




ERWIN RYTER
Uniwersytet Łódzki

 <https://orcid.org/0000-0002-7656-502X>

JUSTYNA RYTER
Uniwersytet Łódzki

 <https://orcid.org/0000-0002-4909-0575>

Granice ingerencji w prawo do prywatności w procesie zwalczania przestępczości oraz zapobiegania jej skutkom

Abstract: In their article, Erwin Ryter and Justyna Ryter make an attempt to answer the following questions: What may be the farthest limit of tolerance towards public authorities' interference with a person's right to privacy in the context of fight against crime as well as the performance of necessary and purposeful procedural actions? Can both the procedural objective and the fact of the violation of the right to privacy of the suspect justify direct or indirect interference with the privacy of persons from the suspect's social environment, even if that interference is a side effect of actions taken against the offender? The authors of this article also raise the issue of privacy violations in relation to various forms of monitoring of persons who are of interest to the authorities conducting the proceedings. In particular, these proceedings may involve keeping various types of registers containing the data of offender, using classified eavesdropping on them, observing their whereabouts, and disclosing their personal data.

Keywords: right to privacy, privacy restriction, invasion of privacy, privacy protection, video surveillance, call control

1. Określenie przedmiotu prawa do prywatności

Prawo do prywatności, jako dobro szczególnej wagi, doczekało się wielu interesujących analiz i jest niezwykle ciekawym zagadnieniem z punktu widzenia granic, po których przekroczeniu można rozważać fakt naruszenia tego dobra wskutek podejmowania działań jednych osób wobec

drugich bądź w wyniku czynności realizowanych przez władze publiczne w stosunku do jednostek.

Jak podaje Marcin Pryciak, zagadnienia prawa i ochrony prywatności w doktrynie formalno-prawnej podejmowano od końca XIX w. Myśl dotycząca tej kategorii pojęciowej rozwijała się jednak już w czasach starożytnych i w perspektywie czasowej możemy ją dostrzec w ideach myślicieli filozoficzno-politycznych różnych epok¹. Z kolei Jakub Rzucidło wskazuje, że źródła prywatności można poszukiwać w różnego rodzaju przekazach czy koncepcjach filozoficzno-prawnych. W zależności od przyjętego ujęcia jedni badacze postrzegają ją jako stan nierozzerwalnie przypisany człowiekowi, towarzyszący mu zawsze, choć nie zawsze uświadomiony, drudzy zaś poszukują jej genezy w XVII- i XVIII-wiecznych rozważaniach o prawie natury i wolności².

Na gruncie polskiego ustawodawstwa prawo do prywatności ujęte jest w art. 47 Konstytucji Rzeczypospolitej Polskiej³, zgodnie z którym każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

W jednym z wyroków Trybunału Konstytucyjnego prawo do prywatności wyrażono w odniesieniu do dwóch płaszczyzn – prawa jednostki do prawnej ochrony sfer jej życia wskazanych w pierwszej części przepisu art. 47 Konstytucji RP oraz prawa do wolności decydowania w sprawach określonych w drugiej części tego przepisu. Pierwszemu prawu jednostki musi towarzyszyć ustawowa regulacja pozwalająca chronić prywatność, życie rodzinne, cześć i dobre imię. Drugie oznacza zakaz ingerencji w wolność kształtowania przez jednostkę jej życia osobistego⁴.

W wyroku Sądu Apelacyjnego w Katowicach z dnia 20 września 2012 r. wskazano z kolei, że ochrona prywatności nie ma charakteru absolutnego również w stosunku do innych (niż publiczne) osób, m.in. ze względu na potrzeby życia w zbiorowości. Nie jest zatem możliwe wypracowanie w tej kwestii jednoznacznych i wyczerpujących kryteriów, które mogłyby odnosić się do wszystkich sytuacji⁵.

¹ M. PRYCIAK: *Prawo do prywatności*. „Studia Erasmiانا Wratislaviensia” 2010, z. 4, s. 213.

² J. RZUCIDŁO: *Prawo do prywatności i ochrona danych osobowych*. W: *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*. Red. M. JABŁOŃSKI. Wrocław 2014, s. 153.

³ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz.U. 1997, nr 78, poz. 483.

⁴ Wyrok Trybunału Konstytucyjnego z dnia 5 marca 2013 r. U 2/11. OTK-A 2013, nr 3, poz. 24. Dz.U. 2013, poz. 375.

⁵ Wyrok Sądu Apelacyjnego w Katowicach z dnia 20 września 2012 r. V ACa 378/12. LEX nr 1220491.

Tym bardziej zatem ochrona prywatności może podlegać ograniczeniom, zaś w pewnych sytuacjach nawet wyłączeniom na gruncie czynności podejmowanych przez władze publiczne w związku z zapobieganiem i zwalczaniem przestępczości.

W odniesieniu do niniejszego opracowania analiza granic naruszenia prawa do prywatności będzie się odnosiła w szczególności do osób dopuszczających się przestępstw lub podejrzewanych o ich popełnienie, wobec których realizuje się określone czynności procesowe, a także sądowe oraz wykonawcze. Ponadto ingerencja w prywatność osoby, która dopuściła się naruszenia porządku prawnego bądź jest podejrzewana o takie naruszenie, może wydawać się naturalną konsekwencją oraz dolegliwością, z którą powinien być się liczyć sprawca czynu zabronionego w chwili podjęcia decyzji o jego popełnieniu. Twierdzenie jednak dotyczące granicy, którą można byłoby uznać za granicę wyznaczającą nieuprawnione naruszenie granic prywatności osoby podejrzanej o popełnienie przestępstwa lub skazanej za popełnienie przestępstwa, należy najpierw oprzeć na rozważaniach odnoszących się do istoty prawa do prywatności oraz do przymiotów, które je definiują.

Prawo do prywatności spotkało się w literaturze z bardzo licznymi analizami, w których dążono szczególnie do określenia, jakie elementy mogą przesądzać o czyjejs prywatności oraz jaka jest granica, której przekroczenie można uznać za obiektywnie uzasadnioną ingerencję w sferę czyjejs poufności oraz intymności. O ile jednak jakakolwiek forma naruszenia czyjejs prywatności zwykle nie znajduje samoistnej akceptacji ze strony społeczeństwa, to sytuacja ta nie wydaje się już tak oczywista w momencie zaingerowania władz publicznych w prywatność osób pozbawionych wolności lub – w nieco szerszym ujęciu – osób naruszających porządek prawny i przez to podlegających różnego rodzaju czynnościom, w tym inwigilacji, realizowanym przez organy państwowe.

Jak wskazuje Agnieszka Grzelak, badania Eurobarometru przeprowadzone w 2011 r. pokazały społeczne olbrzymie poparcie dla przekazywania danych organom ścigania w walce z terroryzmem, co może oznaczać większe przyzwolenie i akceptację dla tych aktów prawnych, w których odstępuje się od prawa do ochrony danych osobowych na rzecz walki z najpoważniejszymi formami przestępczości⁶. Warto nadmienić, że kwestie ochrony danych osobowych zazwyczaj ściśle łączą się z czyjąs prywatnością, a zatem naruszenie danych osobowych może w wielu sytuacjach prowadzić automatycznie do naruszenia granic czyjejs prywatności, a zatem także osoby podejrzanej bądź pozbawionej wolności. W opinii

⁶ A. GRZELAK: *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*. Warszawa 2015, s. 86.

autorów naturalną konsekwencją utraty wolności będzie jednocześnie określona postać ograniczenia prywatności osoby skazanej.

W jednym ze swoich orzeczeń Europejski Trybunał Praw Człowieka (ETPCz) potwierdził, że każde pozbawienie wolności prowadzi do ograniczenia życia prywatnego i rodzinnego więźnia⁷. Co więcej, wskazana forma ograniczenia prywatności, albowiem wymuszona sytuacją pozbawienia wolności, może podlegać kolejnym redukcjom związanym np. ze stosowaniem różnego rodzaju kar dyscyplinarnych, które w jeszcze większym stopniu mogą wpływać na ograniczenie prawa do prywatności skazanego. Takim będzie np. w wypadku zastosowania kary dyscyplinarnej określonej w art. 143 § 1 pkt. 8 k.k.w.⁸, mianowicie w sytuacji umieszczenia osadzonego w celi izolacyjnej na okres do 28 dni.

Ponieważ prawo do prywatności należy uznać za nieodłączny element podstawowych praw i wolności każdego człowieka, to – w zależności od przyjętego stanowiska – wyróżnić można różne grupy cech określające jego istotę.

Interesujące wyjaśnienie w tym zakresie przedstawił Zbyszko Mielnik, powołując się na pogląd Stiga Strömholma⁹, który podjął próbę znalezienia cech wspólnych amerykańskiej koncepcji prywatności i europejskiej – prawa do osobowości. Strömholm wykazał trzy rodzaje działań, mianowicie: wkroczenie w sferę, którą jednostka chce zachować dla siebie i ma w tym uzasadniony interes; zbieranie informacji bez zgody zainteresowanego lub za pomocą metod uznanych za niewłaściwe; czynienie użytku z materiałów o danej osobie dla publikacji lub innych specjalnych celów¹⁰. Pierwsze dwa elementy wskazanej ingerencji zastosowanej wobec osób pozbawionych wolności stanowią nieodłączną rzeczywistość wykonywania wobec nich kary izolacyjnej, stąd określenie granicy, po której przekroczeniu ingerencja ta może zostać uznana za nadmierną, nastęrczać

⁷ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 września 2000 r. w sprawie Messina przeciwko Włochom. Skarga nr 25498/94.

⁸ Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy. Dz.U. 1997, nr 90, poz. 55 [k.k.w.].

⁹ Mielnik podaje nazwisko: Stronholm, można jednak z pewnością stwierdzić, że chodzi o Stiga Strömholma (ur. 1931), szwedzkiego prawnika, profesora prawa, a także pisarza i krytyka literackiego, autora m.in. książki *Right of privacy and rights of the personality. A comparative survey*. Stockholm 1967. <https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf> [dostęp: 24.11.2021] (U. JONASSON: *Om Stig Strömholm – “En vis norrbottning och hans nation”*. 6.04.2015. <http://jonassonulf.blogspot.com/2015/04/om-stig-stromholm-en-vis-norrbottning.html> [dostęp: 24.11.2021]; *Stig Strömholm*. https://sv.wikipedia.org/wiki/Stig_Str%C3%B6mholm [dostęp: 24.11.2021]).

¹⁰ Z. MIELNIK: *Prawo do prywatności (zagadnienia wybrane)*. „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 1996, R. 58, z. 2, s. 31.

może wiele trudności interpretacyjnych, w zależności od tego, co w przypadku określonej grupy więźniów uznaje się za ich prawo do prywatności.

Ponadto prawo do prywatności stało się fundamentem zapoczątkowującym powstanie różnego rodzaju koncepcji filozoficzno-prawnych. Zgodnie z poglądem Jakuba Cichuty, bezpośrednią przyczyną zaistnienia prawa do prywatności jest liberalizm, zaś takie postawienie sprawy wyjaśnia stosunkowo młody wiek tego prawa. Liberalizm był ideologią założycielską w Stanach Zjednoczonych, co tłumaczyłoby amerykańskie pochodzenie prawa do prywatności, natomiast w Europie długo musiał walczyć o swoją pozycję z ideologiami konserwatywnymi, marksistowskimi i monarchistycznymi¹¹. A zatem liberalizm, w którym to idea wolności jest uznawana za wartość nadrzędną, oddziałuje na postrzeganie prawa do prywatności m.in. w kontekście potrzeby bycia niezależnym od innych. Kwestia braku zależności od innych w przypadku osób pozbawionych wolności może być odnoszona wyłącznie do niezwykle ograniczonego kręgu osobistych doznań, jak choćby związanych z wyznawaną religią lub własnymi poglądami, do których prawo powinien mieć każdy więzień niezależnie od zasad panujących na terenie danego zakładu karnego, oczywiście z wyłączeniem poglądów o charakterze nawołującym do przemocy i nienawiści bądź innych powszechnie nieakceptowalnych, nawet gdyby podejmowana była próba uzasadnienia ich kwestią wyrażania wyłącznie prywatnego zdania.

