu 6 miesięcy od wydania ostatecznego orzeczenia w sprawie.

Warunki dopuszczalności skargi oraz sposób i tryb jej składania do EKPC zostały opisane w europejskiej Konwencji praw człowieka i podstawowych wolności oraz w Regulaminie ETPC. Z zasadami wniesienia skargi można się zapoznać także na stronie internetowej Trybunału (w jęz. polskim)[53].

W skardze skarżący może się domagać stwierdzenia naruszenia wskazanych praw lub wolności z EKPC (w przypadku sygnalistów będzie to najczęściej art. 10 Konwencji) lub zapłaty zadośćuczynienia. W przypadku skazania w procesie karnym, po korzystnym wyroku ETPC, skarżący będzie mógł wnioskować o wznowienie postępowania na poziomie krajowym (zob. art. 540 § 3 Kodeksu postępowania karnego).

11. Gdzie można przeczytać więcej o sygnalistach?

Publikacje

• Kobylińska A., Folta, M., *Sygnaliści – ludzie, którzy nie potrafią milczeć: oświadczenia osób ujawniających nieprawidłowości w instytucjach i firmach w Polsce*, Instytut Spraw Publicznych, Warszawa 2015.
• Krzyżanowska-Mierzewska M., Rutkowska A., *Zagadnienia prawne związane z ochroną whistleblowerów w warunkach zatrudnienia w ujęciu orzecznictwa ETPCz*, „Przegląd Sądowy" 2015, nr 4, s. 106-122.
• Ploszka A., *Ochrona demaskatorów (whistleblowers) w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Europejski Przegląd Sądowy" 2014, nr 4, s.12-18.
• Rada Europy, *Whistleblower protection: encouraging reporting*, www.oecd.org/cleangovbiz/toolkit/50042935.pdf.

[53] Zob. Informacja kancelarii Europejskiego Trybunału Praw Człowieka: W jaki sposób prawidłowo wnieść skargę indywidualną do Europejskiego Trybunału Praw Człowieka, http://www.echr.coe.int/Pages/home.aspx?p=applicants/pol&c (dostęp: 2 marca 2016 r.).

• G20, *Compendium of best practices and guiding principles for legislation on the protection of whistleblowers*, http://www.oecd.org/g20/topics/anti-corruption/48972967.pdf
• Świątkowski A.M., *Sygnalizacja (whistleblowing) a prawo pracy*, „Przegląd Sądowy" 2015, nr 5, s. 6-25.
• Wojciechowska-Nowak A., *Jak zdemaskować szwindel? Czyli krótki przewodnik po whistle-blowingu*, Warszawa 2008.
• Wojciechowska-Nowak, A. *Ochrona sygnalistów w Polsce. Stan obecny i rekomendacje zmian*, Warszawa 2012.
• Wojciechowska-Nowak A., *Założenia do ustawy o ochronie praw osób sygnalizujących nieprawidłowości środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych?*, Warszawa 2012.
• Wujczyk M., *Podstawy whistleblowingu w polskim prawie pracy*, „Przegląd Sądowy" 2014, nr 6, s. 114-122.

Strony internetowe

• Sygnalista.pl
Strona prowadzona przez Fundację im. Stefana Batorego, zawierająca przydatne wskazówki dla sygnalistów dotyczące sygnalizowania nieprawidłowości oraz ochrony demaskatorów.
• Nik.gov.pl
Strona Najwyższej Izby Kontroli, na której można dokonać zgłoszenia nieprawidłowości, mogących następnie stać się przedmiotem postępowania kontrolnego NIK.
• Pip.gov.pl/
Strona Państwowej Inspekcji Pracy, poprzez którą można złożyć skargę na naruszenia prawa pracy. Na stronie znajdują się także informacje, gdzie uzyskać bezpłatne porady prawne z zakresu prawa pracy.
• Antykorupcja.gov.pl
Strona prowadzona przez Centralne Biuro Antykorupcyjne, zawierająca przydatne informacje dotyczące sygnalizowania korupcji.
• Hfhr.pl
Strona prowadzona przez Helsińską Fundację Praw Człowieka, zwierająca m.in. wszystkie stanowiska i wystąpienia HFPC.

Rozdział II

Tajemnica dziennikarska. Gwarancje dla dziennikarzy i sygnalistów przekazujących im poufne informacje

Wprowadzenie

Tajemnica dziennikarska stanowi jedną z najistotniejszych gwarancji prawidłowego wykonywania zadań mediów w demokratycznym społeczeństwie. Chroni ona nie tylko dziennikarzy, ale m.in. także osoby, które przekazują im poufne informacje w celu publikacji i z różnych powodów chcą zachować anonimowość. Poza ściśle określonymi przez prawo sytuacjami dziennikarze mają obowiązek zachować w tajemnicy wszelkie informacje, które mogłyby prowadzić do identyfikacji ich źródeł. Dzięki instytucji tajemnicy dziennikarskiej z jednej strony informatorzy, który zastrzegli swoją anonimowość, mogą mieć pewność, że dziennikarz będzie chronił ich dane, a z drugiej – media mogą liczyć na dopływ informacji, których nie uzyskałyby bez istnienia takich gwarancji. Jak podkreśla się w doktrynie, „bywa tak, że inaczej, niż poprzez skorzystanie z anonimowych informacji (publikacji) nie można trafić na ślad patologicznego procederu, wymagającego ujawnienia i napiętnowania w prasie. Tymczasem informatorzy (autorzy), skorzy do przekazania odpowiednich informacji dziennikarzom (redakcjom) tylko poufnie, bez gwarancji dotrzymania tajemnicy, z reguły nie decydowaliby się na kontakt (współpracę) z prasą”[54].

Ze względu na znaczenie ochrony tajemnicy dziennikarskiej dla wolności słowa jest ona jednym z najważniejszych tematów, którymi zajmuje się HFPC w ramach programu Obserwatorium Wolności Mediów w Polsce. Wielokrotnie występowaliśmy w obronie dziennikarzy, wobec których organy ścigania lub inne instytucje prowadziły działania zmierzające do nieuprawnionego ujawnienia informacji objętych tajemnicą dziennikarską[55]. Podkreślaliśmy również konieczność respektowania gwarancji wynikających z tajemnicy przez samych dziennikarzy[56].

Tajemnica dziennikarska może stanowić ważne zabezpieczenie dla sygnalistów, zwłaszcza w kontekście braku odpowiednich regulacji prawnych zapewniających odpowiednią ochronę samym

[54] K. Gotkowicz, B. Kosmus, *Komentarz do art. 15 ustawy – Prawo prasowe* [w:] B. Kosmus, G. Kuczyński (red.), *Prawo prasowe. Koment arz*, Warszawa 2013, s. 129.

[55] Zob. np. Stanowisko HFPC w sprawie pozyskiwania billingów oraz treści informacji tekstowych z dnia 29 grudnia 2011 r., http://www.hfhr.pl/wp-content/uploads/2011/12/stanowisko_hfpc_29_grudnia_2011.pdf; stanowisko HFPC w sprawie poszanowania gwarancji tajemnicy dziennikarskiej z dnia 19 czerwca 2014 r., http://www.hfhr.pl/wp-content/uploads/2014/06/HFPC_stanowisko_19062014_FNL.pdf; Stanowisko HFPC w sprawie inwigilacji dziennikarzy z dnia 15 stycznia 2016 r., http://www.hfhr.pl/wp-content/uploads/2016/01/HFPC_stanowisko_inwigilacja_dziennikarzy.pdf (dostęp: 1 marca 2016 r.).

[56] Opinia przyjaciela sądu HFPC w sprawie naruszenia tajemnicy dziennikarskiej, http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4799:opinia-przyjaciela-sdu-w-sprawie-naruszenia-tajemnicy-dziennikarskiej&catid=40:zkraju&Itemid=34 (dostęp: 1 marca 2016 r.).

demaskatorom. Ze względu na silne gwarancje ochrony źródeł, funkcję kontrolną mediów, a także ich siłę oddziaływania na opinię publiczną sygnaliści często decydują się ujawniać poufne informacje za pośrednictwem dziennikarzy. Droga ta może być nie tylko bardziej bezpieczna niż np. samodzielne zamieszczenie materiałów w internecie, ale także wzmacniać wiarygodność upublicznionych informacji. Materiał przygotowany przez dziennikarza co do zasady daje odbiorcom rękojmię, że został opracowany w zgodzie z wymogami rzetelności dziennikarskiej, a ujawniona informacja została sprawdzona przez dziennikarza na podstawie innych źródeł. Przy czym, jak podkreślono w poprzednim rozdziale Przewodnika, zanim sygnalista ujawni nieprawidłowości na zewnątrz, powinien rozważyć wszystkie okoliczności danej sprawy takie jak: waga ujawnianej informacji, korzyści, które może osiągnąć, rozmiar potencjalnej szkody, którą może wywołać, czy możliwość wykorzystania wewnętrznej procedury naprawczej.

W tej części Przewodnika przedstawiamy podstawowe zagadnienia związane z ochroną tajemnicy dziennikarskiej. Wyjaśnimy, jakie uprawnienia i obowiązki wynikają z tej instytucji dla dziennikarzy oraz jakie gwarancje stwarza ona dla osób przekazujących poufne informacje mediom.

1. Czym jest tajemnica dziennikarska?

Tajemnica dziennikarska jest jedną z prawnie chronionych tajemnic zawodowych, nierozerwalnie związaną z wykonywaniem zadań, jakie powinny wypełniać media w demokratycznym społeczeństwie, a także z prawem obywateli do wiarygodnej i rzetelnej informacji. Bez niej media nie mogłyby realizować w pełni swojej funkcji kontrolnej tzw. publicznego stróża i swobodnie informować o sprawach budzących uzasadnione zainteresowanie opinii publicznej. Tajemnica dziennikarska jest uregulowana w przepisach prawa, a także na gruncie zasad etyki dziennikarskiej.

Istotne znaczenie tajemnicy dziennikarskiej dla pracy dziennikarzy oraz funkcjonowania wolnej prasy podkreśla się w doktrynie prawa, na gruncie międzynarodowego[57] oraz krajowego orzecznictwa sądów, a także standardów wypracowanych przez organizacje międzynarodowe, takie

[57] Europejski Trybunał Praw Człowieka, *Factsheet – journalistic sources protection*, styczeń 2016, http://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf (dostęp: 10 marca 2016 r.).

jak np. Organizacja Narodów Zjednoczonych[58] czy Rada Europy[59].

Przykładowo: zdaniem Sądu Najwyższego tajemnica zawodowa dziennikarza stanowi „istotny czynnik niezależności prasy i stwarza korzystne warunki dla uzyskania zaufania społecznego". Sąd Najwyższy stwierdził, że instytucja ta „pozwala dziennikarzom na własną ocenę różnych przejawów życia społecznego i eliminuje możliwy wpływ na treść publikacji ze strony czynników politycznych i administracyjnych, w tym także policji, organizacji społecznych i zawodowych, różnych grup interesów czy poszczególnych zainteresowanych osób"[60].

Zgodnie z prawem prasowym[61] tajemnica dziennikarska obejmuje:

• prawo autora materiału prasowego do zachowania w tajemnicy swojego nazwiska;
• obowiązek zachowania w tajemnicy danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze;
• obowiązek zachowania w tajemnicy danych osób udzielających dziennikarzowi informacji opublikowanych albo przekazanych do opublikowania;
• obowiązek zachowania w tajemnicy wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

Uwaga! Warunkiem objęcia ochroną autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze czy też informatora dziennikarskiego jest zastrzeżenie przez te osoby nieujawnienia ich danych.
Należy pamiętać też, że nie każdy autor np. publikacji w internecie może być uznany za dziennikarza i w związku tym może powoływać się na tajemnicę dziennikarską (zob. pyt. 10).

Tajemnicę zawodową stanowią wiadomości, które zostały pozyskane w związku z wykonywanym zawodem lub peł-

[58] Raport Specjalnego Sprawozdawcy ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi ws. ochrony dziennikarskich źródeł informacji i sygnalistów z dnia 8 września 2015 r., A/70/361, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361 (dostęp: 10 marca 2016 r.).

[59] Rekomendacja Komitetu Ministrów Rady Europy R(2000)7 z dnia 8 marca 2000 r., https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM (dostęp: 10 marca 2016 r.).

[60] Postanowienie Sądu Najwyższego z dnia 15 grudnia 2004 r., sygn. akt III KK 278/04.

[61] Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 1984 r. Nr 5 poz. 24).

nioną funkcją[62]. Dziennikarz może powoływać się zatem na tajemnicę dziennikarską tylko w kontekście działalności zawodowej. W pozostałym zakresie, gdy działa np. w sferze życia prywatnego, jego sytuacja nie różni się niczym od sytuacji „zwykłych" obywateli[63]. Dziennikarz nie jest związany tajemnicą, jeśli pozyskuje informacje bez intencji przygotowania artykułu prasowego. Osoba, od której zdobył informacje, może stać się jednak osobą chronioną, jeśli dziennikarz w późniejszym czasie zdecyduje, że chciałby wykorzystać zdobytą wiedzę na potrzeby zawodowe[64].

2. W jaki sposób prawo chroni tajemnicę dziennikarską?

Ochrona tajemnicy dziennikarskiej jest elementem wolności słowa, która jest gwarantowana zarówno przez Konstytucję (art. 54, zob. także art. 14), jak i EKPC (art. 10). Nieuzasadnione ujawnienie tajemnicy dziennikarskiej może prowadzić zatem do naruszenia swobody wypowiedzi. Dodatkowo w polskim porządku prawnym znajdują się szczegółowe przepisy odnoszące się do tajemnicy dziennikarskiej. Podstawowe regulacje w tym zakresie zawierają art. 15 i art. 16 ustawy – Prawo prasowe. Przepisy te określają zakres tajemnicy, a także to, kto i na jakich warunkach może się na nią powołać.

Prawo prasowe

Art. 15 ust. 1. Autorowi materiału prasowego przysługuje prawo zachowania w tajemnicy swego nazwiska.
2. Dziennikarz ma obowiązek zachowania w tajemnicy:
1) danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych,
2) wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.
3. Obowiązek, o którym mowa w ust. 2, dotyczy również

[62] J. Sobczak, *Prawo prasowe. Podręcznik akademicki*, Warszawa 2012, s. 313.

[63] Postanowienie Sądu Najwyższego z dnia 20 października 2005 r., sygn. akt II KK 184/05.

[64] Jak pisze K. Gotkowicz, jeżeli dziennikarz poweźmie zamiar przygotowania materiału prasowego po pozyskaniu poufnej informacji, będzie związany tajemnicą na podstawie art. 15 ust. 2 pkt 2. Osoba udzielająca mu informacji będzie chroniona nie jako źródło, ale jako „osoba trzecia" (zob. B. Kosmus, G. Kuczyński (red.), *Prawo prasowe...*, op. cit.).

innych osób zatrudnionych w redakcjach, wydawnictwach prasowych i innych prasowych jednostkach organizacyjnych.

Art. 16 ust. 1. Dziennikarz jest zwolniony od zachowania tajemnicy zawodowej, o której mowa w art. 15 ust. 2, w razie gdy informacja, materiał prasowy, list do redakcji lub inny materiał o tym charakterze dotyczy przestępstwa określonego w art. 254 Kodeksu karnego albo autor lub osoba przekazująca taki materiał wyłącznie do wiadomości dziennikarza wyrazi zgodę na ujawnienie jej nazwiska lub tego materiału.
2. Zwolnienie, o którym mowa w ust. 1, dotyczy również innych osób zatrudnionych w redakcjach, wydawnictwach prasowych i innych prasowych jednostkach organizacyjnych.
3. Redaktor naczelny powinien być w niezbędnych granicach poinformowany o sprawach związanych z tajemnicą zawodową dziennikarza; powierzoną mu informacją albo inny materiał może ujawnić jedynie w wypadkach określonych w ust. 1.

Dodatkowo regulacje dotyczące tajemnicy dziennikarskiej znajdują się w Kodeksie postępowania karnego (art. 180 § 2-5; dalej: k.p.k.). Mają one zastosowanie w ramach prowadzonego postępowania karnego i są uznawane za przepisy szczególne (*lex specialis*)[65] w stosunku do przepisów prawa prasowego, które normują tajemnicę zawodową dziennikarza w sposób generalny[66]. Jak stwierdził Sąd Najwyższy w jednym z orzeczeń, przepisy art. 180 § 2-5 k.p.k. odnoszą się do „sytuacji wycinkowej, obejmującej kwestię składania zeznań w procesie karnym”[67].

Kodeks postępowania karnego

Art. 180 § 2. Osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na

[65] *Lex specialis* – norma szczegółowa, tj. taka, która reguluje odmiennie niż w normie ogólnej skutki prawne pewnej klasy zdarzeń. *Lex specialis derogat legi generali* – reguła kolizyjna wskazująca na pierwszeństwo stosowania normy szczegółowej przed normą ogólną (*lex generalis*), przy czym obie te normy muszą być umieszczone w aktach prawnych o tej samej mocy.

[66] J. Sobczak, *Prawo prasowe...*, op. cit., s. 320.

[67] Uchwała składu 7 sędziów Sądu Najwyższego z dnia 19 stycznia 1995 r., sygn. akt I KZP 15/94.

podstawie innego dowodu. W postępowaniu przygotowawczym w przedmiocie przesłuchania lub zezwolenia na przesłuchanie decyduje sąd, na posiedzeniu bez udziału stron, w terminie nie dłuższym niż 7 dni od daty doręczenia wniosku prokuratora. Na postanowienie sądu przysługuje zażalenie.
§ 3. Zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych.
§ 4. Przepisu § 3 nie stosuje się, jeżeli informacja dotyczy przestępstwa, o którym mowa w art. 240 § 1 Kodeksu karnego.
§ 5. Odmowa przez dziennikarza ujawnienia danych, o których mowa w § 3, nie uchyla jego odpowiedzialności za przestępstwo, którego dopuścił się, publikując informację.

3. Co oznacza prawo autora materiału prasowego do zachowania w tajemnicy swojego nazwiska?

Słowniczek

Materiał prasowy – każdy opublikowany lub przekazany do opublikowania w prasie tekst albo obraz o charakterze informacyjnym, publicystycznym, dokumentalnym lub innym, niezależnie od środków przekazu, rodzaju, formy, przeznaczenia czy autorstwa (art. 7 ust. 2 pkt 4 prawa prasowego).

Dziennikarz, który jest autorem materiału prasowego, może podpisać swoje dzieło pseudonimem, wymyślonym nazwiskiem lub wcale go nie podpisywać (art. 15 ust. 1 prawa prasowego). Prawo to przysługuje nie tylko dziennikarzowi, lecz każdej osobie, która jest autorem materiału prasowego (także niezwiązanej z redakcją), i to niezależnie od tego, czy materiał ten zostanie ostatecznie zakwalifikowany do publikacji, czy też nie[68]. Autor materiału prasowego może także zastrzec swoje dane do wiadomości redakcji. W każdej z tych sytuacji redaktor naczelny danego medium ani żaden z zatrudnionych dziennikarzy oraz innych pracowników

[68] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 8 kwietnia 2010 r., II SA/Wa 1488/09.

redakcji nie może upublicznić ani nikomu ujawnić, w tym organom państwowym, nazwiska autora materiału prasowego bez jego zgody (dotyczy to też wszelkich innych identyfikujących go danych)[69]. Autor nie może być wskazany, nawet jeśli treść materiału prasowego okaże się bezprawna, np. gdy w artykule doszło do naruszenia dóbr osobistych osób trzecich. Osoby poszkodowane publikacją będą mogły wówczas dochodzić swoich praw jedynie od redaktora naczelnego lub wydawcy (art. 38 ust. 1 prawa prasowego). Nie będzie natomiast możliwości uzyskania danych autora materiału prasowego, aby pociągnąć go bezpośrednio do odpowiedzialności.

Ochrona anonimowości autora materiału prasowego

Jeśli autor przesyła do redakcji artykuł do druku podpisany pseudonimem, należy przyjąć, że wyraża tym samym żądanie, aby utwór został opublikowany z takim podpisem[70]. Redakcja nie ma wówczas prawa do ujawnienia bez zgody autora jego prawdziwego imienia i nazwiska ani czytelnikom, ani organom państwowym (poza ściśle określonymi w prawie sytuacjami – zob. pyt. 11 i następne). Aby jednak nie było wątpliwości, że autor pragnie pozostać anonimowy, dobrą praktyką jest jednoczesne przesłanie do redakcji wyraźnego oświadczenia zastrzegającego nieujawnienie jego danych.

4. Na czym polega ochrona dziennikarskich źródeł informacji?

Prawo prasowe zapewnia ochronę osobowym źródłom informacji dziennikarzy (tzw. informatorom), tj. osobom informującym dziennikarzy, współpracujących z nimi lub udzielających im wywiadu, zobowiązując jednocześnie dziennikarzy do określonego zachowania wobec tych osób[71].

Zgodnie z art. 15 ust. 2 pkt 1 dziennikarz ma obowiązek zachowania w tajemnicy danych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych. Ochrona tożsamości informatorów uznawana jest nie tylko za obowiązek mediów, ale jednocześnie za „uprawnienie społeczeństwa"[72], gwarantujące wzmacnianie relacji

[69] J. Sobczak, *Prawo prasowe...*, op. cit., s. 314.

[70] Wyrok Sądu Najwyższego z 6 czerwca 1928 r., sygn. akt K 715/28.

[71] J. Sobczak, *Prawo prasowe...*, op. cit., s. 330.

[72] I. Zielinko, *Tajemnica dziennikarska w prawie prasowym*, „Prokuratura i Prawo" 2009, nr 7-8, s. 150.

zaufania łączącej dziennikarzy i ich źródła. Istotą ochrony dziennikarskich źródeł informacji jest więc przede wszystkim poszanowanie interesów osób przekazujących poufne informacje mediom, które – gdyby ich tożsamość była znana – mogłyby być narażone na rozmaite negatywne konsekwencje w związku z ujawnieniem określonych informacji prasie (np. zagrożenie dla bezpieczeństwa osobistego, zwolnienie z pracy, krytykę środowiska koleżeńskiego, rodziny itd.). Pośrednio dobrami chronionym są także wolność mediów (które mają łatwiejszy dostęp do informacji) i interes publiczny, który wymaga ujawnienia i napiętnowania wszelkiego rodzaju patologii występujących w życiu publicznym[73].

Do potrzeby zapewnienia niezwykle mocnej ochrony dziennikarskim źródłom informacji wielokrotnie odwoływał się Europejski Trybunał Praw Człowieka. W sprawie *Goodwin p. Wielkiej Brytanii*[74] Trybunał podkreślił, że „bez takiej ochrony źródła mogą bać się pomagać prasie w informowaniu opinii publicznej o sprawach wzbudzających zainteresowanie publiczne. W rezultacie ważna rola prasy – publicznego kontrolera – może ulec osłabieniu. Może to również wpłynąć na zdolność prasy do zapewnienia dokładnej i wiarygodnej informacji".

Pojęcie „danych umożliwiających identyfikację" należy interpretować szeroko. Ochroną objęte są nie tylko imię i nazwisko informatora dziennikarskiego, ale wszelkie informacje, które mogłyby przyczynić się do ustalenia jego tożsamości. Mogą to być zatem: rysopis osoby przekazującej informację mediom, zajmowane stanowisko, jej numer telefonu zapisany na billingu rozmów prowadzonych przez dziennikarza[75], metadane komputerowe, adres zamieszkania lub adres e-mail, które pośrednio doprowadzą do zidentyfikowania informatora. Tajemnica może obejmować także treść informacji uzyskanych od źródła, których ujawnienie mogłoby doprowadzić do jego zdekonspirowania.

Tajemnica obowiązuje, gdy informacje przekazywane dziennikarzowi są przeznaczone do opublikowania, niezależnie jednak od tego, czy zostaną ostatecznie wykorzystane w publikacji dziennikarskiej, czy też nie. Dziennikarz ma ponadto obowiązek ochrony źródeł

[73] W. Lis, *Komentarz do art. 15 Prawa prasowego* [w:] W. Lis, P. Wiśniewski, Z. Husak (red.), *Prawo prasowe. Komentarz*, Warszawa 2012, s. 369.

[74] Wyrok ETPC z dnia 27 marca 1996 r. (Wielka Izba) w sprawie *Goodwin p. Wielkiej Brytanii*, skarga nr 28957/95.

[75] E. Ferenc-Szydełko, *Komentarz do art. 15 ustawy – Prawo prasowe* [w:] eadem, *Prawo prasowe. Komentarz*, Warszawa 2008, s. 129.

zarówno wtedy, gdy jest „biernym" beneficjentem ujawnienia mu materiałów przez dobrowolnie działającego informatora, ale także gdy sam aktywnie działa na rzecz pozyskania danej informacji od źródła (zachęcając do ujawnienia informacji, a nawet wynagradzając informatora finansowo za jej przekazanie).

