PRAWO DO OCHRONY DANYCH OSOBOWYCH

Redakcja
WERONIKA ANNA ŁOWICKA, MIKOŁAJ BRZÓSTOWICZ,
WIKTORIA GIBAŁA, NATALIA ZALEWSKA

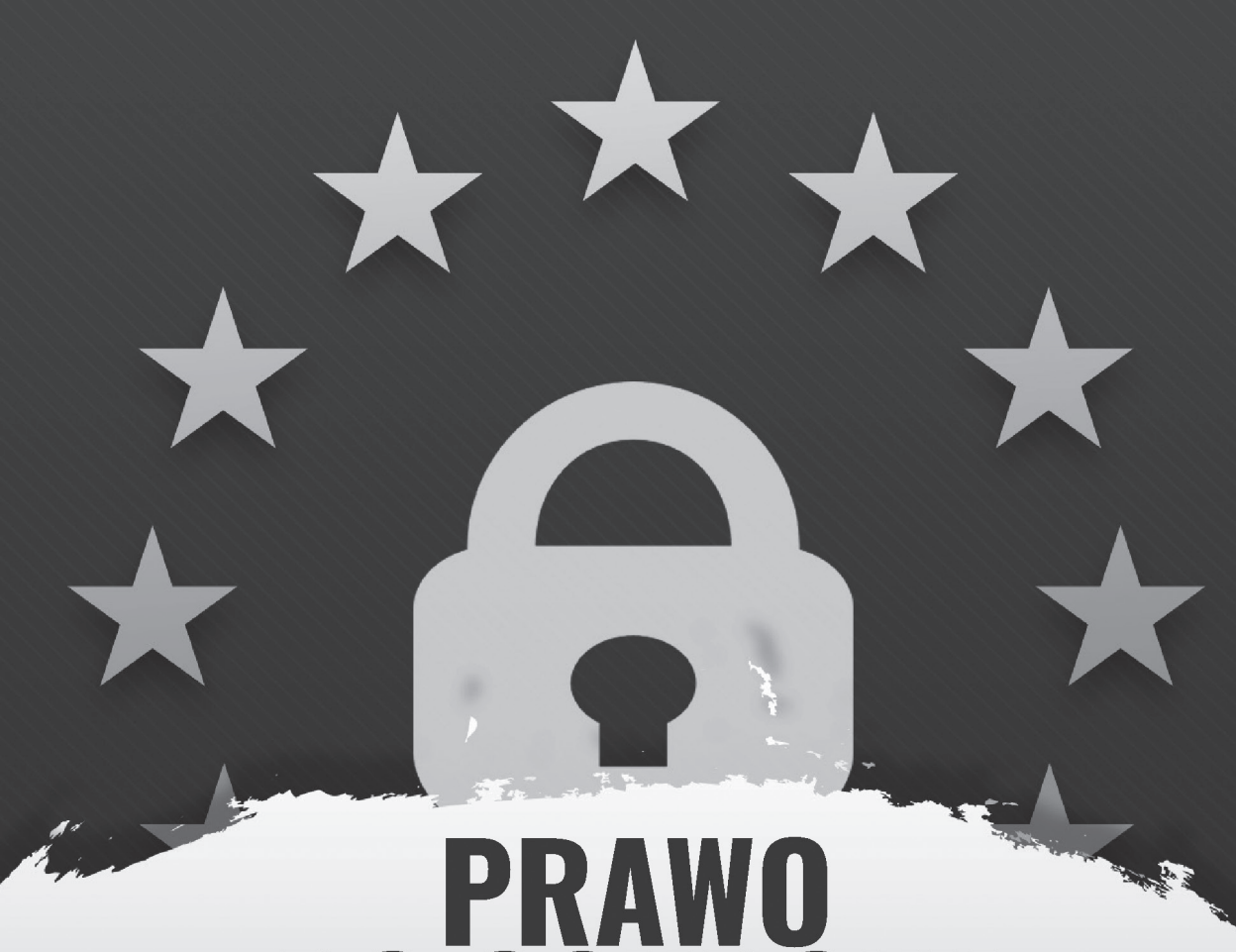
Studenckie Koło Naukowe
Ochrony Danych Osobowych

ARCHAEGRAPH
Wydawnictwo Naukowe

Prawo
do ochrony danych osobowych

Redakcja

weronika anna łowicka, mikołaj brzóstowicz,
wiktoria gibała, natalia zalewska



PRAWO DO OCHRONY DANYCH OSOBOWYCH

Redakcja
WERONIKA ANNA ŁOWICKA, MIKOŁAJ BRZÓSTOWICZ,
WIKTORIA GIBAŁA, NATALIA ZALEWSKA

Studenckie Koło Naukowe
Ochrony Danych Osobowych

ARCHAEGRAPH
Wydawnictwo Naukowe

REDAKCJA:
WERONIKA ANNA ŁOWICKA, MIKOŁAJ BRZÓSTOWICZ,
WIKTORIA GIBAŁA, NATALIA ZALEWSKA

RECENZJA:
DR HAB. MARZENA SZABŁOWSKA-JUCKIEWICZ, PROF. UMK
DR NATALIA DAŚKO
DR KRZYSZTOF KUCHARSKI

KOREKTA REDAKTORSKA, SKŁAD I PROJEKT OKŁADKI
KAROL ŁUKOMIAK

Monografia powstała z inicjatywy

Studenckie Koło Naukowe
Ochrony Danych Osobowych

ISBN: 978-83-67959-67-4

Wersja elektroniczna dostępna na stronie internetowej wydawcy:
www.archaegraph.pl

ARCHAEGRAPH
Wydawnictwo Naukowe

ŁÓDŹ, SIERPIEŃ 2024

SPIS TREŚCI

PRAWO KARNE

PRAWO PRACY

PRAWO PRZEDSIĘBIORCÓW

WIRTUALNY ŚWIAT

Klaudia Modrzejewska

Uniwersytet im. Adama Mickiewicza w Poznaniu

Studentka

OCHRONA DANYCH OSOBOWYCH W SPRAWACH KARNYCH. ISTOTA WPROWADZENIA UJEDNOLICONEGO STANDARDU PRZETWARZANIA DANYCH OSOBOWYCH W KONTEKŚCIE ŚCIGANIA PRZESTĘPSTW NA OBSZARZE PAŃSTW CZŁONKOWSKICH UNII EUROPEJSKIEJ

Wstęp

Od kilku lat obserwujemy dynamiczny postęp technologiczny. Ma on niewątpliwie wiele zalet, ale również wad. Rozwój technologii informacyjnych sprawił, że gromadzenie i przetwarzanie danych na dużą skalę jeszcze nigdy nie było tak łatwe. Jest to o tyle istotne, iż współczesne społeczeństwo można określić mianem „społeczeństwa informacyjnego". Kluczowym aspektem jest swobodny przepływ informacji. Warto podkreślić, iż wśród rozmaitych gromadzonych informacji najważniejsze są dane odnoszące się do osób fizycznych.

Obecnie przetwarzanie danych osobowych to nieodłączny element ludzkiego życia. To zagadnienie jest związane z każdą wykonywaną działalnością. Jako zaletę najczęściej wymienia się możliwość sprawniejszego dopełnienia spraw administracyjnych. Jednocześnie to skłania do gromadzenia i przechowywania rozmaitych danych osobowych w sposób zautomatyzowany. Pociąga to za sobą wiele niebezpieczeństw. Wśród nich możemy wyróżnić wzrost zagrożenia ochrony

prywatności, jak i ryzyko niezgodnego z prawem przetwarzania pozyskanych danych (Fajgielski 2019, s. 15).

Odpowiedzią na zagrożenia wynikające z gromadzenia i przechowywania tychże informacji są niewątpliwie różnorodne akty prawne, które mają zapewnić tak potrzebną ochronę podmiotom danych.

W tym miejscu należy podkreślić, że ochrona prawna danych osobowych wywodzi się z prawa do prywatności. Prawo do prywatności zostało uznane przez społeczeństwa za podstawowe prawo człowieka. Na przestrzeni lat powstało mnóstwo aktów normatywnych, które w rozmaity sposób gwarantowały ochronę prywatności. Została ona wyrażona m.in. w Powszechnej Deklaracji Praw Człowieka, co podkreśla, jak ważne jest to prawo (Motyka 1999, s. 73 - 75).

Za pierwszą ustawę o ochronie danych osobowych uznaje się ustawę uchwaloną w 1970 r. w Hesji, czyli w jednym z landów niemieckich. Natomiast pierwszą ogólnokrajową ustawę uchwalono w Szwecji w 1973 r. (Jagielski 2010, s. 10).

W następnych latach regulacje prawne w zakresie ochrony danych osobowych uchwalono w takich krajach Europy Zachodniej, jak Republika Federalna Niemiec, Austria, czy Luksemburg (Borecka 2006, s. 9).

Z powyższych względów uznaje się, iż początki ochrony prawnej danych osobowych sięgają lat 70. XX w. Zatem jest to dość młoda dziedzina prawa. Aczkolwiek dynamicznie się rozwija i z każdym kolejnym rokiem zyskuje na znaczeniu.

Jednakże, same krajowe regulacje nie wystarczały. Okazywały się za mało skuteczne, co prowadziło do ogromnych problemów prawnych. Aby należycie chronić osoby fizyczne przed niewłaściwym wykorzystywaniem gromadzonych danych osobowych, zdecydowano się uregulować to zagadnienie na poziomie unijnym. Kilka lat temu przeprowadzono istotną reformę, która zmieniła dotychczasowy porządek prawny. Efektem końcowym było wprowadzenie jednolitego standardu ochrony danych osobowych w państwach członkowskich. Natomiast przepisy krajowe mają charakter uzupełniający (Wróbel 2017, s. 40 – 41).

Zwiększona dostępność do danych osobowych wpływała pozytywnie na działanie organów zajmujących się ściganiem i zwalczaniem przestępczości. Z tego względu pojawiła się pilna potrzeba wprowadzenia aktu prawnego, który zapewni ujednolicony standard przetwarzania danych osobowych w ściganiu przestępstw na terenie całej Unii Europejskiej oraz wprowadzenia swoistego standardu jakości danych osobowych. W tym celu powstała Dyrektywa 2016/680 z 27 kwietnia 2016 roku 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 uchylająca decyzję ramową Rady 2008/977/WSiSW.

W mojej pracy skupię się przede wszystkim na zagadnieniu dotyczącym ochrony danych osobowych w sprawach karnych. Wyjaśnię cel i istotę wprowadzenia ujednoliconego standardu przetwarzania danych osobowych w ramach ścigania przestępstw na obszarze państw członkowskich Unii Europejskiej.

Pojęcie ochrony danych osobowych

Sformułowanie ochrona danych osobowych to nazwa powszechnie wykorzystywana, lecz nieprecyzyjna. Jest to nic innego jak skrót pojęciowy. Tak naprawdę pełna nazwa to ochrona osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem danych. Takie sformułowanie wyraźnie wskazuje podmiot ochrony i jednocześnie określa istotę regulacji. Celem ochrony są nie tylko dane odnoszące się do osób fizycznych, lecz ochrona osób, których dane są poddawane przetwarzaniu (Fajgielski 2019, s. 20).

Jeszcze do niedawna ochronę danych osobowych określano jako istotny element ochrony prywatności, z której się wywodzi. Obecnie mówimy już o wyodrębnionej dziedzinie prawa.

Ochrona danych osobowych obejmuje regulacje prawne mające na celu skuteczną ochronę osób, których dane są poddawane przetwarzaniu. W szerszym rozumieniu tego pojęcia obejmuje również kwestię zabezpieczenia danych, czyli określenie w formie przepisów prawnych wymogów dotyczących rozwiązań technicznych i organizacyjnych. Celem wdrożenia tych rozwiązań jest zapewnienie przetwarzania danych osobowych zgodnie z prawem.

Reasumując, prawo ochrony danych osobowych to całokształt przepisów prawnych regulujących przetwarzanie i ochronę danych osobowych. Co istotne, są to przepisy prawne zawarte w różnego rodzaju aktach normatywnych. Wśród nich wyróżniamy przepisy konstytucyjne, przepisy z zakresu prawa unijnego, przepisy krajowe oraz akty wykonawcze.

Istota wprowadzenia minimalnego standardu w sprawach karnych

Prawo do ochrony danych osobowych jest prawem podstawowym, określonym w art. 8 Karty Praw Podstawowych. Wraz z rozwojem technologicznym wzrosła potrzeba opracowywania nowych instrumentów prawnych gwarantujących ochronę tego prawa.

Jednocześnie łatwiejszy dostęp do dużej ilości danych, w tym wydarzeń z przeszłości jest istotnym elementem pracy organów ścigania i zwalczania przestępczości. Co więcej, sami dostawcy usług mogą udostępniać tym organom gromadzone w ramach swojej działalności informacje o konkretnych osobach do prowadzonych postępowań karnych.

Należy uświadomić sobie ogromną skalę przetwarzania danych osobowych w sprawach karnych. Dostęp do informacji nie ogranicza się jedynie do spraw i organów krajowych. Jest on znacznie szerszy, gdyż dostęp posiadają organy ścigania państw członkowskich Unii Europejskiej. Obecnie informacje dostępne dla organów ścigania w jednym państwie członkowskim UE są na podstawie przepisów o interoperacyjności systemów informacyjnych, udostępniane również organom ścigania w innych krajach członkowskich (Boniec – Błaszczyk 2021, s. 29).

Wśród systemów służących do wymiany informacji znajdują się między innymi SIS (Schengen Information System), SIENA (Secure Information Exchange Network Application), PNR (Passenger Name Record), ETIAS (European Travel Information and Authorisation System) czy wizowy system informacyjny VIS (Visa Information System) (Gajda 2019, s. 147 - 150).

Obszar ochrony danych osobowych podlegał już wcześniej regulacjom prawnym. Od 2008 roku aż do wejścia w życie dyrektywy 2016/680 obowiązywała decyzja ramowa Rady 2008/977/WSiSW z 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Aczkolwiek ta decyzja miała dość ograniczony zakres. Dotyczyła wyłącznie przetwarzania danych osobowych udostępnianych czy też przesyłanych pomiędzy państwami członkowskimi Unii Europejskiej. Z tego względu nie miała zastosowania do wszelkich danych gromadzonych w ramach spraw o zasięgu krajowym.

Ograniczony zakres decyzji ramowej wynikał przede wszystkim z braku kompetencji UE do wprowadzenia jednolitego standardu przetwarzania danych na poziomie krajowym. Sytuacja uległa zmianie z chwilą wejścia w życie traktatu z Lizbony. Art. 16 dał jednoznaczną podstawę do podjęcia legislacyjnych działań zmierzających do ujednolicenia standardu przetwarzania danych osobowych na gruncie unijnym, a w konsekwencji do powstania dyrektywy 2016/680 (Gutierrez Zarza 2015, s. 23–29).

Wraz z dynamicznym wzrostem znaczenia danych osobowych, a także sposobów ich gromadzenia pojawiła się konieczność wprowadzenia minimalnego standardu przetwarzania danych osobowych w ściganiu przestępstw w UE, czego wyrazem stała się dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW.

Czynności podejmowane przez organy ścigania należy określić mianem szczególnych, które uzasadniają indywidualne podejście unijnego ustawodawcy do tejże kwestii oraz utworzenie odrębnego aktu prawnego. Nadto, stopień ochrony danych wprowadzony dyrektywą 2016/680 ma sprzyjać budowaniu wzajemnego zaufania, koniecznego do realizacji współpracy europejskiej w sprawach karnych.

Zakres podmiotowy i przedmiotowy dyrektywy 2016/680

Zakres zastosowania dyrektywy 2016/680 określają dwa kryteria: podmiotowe, tj. dotyczące wskazania właściwych organów przetwarzających dane oraz przedmiotowe, czyli odpowiadające wskazanym w niej celom.

Zakres podmiotowy został wskazany w art. 3 pkt. 7 dyrektywy. Zawiera on definicję opisową „organów właściwych". Poprzez nie rozumiemy organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom lub inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Natomiast zakres przedmiotowy został określony w art. 1 ust. 1 dyrektywy. Ma ona zastosowanie w zakresie przetwarzania danych osobowych przez właściwe organy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych, wykonywania kar oraz ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Zatem zakres przedmiotowy został określony w sposób obszerny. Trzeba mieć na uwadze, że oprócz organów policyjnych oraz organów śledczych, w niektórych państwach członkowskich obejmuje również wybrane czynności innych

organów, m.in. służb drogowych mających kompetencje w zakresie nakładania kar za naruszenie przepisów ruchu drogowego.

Problematyczną kwestią jest to, czy aktywność określonego organu w zakresie postępowania z danymi osobowymi powinna być regulowana przez RODO czy też dyrektywę 2016/680. Przyczyną jest fakt, iż ta dziedzina znajduje się na granicy odpowiedzialności karnej i odpowiedzialności administracyjnej, w której organy finansowe posiadają uprawnienia do nakładania środków o charakterze podobnym do sankcji karnych.

Natomiast jedną z największych kontrowersji jest stosowanie przepisów dyrektywy 2016/680 do działań związanych z bezpieczeństwem narodowym. Jest to spowodowane brakiem właściwego podziału pomiędzy zakresem działań organów śledczych a działaniami na rzecz bezpieczeństwa narodowego, co w dalszej perspektywie może prowadzić do celowego omijania standardów w niej wyrażanych, szczególnie praw osoby, której to dane dotyczą (Kusak 2019, s. 11).

Unijne standardy jakości danych osobowych

Jakość ochrony danych osobowych można rozpatrywać na dwóch płaszczyznach: jakości danych oraz jakości przetwarzania. Do jakości danych osobowych zaliczamy dokładność, stosowność, proporcjonalność oraz adekwatność.

Do jednej z najważniejszych zasad związanych z jakością ochrony danych osobowych zalicza się prawidłowość danych. Często jest ona określana mianem dokładności. Oznacza, iż zgromadzone dane muszą odpowiadać rzeczywistości, którą opisują. Dotyczy to nie tylko czynności podejmowanych w ramach gromadzenia tychże danych, lecz również na etapie ich przetwarzania (Krzysztofek 2014, s. 108).

W wielu aktach prawnych (w tym RODO) na przestrzeni lat wskazywano, jak ważny jest postulat dbałości o prawidłowość danych. Dyrektywa 2016/680 także podkreśla, iż jest to zagadnienie o fundamentalnym znaczeniu. Ponadto, wskazuje dokładnie zakres obowiązków, które realizują tę zasadę prawidłowości danych.

Do tych obowiązków zalicza się rozróżnianie pomiędzy danymi osobowymi, czyli różnicowanie danych osobowych bazujących na faktach z danymi, które są oparte na ocenach indywidualnych. Wyróżniamy również tzw. „rozsądne działania". Są one gwarancją, że nieprawidłowe i nieaktualne dane osobowe nie będą w żadnym wypadku udostępniane czy też przesyłane. Rozsądne działania polegają przede wszystkim na jak największej możliwej weryfikacji w zakresie

jakości danych osobowych przed ich przesyłaniem bądź udostępnianiem. Nadto, zamieszcza się do nich również dodatkowe informacje konieczne, by właściwy organ odbierający mógł ocenić stopień wiarygodności i prawidłowości tychże danych, a także ich aktualność (Kusak i Wiliński 2020, s. 42).

Osoba, której dane dotyczą ma możliwość oddziaływania na ich prawidłowość. Gwarantuje to art. 16 dyrektywy 2016/680. Państwa członkowskie muszą zapewnić osobom, których dane dotyczą, prawo uzyskania od administratora sprostowania bez zbędnej zwłoki danych osobowych, w przypadku ich nieprawidłowości. Nadto, takie osoby mają prawo do otrzymania uzupełnienia danych osobowych, które są niekompletne. Mogą to osiągnąć wraz z przedstawieniem oświadczenia o charakterze wspomagającym.

Co więcej, państwa członkowskie mogą nałożyć na administratora wymóg usunięcia danych osobowych oraz zapewnić możliwość osobie, której dane dotyczą, prawo uzyskania od wspomnianego administratora usunięcia jej danych osobowych. Następuje to w przypadku gdy przetwarzanie danych jest niezgodne z brzmieniem art. 4, 8 i 10 dyrektywy 2016/680, albo gdy obowiązek prawny usunięcia danych osobowych spoczywa na administratorze (Klimas 2019, s. 7).

Niewątpliwie osoba, której dane dotyczą, powinna dysponować możliwością kontroli prawidłowości własnych danych. Wprowadzone rozwiązania są słuszne, gdyż umożliwiają eliminowanie przetwarzania niezgodnych z rzeczywistością danych osobowych.

Jednocześnie w dyrektywie przewidziano procedurę dotyczącą odmowy sprostowania czy też usunięcia danych osobowych, a nawet ograniczenia przetwarzania danych. W takiej sytuacji to administrator informuje pisemnie osobę o przyczynach odmowy. Musi również pouczyć taką osobę o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu. Aczkolwiek państwa członkowskie mogą poprzez uchwalenie określonych aktów prawnych ograniczyć ten obowiązek informacyjny. Ma to jednak zastosowanie, tylko w określonych enumeratywnie przypadkach:

1. uniemożliwienie utrudniania czynności postępowań urzędowych, przygotowawczych, sądowych lub procedur,
2. uniemożliwienie zakłócania zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar,
3. chronienia bezpieczeństwa publicznego,
4. chronienia bezpieczeństwa narodowego,
5. chronienia praw i wolności innych osób.

Są to jedyne sytuacje, w których można ograniczyć udzielanie informacji, gdyż to ograniczenie przetwarzania jest działaniem koniecznym, przy jednoczesnym poszanowaniu praw podstawowych osób fizycznych (Kusak i Wiliński 2020, s. 56).