Z kolei Sławomir Ruchała powołał się w swoim opracowaniu na zaprezentowane przez Hannah Arendt „zjawisko kondycji ludzkiej”, opisywane przez nią za pomocą trzech metafor, spośród których jedna została określona jako „zabicie w człowieku osoby prywatnej”, mające stanowić wstępny warunek pełnego opanowania człowieka, niszczącego jego ochronę prawną oraz zabijającego prywatność¹². W pewnym sensie można twierdzić o występowaniu podobnego zjawiska w odniesieniu do osób pozbawionych wolności, w sytuacji, w której oczywista staje się konieczność podporządkowania ich życia, niemalże w każdym aspekcie, warunkom oraz zasadom panującym w jednostce penitencjarnej ze z góry narzuconymi regułami postępowania, mogącymi istotnie wpływać na poczucie ograniczenia prywatności w zależności od stopnia wrażliwości danej osoby.

W analizie istoty prawa do prywatności godne uwagi są powszechnie funkcjonujące akty prawne, a szczególnie Powszechna Deklaracja Praw

¹¹ J. CICHUTA: *Prawo do prywatności jako pochodna poglądów antropologicznych*. W: IDEM: *Prawo do prywatności – współczesne wyzwania*. Warszawa 2019, s. 41.

¹² S. RUCHAŁA: „Współczesne filozoficzne spory o ugruntowanie praw człowieka”. Rozprawa doktorska. Opieka nauk. prof. dr hab. K. ŚLĘCZKA. Uniwersytet Śląski w Katowicach, Wydział Nauk Społecznych, Instytut Filozofii. Katowice 2006, s. 144.

Człowieka¹³, wskazująca w art. 12–15 na kwestie prywatności ujmowane jako: prawo do swobodnego poruszania się, prawo do prywatności życia, prawo do prywatności korespondencji, prawo do mienia oraz prawo do narodowości jako kolebki ludzkiej osobowości, prawo do szukania azylu w innym kraju. Co więcej, prawo do prywatności jako istotny aspekt życia człowieka, mające na celu ochronę ludzkiej egzystencji, określa w ten sposób art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych¹⁴.

Paweł Czarnecki i Andrzej Świątłowski zgodnie potwierdzają, że niektóre akty międzynarodowe odnoszą się do problematyki prawa do prywatności, szczególnie w odniesieniu do zbierania informacji. Przykładem jest art. 12 Powszechnej Deklaracji Praw Człowieka czy art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych¹⁵. Z kolei fakt zbierania o kimś informacji oznacza nic innego jak przetwarzanie danych osobowych regulowane ustawami o ochronie danych oraz innymi aktami prawnymi, co ściśle łączy się z ochroną prywatności, jak również wpływa na sposób jej postrzegania.

W próbie określenia rangi prawa do prywatności fundamentalne znaczenie ma ponadto art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (Europejskiej Konwencji Praw Człowieka, EKPCz)¹⁶, zgodnie z którym każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji, jak również niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Właśnie te aspekty mogą powodować coraz większe wątpliwości związane z określeniem, w jakim momencie dochodzi do przekroczenia indywidualnych

¹³ Powszechna Deklaracja Praw Człowieka. Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.

¹⁴ Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. Dz.U. 1977, nr 38, poz. 167.

¹⁵ P. CZARNECKI, A. ŚWIĄTŁOWSKI: *Prawo do prywatności i zasada prawdy materialnej w kontekście pozyskiwania informacji relevantnych procesowo*. [Publikacja powstała w wyniku realizacji projektu badawczego o nr 2013/08/M/HS5/00038 finansowanego ze środków Narodowego Centrum Nauki]. <https://www.law.uj.edu.pl/~kpk/dowody/wp-content/uploads/2014/03/Prawo-do-prywatno%C5%9Bci-merytoryczna.pdf> [dostęp: 26.05.2021].

¹⁶ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. Dz.U. 1993, nr 61, poz. 284.

granic czyjejs prywatności w związku z prowadzeniem przeciwko tej osobie czynności związanych z danym czynem zabronionym.

Co jednak istotne, zdefiniowanie pojęcia „życie prywatne” w świetle art. 8 EKPCz wciąż jeszcze nastęrcza wiele problemów i trudności¹⁷.

Jak słusznie zauważyła Ivana Roagna Europejski Trybunał Praw Człowieka nigdy nie podał w toku wypracowanych przez siebie interpretacji jednoznacznej i klarownej definicji „życia prywatnego”; dla sędziów strasburskich pojęcie życia prywatnego jest szerokie i nie może być zdefiniowane w sposób wyczerpujący¹⁸. Wszystko będzie zatem zależało od danego stanu faktycznego oraz okoliczności, które mogły doprowadzić do naruszenia prawa do prywatności w czasie realizacji celu, jakim jest ustalenie odpowiedzialności karnej sprawcy.

Przy tej okazji nasuwa się pytanie: czy ingerencja w prawo do prywatności osoby będącej w sferze zainteresowań organów ścigania będzie zawsze prowadzić do jego naruszenia? Otóż niekoniecznie.

Jak wskazuje Grzelak, ingerencja w prawo do prywatności to takie działanie lub zaniechanie władzy publicznej, które narusza prawo do prywatności określone w art. 8 ust. 1 EKPCz, a wykazanie istnienia takiej ingerencji jest zadaniem skarżącego. Z kolei naruszenie wspomnianego prawa to taka ingerencja, która nie może być uzasadniona przyczynami określonymi w art. 8 ust. 2 EKPCz. Zadaniem skarżącego jest wykazanie ingerencji w jego prawo do prywatności¹⁹. Ponadto w opinii autorów, nawet jeśli zachodzi okoliczność zaingerowania władz publicznych w prawo do prywatności osoby znajdującej się w kręgu podejrzanych, to jest to zazwyczaj podyktowane nadrzędnym – w stosunku do indywidualnego interesu jednostki – celem procesowym, bez czego nie byłoby możliwe osiągnięcie pewnych skutków związanych z realizacją zamierzeń postępowania karnego.

Wobec tego, że przedstawiciele władzy publicznej mogą w pewnych sytuacjach przekroczyć barierę czyjejs prywatności z uwagi cel prowadzonych przez siebie czynności, kwestią szczególnie zajmującą będzie próba określenia granicy pomiędzy usprawiedliwionym, jak również pożądanym procesowo, a niesłusznym i celowo godzącym w prywatność podejmowaniem ingerencji w przestrzeń osobistą danej osoby. Nadmierna ingerencja może się przejawiać m.in. w nieuzasadnionym kontrolowaniu treści rozmów telefonicznych odbywanych przez daną osobę, jak również korzystania przez nią z innych form kontaktowania się za pomocą urzą-

¹⁷ A. GRZELAK: *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*. Warszawa 2015, s. 113.

¹⁸ I. ROAGNA: *Ochrona prawa do poszanowania życia prywatnego i rodzinnego w Europejskiej Konwencji o Ochronie Praw Człowieka*. Strasburg 2012, s. 12.

¹⁹ A. GRZELAK: *Ochrona danych osobowych...*, s. 111–112.

dzeń teleinformatycznych, pogwałceniu tajemnicy korespondencji lub, ujętej art. 49 Konstytucji RP, tajemnicy komunikowania się.

W odniesieniu do problematyki kontroli rozmów stwierdzono – na gruncie orzecznictwa strasburskiego – że rozmowy telefoniczne są objęte pojęciami „życia prywatnego” i „korespondencji” w rozumieniu art. 8 Konwencji, środki podsłuchu stanowią „ingerencję władzy publicznej” w wykonywanie prawa zagwarantowanego art. 8 ust. 1 Konwencji. Rejestracja połączeń telefonicznych, tj. przechowywanie danych niezbędnych do ustalenia źródła, odbiorcy, daty, godziny i czasu trwania połączenia, musi być odróżniana od podsłuchu, który jest zjawiskiem niepożądanym i bezprawnym w społeczeństwie demokratycznym, chyba że istnieją ku niemu uzasadnione powody²⁰.

Na gruncie polskich regulacji prawnych prawo do prywatności, w swoim ogólnym znaczeniu, podlega przede wszystkim ścisłej ochronie prawnej zagwarantowanej przez Konstytucję RP.

Ewa Łętowska podkreśla, że ochrona prywatności, obejmująca zakaz wkraczania państwa w bardzo szeroko rozumiane życie prywatne i rodzinne, należy do tych właśnie praw podstawowych jednostki, które chronione są nie tylko konstytucyjnie, lecz nawet na poziomie ponadkonstytucyjnym²¹.

Z uwagi na dość znaczne ryzyko naruszenia czyjejs prywatności w związku z kontrolowaniem i utrwalaniem prowadzonych przez daną osobę rozmów telefonicznych oraz realizowania innych form komunikowania się na odległość za pomocą nowoczesnych urządzeń państwo prawa powinno dysponować odpowiednimi możliwościami kontrolowania zasięgu oraz celu takiej ingerencji, zaś przede wszystkim powinno móc wykazać się przesłankami jej zastosowania wobec określonej osoby, jak również okazania narzędzi egzekwujących moment bezwzględnego zakończenia ingerencji, która przestaje już spełniać swój pierwotny cel, a zaczyna naruszać czyjąś prywatność w sposób całkowicie nieuzasadniony.

Odrębnym problemem może być ponadto kwestia ewentualnego informowania bądź zaniechania spełnienia tej powinności w stosunku do inwigilowanej osoby o dokonywaniu względem niej tego rodzaju czynności. Jednakże na gruncie regulacji dotyczących ochrony danych osobowych w związku ze zwalczaniem i zapobieganiem przestępczości nie zawsze obowiązek informacyjny będzie musiał być spełniony, w przeciwieństwie

²⁰ P. CZARNECKI, A. ŚWIĄTEŃSKI: *Prawo do prywatności...*

²¹ E. ŁĘTOWSKA: *Prawo do prywatności w Europie*. [Materiały edukacyjne przygotowane w ramach programu Socrates Grundtvig Action I, Law through Experience/116881-CP-1-2004-SK-GRUNDTVIG-G11]. http://www.psep.pl/grundtvig/6/prawo_do_prywatnosci.pdf [dostęp: 29.05.2021].

do przetwarzania danych osobowych na gruncie RODO²². Przykładem aktu prawnego, który uprawniał do monitorowania korespondencji lub rozmów, wprawdzie w uzasadnionych sytuacjach, lecz jednocześnie bez wiedzy osób, których to monitorowanie dotyczyło, była obowiązująca w Niemczech ustawa G10 z 13 sierpnia 1968 r. w sprawie ograniczeń tajemnicy korespondencji, poczty i telekomunikacji. Zgodnie z tym przepisem osoby, które zostały poddane monitorowaniu, nie dość, że o tym nie były informowane, to również nie mogły podejmować jakichkolwiek czynności przeciwko skutkom tej inwigilacji, choćby nawet ta oznaczała naruszenie ich prywatności. Na gruncie tak postrzeganego monitorowania niezwykle łatwo może dochodzić do przekroczenia akceptowalnych granic czyjejs prywatności.

Kwestią, na którą warto zwrócić uwagę, może być ponadto sytuacja obserwowania przez władze publiczne osoby znajdującej się w kręgu zainteresowania lub niecelowego, aczkolwiek wymuszonego sytuacją, jednoczesnego obserwowania osoby trzeciej, która może wieść ze sprawcą wspólne życie, zamieszkiwać z nim w jednym domu czy trwale uczestniczyć w jeszcze innych aspektach jego życia osobistego. W okolicznościach tych mogą się pojawić nie tylko wątpliwości dotyczące podstawy prawnej takiego działania, lecz także obiektywna natura etycznej w związku z mimowolnym przyglądaniem się przez organy ścigania życiu prywatnemu osoby zupełnie nieistotnej z punktu widzenia realizowanych przez te organy czynności w stosunku do podejrzanego objętego obserwacją lub innego rodzaju ingerencją ze strony władz. Potrzeba zapewnienia właściwej ochrony życia prywatnego osoby nie znajdującej się w kręgu zainteresowania organów ścigania wymaga przedsięwzięcia przez te organy takich środków, które będą z jednej strony równoważyć interesy związane z celem prowadzonego postępowania, zaś z drugiej gwarantować ochronę prywatności jednostki znajdującej się spoza kręgiem podejrzanych.