Trzeba jednocześnie pamiętać, że dziennikarz, który prowokuje do złamania zawodowych obowiązków (np. ujawnienia tajemnicy służbowej przez źródło), sam dopuszcza się przestępstwa i jak każda osoba może stać się obiektem postępowania organów ścigania. Nie oznacza to jednak, że tajemnica dziennikarska w takiej sytuacji nigdy nie obowiązuje. Wiele zależy od konkretnych okoliczności danej sprawy. Jak pisze I.C. Kamiński, analizując orzecznictwo strasburskie dotyczące ochrony dziennikarskich źródeł informacji, „chociaż pierwsze intuicje mogą prowadzić do wniosku, że w takim przypadku dziennikarski przywilej nie istnieje, to uważam, że racje publiczne związane ze zdobywaną informacją mogą usprawiedliwiać postępowanie dziennikarza i wymagać zachowania ochrony źródła informacji"[76].

5. W jaki sposób informator powinien zastrzec swoją anonimowość, aby być chronionym?

Tajemnica dziennikarska powstaje z chwilą, gdy informator zastrzegł nieujawnianie swoich danych[77]. Jest to warunek przyznania mu ochrony. Jeśli informator chce, aby dziennikarz chronił jego anonimowość, musi uczynić odpowiednie zastrzeżenie.

Zastrzeżenie takie najlepiej zrobić w sposób najbardziej jednoznaczny i niebudzący wątpliwości co do intencji osoby zastrzegającej. Nie wymaga się jednak, aby miało ono jakąś szczególną formę (nie musi być więc wyrażone np. na piśmie, ale może być przekazane w formie ustnej lub drogą elektroniczną). W doktrynie wskazuje się zatem np., że przekazanie materiału prasowego anonimowo lub pod pseudonimem spełniać będzie wymogi skutecznego zastrzeżenia[78]. W jednym w wyroków sąd doszedł do wniosku, że skoro osoba kontaktująca się z dziennikarzem przez internet posłużyła

[76] I.C. Kamiński, *Ochrona dziennikarskich źródeł informacji w Europejskiej Konwencji Praw Człowieka* [w:] T. Kononiuk (red.), *Dziennikarz – utwór – prasa. Księga jubileuszowa z okazji pięćdziesięciolecia pracy naukowej prof. dr. hab. Bogdana Michalskiego*, Warszawa 2014, s. 285-302.

[77] L. Jaworski, *Tajemnica zawodowa dziennikarza w świetle obowiązującego w Polsce prawa. Część 1. Prawo do anonimatu*, „Studia Medioznawcze. Instytut Dziennikarstwa Uniwersytetu Warszawskiego" 2015, nr 1(60), s. 45-55.

[78] Ibidem, s. 51.

się tzw. nickiem, należy przyjąć, że zastrzegła sobie w ten sposób anonimowość[79].

Zastrzeżenie nieujawnienia danych może nastąpić w każdym momencie, tj. w chwili przekazania dziennikarzowi informacji, ale i później (jeśli tożsamość informatora nie została wcześniej ujawniona). Wiąże ono dziennikarza bezterminowo. Te same zasady mają zastosowanie w odniesieniu do kwestii zastrzeżenia nieujawniania danych przez autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, chcącego zachować anonimowość.

6. Czy ochrona źródeł obowiązuje, jeśli informator nielegalnie pozyskał informacje lub dokumenty, które przekazał dziennikarzowi?

Tak. Wskazane okoliczności nie zwalniają dziennikarza z obowiązku ochrony anonimowości informatora. Jak pisze M. Zaremba, „tajemnica dziennikarska obowiązuje bez względu na to, czy informator wszedł w posiadanie przekazywanych informacji w sposób legalny, czy bezprawny, ani też to, czy dostarczając je, narusza tajemnicę państwową, służbową, handlową czy jakąkolwiek inną. Nie ma też znaczenia dla zaistnienia ochrony motywacja informatorów, ani wartość merytoryczna przekazanych przez nich danych. Uzależnienie gwarancji poufności od dobrej wiary źródła informacji czy ich prawdziwości prowadziłoby do podważenia sensu omawianej instytucji. Informatorzy rzadko kiedy kierują się szlachetnymi pobudkami, rolą dziennikarza jest więc weryfikacja uzyskanych od nich wiadomości”[80]. Pogląd ten podziela w swoim orzecznictwie także ETPC, który zauważa, że tajemnica dziennikarska nie może być traktowana jako „zwykły przywilej, który jest przyznawany lub cofany w zależności od legalności lub nielegalności źródeł, lecz stanowi rzeczywisty atrybut prawa do informacji, do którego należy podchodzić z największą uwagą”[81].

Odpowiedzialność dziennikarzy za opublikowanie tajnych informacji otrzymanych od informatora

W orzecznictwie sądów podkreśla się, że w określonych okolicznościach, w szczególności gdy przemawia za tym

[79] Postanowienie Sądu Rejonowego w Jarocinie z dnia 11 kwietnia 2014 r., sygn. akt II Kp 18/14.

[80] M. Zaremba, *Prawo prasowe. Ujęcie praktyczne*, Warszawa 2007, s. 40.

[81] Wyrok ETPC z dnia 27 listopada 2007 r. w sprawie *Tillack p. Belgii*, skarga nr 20477/05.

interes publiczny, dopuszczalne jest wykorzystanie przez dziennikarza w publikacji materiałów objętych klauzulą tajności.

Sąd Najwyższy zauważył, że:

„Dla oceny, czy posłużenie się tego rodzaju [niejawnymi – przy. aut.] dokumentami wyłącza bezprawność z powołaniem na obronę społecznie uzasadnionego interesu, istotne są zawsze konkretne okoliczności rozpoznawanej sprawy. Te, będące podstawą rozstrzygnięcia, nakazywały przyjęcie, że opublikowanie w prasie informacji objętych tajemnicą skarbową, podjęte w obronie społecznie uzasadnionego interesu społecznego w konkretnych okolicznościach faktycznych, może wyłączać bezprawność takiej publikacji. Pokreślić przede wszystkim należy prawdziwość tych informacji, które miały podstawę nie tylko w treści dokumentów objętych tajemnicą skarbową”[82].

Europejski Trybunał Praw Człowieka uznał również, że skazanie dziennikarza za opublikowanie informacji z niejawnego postępowania karnego, o których dziennikarz dowiedział się w trakcie śledztwa dziennikarskiego, stanowiło naruszenie swobody wypowiedzi. Chodziło o ujawnienie informacji z akt postępowania przeciwko sprawcy poważnego wypadku samochodowego, który wzbudzał szerokie zainteresowanie opinii publicznej. Trybunał podkreślił, że media mają obowiązek dostarczać informacje, które dotyczą interesu publicznego. Wziął także pod uwagę, że informacje ujawnione przez dziennikarza nie miały faktycznego wpływu na podważenie zasady domniemania niewinności w tej sprawie ani nie dotyczyły sfery życia prywatnego bohatera materiału. Dlatego skazanie dziennikarza było niedopuszczalne i mogło zniechęcić innych dziennikarzy do poruszania kontrowersyjnych, ale ważnych społecznie tematów[83].

[82] Wyrok Sądu Najwyższego z dnia 27 listopada 2014 r., sygn. akt IV CSK 174/14.

[83] Wyrok ETPC z dnia 1 lipca 2014 r. w sprawie *A.B. p. Szwajcarii*, skarga nr 56925/08.

7. Czy ochrona źródeł obowiązuje, jeśli informator świadomie wprowadził dziennikarza w błąd, narażając go na odpowiedzialność?

Tak. Co do zasady dopiero po sprawdzeniu wiarygodności źródła i przekazanych przez nie materiałów dziennikarz powinien podjąć decyzję o ich ewentualnej publikacji. Weryfikację informacji otrzymanych od osoby zastrzegającej swoją anonimowość i potwierdzenie ich na podstawie innych źródeł nakazują zasady rzetelności dziennikarskiej (art. 12 ust. 1 prawa prasowego). Jeśli następnie dziennikarz ma wątpliwości co do wiarygodności przekazanej mu informacji, może zaniechać publikacji, nie uprawnia go to jednak do ujawnienia informatora. Jeśli dziennikarz wykorzystał fałszywą informację jako przekazaną przez informatora pragnącego zachować anonimowość i zostały przeciwko niemu podjęte działania prawne przez podmiot, którego dotyczyła ta informacja (np. postępowanie o zniesławienie), nie będzie mógł ujawnić informatora, aby uwolnić się od odpowiedzialności. Brak gwarancji utrzymania w poufności danych informatorów w przypadku pozwania lub oskarżenia dziennikarza doprowadziłby do „paraliżu informacyjnego", ponieważ informatorzy obawialiby się zdekonspirowania[84].

Wymóg weryfikacji przekazanych informacji w mniejszym stopniu dotyczy **dokumentów urzędowych** (np. oficjalnego raportu z audytu przeprowadzonego w danej instytucji publicznej). Dziennikarz, który otrzymał taki dokument od informatora, powinien sprawdzić jego autentyczność, natomiast będzie zwolniony z obowiązku dokonania weryfikacji zawartych w nim danych. Może oprzeć się na takim dokumencie, a jeśli okaże się, że zawierał on nieścisłości czy fałszywe informacje, dziennikarz nie powinien zostać pociągnięty do odpowiedzialności. Materiał urzędowy pozostaje wiarygodny tak długo, jak odpowiednie władze – najczęściej te, które materiał przygotowały – skutecznie go nie zakwestionują[85].

Obowiązek weryfikacji informacji otrzymanych od źródła

Dziennikarz otrzymał od informatora, który zastrzegł nieujawnianie swoich danych, dokumenty świadczące o bezprawnym działaniu jego pracodawcy – spółki X. Dziennikarz zaufał informatorowi i wykorzystał otrzymane informacje w artykule prasowym. Ponieważ temat był pilny i redakcja naciskała na szybką publikację, dziennikarz nie podjął żadnych działań w celu sprawdzenia wiarygodności

[84] W. Lis, *Komentarz do art. 15...*, op. cit., s. 401.

[85] Wyrok ETPC z dnia 20 maja 1999 r. w sprawie *Bladet Tromso i Stensaas p. Norwegii*, skarga nr 21980/93.

dokumentów. Po publikacji okazało się, że przekazane informacje są nieprawdziwe i niesłusznie podważają reputację firmy X. Firma wystąpiła przeciwko dziennikarzowi z powództwem o ochronę dóbr osobistych. Dziennikarz będzie musiał liczyć się z poniesieniem odpowiedzialności za artykuł. Nie będzie mógł uniknąć odpowiedzialności, argumentując, że oparł się na dokumentach przekazanych przez osobę trzecią, których nie próbował nawet sprawdzić. Nie będzie też mógł się bronić, ujawniając informatora, który wprowadził go w błąd.

8. Jakie jeszcze informacje objęte są tajemnicą dziennikarską?

Oprócz informacji wymienionych powyżej przedmiotem tajemnicy dziennikarskiej są także wszelkie informacje, które znalazły się w posiadaniu dziennikarza w związku z jego działalnością zawodową, a których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich (art. 15 ust. 2 pkt 2 prawa prasowego). Przy czym nie chodzi tu tylko o interesy informatorów, ale także innych osób trzecich. Mogą to być np. informacje ujawniające informacje z życia prywatnego tych osób czy dane o stanie zdrowia. Przedmiotem ochrony jest w tym przypadku treść określonych informacji, np. znajdujących się w przekazanych przez informatora dokumentach. Dziennikarz musi więc sam dokonać oceny tego rodzaju materiałów, zanim podejmie decyzję o ich publikacji, aby nie narazić się na zarzut naruszenia tajemnicy.

9. Kto jest zobowiązany do ochrony tajemnicy dziennikarskiej?

Tajemnica dziennikarska obowiązuje nie tylko dziennikarzy, ale także redaktora, redaktora naczelnego, inne osoby zatrudnione w redakcjach i wydawnictwach prasowych, niezależnie od stanowiska (także pracowników technicznych czy administracyjnych; art. 15 ust. 3 prawa prasowego). Dotyczy to osób zatrudnionych na umowę o pracę, ale też np. zatrudnionych na podstawie umowy o dzieło czy umowy zlecenia[86]. Nie ma przy tym znaczenia, czy dostęp do poufnych danych osoby te uzyskały w wyniku własnych działań, czy w ramach obowiązków wykonywanych w redakcji[87]. Pracownicy

[86] E. Ferenc-Szydełko, *Komentarz do art. 15 ustawy...*, op. cit., s. 130.

[87] M. Zaremba, *Prawo prasowe...*, op. cit., s. 40. Uchwała Sądu Najwyższego z dnia 19 stycznia 1995 r., sygn. akt I KZP 15/94.

łączący rozmowy telefoniczne lub otwierający listy także mogą wejść w posiadanie informacji objętych tajemnicą dziennikarską, co oznacza, że odnoszą się do nich takie same obowiązki, jakie w tym zakresie ustawodawca nałożył na dziennikarzy. W literaturze można spotkać pogląd, że aby gwarancje wynikające z tajemnicy dziennikarskiej mogły zostać uznane za efektywne, muszą być stosowane w stosunku do wszelkich jej depozytariuszy, którymi w pewnych sytuacjach mogą okazać się jednostki poczty i telekomunikacji oraz tzw. operatorzy sieci telefonicznych[88] (np. jeśli policja zwraca się do nich o udostępnienie danych telekomunikacyjnych dotyczących dziennikarza, np. takich jak billingi).

Słowniczek

Dziennikarz – osoba zajmująca się redagowaniem, tworzeniem lub przygotowywaniem materiałów prasowych, pozostająca w stosunku pracy z redakcją albo zajmująca się taką działalnością na rzecz i z upoważnienia redakcji (art. 7 ust. 2 pkt 5 prawa prasowego).

Redaktor – dziennikarz decydujący lub współdecydujący o publikacji materiałów prasowych (art. 7 ust. 2 pkt 6 prawa prasowego).

Redaktor naczelny – osoba posiadająca uprawnienia do decydowania o całokształcie działalności redakcji (art. 7 ust. 2 pkt 7 prawa prasowego).

Redakcja – jednostka organizująca proces przygotowywania (zbierania, oceniania i opracowywania) materiałów do publikacji w prasie (art. 7 ust. 2 pkt 8 prawa prasowego).

10. Czy blogerzy i dziennikarze obywatelscy także są zobowiązani do zachowania tajemnicy?

Jak wskazano wcześniej, obowiązek ochrony tajemnicy dziennikarskiej rozciąga się na szeroką grupę podmiotów. Z art. 15 ust. 3 prawa prasowego wynika jednak, że są to przede wszystkim dziennikarze i inne osoby powiązane z „redakcjami, wydawnictwami prasowymi i innymi prasowymi jednostkami organizacyjnymi". Jest to związane z tym, że dziennikarze wykonują zawód zaufania publicznego, z którym wiążą się określone prawa i obowiązki o charakterze

[88] I. Zielinko, *Tajemnica dziennikarska w prawie prasowym*, „Prokuratura i Prawo" 2009, nr 7-8, s. 148-168.

prawnym i etycznym. Obejmują one m.in. obowiązek weryfikacji materiałów otrzymanych od informatorów lub uwzględnienie tego, czy interes publiczny uzasadnia daną publikację itd. **Takie obowiązki nie ciążą natomiast na innych autorach, którzy jednocześnie nie mogą korzystać z pewnych „przywilejów" zarezerwowanych dla dziennikarzy, tj. np. powołać na tajemnicę dziennikarską**[89].

Odpowiedź na pytanie, czy tajemnica dotyczy także tzw. blogerów, dziennikarzy obywatelskich i innych osób publikujących w internecie, nie jest łatwa z uwagi na niejasny status blogów czy portali z dziennikarstwem obywatelskim w świetle prawa prasowego. Należy zatem przyjąć, że jeśli osoba taka publikuje na portalu, który w świetle kryteriów określonych w art. 7 ust. 2 pkt 1 prawa prasowego spełnia kryteria „prasy", wówczas stosują się do niej prawa i obowiązki wynikającej z tej ustawy, w tym regulacje dotyczące tajemnicy dziennikarskiej. Takie podejście wymaga jednak każdorazowej oceny charakterystyki danego portalu, która niekiedy może być niejednoznaczna. Np. nieregularnie prowadzony blog poświęcony wąskiej tematyce będącej hobby autora nie mieści się raczej w pojęciu „prasa". Informator powierzający autorowi takiego serwisu poufne informacje nie może być więc pewien, że autor ten będzie zobowiązany do ochrony jego anonimowości. Wątpliwości te nie dotyczą natomiast portali, które zostały zarejestrowane jako „dziennik" lub „czasopismo" na postawie prawa prasowego. Dziennikarze przygotowujący materiały prasowe dla tych serwisów mogą powołać się na tajemnicę dziennikarską[90].

Problem rozciągania praw i obowiązków wynikających z tajemnicy dziennikarskiej na blogerów i dziennikarzy obywatelskich pojawia się w debacie międzynarodowej. O takiej konieczności wspomina np. Specjalny Sprawozdawca ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi w raporcie dotyczącym ochrony dziennikarskich źródeł informacji i sygnalistów[91].

Jego zdaniem zakres stosowania gwarancji wynikających z tajemnicy dziennikarskiej powinien być zależny nie od profesji, jaką formalnie wykonuje dana osoba, ale od funkcji

[89] J. Podkowik, *Ochrona dziennikarskich źródeł informacji w dobie cyfrowej w świetle Konwencji o ochronie praw człowieka i podstawowych wolności oraz Konstytucji RP*, „Przegląd Sejmowy" 2015, nr 3(128), s. 75.

[90] Więcej na ten temat: M. Zaremba, *Prawo prasowe a internet – stan de lege lata i de lege ferenda* [w:] D. Bychawska-Siniarska, D. Głowacka, *Wirtualne media – realne problemy*, Warszawa 2014, s. 153-161, http://www.obserwatorium.org/images/Wirtualne%20media%20-%20realne%20problemy.pdf (dostęp: 15 marca 2016 r.).

[91] Raport Specjalnego Sprawozdawcy ONZ..., op. cit.

publikowanych informacji i ich znaczenia dla interesu publicznego. W związku z tym konieczne jest tworzenie regulacji prawnych na poziomie krajowym dotyczących tajemnicy dziennikarskiej, które mogłyby obejmować nie tylko profesjonalnych dziennikarzy, ale także m.in. blogerów, dziennikarzy obywatelskich czy pracowników organizacji pozarządowych. Zdaniem Specjalnego Sprawozdawcy osoby te często wykonują dziś te same zadanie co tradycyjne media, gromadząc i ujawniając informacje w interesie publicznym. Platforma, za której pośrednictwem prowadzą taką działalność (czy jest to gazeta drukowana, czy strona internetowa), nie powinna być czynnikiem decydującym dla przyznania im ochrony. Specjalny Sprawozdawca wskazał jednocześnie na przykłady państw, w których gwarancjami wynikającymi z tajemnicy dziennikarskiej objęto inne podmioty poza dziennikarzami (np. irlandzki sąd w sprawie *Cornec p. Morrice i Ors* wprost stwierdził, że ochrona ta rozciąga się także na blogerów).

11. Kiedy dziennikarz może być zwolniony z tajemnicy?

Ochrona tajemnicy dziennikarskiej nie ma charakteru absolutnego. Jednakże z uwagi na rolę mediów w kontrolowaniu władzy publicznej i mówieniu o sprawach społecznie ważnych ustawodawca objął tajemnicę dziennikarską stosunkowo silną ochroną, która może być ograniczona jedynie w wyjątkowych, ściśle określonych przez prawo przypadkach.

Zgodnie z art. 16 prawa prasowego dziennikarz jest zwolniony z tajemnicy dziennikarskiej określonej w art. 15 ust. 2 prawa prasowego jedynie w dwóch przypadkach:

1) gdy informacja przekazana przez informatora czy autora materiału prasowego dotyczy przestępstwa należącego do zamkniętego katalogu najcięższych przestępstw określonych w art. 240 k.k.[92]**;**

2) gdy zgodę na ujawnienie swoich danych wyrazi informator prasowy lub autor materiału, który wcześniej zastrzegł sobie anonimowość.

[92] Prawo prasowe nadal odwołuje się wprost do art. 254 starego Kodeksu karnego. Na gruncie obowiązującego Kodeksu karnego należy przyjąć, iż odwołanie to dotyczy obecnego art. 240 k.k.

Ad. 1. Pierwszy przypadek dotyczy sytuacji, w której dziennikarz, zapoznając się z informacją przekazaną przez źródło, listem do redakcji lub innym materiałem prasowym, dowie się o przestępstwie z art. 240 k.k. (dawniej 254 k.k.). Zgodnie z tym przepisem każda osoba, która posiada wiarygodną wiadomość o karalnym przygotowaniu albo usiłowaniu lub dokonaniu czynów zabronionych wskazanych w tym artykule, ma obowiązek niezwłocznego zawiadomienia organów ścigania. Czyny zabronione wskazane w art. 240 k.k. należą do najpoważniejszych przestępstw (stąd prawny obowiązek denuncjacji, w przypadku pozostałych przestępstw istnieje jedynie społeczny obowiązek zawiadomienia organów ścigania). W katalogu przestępstw w art. 240 k.k. znajdują się m.in.: ludobójstwo, masowy zamach, poważne naruszenie międzynarodowego prawa karnego, zamach na konstytucyjny organ RP, szpiegostwo, zamach na życie Prezydenta RP, zabójstwo, sprowadzenie zdarzenia powszechnie niebezpiecznego, bezprawne pozbawienie wolności, wzięcie zakładnika, a także przestępstwa o charakterze terrorystycznym.

Uwaga! Jedynie w odniesieniu do najcięższych przestępstw przeciwko państwu oraz życiu i zdrowiu z art. 240 k.k. dojść może do wyłączenia tajemnicy dziennikarskiej w zakresie ujawnienia osobowego źródła informacji czy autora materiału prasowego, którzy zastrzegli anonimowość. Dziennikarz jest wówczas zwolniony z tajemnicy z mocy samego prawa. W doktrynie i orzecznictwie podkreśla się również, że w tych przypadkach tajemnica w ogóle nie powstaje, a dziennikarz, tak jak każdy inny obywatel, ma bezwzględny obowiązek zawiadomienia organów ścigania[93].

Zawężenie możliwości wyłączenia tajemnicy dziennikarskiej do sytuacji, gdy chodzi o ściganie jedynie najpoważniejszych przestępstw jest zgodne ze standardami międzynarodowymi. Europejski Trybunał Praw Człowieka podkreśla, że samo dążenie do wykrycia sprawców każdego rodzaju przestępstwa nie jest przesłanką wystarczającą. W sprawie *Nordisk Film & Tv A/S p. Danii*[94] ETPC uznał, że ujawnienie materiałów mogących wskazać na osobowe źródło informacji było uzasadnione, ponieważ postępowanie dotyczyło przestępstwa wykorzystania seksualnego dzieci.

[93] J. Sobczak, *Komentarz do art. 16 ustawy – Prawo prasowe* [w:] idem, *Prawo prasowe. Komentarz*, Warszawa 2008; uchwała Sądu Najwyższego, sygn. akt I KZP 15/94, op. cit.

[94] Wyrok ETPC z dnia 8 grudnia 2005 r. w sprawie *Nordisk Film & Tv A/S p. Danii,* skarga nr 40485/02.

Na to, że tylko wąski katalog okoliczności, taki jak ochrona ludzkiego życia lub zapobieżenie poważnemu przestępstwu, może usprawiedliwiać ingerencje w tajemnicę dziennikarską, zwraca także uwagę Komitet Ministrów Rady Europy[95].

Ad. 2. Zgoda informatora czy autora materiału prasowego na ujawnienie ich danych może nastąpić w dowolnej formie (np. za pośrednictwem poczty elektronicznej), także w sposób dorozumiany, jeśli jednoznacznie ujawni ich wolę w tym zakresie[96]. Przepis art. 16 ust. 1 jasno wskazuje, że choć o tajemnicy dziennikarskiej często mówi się jako o „przywileju" przedstawicieli mediów, to w zakresie m.in. ochrony anonimowości osobowych źródeł informacji jest to przede wszystkim obowiązek dziennikarzy, którzy nie mają prawa ujawniać informacji o swoich informatorach, nawet gdyby sami chcieli (zob. także pyt. 16). Dysponentem tajemnicy jest bowiem informator i tylko on może się zgodzić na jej ujawnienie.

12. Czy dziennikarz może być zwolniony z tajemnicy na potrzeby postępowań przed organami wymiaru sprawiedliwości? Kiedy można przesłuchać dziennikarza na okoliczności objęte tajemnicą?