Poza prawidłowością danych należy mieć na uwadze również ich adekwatność, proporcjonalność i stosowność wobec celów, dla których są przetwarzane. Jest to tak ważne, gdyż nie można dopuścić do zbierania i przechowywania blankietowo danych osobowych.

Z tego względu w dyrektywie 2016/680 zagwarantowano, że wszystkie dane osobowe nie będą gromadzone nadmiernie oraz wprowadzono szereg mechanizmów by ograniczyć przedłużanie przechowywania danych. W tym celu administrator ma obowiązek ustalenia terminu ich usuwania bądź okresowego przeglądu. Ważne jest również zapewnienie, że dane osobowe są tylko wtedy przetwarzane, gdy celu nie da się osiągnąć innymi sposobami.

Punktem wyjścia do rozważań o warunkach takich jak stosowność, adekwatność oraz proporcjonalność jest cel przetwarzania określony w art. 1 i art. 4 Dyrektywy 2016/680. Niewątpliwie wymogi adekwatności i stosowności to wyraz zagwarantowania jakości przetwarzania gromadzonych danych. Jest to również rodzaj powiązania rodzaju danych z celem ich przetwarzania. Natomiast ze względu na ilość danych najważniejszy jest wymóg proporcjonalności. Chodzi tutaj o związek między danymi a celem dokonywanego przetwarzania. Jeżeli ilość gromadzonych danych będzie zbyt duża, to wymóg proporcjonalności nie zostanie spełniony (Jatkiewicz 2021, s. 97).

Co więcej, dane osobowe można poddać klasyfikacji ze względu na podmiot a nawet rodzaj danych. Znacznie ułatwia ona ochronę tychże danych osobowych.

Celem wprowadzenia podziału według kryterium podmiotowego było ustanowienie wyraźnego rozróżnienia kategorii osób, których te dane dotyczą:

1. osoby, co do których są uzasadnione przypuszczenia, że zamierzają popełnić lub popełniły czyn zabroniony,
2. osoby skazane za czyn zabroniony,
3. osoby pokrzywdzone czynem zabronionym lub osoby wobec których określone fakty wskazują, że w najbliższym czasie mogą być ofiarą czynu zabronionego,
4. inne osoby, które mogą dostarczyć informacji o czynach zabronionych czy też mają powiązania z takimi osobami.

Natomiast klasyfikacja ze względu na rodzaj danych jest związana z danymi, które z uwagi na sam charakter są niezwykle wrażliwe w kontekście podstawowych wolności i praw. Do nich zalicza się dane, które ujawniają:

1. pochodzenie etniczne bądź rasowe,
2. poglądy polityczne,
3. przekonania światopoglądowe lub religijne,
4. przynależność do związków zawodowych,
5. dane biometryczne oraz genetyczne przetwarzane, aby zidentyfikować osobę fizyczną,
6. zdrowie,
7. seksualność oraz orientację seksualną.

Powyższe dane wymagają szczególnej ochrony, gdyż ich przetwarzanie może doprowadzić do naruszenia podstawowych praw i wolności tych osób. Są to niewątpliwie dane wrażliwe i z tego względu powinny być objęte zwiększonym standardem bezpieczeństwa danych (Klimas 2019, s. 1 - 4).

Unijne standardy przetwarzania danych osobowych

Kolejnym niezmiernie ważnym zagadnieniem jest wspomniany już standard jakości przetwarzania danych osobowych. Można go analizować na dwóch płaszczyznach: jako wyznaczanie prawnych warunków dopuszczalności owego przetwarzania oraz jako wskazanie podstawy do uznania określonych sposobów przetwarzania za niedopuszczalne.

Sednem standardu jest zasada rzetelnego przetwarzania danych osobowych. Wynika z niej bardzo ważny nakaz przejrzystego przetwarzania wobec osoby, której dane dotyczą oraz konieczność przetwarzania jedynie w określonych prawem celach. Istotą jest działanie na podstawie i granicach obowiązującego prawa (Fajgielski 2021, s. 14).

W tym kontekście bardzo ważny jest również stopień świadomości osoby o samym procesie przetwarzania i regułach, na podstawie których się ono odbywa. To również zostało uregulowane w dyrektywie 2016/680. Na mocy dyrektywy wyróżniamy trzy kategorie udostępnianych lub przekazywanych informacji osobie, do której dane się odnoszą:

1. udostępnianie publiczne,
2. przekazane osobie, której dane dotyczą,
3. dostarczane na wniosek.

Do udostępniania publicznego zaliczamy informacje o tożsamości i danych kontaktowych administratora, danych kontaktowych inspektora ochrony danych, a w zależności od sytuacji nawet cele przetwarzania, prawo do wniesienia skargi do organu nadzorczego, a zarazem dane kontaktowe do tego organu oraz prawne żądania od administratora dostępu do danych, sprostowania lub ograniczenia bądź usunięcia danych osobowych (Kusak i Wiliński 2020, s. 66).

Natomiast mianem informacji przekazywanej konkretnej osobie, której dane dotyczą określamy bardziej szczegółowe informacje. Następuje to tylko w określonych sytuacjach. Do takich informacji zaliczamy: okres przechowywania danych osobowych bądź też kryteria służące, by określić ten okres, a nawet kategorie odbiorców danych osobowych (w tym odbiorców w organizacjach międzynarodowych lub w państwach trzecich).

Do grupy informacji dostarczanych na wniosek zaliczamy oprócz obowiązków informacyjnych dostęp bezpośredni do danych. Oznacza to, że państwa członkowskie zapewniają osobie, do której dane się odnoszą, prawo uzyskania potwierdzenia od administratora czy przetwarzane są dotyczące jej dane osobowe. W przypadku ich przetwarzania, przysługuje także prawo dostępu do danych osobowych oraz do informacji takich jak: cele i podstawa prawna przetwarzania, kategorie danych osobowych, w tym informacje o odbiorcach, bądź kategoriach odbiorców), którym dane zostały ujawnione. Jeśli jest to możliwe, to również informacje o planowanym okresie przechowywania danych osobowych, bądź kryteria służące oszacowaniu tego okresu. Nadto, także informacje o prawie do żądania od administratora sprostowania, usunięcia bądź ograniczenia przetwarzania danych osobowych. Wszystkie powyższe informacje powinny zostać przekazane w przystępnej i łatwo dostępnej formie (Boniec – Błaszczyk 2021, s. 32).

Informowanie osób o okolicznościach przetwarzania i możliwym udostępnianiu dostępu do danych znacznie zwiększa transparentność przetwarzania oraz pozwala takim osobom kontrolować legalność działań podejmowanych przez organy ścigania w zakresie przetwarzania danych osobowych.

Podsumowanie

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 uchylająca decyzję ramową Rady 2008/977/WSiSW miała zrewolucjonizować podejście do niezwykle ważnego tematu, jakim jest ochrona danych osobowych w sprawach karnych.

Akt prawny zagwarantował daleko idące uprawnienia dla osób, do których dane osobowe się odnoszą. Wraz ze wspomagającymi je środkami prawnymi miały zapewnić podmiotom o wiele większą kontrolę nad informacjami zbieranymi przez organy ścigania w sprawach karnych, które dotyczą tychże osób fizycznych.

Dyrektywa 2016/680 ma niebagatelne znaczenie, gdyż bardzo wiele danych osobowych jest gromadzone i przetwarzane przez ogrom podmiotów do celów zapobiegania i ścigania przestępczości. Zadaniem aktu prawnego jest zapewnienie bardziej konsekwentnej ochrony danych osobowych osób fizycznych na wyższym poziomie z zakresu obszarów prawa karnego, jak i bezpieczeństwa publicznego.

Jednocześnie jest to próba zagwarantowania integralności oraz kompleksowości reformy ochrony danych. Z tego względu dyrektywę 2016/680 należy uznać za *lex specialis* w zakresie ochrony danych osobowych w prawie karnym, podczas gdy RODO jest *lex generalis* dla ochrony danych osobowych. Dyrektywa 2016/680 w sprawie przetwarzania danych osobowych w prawie karnym jest niestety znacznie mniej znana, aniżeli wspomniane RODO.

Jest to swoisty wymóg dla państw członkowskich Unii Europejskiej, by osiągnęły określony poziom ochrony danych osobowych w sprawach karnych, przy czym nie wskazuje się zamkniętego katalogu środków, które pozwalałyby osiągnąć ten cel. Państwa członkowskie zobowiązują się do wprowadzenia zasad do swoich systemów prawnych.

W odróżnieniu od innych dyrektyw z zakresu ochrony praw osobowych obejmuje ona problematykę przetwarzania tychże danych przez podmioty zaangażowane w ramach systemu sądownictwa karnego, czyli sądy, prokuratura, organy policyjne, a nawet system więziennictwa. Dotyczy to przede wszystkim wykonywania zadań prawnych takich jak zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych oraz wykonywanie orzeczonych kar. Co istotne, dyrektywa reguluje standardy ochrony danych obowiązujące w państwach członkowskich, które są głównymi źródłami informacji Europolu.

Istotą jest ochrona podstawowych praw i wolności osób fizycznych, a szczególnie prawa do ochrony danych osobowych, przy jednoczesnym zapewnieniu swobodnego przepływu danych osobowych między właściwymi organami w ramach całej Unii Europejskiej. Może to zostać osiągnięte poprzez zagwarantowanie wysokiego poziomu ochrony danych osobowych osób fizycznych. Z tego

względu tak ważna jest harmonizacja przepisów we wszystkich państwach członkowskich. To dzięki nim można stworzyć efektywny system ochrony danych osobowych, a nawet wyeliminować różnice utrudniające wymianę informacji między właściwymi organami.

W szeroko pojętym prawie karnym jest to o tyle ważne i dyskusyjne z uwagi na konieczność zagwarantowania swoistej równowagi pomiędzy prawem do ochrony danych osobowych a koniecznością zachowania poufności w przetwarzaniu danych dla dobra postępowania. Jest to szczególnie widoczne na początkowym etapie postępowań karnych.

Bibliografia

Boniec – Błaszczyk D.
2021 *Ochrona danych osobowych w sprawach karnych a zakres uprawnień przysługujących jednostce w świetle dyrektywy 2016/680 oraz ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości,* „Zeszyt Naukowy UAM", nr 11.

Borecka J.
2006 *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych,* „Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie", nr 4.

Fajgielski P.
2019 Prawo ochrony danych osobowych. Zarys wykładu, Warszawa.
2021 *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze", nr 4.

Gajda A.
2019 *Interoperacyjność unijnych systemów informacyjnych w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami,* „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace", nr 37.

Gutierrez Zarza A.
2015 *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer.

Jagielski M.
2010 *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa.

Jatkiewicz P.
2021, *Wybrane aspekty zarządzania bezpieczeństwem danych osobowych,* [w:] *Ekonomia i zarządzanie wobec wyzwań współczesnego świata*, red. M. Tomczyk, K. Kwiecień, Łódź.

Klimas D.
2019 *Dyrektywa 2016/680 z perspektywy pełnomocnika procesowego – zakres przedmiotowy i zasady*, Inform. Justice Programme, Wrocław.
2019 *Prawa osób, których dane dotyczą, w świetle dyrektywy 2016/680*, „Prawo Mediów Elektronicznych", nr 3.

Kusak M.
2017 *Ochrona danych osobowych w sprawach karnych – rekomendacje na tle transpozycji dyrektywy 2016/680/UE*, „Europejski Przegląd Sądowy", nr 10.

Kusak M., Wiliński P.
2020 *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa.

Krzysztofek M.
2014 *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym*, Warszawa.

Motyka K.
1999 *Prawa człowieka. Wprowadzenie. Wybór źródeł*, Lublin.

Wróbel P.
2017 *Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia*, „Prawo Mediów Elektronicznych", nr 4.

Aleksandra Pszczoła
Sebastian Śliwa

Uniwersytet Rzeszowski
Studenci

WPŁYW RODO NA PROCES KARNY: OCHRONA DANYCH OSOBOWYCH W ŚWIETLE PRAWA I INTERESÓW INDYWIDUALNYCH

Problem ochrony danych osobowych jest obecny w wielu dziedzinach prawa i interesów jednostki. W kontekście postępowań karnych, osoba fizyczna jako kluczowy podmiot znajduje się w centrum zainteresowania organów ścigania. Dane osobowe jednostki przenikają do procesu karnego, stanowiąc podstawowe informacje o uczestnikach postępowania. W postępowaniu karnym, głównym celem pozyskiwania danych osobowych jest ustalenie tożsamości osoby będącej przedmiotem zainteresowania organów ścigania. Identyfikacja sprawcy przestępstwa jest kluczowa dla pomyślnego zakończenia dochodzenia i podjęcia odpowiednich działań prawnych.

Przetwarzanie danych osobowych w postępowaniu karnym jest ściśle regulowane przepisami prawa, w tym ustawą o ochronie danych osobowych oraz Kodeksem postępowania karnego. Organom ścigania zależy na zachowaniu zgodności z przepisami oraz poszanowaniu prywatności i praw jednostki.

Ochrona danych osobowych odgrywa kluczową rolę w zapobieganiu nadużyciom i bezprawnemu wykorzystaniu informacji. Organom procesowym zależy na zachowaniu poufności gromadzonych danych, ograniczając dostęp tylko do osób odpowiedzialnych za prowadzenie postępowania. W postępowaniu karnym, dane osobowe mogą być wykorzystane do identyfikacji sprawcy przestępstwa. Analiza informacji na temat podejrzanego może obejmować dane identyfikacyjne,

historię kryminalną, obrazy z monitoringu czy zeznania świadków. Ochrona danych osobowych w postępowaniu karnym jest niezbędna dla zapewnienia sprawiedliwości i legalności działań organów ścigania. Przestrzeganie przepisów prawa oraz dbanie o poufność informacji pozwala osiągnąć równowagę między interesami społecznymi a prawami jednostki.

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 (RODO)[1] stanowi kluczowy akt prawny regulujący ochronę danych osobowych w Unii Europejskiej. Jego wpływ na proces karny jest niezwykle istotny, ponieważ dotyczy nie tylko gromadzenia, ale również przetwarzania i przechowywania informacji o osobach w kontekście postępowań karnych. Rozporządzenie nie wprowadza sankcji karnych za niezgodne z prawem przetwarzanie danych osobowych, jednakże nie jest równoznaczne z faktem, iż prawodawca europejski nie przewidział możliwości ich wprowadzenia przez poszczególne państwa członkowskie. Zgodnie z art. 84 ust 1 RODO „państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83 oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające."

Motyw 149 RODO wprost odwołuje do sankcji karnych „Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach." Jednak nakładanie sankcji za naruszenie przepisów krajowych oraz nałożenie kar administracyjnych nie może powodować, że ta sama osoba nie może być ponownie sądzona lub ukarana za to samo przestępstwo w postępowaniu karnym, a także w zbiegu postępowań karnych z administracyjnymi (Lach 2017).

Ustawodawca krajowy uregulował odpowiedzialność karną za naruszenie przepisów o ochronie danych osobowych w Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (UODO)[2]. Ustawa przewiduję odpowiedzialność karną w przypadkach, gdy:

- Przetwarzanie danych osobowych jest niezgodne z prawem (art. 107 ust. 1 UODO).

[1] Tekst skonsolidowany Dz. U. UE. L 119/1 z 4 maja 2016 z późn. zm.
[2] Tekst. Jedn. Dz.U. 2018 poz. 1000 z późn. zm.

- Przetwarzanie danych osobowych odbywa się przez osobę do tego nieuprawnioną (art. 107 ust. 1 UODO).
- Udaremnianie lub utrudnianie kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych (art. 108 UODO).

Zgodnie z UODO, powyższe występki zagrożone są karami grzywny, ograniczenia wolności albo pozbawienia wolności do lat dwóch, natomiast w sytuacji gdy czyn określony w art. 107 ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Artykuł 1 § 1 Kodeksu karnego stanowi, iż „odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia”[3]. W związku z czym występki określone w art. 107 UODO stanowią przestępstwa powszechne, ściągane z urzędu lub z oskarżenia publicznego, które mogą zostać popełnione przez każdą osobę, której można przypisać zdolność do odpowiedzialności karnej. Każdy kto przetwarza dane osobowe, czyni to w sposób niedopuszczalny lub nie posiada uprawnień do takiego przetwarzania, przetwarza dane w sposób umyślny podlega odpowiedzialności karnej za niedopuszczalne lub niezgodne z prawem przetwarzanie danych osobowych. Przetwarzanie danych osobowych może prowadzić do przestępstwa niezależnie od tego czy sprawca był zobowiązany do stosowania przepisów RODO czy też nie. Sytuacja, gdy sprawca nielegalnie wchodzi w posiadanie danych osobowych, nielegalnie wykorzystuje je lub przetwarza w ramach czynności o charakterze osobistym, również pozostaje przetwarzaniem danych osobowych, podlegającym odpowiedzialności karnej.

Art. 6 ust. 1 RODO, zgodnie z którym przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

[3] Tekst jednolity Dz.U.2024.17 t.j. z późn. zm.

b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (…).

Zgodność z prawem przetwarzania danych osobowych wymaga jedynie istnienia jednej z wymienionych w nim podstaw. W rezultacie, jeśli administrator może udowodnić istnienie innej legalnej podstawy przetwarzania, nie ma potrzeby uzyskiwania zgody. Dodatkowo, interpretacja art. 6 ust. 1 Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO) wspierana jest przez motyw czterdziesty preambuły, gdzie stwierdzono, że "przetwarzanie danych powinno być zgodne z prawem, na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem", oraz motyw czterdziesty trzeci, który wyklucza stosowanie zgody jako podstawy przetwarzania przez organy publiczne.

Warto wspomnieć, że Prezes Urzędu Ochrony Danych Osobowych otrzymuje liczne skargi i wnioski o wszczęcie postępowania od osób niezadowolonych z przetwarzania ich danych osobowych bez zgody. W swoich decyzjach odmawiających uwzględnienia tych wniosków, PUODO wyjaśnia, że każda z podstaw legalizujących przetwarzanie danych osobowych w art. 6 ust. 1 RODO ma autonomię i niezależność[4]. Oznacza to, że każda z tych podstaw jest równoprawna, a zgodność z prawem przetwarzania danych osobowych zachodzi, gdy spełniona zostaje co najmniej jedna z nich. Zgoda osoby, której dane dotyczą, nie jest więc jedyną podstawą przetwarzania danych osobowych; proces ten jest zgodny z RODO również w przypadku, gdy administrator danych wykaże istnienie innej podstawy, niezależnie od zgody osoby, której dane dotyczą. Nadto w jednej z ostatnich aktualizacji PUODO odniósł się do kwestii zgody pracownika

[4] Decyzja ZSZZS.440.727.2018

na przetwarzanie jego danych osobowych w dokumentacji pracowniczej. Wyjaśnił, że pracodawca będący administratorem danych zawartych w aktach osobowych jest związany art. 6 ust. 1 lit c RODO oraz przepisami rozporządzenia Ministra Rodziny Pracy i Polityki Społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej, a nie wolą pracownika.

W Polsce Dyrektywa 2016/680 została wprowadzona do prawa krajowego poprzez uchwalenie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[5]. Ustawa ta wyraźnie określa w art. 3 pkt 1, że jej przepisy nie mają zastosowania do ochrony danych osobowych zawartych między innymi w aktach spraw prowadzonych na podstawie np. Kodeksu postępowania karnego, Kodeksu karnego skarbowego czy Kodeksu postępowania w sprawach o wykroczenia. Z kolei zgodnie z art. 27 tego samego aktu prawnego, w odniesieniu do danych osobowych zgromadzonych w tych postępowaniach, prawa osób, których dane dotyczą, są respektowane jedynie w granicach i na podstawie określonych przepisów regulujących te postępowania.

Dostęp obrońcy, stron lub jakiegokolwiek innego podmiotu do informacji dotyczących toczącego się postępowania karnego, wykroczeniowego, karnoskarbowego itp., włączając w to dane osobowe zawarte w aktach tych postępowań, podlega wyłącznie reżimowi konkretnej ustawy, na mocy której dane postępowanie jest prowadzone (np. Kodeks postępowania karnego). W przypadku ewentualnego odmówienia udzielenia informacji lub dostępu do akt sprawy, musi ono mieć swoje podstawy w przepisach tej właściwej ustawy (np. art. 317 § 2 k.p.k.)[6], nie zaś w RODO ani w wspomnianej ustawie z dnia 14 grudnia 2018 r.

Wyjaśnienie zostało dokładnie przedstawione w projekcie omawianej ustawy[7]. Ustawodawca wyjaśnił, że akta takie jak akta postępowania karnego nie kwalifikują się jako zbiór danych w rozumieniu Dyrektywy 2016/680. Wskazano kilka powodów tego stanowiska:

W aktach spraw postępowania karnego i jego odmian gromadzi się różnorodne informacje oraz materiały dowodowe, na podstawie których organ prowadzący postępowanie i wydający rozstrzygnięcie kształtuje swoje stanowisko co do faktu popełnienia czynu zabronionego, sprawcy tego czynu oraz odpowiedzialności karnej. Fakt, że dokument zawiera dane osobowe wśród innych informacji, nie powoduje, że staje się on zestawem danych osobowych, ani zbiorem danych.

[5] Tekst jedn. Dz.U. 2019 poz. 125 z późn. zm.
[6] Tekst skonsolidowany Dz. U. 1997 Nr 89 poz. 555 z późn. zm.
[7] Druk Sejmowy numer 2989 Sejmu VIII Kadencji

Nie pozwalają na odnalezienie danych osobowych zawartych w materiale dowodowym bez potrzeby przeglądania całego zestawu;

Kryteria porządkujące akta nie dotyczą danych osobowych, lecz kolejności przeprowadzania dowodów lub wątków postępowania dotyczących zazwyczaj odrębnych czynów zabronionych.