2. Naruszenie prywatności osób podejrzewanych o popełnienie przestępstwa w związku z gromadzeniem danych

Naruszenie prywatności osób podlegających różnym formom inwigilacji ze strony władz państwowych, w tym zwłaszcza organów ścigania, może przybrać zróżnicowane formy. Między innymi może do-

²² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.U. UE 4.5.2016, L 119/1.

chodzić do gromadzenia informacji na temat osób w różnego rodzaju rejestrach. Informacje te mogą przybrać postać zarówno danych zwykłych, jak choćby imię i nazwisko, wiek czy też miejsce zamieszkania, jak również danych szczególnych, zwanych wrażliwymi, dotyczących m.in. stanu zdrowia, seksualności, pochodzenia etnicznego itp. W Polsce istnieje wiele rejestrów publicznych, w których gromadzi się dane osobowe. Informacje o wszystkich dostępnych w kraju rejestrach publicznych można uzyskać na stronie Głównego Urzędu Statystycznego. Ponadto dane publiczne, które mogą mieć znacznie dla obywateli oraz przedsiębiorców, znajdują się w bazie danych publicznych. Z punktu widzenia tematyki niniejszego artykułu warto zwrócić uwagę na prowadzony przez Ministerstwo Sprawiedliwości Krajowy Rejestr Karny²³, który jako rejestr nie mający charakteru ogólnodostępnego ani jawnego wymaga złożenia przez zainteresowaną osobę specjalnego wniosku w razie chęci otrzymania informacji w zakresie danych ujętych w art. 1 pkt. 2 Ustawy o Krajowym Rejestrze Karnym. Dane zawarte w Krajowym Rejestrze Karnym, czyli informacje dotyczące karalności oraz wyroków skazujących, składają się na jeden z elementów prywatności danej osoby, biorąc pod uwagę okoliczność, że dane te – w razie ich przypadkowego lub, przeciwnie, celowego ujawnienia – mogą się wiązać z naruszeniem praw i wolności osoby, której naruszenie dotyczy, w tym prywatności tej osoby.

Gromadzenie danych w różnego rodzaju rejestrach publicznych może być zatem powiązane z występowaniem określonych naruszeń, jak również godzić w obszar prywatności, w tym wywoływać określone skutki w sferze naruszenia dóbr osobistych danej osoby. Z punktu widzenia naruszenia prywatności w związku z zapobieganiem i zwalczaniem przestępstwa warto jeszcze zwrócić uwagę na rejestr, który funkcjonuje w Polsce od 1 stycznia 2018 r., mianowicie Rejestr Sprawców Przestępstw na Tle

²³ Zgodnie z art. 1 pkt. 1 i 2 Ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. 2000, nr 50, poz. 580) Rejestr został utworzony celem gromadzenia danych o osobach: 1) prawomocnie skazanych za przestępstwa lub przestępstwa skarbowe; 2) przeciwko którym prawomocnie warunkowo umorzono postępowanie karne w sprawach o przestępstwa lub przestępstwa skarbowe; 3) przeciwko którym prawomocnie umorzono postępowanie karne w sprawach o przestępstwa lub przestępstwa skarbowe na podstawie amnestii; 4) będących obywatelami polskimi prawomocnie skazanymi przez sądy państw obcych; 5) wobec których prawomocnie orzeczono środki zabezpieczające w sprawach o przestępstwa lub przestępstwa skarbowe; 6) nieletnich, wobec których prawomocnie orzeczono środki wychowawcze, poprawcze lub wychowawczo-lecznicze albo którym wymierzono karę na podstawie art. 13 lub art. 94 Ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U. 2018, poz. 969); 7) prawomocnie skazanych za wykroczenia na karę aresztu; 8) poszukiwanych listem gończym; 9) tymczasowo aresztowanych; 10) nieletnich umieszczonych w schroniskach dla nieletnich.

Seksualnym²⁴. W odniesieniu do ewentualnego naruszenia prywatności na gruncie funkcjonowania przedmiotowego rejestru jednym z najbardziej znamienych dylematów – w opinii autorów – może być kwestia powiązania ofiar, w tym ofiar będących osobami najbliższymi dla sprawcy przestępstwa na tle seksualnym, z zamieszczeniem danych sprawcy w tym rejestrze. Innymi słowy, w sytuacji zamieszczenia w rejestrze informacji na temat sprawcy, co może wydawać się słuszne z punktu widzenia dobra ogółu społeczeństwa, osoby pozostające z nim w jakimkolwiek osobistym stosunku bądź innej podobnej relacji mogą niestety ucierpieć ze względu na możliwość powiązania ich danych z osobą sprawcy. Ściślej oznacza to, że problem powiązania sprawcy przestępstwa na tle seksualnym z osobą przez niego pokrzywdzoną, w tym zwłaszcza z osobą mu najbliższą, może wywoływać negatywne skutki w sferze prawa do prywatności osoby pokrzywdzonej. Ponadto pokrzywdzony, który doznał traumatycznych przeżyć wskutek stania się ofiarą przestępstwa na tle seksualnym, może doświadczyć dodatkowo stygmatyzacji wynikającej z powiązania jego osoby z osobą sprawcy oraz charakterem popełnionego przez niego czynu. Wreszcie konsekwencje zamieszczenia danych sprawców w Rejestrze Sprawców Przestępstw na Tle Seksualnym mogą być odczuwalne dla ich rodzin także wtedy, gdy bezpośrednią ofiarą przestępstwa nie jest osoba najbliższa sprawcy. Naruszenie prywatności może się w tym przypadku przejawiać w różnorodnych formach stygmatyzacji sprawców i ich rodzin przez osoby trzecie, które uzyskały informację o zamieszczeniu danych sprawcy w rzeczonym rejestrze.

W opinii autorów gromadzenie danych w różnego rodzaju rejestrach, choć może okazać się przydatne, to zwłaszcza w odniesieniu do Rejestru Sprawców Przestępstw na Tle Seksualnym nie jest pozbawione wad. Jakkolwiek bowiem funkcjonowanie wskazanego rejestru powinno stanowić dodatkowe narzędzie pozwalające na aktywne monitorowanie tej kategorii sprawców w celu zwiększonej ochrony społeczeństwa przed ich czynami, nie powinno jednocześnie prowadzić do naruszenia konstytucyjnych praw i wolności osób będących ofiarami tych sprawców, w tym zwłaszcza poprzez zaingerowanie w ich prywatność. Rejestr może mieć

²⁴ Funkcjonowanie Rejestru Sprawców Przestępstw na Tle Seksualnym regulują następujące akty prawne: Ustawa z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym; Rozporządzenie Ministra Sprawiedliwości z dnia 2 lutego 2017 r. w sprawie określenia trybu i sposobu przekazywania danych do Rejestru Sprawców Przestępstw na Tle Seksualnym; Rozporządzenie Ministra Sprawiedliwości z dnia 13 marca 2017 r. w sprawie przetwarzania oraz przekazywania danych osobowych zgromadzonych w Rejestrze Sprawców Przestępstw na Tle Seksualnym do celów statystycznych oraz badań naukowych; Rozporządzenie Ministra Sprawiedliwości z dnia 31 lipca 2017 r. w sprawie trybu, sposobu i zakresu uzyskiwania i udostępniania informacji z Rejestru z dostępem ograniczonym oraz sposobu zakładania konta użytkownika.

także istotny wpływ na życie prywatne wykluczonych społecznie sprawców i dotyczyć nawet tych osób, których sposób postępowania po skazaniu będzie zapowiadał minimalne prawdopodobieństwo ponownego popełnienia przestępstwa na tle seksualnym.

Na gruncie licznie występującego orzecznictwa sądowego analiza ograniczenia prawa do prywatności osób podlegających wpisowi do Rejestru Sprawców Przystępstw na Tle Seksualnym stała się m.in. przedmiotem rozważań Wojewódzkiego Sądu Administracyjnego w Warszawie, zawartych w wyroku z października 2020 r., w którym stwierdzono, że chociaż wpis do Rejestru Sprawców Przystępstw na Tle Seksualnym jest nałożeniem nowego obowiązku administracyjnego ograniczającego prywatność osób podlegających wpisowi, to jednak następuje to w sposób proporcjonalny i uzasadniony wyższym celem²⁵.

Przechodząc na grunt orzecznictwa strasburskiego stanowiącego o problematyce naruszenia prawa do prywatności w sytuacjach związanych z zapobieganiem i zwalczaniem przestępczości, za warty uwagi należy uznać zwłaszcza wyrok ETPCz w sprawie S. i Marper przeciwko Wielkiej Brytanii²⁶, rozstrzygający na temat sytuacji związanej z gromadzeniem odcisków palców, próbek komórkowych oraz profilu DNA osób, wobec których były wprowadzane podejmowane czynności na etapie wszczętego postępowania karnego, ale ostatecznie sprawa ta nie zakończyła się wydaniem wyroku skazującego. Natomiast bezspornie doszło do zgromadzenia danych, które uznaje się za dane wrażliwe oraz dane biometryczne²⁷. Także i w takich sytuacjach nie jest trudno o naruszenie czyjeś prywatności. Warto bowiem nadmienić, że dane w postaci odcisków palców bądź profilu DNA są niezmiennie w ciągu trwania życia, toteż ich gromadzenie oraz przetwarzanie – nawet w tak istotnym celu, jakim jest zapobieganie przestępczości lub jej zwalczanie – powinno się odbywać w odpowiednich warunkach oraz w racjonalnie uzasadnionych sytuacjach, aby w razie umorzenia postępowania albo innego rodzaju braku kontynuacji prowadzenia czynności przeciwko określonej osobie nie spowodować w jej dobrach osobistych długotrwałego uszczerbku ani innych

²⁵ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 października 2020 r. VII SA/Wa 449/20. LEX nr 3152730.

²⁶ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 grudnia 2008 r. w sprawie S. i Marper przeciwko Wielkiej Brytanii. Skarga nr 30562/04 i 30566/04.

²⁷ Za dane wrażliwe, czy też dane szczególnego rodzaju, uznaje się takie dane, których nieuprawnione ujawnienie bądź naruszenie może prowadzić do naruszenia praw i wolności osoby, której te dane dotyczą. Zgodnie z RODO do danych szczególnego rodzaju zalicza się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne lub dotyczące zdrowia, seksualności lub orientacji seksualnej.

nieodwracalnych krzywd w sferze jej praw lub wolności, zaś szczególnie w obrębie prywatności.

Wspomniane dane biometryczne, zgodnie z art. 4 pkt. 14 RODO, oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Podobną definicję danych biometrycznych zawiera tzw. dyrektywa policyjna, tj. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r.²⁸, w art. 3 pkt. 13, która jest stosowana w związku z zapobieganiem i zwalczaniem przestępczości. Naruszenie danych biometrycznych może z kolei istotnie wpływać na ingerencję w sferę czyjejs prywatności.

Jak słusznie twierdzi Aleksandra Pyka, dane biometryczne należą w pełni do informacji umożliwiających identyfikację osoby lub potwierdzających jednoznaczną identyfikację, a do tego są to dane tym cenniejsze, że niepowtarzalne²⁹. Z tego powodu przetwarzanie tych danych musi się odbywać z zachowaniem najwyższej staranności. Art. 10 dyrektywy policyjnej precyzuje, w jaki sposób może dochodzić do obrotu tymi danymi.