Dziennikarze, przygotowując materiały prasowe na różne społecznie istotne tematy (jak np. nieprawidłowości w instytucjach publicznych), często wchodzą w posiadanie informacji interesujących dla organów ścigania. Organy te, nierzadko w następstwie ukazania się artykułu na dany temat, prowadzą w sprawie własne postępowanie, na którego potrzeby mogą chcieć pozyskać zdobytą przez dziennikarza wiedzę, wzywając go np. na przesłuchanie w charakterze świadka. Należy jednak podkreślić, że przesłuchanie dziennikarza jako świadka w postępowaniu przed organami wymiaru sprawiedliwości na okoliczności objęte tajemnicą dziennikarską (a zwłaszcza w zakresie ujawnienia tożsamości osób, które przekazały poufne informacje mediom) jest co do zasady niedopuszczalne, poza pewnymi sytuacjami określonymi przez prawo. Dziennikarz ma prawo w takiej sytuacji odmówić zeznań na okoliczności objęte tajemnicą.

W postępowaniach cywilnym, administracyjnym, podatkowym czy sądowoadministracyjnym tajemnica dziennikarska ma charakter

[95] Rekomendacja Komitetu Ministrów R (2000)7 w sprawie prawa dziennikarzy do nieujawniania swoich źródeł informacji, pkt 37-40, https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM (dostęp: 10 marca 2016 r.).

[96] E. Ferenc-Szydełko, *Komentarz do art. 16 ustawy – Prawo prasowe* [w:] eadem, *Prawo prasowe...*, op. cit., s. 133-136.

bezwzględny, a jedynym podmiotem, który może z niej zwolnić dziennikarza, jest jej dysponent[97] (tj. informator albo autor materiału prasowego, którzy zastrzegli wcześniej swoją anonimowość).

W postępowaniu karnym istnieje możliwość zwolnienia dziennikarza z tajemnicy w pewnych sytuacjach na podstawie art. 180 § 2-5 k.p.k. Zgodnie z tym przepisem tajemnica dziennikarska podlega zróżnicowanej ochronie w zależności od kategorii objętej nią informacji[98]. Najsilniejszej ochronie podlegają w szczególności dane pozwalające na identyfikację autorów materiałów prasowych oraz dziennikarskich źródeł informacji, którzy zastrzegli swoją anonimowość.

Co do zasady dziennikarz może zostać przesłuchany w postępowaniu karnym na okoliczność faktów objętych tajemnicą, jeśli są spełnione **łącznie** następujące warunki (art. 180 § 2 k.p.k.):

1. Przesłuchanie jest niezbędne dla dobra wymiaru sprawiedliwości (oznacza to, że przesłuchanie dziennikarza na okoliczności objęte tajemnicą dziennikarską jest konieczne, aby ustalić prawdę obiektywną[99]). Przesłanka ta musi być interpretowana zawężająco, w razie wątpliwości należy uznać, że dobro wymiaru sprawiedliwości nie wymaga zwolnienia z tajemnicy[100].

2. Okoliczność nie może być ustalona na podstawie innego dowodu (zwolnienie powinno mieć miejsce w ostateczności, a więc wówczas, gdy wyczerpane zostały inne środki dowodowe[101], np. zeznania innych świadków, dowody z dokumentów itd.).

Uwaga! Zwolnienie z tajemnicy dziennikarskiej wymaga dodatkowo zgody sądu.
Zgoda sądu może zostać wydana na każdym etapie postępowania, także w postępowaniu przygotowawczym na wniosek prokuratora. Sąd, wydając postanowienie w przedmiocie zwolnienia dziennikarza z tajemnicy, powinien to szczegółowo uzasadnić, wykazując, że spełnione zostały oba wyżej wymienione warunki. Nie wystarczy ogólne powołanie się na spełnienie przesłanek z art. 180 § 2 k.p.k., ale trzeba wskazać rzeczywiste działania organów ścigania podjęte

[97] W. Lis, *Komentarz do art. 15...*, op. cit., s. 383.

[98] Ibidem.

[99] Uchwała Sądu Najwyższego z dnia 22 listopada 2002 r., sygn.. akt I KZP 26/02.

[100] K. Brocławik, M. Czajka, *Prawnokarne aspekty ochrony tajemnicy zawodowej radcy prawnego. Część II*, „Radca Prawny" 2001, nr 4, s. 42 i nast. Zob. J. Kosonoga, *Dobro wymiaru sprawiedliwości jako przesłanka dokonywania czynności procesowych w postępowaniu karnym* [w:] W. Cieślak, S. Steinborn (red.), *Profesor Marian Cieślak – osoba, dzieło, kontynuacje*, Warszawa 2013, s. 886-893, za: B. J. Stefańska, *Przeszukanie a tajemnica dziennikarska*, „Prokuratura i Prawo" 2015, nr 6.

[101] E. Nowińska, *Wolność wypowiedzi prasowej*, Warszawa 2007, s. 137.

wcześniej w sprawie. Organy ścigania nie mogą sięgnąć po zwolnienie dziennikarza z tajemnicy, gdy środek ten nie był rzeczywiście niezbędny, a tylko bardziej wygodny do wykorzystania (np. wymagający od policjantów mniejszego nakładu pracy niż inne środki dowodowe). Co ważne, **na postanowienie o zwolnieniu z tajemnicy dziennikarz może złożyć zażalenie**, które rozpozna sąd wyższej instancji.

Dziennikarz, który został prawomocnie zwolniony przez sąd z tajemnicy, nie może już odmówić zeznań na okoliczności nią objęte. Gdyby mimo zwolnienia odmawiał złożenia zeznań, narażałby się, tak jak każdy obywatel, na zastosowanie środków przymusu i kar porządkowych (takich jak obowiązek zapłaty kary pieniężnej czy nawet areszt).

Uwaga! Opisana wyżej możliwość zwolnienia z tajemnicy dziennikarskiej **nie dotyczy** jednak ujawnienia danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych (art. 180 § 3 k.p.k.). W tym zakresie dziennikarz nie może być zwolniony z tajemnicy. Jedynym wyjątkiem od tej zasady są sytuacje, w których informacja dotyczy jednego z najpoważniejszych przestępstw, o jakim mowa w art. 240 § 1 k.k. (art. 180 § 4 k.p.k). Jeśli zatem zachodzą przesłanki z art. 180 § 2 k.p.k. i sprawa nie ma związku z żadnym z przestępstw wymienionych w art. 240 k.k., dziennikarz może być przesłuchany np. tylko w zakresie treści informacji, którą otrzymał od informatora, ponieważ zwolnienie od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację dziennikarskiego źródła. Jeżeli jednak już sama treść informacji może naprowadzić na osobę, która ją przekazała dziennikarzowi, jej ujawnienie także będzie niedopuszczalne.

Zażalenie na zwolnienie z tajemnicy dziennikarskiej

W jednej ze spraw monitorowanych przez HFPC prokuratura wszczęła śledztwo w sprawie ujawnienia poufnych informacji dotyczących pewnego banku, które ukazały się w materiale prasowym autorstwa red. W. w jednej z gazet. Prokurator wezwał dziennikarza na przesłuchanie – w jego trakcie próbował ustalić dane informatora, który przekazał dziennikarzowi informacje. Redaktor odmówił, powołując się na tajemnicę zawodową. Na wniosek prokuratury sąd rejonowy zwolnił dziennikarza z tajemnicy „w zakresie dotyczącym ujawnienia okoliczności oraz personaliów osoby, od której uzyskał stanowiące informacje poufne dokumenty" owego banku. Dziennikarz złożył zażalenie na postanowienie sądu.

Sąd okręgowy rozpoznający zażalenie uchylił postanowienie sądu rejonowego, przekazując sprawę do ponownego rozpoznania. Sąd rejonowy, po ponownym rozpoznaniu sprawy, oddalił wniosek prokuratora, uznając, że nie było podstaw do uchylenia tajemnicy dziennikarskiej w tej sprawie. Sąd zauważył, że przedmiotem postępowania prowadzonego przez prokuraturę nie jest żadne z najpoważniejszych przestępstw określonych w art. 240 Kodeksu karnego. Nie było zatem powodu dla zwolnienia dziennikarza z obowiązku ochrony źródła informacji. Sąd zwrócił również uwagę, że nie uzasadniono w żaden sposób, iż ujawnienie tajemnicy było „niezbędne dla dobra wymiaru sprawiedliwości”[102].

Zasady dotyczące ochrony dziennikarskich źródeł informacji i autorów materiałów prasowych uregulowane w k.p.k. korespondują z treścią art. 16 prawa prasowego, który także odwołuje się do katalogu najpoważniejszych przestępstw z art. 240 § 1 k.k. jako okoliczności uzasadniających zwolnienie dziennikarza z tajemnicy w tym zakresie. W postępowaniu karnym, gdy zachodzi sytuacja określona w art. 180 § 4 k.p.k, wymaga się jednak dodatkowo spełnienia warunków określonych w art. 180 § 2 k.p.k. (m.in. zgody sądu)[103].

Gwarancje ochrony tajemnicy dziennikarskiej dotyczące przesłuchania w postępowaniu karnym

1. Wymóg zgody sądu na przesłuchanie dziennikarza w zakresie okoliczności objętych tajemnicą.

2. Zgoda sądu może być wydana tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości i tylko gdy dana okoliczność nie może być ustalona na podstawie innego dowodu.

3. Dziennikarz może kwestionować prawidłowość postanowienia sądu o zwolnieniu z tajemnicy. Decyzja sądu może być zaskarżona przez dziennikarza i poddana kontroli instancyjnej.

4. Zwolnienie dziennikarza od obowiązku zachowania tajemnicy co do zasady nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji itp. oraz danych informatorów (jeśli osoby te zastrzegły swoją anonimowość, a następnie nie wyraziły

[102] Postanowienie Sądu Rejonowego w Warszawie z dnia 27 czerwca 2012 r., sygn. akt XIV Kp 1358/12.

[103] W. Lis, *Komentarz do art. 15...*, op. cit., s. 388-389, 394.

zgody na ujawnienie swojej tożsamości). Wyjątkiem od tej zasady są jedynie sytuacje, gdy pozyskany materiał prasowy czy informacja dotyczą któregoś z najpoważniejszych przestępstw wymienionych w art. 240 Kodeksu karnego.

Warunki uzasadniające ingerencje w tajemnicę dziennikarską według Europejskiego Trybunału Praw Człowieka

W ocenie ETPC wszelkie czynności podejmowane w celu ujawnienia tożsamości informatora muszą zostać ograniczone do wyjątkowych sytuacji, związanych z konkretną potrzebą, usprawiedliwionych istotną racją społeczną, która w oczywisty sposób przeważa nad nieujawnianiem źródła.

W szczególności każde ograniczenie ochrony dziennikarskich źródeł informacji musi zostać poddane rygorystycznej kontroli, która zakłada m.in.:

- zbadanie nieskuteczności wszelkich alternatywnych środków dowodowych zmierzających do wyjaśnienia okoliczności popełnienia przestępstwa[104];
- uwzględnienie, czy przekazanie dziennikarzowi poufnej informacji i jej publikacja miały służyć interesowi publicznemu (np. ujawniać nadużycia władzy lub korupcję);
- uwzględnienie, czy działania organów państwa dotyczą sprawy o wystarczająco poważnym charakterze, np. jednego z ciężkich przestępstw (zob. wyżej);
- istnienie solidnych podstaw podejrzenia popełnienia takiego przestępstwa, które muszą być szczegółowo wykazane przez organy państwa;
- istnienie rygorystycznej kontroli sądowej środków skutkujących zwolnieniem z tajemnicy dziennikarskiej[105].

Uwaga! Odmowa przez dziennikarza ujawnienia danych, o których mowa w art. 180 § 3 k.p.k., nie uchyla jego odpowiedzialności za przestępstwo, którego się dopuścił, publikując informację (art. 180 § 5 k.p.k.). W określonych okolicznościach sądy mogą jednak uznać za dopuszczalne opublikowanie przez dziennikarzy np. tajnych informacji (zob. pyt. 6).

[104] Zob. Wyrok ETPC z dnia 23 lutego 2003 r. w sprawie *Roemen i Schmitt p. Luksemburgowi*, skarga nr 51772/99; wyrok ETPC z dnia 15 lipca 2003 r. w sprawie *Ernst i inni p. Belgii*, skarga nr 33400/96.

[105] Wyrok ETPC z dnia 14 września 2010 r. (Wielka Izba) w sprawie *Sanoma Uitgevers B.V. p. Holandii*, skarga nr 38224/03.

13. Jakie inne działania organów państwa mogą naruszać tajemnicę dziennikarską?

Organy państwa, poza przesłuchaniem dziennikarza jako świadka w postępowaniu karnym, mogą podejmować wobec przedstawicieli mediów także inne czynności zmierzające do pozyskania informacji objętych tajemnicą dziennikarską, w tym do ujawnienia tożsamości osoby przekazującej dziennikarzowi poufne informacje z zastrzeżeniem anonimowości. Do czynności takich należą np.: przeszukanie redakcji, nakaz wydania korespondencji lub innych dokumentów znajdujących się w posiadaniu dziennikarza, inwigilacja komunikacji dziennikarza prowadzonej za pośrednictwem telefonu lub internetu.

W orzecznictwie ETPC za naruszenie zasad tajemnicy dziennikarskiej uznaje się nie tylko nakaz ujawnienia informatora bezpośrednio skierowany do dziennikarza (np. podczas przesłuchania), ale także inne działania podejmowane przez policję lub prokuraturę, zmierzające do ustalenia osób odpowiedzialnych za ujawnienie poufnych informacji mediom.

Działania naruszające tajemnicę dziennikarską według Europejskiego Trybunału Praw Człowieka

W sprawie *Roemen i Schmitt p. Luksemburgowi*[106], a także w sprawie *Ernst i inni p. Belgii*[107] Trybunał uznał za złamanie tajemnicy dziennikarskiej ingerencję w postaci przeszukania pomieszczeń redakcyjnych i mieszkań dziennikarzy oraz zajęcie znajdujących się tam dokumentów.

W wyroku wydanym przez Wielką Izbę Trybunału w sprawie *Sanoma Uitgevers B.V p. Holandii*[108] ETPC zakwalifikował jako naruszenie tajemnicy dziennikarskiej żądanie organów ścigania skierowane do wydawcy tygodnika motoryzacyjnego, dotyczące wydania materiałów zawierających zdjęcia umożliwiające identyfikację uczestników nielegalnego rajdu samochodowego (wcześniej magazyn opublikował artykuł na ten temat).

Obecnie na rozpoznanie przed ETPC oczekuje sprawa *Bureau of Investigative Journalism i Alice Ross p. Wielkiej Brytanii*, która dotyczy m.in. naruszenia gwarancji ochrony dziennikarskich źródeł informacji w związku z korzystaniem

[106] Wyrok ETPC z dnia 25 lutego 2003 r. w sprawie *Roemen i Schmitt p. Luksemburgowi*, skarga nr 51772/99.

[107] Wyrok ETPC z dnia 15 lipca 2003 r. w sprawie *Ernst i inni p. Belgii*, skarga nr 33400/96.

[108] Wyrok ETPC z dnia 14 września 2010 r. (Wielka Izba) w sprawie *Sanoma Uitgevers B.V. p. Holandii*, skarga 38224/03.

przez brytyjskie służby specjalne z programów masowej inwigilacji komunikacji telefonicznej i internetowej obywateli[109].

Gwarancje wynikające z tajemnicy dziennikarskiej mogą zostać naruszone przez wszelkie czynności lub działania mogące doprowadzić do ustalenia tożsamości informatora, np. przeszukanie redakcji lub mieszkania dziennikarza, zajęcie komputera oraz informatycznych nośników czy też inwigilacja dziennikarzy. W ocenie ETPC takie czynności lub działania są nawet groźniejsze z perspektywy ochrony dziennikarskich źródeł informacji niż bezpośrednie żądanie skierowane do dziennikarza, aby ujawnił tożsamość swojego informatora, ponieważ odbywają się one niezależnie od dziennikarza i poza jego kontrolą[110].

14. Czy organy państwa mogą przeszukać redakcję i zająć znajdujące się tam dokumenty?

Tajemnica dziennikarska może obejmować wszelkie nieosobowe źródła informacji, które znajdują się w posiadaniu dziennikarza (np. dokumenty, osobiste notatki, pliki na komputerze czy dowody z podsłuchu lub billingów telefonicznych)[111]. Czy prawo przewiduje jakieś ograniczenia w zakresie żądania wydania i zajęcia materiałów, które mogą zawierać tajemnicę dziennikarską lub przeszukania siedziby redakcji[112]?

Prawnicy są w tym zakresie podzieleni. Jak pisze W. Lis, „jeśli określona informacja podlega ochronie na podstawie art. 180 k.p.k., a została utrwalona na materialnym nośniku danych, to, co do zasady, nie można jej zatrzymać ani poszukiwać. Zakazy i ograniczenia co do tożsamości informatora przestają wiązać, jeśli czynność dowodowa ma na celu uzyskanie informacji, w przypadku kiedy w grę wchodzi jedno z przestępstw wymienionych w art. 240 k.k. albo tajemnica zostanie uchylona przez jej dysponenta. W pozostałym zakresie podmiotem uprawnionym do wydania zgody na odtajnienie dokumentów zawierających informacje objęte tajemnicą dziennikarską jest sąd”[113]. Na konieczność wzięcia pod uwagę

[109] Skarga nr 58170/13, sprawa została już zakomunikowana brytyjskiemu rządowi.

[110] Wyrok ETPC w sprawie *Roemen i Schmitt p. Luksemburgowi*, op. cit.; wyrok ETPC w sprawie *Ernst i inni p. Belgii*, op. cit.; wyrok ETPC z dnia 16 lipca 2013 r. w sprawie *Nagla p. Łotwie*, skarga nr 73469/10.

[111] W. Lis, *Komentarz do art. 15...*, op. cit., s. 404.

[112] Przeprowadzenie obu czynności reguluje Kodeks postępowania karnego (zob. art. 217 i art. 219-224 k.p.k.).

[113] Ibidem, s. 405.

ograniczeń dotyczących już samego żądania wydania albo poszukiwania rzeczy mogących zawierać tajemnicę dziennikarską wskazuje także orzecznictwo ETPC (zob. niżej oraz pyt. 12-13). Z drugiej strony B.J. Stefańska twierdzi, że „nie ma przeszkód do dokonania tych czynności, a jedynie konieczne jest zachowanie szczególnego trybu postępowania z takimi dokumentami”[114].

Prawo przewiduje natomiast wprost pewne ograniczenia dotyczące wykorzystania w postępowaniu karnym materiałów zawierających informacje objęte tajemnicą dziennikarską, które zostały pozyskane w wyniku zatrzymania rzeczy lub przeszukania redakcji (lub domu dziennikarza). Art. 226 k.p.k. określa, że w kwestii wykorzystania dokumentów zawierających tajemnice państwową, służbową lub zawodową jako dowodów w postępowaniu karnym stosuje się odpowiednio zakazy i ograniczenia określone w art. 178-181 k.p.k. Oznacza to, że w odniesieniu do dokumentów (i innych nośników informacji) zawierających tajemnicę dziennikarską znajdujących się w dyspozycji dziennikarza zastosowanie znajdą zakazy i ograniczenia wynikające z treści art. 180 § 2-4 k.p.k. Jeśli więc np. dokument zawiera informacje identyfikujące dziennikarskiego informatora czy autora materiału prasowego, którzy zastrzegli swoją anonimowość, wykorzystanie ich w postępowaniu karnym jest niedopuszczalne. Jedynym wyjątkiem od tej zasady jest sytuacja, gdy chodzi o informacje o przestępstwie określonym w art. 240 k.k. (wówczas możliwe jest zwolnienie przez sąd z obowiązku zachowania nawet tej części tajemnicy).

Policja w redakcji

Dziennikarz otrzymał od informatora e-mailem informacje ujawniające, że firma X nielegalnie zanieczyszcza środowisko. Po publikacji artykułu na ten temat firma X złożyła zawiadomienie na policji o podejrzeniu popełnienia czynu nieuczciwej konkurencji, wskazując, że obciążające ją informacje zostały najpewniej przekazane przez konkurencyjną firmę Y. W redakcji gazety zjawiła się policja z żądaniem udostępnienia całej zawartości służbowej skrzynki e-mail dziennikarza w celu weryfikacji, czy informacje rzeczywiście przekazał któryś z pracowników firmy Y.

W świetle przedstawionych regulacji taki dowód nie mógłby być jednak wykorzystany w postępowaniu przeciwko firmie Y. Dokumenty związane z działalnością zawodową dziennikarza, mogące służyć identyfikacji osób udzielających mu informacji (takie jak np. zawartość skrzynki poczty

[114] B.J. Stefańska, *Przeszukanie a tajemnica dziennikarska*, op. cit., s. 60.

elektronicznej dziennikarza), staną się dozwolonym środkiem dowodowym jedynie w przypadku najcięższych przestępstw, o których mówi art. 240 § 1 Kodeksu karnego, i po uzyskaniu zgody sądu. Odmienna praktyka stanowiłaby niedopuszczalne obejście zakazu dowodowego istniejącego w Kodeksie postępowania karnego.

Jeśli dziennikarz, u którego dokonano zajęcia np. dokumentu lub komputera (lub odnaleziono je po przeprowadzeniu u niego przeszukania), oświadczy, że znajdują się w nich informacje objęte tajemnicą dziennikarską, prawo przewiduje specjalny tryb postępowania z takimi przedmiotami. W takim przypadku organ przeprowadzający przeszukanie (z reguły policja albo inna służba) nie zapoznaje się z ich treścią, tylko opieczętowuje takie dokumenty i niezwłocznie przekazuje w zabezpieczonej kopercie prokuratorowi lub sądowi, w zależności od tego, czyje postanowienie wykonuje (art. 225 § 1 k.p.k.). O możliwości wykorzystania takiego dokumentu w postępowaniu karnym zgodnie z art. 226 w zw. z art. 180 § 2-4 k.p.k. może zadecydować tylko sąd. Jeśli dokument ten zawiera informacje mogące zidentyfikować informatora, sąd nie będzie mógł dopuścić do jego wykorzystania w postępowaniu (chyba, że materiał dotyczy jednego z najcięższych przestępstw z art. 240 k.k.).

Uwaga! Opisany w art. 225 § 1 k.p.k. tryb postępowania nie obowiązuje, jeśli dokumenty zawierające tajemnicę dziennikarską znajdują się w posiadaniu osoby podejrzanej o popełnienie przestępstwa (art. 225 § 2).

Warto dodać, że przeszukanie zawsze powinno odbywać się z zachowaniem umiaru i poszanowania godności osób, których ta czynność dotyczy, oraz bez wyrządzania niepotrzebnych szkód i dolegliwości (art. 227 k.p.k.). Na postanowienie o wydaniu rzeczy lub przeszukaniu osoba, której dotyczą te czynności (np. dziennikarz), może złożyć zażalenie, jeśli uznaje, że zostały przeprowadzone niezgodnie z prawem (art. 236 k.p.k.). Dziennikarz może również złożyć zażalenie na postanowienie sądu dopuszczające wykorzystanie w postępowaniu karnym np. zajętego dokumentu z redakcji (np. może argumentować, że dokument ten, wbrew pierwotnemu stanowisku sądu, zawiera jednak informacje identyfikujące informatora i dlatego nie powinien zostać dopuszczony przez sąd).

Przeszukanie z umiarem

W 2014 r. ABW wkroczyło do redakcji tygodnika „Wprost" w związku z tzw. „aferą podsłuchową" w celu zajęcia nośników zawierających nagrania podsłuchanych rozmów polityków i urzędników. Akcję tę skrytykowało w pewnym zakresie Ministerstwo Sprawiedliwości, które w informacji[115] opublikowanej po tym zdarzeniu zwróciło uwagę m.in. na brak adekwatności stosowanych środków do sytuacji. W informacji podkreślono, że działania prokuratury powinny dążyć do pełnej realizacji wolności słowa i powinny być „dostosowane do istotnych ograniczeń związanych z zakresem ochrony tajemnicy dziennikarskiej". Zdaniem Ministerstwa w tej perspektywie należało w tym przypadku rozumieć zasadę umiaru i poszanowania godności osób z art. 227 Kodeksu postępowania karnego. Tymczasem, zdaniem Ministerstwa, działania organów państwa były w tej sytuacji „zbyt daleko idące i mogły budzić uzasadnioną obawę naruszenia tajemnicy dziennikarskiej". Ministerstwo uznało m.in., że ewentualne zajęcie komputerów w redakcji tygodnika mogłoby być nadmiernie uciążliwe i nieproporcjonalnie dolegliwe dla dziennikarzy w kontekście prac nad kolejną publikacją. Zauważono również, że zlecona przez prokuratora czynność wykonania kopii binarnej zawartości redakcyjnych komputerów była niezgodna z art. 225 § 1 Kodeksu postępowania karnego („czynność ta skutkuje „odczytaniem" pliku przez oprogramowanie komputera zgrywającego"). Jednocześnie należy dodać, że ostatecznie sąd, który badał zasadność i przebieg akcji ABW w reakcji nie stwierdził w tej sprawie nieprawidłowości[116].