Dodatkowo, postępowanie karne i jego odmiany zapewniają, według ustawodawcy, zwiększoną ochronę dla danych osobowych w porównaniu z ochroną przewidzianą przez Dyrektywę 2016/680. W uzasadnieniu projektu podkreślono również, że podstawą do przetwarzania danych w postępowaniem karnym są przepisy procedury karnej. Przetwarzaniu podlegają dane uzyskane zgodnie z określonymi wymogami formalnymi, przy czym dane te nie mogą być ujawniane w warunkach innych niż określone w przepisach. W postępowaniu karnym muszą być np. zachowane wymogi i ograniczenia określone w art. 156 k.p.k.

Odmowa udzielenia obrońcy informacji o kliencie, argumentowana koniecznością ochrony danych osobowych tegoż klienta, może być postrzegana jako naruszenie prawa do obrony. Pośrednio zwrócił uwagę na to sam ustawodawca, który w uzasadnieniu projektu wspomnianej ustawy napisał: „Na prawo do ochrony danych osobowych, trzeba zatem patrzeć przez pryzmat innych praw, mających pierwszeństwo w pewnej hierarchii praw podstawowych. Prawo to doznaje bowiem ograniczeń – przy zachowaniu zasad subsydiarności i proporcjonalności – w sytuacji, gdy może ono naruszyć prawo podstawowe, stojącym wyżej w hierarchii praw."

W świetle rosnącej skali i złożoności zagrożeń przestępczości transgranicznej, współpraca międzynarodowa w zakresie przekazywania danych osobowych jest niezbędna dla skutecznej walki z przestępczością. Jednocześnie, konieczne jest równoważenie tych działań z zasadami ochrony danych osobowych, zapewniając, że przekazywanie danych odbywa się zgodnie z prawem oraz respektuje prawa jednostek. Optymalne wykorzystanie dostępnych narzędzi prawnych oraz dalszy rozwój mechanizmów współpracy może przyczynić się do zwiększenia bezpieczeństwa obywateli i skuteczniejszego zwalczania przestępczości na szczeblu międzynarodowym.

Dokumenty prawa Unii Europejskiej, takie jak 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 uchylająca decyzję ramową

Rady 2008/977/WSiSW[8], są złożone i precyzyjnie formułowane, dlatego trzeba odwołać się do konkretnych jej artykułów, które precyzują omawiane kwestie. W przypadku Dyrektywy 2016/680, można zauważyć, że jej postanowienia dotyczące zasad przetwarzania danych, praw jednostek oraz obowiązków organów ścigania w zakresie ochrony danych osobowych są rozproszone w różnych artykułach. Dyrektywa 2016/680 stanowi jedno z kluczowych narzędzi prawnych regulujących przekazywanie danych osobowych w celach ścigania przestępstw w Unii Europejskiej. Jej postanowienia precyzują zasady przetwarzania danych, prawa jednostek oraz obowiązki organów ścigania w zakresie ochrony danych osobowych.

Artykuł 4 „Zasady dotyczące przetwarzania danych osobowych przez organy ścigania" określa ogólne zasady przetwarzania danych osobowych przez organy ścigania. W szczególności nakłada obowiązek na te organy przetwarzania danych zgodnie z zasadą proporcjonalności i ograniczenia celu, co oznacza, że dane osobowe powinny być przetwarzane tylko w zakresie niezbędnym do osiągnięcia określonych celów śledztwa lub postępowania karnego. Artykuł zawiera również wymogi dotyczące uczciwości i transparentności przetwarzania danych oraz konieczność zapewnienia bezpieczeństwa danych osobowych.

Oprócz Dyrektywy 2016/680, istnieje szereg innych aktów prawa unijnego, które wpływają na regulacje dotyczące przekazywania danych osobowych. Wśród nich znajdują się inne dyrektywy oraz rozporządzenia, które uzupełniają i precyzują ramy prawne dotyczące ochrony danych osobowych i przekazywania ich w kontekście walki z przestępczością. W sektorze telekomunikacyjnym istnieją również specjalne akty prawne regulujące ochronę danych osobowych, takie jak Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[9]. Te regulacje mogą mieć znaczenie szczególne w kontekście przetwarzania danych telekomunikacyjnych w celach ścigania przestępstw. Oprócz aktów prawa unijnego, istnieją także umowy międzynarodowe między państwami członkowskimi UE oraz zewnętrznymi partnerami, które mogą regulować wymianę danych osobowych w celach ścigania przestępstw. Te umowy mogą uzupełniać i precyzować ramy prawne dotyczące przekazywania danych osobowych między państwami w ramach współpracy policyjnej i sądowej.

[8] Tekst skonsolidowany Dz. U. UE. L 119/89 z 4 maja 2016 z późn. zm.
[9] Tekst skonsolidowany Dz.U.UE.L.2002.201.37 z późn. zm.

Analiza wyzwań dotyczących ochrony danych osobowych związanych z przekazywaniem ich między państwami członkowskimi Unii Europejskiej jest kluczowym zagadnieniem w kontekście współpracy międzynarodowej i walki z przestępczością. Jednym z głównych wyzwań jest zapewnienie, że proces przekazywania danych osobowych pomiędzy państwami członkowskimi odbywa się zgodnie z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, w tym Dyrektywą 2016/680 oraz Rozporządzeniem Ogólnym o Ochronie Danych Osobowych (RODO). Wymaga to skrupulatnego przestrzegania procedur i norm określonych w tych aktach prawnych, aby zagwarantować, że dane są przekazywane w sposób zgodny z prawem i zapewniający odpowiednią ochronę prywatności jednostek.

Wielu obywateli obawia się naruszenia prywatności w związku z przekazywaniem danych osobowych między państwami, dlatego istotne jest, aby procedury przekazywania danych były przejrzyste, zgodne z prawem i zawierały odpowiednie mechanizmy ochrony prywatności, takie jak zabezpieczenia techniczne i organizacyjne, umożliwiające minimalizację ryzyka nieuprawnionego dostępu lub wykorzystania danych.

Przekazywanie danych osobowych między różnymi państwami członkowskimi często wiąże się z koniecznością uwzględnienia różnic kulturowych i prawnych w zakresie ochrony danych osobowych. Każde państwo może mieć inne przepisy i standardy dotyczące ochrony danych, co może prowadzić do wyzwań związanych z dostosowaniem się do tych różnic i zapewnieniem spójności oraz zgodności procedur przekazywania danych. W kontekście przekazywania danych osobowych między państwami członkowskimi kluczową kwestią jest również zapewnienie odpowiedniego poziomu bezpieczeństwa danych. W obliczu rosnących zagrożeń związanych z cyberprzestępczością konieczne jest zastosowanie skutecznych środków ochrony danych, aby zapobiec nieuprawnionemu dostępowi, wyciekom lub innym incydentom naruszającym bezpieczeństwo danych.

Wyzwania związane z ochroną danych osobowych w kontekście przekazywania ich między państwami członkowskimi Unii Europejskiej wymagają starannego uwzględnienia przepisów prawnych, ochrony prywatności jednostek, różnic kulturowych i prawnych oraz zapewnienia wysokiego poziomu bezpieczeństwa danych. Ich skuteczne rozwiązanie jest kluczowe dla zapewnienia bezpiecznej i skutecznej współpracy międzynarodowej w dziedzinie ścigania przestępstw.

Międzynarodowa współpraca policyjna opiera się na przepisach rządowych oraz resortowych oraz na dokumentach umożliwiających lokalną współpracę na obszarach przygranicznych. Realizacja współpracy międzynarodowej Policji

odbywa się na dwóch płaszczyznach. Działania pozaoperacyjne mają na celu opracowanie metod, form i podstaw prawnych praktycznej współpracy policyjnej, nazywanej również współpracą operacyjną. Współpraca operacyjna obejmuje przede wszystkim wymianę informacji poprzez System Informacyjny Schengen (SIS) oraz Krajowe Biuro SIRENE (dla państw strefy Schengen); EUROPOL; INTERPOL - Międzynarodową Organizację Policji Kryminalnej, pomagającą organom ścigania w walce z wszelkimi formami przestępczości; współpracę w ramach sieci oficerów łącznikowych polskiej Policji działających w państwach Unii Europejskiej, tj. Francji, Hiszpanii, Niemczech, na Węgrzech i we Włoszech, oraz państwach spoza UE, tj. w Wielkiej Brytanii, Norwegii, Rosji (stanowisko nieobsadzone), Gruzji, Turcji, Ukrainie oraz Stanach Zjednoczonych Ameryki, oraz współpracę z zagranicznymi oficerami łącznikowymi akredytowanymi w Polsce; oraz bezpośredni dostęp do policyjnych baz danych (osoby zaginione i poszukiwane, karty daktyloskopijne, profile DNA, skradzione pojazdy i dokumenty etc.)[10].

Europejski Urząd Policji, znany również jako Europol, stanowi kluczowy element w zapewnianiu bezpieczeństwa w Unii Europejskiej poprzez koordynację działań policyjnych między państwami członkowskimi. Jednym z kluczowych obszarów jego działalności jest ochrona danych osobowych w kontekście przekazywania ich między różnymi krajami (Gruszczak 2009). W obliczu rosnących wyzwań związanych z przestępczością transgraniczną, coraz istotniejsza staje się współpraca międzynarodowa w dziedzinie ścigania przestępstw. Jednakże, realizacja tej współpracy napotyka na liczne wyzwania związane z ochroną danych osobowych. Staranne uwzględnienie przepisów prawnych, zapewnienie ochrony prywatności jednostek oraz uwzględnienie różnic kulturowych i prawnych są niezbędne dla skutecznego rozwiązania tych problemów. Wysoki poziom bezpieczeństwa danych jest kluczowy dla zapewnienia bezpiecznej i skutecznej współpracy międzynarodowej w dziedzinie zwalczania przestępczości.

Wspólny Organ Nadzorczy Europolu (Joint Supervisory Body of Europol), to organ nadzoru ustanowiony na podstawie art. 34 decyzji Rady z dnia 6 kwietnia 2009 ustanawiającej Europejski Urząd Policji (Europol) odpowiedzialny za nadzór nad działalnością Europolu zmierzający do zapewnienia, że prawa jednostki nie są łamane przez przechowywanie, przetwarzanie i wykorzystywanie informacji znajdujących się w posiadaniu Europolu. Jednocześnie WON Europolu jest organem właściwym do monitorowania dopuszczalności przekazania danych

[10] Info.Policja.pl, *Współpraca Międzynarodowa,* https://info.policja.pl/inf/wspolpraca-miedzynarod/72445,Wspolpraca-miedzynarodowa.html [dostęp: 29.02.2024].

pochodzących ze zbiorów Europolu[11]. Misją Wspólnego Organu Nadzorczego jest dokonywanie niezależnego przeglądu działań Europolu zgodnie z postanowieniami Konwencji o Europolu. Celem tego przeglądu jest zapewnienie, że prawa osób fizycznych nie są naruszane w procesie przechowywania, przetwarzania i wykorzystywania danych przez Europol. Dodatkowo, Wspólny Organ Nadzorczy sprawuje nadzór nad legalnością przekazywania danych pochodzących z Europolu. Każda osoba fizyczna ma prawo zgłosić wniosek do Wspólnego Organu Nadzorczego w celu sprawdzenia czy sposób, w jaki Europol gromadził, przechowywał, przetwarzał i wykorzystywał jej dane osobowe, był rzetelny i zgodny z obowiązującymi przepisami prawnymi. W ten sposób Wspólny Organ Nadzorczy pełni rolę niezależnego pośrednika między osobami fizycznymi a Europolem, zapewniając ochronę praw jednostek w kontekście działalności agencji Europolu[12].

Jeśli Wspólny Organ Nadzorczy (WON) Europolu zauważy naruszenie przepisów określonych w decyzji Rady ustanawiającej Europejski Urząd Policji dotyczących przechowywania, przetwarzania lub wykorzystywania danych osobowych, zgłasza to dyrektorowi Europolu w postaci stosownych skarg, oczekując na udzielenie odpowiedzi w określonym terminie. Dyrektor informuje zarząd Europolu o wszczętej procedurze. W przypadku, gdy odpowiedź dyrektora nie satysfakcjonuje WON Europolu, sprawa zostaje przekazana zarządowi. W trakcie wykonywania swoich obowiązków i w celu zapewnienia spójności stosowania przepisów i procedur dotyczących przetwarzania danych, Wspólny Organ Nadzorczy Europolu nawiązuje współpracę z innymi organami nadzorczymi, gdy jest to konieczne.

Współpraca międzynarodowa w dziedzinie ścigania przestępstw w ramach Unii Europejskiej wiąże się z wieloma wyzwaniami związanymi z ochroną danych osobowych. Konieczne jest uwzględnienie przepisów prawnych, ochrony prywatności jednostek oraz różnic kulturowych i prawnych, aby zapewnić wysoki poziom bezpieczeństwa danych. Skuteczne rozwiązanie tych wyzwań jest kluczowe dla zapewnienia bezpiecznej i efektywnej współpracy międzynarodowej w zwalczaniu przestępczości. Wspólny Organ Nadzorczy Europolu (Joint Supervisory Body of Europol) został ustanowiony w celu nadzoru nad działalnością Europolu i zapewnienia, że prawa jednostek nie są naruszane przez przechowywanie, przetwarzanie i wykorzystywanie danych przez tę agencję. Organ ten jest również

[11] Urząd Ochrony Danych Osobowych „Informacje Ogólne", https://uodo.gov.pl/pl/90/166 [dostęp: 01.03.2024].
[12] Czwarte sprawozdanie z działalności Wspólnego Organu Nadzorczego Europolu.

odpowiedzialny za monitorowanie legalności przekazywania danych pochodzących z Europolu. Każda osoba fizyczna ma prawo zgłosić wniosek do Wspólnego Organu Nadzorczego w celu sprawdzenia czy Europol postępował zgodnie z obowiązującymi przepisami prawnymi dotyczącymi gromadzenia, przechowywania, przetwarzania i wykorzystywania danych osobowych. Wspólny Organ Nadzorczy Europolu odgrywa kluczową rolę w zapewnieniu, że Europol działa w zgodzie z obowiązującymi standardami ochrony danych osobowych. Poprzez niezależne przeglądy działalności Europolu oraz współpracę z innymi organami nadzorczymi, organ ten zapewnia ochronę praw jednostek i skuteczność działań agencji Europolu w zwalczaniu przestępczości na szczeblu międzynarodowym.

Ogólne rozporządzenie o ochronie danych osobowych stało się kluczowym instrumentem prawnym w Unii Europejskiej w zakresie ochrony danych wrażliwych osobowych. Rozporządzenie daje możliwość zabezpieczenia, czy też ograniczenia bezpodstawnego rozprzestrzeniania się wrażliwych informacji, o nas samych. W każdym jednak przypadku mogą zdarzyć się sytuacje w których owe dane zostaną w mniej lub bardziej przypadkowy sposób rozpowszechnione. W związku z tym niezwykle istotne jest aby istniała możliwość, w przypadku naruszeń RODO, aby osoby prywatne mogły dochodzić zadośćuczynienia za niezgodne z ich wolą rozpowszechnienie informacji.

Artykuł 82 ogólnego rozporządzenia o ochronie danych osobowych[13] jest kluczowym przepisem regulującym kwestie ochrony praw osób prywatnych w kontekście nieprawidłowego przetwarzania danych osobowych. Zgodnie z tym artykułem, każda osoba, której prawa lub wolności zostały naruszone w związku z niezgodnym przetwarzaniem danych osobowych, ma prawo do odszkodowania lub zadośćuczynienia za poniesione szkody. Artykuł 4 w punkcie 7 niniejszego rozporządzenia definiuje potencjalnego administratora poufnych informacji, może nim być: osoba fizyczna (członek rodziny, przedsiębiorca), osoba prawna (fundacja, stowarzyszenie, spółka), organ publiczny (urząd gminy, miasta), jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, do których przetwarzania ma prawo zgodnie z wytycznymi niniejszego rozporządzenia. Taki administrator jest w pełni odpowiedzialny za szkody jakie mogły zaistnieć w związku z przechowywaniem danych, jednakże w przypadku kiedy udowodni, że dopełnił obowiązki jakie nakładało rozporządzenie RODO lub działał zgodnie z instrukcjami

[13] Tekst skonsolidowany Dz. U. UE. L 119/1 z 4 maja 2016 z późn. zm.

to odpowiedzialności nie można mu przypisać, o czym stanowi paragraf 3 omawianego wcześniej artykułu.

W polskim porządku prawnym, który implementuje przepisy RODO, art. 82 został uwzględniony w ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych[14]. Wprowadzenie tego przepisu do krajowego porządku prawnego ma na celu zapewnienie spójności między regulacjami unijnymi a krajowymi oraz ułatwienie egzekwowania praw osób dotkniętych naruszeniem RODO. Warto zauważyć, że artykuł 82 RODO i jego implementacja w polskim prawie stanowią istotny element w zapewnieniu skutecznej ochrony danych osobowych oraz praw osób prywatnych. Wspiera to zasadę, że osoby dotknięte naruszeniem danych osobowych powinny mieć skuteczne środki ochrony i możliwość dochodzenia swoich praw przed sądem.

Artykuł 82 RODO[15] stanowi istotny instrument ochrony praw osób prywatnych, ponieważ nakłada na podmioty przetwarzające dane osobowe odpowiedzialność za ewentualne naruszenia. Daje to osobom dotkniętym naruszeniem możliwość dochodzenia swoich roszczeń wobec tych podmiotów. W przypadku faktycznej odpowiedzialności więcej niż jednego podmiotu administrującego naszymi danymi osobowymi możemy skierować roszczenie o odszkodowanie do wszystkich podmiotów. Nie oznacza to jednak, że możemy ubiegać się o zadośćuczynienie od wielu podmiotów, w ramach pojedynczej sprawy. W przypadku niedopełnienia obowiązków, zarządzający danymi odpowiadają solidarnie i też solidarnie dzielą się wypłaconym zadośćuczynieniem w przypadku zasądzenia.

Analiza orzecznictwa sądów polskich stanowi istotny punkt odniesienia w zrozumieniu praktycznych aspektów związanych z zadośćuczynieniem dla osób prywatnych w przypadku naruszeń RODO. W wyroku z dnia 7 lutego 2023 roku (sygn. akt III C 280/22)[16], Sąd Okręgowy w Warszawie podkreślił, że podmiot przetwarzający dane ponosi odpowiedzialność za wszelkie naruszenia RODO, które prowadzą do szkód majątkowych lub niemajątkowych. Zadośćuczynienie dla osób prywatnych w przypadku naruszeń RODO stanowi istotny element ochrony danych osobowych w Polsce.

Naruszenie przepisów RODO może prowadzić do różnych rodzajów szkód dla osoby dotkniętej. W szczególności wyróżnić możemy szkody majątkowe i niemajątkowe. Szkoda majątkowa, jest to rodzaj szkody, który polega na realnych stratach finansowych poniesionych przez osobę dotkniętą naruszeniem RODO.

[14] Tekst. Jedn. Dz.U. 2018 poz. 1000 z późn. zm.
[15] Tekst skonsolidowany Dz. U. UE. L 119/1 z 4 maja 2016 z późn. zm.
[16] Wyrok SO w Warszawie z 7.02.2023 r., III C 280/22, POSP

Przykładem takiej szkody może być utrata danych osobowych prowadząca do kradzieży tożsamości lub nieuprawnionego dostępu do konta bankowego, co może skutkować znacznymi stratami finansowymi dla poszkodowanego. Szkoda niemajątkowa, obejmuje ona szkody, które nie mają wymiernego charakteru finansowego, ale mogą prowadzić do doznań psychicznych lub naruszenia praw osobistych. Przykładem szkody niemajątkowej może być naruszenie prywatności, które prowadzi do doznań psychicznych, stresu czy cierpienia emocjonalnego u osoby dotkniętej (Sinkiewicz 1998, s. 59-74).

Wysokość zadośćuczynienia lub odszkodowania zależy od konkretnych okoliczności sprawy oraz stopnia winy podmiotu przetwarzającego dane. Sąd bierze pod uwagę szereg czynników, m.in. stopień takiego naruszenia, mianowicie czy było celowe, rażąco nieostrożne czy może wynikało z błędu systemowego. Skutki szkody, jakie konsekwencje miało naruszenie dla osoby dotkniętej, zarówno w wymiarze materialnym, jak i psychicznym. Jakie roszczenie zgłasza poszkodowany oraz jakie są jego oczekiwania co do zadośćuczynienia lub odszkodowania. W praktyce, sądy biorą pod uwagę powyższe czynniki oraz inne szczególne okoliczności sprawy, aby ustalić odpowiednią wysokość zadośćuczynienia lub odszkodowania dla osoby dotkniętej naruszeniem RODO.

Warto podkreślić, że celem przyznania zadośćuczynienia lub odszkodowania nie jest tylko rekompensata dla poszkodowanego, z drugiej strony ma to poniekąd stanowić funkcję ostrzegawczą czy też odstraszającą inne podmioty przetwarzające dane od popełniania naruszeń, lekceważenia potencjalnych błędów systemowych, nieuzupełniania i braku renowacji infrastruktury przechowującej dane oraz promowanie odpowiedzialnego podejścia do ochrony danych osobowych. Dzięki temu regulacje dotyczące ochrony danych stają się bardziej skuteczne i przynoszą realne korzyści dla wszystkich stron zaangażowanych w proces przetwarzania danych.