W działalności organów ścigania dane biometryczne są bardzo często przez nie pozyskiwane i następnie przetwarzane. Na przykład w zbiorach danych Centralnej Registratury Daktyloskopijnej³⁰ oraz Automatycznego Systemu Identyfikacji Daktyloskopijnej³¹ gromadzi się dane biometryczne

²⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW. Dz.U. UE 4.5.2016, L 119/89.

²⁹ A. PYKA: *Przetwarzanie danych biometrycznych. Aspekty prawne*. „Studia Prawa Publicznego” 2018, nr 3 (23), s. 138.

³⁰ Jednostka zajmująca się gromadzeniem kart daktyloskopijnych z odbitkami linii papilarnych palców rąk oraz dłoni osób podejrzanych o popełnienie przestępstwa ściganego z oskarżenia publicznego oraz nieletnich, którzy dopuścili się czynów zabronionych przez ustawę jako przestępstwa ściganego z oskarżenia publicznego. W jej ramach funkcjonuje Automatyczny System Identyfikacji Daktyloskopijnej – AFIS, służący do gromadzenia i przeszukiwania obrazów linii papilarnych palców rąk i dłoni pobranych od osób podejrzanych o popełnienie przestępstwa oraz niezidentyfikowanych śladów linii papilarnych (N.N.).

³¹ Jest to system, który funkcjonuje w Polsce od 2000 r. i służy do gromadzenia i przeszukiwania obrazów linii papilarnych palców rąk i dłoni pobranych od osób podejrzanych oraz niezidentyfikowanych śladów linii papilarnych zabezpieczonych na miejscach przestępstw w celu szybkiej identyfikacji osoby.

pod postacią odcisków palców zebranych od osób podejrzewanych o popełnienie czynu zabronionego. Zgodnie z motywem 51 dyrektywy policyjnej, proces przetwarzania danych biometrycznych może stwarzać ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. To z kolei może prowadzić do uszczerbku fizycznego, szkód majątkowych i niemajątkowych, w szczególności: gdy przetwarzanie może skutkować dyskryminacją, kradzieżą lub sfałszowaniem tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych chronionych tajemnicą służbową, niedozwolonym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; gdy osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi³².

Warto jeszcze zwrócić uwagę na potencjalną sytuację, w której władze publiczne najpierw zbiorą i zgromadzą informacje oddziałujące w szczególny sposób na sferę czyjejs prywatności, zaś następnie dane te okażą się całkowicie nieprzydatne dla celów wszczętego postępowania. Czy zatem w tej sytuacji można się doszukiwać jakichkolwiek pozytywnych aspektów gromadzenia tego rodzaju danych, uwzględniając cel w postaci zapobiegania i zwalczania przestępczości? W opinii autorów takie działanie jest jak najbardziej uzasadnione. Gromadzenie nawet wysoce newralgicznych danych i informacji pozwoli bowiem, po pierwsze, na wyeliminowanie z kręgu podejrzanych osób nie mających nic wspólnego z popełnieniem określonego czynu, a po drugie, na swobodne prowadzenie niezbędnych oraz celowych czynności procesowych przez organy władzy publicznej, które powinny dysponować możliwością podejmowania czynności adekwatnych do danej sprawy.

Odrębną kwestią jest jeszcze sytuacja gromadzenia danych, które zaliczają się do tzw. danych prywatnych, przy okazji prowadzenia czynności związanych z konkretnym naruszeniem prawa. Sytuację tego rodzaju doskonale obrazuje sprawa Panteleyenکو przeciwko Ukrainie³³, która polegała na tym, że władze publiczne zbyt szeroko zbierały dane dotyczące notariusza podejrzewanego o fałszowanie dokumentów i gromadziły informacje dotyczące m.in. jego pobytu w szpitalu psychiatrycznym. A zatem dane dotyczące zdrowia – w świetle art. 10 dyrektywy policyjnej – mogą być przetwarzane wyłącznie wtedy, jeżeli jest to bezwzględnie niezbędne, podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, oraz: jest dopuszczone prawem Unii Europejskiej lub

³² Zob. motyw 51 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych...

³³ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 29 czerwca 2006 r. w sprawie Panteleyenکو przeciwko Ukrainie. Skarga nr 11901/02. LEX nr 182356.

prawem państwa członkowskiego; jest niezbędne dla ochrony żywotnych interesów osoby fizycznej, której dane dotyczą, lub innej osoby; lub takie przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą. Niezwykle więc łatwo może dojść do nieuprawnionego naruszenia granic prywatności osoby, której dane są zbierane w celu nie wynikającym bezpośrednio z istoty czynności procesowych. W tym wypadku granicą mogło być zbieranie danych wyłącznie niezbędnych dla stwierdzenia, czy faktycznie mogło dojść do fałszowania dokumentów, co zdecydowanie nie uprawniało organów do dowiadywania się o stanie zdrowia podejrzewanej osoby ani tym bardziej do gromadzenia informacji na temat stanu jej zdrowia, w tym odbytych hospitalizacji. Gromadzenie różnych danych, w tym danych wrażliwych, może ponadto stwarzać pokusę ich nieuprawnionego wykorzystania.

Przywołany przykład wskazuje na jeszcze jedną niepożądaną praktykę, mianowicie na to, że nieograniczone zbieranie informacji na temat osoby podejrzewanej o działalność przestępczą może prowadzić do uzyskania informacji zbyt szerokich, nieuzasadnionego konkretnym celem ich gromadzenia, i istotnie przyczyniać się do naruszenia sfery prywatności. W szczególności może to dotyczyć informacji na temat stanu zdrowia, w tym zdrowia psychicznego. Niekontrolowane ujawnienie tego rodzaju danych może z kolei wpływać nie tylko na sferę komfortu danej osoby, lecz także na jej wizerunek i inne dobra osobiste, co może mieć szczególne znaczenie, gdy osoba ta wykonuje zawód zaufania publicznego.

Warto również wskazać na sprawę Rotaru przeciwko Rumunii³⁴, której istotą jest brak podstaw prawnych do przechowywania i udostępniania przez władze informacji z życia prywatnego jednostki. Problemem na gruncie tej sytuacji był także brak możliwości skorygowania przez Rumuńskie Służby Informacji akt dotyczących skarżącego, jak również pozbawienie go możliwości wniesienia skutecznego środka odwoławczego. ETPCz uznał, że gromadzenie przez władze publiczne informacji o życiu prywatnym jednostki, posługiwanie się nimi i odmowa ich sprostowania oznaczają ingerencję w prawo do poszanowania życia prywatnego.

Należy jeszcze wspomnieć, że wprowadzone na mocy dyrektywy policyjnej reguły ochrony danych osobowych, nierozdzielnie łączące się z kwestią ochrony prywatności, doskonale pokazały, jak istotne jest, aby podmiot zbierający dane czynił to z zachowaniem zasady celowości, jak również minimalizacji danych, dzięki czemu zbierane dane są adekwatne

³⁴ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii. Skarga nr 28341/95.

do celu, co nie prowadzi do zbyt nadmiernego zaingerowania w czyjąś prywatność. Ponadto, jak wskazuje motyw 29 dyrektywy policyjnej, dane osobowe należy zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach mieszczących się w zakresie zastosowania dyrektywy i nie należy ich przetwarzać w celach niezgodnych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych i wykonywaniem kar, w tym z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom.

Granica pomiędzy naruszeniem prywatności osoby podejrzewanej lub skazanej a naruszeniem dodatkowo jej danych osobowych jest zazwyczaj bardzo płynna i wydaje się nawet, że już sam fakt naruszenia prywatności będzie zawsze – przynajmniej w jakimś stopniu – stanowił także naruszenie zasad ochrony danych osobowych.

Władze publiczne gromadzące różnego rodzaju informacje osobowe, zwłaszcza w różnego typu rejestrach, aby nie spotkać się z zarzutem bezprawnego ich wykorzystywania bądź przekroczenia granic prywatności, powinny zadbać o zapewnienie osobom, których dane dotyczą, dostępu do tych danych, jak również prawo do ich poprawienia lub do usunięcia danych wadliwych lub nieaktualnych, chyba że w ustawie wprost nie przewidziano konieczności spełnienia tych obowiązków. Wszelka bowiem ingerencja władz publicznych w życie prywatne powinna zawsze pozostawać w zgodności z obowiązującym prawem.

W literaturze wskazuje się na kryteria, których spełnienie może uprawniać organy do zaingerowania w prywatność osoby podejrzanej lub skazanej. Zalicza się do nich w szczególności określenie rodzaju przestępstwa, którego podejrzenie popełnienia bądź popełnienie może uzasadniać oddziaływanie na czyjąś prywatność, nawet w sposób uznawany powszechnie za nadmierny, z tym zaznaczeniem, że chodzi o przestępstwa „poważniejszej” natury. Ponadto podstawa ograniczenia czyjejś prywatności powinna znaleźć uzasadnienie w krajowym porządku prawnym, jak również powinien być określony sposób dostępu do tych danych, czas ich przechowywania i krąg osób lub podmiotów, którym dane mogą zostać udostępnione. W przeciwnym bowiem razie granica pomiędzy realizowaniem czynności procesowych uchodzących nawet za najbardziej niezbędne i celowe a przekroczeniem akceptowalnego marginesu naruszenia prywatności danej osoby będzie na tyle nieprecyzyjna, że stworzy pole dla dopuszczania się nadmiernej ingerencji, która nie powinna się zdarzyć w państwie prawa i wobec której powinno się wypracować określone rozwiązania.

3. Poszanowanie prawa do prywatności w sytuacji kontrolowania i utrwalania rozmów telefonicznych oraz poznawania lokalizacji telefonu i spisu połączeń internetowych

Obowiązujące aktualnie przepisy Kodeksu postępowania karnego³⁵ regulują – w rozdz. 26 – kwestię warunków zastosowania przesłanek kontrolowania i utrwalania rozmów. Istotą tej kontroli powinno być to, że organy kontrolujące nie przekraczają swoich uprawnień, nie ingerują w życie prywatne kontrolowanych osób nadmiernie, nieuzasadnienie ani niecelowo ani nie oddziałują zbyt daleko na sferę ich prywatności. Ingerencja powinna być w tym wypadku traktowana nie jako zasada postępowania w danej sytuacji, lecz jako wyjątek, gdy w inny sposób nie można ustalić faktów interesujących organy ścigania. Art 237 § 3 k.p.k.³⁶ wskazuje odniesienie

³⁵ Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego. Tj. Dz.U. 2021, poz. 534 [k.p.k.].

³⁶ W świetle art. 237 § 3 k.p.k. kontrola i utrwalanie treści rozmów telefonicznych może być uzasadnione, gdy toczące się postępowanie bądź uzasadniona obawa popełnienia nowego przestępstwa dotyczy: zabójstwa; narażenia na niebezpieczeństwo powszechne lub spowodowania katastrofy; handlu ludźmi; uprowadzenia osoby; wymuszania okupu; uprowadzenia statku powietrznego lub wodnego; rozboju, kradzieży rozbójniczej lub wymuszenia rozbójniczego; zamachu na niepodległość lub integralność państwa; zamachu na konstytucyjny ustrój państwa lub jego naczelné organy, albo na jednostkę Sił Zbrojnych Rzeczypospolitej Polskiej; szpiegostwa lub ujawnienia informacji niejawnych o klauzuli tajności „tajne” lub „ściśle tajne”; gromadzenia broni, materiałów wybuchowych lub radioaktywnych; fałszowania oraz obrotu fałszywymi pieniędzmi, środkami lub instrumentami płatniczymi albo zbywalnymi lub zbywalnymi dokumentami uprawniającymi do otrzymania sumy pieniężnej, towaru, ładunku albo wygranej rzeczowej albo zawierającymi obowiązek wpłaty kapitału, odsetek, udziału w zyskach lub stwierdzenie uczestnictwa w spółce; podrabiania lub przerabiania faktur lub używania faktur podrobionych lub przerobionych w zakresie okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym oraz wystawiania i używania faktur poświadczających nieprawdę co do okoliczności faktycznych mogących mieć znaczenie dla określenia wysokości należności publicznoprawnej lub jej zwrotu albo zwrotu innej należności o charakterze podatkowym; wytwarzania, przetwarzania, obrotu i przemytu środków odurzających, prekursorów, środków zastępczych lub substancji psychotropowych; zorganizowanej grupy przestępczej; mienia znacznej wartości; użycia przemocy lub groźby bezprawnej w związku z postępowaniem karnym; składania fałszywych zeznań oraz przedstawiania przez biegłego, rzeczoznawcę lub tłumacza fałszywej opinii, ekspertyzy lub tłumaczenia; fałszywego oskarżenia innej osoby o popełnienie przestępstwa, przestępstwa skarbowego lub wykroczenia skarbowego; tworzenia fałszywych dowodów lub innych podstępnych zabiegów, kierujących przeciwko innej osobie ściganie o przestępstwo, przestępstwo skarbowe lub wykroczenie skarbowe albo podejmowania takich zabiegów w toku postępowania; zatajenia dowodów niewinności osoby podejrzanej o popełnienie przestępstwa, przestępstwa skarbowego lub wykroczenia skarbowego; zawiadomienia organu powołanego do ścigania o niepopelnionym przestępstwie lub przestępstwie skarbowym; po-

do konkretnych czynów, które – w razie podejrzenia ich popełnienia – uprawniają do przeprowadzenia kontroli i utrwalenia treści rozmów.