Przeszukanie redakcji a tajemnica dziennikarska w orzecznictwie Europejskiego Trybunału Praw Człowieka

Trybunał wielokrotnie dochodził do wniosku, że przeszukanie redakcji i zajęcie znajdujących się w niej dokumentów stanowi naruszenie art. 10 EKPC (wolność słowa). Co więcej, stwierdzał, że takie czynności naruszają również art. 8 EKPC (tj. prawo do „poszanowania mieszkania" wydawcy,

[115] Informacja Ministra Sprawiedliwości o czynnościach podjętych 18 czerwca 2014 roku przez organy ścigania wobec redaktora naczelnego „Wprost" – Sylwestra Latkowskiego w związku z tzw. aferą podsłuchową, 20 czerwca 2014 r., https://ms.gov.pl/pl/informacje/download,6142,0.html (dostęp: 15 marca 2016 r.).

[116] M. Duda, *Sąd: przeszukanie w redakcji „Wprost" było zgodne z prawem*, tvn24.pl, 21 lipca 2014 r., http://www.tvn24.pl/wiadomosci-z-kraju,3/sad-przeszukanie-w-redakcji-wprost-bylo-zgodne-z-prawem,451835.html (dostęp: 15 marca 2016 r.).

chronionego jako element prawa do prywatności)[117]. W szczególności Trybunał uznawał, że przeszukanie prowadziło do złamania Konwencji, gdy organy państwa mogły zrealizować ten sam cel za pomocą mniej inwazyjnych metod, a zakres tej czynności nie był wystarczająco wąsko określony (np. gdy nakaz nie dotyczył zajęcia konkretnych materiałów, ale „wszelkich dokumentów mogących mieć związek ze sprawą")[118].

Co więcej, już samo postanowienie polegające na żądaniu przekazania danych znajdujących się w dyspozycji dziennikarza (wydawcy), niezależnie od ewentualnych następczych środków prawnych w celu egzekucji postanowienia, może stanowić – w świetle wyroku ETPC w sprawie *Financial Times Ltd. i inni p. Wielkiej Brytanii* – ingerencję w prawo zagwarantowane na mocy art. 10 Konwencji[119].

Jedną z nielicznych spraw, w których Trybunał nie stwierdził naruszenia Konwencji w związku z przeszukaniem redakcji i zajęciem w niej nośników danych, była sprawa *Stichting Ostade Blade p. Holandii*[120]. Holenderska policja szukała w redakcji listu nadesłanego do gazety po serii ataków terrorystycznych. Autor listu przedstawiał się w nim jako rzekomy sprawca ataków. ETPC uznał, że w takim przypadku informator, który przyznaje się do popełnienia poważnego przestępstwa i zwraca się do dziennikarzy, ponieważ szuka rozgłosu dla swoich działań, nie podlega ochronie jako dziennikarskie źródło informacji.

Podsumowując, należy zauważyć, że:

1. Możliwość dowodzenia okoliczności objętych tajemnicą dziennikarską jest ograniczona również w odniesieniu do innych niż zeznanie świadka środków dowodowych, dlatego niedopuszczalną praktyką organów ścigania byłyby próby obejścia przedstawionych ograniczeń poprzez dokonywanie przeszukań lokali służbowych redakcji oraz prywatnych mieszkań osób zobowiązanych do zachowania tajemnicy.

[117] Wyrok ETPC z dnia 18 marca 2013 r. w sprawie *Saint-Paul Luxembourg S.A. p Luksemburgowi*, skarga nr 26419/10.

[118] Ibidem.

[119] Wyrok ETPC z dnia 15 grudnia 2009 r. w sprawie *Financial Times Ltd. i inni p. Wielkiej Brytanii*, skarga nr 821/03.

[120] Wyrok ETPC z dnia 27 maja 2014 r. w sprawie *Stichting Ostade Blade p. Holandii*, skarga nr 8406/06.

2. W polskim prawie nie ma jednak przepisu, który wyraźnie zakazywałby przeprowadzenia przeszukania w redakcji czy żądania wydania dokumentów, komputerów czy dysków znajdujących się w posiadaniu dziennikarza.

3. Jednocześnie organy państwa powinny kierować się wytycznymi ETPC przy podejmowaniu decyzji o podjęciu takich działań wobec przedstawicieli mediów, mając również na uwadze szczególny charakter pracy dziennikarskiej i jej rolę w zapewnianiu dostępu opinii publicznej do informacji.

4. Polskie prawo ogranicza ponadto możliwość wykorzystania dokumentów i innych nośników informacji zawierających tajemnicę dziennikarską w postępowaniu karnym. Przewiduje także specjalny tryb postępowania z materiałami wydanymi lub odnalezionymi w trakcie przesłuchania, co do których zostało zgłoszone zastrzeżenie, że zawierają informacje objęte tajemnicą.

Izba Wydawców Prasy w liście z 2010 r. do ministra sprawiedliwości zwróciła uwagę, że prawo powinno stwarzać silniejsze gwarancje ochrony tajemnicy dziennikarskiej w przypadku żądania od dziennikarza wydania dokumentów i innych przedmiotów, które zawierają poufne informacje, a także przeszukania redakcji. W liście podkreślono:

„Przepisy Kodeksu postępowania karnego nie przewidują wprost sytuacji, w której wydawcy prasowemu przysługiwałoby prawo odmowy wydania dokumentu lub odmowy jego ujawnienia w toku przeszukania do czasu orzeczenia sądu o wydaniu tego dokumentu. Przepisy art. 225 i art. 226 Kodeksu postępowania karnego nie stanowią wystarczającej ochrony, ponieważ umożliwiają organom ścigania zajęcie dokumentów zawierających informacje o tożsamości źródeł informacji, blokując jedynie możliwość ich procesowego wykorzystania. […]

Nowelizacja [k.p.k. – przyp. aut.] powinna umożliwiać wydawcy prasy zatrzymanie dokumentów zawierających informacje o tożsamości źródeł informacji dziennikarzy u wydawcy i wydanie ich dopiero, gdy uprawomocni się orzeczenie sądu nakazujące ich wydanie. W przypadku przeszukania do dokumentów zawierających informacje o tożsamości źródeł informacji dziennikarzy powinien mieć zastosowanie tryb przewidziany w przepisach art. 225 § 3 Kodeksu postępowania karnego, przy czym w przepisie tym powinno być wyraźnie wskazane, że ujawnienie dokumentów obejmujących okoliczności związane z wykonywaniem funkcji obrońcy, jak również dokumentów zawierających informacje

o tożsamości źródeł informacji dziennikarzy powinno nastąpić dopiero po uprawomocnieniu się postanowienia sądu o ich zatrzymaniu dla celów postępowania”[121].

15. Czy inwigilacja dziennikarza może naruszać gwarancje tajemnicy dziennikarskiej?

Kontrola rozmów telefonicznych oraz utrwalanie przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, a także monitorowanie tzw. metadanych dotyczących dziennikarza (billingów, danych dotyczących jego aktywności w internecie) również stanowi istotne zagrożenie dla tajemnicy dziennikarskiej, zwłaszcza w zakresie ochrony źródeł informacji. Zasady dopuszczalności stosowania tego rodzaju środków wobec przedstawicieli mediów zostały omówione bardziej szczegółowo w kolejnym rozdziale Przewodnika.

16. Czy dziennikarz może sam zwolnić się z tajemnicy dziennikarskiej?

Należy podkreślić, że aby gwarancje wynikające z tajemnicy dziennikarskiej mogły być w pełni realizowane, muszą być respektowane zarówno przez instytucje państwa, jak i samych przedstawicieli mediów. Jak podkreśla się w orzecznictwie sądów, tajemnica dziennikarska ma przede wszystkim służyć ochronie osób przekazujących mediom poufne informacje, a nie ochronie samych dziennikarzy[122]. W literaturze i orzecznictwie zwraca się ponadto uwagę, że to informator jest dysponentem tajemnicy dziennikarskiej i to on może podjąć decyzję o jej zniesieniu, a dziennikarz jest jedynie depozytariuszem tajemnicy zobowiązanym do jej zachowania i nie ma prawa „decydować ani o jej zakresie czasowym i przedmiotowym, ani tym bardziej sam się z niej zwolnić”[123].

Uzależnienie ochrony źródeł od woli dziennikarzy, nie dawałoby informatorom wystarczającej gwarancji ochrony i wystawiałoby ich na zbyt duże ryzyko. Dlatego dziennikarz nie może dowolnie decydować o tym, czy ujawni swojego informatora, czy też nie. Jak pisze I. Dobosz, „gdyby tajemnica dziennikarska była uprawnieniem dziennikarza, mógłby on z niej korzystać w sytuacji dla siebie dogodnej (np. nie podając danych swoich informatorów), a w sytuacji

[121] List Izby Wydawców Prasy do Ministra Sprawiedliwości z dnia 15 listopada 2010 r.

[122] Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 28 czerwca 2011 r., I OSK 1217/10.

[123] W. Lis, *Komentarz do art. 15...*, op. cit., s. 382; zob. także postanowienie Sądu Najwyższego z 20 października 2005 r., sygn. akt II KK 184/05.

niesprzyjającej (np. w razie grożącego mu procesu prasowego) ujawnić informatorów, przez co miałby z pewnością korzystniejszą dla siebie sytuację procesową"[124]. Podobny pogląd wyraża S. Zabłocki, który podkreśla, że nie może dojść do samozwolnienia się dziennikarza z tajemnicy dziennikarskiej, i odrzuca stanowczo stanowisko o jedynie etycznym charakterze takiej tajemnicy, kładąc nacisk na prawny charakter tego obowiązku[125]. Samozwolnienie się dziennikarza z tajemnicy jest więc niedopuszczalne, nawet jeśli informator świadomie wprowadził dziennikarza w błąd i naraził go na odpowiedzialność za opublikowanie fałszywych informacji (zob. pyt. 7).

17. Co grozi za naruszenie tajemnicy dziennikarskiej?

Za niedochowanie tajemnicy dziennikarskiej przez dziennikarzy, np. poprzez nieuzasadnione ujawnienie tożsamości informatora, który zastrzegł swoją anonimowość, dziennikarze mogą zostać pociągnięci do odpowiedzialności. Zgodnie z art. 49 prawa prasowego naruszenie tajemnicy zawodowej przez dziennikarza jest przestępstwem, które jest zagrożone karą grzywny albo ograniczenia wolności. Dziennikarze oraz inni depozytariusze tajemnicy dziennikarskiej (np. inne osoby zatrudnione w redakcji) mogą ponadto podlegać odpowiedzialności karnej na podstawie art. 266 k.k. dotyczącego ujawnienia tajemnicy zawodowej. Za przestępstwo to grozi kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Oprócz odpowiedzialności karnej dziennikarz (redaktor naczelny, wydawca) może zostać pociągnięty do odpowiedzialności cywilnej za naruszenie dóbr osobistych informatora czy autora materiału prasowego, którego tożsamość bezprawnie ujawnił[126].

Za bezpodstawne naruszenie gwarancji wynikających z tajemnicy dziennikarskiej odpowiedzialność może ponieść także funkcjonariusz organu państwowego, który np. podejmował działania zmierzające do obejścia przepisów chroniących tę tajemnicę. Takie zachowanie może spotkać się z zarzutem przekroczenia uprawnień przez funkcjonariusza publicznego (art. 231 k.k.)[127]. Funkcjonariusz

[124] I. Dobosz, *Prawo i etyka w zawodzie dziennikarza*, Kraków 2008, s. 66.

[125] S. Zabłocki, *Problem „samozwolnienia się" dziennikarza z tajemnicy anonimatu* [w:] J. Jakubowska-Hara, C. Nowak, J. Skupiński (red.), *Reforma prawa karnego. Propozycje i komentarze. Księga pamiątkowa Prof. Barbary Kunickiej-Michalskiej,* Warszawa 2008, s. 464-478.

[126] Opinia przyjaciela sądu HFPC ws. naruszenia tajemnicy dziennikarskiej, 17 lutego 2016 r., http://www.obserwatorium.org/images/Amicus-1.pdf (dostęp: 10 marca 2016 r.).

[127] W. Gontarski, *Prokurator nadużywa władzy*, „Rzeczpospolita", 13 grudnia 2004 r.

bądź organ państwowy, w którym funkcjonariusz ten pracuje, może zostać ponadto pociągnięty do odpowiedzialności cywilnej za naruszenie dóbr osobistych (zob. sprawa red. B. Wróblewskiego opisana w rozdziale III Przewodnika).

Odpowiedzialność organów państwa za naruszenie tajemnicy

Dziennikarz X napisał artykuł na temat korupcji w Ministerstwie Y. Dwa dni później policja na polecenie prokuratury zrobiła przeszukanie w redakcji, w której pracował dziennikarz, i zajęła jego służbowy komputer, argumentując, że istniało uzasadnione podejrzenie, iż dziennikarz bezprawnie rozpowszechniał w internecie utwory, do których nie miał praw autorskich. Później okazało się jednak, że zarzut ten się nie potwierdził, a organy ścigania nie miały w istocie żadnych podstaw do przyjęcia, że X rzeczywiście dopuścił się przestępstwa. Był to jedynie pretekst, aby uzyskać dostęp do zawartości komputera dziennikarza i ustalić, kto przekazał mu informację na temat nieprawidłowości w Ministerstwie (w sprawie przecieku toczyło się już postępowanie przygotowawcze). Dziennikarz złożył w najbliższej jednostce policji zawiadomienie o podejrzeniu popełnienia przestępstwa nadużycia uprawnień przez prokuratora, który wydał nakaz przeszukania i zajęcia komputera. Postanowił ponadto skierować przeciwko prokuraturze powództwo o ochronę dóbr osobistych przed sądem cywilnym.

18. Jakie inne uprawnienia, poza ochroną anonimowości, mają osoby przekazujące informacje mediom?

Prawo prasowe przyznaje osobom, które udzielają dziennikarzom informacji lub wywiadu (także nie zastrzegając anonimowości), pewne uprawnienia względem mediów. Przede wszystkim zgodnie z art. 12 ust. 1 pkt 2 prawa prasowego „dziennikarz jest obowiązany chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów i innych osób, które okazują mu zaufanie". Dziennikarz nie może publikować lub rozpowszechniać w inny sposób informacji „utrwalonych za pomocą zapisów fonicznych i wizualnych" bez zgody osób udzielających mu tych informacji (art. 14 ust. 1 prawa prasowego). Jeśli zatem dziennikarz nagrywa swojego rozmówcę na dyktafon lub kamerę, co do zasady powinien uzyskać jego zgodę na upublicznienie takich nagrań. Ponadto osoba udzielająca informacji może z ważnych powodów społecznych lub

osobistych zastrzec termin i zakres jej opublikowania (art. 14 ust. 3 prawa prasowego). Co więcej, dziennikarz nie może opublikować informacji, jeżeli osoba udzielająca jej zastrzegła to ze względu na tajemnicę zawodową (art. 14 ust. 5 prawa prasowego).

Prawo chroni także przed ingerencją mediów w sferę życia prywatnego osób znajdujących się w ich obszarze zainteresowania. Zgodnie z art. 14 ust. 6 praw prasowego „nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby". Rozmówca dziennikarza ma także prawo poprosić o autoryzację swojej dosłownie cytowanej wypowiedzi. Dziennikarz jest związany takim żądaniem, nie może odmówić swojemu interlokutorowi autoryzacji, o ile wypowiedź ta nie była uprzednio publikowana (art. 14 ust. 2 prawa prasowego). Należy jednocześnie podkreślić, że zgodnie z art. 14 ust. 4 prawa prasowego rozmówca dziennikarza nie może jednak uzależniać udzielenia informacji od sposobu jej skomentowania lub uzgodnienia tekstu wypowiedzi dziennikarskiej (z zastrzeżeniem wynikającym z art. 14 ust. 2).

19. Gdzie można przeczytać więcej na temat gwarancji wynikających z tajemnicy dziennikarskiej?

Publikacje:

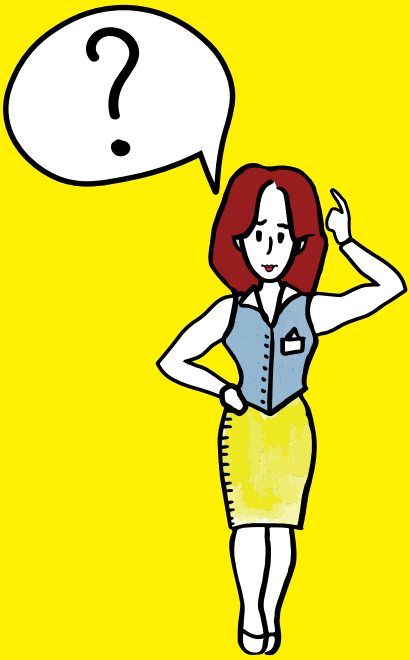
• I. C. Kamiński, *Ochrona dziennikarskich źródeł informacji w Europejskiej Konwencji Praw Człowieka* [w:] T. Kononiuk (red.) *Dziennikarz – utwór – prasa. Księga jubileuszowa z okazji pięćdziesięciolecia pracy naukowej prof. dr. hab. Bogdana Michalskiego*, Warszawa 2014.
• B. Kosmus, G. Kuczyński (red.), *Prawo prasowe. Komentarz*, Warszawa 2013.
• W. Lis, P. Wiśniewski, Z. Husak (red.), *Prawo prasowe. Komentarz*, Warszawa 2012.
• J. Sobczak, *Prawo prasowe. Podręcznik akademicki*, Warszawa 2012.
• M. Zaremba, *Prawo prasowe. Ujęcie praktyczne*, Warszawa 2007.

Strony internetowe:

• Obserwatorium.org
Strona internetowa programu Obserwatorium Wolności Mediów w Polsce Helsińskiej Fundacji Praw Człowieka, która zawiera informacje na temat spraw związanych z tajemnicą dziennikarską monitorowanych przez Fundację oraz opinie przyjaciela sądu przygotowywane w tych sprawach.

Rozdział III

Dziennikarze i sygnaliści - zagrożenia w dobie nowoczesnych technologii



Wprowadzenie

Przyjęta w styczniu 2016 r. nowelizacja ustawy o Policji[128] rozbudziła w Polsce na nowo debatę o anonimowości i bezpieczeństwie w sieci. Tendencję do zaostrzania regulacji umożliwiających służbom inwigilację obywateli można zaobserwować nie tylko w naszym kraju, ale także w innych państwach europejskich oraz w Stanach Zjednoczonych. Grupą szczególnie narażoną na inwigilację są dziennikarze, ale także dziennikarskie źródła informacji, w tym sygnaliści, którzy ujawniając nieprawidłowości, korzystają z pomocy przedstawicieli mediów.

Zgodnie z badaniem[129] przeprowadzonym przez Pew Research Center we współpracy z Uniwersytetem Columbia na próbie 671 dziennikarzy śledczych prawie 2/3 (64%) spośród badanych uważa, że rząd USA miał dostęp do ich danych telekomunikacyjnych. Natomiast 8 na 10 dziennikarzy zadeklarowało, że ich zdaniem praca w tym zawodzie zwiększa ryzyko zainteresowania ze strony służb specjalnych. Dziennikarze stwierdzili również, że zagrożenie inwigilacją ma negatywny wpływ na gotowość informatorów do ujawniania istotnych z punktu widzenia interesu publicznego faktów. Specjalny Sprawozdawca ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi zaznaczył w jednym ze swoich raportów[130], że „powszechne wykorzystywanie urządzeń elektronicznych razem z możliwością rządu wglądu w dane i ślady, które te urządzenia za sobą zostawiają, stanowi poważne wyzwanie dla poufności i anonimowości dziennikarskich źródeł informacji i sygnalistów”[131].

W praktyce problem nieuprawnionego ujawnienia tożsamości informatorów wystąpił w wielu sprawach, w których rząd Stanów Zjednoczonych zidentyfikował dziennikarskie źródła informacji na podstawie danych pochodzących z rozmów telefonicznych

[128] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 147).

[129] Pew Research Center, Centrum Cyfrowego Dziennikarstwa Uniwersytetu Columbia, *Investigative Journalists and Digital Security. Perceptions of Vulnerability and Changes in Behavior*, 2016, http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf (dostęp: 15 marca 2016 r.).

[130] Raport Specjalnego Sprawozdawcy ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi ws. ochrony dziennikarskich źródeł informacji i sygnalistów z dnia 8 września 2015 r., A/70/361, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361 (dostęp: 10 marca 2016 r.).

[131] J. Posetti, *Protecting journalism sources in the digital age*, Paryż 2015.

oraz e-maili[132]. Istnieją również potwierdzone przypadki inwigilacji dziennikarzy w Polsce. Można tu wskazać chociażby sprawę 10 dziennikarzy, których billingi były pobierane przez Centralne Biuro Antykorupcyjne (informację tę ujawniła „Gazeta Wyborcza" w 2010 r.[133]) czy sprawę trojga dziennikarzy, których dane telekomunikacyjne pozyskała Wojskowa Prokuratura Garnizonowa w Poznaniu w 2010 r.[134]. W 2016 r. media informowały, że w latach 2014-2015 służby specjalne miały stosować inwigilację wobec 52 dziennikarzy[135].

W rozdziale II Przewodnika podkreślaliśmy, że ochrona informatorów nie jest przywilejem, ale przede wszystkim obowiązkiem dziennikarzy. **Obowiązek ten obejmuje nie tylko konieczność powstrzymania się od ujawnienia komukolwiek danych informatora, który zastrzegł swoją anonimowość, ale także podjęcie przez dziennikarzy odpowiednich działań, wzmacniających bezpieczeństwo źródła informacji.** Jak słusznie wskazuje się w doktrynie prawa, „dziennikarz, spotykając się z informatorami, powinien zadbać o to, aby nie wyniknęła stąd krzywda dla tych osób. Powinien przede wszystkim zadbać o odpowiednie warunki poufności takiego spotkania, a więc np. powinno się ono odbywać podczas dyżuru w redakcji, a nie w zakładzie pracy informatora czy w jego domu"[136]. Dziś każdy dziennikarz musi się zastanowić, w jaki sposób może chronić swoje źródła informacji nie tylko w przypadku tradycyjnych metod kontaktowania się z informatorami, ale także w kontekście zagrożeń związanych z wykorzystywaniem nowoczesnych technologii.

Rozwój nowoczesnych technologii ułatwia komunikację dziennikarzy i ich źródeł informacji, ale powoduje też nowe zagrożenia, narażając przedstawicieli mediów i ich informatorów na coraz bardziej wyrafinowane sposoby inwigilacji. Prawo nie zapewnia w pełni efektywnych gwarancji dla ochrony tajemnicy dziennikarskiej przed takimi działaniami. Ważnym elementem warsztatu

[132] PEN America, *Chilling effects: NSA surveillance drives U.S. writers to self-censor, Nowy Jork 2013. Human Rights Watch, American Civil Liberties Union, With liberty to monitor all: how large-scale U.S. surveillance is harming journalism, law and American democracy*, Nowy Jork 2014.

[133] W. Czuchnowski, *Dziennikarze na celowniku służb*, Gazeta Wyborcza, 8 października 2010 r., http://wyborcza.pl/1,76842,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html (dostęp: 15 marca 2016 r.).

[134] Zob. IAR, *Dziennikarz o Przybyle: to była inwigilacja*, polskieradio.pl, 9 stycznia 2012 r. http://www.polskieradio.pl/5/3/Artykul/514446,Dziennikarz-o-Przybyle-to-byla-inwigilacja (dostęp: 15 marca 2016 r.).

[135] PAP, *Inwigilacja dziennikarzy: szef służb specjalnych zawiadomi prokuraturę w marcu*, Rzeczpospolita, 14 marca 2016 r., http://www.rp.pl/Prawo-karne/303149906-Inwigilacja-dziennikarzy-szef-sluzb-specjalnych-zawiadomi-prokurature-w-marcu.html (dostęp: 15 marca 2016 r.).

[136] E. Nowińska, *Wolność wypowiedzi...*, op. cit., s. 131.

współczesnych dziennikarzy jest więc korzystanie z technicznych metod zwiększających bezpieczeństwo komunikacji. Dziennikarze, jako jedna z grup zawodowych najbardziej narażonych na inwigilację, powinni stosować te narzędzia, aby skuteczniej chronić swoich informatorów.