Samo zadośćuczynienie przysługuje na mocy art. 448 Kodeksu cywilnego z dnia 23 kwietnia 1964 r.[17], który stanowi kluczowy fundament w przypadku naruszeń dóbr osobistych. Zgodnie z tym artykułem, sąd może przyznać stosowną sumę z tytułu zadośćuczynienia osobie poszkodowanej w przypadku naruszenia jej dóbr osobistych. Co istotne, na żądanie osoby poszkodowanej, odpowiednia suma pieniężna może zostać przeznaczona na wskazany cel społeczny. Jest to szczególnie istotne w przypadku, gdy osoba poszkodowana życzy sobie, aby zadośćuczynienie miało również wymiar społeczny, na przykład wsparcie

[17] Tekst skonsolidowany Dz. W. 1964 Nr 16 poz. 93 z późn. zm.

organizacji charytatywnych lub fundacji działających na rzecz ochrony praw człowieka.

Zadośćuczynienie ma głównie służyć naprawieniu szkody, która powstała w wyniku naruszenia przepisów. Jest to działanie kompensacyjne, które ma na celu przywrócenie równowagi oraz zrekompensowanie wyrządzonej szkody. Osoba dotknięta naruszeniem, na przykład poprzez utratę danych osobowych lub naruszenie prywatności, ma prawo do otrzymania rekompensaty za poniesione straty. Dążenie do przywrócenia równowagi i zadośćuczynienie za wyrządzone krzywdy stanowi istotny aspekt tego procesu (Szpunar 1991, s. 89).

Dodatkowo, zadośćuczynienie ma także funkcję prewencyjną. Poprzez nakładanie finansowej odpowiedzialności na podmioty przetwarzające dane, wprowadza się dodatkową warstwę dyscypliny i obowiązków. Określenie wysokości ewentualnego zadośćuczynienia może zachęcać te podmioty do przestrzegania bardziej rygorystycznych i ostrożnych praktyk w zakresie ochrony danych osobowych. Ten aspekt jest istotny, ponieważ może przyczynić się do zmniejszenia liczby przyszłych naruszeń i podniesienia ogólnych standardów ochrony danych (Dyka 2001, s. 637). W ten sposób, zadośćuczynienie w kontekście naruszeń RODO nie tylko rekompensuje poszkodowanym szkody, ale także pełni funkcję prewencyjną, zabezpieczającą, przyczyniając się do poprawy ogólnego poziomu ochrony danych osobowych. Dzięki temu podejściu, system ochrony danych staje się bardziej skuteczny i odpowiedzialny, chroniąc prywatność i prawa osób fizycznych.

Ewentualne ograniczenia w zapewnieniu rekompensaty lub odszkodowania w sytuacjach naruszenia danych osobowych mogą wynikać z różnych czynników. Z braku dowodów, konieczności udowodnienia szkody oraz związku przyczynowego między naruszeniem danych a poniesionymi stratami może stanowić wyzwanie, zwłaszcza jeśli nie ma jednoznacznych dowodów na szkody materialne lub niematerialne. Przez problemy z identyfikacją sprawcy a co za tym idzie z ustaleniem odpowiedzialności sprawcy naruszenia przepisów dotyczących danych osobowych może być trudne, zwłaszcza w przypadku ataków hackerskich lub nieuprawnionego dostępu do danych.

Potencjalne drogi postępowania w kontekście dochodzenia swoich praw przed sądem w wyniku naruszenia danych osobowych mogą obejmować kilka różnych ścieżek, zależnie od charakteru naruszenia oraz preferencji osoby poszkodowanej. Osoba poszkodowana może złożyć skargę do właściwego organu nadzorczego ds. ochrony danych osobowych co gwarantuje art. 9 ust. 2 ustawy

o ochronie danych osobowych[18]. W przypadku Unii Europejskiej jest to Europejski Inspektor Ochrony Danych, a w poszczególnych krajach członkowskich - odpowiedni organ krajowy, przykładowo Prezes Urzędu Ochrony Danych Osobowych w Polsce. Organ taki może przeprowadzić dochodzenie w sprawie naruszenia i nałożyć sankcje administracyjne na sprawcę. Jeśli naruszenie danych osobowych ma charakter kryminalny, osoba poszkodowana może zgłosić sprawę organom ścigania, takim jak policja czy prokuratura. Organizacje i firmy są również zobowiązane do zgłoszenia poważnych naruszeń danych osobowych organom ścigania. Osoba poszkodowana może wnieść pozew cywilny w celu dochodzenia odszkodowania lub zadośćuczynienia za poniesione szkody. W tym przypadku dochodzenie praw może obejmować zarówno szkody materialne, jak i niematerialne wspomniane wcześniej. Istnieje również możliwość wnoszenia grupowych pozwów przeciwko podmiotom przetwarzającym dane osobowe. Grupa poszkodowanych może zostać zorganizowana przez organizacje pozarządowe lub adwokatów reprezentujących poszkodowanych, co może znacznie ułatwić dostęp do sprawiedliwości i uzyskania zadośćuczynienia dla osób dotkniętych naruszeniem danych. Osoba poszkodowana może także rozważyć mediację lub arbitraż jako alternatywne metody rozwiązywania sporów. Wszystkie te drogi postępowania mają swoje zalety i ograniczenia, dlatego wybór odpowiedniej ścieżki powinien być dokładnie rozważony z uwzględnieniem indywidualnej sytuacji oraz preferencji osoby poszkodowanej.

W dobie cyfryzacji i wzmożonej aktywności online, gromadzenie danych osobowych w ramach postępowań karnych stało się nieodłącznym elementem działań organów ścigania. Jednakże, wraz z potrzebą przechowywania tych informacji, mogą zaistnieć problemy i powstać potencjalne niedociągnięcia związane z tym procesem, które mogą prowadzić do naruszeń prywatności jednostek oraz niewłaściwego przetwarzania ich danych osobowych.

Brak odpowiedniej zgody na zbieranie danych osobowych jest jednym z kluczowych problemów w kontekście postępowań karnych w Polsce. Zgodnie z obowiązującym prawem o ochronie danych osobowych, takie zgody są kluczowe dla legalnego przetwarzania danych. Jednakże, w przypadku postępowań karnych, organy ścigania często zbierają dane osobowe bez wyraźnej zgody osoby, co stwarza istotne ryzyko naruszenia jej praw.

Prawo o ochronie danych osobowych, zarówno krajowe jak i europejskie, jasno określa, że zbieranie danych osobowych wymaga wyraźnej zgody osoby,

[18] Tekst. Jedn. Dz.U. 2018 poz. 1000 z późn. zm.

chyba że istnieje inna podstawa prawna do przetwarzania danych. Jednakże, w przypadku postępowań karnych, organy ścigania często argumentują konieczność zebrania danych osobowych w imię interesu publicznego, bez konieczności uzyskania zgody osoby. Do czego też przyznaje prawo art. 20 par. 1 w punkcie 1d, Ustawy o Policji z dnia 6 kwietnia 1990 r.[19], ,,Przetwarzanie informacji, w tym danych osobowych, przez Policję może mieć charakter niejawny, odbywać się bez zgody i wiedzy, osoby której dane dotyczą, oraz z wykorzystaniem środków technicznych. Służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Policji informacji, w tym danych osobowych.'' Z jednej strony może się to obywatelom wydawać zbytnią ingerencją w ich prawa i wolności osobiste, nikt nie chce aby niektóre informacje były znane szerszej grupie osób. Jednakże uzależnienie doprowadzenia postępowania i przewodu sądowego do skutku, osądzenie osób winnych, wyłącznie od zgody poszczególnych obywateli na przekazanie ich danych personalnych służbom publicznym nie mogłoby mieć racji bytu. Niektórzy mogą to uznać za znaczne naruszenie praw osobistych jednakże organy ścigania muszą mieć pewność jakiej osobie zarzucają konkretny czyn a kto jest niewinny.

Praktyka nieskrępowanej możliwości pozyskiwania danych osobowych jest obarczona ryzykiem naruszenia praw jednostki. Brak zgody na zbieranie danych osobowych oznacza, że osoba może nie być świadoma, że jej dane są gromadzone i przetwarzane przez organy ścigania. Jest to szczególnie problematyczne w przypadku danych wrażliwych, takich jak informacje o stanie zdrowia czy orientacji seksualnej, które mogą być zbierane w ramach postępowań karnych. Ponadto, brak odpowiedniej zgody na zbieranie danych osobowych może prowadzić do niewłaściwego wykorzystania tych danych. Organom ścigania może brakować przejrzystości w zakresie, w jaki sposób i w jakim celu dane są gromadzone oraz przetwarzane, co stwarza ryzyko nadużycia i naruszenia prywatności osób fizycznych. Organy ścigania powinny zwracać szczególną uwagę na przestrzeganie zasad przejrzystości oraz umożliwienie osobom objętym postępowaniami karnymi świadomego udzielenia zgody na przetwarzanie ich danych osobowych. Działania te są kluczowe dla zapewnienia poszanowania praw jednostki oraz prawidłowego przetwarzania danych osobowych w procesie sądowym.

Zbieranie nadmiernych informacji stanowi kolejny aspekt nadużycia Organom ścigania często brakuje precyzji w zakresie danych, które są niezbędne do przeprowadzenia postępowania karnego, co może prowadzić do

[19] Tekst skonsolidowany Dz. U. 1990 Nr 30 poz. 179 z późn. zm.

gromadzenia zbyt dużych ilości danych osobowych. Jest to problematyczne z kilku powodów. Między innymi, prowadzi to do niepotrzebnego naruszenia prywatności jednostki. Zbieranie i przechowywanie danych, które nie są niezbędne dla prowadzenia postępowania karnego, jest nieetyczne i narusza prawo do prywatności jednostki. Dodatkowo, może to stworzyć atmosferę nieufności wobec organów ścigania oraz systemu sądowego, co może zaszkodzić zaufaniu społecznemu. Zbieranie nadmiernych informacji niesie ze sobą również ryzyko ich nieuprawnionego wykorzystania. Wrażliwe informacje, takie jak dane medyczne, mogą być wykorzystane w sposób niezgodny z prawem lub etyką, co stanowi istotne zagrożenie dla bezpieczeństwa jednostki. Ponadto, zbieranie nadmiernych informacji może również wpłynąć na efektywność postępowań karnych. Przetwarzanie nadmiernych ilości danych może być czasochłonne, kosztowne, a także niepotrzebnie wydłużać proces. Dodatkowym problemem jest nieaktualność gromadzonych danych. Mogą powstawać przypadki kiedy to organy ścigania z powodu rozciągłości postępowania korzystają z nieaktualnych lub niezweryfikowanych danych, co może prowadzić do błędów w procesach karnych oraz niesłusznych oskarżeń. Edukacja pracowników organów ścigania w zakresie ochrony danych osobowych oraz świadomość społeczna na temat znaczenia prywatności i bezpieczeństwa danych są kluczowe dla skutecznego przeciwdziałania zbieraniu nadmiernych informacji w ramach postępowań karnych. Tylko poprzez ścisłe przestrzeganie zasad ochrony danych osobowych można zapewnić poszanowanie praw jednostki oraz prawidłowe funkcjonowanie systemu sądowego.

W związku z powyższymi rozważaniami, stwierdzamy, że problematyka ochrony danych osobowych w kontekście postępowania karnego wymaga dalszych badań i działań zarówno na poziomie legislacyjnym, jak i praktycznym. Wprowadzenie Rozporządzenia Ogólnego o Ochronie Danych Osobowych stanowiło krok naprzód w kierunku zapewnienia większej ochrony prywatności jednostek, jednakże zauważamy, że istnieją obszary, które wymagają bardziej szczegółowego uregulowania oraz egzekwowania. Niezwykle istotne jest, aby organy ścigania oraz instytucje odpowiedzialne za prowadzenie postępowań karnych były świadome i skrupulatnie przestrzegały zasad RODO, zarówno w zakresie gromadzenia, przetwarzania, jak i przechowywania danych osobowych. Jednocześnie należy zagwarantować, że jednostki, których dane dotyczą, mają możliwość skutecznego egzekwowania swoich praw w przypadku naruszeń.

W kontekście zadośćuczynienia dla osób prywatnych w przypadku naruszeń RODO, należy dokładnie analizować możliwości oraz ograniczenia w zapewnieniu rekompensaty za krzywdy materialne i niematerialne. Wspierając się dogłębną

analizą prawną, można opracować wytyczne dotyczące postępowania w przypadku naruszenia danych osobowych, aby jednostki miały jasną ścieżkę dochodzenia swoich praw przed sądem. Warto również skoncentrować się na identyfikacji potencjalnych niedociągnięć w procesach gromadzenia, przetwarzania i zabezpieczania danych osobowych w ramach postępowania karnego oraz podjąć działania mające na celu ich naprawę. Świadomość tych zagrożeń, wymienionych w niniejszym artykule bądź innych oraz podejmowanie działań zapobiegawczych pozwoli na skuteczną ochronę danych osobowych oraz zachowanie równowagi między efektywnością działań karnościgowych a poszanowaniem praw jednostek.

BIBLIOGRAFIA

Akty Prawne

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, tekst jednolity, (tekst jedn. Dz. W. 1964 Nr 16 poz. 93 z późn. zm.)

Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity (tekst jedn. Dz. U. 1990 Nr 30 poz. 179 z późn. zm.)

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny tekst jednolity (tekst jedn. Dz.U.2024.17 z późn. zm.)

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego tekst jednolity (tekst jedn. Dz. U. 1997 Nr 89 poz. 555 z późn. zm.)

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

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (tekst jedn. Dz.U. 2019 poz. 125 z późn. zm.)

Dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (tekst skonsolidowany Dz.U.UE.L.2002.201.37 z późn. zm.)

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 uchylająca decyzję ramową Rady 2008/977/WSiSW (tekst skonsolidowany. Dz. U. UE. L 119/89 z 4 maja 2016 z późn. zm.)

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) (tekst skonsolidowany. Dz. U. UE. L 119/1 z 4 maja 2016 z późn. zm.)

Czwarte sprawozdanie z działalności Wspólnego Organu Nadzorczego Europolu Decyzja ZSZZS.440.727.2018.

Druk nr 2989 Rządowy projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy numer 2989 Sejmu VIII Kadencji).

Orzecznictwo

Wyrok Sądu Okręgowego w Warszawie z dnia 7 lutego 2023 roku, sygn. akt III C 280/22.

Literatura

Dyka I.

2001 *Zasady przyznawania i ustalania wysokości zadośćuczynienia pieniężnego w razie naruszenia dobra osobistego*, „Kwartalnik Prawa Prywatnego", nr 3.

Gruszczak A.

2009 *Europejski Urząd policji (Europol) –okoliczności i geneza powstania,* „Politeja", nr 2(12).

Lach A.

2017 *Sankcje administracyjne i karne a zakaz podwójnego karania w świetle najnowszego orzecznictwa ETPCz i TS,* Lex.

Sinkiewicz A.

1998 *Pojęcie i rodzaj szkody w polskim prawie cywilnym*, „Rejent'', nr 2.

Szpunar A.
1975 *Ustalenie odszkodowania w prawie cywilnym*, Warszawa.

Źródła internetowe

Info.Policja.pl, *Współpraca Międzynarodowa*, https://info.policja.pl/inf/wspolpraca-miedzynarod/72445,Wspolpraca-miedzynarodowa.html [dostęp: 29.02.2024].

Mrożek J.W.
2022 *Odpowiedzialność karna a RODO*, https://rodoradar.pl/odpowiedzialnosc-karna-a-rodo/ [dostęp: 29.02.2024].

Urząd Ochrony Danych Osobowych „Informacje Ogólne", https://uodo.gov.pl/pl/90/166 [dostęp: 01.03.2024].

mgr **Patryk Łuczyński**
Uniwersytetu Łódzkiego
Absolwent

ODPOWIEDZIALNOŚĆ KARNA Z TYTUŁU NIELEGALNEGO PRZETWARZANIA DANYCH OSOBOWYCH

WPROWADZENIE

Dane osobowe stały się walutą XXI wieku. Płacimy nimi na co dzień, często nie zdając sobie nawet sprawy, że uzyskując pozornie bezpłatne usługi, poświęcamy w ten sposób pewną cząstkę swojej prywatności – np. zapisując się do różnego rodzaju newsletterów w zamian za zniżkę na zakupy, korzystając z „bezpłatnych" webinarów, czy też korzystając ze zniżek oferowanych w zamian za zgody marketingowe. Sami też zawężamy zakres naszej prywatności korzystając coraz to chętniej z różnego rodzaju mediów społecznościowych, na których prezentujemy różne obszary swojego życia prywatnego, w tym często nawet bardzo intymne i niegdyś ściśle chronione obszary tego życia. Powyższemu zjawisku sprzyja też rozwój społeczeństwa informacyjnego, które oparte jest właśnie na danych, informacji i wiedzy (Behr 2018, s. 20). Utopią byłoby obecnie stwierdzenie, że funkcjonowanie w rozwiniętym społeczeństwie możliwe byłoby bez ujawniania jakichkolwiek informacji na swój temat. Wydaje się to niemożliwe chociażby ze względu na związanie nas przepisami prawa, które już same w sobie wymagają ujawniania pewnych informacji na nasz temat. Samo zresztą ujawnianie i przetwarzanie informacji nie jest zjawiskiem negatywnym (Bielak-Jomaa, Soczyński 2017, s. 8) i sprzyja rozwojowi społecznemu i gospodarczemu.

Nie można jednak tracić z pola widzenia, że poszerzanie granic udostępnianych o nas informacji i coraz łatwiejsza dostępność do nich, sprzyja różnego

rodzaju nadużyciom w procesie ich przetwarzania, w tym naruszeniu naszej prywatności wbrew naszej woli, a także wykorzystywaniu takich danych osobowych w działalności przestępczej. Ryzyko dla jednostki związane z przetwarzaniem jej danych osobowych, które często odbywa się poza jej wiedzą i z wykorzystaniem rozwijającej się technologii, wymusza odpowiednią reakcję ze strony prawodawcy. Przejawem takiej reakcji jest wprowadzanie norm prawnokarnych, które mają zabezpieczać jednostki przed nielegalnym przetwarzaniem ich danych osobowych. To właśnie analiza norm prawnokarnych będzie przedmiotem niniejszego artykułu, w którym omówione będą zarówno przepisy karne zawarte bezpośrednio w regulacjach o ochronie danych osobowych, jak też przepisy części szczególnej Kodeksu karnego związane z ochroną informacji, w tym danych osobowych.

ŹRÓDŁA PRAWA OCHRONY DANYCH

Omówienie zagadnień związanych z nielegalnym przetwarzaniem danych osobowych i reakcją karnoprawną na takie działanie, musi poprzedzić krótka analiza źródeł prawa ochrony danych osobowych. Normy karnoprawne nie istnieją bowiem w próżni, lecz zabezpieczać mają one określone i społecznie akceptowalne wartości, które określane są najczęściej w normach prawnych innego typu – normach konstytucyjnych, cywilnoprawnych i administracyjnoprawnych. To one będą też wyznaczały granice legalnego i nielegalnego przetwarzania danych osobowych, które będzie zagrożone sankcja karną. Jednocześnie trzeba podkreślić, że poniższe omówienie ma jedynie charakter przyczynkowy i nie stanowi głównego przedmiotu niniejszej pracy.

W pierwszej kolejności należy wskazać, że prawo ochrony danych osobowych stanowi jedno z praw człowieka. Tradycyjnie prawo to przedstawiane jest jako jeden z elementów prawa do prywatności. Przy takim ujęciu jego źródłem jest już art. 12 Powszechnej Deklaracji Praw Człowieka z 1948 r., który przewiduje, że:

> „nikt nie będzie podlegać arbitralnemu wkraczaniu w jego życie prywatne, rodzinne, mieszkanie lub korespondencję, ani też zamachom na jego honor i reputację. Każdy jest uprawniony do ochrony prawnej przed takim wkraczaniem lub takimi zamachami".

Wśród międzynarodowych źródeł prawa odnoszących się do prywatności i wchodzącej w jej skład ochrony danych osobowych, wymienić należy też art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych.

W ramach aktów prawnych Rady Europy ochrona prywatności i związana z nią ochrona danych osobowych uregulowana jest w art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, który stanowi, że:

> 1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.
>
> 2. 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 osób.