Zastosowanie podsłuchu, w następstwie którego dojdzie do wkroczenia w sferę czyjejś prywatności, może być przede wszystkim uzasadnione wysoką wartością poznawczą stosowania tej metody, jak również znaczną skutecznością w zwalczaniu i zapobieganiu przestępczości, przy czym jeśli uzyskanie dowodu może nastąpić inną – niż zastosowanie podsłuchu – drogą, to należy zaniechać kontroli i utrwalania rozmów i zastosować tę odmienną metodę. Oznacza to, że zasady poszanowania prywatności znajdują zastosowanie nawet w stosunku do osób naruszających porządek prawny, wobec których w pierwszej kolejności powinno się zastosować metody jak najmniej dolegliwe. A zatem dopiero po spełnieniu określonych warunków proceduralnych osoby te powinny się liczyć z ingerencją władz w ich prywatność poprzez stosowanie podsłuchu.

Należy też wskazać, że zgodnie z art. 237 § 4 k.p.k. kontrola i utrwalanie treści rozmów telefonicznych są dopuszczalne w stosunku do osoby podejrzanej, oskarżonego, pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony albo która może mieć związek ze sprawcą lub z grożącym przestępstwem.

Jak zauważa Michał Błoński, opierając się na Postanowieniu Sądu Najwyższego z dnia 25 marca 2010 r. w sprawie I KZP 2/10³⁷, nieuprawnione byłoby założenie, że przyjęte w art. 237 § 1 k.p.k.³⁸ rozwiązanie ustawowe dopuszcza kontrolę wypowiedzi jednego tylko uczestnika rozmowy, tzn. wypowiedzi tylko tej osoby, która wymieniona została przez sąd w postanowieniu wydanym na podstawie art. 237 § 1 i 3 k.p.k. Tego rodzaju interpretacja prowadziłaby bowiem do absurdalnej sytuacji, w której procesowe wykorzystanie wypowiedzi rozmówcy takiej osoby zależałoby w każdym wypadku od wyrażenia przez sąd w tym względzie odrębnej zgody „następczej”³⁹.

plecznictwa; niezawiadomienia o przestępstwie; łapownictwa i płatnej protekcji; stręczycielstwa, kuplerstwa i sutenerstwa; przestępstw określonych w rozdz. XVI Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 2019, poz. 2460; Dz.U. 2020, poz. 374, 695 i 875) oraz w art. 5–8 Rzymskiego Statutu Międzynarodowego Trybunału Karnego, sporządzonego w Rzymie dnia 17 lipca 1998 r. (Dz.U. 2003, poz. 708; Dz. U. 2018, poz. 1753).

³⁷ Postanowienie Sądu Najwyższego z dnia 25 marca 2010 r. w sprawie I KZP 2/10. http://webcache.googleusercontent.com/search?q=cache:a_KbvEgslBAJ:www.policja.pl/download/1/74085/I-KZP-000210.pdf+&cd=1&hl=pl&ct=clnk&gl=pl [dostęp: 20.11.2021].

³⁸ Zgodnie z art. 237 § 1 k.p.k. po wszczęciu postępowania sąd na wniosek prokuratora może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa.

³⁹ M. BŁOŃSKI: *Zakres przedmiotowy i podmiotowy podsłuchu procesowego*. „Palestra” 2012, nr 7–8, s. 89.

Krytyczna ocena takiego stanowiska Sądu Najwyższego zakłada, że nieuprawnione jest rozszerzanie katalogu osób, wobec których dozwolone są kontrola i utrwalanie rozmów, bez wydania następczej zgody sądu, gdyż taki sposób postępowania może powodować naruszenie art. 237 § 4 k.p.k. poprzez stosowanie tej instytucji do osób tam nie wymienionych, a ponadto w takim przypadku dochodzi do naruszenia norm konstytucyjnych i konwencyjnych, w tym prawa do prywatności⁴⁰, z czym należy się zgodzić, mając na względzie konieczność zapewnienia ochrony prywatnej sfery osób podlegających kontroli i utrwalaniu rozmów.

Kwestia naruszenia tajemnicy komunikowania się, zwanej tajemnicą telekomunikacyjną, zajmuje ponadto art. 159 ust. 1 Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne⁴¹, zgodnie z którym tajemnica komunikowania się obejmuje szerokie spektrum danych, przykładowo: dane dotyczące użytkownika, treść indywidualnych komunikatów, dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, oznaczające wszelkie dane przetwarzane w sieci telekomunikacyjnej wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych, dane o lokalizacji.

Do naruszenia prywatności może także dojść wskutek śledzenia czyjejs lokalizacji przez organy ścigania. Zgodnie z art. 171 ust. 8 Prawa telekomunikacyjnego przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia służbom, które ustawowo są powołane do niesienia pomocy, dostępu do identyfikacji linii wywołującej oraz danych dotyczących lokalizacji, bez uprzedniej zgody zainteresowanych abonentów lub użytkowników, jeżeli jest to konieczne do umożliwienia tym służbom wykonywania ich zadań możliwie najbardziej efektywnie. Oznacza to, że osoba, której lokalizacja będzie tak śledzona, najczęściej nie będzie świadoma wdrożenia wobec niej tego rodzaju procedury. Co więcej, pozwala na to także art. 20 ust. 1d Ustawy z dnia 6 kwietnia 1990 – O Policji⁴², stanowiący o tym, że przetwarzanie informacji, w tym danych osobowych, przez Policję może mieć charakter niejawnny, odbywać się bez zgody i wiedzy osoby, której dane dotyczą, oraz z wykorzystaniem środków technicznych.

Policja jest bowiem uprawniona do przetwarzania wielorakich informacji, w tym danych osobowych, w zakresie niezbędnym do realizacji zadań ustawowych lub wykonywania uprawnień związanych z prowa-

⁴⁰ Ibidem.

⁴¹ Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Dz.U. 2004, nr 171, poz. 1800.

⁴² Ustawa z dnia 6 kwietnia 1990 r. – O Policji. T.j. Dz.U. 2021, poz. 1882.

dzeniem postępowań administracyjnych, realizacją czynności administracyjno-porządkowych oraz innych czynności, do których przeprowadzania funkcjonariusze Policji są uprawnieni na podstawie ustaw, w celach innych niż określone w art. 1 pkt. 1 Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości⁴³. Ponadto Policja dysponuje prawem przetwarzania danych osobowych, o których mowa w art. 9 i art. 10 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE⁴⁴, z wyłączeniem danych dotyczących kodu genetycznego.

Kwestia śledzenia danych o czyjejs lokalizacji zajmowała ponadto m.in. Rzecznika Praw Obywatelskich RP, który zwracał się o zajęcie stanowiska w tej kwestii do innych organów nie tylko na gruncie związanym ze zwalczaniem i zapobieganiem przestępczości⁴⁵.

Zbieranie informacji o obywatelach poprzez analizowanie dotyczących ich danych telekomunikacyjnych może prowadzić – w określonych sytuacjach – do naruszenia konstytucyjnych praw oraz wolności, w tym zwłaszcza prywatności osoby podlegającej inwigilacji.

Kwestie naruszenia granic prywatności w związku ze śledzeniem lokalizacji osoby podejrzanej bądź instalowaniem podsłuchów przez władze państwowe stały się przedmiotem analiz również ETPCz. Warto zwrócić uwagę na jeden z niedawnych wyroków Trybunału Sprawiedliwości Unii Europejskiej, z 2 marca 2021 r., wydany w sprawie C-746/18, którego treść niezwykle interesująco odnosi się do kwestii prywatności osób w sytuacjach związanych z dostępem organów władzy publicznej do zbioru danych o ruchu osób lub danych o lokalizacji osób.

Trybunał uznał bowiem, że dostęp – w celach karnych – do danych pochodzących z łączności elektronicznej i dotyczących ruchu lub lokalizacji, które pozwalają na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego, jest dozwolony jedynie w celu zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom bezpieczeństwa

⁴³ Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Dz.U. 2019, poz. 125.

⁴⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych...

⁴⁵ Zob. wystąpienie Rzecznika Praw Obywatelskich z dnia 15 kwietnia 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych w związku z możliwym naruszeniem prywatności przy stosowaniu aplikacji „Kwarantanna domowa”. <https://www.rpo.gov.pl/sites/default/files/Wyst%C4%85piecie%20do%20Prezesa%20UODO%2C%2015.04.2020.pdf> [dostęp: 26.05.2021].

publicznego. Prawo Unii Europejskiej stoi ponadto na przeszkodzie przepisom krajowym, przyznającym prokuraturze kompetencję udzielania zezwoleń na dostęp organu władzy publicznej do wspomnianych danych w celu prowadzenia postępowania przygotowawczego⁴⁶.

Zbieranie przez organy ścigania w drodze kontroli i utrwalania rozmów informacji o osobach podlegających takim czynnościom może dostarczać cennej wiedzy na temat życia prywatnego danej osoby na podstawie analizy wykonywanych przez tę osobę połączeń oraz w związku z badaniem lokalizacji użytkowanego przez nią urządzenia. Jednakże ingerencja władz publicznych w prywatność inwigilowanej osoby nie zawsze znajdzie uzasadnienie, nawet gdy celem jest zapobieganie lub zwalczanie przestępczości.

ETPCz wypowiedział się w kwestii kontrolowania przemieszczania się osoby a naruszenia jej prywatności także w innych orzeczeniach, np. w wyroku w sprawie Uzun przeciwko Niemcom⁴⁷. Między innymi stwierdzono, że w ocenie, czy w przypadku stosowania środków inwigilacji poza domem lub pomieszczeniami prywatnymi danej osoby wchodzi w grę jej życie prywatne, należy uwzględnić wiele elementów. Jednakże ogólną konkluzją ETPCz było stwierdzenie, że zbieranie danych o przemieszczaniu się danej osoby prowadzi do systematycznego zbierania i przechowywania danych o inwigilowanej osobie, stąd może prowadzić do naruszenia jej prywatności.