W rozdziale III Przewodnika wyjaśniamy, na czym może polegać inwigilacja dziennikarzy (oraz innych obywateli) i jakie są jej ograniczenia w związku z koniecznością poszanowania ochrony tajemnicy dziennikarskiej. Przedstawimy także praktyczne narzędzia zwiększające bezpieczeństwo korzystania z nowoczesnych technologii przez dziennikarzy, m.in. w celu komunikacji ze źródłami informacji (np. sygnalistami). Opiszemy również możliwości dochodzenia praw w przypadku nieuzasadnionej inwigilacji przedstawicieli mediów.

1. Czy inwigilacja dziennikarzy jest dopuszczalna?

Niewątpliwie ochrona bezpieczeństwa obywateli i walka z poważną przestępczością może w określonych sytuacjach usprawiedliwiać pewną ingerencję w prawa i wolności obywatelskie, do której dochodzi przy użyciu tajnych technik operacyjnych przez organy państwa. Ingerencja ta jednak nigdy nie może wykraczać poza niezbędny zakres. Jak pisze W. Osiatyński, aby uniknąć nadużyć władzy i łamania praw w takich przypadkach, konieczne jest „ustanowienie standardów określających, jakie prawa, w jakich sytuacjach, w jakim stopniu i z użyciem jakich procedur mogą zostać zawieszone. Równie ważne jest to, by standardy te były stosowane z uwzględnieniem zasady proporcjonalności”[137].

Nie każda ingerencja w prawa i wolności obywatelskie może być zatem usprawiedliwiona względami bezpieczeństwa. W tym kontekście należy podkreślić, że inwigilacja dziennikarzy w związku z ich działalnością zawodową stanowi przykład szczególnie poważnej ingerencji, zarówno z punktu widzenia ochrony prawa do prywatności, jak i wolności słowa. Dlatego też może być stosowana jedynie wtedy, gdy uzasadniają ją wyjątkowe okoliczności.

Każda forma inwigilacji dziennikarzy budzi szczególne kontrowersje w świetle chroniącej tę grupę zawodową tajemnicy dziennikarskiej, w tym przede wszystkim ze względu na konieczność ochrony dziennikarskich źródeł informacji. Odnosi się to zarówno do inwigilacji, która ujawnia treść prowadzonej przez dziennikarzy komunikacji (np. podsłuchy), jak i pozyskiwania tzw. metadanych, które

[137] W. Osiatyński, *Prawa człowieka i ich granice*, Kraków 2011, s. 90-91.

– choć nie odnoszą się do treści komunikatów – często wystarczają do tego, aby zidentyfikować źródło informacji. Do takich metadanych należą np. billingi telefoniczne, dane dotyczące miejsca, z którego loguje się telefon komórkowy do stacji przekaźnikowej, czy te związane z aktywnością w internecie. Wszystkie te dane mogą prowadzić do ujawnienia tożsamości dziennikarskiego informatora, a ich pobieranie i analiza przez służby w celu identyfikacji źródła informacji może oznaczać obejście istniejących gwarancji wynikających z tajemnicy dziennikarskiej (zob. więcej pyt. 3-5).

Co więcej, działania zmierzające do ustalenia tożsamości źródeł dziennikarskich w sposób niezależny od dziennikarza (np. przez analizę dokumentów czy metadanych), są uznawane za środek znacznie bardziej drastyczny i groźny niż żądanie ujawnienia informatora mające miejsce podczas bezpośredniego przesłuchania. Z orzecznictwa ETPC (zob. sprawy *Roemen i Schmitt p. Luksemburgowi*[138] oraz *Ernst i Inni p. Belgii*[139]) wynika bowiem, że depozytariuszem tajemnicy podczas przesłuchania jest sam dziennikarz, który ma wówczas rzeczywistą kontrolę nad jej ujawnieniem. Tymczasem informator, wiedząc, że prawo zezwala na podjęcie wielu niezależnych od dziennikarza działań, które mogą doprowadzić do ujawnienia jego tożsamości, nie może polegać na zaufaniu do przedstawicieli mediów. Tym samym może nie być skłonny do przekazywania dziennikarzom ważnych informacji, utrudniając realizację przynależnej im funkcji kontrolnej. Łatwy dostęp organów państwowych do wszelkich środków inwigilacji, które mogą być podejmowane wobec dziennikarzy, stwarza zatem dla informatora, w kontekście jego poczucia bezpieczeństwa, znacznie groźniejszą sytuację – traci on pewność, że jego dane pozostaną pod ochroną tajemnicy dziennikarskiej.

W rekomendacji Komitetu Ministrów Rady Europy o prawie dziennikarzy do nieujawniania swoich źródeł informacji[140] podkreślono, że podsłuchy stosowane w stosunku do dziennikarzy lub ich przełożonych oraz wszelkie inne sposoby inwigilacji są niedopuszczalne, jeśli mają na celu obejście prawa do zachowania w tajemnicy tożsamości dziennikarskiego źródła informacji.

W świetle tej rekomendacji co do zasady, poza ściśle określonymi, wyjątkowymi przypadkami, niedopuszczalne

[138] Wyrok ETPC z dnia 25 lutego 2003 r. w sprawie *Roemen i Schmitt p. Luksemburgowi,* skarga nr 51772/99.

[139] Wyrok ETPC z dnia 15 lipca 2003 r. w sprawie *Ernst i inni p. Belgii*, skarga nr 33400/96.

[140] Rekomendacja Komitetu Ministrów Rady Europy R(2000)7 z dnia 8 marca 2000 r., https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM (dostęp: 10 marca 2016 r.).

będą więc jakiekolwiek działania służb wobec dziennikarzy nakierowane na identyfikację ich informatorów. Dotyczy to wszelkich form inwigilacji takich jak: stosowanie podsłuchu, analiza aktywności dziennikarza w internecie, analiza billingów, śledzenie dziennikarza czy wykorzystywanie monitoringu wizyjnego do ustalenia, z kim się spotyka.

Dziennikarz na celowniku CBA

Jedna z głośniejszych spraw dotyczących inwigilacji, w którą zaangażowana była HFPC, dotyczyła dziennikarza Bogdana Wróblewskiego. „Gazeta Wyborcza" opublikowała w 2010 r. artykuł[141], w którym ujawniła, że CBA bez żadnego konkretnego powodu monitorowało billingi 10 znanych dziennikarzy. Jeden z nich, B. Wróblewski, wystąpił przeciwko CBA z powództwem o ochronę dóbr osobistych.

Sąd Okręgowy w Warszawie uwzględnił powództwo dziennikarza i nakazał CBA opublikowanie przeprosin oraz zniszczenie wszystkich danych zgromadzonych w trakcie inwigilacji[142]. Sąd uznał, że pozyskiwanie przez służbę specjalną billingów dziennikarza, mimo – co do zasady – szerokich kompetencji w zakresie dostępu do danych telekomunikacyjnych, było bezprawne. W ocenie sądu stanowiło to naruszenie prawa do prywatności, tajemnicy komunikowania się oraz obejście gwarancji wynikających z tajemnicy dziennikarskiej, które naraziło powoda na utratę zaufania informatorów. W uzasadnieniu wyroku sąd wskazał:

„[W] niniejszej sprawie doszło do naruszenia dóbr osobistych powoda Bogdana Wróblewskiego przez organy władzy publicznej poprzez bezprawne pobieranie przez funkcjonariuszy CBA billingów rozmów z 2 telefonów, z których korzystał powód, a działanie to było bezprawne. [...] Przepis art. 18 ust. 1 ustawy o CBA [stanowiący podstawę sięgania przez CBA do danych telekomunikacyjnych – przyp. aut.] może być interpretowany tylko w taki sposób, w jaki będzie możliwe pogodzenie jego treści z podstawowymi wolnościami i prawami człowieka i obywatela – a więc w sposób ścieśniający. [...]

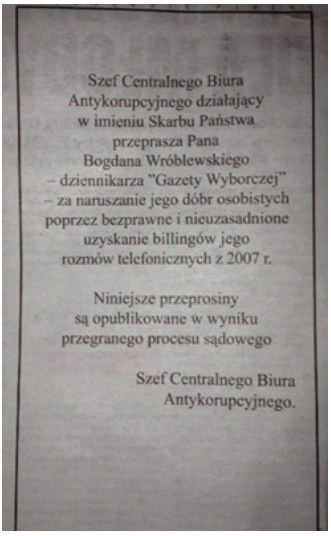
Podzielić należy stanowisko uczestniczącej w procesie Helsińskiej Fundacji Praw Człowieka, że CBA [...] sięgnęło po

[141] W. Czuchnowski, *Dziennikarze na celowniku...*, op. cit.

[142] Wyrok Sądu Okręgowego w Warszawie z dnia 26 kwietnia 2012 r., sygn. akt II C 626/11.

instrument prawny, który był dla CBA wygodny, ponieważ nie wymagał zwiększonego nakładu pracy funkcjonariuszy oraz był mało gwarancyjny dla osoby, której dotyczył, gdyż CBA w świetle ustawy o CBA nie miało obowiązku poinformowania powoda o podjętych działaniach, jak również nie miało obowiązku uzyskania zgody sądu".

Sąd Apelacyjny oddalił apelację CBA[143].


Szef Centralnego Biura
Antykorupcyjnego działający
w imieniu Skarbu Państwa
przeprasza Pana
Bogdana Wróblewskiego
– dziennikarza "Gazety Wyborczej"
– za naruszanie jego dóbr osobistych
poprzez bezprawne i nieuzasadnione
uzyskanie billingów jego
rozmów telefonicznych z 2007 r.

Niniejsze przeprosiny
są opublikowane w wyniku
przegranego procesu sądowego

Szef Centralnego Biura
Antykorupcyjnego.

Fot. 1. Przeprosiny Szefa CBA, które ukazały się w prasie 9 maja 2013 r. po wygranym procesie z powództwa red. Bogdana Wróblewskiego.

2. Czy sygnaliści ujawniający inwigilację obywateli, w tym grup chronionych takich jak dziennikarze, podlegają ochronie?

W ujawnieniu przypadków bezprawnej inwigilacji obywateli, ze względu na tajny charakter tych czynności, ważną rolę odgrywają media oraz sygnaliści, którzy mają dostęp do niejawnych informacji i nie chcą godzić się na nadużycia. Przykładem współpracy dziennikarzy i sygnalistów w tym zakresie jest chociażby przypadek Edwarda Snowdena, który nawiązał kontakt z dziennikarzami Laurą Poitras i Glennem Greenwaldem. Jak podkreślono w raporcie Agencji Praw Podstawowych, „dziennikarze i sygnaliści ujawniający informacje na temat tajnych działań służb, o których jednostki objęte inwigilacją nie są nigdy informowane, przyczyniają się istotnie do

[143] Wyrok Sądu Apelacyjnego w Warszawie z dnia 26 kwietnia 2013 r., sygn. akt I ACa 1002/12.

możliwości dochodzenia praw przez ofiary takich działań. Przykładem są działania Snowdena, które doprowadziły do wszczęcia postępowań sądowych zarówno na poziomie międzynarodowym, jak i krajowym". Agencja zwraca w tym kontekście uwagę, że media są ważnym elementem systemu nadzoru nad działaniami służb[144]. Na konieczność ochrony dziennikarzy i sygnalistów (m.in. jako dziennikarskich źródeł informacji) zwrócił także uwagę Parlament Europejski w rezolucji dotyczącej amerykańskich programów masowej inwigilacji[145].

Czy osoby ujawniające nadużycia służb mogą zatem uniknąć negatywnych konsekwencji upublicznienia tajnych informacji? Zgromadzenie Parlamentarne Rady Europy w jednej z rezolucji wezwało kraje członkowskie do zapewnienia ochrony sygnalistom, którzy demaskują przypadki stosowania bezprawnej inwigilacji[146]. Podobne stanowisko zajął w jednym z wyroków ETPC, który jednocześnie zwrócił uwagę na szczególne publiczne znaczenie ujawnienia informacji na temat inwigilowania takich grup jak dziennikarze[147].

Sygnalista, który ujawnił bezprawną inwigilację dziennikarzy

Constantin Bucur był pracownikiem jednej z rumuńskich służb specjalnych (SRI), w której zaobserwował nieprawidłowości w stosowaniu podsłuchów, m.in. wobec polityków oraz dziennikarzy. Powiadomił o tym szefa, który doradził mu, aby nie informował nikogo o swoich spostrzeżeniach. C. Bucur skontaktował się następnie z jednym z posłów zasiadających w komisji parlamentarnej kontrolującej służby. Ten odpowiedział jednak, że komisja nie będzie w stanie efektywnie zająć się sprawą. Ostatecznie funkcjonariusz, za radą posła, opowiedział o nieprawidłowościach podczas konferencji prasowej. Za ujawnienie tajnych informacji został skazany na 2 lata pozbawienia wolności z warunkowym zawieszeniem wykonania kary.

[144] Agencja Praw Podstawowych (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks*, Raport 2015, s. 31, 66.

[145] Rezolucja Parlamentu Europejskiego z 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188 (INI)).

[146] Resolution 2045 (2015) Mass surveillance z dnia 21 kwietnia 2015 r., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en (dostęp: 15 marca 2016 r.).

[147] Wyrok ETPC z dnia 8 stycznia 2013 r. w sprawie *Bucur i Toma p. Rumunii*, skarga nr 40238/02.

Europejski Trybunał Praw Człowieka stwierdził w tej sprawie naruszenie art. 10 Konwencji (wolność słowa)[148]. Trybunał stwierdził, że w świetle kryteriów wypracowanych we wcześniejszym orzecznictwie (zob. rozdział I) C. Bucura należało uznać za sygnalistę, który zasługiwał na ochronę. Trybunał przyznał też, że skarżący działał w dobrej wierze i w interesie publicznym oraz najpierw wykorzystał wszystkie inne, mniej inwazyjne metody zwrócenia uwagi na problem. ETPC podkreślił także wyjątkowo istotne dla debaty publicznej znaczenie ujawnionych nieprawidłowości (tj. bezprawnego podsłuchiwania dziennikarzy i polityków).

Skarżącymi w sprawie byli również dziennikarz Micea Toma oraz jego córka, należący do osób, w stosunku do których stosowano podsłuchy ujawnione przez C. Bucura. Trybunał uznał, że w ich przypadku doszło do naruszenia prawa do prywatności (gwarantowanego art. 8 EKPC) ze względu na brak odpowiednich regulacji krajowych chroniących przed nielegalną inwigilacją i gwarantujących bezpieczeństwo danych pozyskanych w trakcie procedur inwigilacyjnych.

3. Na czym może polegać inwigilacja?

Podsłuch procesowy

W polskim prawie głównym przepisem regulującym stosowanie podsłuchów jest art. 237 k.p.k., zgodnie z którym „po wszczęciu postępowania sąd na wniosek prokuratora może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych". Jest to tzw. podsłuch procesowy, który może zostać wykorzystany dopiero po formalnym wszczęciu postępowania karnego. Przepis doprecyzowuje dalej, że utrwalenie rozmów może nastąpić jedynie w celu uzyskania bądź zabezpieczenia dowodów lub by zapobiec popełnieniu kolejnego ciężkiego przestępstwa. W art. 237 k.p.k. przewidziano również, że w przypadku niecierpiącym zwłoki o zastosowaniu podsłuchu może zadecydować sam prokurator. Jednakże następnie w ciągu 3 dni będzie musiał się zwrócić do sądu z wnioskiem o zatwierdzenie jego postanowienia. Jeżeli sąd stwierdzi, że utrwalanie i kontrolowanie rozmów było nieuzasadnione, nakaże zniszczenie wszystkich zapisów. Warte podkreślenia jest również to, że stosowanie podsłuchu procesowego możliwe jest jedynie przez 3 miesiące z możliwością jednokrotnego przedłużenia o kolejny okres 3 miesięcy.

[148] Ibidem.

Kontrola operacyjna

Polskie prawo przewiduje ponadto, że dostęp do rozmów telefonicznych (stosowanie podsłuchów) lub do innych form komunikacji nastąpić może na gruncie tzw. kontroli operacyjnej, która może być wszczęta jeszcze przed formalnym rozpoczęciem postępowania karnego. Jej stosowanie regulowane jest przez ustawę o Policji, a także ustawy regulujące działanie innych uprawnionych służb, takich jak np. Centralne Biuro Antykorupcyjne czy Agencja Bezpieczeństwa Wewnętrznego. Zgodnie z ustawą z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw[149], kontrola operacyjna regulowana jest analogicznie w stosunku do każdej ze służb i polega na „1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; 2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; 3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; 4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; 5) uzyskiwaniu dostępu i kontroli zawartości przesyłek". Kontrola operacyjna może zostać podjęta jedynie wtedy, gdy inne środki okażą się nieskuteczne i tylko w celu ustalenia lub powstrzymania sprawców określonych w przepisach umyślnych przestępstw ściganych z oskarżenia publicznego albo w celu zyskania lub utrwalenia dowodów. Zarządza ją sąd okręgowy na wniosek szefów służb lub komendantów i po uzyskaniu pisemnej zgody odpowiedniego prokuratora. W wypadkach niecierpiących zwłoki kontrolę operacyjną mogą zarządzić samodzielnie szefowie służb lub komendanci. W takiej sytuacji wymagana jest jednak następcza zgoda sądu. W przypadku gdyby sąd nie wydał takiej zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, szefowie służb lub komendanci powinni wstrzymać wszelkie podjęte czynności i zniszczyć zebrane materiały. Kontrola operacyjna może trwać 6 miesięcy, przy czym istnieje możliwość jednokrotnego przedłużenia jej o kolejne 12 miesięcy.

Podsłuchiwanie dziennikarzy naruszeniem praw człowieka

Dziennikarze opublikowali artykuł na temat nieprawidłowości w jednej z holenderskich służb specjalnych. Następnie, prowadząc dziennikarskie śledztwo, odkryli, że ich telefony były podsłuchiwane, a oni sami obserwowani przez służby. Europejski Trybunał Praw Człowieka stwierdził naruszenie wolności słowa (art. 10 europejskiej Konwencji

[149] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji..., op. cit.

o ochronie praw człowieka i podstawowych wolności) oraz prawa do prywatności (art. 8). Trybunał uzasadnił wyrok tym, że działania służb zostały podjęte w celu poznania dziennikarskiego źródła informacji. Ponadto holenderskie prawo nie zapewniało odpowiednich gwarancji proceduralnych przed stosowaniem arbitralnej inwigilacji przez służby[150].

Dostęp do danych telekomunikacyjnych, pocztowych i internetowych

Sąd i prokuratura (w postępowaniu karnym) oraz służby policyjne i specjalne (w ramach tzw. czynności operacyjno-rozpoznawczych prowadzonych przed wszczęciem postępowania karnego) mogą pozyskiwać tzw. metadane dotyczące komunikacji telefonicznej lub internetowej. Przypomnijmy, że są to dane, które odnoszą się do faktu komunikacji, choć nie ujawniają bezpośrednio jej treści. Jednak zestawione ze sobą, a zwłaszcza monitorowane przez dłuższy czas mogą dostarczyć wielu informacji na temat różnych aspektów życia osoby, której dotyczą. Jak pisze J. Podkowik, „korzystanie z telefonu, internetu i innych źródeł przekazywania bądź przetwarzania informacji pozostawia w wirtualnej przestrzeni autonomiczny znak, niczym odcisk linii papilarnych. Analiza takich metadanych generalnie pozwala doprowadzić do wykrycia tego, kto wytworzył dany plik i jakie osoby komunikowały się ze sobą"[151].

Do danych telekomunikacyjnych należą – jak już wspomniano – m.in. billingi rozmów telefonicznych oraz dane o miejscu logowania telefonów komórkowych. Zgodnie z prawem telekomunikacyjnym operatorzy telekomunikacyjni są zobowiązani przechowywać te dane przez okres 12 miesięcy i udostępniać je uprawnionym służbom (art. 180a ustawy – Prawo telekomunikacyjne[152]). W postępowaniu karnym dostęp do tych danych reguluje art. 218 § 1 k.p.k. W przypadku policji i służb specjalnych dostęp do danych w ramach czynności operacyjno-rozpoznawczych odpowiednie regulacje zawarte są w poszczególnych ustawach kompetencyjnych. Nowelizacja ustawy o Policji i innych ustaw z 15 stycznia 2016 r. uregulowała dodatkowo, na podobnych zasadach, kwestię dostępu

[150] Wyrok ETPC z dnia 22 listopada 2012 r. w sprawie *Telegraaf Media Nederland Landelijke Media B.V. i inni p. Holandii*, skarga nr 39315/06.

[151] J. Podkowik, *Ochrona dziennikarskich źródeł informacji w dobie cyfrowej w świetle Konwencji o ochronie praw człowieka i podstawowych wolności oraz Konstytucji RP*, „Przegląd Sejmowy" 2015, nr 3(128), s. 76.

[152] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243 j.t.).

służb do tzw. danych internetowych[153] (np. numer IP, historia odwiedzanych stron internetowych, wyszukiwane hasła i inne dane dotyczące aktywności w internecie) oraz danych pocztowych.

Zgodnie z orzecznictwem Trybunału Konstytucyjnego ochrona prawa do prywatności obejmuje „wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI”[154].

Zbadanie billingów telefonicznych oraz innych danych o połączeniach telefonicznych lub korzystaniu z internetu dotyczących przedstawicieli mediów wzbudza poważne wątpliwości w kontekście zgodności z gwarancjami ochrony dziennikarskich źródeł informacji. Podjęte czynności pozwalają bowiem na zweryfikowanie kręgu rozmówców dziennikarza i w konsekwencji wytypowanie dziennikarskiego informatora. Zdaniem niektórych przedstawicieli doktryny prawniczej wyciąg z billingów udostępniany przez operatorów telekomunikacyjnych należy traktować jako dokument zawierający tajemnicę dziennikarską. Dla oceny bezprawności ingerencji w dziennikarskie źródła informacji nie ma więc znaczenia fakt, że żądanie przekazania wykazu połączeń nie dotyczy bezpośrednio dziennikarza, ale operatora telekomunikacyjnego, który jest „wytwórcą” dokumentu zawierającego te chronione dane[155]. Wyroki sądów także potwierdziły, że pozyskiwanie danych telekomunikacyjnych dziennikarzy może naruszać gwarancje wynikające z tajemnicy dziennikarskiej (zob. wyżej sprawę Bogdana Wróblewskiego oraz sprawę dziennikarzy opisaną w odpowiedzi na pyt. 5).

[153] Ogólna podstawa prawna dostępu do tych danych zawarta jest w art. 18 ust. 6 Ustawy o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422 j.t. ze zm.).

[154] Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11.

[155] A. Bojańczyk, *Billingi jednak na specjalnych prawach*, „Rzeczpospolita”, 1 grudnia 2005 r. Więcej na temat dostępu służb do billingów dziennikarzy w kontekście tajemnicy dziennikarskiej zob. M. Zaremba, *Jeszcze jeden głos w sprawie prawnej ochrony tajemnicy billingów dziennikarzy*, obserwatorium.org., 9 maja 2012 r. http://www.obserwatorium.org/images/billingi%20artykul_M_Zaremba.pdf (dostęp: 15 marca 2016 r.).

HFPC krytycznie o nowej ustawie o Policji

Zasady prowadzenia kontroli operacyjnej oraz zasady dostępu do danych telekomunikacyjnych, pocztowych i internetowych przez służby policyjne i specjalne w formie nadanej jej przez ustawę z 15 stycznia 2016 r. o zmianie ustawy o Policji i innych ustaw spotkały się z krytyką wielu środowisk. Krytyczną opinię przedstawiła także HFPC[156]. Przyjęta nowelizacja, zdaniem HFPC, nie realizuje wytycznych zawartych w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11), w którym zakwestionowano część wcześniej obowiązujących regulacji w tym zakresie. Nowelizacja nie odpowiada również zaleceniom wynikających z wyroku Trybunału Sprawiedliwości Unii Europejskiej w tzw. sprawie *Digital Rights Ireland*, w którym unieważniono unijną dyrektywę dotyczącą dostępu służb do danych telekomunikacyjnych[157].

Sprzeciw budzi m.in. brak zapewnienia w nowej ustawie systemu niezależnej kontroli nad działaniami służb, włączenie do przyjętych regulacji dostępu do danych internetowych i brak zapewnienia odpowiedniej ochrony tajemnic zawodowych (w tym tajemnicy dziennikarskiej). **W przypadku dostępu służb do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego, których dotyczy tajemnica zawodowa, Trybunał Konstytucyjny uznał m.in., że może być to jeden z obszarów, w których należałoby rozważyć stosowanie uprzedniej kontroli sądu nad pozyskiwaniem danych** (oznaczałoby to wyrażenie zgody przez sąd przed zarządzeniem inwigilacji). Ustawodawca dotychczas nie wprowadził jednak takiego rozwiązania. Nowe przepisy zostały zaskarżone przez Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego[158].