Prawo do ochrony danych osobowych jest też prawem podstawowym Unii Europejskiej. Mowa o nim już w art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej, który stanowi, że: „każda osoba ma prawo do ochrony danych osobowych jej dotyczących". Prawo to jest również wymienione jest jako jedno z praw podstawowych w art. 7 i art. 8 Karty praw podstawowych Unii Europejskiej:

> Art. 7. Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się.
>
> Art. 8. 1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.
>
> 2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.
>
> 3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

Przedmiotowe prawo jest też oczywiście przedmiotem regulacji Konstytucji Rzeczypospolitej polskiej. Na gruncie konstytucyjnym powstały jednak wątpliwości, czy prawo to jest samodzielnym prawem podmiotowym, czy też jedynie elementem szerzej rozumianego prawa do prywatności, co wynika z ustalenia relacji pomiędzy art. 47 Konstytucji RP, przewidującym, że:

> Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

a art. 51 Konstytucji RP, który wskazuje, że:

> 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

> 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
>
> 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
>
> 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
>
> 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Początkowo ochrona danych osobowych postrzegana była jako element prawa do prywatności. Wskazywano, że jest to „wyspecjalizowana postać" tego prawa (Sajfan 1999, s. 10). Poglądowi takiemu sprzyjało stanowisko wyrażone przez Trybunał Konstytucyjny w wyroku z 19.05.1998 r. U 5/97, w którym wskazano, że regulacja art. 51 Konstytucji RP jest przejawem prawa do prywatności w aspekcie ochrony danych osobowych, a tym samym stanowi „konkretyzację prawa do prywatności w aspektach proceduralnych". Poglądowi temu trudno odebrać słuszność, bowiem niewątpliwie dane osobowe wchodzą w zakres prawa do prywatności sensu largo. Trzeba jednak zgodzić się też ze stanowiskiem, że prawo do ochrony danych osobowych nie może być rozumiane wyłącznie jako prawo do prywatności (Czerniawski 2022, s. 23). Gdyby taka była intencja prawodawcy, to z pewnością nie wyodrębniałby on prawa do ochrony danych osobowych w osobnym przepisie Konstytucji RP. Nie można też pomijać faktu, że rozwój technologicznym, postęp w zakresie praw informacyjnych i zmiany w zakresie postrzegania prywatności i jej ram, powodują że prawo do ochrony danych osobowych sięga do obszarów, które nie będą wchodziły w zakres prywatności, jak chociażby do ochrony danych publicznie dostępnych (Wygoda 2022, s. 50) – z mocy ustawy czy też na skutek działania jednostki. Zasadny jest wobec tego pogląd, że na gruncie Konstytucji RP mamy do czynienia z dwoma prawami podmiotowymi, tj. prawem do prywatności (art. 47) i prawem do ochrony danych osobowych (art. 51), a pomiędzy prawami tymi występuje relacja krzyżowania. Nie są one jednak ze sobą nierozerwalnie związane, a naruszenie jednego z nich nie musi wiązać się z naruszeniem drugiego (Barta, Markiewicz 1999, s. 380). Stanowisko takie znajduje potwierdzenie w orzecznictwie, w którym wskazuje się, że:

> Reżim ochrony prawa do prywatności mieszczący się w ramach powszechnych dóbr osobistych (oparty na przepisach Konstytucji i przepisach prawa cywilnego) i reżim ochrony danych osobowych (oparty na przepisach Konstytucji oraz ustawy o ochronie danych osobowych), są wobec siebie niezależne (wyrok Sądu Apelacyjnego w Warszawie z 25.11.2016 r. I ACa 1565/15).

Zagrożenia dla jednostek związane z przetwarzaniem danych osobowych, a także potrzeba pogodzenia ochrony tych danych z koniecznością rozwoju społecznego i technologicznego, do którego niezbędny jest dostęp do informacji, w tym danych osobowych i ich przetwarzanie, wymusiły też odpowiednią reakcję w prawodawstwie zwykłym. Przejawem takiej reakcji na gruncie prawa Unii Europejskiej była przyjęta 24 października 1995 r. dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu takich danych[1]. Dyrektywa miała na celu harmonizację ochrony danych osobowych w państwach członkowskich. Na gruncie krajowym pierwszym kompleksowym przejawem reakcji ustawodawcy na potrzebę ochrony danych osobowych była ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych[2]. Warto wskazać, że już powyższa ustawa przewidywała szereg przepisów karnych związanych z nielegalnym lub nieuprawnionym przetwarzaniem danych osobowych, a także naruszeniem innych obowiązków administratora.

Aktualnie kompleksowym aktem prawnym regulującym ochronę osób fizycznych w związku z przetwarzaniem ich danych osobowych jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. o ochronie osób fizycznych w związku z przetwarzaniem ich danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) („RODO")[3]. Skorzystanie z rozporządzenia jako narzędzia regulacji prawa ochrony danych powoduje, ze w całej Unii Europejskiej obowiązuje zasadniczo jeden akt normatywny. Zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej rozporządzenie ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich UE. Nie wymaga ono implementacji do prawa krajowego i w założeniach ma zapewniać jednostkom analogiczny poziom ochrony danych osobowych we wszystkich państwach członkowskich. Z art. 1 ust. 2 RODO dowiadujemy się, że chroni ono „podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych". RODO normuje ogólne zagadnienia związane z ochroną danych osobowych, w szczególności wprowadza definicje związane z tym obszarem, określa zasady przetwarzania danych, wprowadza podstawy legalizujące przetwarzanie danych,

[1] Dz. U. UE. L. 1995.281.31.
[2] Dz. U. z 2016 r. poz. 922.
[3] Dz. U. UE. L. 2016.119.1

reguluje prawa podmiotów danych, a także konsekwencje administracyjnoprawne i cywilnoprawne związane z naruszeniem przepisów tego aktu.

Pomimo tego, że RODO stanowi podstawowy akt regulujący ochronę danych osobowych, to pewne obszary wymagają doregulowania po stronie ustawodawcy krajowego, z uwagi na brak kompetencji prawodawcy unijnego do regulacji zagadnień proceduralnych i kwestii ustrojowych związanych z wyznaczeniem organu nadzorczego (Fajgielski 2022, s. 778). Samo RODO wskazuje też obszary, których uregulowanie lub zakres uregulowania pozostawiony został uznaniu państw członkowskich, a przejawem takiego obszaru jest wprowadzenie dodatkowych sankcji związanych z naruszeniami przepisów o ochronie danych osobowych, w tym sankcji karnych. Wskazane wyżej zagadnienia, których uregulowanie jest przedmiotem ustawodawcy stały się przedmiotem ustawy z 10 maja 2018 r. o ochronie danych osobowych („u.o.d.o."). Warto wskazać, że pomimo swojej nazwy sama ustawa w niewielkim zakresie odnosi się do ochrony danych osobowych sensu stricte, gdyż ta materia uregulowana jest przede wszystkim w RODO. Ustawa o ochronie danych osobowych skupia się na regulacji kwestii proceduralnych, a także kwestii ustrojowych związanych z wyznaczeniem i pozycją Prezesa Urzędu Ochrony Danych Osobowych, jako organu nadzorczego w sprawach ochrony danych. Reguluje też ona pewne wyjątki od zastosowania RODO, sposób prowadzenia kontroli w sprawach naruszenia przepisów o ochronie danych osobowych, a także najbardziej interesujące nas zagadnienie – sankcje karne. Trzeba jednak podkreślić, że istotnym niedopowiedzeniem byłoby zakończenie rozważań na temat źródeł ochrony danych osobowych na wskazaniu jedynie ww. aktów prawnych. W prawie krajowym kwestie ochrony danych osobowych uregulowane są też bowiem w szeregu innych ustaw i pomimo, że regulacje te mają zwykle charakter fragmentaryczny, to odgrywają istotne znaczenie praktyczne. Przykładem takiej regulacji są przepisy ustawy z 26 czerwca 1974 r. Kodeks pracy, która reguluje kwestie ochrony danych osobowych na etapie rekrutacji i zatrudnienia przez wskazanie katalogu danych osobowych, których pracodawca może żądać od pracownika lub kandydata na pracownika, określenie zasad stosowania monitoringu wizyjnego w zakładzie pracy, czy też wykorzystania innych form monitorowania. Ochronie danych osobowych poświęcona jest też m.in. ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, która określa m.in. zasady i warunki ochrony danych osobowych przetwarzanych w ramach postępowań karnych. Trzeba też w końcu zauważyć, że ochrona informacji – w tym też danych osobowych – jest przedmiotem regulacji karnej, w szczególności rozdziału XXXIII

– przestępstwa przeciwko ochronie informacji zawartego w ustawie z 6 czerwca 1997 r. Kodeks karny („k.k.").

OCHRONA DANYCH OSOBOWYCH A PRZEPISY KARNE

Przepisy prawa karnego co do zasady nie służą do regulacji stosunków społecznych, lecz jedynie do ich zabezpieczenia. Co więcej, stosowanie odpowiedzialności karnej, jako *ultima ratio*, powinno być ograniczone do tych sytuacji, w których niewystarczające jest zastosowanie sankcji innego rodzaju – w szczególności, gdy niewystarczająca jest odpowiedzialność cywilno-, czy administracyjnoprawna. W przypadku sankcji karnych związanych z naruszeniem przepisów o ochronie danych osobowych w doktrynie podaje się w wątpliwość zasadność ich wprowadzenia, szczególnie w obliczu dotkliwych sankcji administracyjnoprawnych (czy też administracyjno-karnych), które zabezpieczają ich przestrzeganie (Sołtys 2019, s. 29-52). Nie rozstrzygając zasadności tych zarzutów, trzeba zwrócić uwagę, że w systemie prawnym funkcjonuje obecnie szereg przepisów karnych, które zabezpieczają prawidłowe przetwarzanie danych osobowych, czy szerzej – informacji. Tym samym ustalenie zakresu kryminalizacji nielegalnego przetwarzania danych osobowych nie może ograniczać się jedynie do analizy art. 107 u.o.d.o., który oczywiście ma w tym zakresie pierwszorzędne znaczenie, lecz wymaga sięgnięcia też do przepisów części szczególnej Kodeksu karnego, w szczególności do art. 190a § 2, art. 266, art. 267 oraz art. 268, które penalizują określone działania związane z bezprawnym przetwarzaniem danych.

Wypada już na wstępie wskazać, że zarówno w stosunku do tych przestępstw, które uregulowane są w Kodeksie karnym, jak też do występków uregulowanych w u.o.d.o. stosuje się przepisy części ogólnej k.k. W związku z tym pomimo tego, że w dalszej części mowa będzie o dokonaniu określonych przestępstw, to karane jest również usiłowanie ich dokonania, czy też podżeganie do ich popełnienia. Przed nawias wypada też wyciągnąć to, że odpowiedzialność karną za nielegalne przetwarzanie danych osobowych – zarówno w ujęciu wynikającym z u.o.d.o., jak też z przepisów k.k., które penalizują poszczególne nielegalne czynności przetwarzania, ponosić mogą wszelkie osoby zdolne do ponoszenia odpowiedzialności karnej. Wszystkie z opisanych poniżej przestępstw mają bowiem charakter przestępstw powszechnych, a zatem odpowiedzialność za ich popełnienie ponosić może co do zasady osoba, która ukończyła 17 rok życia i której można przypisać winę w popełnieniu czynu zabronionego.

OCHRONA DANYCH OSOBOWYCH NA GRUNCIE U.O.D.O.

Szeroka gama czynów zabronionych uregulowana była w nieobowiązującej już ustawie o ochronie danych osobowych z 1997 r. W ostatnio obowiązującej przed uchyleniem wersji, ustawa ta penalizowała takie czyny zabronione jak:

1. niedopuszczalne przetwarzanie danych osobowych w zbiorze, jak też przetwarzanie takich danych osobowych przez osobę nieuprawnioną (art. 49),
2. udostępnienie lub umożliwienie dostępu do danych osobowych przetwarzanych w zbiorze osobom nieupoważnionym (art. 51),
3. naruszenie, choćby nieumyślnie, obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem (art. 52),
4. niezgłoszenie do rejestru zbioru danych pomimo obowiązku dokonania takiego zgłoszenia (art. 53),
5. niedopełnienie przez administratora obowiązków informacyjnych wobec osoby, której dane dotyczą (art. 54),
6. udaremnianie lub utrudnianie wykonywania czynności kontrolnych przez upoważnionego inspektora (art. 54a).

Wskazanym wyżej regulacjom zarzucano niską efektywność, na co wskazywały statystyki związane z wykrywaniem i ściganiem sprawców ww. czynów zabronionych. W stosunku do nielegalnego lub nieuprawnionego przetwarzania danych osobowych, braku efektywności dopatrywano się w tym, że działanie sprawcy musiało odbywać się na zbiorze danych (Barta, Litwiński 2016, s. 447-448).

Zmiany w sferze sankcji karnych nastąpiły po rozpoczęciu obowiązywania RODO, czyli w 2018 roku, kiedy to doszło też do uchylenia przepisów dotychczas obowiązującej ustawy o ochronie danych osobowych z 1997 r. Przepisy RODO nie wprowadzają sankcji karnych za naruszenie przewidzianych w nim obowiązków, ograniczając się jedynie do uregulowania zasad odpowiedzialności cywilnoprawnej oraz administracyjnoprawnej, w tym dotkliwych administracyjnych kar pieniężnych. Jednocześnie jednak przepisy tego aktu przyznają państwom członkowskim prawo wdrożenia innych sankcji, wskazując w art. 84 ust. 1 RODO, że:

> Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające

> administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

Dodatkowo w motywach 149 i 152, prawodawca unijny wyjaśnił, że:

> (149) Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Sankcje karne mogą również obejmować pozbawienie zysków wynikających z naruszenia niniejszego rozporządzenia. Jednak nałożenie sankcji karnych za naruszenie takich krajowych przepisów oraz nałożenie sankcji administracyjnych nie powinno prowadzić do naruszenia zasady ne bis in idem, zgodnie z wykładnią Trybunału Sprawiedliwości.
>
> (152) W sytuacjach, w których niniejsze rozporządzenie nie harmonizuje sankcji administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia niniejszego rozporządzenia, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające sankcje. Charakter takich sankcji (karny lub administracyjny) powinno określać prawo państwa członkowskiego.

Prawodawca krajowy zdecydował się skorzystać z uprawnienia do ustanowienia dodatkowych sankcji za najpoważniejsze – w swojej ocenie – naruszenia przepisów o ochronie danych, wprowadzając w tym celu przepisy karne art. 107 i art. 108 u.o.d.o. W art. 108 § 1 u.o.d.o. przewidziano odpowiedzialność za udaremnianie lub utrudnianie przeprowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych, co powoduje, że przepis ten odpowiada zakresowo art. 54a ustawy o ochronie danych osobowych z 1997 r. Z kolei w § 2 ww. przepisu penalizacji poddane zostało niedostarczenie w toku postępowania w sprawie nałożenia administracyjnej kary pieniężnej dokumentów niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej. Dla potrzeb niniejszego artykułu istotne znaczenie ma natomiast art. 107 u.o.d.o. w brzmieniu:

> Art. 107. [Nielegalne przetwarzanie danych osobowych]
>
> 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
>
> 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Wskazany przepis odpowiada zasadniczo treści art. 49 ustawy o ochronie danych osobowych z 1997 r., z tym wyjątkiem, że nie wymaga on obecnie, aby dane osobowe przetwarzane w sposób opisany we wskazanym przepisie znajdowały się w zbiorze. To z kolei prowadzi do poszerzenia się przedmiotowego zakresu penalizacji nielegalnego lub nieuprawnionego przetwarzania danych.

Obecne brzmienie u.o.d.o. prowadzi do wniosku, że ustawodawca zdecydował się na znaczne ograniczenie liczby przepisów karnych w porównaniu do poprzednio obowiązującej ustawy o ochronie danych osobowych z 1997 r. Na etapie projektowania nowej ustawy dostrzeżono słusznie nieefektywność wcześniejszej regulacji, ale też dostrzeżono, że prawo karne jako *ultima ratio*, powinno być zarezerwowane dla najcięższych naruszeń przepisów i to takich, dla których sankcja administracyjnoprawna – przewidziana w RODO – może być niewystarczająca (Uzasadnienie do projektu ustawy o ochronie danych osobowych z projektami aktów wykonawczych, druk Sejmowy 2410 z 5.04.2018 r.). Zmiany te należy ocenić pozytywnie, bowiem eliminują one przynajmniej częściowo wątpliwości co do nadmiarowości regulacji karnej w obszarze ochrony danych osobowych, którą było penalizowanie takich czynów jak brak obowiązku odpowiedniego zabezpieczenia danych osobowych, czy też niezrealizowanie obowiązku informacyjnego wobec osoby, której dane dotyczą.

ZASTOSOWANIE PRZEPISÓW U.O.D.O. A ZAKRES ZASTOSOWANIA RODO

Przed przejściem do szczegółowej analizy art. 107 u.o.d.o. należy zwrócić uwagę na zakres obowiązywania przepisów u.o.d.o., który ma wpływ na możliwość stosowania sankcji karnych. Ustawodawca w art. 1 ust. 1 wskazał, że:

> Ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 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/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej "rozporządzeniem 2016/679".

Literalne brzmienie wskazanego przepisu nie pozostawia wątpliwości, że przepisy u.o.d.o., a tym samym również przepisy karne, stosuje się wyłącznie do takiego przetwarzania danych osobowych, które pozostaje w zakresie terytorialnego i materialnego obowiązywania RODO. *A contrario* nie można stosować

sankcji karnych do czynów, które nie będą podlegały przepisom RODO, w szczególności takim, które objęte będą wyjątkami od obowiązku stosowania tego aktu. Terytorialny zakres obowiązywania RODO wyznaczony jest art. 3 tego aktu. Z perspektywy artykułu istotniejsze znaczenie ma jednak materialny zakres stosowania przepisów ww. aktu, który wynika z art. 2 RODO wskazującego, że przepisy tego aktu, a tym samym – przepisy u.o.d.o. stosujemy do:

1. przetwarzania danych osobowych **osób fizycznych** – tym samym przetwarzanie ma dotyczyć danych osobowych żyjących ludzi. Nie stosuje się przepisów RODO do przetwarzania informacji o osobach zmarłych ani o osobach prawnych,
2. przetwarzania danych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić cześć zbioru danych – zautomatyzowane przetwarzanie danych można rozumieć, jako przetwarzanie (całkowite lub częściowe) z wykorzystaniem komputera lub systemu informatycznego, zaś przetwarzanie inne niż zautomatyzowane jako przetwarzanie manualne,
3. z wyjątkiem przetwarzania danych osobowych:
    - w ramach działalności nieobjętej zakresem prawa Unii – przejawem takiej działalności są działania odnoszące się do bezpieczeństwa narodowego (Fajgielski 2022, s. 95),
    - przez państwo członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdziału 2 TUE – chodzi w tym zakresie o działania dotyczące wspólnej polityki zagranicznej i bezpieczeństwa Unii Europejskiej,
    - przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze – chodzi o takie czynności, które pozostają bez związku z działalnością zawodową, handlową lub społeczną, związane przede wszystkim z życiem prywatnym lub rodzinnym jednostki (por. Lubasz 2018, s. 134-135; wyrok Trybunału Sprawiedliwości UE z 6.11.2003 r. C-101/01),
    - przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Wymaga jednak odnotowania, że w doktrynie pojawił się też odmienny pogląd, który zakłada, że przepisy karne u.o.d.o. dotyczące niedopuszczalnego lub nieuprawnionego przetwarzania danych osobowych stosuje się „bez względu na to, czy do przetwarzania stosuje się RODO czy też nie" (Gawroński, Kloc 2018, s. 674). Pogląd taki nie zasługuje na akceptację, bowiem pozostaje w sprzeczności z literalnym brzmieniem art. 1 ust. 1 u.o.d.o. Normę prawną i opis czynu karalnego rekonstruować należy nie tylko na gruncie konkretnego przepisu, lecz z uwzględnieniem m.in. zakresu podmiotowego i przedmiotowego ustawy, w której dany przepis został uregulowany (por. Zoll 2016, s. 40) – co w przypadku art. 107 u.o.d.o. wymaga uwzględnienia również art. 1 ust. 1 tej ustawy. Wobec tego, przyjęcie poglądu zaprezentowanego przez ww. autorów, prowadziłoby do rozszerzającej wykładni normy prawnej prawa karnego, co jest niedopuszczalne szczególnie w sytuacji, gdy wykładnia taka byłaby niekorzystna dla oskarżonego – a tak niewątpliwie byłoby w ww. sytuacji wobec poszerzenia granic penalizacji.

Podsumowując, przyjąć należy, że przepisy karne przewidziane w u.o.d.o. stosuje się tylko do takich przypadków nielegalnego lub nieuprawnionego przetwarzania danych osobowych, do których zastosowanie znajdują przepisy RODO. Tym samym, nie będzie mogło być rozpatrywane na gruncie ww. przepisów przetwarzanie danych osobowych dokonane, np. przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Przykładem takich czynności może być zapoznanie się ujawnioną w Internecie bazą imion i nazwisk oraz numerów PESEL, na którą internauta natknie się w czasie standardowego przeglądania sieci. Pomimo, że zapoznanie się z danymi osobowymi stanowi operacje przetwarzania danych osobowych i trudno przyjąć, aby rzeczony internauta dysponował uprawnieniem do przetwarzania tych danych, to nie znajdą do niego zastosowania przepisy u.o.d.o., bowiem korzysta on z wyłączenia przewidzianego w art. 2 ust. 2 lit. c RODO. Oczywiście sytuacja ta wyglądałaby odmiennie, gdyby internauta uzyskał dostęp do ww. bazy danych na skutek przełamania lub ominięcia zabezpieczeń, bądź gdyby wykorzystał wskazane dane.

NIELEGALNE LUB NIEUPRAWNIONE PRZETWARZANIE DANYCH – ART. 107 U.O.D.O.

Czyn zabroniony opisany w art. 107 u.o.d.o. może być popełniony w dwóch postaciach, a mianowicie przez:

1. przetwarzanie danych osobowych, choć ich przetwarzanie nie jest dopuszczalne, albo
2. przetwarzanie danych osobowych przez osobę, która do ich przetwarzania nie jest uprawniona.