Słuszne wydaje się zatem stwierdzenie, że nie każda czynność podejrzenia popełnienia jednego z przestępstw ujętych w katalogu czynów w art. 237 § 3 k.p.k. uzasadniać będzie sięganie – zwłaszcza na etapie postępowania przygotowawczego – po dalece ingerującą w prywatność danej osoby inwigilację. ETPCz wskazał w szczególności na niebezpieczeństwo zbyt łatwego przekroczenia granic słusznej i uzasadnionej ingerencji w czyjąś prywatność przy nie do końca usprawiedliwionym i jasno sprecyzowanym celu prowadzonego postępowania, szczególnie na etapie przygotowawczym. Chodzi zwłaszcza o przestępstwa „łżejszej natury”, w związku z którymi ostateczny cel prowadzonego postępowania może okazać się zyskiem zbyt małym w stosunku do zbyt dużego ryzyka nakładów, jakie zostaną poniesione wskutek zastosowanej wobec danej osoby ingerencji w jej życie prywatne. Nie można także wykluczyć pośredniego oddzia-

⁴⁶ Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 2 marca 2021 r. – postępowanie karne przeciwko H.K. Skarga nr C-746/18; zob. też Trybunał Sprawiedliwości Unii Europejskiej. Komunikat prasowy nr 29/21. Luksemburg, 2 marca 2021 r. Wyrok w sprawie C-746/18 H.K./Prokuratuur. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-03/cp210029pl.pdf> [dostęp: 27.05.2021].

⁴⁷ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 września 2010 r. w sprawie Uzun przeciwko Niemcom. Skarga nr 35623/05. LEX nr 599284.

ływania na życie prywatne innych osób, z którymi „przy okazji” osoba sprawdzana będzie miała do czynienia, np. w trakcie prowadzonych rozmów telefonicznych bądź poprzez realizację kontaktu za pośrednictwem internetu.

Rzecznik Praw Obywatelskich zauważył, że polskie prawo nie spełnia wymogów wynikających z prawa Unii Europejskiej, które znalazły odzwierciedlenie w zaprezentowanym wyroku Trybunału Sprawiedliwości Unii Europejskiej. Uchwalona 15 stycznia 2016 r. nowelizacja Ustawy o zmianie ustawy o Policji i niektórych innych ustaw⁴⁸ dała służbom prawo do uzyskiwania danych telekomunikacyjnych, internetowych i pocztowych oraz do przetwarzania tych danych bez wiedzy i zgody osoby, której dotyczą, o czym też już wspomniano w niniejszym opracowaniu. Prawo to zostało przyznane w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych⁴⁹.

Biorąc pod uwagę art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Ponadto zgodnie z art. 49 zapewnia się wolność i ochronę tajemnicy komunikowania się. Ograniczenie tych praw może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej wskazany. Niezwykle istotne kwestie określa ponadto art. 51 Konstytucji RP, stanowiący o okolicznościach legalizujących ujawnienie danych osobowych zarówno ze strony osoby, której dane dotyczą, jak i ze strony władz publicznych gromadzących dane o obywatelach.

Do bardzo interesujących wniosków prowadzi ponadto sprawa Allen przeciwko Wielkiej Brytanii⁵⁰. Służby więzienne dokonały bowiem nagrania prywatnej rozmowy więźnia z przyjacielem w więziennej strefie odwiedzin, a także ze współwięźniem w celi. ETPCz uznał, że wykorzystywanie urządzeń nagrywających w celi i w strefie odwiedzin stanowiło ingerencję w prawo do prywatności. Trudno się dziwić takiej interpretacji ETPCz, skoro osadzeni co do zasady nie mają wpływu na miejsce odbywania rozmów, także i tych, które chcieliby zachować w poufności, a które mogą stać się przedmiotem niechcianej inwigilacji prowadzącej do zaingerowania w sferę prywatności.

⁴⁸ Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji i niektórych innych ustaw. Dz.U. 2016, poz. 147.

⁴⁹ Rzecznik Praw Obywatelskich. [Raport]. https://www.rpo.gov.pl/pl/raport_1/853 [dostęp: 15.04.2021].

⁵⁰ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 12 lipca 2013 r. w sprawie Allen przeciwko Wielkiej Brytanii. Skarga nr 25424/09.

Innym orzeczeniem rozstrzygającym na temat kontrolowania rozmów telefonicznych więźnia jest sprawa Doerga przeciwko Holandii⁵¹. Stan faktyczny sprawy dotyczył przekazanej policji przez Subhasa Ranbiera Doergę informacji o planowanej ucieczce trzech współwięźniów, którzy dodatkowo mieli planować wzięcie zakładników. W związku z tym rozpoczęto podsłuchiwanie i rejestrowanie rozmów telefonicznych prowadzonych przez Doergę. Podsłuchiwany zarzucił administracji penitencjarnej naruszenie art. 8 EKPCz, z czym zgodził się ETPCz poprzez stwierdzenie, że monitorowanie kontaktów więźniów ze światem zewnętrznym, w tym rozmów telefonicznych, bywa konieczne, ale regulujące to przepisy muszą być wystarczająco jasne i szczegółowe. Jak wyjaśnił Marek Nowicki, na gruncie prezentowanej sytuacji ETPCz stwierdził, że przepisom wchodzącym w grę w analizowanej sprawie zabrakło jasności i szczegółowości, a okólnikowi i wewnątrzwięziennym paragrafom – precyzji⁵².

Okoliczność znacznie ułatwionego dziś pozyskiwania danych w postaci nagrań rozmów dzięki postępowi technicznemu i praktycznie nieograniczonej dostępności do urządzeń rejestrujących nie uzasadnia zbierania tego rodzaju informacji bez legitymowania się ściśle określoną podstawą prawną. To bowiem nie tylko prowadzi do różnego rodzaju nadużyć, w tym także do ewidentnego naruszenia prawa do prywatności, lecz także stwarza niebezpieczeństwo rutynowego powtarzania tej praktyki, zwłaszcza względem osób, które dysponują ograniczonymi lub nieznacznymi możliwościami wyrażenia zgody na tego rodzaju metody pozyskiwania informacji lub ewentualnie sprzeciwienia się takim praktykom. Tym bardziej dotyczyć to będzie osób pozbawionych wolności, które często nie mają żadnej możliwości wpływania na sposób poszanowania granic ich prywatności przez osoby wykonujące wobec nich karę izolacyjną.

O wadze omawianego zagrożenia stanowi ponadto motyw 3 dyrektywy policyjnej, w którym wskazano, że technologia pozwala na przetwarzanie danych osobowych na niespotykaną dotąd skalę. Z tego można wywieść wnioski, że funkcjonowanie, dostępność oraz łatwość wykorzystania urządzeń rejestrujących aktywność danej osoby oraz przetwarzania w ten sposób jej danych mogą w tak samo prosty sposób prowadzić do przekroczenia granic czyjeś prywatności, m.in. gdy dotyczy to osób pozbawionych wolności, przy czym osobom tym nie można całkowicie odebrać prawa do jakiegokolwiek prywatności.

⁵¹ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 27 kwietnia 2004 r. w sprawie Doerga przeciwko Holandii. Skarga nr 50210/99; szerzej zob. M. Nowicki: *Nowy Europejski Trybunał Praw Człowieka. Wybór orzeczeń 1999–2004*. Kraków 2005, s. 896–898.

⁵² *Ibidem*, s. 898.

Ponadto w motywie 29 podkreślono konieczność zbierania danych w konkretnych, wyraźnych i prawnie uzasadnionych celach mieszczących się w zakresie zastosowania rzeczonyj dyrektywy, a zatem dane nie powinny być zbierane w celach niezgodnych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych i wykonywaniem kar, w tym z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom. Trzymając się zatem takiej interpretacji, wkraczanie w prywatność osoby będącej w zasięgu zainteresowania organów ścigania będzie uzasadnione, jeśli nie dojdzie do niego w celach nie związanych bezpośrednio ze zwalczaniem lub zapobieganiem przestępczości z uwzględnieniem wszelkich przesłanek zaingerowania w sferę prywatności.

4. Stosowanie monitoringu wizyjnego na terenie zakładów karnych oraz jego wpływ na sferę życia prywatnego osadzonych

Kwestii akceptowalnego przekroczenia granic prywatności więźnia nie sposób nie przedstawić w odniesieniu do rutynowo stosowanego monitoringu wizyjnego, zwłaszcza w zakładach karnych. Oznacza to, że w wielu sytuacjach stosowanie monitoringu wizyjnego w związku ze zwalczaniem i zapobieganiem przestępstwom wydaje się w pełni uzasadnione. Jednak przetwarzanie pozyskiwanych w ten sposób danych, zgodnie z motywem 26 dyrektywy policyjnej, musi się odbywać zgodnie z prawem, w sposób rzetelny i przejrzysty względem zainteresowanej osoby fizycznej oraz ma służyć wyłącznie konkretnym celom określonym prawem. Ustawodawca ponownie zwrócił uwagę na konieczność ograniczenia stosowania monitoringu wizyjnego wyłącznie do niezbędnych celów, co powinno mieć zastosowanie także na terenie zakładów karnych.

Interesujące w tym zakresie jest orzeczenie ETPCz z dnia 27 sierpnia 2019 r. w sprawie Izmestiew przeciwko Rosji⁵³. Skarżący został skazany na karę dożywotniego pozbawienia wolności. Jednym z jego zarzutów, jaki stał się przedmiotem rozpoznania przez ETPCz, było monitorowanie celi, w której przebywał przez całą dobę. W toku ustaleń stwierdzono, że krajowe przepisy, które miały regulować kwestię prawa do prywatności, nie zostały sformułowane dostatecznie jasno, co z kolei nie pozwalało na jednoznaczne stwierdzenie, czy stosowanie monitoringu wizyjnego powinno zostać ograniczone wyłącznie do przypadków niezbędnych w demokratycznym państwie. Sędziowie ETPCz zwrócili uwagę na to, że

⁵³ Wyrok Europejskiego Trybunału Praw Człowieka z 27 sierpnia 2019 r. w sprawie Izmestiew przeciwko Rosji. Skarga nr 74141/10.

rosyjski Trybunał Konstytucyjny stwierdził, iż stosowanie wobec osoby przebywającej w celi monitoringu wizyjnego stanowi naturalny skutek odbywania przez nią kary pozbawienia wolności, co można interpretować – zgodnie z wyrażoną przez autorów na początku artykułu wątpliwością – jako konsekwencję, a nawet dolegliwość, z jaką powinien liczyć się sprawca, który naruszył porządek prawny. Zgodnie ze stanowiskiem, jakie w tej kwestii zajął Sąd Najwyższy Federacji Rosyjskiej, osadzonego wystarczy jedynie poinformować, że stosuje się wobec niego monitoring wizyjny, nie jest zaś potrzebna jakakolwiek decyzja w tym zakresie, z czego można wywieść, że ewentualne nadmierne kontrolowanie życia więźnia, w tym nieodłącznie jego prywatności, stanowić będzie czynność realizowaną w zależności od norm przyjętych w danym zakładzie karnym.

Odnosząc się zatem do prezentowanego stanu faktycznego, ETPCz uznał, że prawo rosyjskie w obszarze odnoszącym się do kwestii stosowania monitoringu wizyjnego nie było wystarczająco precyzyjne i nie wskazywało w sposób konkretny, w jaki sposób władze krajowe mogą wykorzystywać monitoring wizyjny w odniesieniu do osób odbywających karę pozbawienia wolności, co mogło prowadzić, z jednej strony, do nadużyć, z drugiej zaś, do niezapewnienia skazanym minimalnego stopnia ochrony, który powinien być standardem w państwie prawa. Co więcej stwierdzono naruszenie art. 8 EKPCz.

Brzmienie tego wyroku może mieć znaczenie także dla polskich regulacji prawnych odnoszących się do stosowania monitoringu wizyjnego wobec osób pozbawionych wolności.

Kwestię stosowania monitoringu w polskich zakładach karnych reguluje art. 73a § 1 k.k.w., dający przyzwolenie na monitorowanie wizyjne lub foniczne zakładów karnych, co może się odbywać za pomocą wewnętrznego systemu urządzeń rejestrujących obraz lub dźwięk, a także z wykorzystaniem systemu telewizji przemysłowej.