Ataki hakerskie

Kolejnym zagrożeniem dla dziennikarzy są ataki hakerskie, których celem mogą być np. komputery należące do dziennikarzy lub strony

[156] Uwagi HFPC do projektu zmian w uprawnieniach służb, http://www.hfhr.pl/uwagi-hfpc-do-projektu-zmian-w-uprawnieniach-sluzb/ (dostęp: 15 marca 2016 r.).

[157] Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r. w sprawie *Digital Rights Ireland Ltd p. Minister for Communications, Marine and Natural Resources i inni oraz Kärntner Landesregierung i inni*, sygn. akt C-293/12

[158] Wniosek RPO do Trybunału Konstytucyjnego z dnia 18 lutego 2016 r., https://www.rpo.gov.pl/sites/default/files/Wniosek_do_TK_kontrola_operacyjna.pdf (dostęp: 15 marca 2016 r.).

internetowe mediów. W 2014 r. głośny był przypadek ataków na systemy komputerowe dużych tytułów prasowych, takich jak „Forbes", „Financial Times" czy też „New York Times". Miały one zostać przeprowadzone przez hakerów działających wprost na zlecenie rządu lub też wspieranych przez rząd[159]. Możliwość zgodnego z prawem korzystania z narzędzi hakerskich przez polskie służby (np. w ramach kontroli operacyjnej) wzbudza duże wątpliwości. Trudno jest też uzyskać informacje na temat faktycznego stosowania tego rodzaju środków.

Złośliwe oprogramowanie w służbie państwu?

Jednym z narzędzi, które może być wykorzystywane przez organy państwa do inwigilowania obywateli, jest tzw. RCS (Remote Control System – system zdalnego zarządzania). Jest to złośliwe oprogramowanie pozwalające na monitorowanie komputerów i telefonów, a także pozyskiwanie danych przechowywanych na tych urządzeniach. RCS sprzedawany jest przez włoską firmę Hacking Team. Na początku 2014 r. naukowcy z Uniwersytetu w Toronto opublikowali raport, w którym przedstawili listę klientów przedsiębiorstwa. Wśród nich znalazły się m.in. instytucje publiczne ze Stanów Zjednoczonych, Wielkiej Brytanii, Kazachstanu, Rosji, a także Polski.

W związku z tymi doniesieniami HFPC postanowiła wystąpić do ABW i CBA z wnioskiem o informacje, czy polskie służby korzystają z RCS. ABW w odpowiedzi stwierdziło, że nie posługuje się tym oprogramowaniem. CBA odmówiło natomiast udzielenia jakiejkolwiek informacji, powołując się na tajemnicę prawnie chronioną. W konsekwencji Fundacja złożyła skargę do Wojewódzkiego Sądu Administracyjnego na tę decyzję. Sąd skargę jednak oddalił. Jak wyjaśnił w uzasadnieniu, w tej sprawie zachodził konflikt między prawem do prywatności i bezpieczeństwem państwa, a CBA w obliczu zagrożenia cyberprzestępczością ma prawo nie udostępniać informacji o stosowanych przez nią technikach[160]. HFPC wniosła następnie skargę do Naczelnego Sądu Administracyjnego, która oczekuje na rozpoznanie.

[159] J. Wagstaff, *Journalists, media under attack from hackers: Google researchers,* reuters.pl, 28 marca 2014 r., http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328 (dostęp: 15 marca 2016 r.).

[160] Sąd oddalił skargę HFPC dot. udostępnienia informacji o programie umożliwiającym monitorowanie komputerów, 13 lutego 2015 r., http://www.hfhr.pl/sad-oddalil-skarge-hfpc-dot-udostepnienia-informacji-o-programie-umozliwiajacym-monitorowanie-komputerow/ (dostęp: 15 marca 2016 r.).

Inwigilacja i korzystanie z narzędzi hakerskich przez organy państwa to nie jedyne niebezpieczeństwo, na które narażeni są dziennikarze w sieci. W równym stopniu niebezpieczne okazać się mogą ataki hakerskie, których sprawcą są podmioty prywatne. Motywy takich sprawców mogą być zupełnie przyziemne i niekoniecznie ataki muszą brać za cel jedynie duże gazety, ale również mniejsze redakcje. Nietrudno wyobrazić sobie sytuację, gdy atakujący będzie próbował wykraść poufne informacje, by następnie użyć je do szantażu.

Jak cyberprzestępcy mogą wykraść nasze dane?

Cyberprzestępcy, chcąc uzyskać dostęp do poufnych danych, bardzo często posługują się technikami inżynierii społecznej, wychodząc z założenia, że człowiek stanowi najsłabszy element systemu zabezpieczeń.

Przykładowo: dziennikarz może otrzymać e-mail od pozornie wiarygodnej osoby, która będzie chciała ujawnić istotne z punktu widzenia opinii społecznej informacje, i na potwierdzenie załącza plik o nazwie „dokumenty". Jednakże w momencie, gdy dziennikarz otworzy załączniki, jego komputer zostaje zainfekowany. Ofiarami ataków mogą również paść dziennikarscy informatorzy. W takim przypadku hakerzy zazwyczaj będą próbowali podszywać się pod dziennikarzy, próbując w ten sposób przekonać ich do wyjawienia wrażliwych informacji[161]. Niezmiernie istotne jest, by za każdym razem starać się weryfikować tożsamość osoby, która próbuje się z nami skontaktować, i nie otwierać przesyłanego w e-mailu załącznika, ponieważ istnieje niebezpieczeństwo, że może on zawierać wirusy.

Zablokowanie strony internetowej gazety

W Polsce jednym z głośnych ostatnio cyberataków na redakcję gazety był atak na stronę tygodnika „wSieci". Przeprowadziła go grupa określająca się jako Cyber Justice Team. Na ich oficjalnym profilu na Twitterze można wyczytać, że są aktywistami walczącymi z niesprawiedliwością. Powodem ataku była okładka papierowego wydania tygodnika przedstawiająca kobietę szarpaną przez ciemnoskórych mężczyzn. Obrazowi towarzyszył tytuł: „Islamski gwałt na Europie". Przedstawiciele Cyber Justice

[161] D. Krivokapić, V. Joler (red.), *Guide to online media autonomy: security risks and protection mechanisms. Walking on the digital age, Share Foundation*, 2015, http://www.shareconference.net/sites/default/files/u742/vodic_walking_eng_web.pdf, s. 26 (dostęp: 15 marca 2016 r.).

Team uznali to za przejaw ksenofobicznej propagandy i doprowadzili do unieruchomienia strony gazety na kilka dni. Prawdopodobnie zastosowali tzw. atak DDoS (ang. *Distributed Denial of Service* – rozproszona odmowa usługi), który polega na obciążeniu strony tak dużą liczbą zapytań, że przestaje ona w konsekwencji działać[162].

Inne środki techniczne

Należy pamiętać, że rozwój technologiczny umożliwia stosowanie coraz nowszych środków technicznych podczas czynności operacyjnych prowadzonych przez służby państwa. Jak wskazano wyżej na przykładzie RCS, katalog narzędzi, które mogą być używane, nie jest jasno określony w przepisach, a informacja na ten temat nie jest udostępniana przez służby. Narzędzia te mogą obejmować także np. użycie monitoringu wizyjnego, dronów czy GPS[163].

4. Czy prawo chroni dziennikarzy i ich źródła przed inwigilacją?

Polski porządek prawny nie przewiduje w pełni efektywnych mechanizmów, które chroniłyby dziennikarzy i ich źródła przed inwigilacją. Omówione w rozdziale II regulacje dotyczące tajemnicy dziennikarskiej sprawdzają się przede wszystkim w ramach postępowania karnego. Jednak w przypadku działań podejmowanych przez organy państwa w ramach czynności operacyjno-rozpoznawczych możliwości stosowania różnych technik inwigilacyjnych, które daje nowoczesna technologia, wymykają się obecnym ramom prawnym. Sami dziennikarze przyznają, że możliwości ochrony informatorów znacznie zmalały w obliczu rozwoju technicznych środków inwigilacji[164].

Dopiero wspomniana wyżej niedawna nowelizacja ustawy o Policji i innych ustaw wprowadziła pewne regulacje dotyczące tajemnicy dziennikarskiej (i innych tajemnic zawodowych) podczas stosowania kontroli operacyjnej[165]. W przypadku m.in. tajemnicy

[162] *Strona „W Sieci" nie działa. Zaatakowana przez hakerów za „nazistowską antymuzułmańską" okładkę*, gazeta.pl, 21 lutego 2016 r. http://wiadomosci.gazeta.pl/wiadomosci/1,114871,19659427,tango-down-strona-w-sieci-zaatakowana-przez-hakerow.html (dostęp: 10 marca 2016 r.).

[163] Zob. informację na temat prowadzonego przez HFPC postępowania ws. stosowania GPS przez policję: http://www.hfhrpol.waw.pl/precedens/aktualnosci/komendant-glowny-policji-ma-udostepnic-informacje-o-gps.html (dostęp: 15 marca 2016 r.).

[164] J. Posetti, *Protecting journalism...*, op. cit.

[165] Zob. np. art. 19 ust. 15 f-j Ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 1990 r. Nr 30 poz. 179).

dziennikarskiej nowe przepisy nakazują następczą weryfikację materiałów zgromadzonych w ramach takiej kontroli oraz ustanawiają wymóg uzyskania zgody sądu na dopuszczanie ich do wykorzystania w późniejszym postępowaniu. Nowe regulacje określają również postępowanie z materiałami w sytuacji, gdy tajemnicy nie uchylono. Zgodnie z tymi przepisami komendant główny policji, komendant CBŚ, komendant wojewódzki policji, a także szefowie innych uprawnionych służb mają obowiązek przekazać prokuratorowi materiały zebrane w toku kontroli operacyjnej, jeśli mogą one zawierać m.in. tajemnice dziennikarską. Prokurator przekazuje je następnie niezwłocznie do sądu, który zarządził kontrolę operacyjną lub wyraził na nią zgodę. Sąd wydaje wówczas niezwłocznie postanowienie o dopuszczeniu tych materiałów do wykorzystania w postępowaniu karnym, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a dana okoliczność nie może być ustalona na podstawie innego dowodu. Sąd zarządza także niezwłoczne zniszczenie materiałów, których wykorzystanie w postępowaniu karnym jest niedopuszczalne. Dopuszczony materiał nie może być jednak objęty zakazem dowodowym określonym w art. 180 § 3 k.p.k. (tj. m.in. zawierać informacje mogące identyfikować dziennikarskiego informatora), za wyjątkiem sytuacji, gdy dotyczy jednego z najpoważniejszych przestępstw z art. 240 k.k. Na postanowienie sądu w przedmiocie dopuszczenia do wykorzystania w postępowaniu karnym ww. materiałów przysługuje zażalenie tylko prokuratorowi (przyjęta regulacja nie przewiduje możliwości złożenia takiego zażalenia przez dziennikarza). Należy jednocześnie zaznaczyć, że wprowadzone rozwiązanie zostało uznane przez środowiska dziennikarskie, pozarządowe i Rzecznika Praw Obywatelskich za niedostatecznie chroniące tajemnicę dziennikarską[166].

Jak wskazano wyżej (zob. pyt. 3 – „HFPC krytycznie o nowej ustawie o Policji"), wbrew zaleceniom Trybunału Konstytucyjnego nowelizacja nie wprowadziła szczególnych gwarancji dla ochrony tajemnicy dziennikarskiej w kontekście dostępu uprawnionych służb do danych telekomunikacyjnych, internetowych czy pocztowych, uzyskanego w ramach czynności operacyjno-rozpoznawczych.

Pomimo niewprowadzenia szczegółowych rozwiązań prawnych zapewniających w pełni efektywną ochronę tajemnicy dziennikarskiej w toku czynności operacyjno-

[166] Zob. Uwagi HFPC do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154), 30 grudnia 2015 r., http://www.hfhr.pl/wp-content/uploads/2015/12/HFPC_opinia_ustawa_o_policji_30122015.pdf; opinia Izby Wydawców prasy w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy nr 154), 26 stycznia 2016 r., http://www.senat.gov.pl/gfx/senat/userfiles/_public/k9/dokumenty/konsultacje_ustawy/071/071_iwp.pdf (dostęp: 15 marca 2016 r.), a także wniosek RPO do Trybunału Konstytucyjnego, op. cit.

-rozpoznawczych, należy jednak podkreślić, że wszystkie organy państwa mają obowiązek respektować zakres i granice tej tajemnicy określone w art. 15-16 prawa prasowego. Niedopuszczalne jest zatem podejmowanie jakichkolwiek działań przez służby policyjne i specjalne, które byłyby nakierowane na obejście gwarancji wynikających z tych przepisów, zwłaszcza w odniesieniu do najsilniej chronionych elementów tajemnicy dziennikarskiej, tj. działań zmierzających m.in. do nieuprawnionej identyfikacji dziennikarskich źródeł informacji. Dopuszczalność inwigilacji dziennikarzy w związku z ich działalnością zawodową jest więc znacznie bardziej ograniczona niż inwigilacja osób niewykonujących tego zawodu.

Niżej (pyt. 7) przedstawiamy też kilka praktycznych porad, dzięki którym dziennikarze mogą zmniejszyć ryzyko ingerencji w ich tajemnicę zawodową.

5. Jak dziennikarze mogą dochodzić swoich praw w przypadku nieuzasadnionej inwigilacji?

Gdy dziennikarz dowiaduje się, że prowadzono wobec niego nieuzasadnioną inwigilację, może skorzystać z różnych narzędzi prawnych, aby dochodzić swoich praw. Możliwości te zależą od szczegółowych okoliczności sprawy, a także od tego, czy inwigilacja była prowadzona w ramach postępowania karnego, czy też w ramach czynności operacyjno-rozpoznawczych. W tym drugim przypadku podstawowym problemem z dochodzeniem praw jest to, że osoby, wobec których prowadzona jest inwigilacja, nie są o tym nigdy oficjalnie informowane.

Jeśli skorzystano z tzw. podsłuchu procesowego lub doszło do pozyskiwania przez organy ścigania danych telekomunikacyjnych w ramach postępowania karnego, należy doręczyć osobie zainteresowanej postanowienie o zastosowaniu tego środka, które podlega zaskarżeniu przed sądem (art. 218 i art. 239 k.p.k.). Chociaż doręczenie takiego postanowienia może zostać odroczone nawet do czasu zakończenia postępowania, to jednak ostatecznie osoba, której dotyczyła inwigilacja, dowie się o tym i składając zażalenie na postanowienie, będzie mogła zakwestionować zasadność działań służb przed sądem. Nawet jeśli do takiej kontroli dojdzie ex post, to istniejący w prawie obowiązek notyfikacji faktu stosowania inwigilacji może powodować, że uprawnione służby będą sięgały po tego rodzaju narzędzia z większą ostrożnością. Ponadto, jeśli sąd, rozpoznając zażalenie, stwierdzi, że inwigilację prowadzono z naruszeniem prawa, takie orzeczenie może pomóc w późniejszym

dochodzeniu praw przez dziennikarza, np. w procesie cywilnym o ochronę dóbr osobistych (zob. niżej).

Postanowienie o pobraniu danych telekomunikacyjnych dziennikarzy pod kontrolą sądu

Pod koniec 2011 r. media ujawniły, że Wojskowa Prokuratura Garnizonowa w Poznaniu zażądała udostępnienia danych telekomunikacyjnych (obejmujących okres od 30 kwietnia do 15 listopada 2010 r.) trojga dziennikarzy ogólnopolskich mediów badających sprawę tzw. katastrofy smoleńskiej. Dodatkowo prokuratura żądała od operatorów usług telefonicznych przekazania treści wiadomości tekstowych z inwigilowanych telefonów (to żądanie nie zostało zrealizowane). Billingi dziennikarzy zostały pobrane w ramach postępowania w sprawie przecieków ze śledztwa dotyczącego katastrofy smoleńskiej (do prasy przedostały się z niego tajne informacje). Dwóch dziennikarzy złożyło post factum zażalenie na postanowienie prokuratury o pobraniu billingów.

Sąd Rejonowy dla Warszawy-Mokotowa uwzględnił zażalenia dziennikarzy i uchylił postanowienia prokuratorskie[167]. Sąd stwierdził, że żądanie udostępnienia danych telekomunikacyjnych dziennikarzy stanowiło w tym przypadku obejście gwarancji wynikających z tajemnicy dziennikarskiej i nie mieściło się w związku z tym w granicach prawa. Sąd uznał, że „żądanie przez autora zaskarżonego postanowienia od operatora sieci telefonii mobilnej wydania billingów, które miałyby prowadzić do identyfikacji dziennikarskich informatorów […], byłoby prawnie niedopuszczalne, a to z tej racji, że billingi telefonu dziennikarza zawierające dane umożliwiające identyfikację jego informatorów (tajemnicę dziennikarską) pozostają pod całkowitą ochroną art. 226 k.p.k. i nie mogą być wykorzystane w postępowaniu karnym".

Prawo nie przewiduje jednak obowiązku poinformowania osoby, wobec której stosowano inwigilację, gdy działo się to w ramach czynności operacyjno-rozpoznawczych (tj. w ramach kontroli operacyjnej lub dostępu do danych telekomunikacyjnych, internetowych, pocztowych). Oznacza to, że osoba, której np. telefon podsłuchiwano lub monitorowano jej billingi, co do zasady się o tym nie dowie, chyba że następnie materiały te zostaną wykorzystane w postępowaniu karnym. Jednostka nie otrzymuje więc żadnego postanowienia o zastosowaniu tych środków i w związku z tym nie ma możliwości zakwestionować zasadności ich użycia.

[167] Postanowienia Sądu Rejonowego dla Warszawy-Mokotowa z dnia 19 marca 2012 r., sygn. akt XIV Kp 498/12 i XIV Kp 497/12.

Do dziś nie zostało wykonane postanowienie sygnalizacyjne Trybunału Konstytucyjnego z 25 stycznia 2006 r. (sygn. akt S 2/06), w którym Trybunał zwrócił ustawodawcy uwagę na konieczność zagwarantowania ochrony konstytucyjnych praw osób poddanych kontroli operacyjnej. Ma to polegać na wprowadzeniu obowiązku informowania osób, wobec których prowadzono kontrolę operacyjną i następnie ją zakończono, o samym fakcie pozyskania danych. Na potrzebę wprowadzenia takiego mechanizmu i wykonania wspomnianego postanowienia sygnalizacyjnego Trybunał zwrócił też uwagę w wyroku z 30 lipca 2014 r. (sygn. akt K 23/11).

Jeśli dziennikarz podejrzewa bądź dowie się w jakiś sposób (np. w wyniku śledztwa dziennikarskiego lub na skutek działań sygnalisty, który ujawni mu taką informację) o tym, że prowadzono wobec niego nieuzasadnioną inwigilację, niezależnie od tego, czy działo się to w ramach postępowania karnego, czy czynności operacyjno-rozpoznawczych, może wystąpić z powództwem o ochronę dóbr osobistych przeciwko służbie odpowiedzialnej za podjęte działania (art. 23-24 k.c.). W takim powództwie można wskazywać zarówno na naruszenie prawa do prywatności, jak i gwarancji wynikających z tajemnicy dziennikarskiej (zob. opisana wyżej wygrana sprawa red. B. Wróblewskiego). W ramach takiego postępowania można domagać się wszelkich środków służących naprawieniu naruszenia prawa, np. przeprosin, a nawet zadośćuczynienia za krzywdę (art. 448 k.c.).

W przypadku stosowania nieuzasadnionej inwigilacji dziennikarz może także złożyć na policji lub w prokuraturze zawiadomienie o podejrzeniu popełnienia przestępstwa, polegającego na przekroczeniu uprawnień przez funkcjonariuszy odpowiedzialnych za podjęte działania, aby w ten sposób pociągnąć ich do odpowiedzialności karnej (art. 231 k.k.).

W sprawie *Zakharov p. Rosji*[168] Wielka Izba Europejskiego Trybunału Praw Człowieka stwierdziła naruszenie prawa do prywatności (art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności) w związku z obowiązującym w Rosji system niejawnego kontrolowania rozmów przeprowadzanych za pomocą telefonów komórkowych. Co interesujące, sam skarżący nie wykazał, aby jego rozmowy były przedmiotem inwigilacji przez służby. Wielka Izba doszła jednak do wniosku, że o naruszeniu Konwencji przesądziła analiza rosyjskiego prawa,

[168] Wyrok ETPC z dnia 4 grudnia 2015 r. w sprawie *Zakharov p. Rosji*, skarga nr 47143/06.

które nie stwarzało odpowiednich gwarancji zabezpieczających przed arbitralnym wykorzystywaniem uprawnień przez służb. W szczególności zauważono, że rosyjski system nie przewidywał obowiązku jakiejkolwiek notyfikacji osób poddanych inwigilacji ani nie wprowadzał efektywnych środków w celu zakwestionowania zasadności tych działań. W tej sytuacji Wielka Izba uznała, że nie można oczekiwać od skarżącego przestawienia dowodu, że stał się on ofiarą inwigilacji. Wystarczy sama przynależność do grupy osób, wobec której zgodnie z regulacjami krajowymi dozwolone jest stosowanie podsłuchów, a także brak realnej możliwości dochodzenia praw w razie ich bezprawnego użycia. Podobne stanowisko ETPC zajął w wyroku *Szabó i Vissy p. Węgrom*[169].

6. Jak chronić informacje? Praktyczne narzędzia

W obliczu braku wystarczających gwarancji dla ochrony dziennikarskich źródeł informacji w przepisach regulujących czynności operacyjno-rozpoznawcze istotne staje się podnoszenie świadomości dziennikarzy o działaniach, jakie mogą podjąć, aby minimalizować ryzyko ingerencji w tajemnicę zawodową. **W świecie cyfrowym korzystanie z narzędzi podnoszących bezpieczeństwo komunikacji w sieci oraz bezpieczeństwo przechowywanych dokumentów w wersji elektronicznej powinno być elementem etyki zawodowej dziennikarzy. Powinno być także traktowane jako element prawnego obowiązku ochrony źródeł informacji**. Jak wspomniano wcześniej, jednym z rozwiązań jest ograniczenie korzystania z niektórych narzędzi internetowych (np. takich, które umożliwiają przechowywanie poufnych danych w tzw. chmurze) na rzecz rozwiązań bardziej tradycyjnych. Jak pisze J. Podkowik, „jeśli dziennikarz korzysta z łączności telefonicznej lub internetu albo też przetwarza dane elektroniczne, to zakres przysługującej ochrony jest znacząco mniejszy, niż gdy kontaktuje się z informatorem osobiście lub gdy nie używa nowoczesnych technik przetwarzania danych”[170].

Istnieją ponadto techniczne możliwości pozwalające zwiększyć bezpieczeństwo posiadanych informacji i prowadzonej komunikacji w świecie nowych technologii. Poniżej zamieściliśmy kilka praktycznych porad, które mogą okazać się przydatne zarówno dla dziennikarzy, jak i sygnalistów. Należy mieć jednak na uwadze, że są to jedynie podstawowe wskazówki, które nie dają stuprocentowej

[169] Wyrok ETPC z dnia 12 stycznia 2016 r. w sprawie *Szabó i Vissy p. Węgrom*, skarga nr 37138/14.

[170] J. Podkowik, *Ochrona dziennikarskich…*, op. cit., s. 183.

gwarancji anonimowości. Osoby zainteresowane pogłębieniem swojej wiedzy w tej dziedzinie zachęcamy do zapoznania się z licznymi publikacjami dostępnymi w internecie (przykładowe pozycje znajdują się końcu rozdziału).

Jak dziennikarz może narazić swojego informatora na zdemaskowanie?

Z dziennikarzem skontaktował się mężczyzna, który przedstawił się jako pracownik jednej z dużych spółek Skarbu Państwa. Poinformował dziennikarza, że może mu udostępnić poufne dokumenty świadczące o poważnych nieprawidłowościach w spółce. Dziennikarz zaproponował mężczyźnie spotkanie w godzinach pracy w restauracji położonej niedaleko miejsca pracy informatora. W tym samym miejscu spotykali się następnie kilkukrotnie, nie wyłączając przy tym telefonów komórkowych (co oznaczało, że ich telefony wiele razy logowały się w tym samym momencie do tej samej stacji przekaźnikowej). Dla potrzeb uzupełnienia informacji uzyskanych w trakcie spotkań, dziennikarz pisał wiadomości do informatora na jego służbowy adres e-mail. Żaden z mężczyzn nie korzystał z programów szyfrujących pocztę elektroniczną. Do swojej skrzynki e-mail dziennikarz logował się, stosując hasło „12345" (hasłem tym dziennikarz posługiwał się także, korzystając z innych usług internetowych). Dziennikarz, próbując dowiedzieć się czegoś więcej o swoim informatorze, wyszukiwał ponadto informacje na jego temat w internecie, korzystając z nieszyfrowanego połączenia.