Przestępstwo to może być popełnione w typie podstawowym, jeżeli przedmiotem przetwarzania są dane osobowe zwykłe (ust. 1), jak też w typie kwalifikowanym, gdy przetwarzaniem objęte są dane osobowe szczególnych kategorii (ust. 2). Wskazane przepisy mają charakter przepisów blankietowych (Bekrycht, Leszczyński, Łabieniec 2021), gdyż do zdekodowania ich treści konieczne jest sięgnięcie do innych przepisów regulujących kwestie legalności przetwarzania i uprawnień do dokonywania takiej czynności, jak też definiujących pojęcie danych osobowych i przetwarzania, które jest kluczowe dla ustalenia zakresu penalizacji wskazanej normy. Przepisami takimi są przepisy RODO, które w art. 4 pkt 1-2 definiują pojęcie danych osobowych i przetwarzania jako:

> 1) „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą") (…)
>
> 2) „przetwarzanie" oznacza operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Pojęcie danych osobowych przyjęte na gruncie art. 4 pkt 1 RODO jest bardzo pojemne, a wyjaśnienie wszelkich związanych z nim wątpliwości wykracza poza granice tego opracowania. Wyróżnia się dwie kategorie danych osobowych, tj. dane osobowe zwykłe, w tym dane osobowe karne obejmujące informacje o wyrokach skazujących, czynach zabronionych oraz powiązanych z nimi środkach bezpieczeństwa, a także dane osobowe szczególnych kategorii. Danymi osobowymi mogą być wszelkiego rodzaju informacje, nie tylko takie, które intuicyjnie utożsamiamy z takimi danymi, jak imię i nazwisko, adres zamieszkania, numer PESEL, numer dowodu osobistego, czy wizerunek (por. Łuczyński,

2023), ale też takie, których związek z konkretną osobą fizyczną nie zawsze jest oczywisty, np. adres IP, numer księgi wieczystej (zob. decyzja Prezesa UODO z 7.07.2022 r. DKN.5131.27.2022, wyrok WSA w Warszawie z 5.05.2021 r. II SA/Wa 2222/20), adres e-mail (zob. decyzja prezesa UODO z 31.07.2023 r. DS.523.5172.2022)[4], numer kadrowy, czy numer rachunku bankowego, pod warunkiem, że identyfikują albo pozwalają na identyfikację konkretnego człowieka. Danymi osobowymi zwykłymi, o których wyżej mowa są wszelkie informacje identyfikujące lub pozwalające na identyfikację osoby fizycznej, które nie są danymi szczególnych kategorii. Z kolei zakres informacji, które uważane są za dane osobowe szczególnych kategorii wyznacza art. 9 ust. 1 RODO, który wskazuje, że w zakres tych danych wchodzą dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Przykładem danych osobowych szczególnych kategorie są informacje o przebywaniu przez konkretną osobę na zwolnieniu lekarskim (zob. decyzja Prezesa UODO z 25.11.2022 r. DS.523.2704.2022)[5].

Podział danych osobowych na dane osobowe zwykłe i dane osobowe szczególnych kategorii ma istotne znaczenie na gruncie art. 107 u.o.d.o., bowiem jak już wcześniej wskazano, kategorie danych determinują, czy mamy do czynienia z występkiem w typie podstawowym, który zagrożony jest grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat dwóch, czy też w typie kwalifikowanym, który zagrożony jest grzywną, karą ograniczenia wolności albo pozbawienia wolności do lat trzech.

---

[4] We wskazanej decyzji Prezes UODO udzielił upomnienia za naruszenie art. 6 ust. 1 RODO, które polegało na udostępnieniu podmiotom do tego nieuprawnionym danych osobowych Pana B.K. w zakresie adresu poczty elektronicznej. W uzasadnieniu decyzji Prezesa UODO wskazano, że: *„adres poczty elektronicznej Skarżącego: […] – udostępniony w liście mailingowej wiadomości elektronicznej Spółki z dnia […] czerwca 2022 r. – stanowi dane osobowe w rozumieniu rozporządzenia 2016/679 tym bardziej, że zawiera w swej konstrukcji jego imię i nazwisko. Umożliwia on bowiem pozostałym odbiorcom wiadomości jednoznaczną identyfikację Skarżącego bez poniesienia nadmiernych kosztów, działań lub czasu"*

[5] W decyzji Prezes UODO udzielił administratorowi upomnienia za naruszenie art. 9 ust. 1 RODO do którego doszło na skutek udostępnienia nieuprawnionej osobie danych osobowych skarżącej w zakresie danych dotyczących zdrowia, tj. udostępnienia informacji o fakcie przebywania przez nią na zwolnieniu lekarskim pełnomocnikowi kontrahenta. W uzasadnieniu decyzji wskazano: *„Informacja o przebywaniu przez Skarżącą na zwolnieniu lekarskim jest daną dotyczącą zdrowia, ponieważ ujawnia informację o stanie zdrowia Skarżącej oraz o korzystaniu przez nią z usług opieki zdrowotnej, jako że sam fakt otrzymania zwolnienia lekarskiego oznacza, że Skarżąca z takiej usługi skorzystała, jak również, że z uwagi na stan zdrowia nie powinna ona wykonywać pracy na zajmowanym stanowisku".*

Dla ustalenia zakresu ww. normy prawnej znaczenie ma też pojęcie przetwarzania danych. W pewnym skrócie można przyjąć, że jest nim dokonywanie jakichkolwiek operacji na danych osobowych w ramach całego cyklu ich życia – czyli od momentu pozyskania aż do momentu ich usunięcia. Operacje takie mogą być dokonywane zarówno w formie zautomatyzowanej, jak też w formie niezautomatyzowanej, co oznacza, że w zakres przetwarzania wejdzie przetwarzanie z wykorzystaniem algorytmów, baz danych, komputerów, jak też takie przetwarzanie, które odbywać będzie się z pomocą papierowych nośników danych, w sposób manualny.

Kolejnym elementem omawianej normy art. 107 u.o.d.o., który wymaga wyjaśnienia jest pojęcie nielegalnego przetwarzania danych. Pojęcie to jest nieostre i niezdefiniowane. To z kolei prowadzi do istotnych rozbieżności, które powstały w doktrynie na tle dekodowania zakresu kryminalizacji art. 107 u.o.d.o. Maciej Nawacki (Nawacki 2021, s. 317) twierdzi, że:

> zakres kryminalizacji art. 107 UODO ograniczony jest do najpoważniejszych naruszeń ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO i art. 33 ust. 1 RODO. Dany czyn wyczerpuje znamiona przestępstwa nielegalnego przetwarzania danych, o ile stanowi jednocześnie naruszenie ochrony danych osobowych.

W ocenie ww. autora, z przestępstwem nielegalnego przetwarzania danych osobowych, o którym mowa w art. 107 u.o.d.o. mielibyśmy do czynienia jedynie w sytuacji, gdy działanie, o którym mowa w tym przepisie, stanowiłoby jednocześnie naruszenie ochrony danych osobowych zdefiniowane w art. 4 pkt. 12 RODO, jako:

> naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

Takie stanowisko nie zasługuje na aprobatę, gdyż prowadziłoby do znaczącego zawężenia zakresu kryminalizacji. Autorowi ww. poglądu zdaje się umykać fakt, że samo naruszenie ochrony danych osobowych nie zawsze skutkuje przetwarzaniem danych osobowych w sposób niedopuszczalny, o którym mowa w art. 107 u.o.d.o. Naruszenie ochrony danych osobowych dotyczy zwykle takich danych, które przetwarzane są w sposób legalny (w oparciu o przesłanki legalizujące, o których mowa w art. 6 ust. 1 lub art. 9 ust. 2 RODO), ale w stosunku, do których dochodzi do utraty atrybutu poufności, dostępności lub integralności. Trzeba też pamiętać, że co do zasady zapewnienie bezpieczeństwa danych osobowych

jest obowiązkiem administratora danych i podmiotu przetwarzającego, a uchybienie temu obowiązkowi jest przedmiotem odpowiedzialności administracyjnoprawnej na gruncie RODO i odpowiedzialność taka jawi się jako wystarczająca. Przyjęcie stanowiska zaproponowanego przez M. Nawackiego prowadziłoby też do niedających się zaakceptować wniosków, że np. pobranie cudzych danych osobowych z ogólnodostępnych baz danych (np. KRS, CEIDG) i wykorzystanie ich do zaciągnięcia na ich podstawie zobowiązań finansowych, nie mogłoby być rozpatrywane jako nielegalne przetwarzanie danych osobowych, gdyż nie doszłoby do naruszenia bezpieczeństwa. Należy też przyjąć, że racjonalny ustawodawca konstruując treść art. 107 u.o.d.o. i chcąc powiązać nielegalne przetwarzanie danych osobowych z naruszeniem ochrony danych osobowych dałby temu wyraz w treści przepisu.

Inne spojrzenie na niedopuszczalne lub nieuprawnione przetwarzanie danych osobowych prezentuje P. Poniatowski (Poniatowski 2021, s. 73-77) według którego niedopuszczalność przetwarzania danych osobowych będzie zachodziła w razie przetwarzania danych pomimo braku co najmniej jednej z przesłanek legalizujących, o których mowa w art. 6 ust. 1 albo art. 9 ust. 2 RODO, jak też wówczas, gdy przetwarzanie następuje z naruszeniem zasad przetwarzania wymienionych w art. 5 lit. b-e RODO, czyli zasady ograniczenia celu, minimalizacji danych, prawidłowości lub ograniczenia przetwarzania. Wskazany autor utożsamia też niedopuszczalne przetwarzanie danych osobowych z przetwarzaniem danych pomimo wniesienia uzasadnionego sprzeciwu wobec przetwarzania, przetwarzania danych mimo prawnego obowiązku ich usunięcia, czy też przetwarzanie danych zebranych w związku z oferowaniem usług społeczeństwa informacyjnego pomimo żądania ich usunięcia, a także przetwarzanie polegające na przekazaniu danych do państwa trzeciego wbrew przepisom RODO. Poglądy ww. autora wydają się prowadzić do rozszerzającej interpretacji art. 107 u.o.d.o.

Warto wskazać, że wskazany przepis u.o.d.o. stanowi o przetwarzaniu danych osobowych, choć ich przetwarzanie nie jest dopuszczalne. Brak jest zatem podstaw do rozszerzania zakresu penalizacji na naruszanie zasad przetwarzania określonych w art. 5 RODO. Wydaje się, że intencją prawodawcy było powiązanie normy karnej z przetwarzaniem danych osobowych, które nie będzie mogło być oparte na żadnej z przesłanek legalizujących przetwarzanie, o których mowa w art. 6 ust. 1 RODO w stosunku do danych osobowych zwykłych lub art. 9 ust. 2 RODO, w przypadku danych osobowych szczególnych kategorii, i tak też należy postrzegać niedopuszczalne przetwarzanie (Barta 2018, s. 310-311). W grę wchodzą przy tym zarówno sytuacje, gdy od początku brak jest podstawy do

przetwarzania danych osobowych, np. zgody na przetwarzanie danych, czy prawnie uzasadnionego interesu w przetwarzaniu takich danych, jak też takie sytuacje, gdy podstawa przetwarzania odpadnie w trakcie tych operacji – np. na skutek wyrażenia skutecznego sprzeciwu wobec przetwarzania danych w związku z marketingiem bezpośrednim albo sprzeciwu wobec przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu administratora w związku ze szczególną sytuacją podmiotu danych. Podstawa taka odpadnie też w momencie wycofania zgody na przetwarzanie danych osobowych, która to czynność prowadzić będzie do tego, że dane osobowe, których przetwarzanie oparte było wyłącznie na tej podstawie, nie może być kontynuowane.

Drugą czynnością sprawczą na gruncie art. 107 u.o.d.o. jest przetwarzanie danych osobowych przez osobę, która do takiego przetwarzania nie jest uprawniona. Na podstawie przepisów RODO do przetwarzania danych osobowych uprawniony jest administrator, czyli podmiot (osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot), który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt. 7 RODO), a w oparciu o jego polecenie również podmiot przetwarzający, czyli podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt. 8 RODO). Ponadto, dane osobowe mogą być przetwarzane również przez osoby, które zostały upoważnione do tego przez administratora lub podmiot przetwarzający, w szczególności przez pracowników takich podmiotów.

Nieuprawnione przetwarzane danych osobowych może więc polegać na tym, że osoba, która dokonuje takiej czynności nie jest w ogóle uprawniona do przetwarzania danych osobowych, np. gdy dokona ona przywłaszczenia bazy danych osobowych. Z takim nieuprawnionym przetwarzaniem możemy też mieć jednak do czynienia, gdy osoba upoważniona do przetwarzania danych osobowych przekroczy zakres tego upoważnienia, np. gdy pracownik upoważniony wyłącznie do przetwarzania danych osobowych na potrzeby nadawania uprawnień do systemów informatycznych, dopuści się przetwarzania danych osobowych zawartych w aktach osobowych pracowników, czy też gdy pracownik działu kadr odpowiedzialny za sporządzenie dla pracowników deklaracji PIT-11 postanowi zaoferować swoim kolegom i koleżankom z pracy swoje prywatne usługi księgowe, kierując na ich prywatne numery telefonu pozyskane z akt pracowniczych wiadomości SMS z ofertą rozliczenia PIT-36.

Warto wskazać, że osoba dopuszczająca się przetwarzania danych osobowych bez odpowiedniego uprawnienia może jednocześnie dopuszczać się przetwarzania danych osobowych, pomimo, że nie jest ono dopuszczalne. Przykładem takiej

sytuacji jest sprawa rozpatrywana przez Sąd Rejonowy w Toruniu, która zakończyła się wyrokiem z 23.06.2022 r. II K 1544/21. Sąd uznał w przedmiotowej sprawie za winną popełnienia przestępstwa z art. 107 ust. 1-2 u.o.d.o. oskarżoną, która jako lekarz ginekolog logowała się z wykorzystaniem cudzego numeru PESEL na profil osoby, do której ten numer należał – w systemie medycznym (jak wydaje się z uzasadnienia orzeczenia), uzyskując w ten sposób dostęp do danych osobowych takiej osoby, w tym do danych dotyczących jej zdrowia.

Czyny zabronione opisane w art. 107 u.o.do. mogą być popełnione jedynie umyślnie w zamiarze bezpośrednim, jak i ewentualnym (Słabuszewski 2020, s. 177). Omawiane występki mają charakter powszechny, co oznacza, że mogą one zostać popełnione przez każdą osobę zdolną do ponoszenia odpowiedzialności karnej na gruncie Kodeksu karnego, z tym zastrzeżeniem, że sprawcą nieuprawnionego przetwarzania danych osobowych, może być jedynie taka osoba, która w konkretnych okolicznościach faktycznych takim uprawnieniem nie dysponuje. W tym zakresie wskazać wypada, że upoważnienie do przetwarzania danych osobowych może wynikać z przepisu ustawy, statusu (administratora), jak też z czynności prawnej, np. zawartej umowy powierzenia, która upoważnia podmiot przetwarzający do przetwarzania danych osobowych w imieniu administratora, a także z oświadczenia administratora lub podmiotu przetwarzającego, którzy mogą upoważnić do przetwarzania w ich imieniu danych osobowych swoich pracowników lub współpracowników. Istotne jest przy tym, że upoważnienie może też wynikać z okoliczności faktycznych, np. pracy na określonym stanowisku, które ściśle wiąże się z określonymi operacjami przetwarzania danych.

Warto również wskazać, że nielegalne lub nieuprawnione przetwarzanie danych osobowych ma charakter przestępstwa formalnego. Do wypełnienia znamion tych czynów nie jest konieczne nastąpienie jakiegokolwiek skutku, a w szczególności wystąpienie szkody majątkowej lub niemajątkowej u osoby, której dane dotyczą. Ściganie tych czynów następuje z urzędu. Z uwagi na ustawowe zagrożenie karą przewidziane za omawiany występek, możliwe jest zastosowanie wobec sprawcy warunkowego umorzenia postępowania, jak też odstąpienie od wymierzenia kary (por. Łuczak-Tarka 2019, s. 532).

Odnotowania wymaga także to, że w doktrynie podnoszone są wątpliwości co do zgodności art. 107 u.o.d.o. z Konstytucją RP, a w szczególności zasadą proporcjonalności i określoności przepisów. Zarzuty te odnoszą się m.in. do niedostatecznie precyzyjnego określenia strony przedmiotowej omawianego występku nielegalnego przetwarzania danych (Sołtys 2019, s. 39-40). Zarzutom tym trudno odebrać słuszność, o czym świadczą wskazane wyżej różnice w interpretacji

znamion art. 107 u.o.d.o., które w zależności od przyjętej wersji mogą prowadzić do przyjęcia bardzo szerokiego lub wąskiego zakresu penalizacji. Trudności w wykładni znamion art. 107 u.o.d.o., która jak już wyżej wskazano wymaga uwzględnienia art. 1 ust. 1 u.o.d.o. widoczne są również w orzecznictwie, przy czym trzeba podkreślić, że dotychczasowe orzecznictwo w sprawach nielegalnego lub nieuprawnionego przetwarzania danych osobowych jest bardzo skromne. Warto jednak zwrócić uwagę na wyrok Sądu Rejonowego w Lesznie z 5.06. 2023 r. II K 761/21, który zapadł w sprawie nielegalnego przetwarzania danych osobowych. Stan faktyczny, który był przedmiotem oceny sądu wyglądał następująco – mężczyzna zwrócił się do Sądu o wgląd w akta postępowania sądowego, którego był stroną. Po zgłoszeniu się do Sądu przy stanowisku ochrony mężczyźnie udostępniono akta postępowania. Okazało się jednak, że wraz z aktami przekazano mu odręczne notatki sędziego poczynione w sprawie, której dotyczyły akta, które to notatki były jednak dokonane na kserokopiach projektów orzeczeń w innych sprawach, a projekty te obejmowały też dane stron i uczestników tych postepowań. Notatki te nie były wpięte do akt i ponumerowane, jednak zostały udostępnione mężczyźnie wraz z aktami sprawy, w której był on stroną. Mężczyzna ten złożył wniosek o dokonanie fotokopii konkretnych, wskazanych przez siebie kart sprawy i zgodnie z zarządzeniem prezesa sądu uzyskał na to zgodę – nie obejmowała ona zgody na fotokopie projektów orzeczeń, o których wyżej mowa. Oskarżony wykonał fotokopie akt, w tym sfotografował też odręczne notatki sędziego poczynione na ww. dokumentach. Następnie skontaktował się on z inspektorem ochrony danych Sądu informując go, że jest w posiadaniu danych osobowych osób trzecich, wobec których toczą się postępowania przed Sądem. Jak wynika z uzasadnienia ww. wyroku, oskarżony miał sugerować inspektorowi ochrony danych błąd po stronie pracownika Sądu, a dalej poinformować inspektora, ze trafił na te dane przez przypadek przeglądając akta swojej sprawy. W związku z ww. stanem faktycznym mężczyzna został oskarżony o przestępstwo z art. 107 ust. 1 u.o.d.o., które miał popełnić w ten sposób, że nie będąc do tego uprawnionym podczas czynności zapoznawania się z aktami sprawy, przetwarzał dane osobowe stron i uczestników innych postępowań toczących się w Sądzie, przez wykonywanie fotokopii materiałów niestanowiących integralnej całości z udostępnionymi mu aktami, niezgodnie z zarządzeniem o wyrażeniu zgody na wykonanie fotokopii materiałów. Wskazany wyrok był przedmiotem postępowania apelacyjnego, w którym Sąd Okręgowy w poznaniu utrzymał zaskarżony wyrok w mocy.

Nie oceniając słuszności wskazanych orzeczeń zauważyć należy, że ze sporządzonych w sprawie uzasadnień – sądu I i II instancji, nie wynika aby przedmiotem zainteresowania sądu była analiza działania oskarżonego z perspektywy materialnego zakresu zastosowania RODO, a tym samym, aby sądy oceniły, czy w sprawie możliwe było stosowanie przepisów u.o.d.o. Kwestia ta nie jest natomiast oczywista, bowiem samo dokonanie czynności przeglądania akt zdaje się nie wykraczać poza przetwarzanie danych osobowych w ramach czynności o czysto osobistym charakterze. Takiego charakteru czynności nie dyskwalifikuje wykonanie fotokopii akt, w tym również takich, w których przez błąd sądu znalazły się dane osobowe innych osób. Postulować należy zatem, aby w podobnych sprawach sądy dawały wyraz szczegółowej analizie znamion osądzanych czynów, w tym uwzględnieniu zakresu zastosowania danej ustawy.

Kończąc rozważania związane z art. 107 u.o.d.o. warto zwrócić uwagę na statystyki związane z postępowaniami karnymi dotyczącymi tego przepisu. W poniższej tabeli przedstawiona została liczba postępowań karnych wszczętych, a także zakończonych skierowaniem do sądu aktów oskarżenia przez prokuratorów[6]:

	2022 r.	**2023 r.**
Liczba postępowań wszczętych	771	755
Liczba aktów oskarżenia i wniosków o wyrok skazujący	108	129

Również w statystykach policyjnych dostrzegalne są postępowania związane z naruszeniem przepisów art. 107 § 1-2 u.o.d.o., co obrazuje poniższa tabela[7]:

	Postępowania wszczęte	**Postępowania stwierdzone**	**Postępowania wykryte**
2022 r.	430	230	103
2023 r.	514	742	572

Wskazane statystyki pokazują, że chociaż problem odpowiedzialności karnej za nielegalne lub nieuprawnione przetwarzanie danych osobowych nie jest tak szeroko komentowany, jak odpowiedzialność administracyjnoprawna, to ma on jednak praktyczne znaczenie i pozostaje w obszarze zainteresowania organów ścigania. Ubolewać należy natomiast nad tym, że Minister Sprawiedliwości

[6] Dane Prokuratury Krajowej pozyskane przez autora w trybie dostępu do informacji publicznej.
[7] Dane Komendy Głównej Policji pozyskane przez autora w trybie dostępu do informacji publicznej.

nie prowadzi statystyk dotyczących wyroków skazujących zapadłych na gruncie art. 107 u.o.d.o., które pozwoliłyby ocenić zasadność skierowanych do sądów aktów oskarżenia.