Należy podzielić pogląd Moniki Niedźwieckiej, która zauważyła, że zastrzeżenie może budzić zbyt ogólne sformułowanie przesłanki zastosowania monitoringu, jaką jest zapewnienie bezpieczeństwa i porządku na terenie zakładu karnego⁵⁴. Zgodnie bowiem z brzmieniem art. 73a § 8 k.k.w., o stosowaniu monitorowania w określonych miejscach i pomieszczeniach decyduje dyrektor zakładu karnego, mając na celu zapewnienie porządku i bezpieczeństwa w zakładzie karnym. Jednocześnie nie wskazano, jakich środków wdrożenie mogłoby przyczynić się do zapewnienia co najmniej podstawowego poziomu bezpieczeństwa. W konsekwencji podejmowania decyzji w tym zakresie przez dyrektora zakładu

⁵⁴ M. NIEDŹWIECKA: *Monitoring jak środek zwiększający poziom bezpieczeństwa w zakładach karnych*. „Probacja” 2019, nr 4, s. 104.

karnego należy liczyć się z różnego rodzaju skutkami, w tym godzącymi w prywatność osadzonych.

W przeciwieństwie do monitoringu stosowanego powszechnie, monitorowanie więźniów w zakładach karnych może obejmować obszary takie jak: cele mieszkalne wraz z częścią przeznaczoną na cele sanitarno-higieniczne, łaźnie, pomieszczenia przeznaczone do obywatnia widzeń, miejsca zatrudnienia osadzonych, ciągi komunikacyjne, place spacerowe, miejsca służące do obserwacji terenu zakładu karnego na zewnątrz budynków oraz linie ogrodzenia zewnętrznego. Dozwolone jest ponadto monitorowanie w sytuacjach, w których mogą być widoczne intymne części ciała osoby skazanej, oraz podczas wykonywania przez nią intymnych czynności fizjologicznych. Wydaje się, że takie postępowanie w stopniu bardzo wysokim ingeruje w prywatność osoby skazanej. Istotne jest, że z monitorowania fonicznego wyłącza się informacje objęte tajemnicą spowiedzi lub tajemnicą prawnie chronioną. Brak jest natomiast konkretnych regulacji, jak zasady te miałyby być realizowane.

Monitorowaniu mogą także podlegać osoby znajdujące się w sferze zainteresowań organów ścigania w związku z podejrzeniem popełnienia przez nie przestępstwa, a zatem podejmujące określone działania w warunkach wolnościowych. W wyroku Perry przeciwko Wielkiej Brytanii⁵⁵ ETPCz stwierdził, że monitorowanie działań jednostki w miejscu publicznym za pomocą kamer nie prowadzi do ingerencji w życie prywatne, jak również że publikacja tak pozyskanego materiału w sposób wykraczający poza zwykłe jego wykorzystanie, do innych celów niż ochrona bezpieczeństwa, narusza zasadę poszanowania tej sfery życia.

W skardze skierowanej do Trybunału Stephen Perry zarzucił naruszenie prawa do poszanowania życia prywatnego poprzez tajne filmowanie go za pomocą kamery, do którego doszło na komisariacie policji. Obrazy z nagrania zostały później wykorzystane w toczącym się przeciwko niemu postępowaniu karnym. A zatem filmowanie i posłużenie się w procesie materiałem uzyskanym w ten sposób było ingerencją w życie prywatne, co potwierdził ETPCz, stwierdzając naruszenie art. 8 Konwencji i zarazem uwzględniając skargę Perry'ego.

Stosowanie monitoringu wizyjnego zwłaszcza na terenie zakładu karnego podyktowane jest przede wszystkim potrzebą zapewnienia bezpieczeństwa w miejscach narażonych na różnego rodzaju nadużycia.

Dzięki rozwojowi technologii forma sprawowania kontroli nad więźniami w postaci monitoringu staje się coraz bardziej powszechnym zja-

⁵⁵ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 lipca 2003 r. w sprawie Perry przeciwko Wielkiej Brytanii. Skarga nr 63737/00; szerzej zob. M. Nowicki: *Nowy Europejski Trybunał Praw Człowieka...*, s. 882–884.

wiskiem, które może także prowadzić do zbyt radykalnego wkroczenia w sferę prywatności osadzonych, skoro Kodeks karny wykonawczy pozwala nawet na monitorowanie najbardziej intymnych czynności realizowanych przez więźniów.

Zgodnie z raportem Krajowego Mechanizmu Prewencji z 2012 r. odnoszącym się do kwestii monitoringu wizyjnego w miejscach pozbawienia wolności⁵⁶ Rzecznik Praw Obywatelskich zwrócił uwagę na liczne skargi, które wpływały od osób pozbawionych wolności, a dotyczyły w dużej mierze stosowania kamer w celach mieszkalnych. Zanim do Kodeksu karnego wykonawczego wprowadzono regulacje dotyczące możliwości stosowania w jednostkach penitencjarnych monitoringu, kwestia ta była przedmiotem Rozporządzenia Ministra Sprawiedliwości z 31 października 2003 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej⁵⁷. Zgodnie ze wskazanym raportem wprowadzenie do Kodeksu karnego wykonawczego przepisów regulujących stosowanie wideonadzoru wobec skazanych i tymczasowo aresztowanych spowodowało nadanie ustawowego charakteru ingerencji państwa w prawo do prywatności⁵⁸.

Należy nadmienić, że osoby skazane nie mają co do zasady wpływu na stosowanie wobec nich monitoringu nawet w miejscach uchodzących za obszary silnie kojarzone ze sferą prywatności, jak choćby wspomniane już strefy spoczynku czy też miejsca wykonywania czynności fizjologicznych.

We wspomnianym raporcie Krajowego Mechanizmu Prewencji wskazano, że stosowanie metody nadzoru w postaci monitoringu niesie ryzyko potencjalnych i rzeczywistych nadużyć, m.in.: nieproporcjonalnego wykorzystywania jej w codziennej pracy (np. do kontrolowania wszystkich aspektów życia człowieka, nawet jeśli nie ma to wpływu na bezpieczeństwo), zastępowania monitoringiem bezpośredniego kontaktu z człowiekiem, udostępniania obrazu z kamer osobom nie posiadającym kompetencji, niewłaściwego zabezpieczenia danych z monitoringu.

W opinii autorów przedstawione sytuacje stwarzają mogą pole do nadmiernego – zarówno świadomego, jak i nieświadomego – przekraczania granic prywatności osób pozbawionych wolności, wobec czego ingerencja taka, skoro musi zostać przeprowadzona, powinna się odbywać w sposób możliwie najmniej dotkliwy, jak również z uwzględnieniem

⁵⁶ Zob. *Monitoring wizyjny w miejscach pozbawienia wolności. Raport Krajowego Mechanizmu Prewencji*. Warszawa 2012. <https://www.rpo.gov.pl/sites/default/files/Raport%20monitoring%20wizyjny.pdf> [dostęp: 30.05.2021].

⁵⁷ Rozporządzenie Ministra Sprawiedliwości z dnia 31 października 2003 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej. Dz.U. 2003, nr 194, poz. 1902, ze zm.

⁵⁸ Zob. *Monitoring wizyjny w miejscach pozbawienia wolności...*

zasad wynikających m.in. z dyrektywy policyjnej, wskazującej w szczególności na taką formę przetwarzania danych, która powinna być zgodna z prawem, rzetelna i przejrzysta względem osób fizycznych oraz powinna służyć wyłącznie konkretnym celom określonym prawem. Oznacza to, że sposób, cel oraz zasięg stosowania monitoringu wizyjnego powinny być uzależnione nie tylko od rodzaju monitorowanego miejsca, ale także od kategorii skazanych podlegających monitorowaniu. Powinny być zatem odmienne w wypadku tymczasowo aresztowanych, skazanych na karę dożywotniego pozbawienia wolności czy też osób nie wymagających stosowania wobec nich wzmoczonego dozoru.

W opinii autorów – w próbie oceny ewentualnych postulatów zmian w zakresie stosowania monitoringu wizyjnego na terenie zakładów karnych – znacznie może mieć zbyt ogólna konstrukcja przepisów Kodeksu karnego wykonawczego odnoszących się do warunków, w jakich dyrektor danego zakładu karnego autonomicznie podejmuje decyzje dotyczące sposobu monitorowania osadzonych. Zgodnie bowiem z art. 73 a § 8 k.k.w. o stosowaniu monitorowania w określonych miejscach i pomieszczeniach decyduje dyrektor zakładu karnego, mając na celu zapewnienie porządku i bezpieczeństwa w zakładzie karnym

Podsumowanie

Prawo do prywatności, które w literaturze nie doczekało się dokładnego zdefiniowania, stanowi fundamentalne prawo każdego człowieka do samostanowienia. Niezwykle istotnym atrybutem prywatności każdej osoby jest jej nietykalność oraz wolność, dzięki którym każda niezależna osoba ma możliwość autonomicznego podejmowania decyzji o własnej najbardziej intymnej sferze oraz o tym, kto w tę sferę może wkroczyć, jak również w jakim stopniu. Swobodą tą nie dysponują lub dysponują w bardzo ograniczonym zakresie w szczególności osoby odbywające karę pozbawienia wolności. Naruszenie prywatności osób obserwowanych przez organy ścigania może mieć swoje początki już na etapie podejmowania czynności operacyjno-rozpoznawczych.

Natomiast granicą możliwej do zaakceptowania ingerencji w prywatność osób w związku ze zwalczaniem i zapobieganiem przestępczości może być zbieranie takich informacji, które w pewnym momencie okażą się wystarczające dla osiągnięcia celu danego postępowania. Oznacza to, że nie jest dopuszczalne, jak to miało miejsce we wspomnianej sprawie Panteleyenko przeciwko Ukrainie, zbieranie informacji wszelkich, zwłaszcza tych, które nie mają związku z interesującą organy kwestią, a pozostają w sferze informacji uznawanych za wrażliwe, wysoce poufne,

dotyczące m.in. osobistych poglądów na newralgiczne tematy czy zdrowia psychicznego. A zatem każde nadmierne i nie poparte celem związanym z daną czynnością zbieranie informacji może oznaczać nieuprawnione naruszenie granic czyjejs prywatności.

W opinii autorów najpoważniejsze niebezpieczeństwo dla nadmiernego naruszenia granic prywatności może dotyczyć w szczególności osób pozbawionych wolności, które często nie tylko nie są świadome swoich praw, ale także nie mają żadnego wpływu na stosowane wobec nich środki inwigilacji. Kwestią równie newralgiczną, lecz wymagającą przedsięwzięcia odrębnej analizy ze względu na wielowątkowość tego zagadnienia, będzie sposób wykonywania czynności związanych z procesem zapobiegania i zwalczania przestępczości, m.in. realizowania kary pozbawienia wolności wobec kobiet, w tym matek, znacznie trudniej niż mężczyźni znoszących izolację od społeczeństwa, szczególnie w sferze prywatności oraz intymności.

Biorąc pod uwagę złożoność prezentowanej tematyki w powiązaniu z możliwym przekroczeniem bariery prywatności wskutek podejmowanych przez organy ścigania czynności, pożądaną praktyką – w tworzeniu regulacji prawnych odnoszących się do właściwego posługiwania się środkami służącymi inwigilowaniu – mogłoby być poleganie na opiniach ekspertów, zanim dojdzie do wdrożenia uregulowań prawnych odnoszących się do ograniczania konstytucyjnie chronionych praw oraz podstawowych wolności. Warto nadmienić, że duże znaczenie może mieć zwłaszcza umiejętność właściwego stosowania rozwiązań technicznych służących monitorowaniu osób w formie wizji, fonii, śledzenia lokalizacji czy też zakładania podsłuchów, którego wyniki następnie mogą być utrwalane za pomocą określonych metod i sprzętów w celu późniejszego odtworzenia. Dla ochrony prywatności kluczowe znaczenie będzie mieć – na tym gruncie – właściwe zabezpieczenie utrwalonych danych przed możliwą ingerencją niepożądanych osób, jak również umiejętność zapobiegnięcia wyciekowi informacji mogącemu narazić osoby, których dane dotyczą, na znaczne naruszenie prawa do prywatności, wskutek utraty kontroli nad zebranymi danymi.