Takie zachowanie dziennikarza powodowało, że pozostawiał on wiele „śladów", które mogły znacząco ułatwić powiązanie z nim pracownika spółki, który przekazał mu poufne materiały. Po ukazaniu się artykułu zawierającego informacje przekazane przez informatora, analiza danych telekomunikacyjnych oraz danych internetowych dziennikarza mogłaby łatwo naprowadzić na źródło, od którego dziennikarz je otrzymał. Dziennikarz powinien na przyszłość w bardziej rozważny sposób kontaktować się ze swoim informatorem (spotykać się z nim w różnych, bardziej neutralnych miejscach, bez telefonów komórkowych itd.), a także pomyśleć o stosowaniu narzędzi wzmacniających ochronę prywatności komunikacji internetowej i telefonicznej.

Silne hasła

Bezpieczne hasło jest kluczowe dla każdego, kto poważnie myśli o ochronie swoich danych. Stanowi ono pierwszą (a w wielu przypadkach również jedyną) barierę między poufnymi informacjami a każdym, kto chce uzyskać do nich dostęp. Można posłużyć się zaporami sieciowymi, zabezpieczać skrzynki pocztowe lub szyfrować dyski, ale nie przyniesie to skutku, jeżeli hasło będzie słabe lub pozwoli się, by wpadło ono w niepowołane ręce[171]. Niestety większość z nas bagatelizuje zagrożenie i najczęściej stosuje łatwe do zgadnięcia i podatne na ataki hasła.

Konsekwencje złamania słabego hasła

O tym, jak druzgocące w skutkach może okazać się używanie słabego hasła, przekonał się dziennikarz piszący dla popularnego na całym świecie bloga technologicznego Gizmodo. W 2012 r. ktoś uzyskał dostęp do jego konta na iCloud, czyli oprogramowania, które umożliwia synchronizację urządzeń firmy Apple. Zaraz potem, korzystając z zapasowego konta e-mail w iCloud, osobie tej udało się zresetować hasło dziennikarza na skrzynce pocztowej gmail. Na koniec bezpowrotnie usunięto wszystkie dane z telefonu komórkowego, tabletu i komputera. Swoim osiągnięciem haker pochwalił się, używając konta na Twitterze dziennikarza, do którego również uzyskał dostęp.

Zanim przejdziemy do wyjaśnienia, czym powinno charakteryzować się mocne hasło, chcielibyśmy najpierw wyjaśnić, w jaki sposób hakerzy mogą próbować je złamać. Dzięki temu łatwiej można zrozumieć, jakich kombinacji znaków lepiej nie stosować. Jedną z najpopularniejszych metod stosowanych przez cyberprzestępców jest tzw. atak słownikowy. Polega on na próbie włamania do chronionego hasłem komputera przez systematyczne wprowadzanie kolejnych słów ze sporządzonej wcześniej listy (słownika). By ograniczyć czas potrzebny na skuteczne przeprowadzenie ataku, hakerzy najczęściej nie stosują wszystkich możliwych kombinacji znaków, tylko ograniczają się do jakiegoś podzbioru najbardziej prawdopodobnych możliwości, np. słów występujących w danym języku, najczęściej stosowanych haseł itp.

Dobre hasło powinno odznaczać się dwiema cechami. Być:
- trudne do odgadnięcia;
- dobrane w taki sposób, aby minimalizować szkody po udanym włamaniu.

[171] Tactical Technology Collective, Front Line Defenders, *Create and maintain secure passwords*, security in-a-box.org, https://securityinabox.org/en/guide/passwords (dostęp: 5 marca 2016 r.).

Odnosząc się do pierwszego z wymienionych warunków, należy stwierdzić, że hasło powinno być przede wszystkim długie. Najlepiej by składało się z 10 lub więcej znaków. Należy również pamiętać, żeby nie używać fragmentów słów, tylko kombinacje małych i wielkich liter, cyfr, a także znaków specjalnych, takich jak np. $, #, @, !, itd. Dzięki temu zmniejsza się prawdopodobieństwo, że hasło będzie mogło być złamane w krótkim czasie. Warto pamiętać, żeby w haśle nie zawierać informacji, które dotyczą nas bezpośrednio, jak np. data urodzin czy imię zwierzęcia[172].

Jak zapamiętać skomplikowane hasło?

Opracowanie skomplikowanego hasła nie jest problemem. Każdy może wpisać na klawiaturze losowy ciąg znaków i wykorzystywać go później do ochrony poufnych informacji. Tak stworzone hasło łatwo można jednak zapomnieć i stracić dostęp do danych. Z pomocą przychodzą proste mnemotechniki. Jedną z metod jest wybranie fragmentu piosenki i wykorzystanie go jako bazy do opracowania hasła[173], np. „i wtedy na brzegu pojawił się diabeł, do ciebie nad wodą zbudował przeprawę" można przerobić na łatwe do zapamiętania: Iwnbp$ddcnw2P. Dobrym rozwiązaniem jest także skorzystanie z menedżerów haseł, np. darmowego programu KeePass. Umożliwiają one przechowywanie wszystkich naszych haseł i loginów w jednym miejscu. Dostęp do nich jest możliwy jedynie po wprowadzeniu hasła głównego. Wszystkie informacje są dodatkowo zabezpieczone przez stosowanie szyfrowania. Dzięki programom takim jak KeePass nie musimy pamiętać dziesiątków haseł, tylko jedno.

Jeżeli chodzi o minimalizację szkód po złamaniu hasła, powinno się zadbać, aby hasło było unikalne, tzn. nie należy stosować jednego hasła do kilku kont. W przeciwnym razie haker może uzyskać dostęp do wszystkich poufnych informacji, a nie tylko niektórych. Hasło powinno się ponadto systematycznie zmieniać, najlepiej co najmniej raz na 3 miesiące. Im dłużej używa się jednego zestawu znaków, tym więcej czasu daje się innym na jego złamanie. Nie należy również zapominać o tym, że jeżeli haker odgadł nasze hasło, to będzie z niego korzystać, dopóki go nie zmienimy[174].

[172] Ibidem.

[173] D. Jemielniak, *Poradnik unikania inwigilacji*, 2016, s. 1, https://t.co/0ySKHuAvjy (dostęp: 15 marca 2016 r.).

[174] Tactical Technology Collective, Front Line Defenders, *Create and maintain...*, op. cit.

Ranking najgorszych haseł

Firma informatyczna SplashData co roku publikuje listę 25 najczęściej używanych i jednocześnie najprostszych do złamania haseł. Internauci najczęściej wykorzystują proste, wynikające z układu klawiatury ciągi znaków. W 2015 r. ranking wyglądał następująco[175]:

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 1234567890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. starwars

Szyfrowanie

Szyfrowanie poufnych informacji przypomina przechowywanie ich w sejfie. Tylko te osoby, które mają klucz lub znają odpowiednią kombinację zamka, mogą się do nich dostać[176]. Niektóre urządzenia posiadają domyślnie zainstalowane programy szyfrujące. Użytkownicy komputerów Apple'a mogą skorzystać np. z systemu FileVault. Dzięki niemu raz zaszyfrowany dysk odczytać można jedynie przy użyciu hasła lub specjalnego klucza zabezpieczającego. Komputery z systemem Windows posiadają natomiast wbudowany program BitLocker[177]. Pozwala on na szyfrowanie zarówno całego dysku twardego komputera, jak i nośników zewnętrznych. Niestety korzystanie z oprogramowania oferowanego przez duże korporacje obarczone jest pewnym ryzykiem. Ponieważ jest ono oparte na zamkniętym kodzie, znanym jedynie samemu przedsiębiorstwu, nie mamy pewności, że nie zawiera ono tzw. tylnych furtek (ang. *backdoor*), czyli umyślnie stworzonej luki w zabezpieczeniu umożliwiającej dostęp do urządzenia. Alternatywą dla FileVault czy BitLockera

[175] SplashData, *Worst passwords of 2015*, 2016, https://www.teamsid.com/wp-content/uploads/2016/01/TeamsID-IG-Worst-Password-V3.pdf (dostęp: 15 marca 2016 r.).

[176] Ibidem.

[177] BitLocker dostępny jest domyślnie dla Windowsów Vista i 7 (w wersjach Ultimate i Enterprise), Windows 8 (w wersjach Pro i Enterprise), a także Windows 10.

jest np. oparty na idei otwartego oprogramowania VeraCrypt[178]. Pozwala on na szyfrowanie całych dysków lub też partycji, czyli wydzielonych obszarów. Odczytanie danych możliwe jest jedynie po wprowadzeniu hasła. VeraCrypt umożliwia również zabezpieczenie plików dwoma różnymi hasłami, które dają różny dostęp do treści. Dzięki temu, gdy ktoś zmusza nas do podania hasła, możemy ujawnić to, które nie zapewnia pełnego dostępu[179].

7. Czy można pozostać anonimowym w sieci?

To, co robimy w internecie, jest non stop monitorowane. Niekoniecznie musi chodzić tu o służby wywiadowcze. Nasze dane nieustannie zbierają inne podmioty, takie jak np. dostawcy usług (ISP – Internet Service Providers), czy też wielkie korporacje. W przypadku sygnalistów czy dziennikarzy porozumiewających się ze swoimi źródłami nie zawsze kluczowa jest informacja o treści wiadomości, ale sam fakt komunikacji (zob. pyt. 3). Dlatego rodzi się pytanie, jak osoby te mogą pozostać anonimowe? Rozwiązaniem może być skorzystanie z tzw. sieci Tor lub VPN. Ta pierwsza jest skrótem od angielskiego *The Onion Router* i umożliwia tzw. trasowanie cebulowe, czyli technikę służącą do anonimizacji sieci komputerowej poprzez wielokrotne szyfrowanie danych i przesyłanie ich przez szereg serwerów pośredniczących. Zabiegi te mają na celu jak najdokładniejsze ukrycie naszych wirtualnych śladów. Tor jest darmowy i aby z niego korzystać, wystarczy zainstalować specjalną przeglądarkę. Ma jednak kilka poważnych wad, które uniemożliwiają korzystanie z niego przez cały czas. Po pierwsze, wykorzystywanie wielu serwerów powoduje, że działa on bardzo wolno[180]. Po drugie, wiele serwisów (w szczególności państwowych) może blokować łączność z siecią Tor[181]. Po trzecie, osoby korzystające z Tora, mogą przyciągnąć uwagę służb przez sam fakt używania tego narzędzia.

Tor a działalność przestępcza

Tor został stworzony w USA z myślą o ochronie rządowej komunikacji. Obecnie jest jednak wykorzystywany praktycznie

[178] Otwarte oprogramowanie (*open source*) umożliwia użytkownikom dokładne śledzenie kodu źródłowego i dokonywanie w nim zmian.

[179] C.F. Kleberg, *The death of source protection?. Protecting journalists' sources in a post-Snowden age"*, 2015, http://www.lse.ac.uk/media@lse/documents/Death--of-Source-Protection-Carl-Fridh-Kleberg.pdf, s. 10, 11 (dostęp: 16 marca 2016 r.).

[180] C. Kleberg, *The death...*, op. cit., s. 8, 9.

[181] Zob.: A. Obem, *Detektor cebuli na rządowych serwerach. O tym, jak wspierając anonimową komunikację, trafiliśmy na blokadę Tora, panoptykon.org, 15 grudnia 2015 r.*, https://panoptykon.org/wiadomosc/detektor-cebuli-na-rzadowych-serwerach-o-tym-jak-wspierajac-anonimowa-komunikacje (dostęp: 15 marca 2016 r.).

przez wszystkich – od agentów wywiadu i organy ścigania po aktywistów oraz dziennikarzy i sygnalistów. Niestety, wysoki poziom anonimowości zachęca również przestępców. W związku z tym co jakiś czas w mediach pojawiają się artykuły informujące, że Tor jest „siedliskiem hakerów i pedofilów"[182]. Czytając te doniesienia, nie należy jednak zapominać, że każde narzędzie można wykorzystać zarówno do dobrych, jak i złych celów.

VPN czyli wirtualna sieć prywatna (ang. *Virtual Private Network*) sprawia, że dostawca usługi, a także pośrednicy nie wiedzą, jaki rodzaj danych przesyłamy. Nie będą w stanie odróżnić dokumentu tekstowego od pliku dźwiękowego lub muzyki. Nie zobaczą również samej treści komunikacji. Właściwie będą mogli jedynie stwierdzić, że przesyłamy zaszyfrowane dane[183]. Działanie wirtualnej sieci prywatnej najlepiej wytłumaczyć, posługując się metaforą. Jeżeli przesyłanie danych porównamy do jazdy samochodem, to VPN będzie zamkniętym garażem, w którym zmieniamy pojazd, gubiąc jednocześnie wszystkich tych, którzy nas śledzili. Korzystanie z VPN wymaga wykupienia usług u jednej z firm działających w internecie[184]. W przeciwieństwie do Tora usługi VPN są płatne. Połączenie jest jednak o wiele szybsze[185].

Specjalny Sprawozdawca ONZ o szyfrowaniu

Na istotną rolę Tora i VPN dla korzystania ze swobody wypowiedzi zwraca uwagę w jednym ze swoich raportów[186] Specjalny Sprawozdawca ONZ ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi. Jak zauważył, „niektóre państwa blokują strony internetowe o określonej treści [...], a także penalizują zniesławienie [...] celem uciszenia dziennikarzy, obrońców praw człowieka i aktywistów. Łączenie się z internetem za pośrednictwem VPN, a także używanie sieci Tor lub serwisów proxy, połączone z korzystaniem z narzędzi szyfrujących,

[182] Zob. S. Czubkowska, *Co to jest TOR? Wolna amerykanka w sieci, czyli siedlisko hackerów i pedofilów*, dziennik.pl, 2 listopada 2014 r., http://technologia.dziennik.pl/aktualnosci/artykuly/474088,co-to-jest-tor-siedlisko-hackerow-pedofilow-i-przestepcow.html (dostęp: 15 marca 2016 r.).

[183] D. Jemielniak, *Poradnik unikania...*, op. cit., s. 2.

[184] Tutaj znaleźć można zestawienie najlepszych serwisów VPN wg PCMag: http://www.pcmag.com/article2/0,2817,2403388,00.asp (dostęp: 15 marca 2016 r.).

[185] D. Jemielniak, *Poradnik unikania...*, op. cit., s. 2.

[186] Specjalny Sprawozdawca ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi ws. szyfrowania i anonimowości w środowisku cyfrowym z dnia 22 maja 2015 r., nr A/HRC/29/32, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx ;(dostęp: 10 marca 2016 r.).

może być jedynym sposobem, by w takich warunkach uzyskać dostęp do informacji lub je rozpowszechnić". Zdaniem Specjalnego Sprawozdawcy państwa nie powinny co do zasady ograniczać możliwości korzystania prze obywateli z programów szyfrujących oraz możliwości anonimowego używania internetu. Wręcz przeciwnie, powinny promować rozwiązania prawne i technologiczne wzmacniające ochronę prywatności w sieci.

8. Jak bezpiecznie się komunikować?

Bezpieczna komunikacja w internecie

Jedną z najczęściej stosowanych form komunikacji dziennikarzy ze swoimi informatorami jest poczta elektroniczna. Informatorzy mogą preferować ten sposób przekazywania informacji, ponieważ daje im większe poczucie anonimowości niż spotkanie twarzą w twarz. Poczta elektroniczna jest jednak stosunkowo łatwa do monitorowania i bardzo podatna na ataki hakerskie[187]. W celu zwiększenia bezpieczeństwa zaleca się przede wszystkim skorzystanie z narzędzi szyfrujących, takich jak np. PGP (Pretty Good Privacy – pol. tłum.: „całkiem niezła prywatność")[188]. PGP chronią wiadomości poprzez generowanie kluczy, które mogą składać się nawet z kilku tysięcy znaków. Z szyfrowania poczty można skorzystać, instalując specjalne programy[189]. Należy jednak pamiętać, że PGP zadziałają jedynie wtedy, gdy obie strony komunikacji będą z nich korzystały[190]. Obecnie najczęściej polecaną implementacją PGP jest GNU PG.

Zniechęcony informator

Jak istotne jest korzystanie z oprogramowania do szyfrowania poczty, przekonał się amerykański prawnik i dziennikarz Glenn Greenwald. Jak relacjonuje w swojej książce[191], w 2012 r. zgłosił się do niego za pośrednictwem poczty elektronicznej człowiek o pseudonimie Cincinnatus (jak się później okazało, był to Edward Snowden), pisząc, że jest w posiadaniu tajnych, ważnych z punktu widzenia interesu

[187] C. Kleberg, *The death...*, op. cit., s. 9.

[188] Więcej o szyfrowaniu poczty: http://sekurak.pl/szyfrowanie-poczty-w-thunderbird/ (dostęp: 10 marca 2016 r.).

[189] Więcej o działaniu PGP: http://di.com.pl/pgp-pretty-good-privacy-poradnik--dla-poczatkujacych-49995 (dostęp: 10 marca 2016 r.).

[190] A. Obem, M. Czyżewski, K. Szymielewicz, *Prywatność w sieci. Odzyskaj kontrolę*, panoptykon.org, 27 stycznia 2014 r., https://panoptykon.org/wiadomosc/prywatnosc-zrob-sam

[191] G. Greenwald, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

publicznego informacji, które chciałby przekazać dziennikarzowi. Ich przesłanie uzależnił jednak od zainstalowania przez dziennikarza PGP. Greenwald jednak bardzo długo z tym zwlekał, obawiając się (jak się później okazało, niesłusznie), że czynność ta będzie bardzo skomplikowana i czasochłonna, czym lekko zirytował informatora. W książce dziennikarz tak opisuje tę sytuację:

„W obliczu mojej bezczynności C. nasilił działania. Wyprodukował dziesięciominutowy film PGP dla dziennikarzy. Wykorzystując software generujący głos, film instruował w łatwy sposób, krok po kroku, jak zainstalować program kodujący. Zawierał też diagramy i ilustracje. A ja wciąż to ignorowałem. Jak mi później powiedział C., w tym momencie poczuł się zniechęcony. «To ja jestem gotów zaryzykować wolność, a nawet może życie – myślał – by przekazać temu facetowi tysiące ściśle tajnych dokumentów z najbardziej tajnej agencji w kraju – przeciek, który przyniesie dziesiątki, jeśli nie setki sensacyjnych dziennikarskich materiałów – a jemu się nawet nie chce zainstalować programu kodującego!». Znalazłem się właśnie blisko utraty jednego z największych i obarczonych największymi konsekwencjami przecieku na temat bezpieczeństwa narodowego w historii Stanów Zjednoczonych”[192].

Dziennikarze i ich informatorzy mogą rozważyć również komunikację przy pomocy internetowych komunikatorów. Korzystanie z popularnego Skype’a niekoniecznie jest jednak najlepszym rozwiązaniem z uwagi na to, że jak wynika z informacji, do których dotarł Edward Snowden, dane o prowadzonych przez niego połączeniach mogły być przekazywane Narodowej Agencji Bezpieczeństwa (NSA)[193]. Dobrą alternatywą może okazać się program Jitsi, który umożliwia szyfrowanie zarówno komunikacji tekstowej, jak i połączeń głosowych.

Bezpieczna komunikacja przez telefon

Najlepszym sposobem na zabezpieczenie treści rozmowy telefonicznej jest wykorzystywanie jednego z wielu dostępnych w internecie bezpłatnych programów szyfrujących. Popularnym programem do szyfrowania połączeń jest Signal. Dostępny jest zarówno w wersji na iPhony, jak i telefony z Androidem. Aplikacja szyfruje nie tylko treść samych rozmów, ale również SMS-y. Trzeba jednak

[192] Ibidem, s. 18.

[193] G. Greenwald, *Microsoft handed the NSA access to encrypted messages*, The Guardian, 12 lipca 2013 r., http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (dostęp: 15 marca 2016 r.).

pamiętać, że wymaga ona połączenia z internetem. Ponadto obie strony muszą mieć Signala zainstalowanego na swoich urządzeniach. Na szczęście aplikacja powiadamia, który z naszych kontaktów z niego korzysta.

9. Gdzie można znaleźć więcej informacji na temat narzędzi wzmacniających ochronę prywatności w internecie?

Dla wszystkich, którzy chcą poszerzyć swoją wiedzę o ochronie informacji, szczególnie polecamy następujące pozycje:

Źródła polskie

• Jemielniak D., *Poradnik unikania inwigilacji*, 2016, https://dl.dropboxusercontent.com/u/7820278/inwigilacja.pdf
• Obem A., Czyżewski M., Szymielewicz K., *Prywatność w sieci. Odzyskaj kontrolę*, 27 stycznia 2014 r., https://panoptykon.org/wiadomosc/prywatnosc-zrob-sam
• Strona internetowa: Niebezpiecznik.pl

Źródła zagraniczne

•Kleberg C.F., *The death of source protection?. Protecting journalists' sources in a post-Snowden age*, 2015, http://www.lse.ac.uk/media@lse/documents/Death-of-Source-Protection-Carl-Fridh-Kleberg.pdf
• Vitaliev D., *Digital Security and Privacy for Human Rights Defenders*, 2007.
• Strona internetowa: securityinabox.org (projekt organizacji Tactical Technology Collective i Front Line Defenders).

Bibliografia

Akty prawne

• Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 147).
• Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243 j.t.).
• Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2012 r. poz. 270 j.t.).
• Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r. poz. 2135 j.t.).
• Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 1997 r. Nr 89 poz. 555 ze zm.).
• Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88 poz. 553).
• Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78 poz. 483 ze zm.).
• Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz.U. z 1984 r. Nr 5 poz. 24).
• Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2014 r. poz. 1502 j.t.).
• Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2014 r. poz. 101 j.t.).
• Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2014 r. poz. 121 j.t.).
• Europejska Konwencja o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 (Dz.U. z 1993 r. Nr 61 poz. 284 ze zm.).

Orzecznictwo

Wyroki trybunałów międzynarodowych

• Wyrok ETPC z dnia 12 stycznia 2016 r. w sprawie *Szabó i Vissy p. Węgrom*, skarga nr 37138/14.
• Wyrok ETPC z dnia 4 grudnia 2015 r. w sprawie *Zakharov p. Rosji,* skarga nr 47143/06.
• Wyrok ETPC z dnia 1 lipca 2014 r. w sprawie *A.B. p. Szwajcarii,* skarga nr 56925/08.
• Wyrok ETPC z dnia 27 maja 2014 r. w sprawie *Stichting Ostade Blade p. Holandii,* skarga nr 8406/06 .
• Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r. w sprawie *Digital Rights Ireland Ltd p. Minister for Communications, Marine and Natural Resources i inni oraz Kärntner Landesregierung i inni,* sygn. akt C-293/12.
• Wyrok ETPC z dnia 16 lipca 2013 r. w sprawie *Nagla p. Łotwie*, skarga nr 73469/10.

• Wyrok ETPC z dnia 18 marca 2013 r. w sprawie *Saint-Paul Luxemburg S.A. p. Luksemburgowi,* skarga nr 26419/10.
• Wyrok ETPC z dnia 8 stycznia 2013 r. w sprawie *Bucur i Toma p. Rumunii,* skarga nr 40238/02.
• Wyrok ETPC z dnia 22 listopada 2012 r. w sprawie *Telegraaf Media Nederland Landelijke Media B.V. i inni p. Holandii,* skarga nr 39315/06.
• Wyrok ETPC z dnia 18 października 2011 r. w sprawie *Sosinowska p. Polsce,* skarga nr 10247/09.
• Wyrok ETPC z dnia 12 września 2011 r. w sprawie *Palomo Sanches i inni p. Hiszpanii,* skargi nr 28955/06, 28957/06, 28959/06 i 28964/06.
• Wyrok ETPC z dnia 21 lipca 2011 r. w sprawie *Heinisch p. Niemcom,* skarga nr 28274/08.
• Wyrok ETPC z dnia 14 września 2010 r. (Wielka Izba) w sprawie *Sanoma Uitgevers B.V p. Holandii,* skarga nr 38224/03.
• Wyrok ETPC z dnia 15 grudnia w sprawie *Financial Times Ltd. i inni p. Wielkiej Brytanii,* skarga nr 821/03.
• Wyrok ETPC z dnia 16 lipca 2009 r. w sprawie *Wojtas-Kaleta p.Polsce,* skarga nr 20436/02.
• Wyrok ETPC z dnia 19 lutego 2009 r. w sprawie *Marchenko p. Ukrainie,* skarga nr 4063/04.
• Wyrok ETPC z dnia 16 grudnia 2008 r. w sprawie *Frankowicz p. Polsce,* skarga nr 53025/99.
• Wyrok ETPC z dnia 12 lutego 2008 r., w sprawie *Guja p. Mołdawii,* skarga nr 14277/04.
• Wyrok ETPC z dnia 27 listopada 2007 r. w sprawie *Tillack p. Belgii,* skarga nr 20477/05.
• Wyrok ETPC z dnia 8 grudnia 2005 r. w sprawie *Nordisk Film & Tv A/S p. Danii,* skarga nr 40485/02.
• Wyrok ETPC z dnia 15 lipca 2003 r. w sprawie *Ernst i inni p. Belgii,* skarga nr 33400/96.
• Wyrok ETPC z dnia 23 lutego 2003 r. w sprawie *Roemen i Schmit p. Luksemburgowi,* skarga nr 51772/99
• Wyrok ETPC z dnia 29 lutego 2000 r. w sprawie *Fuentes Bobo p. Hiszpanii,* skarga nr 39293/98.
• Wyrok ETPC z dnia 20 maja 1999 r. w sprawie *Rekvenyi p. Węgrom,* skarga nr 24348/94.
• Wyrok ETPC z dnia 20 maja 1999 r. w sprawie *Bladet Tromso i Stensaas p. Norwegii,* skarga nr 21980/93.
• Wyrok ETPC z dnia 25 listopada 1997 r. w sprawie w *Grigoriades p. Grecji,* skarga nr 24348/94.
• Wyrok ETPC z dnia 27 marca 1996 r. (Wielka Izba) w sprawie *Goodwin p. Wielkiej Brytanii,* skarga nr 28957/95.