NIELEGALNE I NIEUPRAWNIONE PRZETWARZANIE DANYCH OSOBOWYCH NA GRUNCIE K.K.

Przed omówieniem poszczególnych przepisów k.k. znajdujących zastosowanie do nielegalnego lub nieuprawnionego przetwarzania danych osobowych, należy wskazać, że przepisy części szczególnej k.k. dotyczą przede wszystkim przestępstw przeciwko bezpieczeństwu informacji. Nie powinno jednak budzić wątpliwości, że przepisy te chronią też, co do zasady, bezpieczeństwo danych osobowych, gdyż są nimi, co wynika z przytoczonej już wcześniej definicji danych osobowych przyjętej w art. 4 pkt. 1 RODO, **wszelkie informacje** o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

W ramach uwag natury ogólnej trzeba też dostrzec, że ze względu na to, że zachowanie sprawcy związane z nielegalnym lub nieuprawnionym przetwarzaniem danych osobowych będzie wielokrotnie wyczerpywało znamiona zarówno przestępstwa z u.o.d.o., jak też przestępstwa penalizowanego w k.k., dochodzić będzie do zbiegu przepisów.

Z uwagi na ramy niniejszego opracowania nie jest możliwe omówienie wszelkich czynów zabronionych uregulowanych w k.k., które mogą wiązać się z nielegalnym lub nieuprawnionym przetwarzaniem danych. Z tego powodu dalsze rozważania zostaną skupione wokół art. 190a § 2, art. 266 § 1, art. 267 § 1-2 k.k. oraz art. 268 § 1-2 k.k. Warto jednak dostrzec, że równie często nielegalne przetwarzanie danych osobowych może wiązać się z przestępstwem oszustwa, o którym mowa w art. 286 k.k., przestępstwem zniesławienia, o którym mowa w art. 212 k.k, rozpowszechnianiem bez uprawnienia informacji z postępowania przygotowawczego lub rozprawy z wyłączeniem jawności, o którym mowa w art. 241 k.k.

Kradzież tożsamości

Pierwszym przepisem części szczególnej k.k., na który należy zwrócić uwagę przy omawianiu nielegalnego lub nieuprawnionego przetwarzania danych osobowych jest tzw. kradzież tożsamości penalizowana w art. 190a § 2 k.k., który stanowi, że tej samej karze, jak za uporczywe nękanie podlega ten, kto:

> podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, przez co wyrządza jej szkodę majątkową lub osobistą.

Wykorzystanie cudzych danych osobowych do podszycia się pod taką osobę, stanowi przetwarzanie tych danych osobowych w sposób nieuprawniony, bowiem czynność taka nie może być oparta na żadnej z przesłanek legalizujących, o których mowa w art. 6 ust. 1 lub art. 9 ust. 2 RODO.

Wskazany występek wymaga podszycia się pod inną osobę fizyczną, co wyłącza spod zakresu penalizacji tego przepisu podszywanie się pod inne podmioty, np. osoby prawne lub organy publiczne, a także podszywanie się pod osoby zmarłe (por. Kosonoga 2023). Warto jednak wskazać, że przyjęcie takiego rozumienia ww. przepisu pozwala postawić ustawodawcy zarzut zbędnego rozdrobnienia sposobów jego popełnienia wskazanych w treści przepisu. Zbędne jest bowiem odwoływanie się odrębnie do kategorii wizerunku, danych osobowych oraz innych danych, za pomocą których publicznie identyfikowana jest osoba fizyczna, bowiem zarówno „wizerunek", jak też „inne dane", o których mowa w tym przepisie, wchodzą w pojęcie danych osobowych.

Podszywanie się, o którym mowa w art. 190a § 2 k.k. oznacza podawanie się fałszywie za kogoś innego. Dla kryminalizacji podszycia się na gruncie omawianego występku konieczne jest, aby nastąpiło ono z wykorzystaniem danych osobowych innej osoby, przy czym wystarczające będzie jednorazowe wykorzystanie takich danych (Mozgawa 2015, s. 509-510). Ściganie przestępstwa kradzieży tożsamości następuje na wniosek pokrzywdzonego.

W wyniku nowelizacji k.k. z 7 lipca 2022 r. wskazany przepis został zmieniony w ten sposób, że dotychczasowe znamię kierunkowe, którym było działanie sprawcy „w celu wyrządzenia szkody", zastąpiono znamieniem skutku, którym jest „wyrządzenie szkody majątkowej lub osobistej". Pojęcie szkody na gruncie wskazanego przepisu należy rozumieć szeroko. Szkodą osobistą będzie przede wszystkim uszczerbek w zakresie dóbr osobistych, np. naruszenie dobrego imienia, istotne naruszenie prywatności, zaś szkodą majątkową będzie zasadniczo zmniejszenie aktywów, zwiększenie pasywów lub utrata spodziewanych korzyści (por. Łuczyński 2023, s. 10). Wskazana zmiana spowodowała też, że omawiany występek z formalnego, którym był do czasu wejścia w życie nowelizacji k.k. z 7.07.2022 r. zmienił się w występek o charakterze materialnym, dla bytu którego wymagane jest wystąpienie szkody.

Mając na uwadze, że jak wyżej wskazano, podszywanie się pod inna osobę z wykorzystaniem jej danych osobowych, będzie stanowiło co do zasady nielegalne

przetwarzanie takich danych osobowych, występek opisany w art. 190a § 2 k.k. pozostaje w zbiegu z art. 107 § 1-2 u.o.d.o. Co istotne, może się okazać, że sprawca, który podszywa się pod inną osobę z wykorzystaniem jej danych osobowych nie będzie mógł ponieść odpowiedzialności na gruncie art. 190a § 2 k.k., ponieważ brak będzie w tym zakresie wniosku o ściganie ze strony pokrzywdzonego albo nie dojdzie do wypełnienia znamion tego występku przez nienastąpienie szkody majątkowej lub niemajątkowej. W takiej sytuacji osoba taka będzie jednak mogła ponieść odpowiedzialność z art. 107 § 1-2 u.o.d.o., dla której ani wniosek o ściganie, ani nastąpienie skutku nie jest wymagane.

Bezprawne ujawnienie informacji

Przejawem nielegalnego przetwarzania danych osobowych może być również bezprawne ujawnienie takich danych, które stanowią jednocześnie informacje. Z kolei bezprawne ujawnienie informacji penalizowane jest na gruncie art. 266 § 1 k.k., który stanowi:

Art. 266.

> § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Zakres kryminalizacji ww. występku jest szerszy niż jedynie nielegalne lub nieuprawnione przetwarzanie danych osobowych. Informacjami, o których mowa w ww. przepisie mogą być też bowiem dane nieosobowe. Trzeba jednak przyjąć, że w zakresie w którym w okolicznościach wskazanych w omawianym przepisie prawa dochodzi do ujawnienia danych osobowych, wskazany przepis pozostaje w zbiegu z art. 107 u.o.d.o.

Należy podkreślić, że ujawnienie lub wykorzystanie, o którym mowa w art. 266 k.k. stanowi operację przetwarzania w rozumieniu art. 4 pkt. 2 RODO. Ujawnienie, o którym mowa w omawianym przepisie może nastąpić przez działanie lub zaniechanie (Hoc 2012, s. 64) i polega na uczynieniu informacji wiadomą i dostępną dla innej, osoby nieupoważnionej do poznania danej informacji (Razowski 2021, s. 1149). Nie będzie stanowiło ujawnienia przekazanie informacji osobie nieuprawnionej, jeżeli nie będzie ona miała możliwości faktycznego zapoznania się z informacją, np. na skutek przekazania jej w formie zaszyfrowanej bez klucza dostępu (Lach 2020, s. 1315-1316). Wykorzystanie informacji

polega zasadniczo na podjęciu przez sprawcę jakichkolwiek działań, dla których znajomość informacji objętych tajemnicą była podstawowym impulsem i która posłużyła sprawcy w jakiejkolwiek działalności, w szczególności politycznej, gospodarczej lub naukowej (Marek 2010, s. 567).

Dla bytu ww. przestępstwa kluczowe znaczenie ma to, że sprawca dokonuje ujawnienia informacji z naruszeniem obowiązku poufności. Źródłem tego obowiązku może być przepis ustawy lub przyjęte na siebie zobowiązanie wynikające z umowy lub jednostronnej czynności prawnej. Zobowiązanie takie może wynikać również z zobowiązania pracownika przez pracodawcę do zachowania określonych informacji w tajemnicy (Gardocki 2007, s. 311). Istotne jest również to, że ujawniana informacja ma być informacją, z którą sprawca zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową. Biorąc to pod uwagę, nie popełni omawianego przestępstwa osoba, która uzyska informację z innego źródła, np. osoba, która rozpowszechnia informację z drugiej ręki, tzn. gdy informację wykorzystuje lub ujawnia inna osoba niż ta, która pierwotnie uzyskała ją w związku z pełnioną funkcją lub wykonywaną pracą/działalnością (Kunicka-Michalska, 2000, s. 649).

Mając na uwadze powyższe, wielokrotnie wskazany przepis może pozostawać w zbiegu z przepisem art. 107 u.o.d.o. Do sytuacji takiej dojdzie każdorazowo, jeżeli w zakres informacji ujawnianej lub wykorzystywanej w sposób opisany w art. 266 § 1 k.k. wchodzić będą dane osobowe. Nie sposób bowiem przyjąć, że wykorzystanie lub ujawnienie danych osobowych w sposób naruszający obowiązek poufności, znajdzie oparcie w którejkolwiek z przesłanek legalizujących taką czynność na gruncie RODO. Częstokroć takie zachowanie będzie zresztą stanowiło po stronie administratora danych naruszenie ochrony danych osobowych, bowiem obowiązkiem administratora jest ochrona danych osobowych m.in. przed ich nieuprawnionym ujawnieniem. Na koniec wypada wskazać, że występek z art. 266 § 1 k.k. ścigany jest na wniosek pokrzywdzonego.

Bezprawne uzyskanie informacji

Z niedopuszczalnym lub nieupoważnionym przetwarzaniem danych osobowych związany jest również art. 267 § 1-2 k.k., który przewiduje bezprawne uzyskanie informacji wskazując:

> Art. 267. [Bezprawne uzyskanie informacji]
>
> § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub

> przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

W § 1 wskazanego przepisu spenalizowano uzyskanie przez sprawcę bez uprawnienia dostępu do nieprzeznaczonej dla niego informacji, które to uzyskanie dostępu ma nastąpić przez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia. Przedmiotem ochrony wskazanego przepisu jest poufność informacji, a także prawo do dysponowania informacją z wyłączeniem innych osób (Kozłowska-Kalisz 2015, s. 714). Przestępstwo to będzie godziło w dane osobowe, jeżeli informacja, o której mowa w tym przepisie, będzie obejmowała właśnie takie dane.

Dla zaistnienia wskazanego przestępstwa konieczne jest uzyskanie przez sprawcę dostępu do nieprzeznaczonej dla niego informacji na skutek co najmniej jednego ze sposobów wskazanych w przepisie, czyli przez:

1. **otwarcie zamkniętego pisma** – czynność ta zakłada przełamanie zabezpieczeń pisma, którym może być po prostu jego zaklejenie. Nie będzie naruszeniem omawianego przepisu zapoznanie się z treścią pisma nieprzeznaczonego dla adresata, jeżeli nie będzie ono zamknięte, np. będzie znajdowało się w otwartej kopercie – pod warunkiem, że nie będzie chronione w inny ze sposobów przewidzianych w przedmiotowym przepisie. Co istotne, w doktrynie wskazuje się, że czynność sprawcza otwarcia zamkniętego pisma może odbyć się nawet bez niszczenia opakowania, z wykorzystaniem odpowiednich narzędzi, np. przez prześwietlenie listu (Wróbel 2013). Warto jednocześnie podkreślić, że znamion ww. występku nie wyczerpie samo odebranie korespondencji adresowanej do innej osoby, jak też otwarcie pisma bez zapoznania się z jego zawartością (Kunicka-Michalska 2000, s. 693-694) – chociaż w tym ostatnim przypadku można mówić o usiłowaniu popełnienia przedmiotowego czynu, jeżeli sprawca miał zamiar zapoznania się z treścią takiego pisma,
2. **podłączenie się do sieci telekomunikacyjnej** – siecią, o której mowa w przedmiotowym przepisie może być zarówno telekomunikacyjna sieć przewodowa, jak też sieć bezprzewodowa (zob. Druk sejmowy nr 458, Sejm VI kadencji, Uzasadnienie rządowego projektu ustawy o zmianie

ustawy – Kodeks karny oraz niektórych innych ustaw, s. 4-5.). Co istotne, jeżeli sprawca podłączając się do sieci telekomunikacyjnej bez uprawnienia uzyska dostęp do nieprzeznaczonych dla niego informacji – będzie on odpowiadał na podstawie art. 267 § 1 k.k., jeżeli zaś jego działanie wiążące się z nieuprawnionym podłączeniem do sieci telekomunikacyjnej będzie następowało z wykorzystaniem urządzenia podsłuchowego, wizualnego lub innego urządzenia bądź oprogramowania, które jednak nie doprowadzi do uzyskania dostępu do nieprzeznaczonej dla niego informacji, ale będzie zmierzało do jej pozyskania, sprawca będzie odpowiadał na podstawie art. 267 § 3 k.k. (Radoniewicz 2015, s. 290).

3. kolejnym ze sposobów działania sprawcy może być **przełamanie zabezpieczeń informacji** (elektronicznych, magnetycznych, informatycznych lub innych szczególnych). Zabezpieczenie obejmuje „wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalnej lub posiadania szczególnego urządzenia lub kodu" (Wróbel 2013). W praktyce nie ma znaczenia forma zabezpieczenia, tzn. czy ma ono charakter elektroniczny, magnetyczny, informatyczny czy też inny szczególny charakter. Najpopularniejszymi zabezpieczeniami jest oczywiście stosowanie hasła dostępu, czy też szyfrowanie danych,
4. ostatnim ze sposobów działania sprawcy określonych w art. 267 § 1 k.k. jest uzyskanie dostępu do nieprzeznaczonej dla niego informacji na skutek **ominięcia zabezpieczeń**. Ominięcie to może polegać na całym szeregu czynności, które polegać będą np. na wykorzystaniu socjotechniki, czy inżynierii społecznej celem wyłudzenia określonych danych, np. hasła dostępu, które zostanie następnie wykorzystane przez sprawcę do dostępu do systemu, wprowadzeniu w błąd systemu, np. przez fałszowanie adresów IP użytkownika, czy adresów stron www, wykorzystywaniu luk w systemach, aplikacjach lub protokołach (Radoniewicz 2015, s. 293).

Należy podkreślić, że ze wskazanym występkiem nie będziemy mieli do czynienia, jeżeli uzyskanie nieuprawnionego dostępu do informacji, która nie będzie zabezpieczona. Co również istotne, w doktrynie słusznie wskazuje się, że zabezpieczenie nie powinno mieć jedynie charakteru iluzorycznego, lecz powinno stanowić faktyczną przeszkodę w uzyskaniu dostępu do informacji (Koszut 2004, s. 14 i n.). Popełnienie omawianego przestępstwa nie wymaga aby sprawca zapoznał się z uzyskaną informacją lub ją wykorzystał. Wystarczające jest, aby

uzyskał on do niej dostęp, przy czym – co również istotne – nie ma znaczenia, czy informacja, do której sprawca uzyskał dostęp jest tą informacją, która była przez niego poszukiwania lub która była mu przydatna (Kalitowski 2012, s. 1207). Popełnienie omawianego występku możliwe jest jedynie w sposób umyślny, w zamiarze bezpośrednim, a jego ściganie następuje z urzędu, jednak na wniosek pokrzywdzonego.

Uwagi wymaga też art. 267 § 2 k.k., który penalizuje uzyskanie bez uprawnień dostępu do całości lub części systemu informatycznego. Realizacja znamion tego występku nie wymaga przełamania lub ominięcia zabezpieczeń. Dzięki temu sprawcą ww. przestępstwa może zostać osoba, która wykorzysta hasło dostępu podejrzane podczas wprowadzania go przez inną, uprawnioną osobę (Lach 2020, s. 1323), jak też sprawca, który uzyska dostęp do systemu przy wykorzystaniu haseł zapisanych przy komputerze lub nawet do takiego systemu, który nie jest w ogóle zabezpieczony hasłem, ale do użytkowania którego dana osoba nie jest upoważniona.

Związek nielegalnego lub nieuprawnionego przetwarzania danych osobowych z opisanym wyżej bezprawnym uzyskaniem informacji jest namacalny. Nie trudno wyobrazić sobie bowiem sytuację, w której sprawca celowo otwiera zamknięte pismo, aby zapoznać się ze znajdującymi się w nim danymi osobowymi, czy też przełamuje zabezpieczenia systemu informatycznego, celem uzyskania dostępu do takich danych. Podobnie jak przy wcześniej omawianych występkach, takie działanie nie może być uzasadnione żadną z przesłanek legalizujących przetwarzanie danych. W stosunku do występku, o którym mowa w art. 267 § 2 k.k. przykładem wypełnienia go i zbiegu z nieuprawnionym przetwarzaniem danych osobowych może być, np. zalogowanie się przez pracownika do konta użytkownika innego pracownika, który posiada inny zakres uprawnień systemowych, z wykorzystaniem znalezionego lub podejrzanego hasła.

Utrudnienie zapoznania się z informacją

Ostatnim z przepisów części szczególnej k.k., który może pozostawać w zbiegu z przestępstwem nielegalnego lub nieuprawnionego przetwarzania danych osobowych jest art. 268 § 1-2 k.k. przewidujący utrudnianie zapoznania się z informacją:

> Art. 268. [Utrudnianie zapoznania się z informacją]
>
> § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia

> zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

Wskazany przepis wśród czynności sprawczych wymienia działania, które na gruncie przepisów RODO uznać należy za operację przetwarzania. Należy do nich: 1) niszczenie , 2) uszkadzanie, 3) usuwanie, 4) zmienianie zapisu istotnej informacji, 5) a także inne czynności, które skutkują uniemożliwieniem zapoznania się z informacją lub znacznym utrudnieniem w zapoznaniu się z nią przez osobę uprawnioną (Lach 2020, s. 1327). Wskazany katalog zachowań sprawcy ma zatem charakter otwarty. Istotne jest natomiast, aby skutkiem działania sprawcy było uniemożliwienie lub znaczące utrudnienie zapoznania się z informacją przez osobę uprawnioną.

Działania sprawcy mogą być skierowane zarówno wobec samego zapisu informacji, jak i wobec nośnika, na którym informacje takie są utrwalone. Istotność informacji, o której mowa w omawianym przepisie należy rozumieć w sposób zobiektywizowany, ale uwzględniający kryteria dotyczące interesów dysponenta informacji (Lipiński 2021, s. 1168). Informacja może mieć charakter istotny, np. z perspektywy konkretnej organizacji. Niewątpliwie za informację istotną będzie można uznać, np. dane osobowe, których posiadanie jest niezbędne dla zapewnienia działalności danej organizacji, a których nieuprawnione usunięcie lub zmodyfikowanie albo utrudnienie dostępu do nich uprawnionym osobom, stanowić może też naruszenie ochrony danych osobowych, generujące odpowiedzialność po stronie administratora.

Kwalifikowaną postacią omawianego przestępstwa jest zniszczenie, uszkodzenie, usunięcie lub zmienienie istotnej informacji albo w inny sposób udaremnienie lub znaczące utrudnienie osobie uprawnionej zapoznania się z nią, jeżeli działania te dotyczą zapisu na informatycznym nośniku danych. Informatycznym nośnikiem danych będzie np. dysk twardy komputera, pendrive, a także inny zewnętrzny nośnik pamięci. Wyższą odpowiedzialność będzie więc ponosił sprawca, który, np. dokonuje usunięcia informacji z takiego nośnika danych, czy też dokonuje on uniemożliwienia lub utrudnienia dostępu na skutek zaszyfrowania znajdujących się na takim nośniku informacji.

Zbieg omawianego występku z art. 107 u.o.d.o. może wystąpić w sytuacji, gdy zniszczenie, uszkodzenie, usunięcie lub zmiana dotyczyć będzie danych osobowych, a także gdy sprawca w inny sposób udaremni lub znacznie utrudni

dostęp do takich danych osobowych uprawnionej osobie – czyli co do zasady administratorowi lub upoważnionemu podmiotowi przetwarzającemu. Przykładem tego może być sytuacja, w której pracownik upoważniony do przetwarzania danych osobowych, np. w zakresie niezbędnym do naliczania wynagrodzeń i prowadzenia akt pracowniczych, po zakończeniu współpracy z pracodawcą postanowi na złość zniszczyć akta osobowe. Takie działanie będzie bowiem stanowiło występek z art. 268 § 1 k.k., jak również przetwarzanie danych osobowych w zakresie, w którym pracownik taki nie był uprawniony.

PODSUMOWANIE

Dokonana powyżej analiza wskazuje, że w polskim systemie prawnym mamy do czynienia z szeregiem przepisów prawnych, których bezpośrednim lub pośrednim celem jest ochrona osób fizycznych w związku z przetwarzaniem ich danych osobowych, czy też ochrona prywatności takich osób, a także ochrona przetwarzanych informacji.

Usankcjonowane w art. 107 § 1-2 u.o.d.o. przestępstwa niedopuszczalnego lub nieuprawnionego przetwarzania danych osobowych mają charakter ogólny. Ich granice są nieostre, a odkodowanie tych granic wymaga sięgnięcia do przepisów RODO. Zastosowanie tych przepisów wymaga też ustalenia, że w konkretnych okolicznościach przetwarzanie danych osobowych, które podlega kwalifikacji jako niedopuszczalne lub dokonywane przez nieuprawnioną osobę, odbywa się w oparciu o przepisy RODO. W przeciwnym wypadku wskazany art. 107 u.o.d.o. nie znajdzie zastosowania.