Bardzo cennych uwag w przedmiocie nadmiernego przekroczenia granic prywatności w stosunku do osadzonych dostarcza wspomniany raport Krajowego Mechanizmu Prewencji z 2012 r., w którym wskazano na grupę problemów związanych ze stosowaniem monitoringu w miejscach pozbawienia wolności, dotyczących nie tylko zakładów karnych, ale także izb wytrzeźwień, policyjnych izb dziecka czy zakładów poprawczych.

Na kwestię znacznego niebezpieczeństwa związanego z gromadzeniem i wykorzystaniem materiałów zebranych w postępowaniu karnym

prowadzącymi nieuchronnie do naruszenia prywatności wskazuje także Zdzisław Brodzisz, zwracając uwagę na wystąpienie sytuacji wręcz rażącego naruszenia prywatności przez – formalnie zgodne z literą prawa – stosowanie podsłuchu w sferze ściśle osobistej lub wykorzystywanie dowodowe uzyskanych tą drogą materiałów⁵⁹.

W szczególności miały to być upublicznione przez media przypadki udostępnienia z akt sprawy karnej i wykorzystania w procesie cywilnym zapisów prywatnych rozmów uzyskanych w drodze podsłuchu⁶⁰, pozostawiania w aktach spraw zapisów prywatnych rozmów osób związanych więzami rodzinnymi o treści nie mającej znaczenia dla prowadzonego postępowania karnego⁶¹ lub wykorzystania w procesie karnym przeciwko osobie faktycznie pokrzywdzonej, jako dowodu popełnienia przez nią występku o niewielkim ciężarze gatunkowym, prywatnego, nielegalnego i sporządzonego w celu szantażu nagrania zawierającego treści jednoznacznie intymne⁶².

Konkluzją niniejszej analizy jest ponadto kwestia uznania, czy w danej sytuacji pierwszorzędного znaczenia powinno nabrać dobro ogólne czy też indywidualne prawo każdego człowieka do zachowania informacji mieszczących się w sferze własnej prywatności wyłącznie dla siebie, zwłaszcza w odniesieniu do art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, jak również określonego w art. 47 Konstytucji RP prawa do ochrony życia prywatnego. Zaprezentowane uwagi miały również prowadzić do wskazania obszarów potencjalnie najbardziej zagrożonych ingerencją władz publicznych w sferę prywatności w trakcie wykonywania przez nie zadań związanych z zapobieganiem i zwalczaniem przestępczości. Rozważania nie pozwoliły jednak na precyzyjne wyodrębnienie momentu, który mógłby zostać uznany za przekroczenie granic prywatności w realizacji wspomnianych celów w procesie zwalczania przestępczości oraz zapobiegania jej skutkom. Prywatność danej osoby jest bowiem dobrem ściśle indywidualnym, zaś przekroczenie akceptowalnych granic zaingerowania w jej prywatność będzie wymagało pogłębionej analizy, aby rzeczony moment móc jak najbardziej precyzyjnie określić.

⁵⁹ Z. BRODZISZ: *Ochrona prywatności w procesie karnym – porównanie regulacji prawnych polskich i niemieckich*. „Prokuratura i Prawo” 2013, nr 4, s. 39.

⁶⁰ *Śledztwo ws. podsłuchów dziennikarzy*. „Gazeta Wyborcza” 24.03.2010.

⁶¹ B. WRÓBLEWSKI: *Mąż i żona na podsłuchu*. „Gazeta Wyborcza” 17.03.2010.

⁶² *Z Senatu do więzienia? Wygaśł immunitet, wraca śledztwo*. Dziennik.pl, 14.11.2011. <https://wiadomosci.dziennik.pl/wydarzenia/artykuly/366418,krzysztof-piesiewicz-bedzie-przesluchany-ws-narkotykow-wraca-sledztwo.html> [dostęp: 16.11.2021].

Bibliografia

Literatura

- BŁOŃSKI M.: *Zakres przedmiotowy i podmiotowy podstuchu procesowego*. „Palestra” 2012, nr 7–8.
- BRODZISZ Z.: *Ochrona prywatności w procesie karnym – porównanie regulacji prawnych polskich i niemieckich*. „Prokuratura i Prawo” 2013, nr 4.
- CICHUTA J.: *Prawo do prywatności jako pochodna poglądów antropologicznych*. W: IDEM: *Prawo do prywatności – współczesne wyzwania*. Warszawa 2019.
- GRZELAK A.: *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*. Warszawa 2015.
- MIELNIK Z.: *Prawo do prywatności (zagadnienia wybrane)*. „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 1996, R. 58, z. 2.
- NIEDŹWIECKA M.: *Monitoring jak środek zwiększający poziom bezpieczeństwa w zakładach karnych*. „Probacja” 2019, nr 4.
- NOWICKI M.: *Nowy Europejski Trybunał Praw Człowieka. Wybór orzeczeń 1999–2004*. Kraków 2005.
- PRYCIĄK M.: *Prawo do prywatności*. „Studia Erasmiana Wratislaviensia” 2010, z. 4.
- PYKA A.: *Przetwarzanie danych biometrycznych. Aspekty prawne*. „Studia Prawa Publicznego” 2018, nr 3 (23).
- ROAGNA I.: *Ochrona prawa do poszanowania życia prywatnego i rodzinnego w Europejskiej Konwencji o Ochronie Praw Człowieka*. Strasburg 2012.
- RUCHAŁA S.: „Współczesne filozoficzne spory o ugruntowanie praw człowieka”. Rozprawa doktorska. Opieka nauk. prof. dr hab. K. ŚLĘCZKA. Uniwersytet Śląski w Katowicach, Wydział Nauk Społecznych, Instytut Filozofii. Katowice 2006.
- RZUCIDŁO J.: *Prawo do prywatności i ochrona danych osobowych*. W: *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*. Red. M. JABŁOŃSKI. Wrocław 2014.
- STRÖMHOLM S.: *Right of privacy and rights of the personality. A comparative survey*. Stockholm 1967. <https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf> [dostęp: 24.11.2021].
- Śledztwo ws. podstuchów dziennikarzy. „Gazeta Wyborcza” 24.03.2010.
- WRÓBLEWSKI B.: *Mąż i żona na podstuchu*. „Gazeta Wyborcza” 17.03.2010.

Akty prawne

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz.U. 1997, nr 78, poz. 483.
- Ustawa z dnia 6 kwietnia 1990 r. – O Policji. T.j. Dz.U. 2021, poz. 1882.
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy. Dz.U. 1997, nr 90, poz. 55.
- Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego. T.j. Dz.U. 2021, poz. 534.

- Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym. Dz.U. 2000, nr 50, poz. 580.
- Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Dz.U. 2004, nr 171, poz. 1800.
- Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji i niektórych innych ustaw. Dz.U. 2016, poz. 147.
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Dz.U. 2019, poz. 125.
- Powszechna Deklaracja Praw Człowieka. Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana w dniu 10 grudnia 1948 r.
- Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. Dz.U. 1977, nr 38, poz. 167.
- Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. Dz.U. 1993, nr 61, poz. 284.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.U. UE 4.5.2016, L 119/1.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW. Dz.U. UE 4.5.2016, L 119/89.
- Rozporządzenie Ministra Sprawiedliwości z dnia 31 października 2003 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej. Dz.U. 2003, nr 194, poz. 1902, ze zm.

Orzecznictwo

- Wyrok Trybunału Konstytucyjnego z dnia 5 marca 2013 r. U 2/11. OTK-A 2013, nr 3, poz. 24. Dz.U. 2013, poz. 375.
- Wyrok Sądu Apelacyjnego w Katowicach z dnia 20 września 2012 r. V ACA 378/12. LEX nr 1220491.
- Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 października 2020 r. VII SA/Wa 449/20. LEX nr 3152730.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 maja 2000 r. w sprawie Rotaru przeciwko Rumunii. Skarga nr 28341/95.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 września 2000 r. w sprawie Messina przeciwko Włochom. Skarga nr 25498/94.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 lipca 2003 r. w sprawie Perry przeciwko Wielkiej Brytanii. Skarga nr 63737/00.

- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 27 kwietnia 2004 r. w sprawie Doerga przeciwko Holandii. Skarga nr 50210/99.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 29 czerwca 2006 r. w sprawie Panteleyenکو przeciwko Ukrainie. Skarga nr 11901/02. LEX nr 182356.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 grudnia 2008 r. w sprawie S. i Marper przeciwko Wielkiej Brytanii. Skarga nr 30562/04 i 30566/04.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 września 2010 r. w sprawie Uzun przeciwko Niemcom. Skarga nr 35623/05. LEX nr 599284.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 12 lipca 2013 r. w sprawie Allen przeciwko Wielkiej Brytanii. Skarga nr 25424/09.
- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 27 sierpnia 2019 r. w sprawie Izmestiew przeciwko Rosji. Skarga nr 74141/10.
- Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 2 marca 2021 r. – postępowanie karne przeciwko H.K. Sprawa C-746/18.

Źródła internetowe

- CZARNECKI P., ŚWIATŁOWSKI A.: *Prawo do prywatności i zasada prawdy materialnej w kontekście pozyskiwania informacji relewantnych procesowo*. [Publikacja powstała w wyniku realizacji projektu badawczego o nr 2013/08/M/HS5/00038 finansowanego ze środków Narodowego Centrum Nauki]. <https://www.law.uj.edu.pl/~kpk/dowody/wp-content/uploads/2014/03/Prawo-do-prywatno%C5%9Bci-merytoryczna.pdf> [dostęp: 26.05.2021].
- JONASSON U.: *Om Stig Strömholm – “En vis norrbottning och hans nation”*. 6.04.2015. <http://jonassonulf.blogspot.com/2015/04/om-stig-stromholm-en-vis-norrbottning.html> [dostęp: 24.11.2021].
- ŁĘTOWSKA E.: *Prawo do prywatności w Europie*. [Materiały edukacyjne przygotowane w ramach programu Socrates Grundtvig Action I, Law through Experience/116881-CP-1-2004-SK-GRUNDTVIG-G11]. http://www.psep.pl/grundtvig/6/prawo_do_prywatnosci.pdf [dostęp: 29.05.2021].
- Monitoring wizyjny w miejscach pozbawienia wolności. Raport Krajowego Mechanizmu Prewencji*. Warszawa 2012. <https://www.rpo.gov.pl/sites/default/files/Raport%20monitoring%20wizytjny.pdf> [dostęp: 30.05.2021].
- Postanowienie Sądu Najwyższego z dnia 25 marca 2010 r. w sprawie I KZP 2/10. http://webcache.googleusercontent.com/search?q=cache:a_KbvEgslBAJ:www.policja.pl/download/1/74085/I-KZP-000210.pdf+&cd=1&hl=pl&ct=clnk&gl=pl [dostęp: 20.11.2021].
- Rzecznik Praw Obywatelskich. [Raport]. https://www.rpo.gov.pl/pl/raport_1/853 [dostęp: 15.04.2021].
- Stig Strömholm*. https://sv.wikipedia.org/wiki/Stig_Str%C3%B6mholm [dostęp: 24.11.2021].
- Trybunał Sprawiedliwości Unii Europejskiej. Komunikat prasowy nr 29/21. Luksemburg, 2 marca 2021 r. Wyrok w sprawie C-746/18H.K./Prokuratuur. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-03/cp210029pl.pdf> [dostęp: 27.05.2021].

- Wystąpienie Rzecznika Praw Obywatelskich z dnia 15 kwietnia 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych w związku z możliwym naruszeniem prywatności przy stosowaniu aplikacji „Kwarantanna domowa”. <https://www.rpo.gov.pl/sites/default/files/Wyst%C4%85pienie%20do%20Prezesa%20UODO%2C%2015.04.2020.pdf> [dostęp: 26.05.2021].
- Z Senatu do więzienia? Wygaś immunitet, wraca śledztwo.* Dziennik.pl, 14.11.2011. <https://wiadomosci.dziennik.pl/wydarzenia/artykuly/366418,krzysztof-piesiewicz-bedzie-przegluchany-ws-narkotykow-wraca-sledztwo.html> [dostęp: 16.11.2021].