Wyroki sądów polskich

• Wyrok Sądu Rejonowego dla Warszawy Mokotowa z dnia 26 stycznia 2016 r., sygn. akt VIII K 161/14.

• Wyrok Sądu Najwyższego z dnia 27 listopada 2014 r., sygn. akt IV CSK 174/14.
• Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r., sygn. akt K 23/11.
• Postanowienie Sądu Rejonowego w Jarocinie z dnia 11 kwietnia 2014 r., sygn. akt II Kp 18/14.
• Wyrok Sądu Rejonowego w Bydgoszczy z dnia 3 lutego 2014 r., sygn. akt VI K 445/13/MK.
• Wyrok Sądu Najwyższego z dnia 28 sierpnia 2013 r., sygn. akt I PK 48/13
• Wyrok Sądu Apelacyjnego w Warszawie z dnia 26 kwietnia 2013 r., sygn. akt I ACa 1002/12.
• Postanowienie Sądu Rejonowego w Warszawie z dnia 27 czerwca 2012 r., sygn. akt XIV Kp 1358/12.
• Wyrok Sądu Okręgowego w Warszawie z dnia 26 kwietnia 2012 r., sygn. akt II C 626/11.
• Postanowienie Sądu Rejonowego dla Warszawy-Mokotowa z dnia 19 marca 2012 r., sygn. akt XIV Kp 498/12.
• Postanowienie Sądu Rejonowego dla Warszawy-Mokotowa z dnia 19 marca 2012 r., sygn. akt XIV Kp 497/12.
• Wyrok Sądu Rejonowego w Kędzierzynie-Koźlu z dnia 13 września 2011 r., sygn. akt IV P 2/10.
• Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 28 czerwca 2011 r., sygn. akt I OSK 1217/10.
• Wyrok Sądu Rejonowego w Łodzi z dnia 23 maja 2011 r., sygn. akt XP 263/09.
• Wyrok Sądu Okręgowego w Warszawie z dnia 27 maja 2010 r., sygn. akt XXI PA 154/10.
• Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 8 kwietnia 2010 r., sygn. akt II SA/Wa 1488/09.
• Wyrok Sądu Rejonowego dla Warszawy-Żoliborza z dnia 8 grudnia 2009, sygn. akt VII P 660/08.
• Postanowienie Sądu Najwyższego z dnia 20 października 2005 r., sygn. akt II KK 184/05.
• Wyrok Sądu Okręgowego w Katowicach z dnia 12 lipca 2005 r., sygn. akt IX Pa 245/05.
• Postanowienie Sądu Najwyższego z dnia 15 grudnia 2004 r., sygn. akt III KK 278/04.
• Wyrok Sądu Rejonowego w Mikołowie z dnia 9 grudnia 2004 r., sygn. akt IV P 763/04.
• Uchwała Sądu Najwyższego z dnia 19 stycznia 2004 r., sygn. akt I KZP 15/94.
• Uchwała Sądu Najwyższego z 22 listopada 2002 r., sygn. akt I KZP 26/02.
• Uchwała składu 7 sędziów Sądu Najwyższego z dnia 19 stycznia 1995 r., sygn. akt I KZP 15/94.
• Wyrok Sądu Najwyższego z 6 czerwca 1928 r., sygn. akt K 715/28.

Książki, artykuły

• Bodnar A., Ploszka A., *Europa uczy się ochrony sygnalistów. Dzięki Snowdenowi,* 2015, https://wszystkoconajwazniejsze.pl/adam-bodnar-adam-ploszka-europa-uczy-sie-ochrony-sygnalistow-dzieki-snowdenowi/ (dostęp: 15 marca 2016 r.).
• Bojańczyk A., *Billingi jednak na specjalnych prawach,* Rzeczpospolita, 1 grudnia 2005.
• Brocławik K., Czajka, M., *Prawnokarne aspekty ochrony tajemnicy zawodowej radcy prawnego, część II,* „Radca Prawny" 2001, nr 4.
• Czubkowska S., *Co to jest TOR? Wolna amerykanka w sieci, czyli siedlisko hackerów i pedofilów,* 2 listopada 2014 r., http://technologia.dziennik.pl/aktualnosci/artykuly/474088,co-to-jest-tor-siedlisko-hackerow-pedofilow-i-przestepcow.html (dostęp: 15 marca 2016).
• Czuchnowski W., *Dziennikarze na celowniku służb*, Gazeta Wyborcza, 8 października 2010, http://wyborcza.pl/1,76842,8480752,-Dziennikarze_na_celowniku_sluzb_specjalnych.html (dostęp: 8 lutego 2016 r.).
• Dobosz I., *Prawo i etyka w zawodzie dziennikarza,* Kraków 2008.
• Głowacka D., *Praktyczny przewodnik po art. 212 k.k,* Warszawa 2012 r., http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4479:praktyczny-przewodnik-po-art-212-kk-broszura-informacyjna&catid=51:publikacjerozne&Itemid=41 (dostęp: 26 lutego 2016).
• Gontarski W., *Prokurator nadużywa władzy,* Rzeczpospolita, 13 grudnia 2004 r.
• Gotkowicz K., Kosmus B., *Komentarz do art. 15 ustawy – Prawo prasowe* [w:] B. Kosmus G. Kuczyński (red.), *Prawo prasowe. Komentarz,* Warszawa 2013.
• Greenwald G., *Snowden. Nigdzie się nie ukryjesz,* Warszawa 2014.
• Greenwald G., *Microsoft handed the NSA access to encrypted messages*, The Guardian, 12 lipiec 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (dostęp: 1 marca 2016).
• Ferenc-Szydełko E., *Prawo prasowe. Komentarz*, Warszawa 2008.
• Jaworski L., *Tajemnica zawodowa dziennikarza w świetle obowiązującego w Polsce prawa. Część 1. Prawo do anonimatu*, Studia Medioznawcze / Instytut Dziennikarstwa Uniwersytetu Warszawskiego" 2015, nr 1, s. 45-55.
• Jemielniak D., *Poradnik unikania inwigilacji*, 2016, https://dl.dropboxusercontent.com/u/7820278/inwigilacja.pdf (dostęp: 15 marca 2016 r.).
• Kamiński I.C., *Ograniczenia swobody wypowiedzi dopuszczalne w Europejskiej Konwencji Praw Człowieka. Analiza krytyczna*, Warszawa 2010.
• Kleberg C.F., *The death of source protection?. Protecting journalists' sources in a post-Snowden age*, 2015, http://www.lse.ac.uk/media@lse/documents/Death-of-Source-Protection-Carl-Fridh-Kleberg.pdf (dostęp: 15 marca 2016 r.).

• Kobylińska A., Folta M., *Sygnaliści – ludzie, którzy nie potrafią milczeć: oświadczenia osób ujawniających nieprawidłowości w instytucjach i firmach w Polsce*, Instytut Spraw Publicznych, Warszawa 2015.
• Kondracki J., Stępiński, K., *Billingi pod osłoną tajemnicy dziennikarskiej*, „Rzeczpospolita", 10 października 2010 r.
• Kosonoga J., *Dobro wymiaru sprawiedliwości jako przesłanka dokonywania czynności procesowych w postępowaniu karnym* [w:] W. Cieślak, S. Steinborn (red.), *Profesor Marian Cieślak – osoba, dzieło, kontynuacje*, Warszawa 2013, s. 886-893.
• Krivokapić D., Joler, V. (red.), *Guide to online media autonomy: security risks and protection mechanisms. Walking on the digital age,* Share Foundation, Oxford 2015, http://www.shareconference.net/sites/default/files/u742/vodic_walking_eng_web.pdf (dostęp: 15 marca 2016 r.).
• Krzyżanowska-Mierzewska M., Rutkowska A., *Zagadnienia prawne związane z ochroną whistleblowerów w warunkach zatrudnienia w ujęciu orzecznictwa ETPCz*, „Przegląd Sądowy" 2015, nr 4, s. 106-122.
• Kuczyński G. (red.), *Komentarz do art. 16 ustawy – Prawo prasowe* [w:] *B. Kosmus, G. Kuczyński (red.), Prawo prasowe. Komentarz, Warszawa 2013.*
• Lis W., *Komentarz do art. 15 Prawa prasowego* [w:] W. Beczek (red.), *Prawo prasowe. Komentarz*, Warszawa 2012.
• Litwiński P., *Korporacyjne systemy raportowania nadużyć (whistleblowing hotlines) a ochrona danych osobowych* [w:] A. Mednis (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013, s. 113-127.
• Nowińska E., *Wolność wypowiedzi prasowej*, Warszawa 2007.
• Obem A., Czyżewski M., Szymielewicz K., *Prywatność w sieci. Odzyskaj kontrolę*, 27 stycznia 2014 r., https://panoptykon.org/wiadomosc/prywatnosc-zrob-sam (dostęp: 8 marca 2016 r.).
• Obem A., *Detektor cebuli na rządowych serwerach. O tym, jak wspierając anonimową komunikację, trafiliśmy na blokadę Tora*, 15 grudnia 2015 r., https://panoptykon.org/wiadomosc/detektor-cebuli-na-rzadowych-serwerach-o-tym-jak-wspierajac-anonimowa-komunikacje (dostęp: 8 marca 2016 r.).
• Orliński W., *Inwigilacja w sieci. Internet jest nasz*, Gazeta Wyborcza 14 stycznia 2016 r., http://wyborcza.pl/duzyformat/1,150171,19469932,inwigilacja-w-sieci-internet-nie-jest-nasz.html, (dostęp: 2 marca 2016 r.).
• Osiatyński W., *Prawa człowieka i ich granice*, Kraków 2011.
• Pązik A., *Wyłączenie bezprawności naruszenia dobra osobistego na podstawie interesu społecznego*, Warszawa 2014.
• Podkowik J., *Ochrona dziennikarskich źródeł informacji w dobie cyfrowej w świetle Konwencji o ochronie praw człowieka i podstawowych wolności oraz Konstytucji RP,* „Przegląd Sejmowy" 2015, nr 3(128), s. 67-87.
• Polański J., *Programy nagradzania informatorów w prawie państwa europejskich*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, nr 9 (3), s. 10-33.

• Ploszka A., *Ochrona demaskatorów (whistleblowers) w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Europejski Przegląd Sądowy" 2014, nr 4, s. 12-18.
• Posetti J., *Protecting journalism sources in the digital age*, UNESCO Publishing 2015.
• Rogowski W., *Whistleblowing: bohaterstwo, zdrada czy interes?*, „Przegląd Corporate Governance" 2007, nr 1, s. 23-41.
• Sobczak J., *Komentarz do art. 16 ustawy – Prawo prasowe,* [w:] *Prawo prasowe. Komentarz*, Warszawa 2008.
• Sobczak J., *Prawo prasowe. Podręcznik akademicki*, Warszawa 2012.
• Stefańska J., *Przeszukanie a tajemnica dziennikarska*, P„Prokuratura i Prawo" 2015, nr 6.
• Świątek-Barylska I., *Whistleblowing w praktyce. Postawy i zachowania pracowników organizacji gospodarczych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2012, nr 249, s. 403–412.
• Świątkowski A.M., *Sygnalizacja (whistleblowing) a prawo pracy*, „Przegląd Sądowy" 2015, nr 5, s. 6-25.
• Vitaliev D., *Digital Security and Privacy for Human Rights Defenders*, 2007.
• Wagstaff J., *Journalists, media under attack from hackers: Google researchers*, Reuters, 28 marca 2014, http://www.reuters.com/article/us-media-cybercrime-idUSBREA2R0EU20140328 (dostęp: 15 marca 2016 r.).
• Wojciechowska-Nowak A., *Założenia do ustawy o ochronie praw osób sygnalizujących nieprawidłowości środowisku zawodowym. Jak polski ustawodawca może czerpać z doświadczeń państw obcych?*, Fundacja Batorego, Warszawa 2012.
• Wojciechowska-Nowak A. *Ochrona sygnalistów w Polsce. Stan obecny i rekomendacje zmian*, Warszawa 2012.
• Wojciechowska-Nowak A., *Ochrona prawna sygnalistów w doświadczeniu sędziów sądów pracy. Raport z badań*, Warszawa 2011.
• Wujczyk M., *Podstawy whistleblowingu w polskim prawie pracy,* „Przegląd Sądowy" 2014, nr 6, s. 114-122.
• Zabłocki S., *Problem „samozwolnienia się" dziennikarza z tajemnicy anonimatu* [w:] J. Jakubowska-Hara, C. Nowak, J. Skupiński, (red.), *Reforma prawa karnego. Propozycje i komentarze. Księga pamiątkowa Prof. Barbary Kunickiej-Michalskiej,* Warszawa 2008.
• Zaremba M., *Prawo prasowe a internet – stan de lege lata i de lege ferenda* [w:] D. Bychawska-Siniarska, D. Głowacka, *Wirtualne media – realne problemy,* Warszawa 2014, s. 153-161, http://www.obserwatorium.org/images/Wirtualne%20media%20-%20realne%20problemy.pdf (dostęp: 15 marca 2016 r.).
• Zaremba M., *Jeszcze jeden głos w sprawie prawnej ochrony tajemnicy billingów dziennikarzy*, obserwatorium.org., 9 maja 2012 r. http://www.obserwatorium.org/images/billingi%20artykul_M_Zaremba.pdf (dostęp: 15 marca 2016 r.).
• Zaremba M., *Prawo prasowe. Ujęcie praktyczne*, Warszawa 2007.
• Zielinko I., *Tajemnica dziennikarska w prawie prasowym*, „Prokuratura i Prawo" 2009, nr 7-8, s. 148-168.

Raporty, przewodniki, opinie, zalecenia

• Wniosek RPO do Trybunału Konstytucyjnego z dnia 18 lutego 2016 r., https://www.rpo.gov.pl/sites/default/files/Wniosek_do_TK_kontrola_operacyjna.pdf (dostęp: 15 marca 2016 r.).
• Opinia przyjaciela sądu HFPC w sprawie naruszenia tajemnicy dziennikarskiej z dnia 17 lutego 2016 r., http://www.obserwatorium.org/index.php?option=com_content&view=article&id=4799:opinia-przyjaciela-sdu-w-sprawie-naruszenia-tajemnicy-dziennikarskiej&catid=40:zkraju&Itemid=34 (dostęp: 1 marca 2016 r.)
• Opinia Izby Wydawców prasy w sprawie poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych (druk sejmowy nr 154) z dnia 26 stycznia 2016 r., http://www.senat.gov.pl/gfx/senat/userfiles/_public/k9/dokumenty/konsultacje_ustawy/071/071_iwp.pdf (dostęp: 11 marca 2016 r.).
• Stanowisko HFPC w sprawie inwigilacji dziennikarzy z dnia 15 stycznia 2016 r., http://www.hfhr.pl/wp-content/uploads/2016/01/HFPC_stanowisko_inwigilacja_dziennikarzy.pdf (dostęp: 1 marca 2016 r.)
• Pew Research Center, Centrum Cyfrowego Dziennikarstwa Uniwersytetu Columbia, *Investigative Journalists and Digital Security. Perceptions of Vulnerability and Changes in Behavior*, 2016, http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf (dostęp: 10 lutego 2016 r.)
• Europejski Trybunał Praw Człowieka, *Factsheet – journalistic sources protection*, styczeń 2016, http://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf , (dostęp: 10 marca 2016 r.)
• Uwagi Helsińskiej Fundacji Praw Człowieka do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych (druk sejmowy nr 154) z dnia 30 grudnia 2015 r., http://www.hfhr.pl/wp-content/uploads/2015/12/HFPC_opinia_ustawa_o_policji_30122015.pdf (dostęp: 5 marca 2016 r.).
• Wystąpienie Rzecznika Praw Obywatelskich z 18 grudnia 2015 r. do Ministra Pracy i Polityki Społecznej (II.7040.104.2015AF/LN).
• List HFPC z dnia 17 grudnia.2015 r. do Prezesa Wojewódzkiego Szpitala w S., http://www.obserwatorium.org/index.php?option=-com_content&view=article&id=4782:prawo-pielgniarek-i-poonych--do-sygnalizowania-o-nieprawidowociach&catid=47:aktualnosciprog&Itemid=66 (dostęp: 4 marca 2016 r.).
• Rezolucja Zgromadzenia Parlamentarnego Rady Europy z dnia 21 kwietnia 2015 r. nr 2045 (2015) w sprawie masowej inwigilacji, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en (dostęp: 15 marca 2016 r.).
• Share Foundation, *Guide to online media autonomy: security risks and protection mechanisms. Walking on the digital age*, 2015, http://www.shareconference.net/sites/default/files/u742/vodic_walking_eng_web.pdf (dostęp: 2 marca 2016 r.).

• Raport Specjalnego Sprawozdawcy ONZ ws. ochrony dziennikarskich źródeł informacji i sygnalistów z dnia 8 września 2015, A/70/361, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361 (dostęp: 10 marca 2016 r.).
• Raport Specjalnego Sprawozdawcy ds. promocji oraz ochrony prawa do wolności wyrażania opinii oraz wolności wypowiedzi ws. szyfrowania i anonimowości w środowisku cyfrowym z dnia 22 maja 2015 r., nr A/HRC/29/32, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (dostęp: 10 marca 2016 r.).
• Agencja Praw Podstawowych (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks*, 2015.
• Rekomendacja Komitetu Ministrów Rady Europy CM/Rec (2014) z dnia 19 lutego 2014 r. dotycząca ochrony sygnalistów, https://www.msz.gov.pl/resource/161bbca4-55d0-4c79-834f-c2d4f4f4559d:JCR (dostęp: 17 marca 2016 r.).
• Rezolucja Parlamentu Europejskiego z 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188 (INI)).
• Human Rights Watch, American Civil Liberties Union, *With liberty to monitor all: how large-scale U.S. surveillance is harming journalism, law and American democracy*, Nowy Jork, 2014.
• Zalecenia Whistleblowing International Network, kwiecień 2013 r., https://whistleblowingnetwork.org/other-resources/europe-and-international/international-best-practices-for-whistleblower-policies/ (dostęp: 3 marca 2016 r.).
• Transparency International, *International Principles for Whistleblower Legislation Best practices for laws to protect whistleblowers and support whistleblowing in the public interest*, 2013, http://www.transparency.org/whatwedo/publication/international_principles_for_whistleblower_legislation (dostęp: 2 marca 2016).
• Rada Europy, Whistleblower protection: encouraging reporting, lipiec 2012, www.oecd.org/cleangovbiz/toolkit/50042935.pdf (dostęp: 24 marca 2016 r.).
• G20, *Compendium of best practices and guiding principles for legislation on the protection of whistleblowers*, 2012, http://www.oecd.org/g20/topics/anti-corruption/48972967.pdf (dostęp: 24 marca 2016 r.).
• Stanowisko HFPC w sprawie pozyskiwania billingów oraz treści informacji tekstowych z dnia 29 grudnia 2011 r., http://www.hfhr.pl/wp-content/uploads/2011/12/stanowisko_hfpc_29_grudnia_2011.pdf (dostęp: 16 marca 2016 r.).
• Praktyczny przewodnik w sprawie kryteriów dopuszczalności skargi do ETPC, grudzień 2011 r., https://www.msz.gov.pl/resource/29734ee5-a2c2-4b2c-b09f-ce7f58b1fef3:JCR (dostęp: 17 marca 2016 r.).

• Rezolucja Zgromadzenia Parlamentarnego Rady Europy z dnia 29 kwietnia 2010 r. w sprawie ochrony demaskatorów, nr 1729.
• Wystąpienie Rzecznika Praw Obywatelskich z dnia 3 marca 2009 r. do Ministra Pracy i Polityki Społecznej (sygn. RPO-606960-III/09/RP/AF).
• Rekomendacja Komitetu Ministrów Rady Ministrów R (2000)7 z dnia 8 marca 2000 r. w sprawie prawa dziennikarzy do nieujawniania swoich źródeł informacji, https://wcd.coe.int/ViewDoc.jsp?id=342907&Site=CM (dostęp: 10 marca 2016 r.).
• Informacja kancelarii Europejskiego Trybunału Praw Człowieka: W jaki sposób prawidłowo wnieść skargę indywidualną do Europejskiego Trybunału Praw Człowieka, http://www.echr.coe.int/Pages/home.aspx?p=applicants/pol&c (dostęp: 2 marca 2016 r.).
• Wskazówki ICC dla sygnalistów, http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/corporate-responsibility-and-anti-corruption/whistleblowing/ (dostęp: 17 marca 2016 r.).

O Autorach

Dorota Głowacka - prawniczka, absolwentka Wydziału Prawa i Administracji Uniwersytetu Łódzkiego, doktorantka w Katedrze Prawa Międzynarodowego i Stosunków Międzynarodowych WPiA UŁ. Koordynatorka programu Obserwatorium Wolności Mediów w Polsce Helsińskiej Fundacji Praw Człowieka, specjalizuje się w zagadnieniach związanych ze swobodą wypowiedzi i prawem do prywatności.

Adam Ploszka - absolwent prawa i stosunków międzynarodowych na Uniwersytecie Warszawskim, doktorant w Zakładzie Praw Człowieka WPiA UW. Koordynator programu Klinika Prawa Człowieka a Podatki oraz prawnik w programie Obserwatorium Wolności Mediów w Polsce Helsińskiej Fundacji Praw Człowieka.

Marcin Sczaniecki - student V roku prawa Akademii Leona Koźmińskiego, współpracownik programu Obserwatorium Wolności Mediów w Polsce Helsińskiej Fundacji Praw Człowieka.

Helsińska Fundacja Praw Człowieka

Helsińska Fundacja Praw Człowieka została utworzona w 1989 r. przez członków Komitetu Helsińskiego w Polsce i obecnie jest jedną z największych organizacji pozarządowych w Polsce. Jej działalność obejmuje prowadzenie monitoringu i badań w zakresie przestrzegania praw człowieka, udzielanie pomocy prawnej Polakom i cudzoziemcom, prowadzenie litygacji strategicznej oraz innych działań w interesie publicznym. Fundacja współpracuje z międzynarodowymi instytucjami zajmującymi się prawami człowieka, od 2007 r. ma status konsultacyjny przy Radzie Społeczno-Gospodarczej ONZ (ECOSOC).

Więcej informacji o Fundacji: www.hfhr.pl

Obserwatorium Wolności Mediów w Polsce

Obserwatorium Wolności Mediów w Polsce jest jednym z programów prawnych Helsińskiej Fundacji Praw Człowieka. Istnieje od 2008 r. Program działa na rzecz podnoszenia standardów wolności słowa w tradycyjnych mediach oraz w internecie. Prawnicy programu udzielają pomocy prawnej dziennikarzom oraz prowadzą tzw. litygację strategiczną w indywidualnych sprawach o precedensowym znaczeniu dla swobody wypowiedzi. Przygotowują m.in. opinie amicus curiae w postępowaniach sądowych, skargi do Europejskiego Trybunału Praw Człowieka i obserwują procesy sądowe. Prawnicy „Obserwatorium" działają także na rzecz zmiany regulacji prawnych (m.in. prawa prasowego, kodeksu karnego). Prowadzą również działalność edukacyjną, organizując konferencje, wykłady otwarte oraz wydając publikacje poświęcone problematyce wolności słowa.

Więcej informacji o programie: www.obserwatorium.org

W serii praktycznych przewodników opracowanych w ramach Obserwatorium Wolności Mediów w Polsce ukazały się dotychczas także:

- Praktyczny przewodnik po art. 212 k.k.
- Media w okresie wyborczym. Przewodnik dla dziennikarzy
- Wolność artystyczna. Praktyczny przewodnik

Wszystkie przewodniki dostępne są na stronie internetowej programu w zakładce „Publikacje".