Brak stosowania przepisów u.o.d.o. nie oznacza, że każda operacja na danych osobowych jest dozwolona. Jak bowiem wskazano we wcześniejszej części artykułu, szeroko rozumiane nielegalne przetwarzanie danych osobowych penalizowane jest też przez szereg przepisów części ogólnej Kodeksu karnego, które nie skupiają się jednak na całościowym uregulowaniu nielegalnego przetwarzania, lecz na poszczególnych operacjach przetwarzania penalizując m.in. nielegalne przetwarzanie w zakresie podszywania się pod inną osobę z wykorzystaniem jej danych osobowych, bezprawne ujawnienie lub wykorzystanie informacji objętych obowiązkiem zachowania w poufności, bezprawne uzyskanie dostępu do informacji przez otwarcie zamkniętego pisma lub przełamanie albo ominięcie zabezpieczeń, czy też nieuprawnioną ingerencję w dostępność lub integralność danych. Stosowanie tych przepisów nie jest uzależnione od zakresu materialnego zastosowania RODO.

Jednocześnie, w zakresie, w którym dochodzić będzie do naruszenia art. 107 u.o.d.o. wielokrotnie dochodzić będzie również do zbiegu z omówionymi przepisami części szczególnej Kodeksu karnego, a zbieg ten może mieć charakter zbiegu pomijalnego (jak przy zbiegu art. 107 u.o.d.o. z art. 190a § 2 k.k.), jak też zbiegu kumulatywnego (np. przy zbiegu art. 107 u.o.d.o. z art. 266 § 1-2 k.k., art. 267 § 1 k.k., czy art. 268 § 1-2 k.k.).

BIBLIOGRAFIA

Barta J., Markiewicz R.
1999 *Prawo do prywatności w społeczeństwie informatycznym*, „Ethos".

Barta P.
2018 [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa.

Barta P., Litwiński P.
2016 *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa,

Behr J.
2018 *Środki prawne ochrony danych osobowych*, Wrocław.

Bekrycht T., Leszczyński J., Łabieniec P.
2021 *Podstawy doktryny prawnej*, Warszawa.

Bielak-Jomaa, Soczyński T.
2017 *Problematyka ochrony danych osobowych kandydatów do pracy w obliczu zjawiska kradzieży tożsamości*, [w:] *Kradzież tożsamości w Internecie,* red. A. Gołebiowska, Szczytno.

Czerniawski M.
2022 *Ochrona danych osobowych w prawie międzynarodowym*, [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa.

Gardocki L.
2007 *Prawo karne*, Warszawa.

Gawroński M., Kloc K.
2018 *Ochrona danych osobowych. Przewodnik ze wzorami*, red. M. Gawroński, Warszawa.

Hoc S.
2012 *Karnoprawna ochrona informacji*, Opole.

Kalitowski M.
2012 [w:] *Kodeks karny. Komentarz*, wyd. V, red. M. Filar, Warszawa.

Kosonoga J.
2023 [w:] *Kodeks karny. Komentarz*, Wyd. 6, red. R.A. Stefański, Warszawa.

Koszut R.
2004 *O niektórych kwestiach spornych z 1997 r. na tle ujęcia przestępstwa hakingu w kodeksie karnym*, „Monitor Prawniczy" dodatek PME.

Kozłowska-Kalisz P.
2015 [w:] *Kodeks karny. Komentarz*, wyd. VII, red. M. Mozgawa, Warszawa.

Kunicka-Michalska B.
2000 *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII kodeksu karnego. Komentarz*, Warszawa.

Lach A.
2020 [w:] *Kodeks karny. Komentarz,* wyd. III, red. V. Konarska-Wrzosek, Warszawa.

Lipiński K.
2021 [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa.

Łuczak-Tarka J.
2019 [w:] *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa.

Łuczyński P.
2023 *Open Source Intelligence w kontekście wybranych czynów zabronionych*, „Paragraf. Studia z Prawa i Administracji", nr 2.

Marek A.
2010 *Kodeks karny. Komentarz*, wyd. V, Warszawa.

Mozgawa M.
2015 *Kodeks karny. Komentarz*, wyd. VII, Warszawa

Nawacki M.
2021 *Kryminalizacja naruszeń ochrony danych osobowych*, „Studia Prawnoustrojowe UWM", nr 52.

Radoniewicz F.
2015 *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa.

Razowski T.
2021 [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Warszawa.

Sajfan M.
1999 *Ochrona danych osobowych – granice autonomii informacyjnej*, [w:] *Ochrona danych osobowych,* red. M. Wyrzykowski, Warszawa.

Słabuszewski R.
2020 *Odpowiedzialność karna według ustawy o ochronie danych osobowych,* [w:] *Bezpieczeństwo danych osobowych. Geneza, zakres odpowiedzialność. Wybrane zagadnienia*, red. J. Sikorski, B. Jagusiak, Gorzów Wlkp.

Sołtys B.
2019 *Wątpliwości wokół konstytucyjności sankcji karnych i administracyjno-karnych za naruszenie przepisów o ochronie danych osobowych,* „Przegląd Sądowy", nr 5.

Wróbel W.
2013 [w:] *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, wyd. IV, red. A. Zoll, Warszawa.

Wygoda K.
2022 *Prawo do ochrony danych osobowych w Konstytucji RP*, [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa.

Zoll A.
2016 [w:] *Kodeks karny. Część ogólna. Tom I. Cześć I. Komentarz do art. 1-52*, red. W. Wróbel, Warszawa.

Agnieszka Anna Szymczak

Uniwersytet im. Mikołaja Kopernika w Toruniu

Studentka

OCHRONA DANYCH OSOBOWYCH W PROCESIE REKRUTACJI – ASPEKTY PRAWNE I WYZWANIA

Wstępne naświetlenie problematyki ochrony danych osobowych w procesie rekrutacji

W obecnej rzeczywistości dynamiczny rozwój technologii informacyjnych niesie za sobą nowe wyzwania zwłaszcza w obszarze rekrutacji, który staje się szczególnie podatny na naruszenia prywatności osób biorących w nim udział. Wywód ma na celu przedstawienie kluczowych zagadnień ochrony danych osobowych w kontekście procedur rekrutacyjnych oraz wskazanie reguł panujących w tym procesie. Wraz z rosnącym zastosowaniem zaawansowanych narzędzi analitycznych przez pracodawców do oceny kwalifikacji kandydatów znaczenie przechowywania danych w procesie rekrutacji nabiera większego znaczenia. Jednakże wedle obowiązujących przepisów prawa o ochronie danych osobowych, takich jak Ogólne Rozporządzenie o Ochronie Danych (RODO) oraz ustawa o ochronie danych osobowych, instytucje rekrutacyjne są zobowiązane do obligatoryjnego przestrzegania zasad zbierania, przetwarzania oraz przechowywania danych osobowych. Skoncentrowanie na ochronie prywatności kandydatów staje się priorytetem, a wszelkie uchybienia w tym obszarze mogą generować liczne konsekwencje prawne. Ochrona danych osobowych w procesie rekrutacji stawia przed pracodawcami liczne wyzwania prawne, którym stawienie czoła wymaga skutecznych działań w celu zapewnienia prywatności kandydatów. Prezentowana analiza skupia się na zidentyfikowaniu prawnie uregulowanych aspektów procesu rekrutacyjnego, odnosząc się przy tym do Kodeksu Pracy, ustawy o ochronie

danych osobowych oraz RODO. Podkreśla znaczenie ochrony prywatności kandydatów jako wartości priorytetowej, stawiającej przed pracodawcami wyzwania prawne, które wymagają skutecznych działań w celu osiągnięcia balansu między efektywnością procesu rekrutacyjnego, a przestrzeganiem norm ochrony danych osobowych. Tematyka ochrony danych osobowych w procesie rekrutacji jest kluczowa z perspektywy prawnej, społecznej ,a także etycznej, zwłaszcza w kontekście dynamicznego rozwoju technologii informacyjnych. Konieczność zdefiniowania klarownych ram ochrony prywatności kandydatów wynika ze współczesnych wyzwań. Rola przechowywania danych w procesie rekrutacji stała się istotna szczególnie w kontekście wykorzystania zaawansowanych narzędzi analitycznych przez pracodawców. Przestrzeganie obowiązujących przepisów prawnych zwłaszcza Ogólnego Rozporządzenia o Ochronie Danych (RODO) jest kluczowe dla procesów rekrutacyjnych. Warto podkreślić, że wszelkie nieścisłości lub naruszenia w obszarze ochrony danych osobowych mogą skutkować poważnymi konsekwencjami prawno-organizacyjnymi dla instytucji rekrutacyjnych.

Słowem wstępu znaczenie ochrony danych osobowych w procesie rekrutacji wykracza poza zagwarantowanie jednostkom prawa do prywatności. Stanowi ona znaczący element strategii mającej na celu przeciwdziałanie dyskryminacji i zagrożeniom związanym z cyberprzestępczością. Dodatkowo wzmożenie społecznej świadomości dotyczącej ochrony danych wpisuje się w kontekst budowania zaufania między instytucjami rekrutacyjnymi a kandydatami. Podjęcie tematu ochrony danych w ramach doktryny prawa jest uzasadnione ze względu na współczesne wyzwania wynikające z dynamicznego rozwoju technologii. Efektywne połączenie procedur rekrutacyjnych z poszanowaniem praw i prywatności kandydatów wymaga stałego dostosowywania się do aktualnych ram prawnych.

W kontekście dalszej analizy ochrony danych osobowych w procesie rekrutacji skupić należy się na elementarnych zagadnieniach stanowiących fundament tego obszaru. Przede wszystkim omówienia wymaga rola administratora danych osobowych w rekrutacji, kładąc nacisk na istotną funkcję zarządzania danymi kandydatów. Następnie omówione zostaną podstawy prawne przetwarzania danych w tym kontekście, aby zrozumieć ramy prawne kształtujące procedury rekrutacyjne. Kolejnym krokiem będzie skoncentrowanie się na zakresie danych osobowych zbieranych od kandydatów z uwzględnieniem zasady minimalizacji, która ma na celu ograniczenie zbierania informacji do absolutnie niezbędnego minimum. Ważnym aspektem do rozważenia będzie również kwestia zgody na przetwarzanie danych w procesie rekrutacji. W tym kontekście przyjrzeć należy się znaczeniu świadomej zgody kandydatów i jej roli w budowaniu zaufania między

stronami procesu rekrutacyjnego. Następnie poruszona zostanie kwestia okresu przechowywania danych zebranych w trakcie rekrutacji. Na zakończenie analizie zostanie poddany obowiązek informacyjny w procesie rekrutacji. Poruszone zostanie również zagadnienie danych biometrycznych stale wykorzystywanych w procesie rekrutacji pod postacią zdjęć kandydatów załączanych do CV. Wszystkie te aspekty stanowią istotną część analizy ochrony danych osobowych w rekrutacji mającej na celu zrozumienie i poszanowanie praw kandydatów, a także efektywne i zgodne z przepisami przeprowadzanie procesów rekrutacyjnych. Zastrzec należy jednak , że problem ochrony danych osobowych w procesie rekrutacji jest bardzo szeroki w związku z tym odniesienie się do wszystkich aspektów nie jest możliwe dlatego też rozważania nad tą problematyką ograniczają się do kwestii zasadniczych.

Rola administratora danych osobowych w zatrudnieniu

W aspekcie rozważań dotyczących ochrony danych osobowych w procesie rekrutacji rozpoczęcie analizy skoncentrować należy na fundamentalnej kwestii związanej z zagadnieniem administratora danych osobowych. Zgodnie z art. 4 pkt. 7 Rozporządzenia Ogólnego o Ochronie Danych (RODO), termin "administrator" obejmuje jednostki fizyczne lub prawne, organy publiczne, jednostki lub inne podmioty, które samodzielnie lub wspólnie z innymi ustalają cele i metody przetwarzania danych osobowych. W przypadku ,gdy cele i metody przetwarzania są ustalone w prawie Unii lub państwa członkowskiego administrator może być wyznaczony zgodnie z przepisami prawa Unii lub państwa członkowskiego lub też mogą zostać określone konkretne kryteria jego wyznaczania. Administrator danych osobowych pełni decyzyjną rolę w określaniu celów i metod przetwarzania danych osobowych. Kluczowymi elementami tego statusu są zdolność do ustalania celów przetwarzania oraz metody, za pomocą których dane osobowe są przetwarzane. Nawet jeżeli administrator nie posiada bezpośredniego dostępu do przetwarzanych danych, to to właśnie on decyduje o celach i zleca przetwarzanie danych osobom trzecim. Podstawowe obowiązki administratora danych obejmują przestrzeganie postanowień RODO zwłaszcza w kontekście udzielania informacji osobom, których dane są przetwarzane. Dodatkowo administrator zobowiązany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych. Warto podkreślić możliwość wspólnego pełnienia roli administratora danych przez co najmniej dwa podmioty, o ile wspólnie ustalą cele i metody przetwarzania danych.

W takiej sytuacji mówi się o współadministratorach danych osobowych zgodnie z postanowieniami art. 26 RODO. Administrator danych osobowych ponosi szereg obowiązków wynikających z RODO w tym obowiązek informacyjny oraz zabezpieczania danych osobowych. W kontekście danych pracowników rolę administratora danych pełnią przede wszystkim pracodawcy, gdyż są oni administratorami danych w rozumieniu ustawy o ochronie danych osobowych z 2018 r. i ogólnego rozporządzenia o ochronie danych. Często spotykanym wzorcem procedury rekrutacyjnej jest schemat, w ramach którego pracodawca pełniący równocześnie funkcję administratora danych osobowych samodzielnie gromadzi informacje o potencjalnych kandydatach do zatrudnienia. Rozpowszechnioną praktyką w środowisku pracodawców jest zamieszczanie ogłoszeń o pracę na własnej witrynie internetowej. W tym kontekście pracodawca przejmuje kierownicze zadania w całym procesie rekrutacyjnym angażując własnych pracowników do przetwarzania danych kandydatów. Termin "pracownik pracodawcy" obejmuje jednostki autoryzowane do operowania danymi zgodnie z postanowieniami art. 29 i art. 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Niemniej jednak w ramach tej procedury wykorzystuje się również usługi zewnętrznych podmiotów, takich jak agencje rekrutacyjne, które mogą pełnić rolę podmiotu przetwarzającego, co wymaga nawiązania umowy powierzenia danych zgodnie z zapisami art. 28 RODO. Ważne jest wskazanie różnicy pomiędzy sytuacją, w której pracodawca pozyskuje dane z bazy agencji rekrutacyjnej ,(która pełni rolę administratora danych) a przypadkiem, gdy pracodawca samodzielnie gromadzi dane potencjalnych kandydatów. W pierwszym scenariuszu zachodzi udostępnienie danych pomiędzy niezależnymi administratorami tj. agencją rekrutacyjną ,a pracodawcą przy czym oba te podmioty posiadają odrębne podstawy prawne do przetwarzania danych. Ponadto dopuszczalne jest skorzystanie z usług agencji pracy tymczasowej (APT), której zadaniem jest przeprowadzenie procesu rekrutacji pracowników tymczasowych ,a następnie skierowanie ich do pracy u pracodawcy. Agencja ta pozyskuje i weryfikuje kandydatów będąc jednocześnie stroną umowy o pracę z pracownikami tymczasowymi, po czym przekazuje dane pracodawcy. Zróżnicowanie relacji i funkcji uczestniczących podmiotów w procesie rekrutacji wymaga szczegółowej analizy zwłaszcza z perspektywy zapewnienia zgodności z przepisami prawa pracy, RODO oraz ewentualnych umów powierzenia danych do przetwarzania.

Analizując rolę pracodawcy pełniącego funkcję administratora danych osobowych należy zaznaczyć, że istnieje szereg obowiązków, które wymagają należytego spełnienia przez niego. Pracodawca jako administrator danych zobligowany

jest do udzielania kandydatom na pracowników pełnych informacji dotyczących celów i zakresu przetwarzania ich danych osobowych. W tym kontekście konieczne jest dostarczenie informacji ,takich jak tożsamość, dane kontaktowe, informacje dotyczące przedstawiciela (jeżeli taki występuje), a także dane kontaktowe inspektora ochrony danych, w wypadkach gdyby było to konieczne. Podkreśla się, że jako administrator danych osobowych pracodawca ma obowiązek precyzyjnego określenia celów przetwarzania, podstaw prawnych oraz dostarczenia informacji na temat odbiorców danych. Administrator danych winien również zapewnić kompleksowe informacje dotyczące okresu przechowywania danych, a także poinformować kandydata o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania dostarczonych przez niego danych osobowych. W sytuacji, gdy przetwarzanie danych osobowych kandydata opiera się na art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO pracodawca-administrator danych ma obowiązek przekazania informacji na temat prawa do odwołania zgody w dowolnym momencie, nie wpływając tym samym na zgodność z prawem przetwarzania dokonanego przed odwołaniem zgody. Dodatkowo pracodawca w roli administratora danych powinien przekazać informację odnośnie prawa kandydata do złożenia skargi do organu nadzorczego. Warto zauważyć, że reszta zasad dotyczących przetwarzania danych osobowych oraz obowiązków administratora danych w tym obszarze została szczegółowo uregulowana w rozdziale II RODO.

W odniesieniu do powyższych rozważań kontynuacja charakterystyki zagadnienia (ochrony danych osobowych w procesie rekrutacji) koncentruje się na wskazaniach zawartych w poradniku Urzędu Ochrony Danych Osobowych (UODO) dotyczącym przetwarzania danych osobowych w rekrutacji, datowanego na październik 2018 roku, zatytułowanego "Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców"[1]. UODO wskazuje, że w kontekście procesu rekrutacji zgodnie z zasadami etycznymi i przepisami prawa pracodawca powinien ograniczać przetwarzanie danych osobowych kandydatów do pracy jedynie do informacji absolutnie niezbędnych dla podjęcia decyzji o zatrudnieniu (str.32;39). Wskazuje się, że pracodawca nie powinien żądać od kandydata danych, które nie są konieczne do efektywnego przeprowadzenia procesu rekrutacji. Zbieranie danych osobowych musi odbywać się zgodnie z prawem, a pracodawca musi wykazać zgodność celu pozyskiwania danych z prawem oraz konieczność ich zbierania dla realizacji tego celu. Ważne jest unikanie zbierania nadmiarowych informacji, które nie są istotne dla procesu rekrutacyjnego, aby

[1] https://orka.sejm.gov.pl/BOP_info.nsf/0/43826AB057FD3661C125832E00368D2F/%24File/Poradnik%20dotycz%C3%84%E2%80%A6cy%20zatrudnienia.pdf.

uniknąć naruszeń postanowień RODO i przepisów prawa pracy. W przypadku przetwarzania danych zebranych z Curriculum Vitae (CV) osoby ubiegającej się o zatrudnienie wykraczających poza zakres przewidziany przepisami prawa pracy pojawia się kwestia zgody (str.11). Pracodawca jest uprawniony do przetwarzania dodatkowych danych ,ale tylko, o ile kandydat wyrazi na to wyraźną zgodę, która może być założona przez jasne oświadczenie lub zachowanie wskazujące na akceptację przetwarzania danych osobowych. W przypadku szczególnych kategorii danych takich jak dane wrażliwe (str.12) pracodawca musi podjąć odpowiednie kroki w celu właściwego postępowania z tymi danymi, zwłaszcza jeśli kandydat dobrowolnie dostarczył informacje dotyczące np. swojego stanu zdrowia. Bez odrębnej zgody kandydata na przetwarzanie takich danych oraz braku obowiązującego przepisu prawa nakazującego pracodawcy ich przetwarzanie pracodawca jest zobowiązany do usunięcia tych danych. Ewentualna zgoda na przetwarzanie szczególnych kategorii danych powinna być wyraźna i może być przedstawiona w formie odrębnego oświadczenia. W kontekście przyszłych procesów rekrutacyjnych pracodawca nie ma prawa wykorzystywać danych pozyskanych od kandydatów w ramach konkretnego procesu rekrutacyjnego ,chyba że kandydat wyraził na to wyraźną zgodę (str.12). Dotyczy to również informacji zebranych z portali społecznościowych. Rola agencji zatrudnienia jest precyzyjnie określana zwłaszcza ,gdy pracodawca powierza agencji zadanie przeprowadzenia rekrutacji. Agencja staje się administratorem danych osobowych kandydatów, a jej obowiązkiem jest informowanie kandydatów podczas zbierania danych. Pracodawca uzyskuje dane tylko tych kandydatów, którzy wyrazili odpowiednią zgodę. W kwestii uzyskiwania informacji od poprzednich pracodawców kandydata pracodawca musi przestrzegać norm związanych z ochroną prywatności i uzyskać zgodę kandydata. W kontekście procesu rekrutacji istnieje szereg podstaw prawnych regulujących przetwarzanie danych osobowych, z którymi pracodawca powinien się zaznajomić. W pierwszym rzędzie zgodnie z art. 6 ust. 1 lit. b Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO) przetwarzanie danych osobowych jest uzasadnione, gdy jest to niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie tej osoby przed zawarciem umowy. Kolejnym zasadniczym aspektem jest art. 6 ust. 1 lit. c RODO, który określa, że przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych. Poradnik stworzony przez UODO niewątpliwie stanowi względnie przejrzystą instrukcję skierowaną do pracodawców w odniesieniu do właściwego przetwarzania danych osobowych zarówno osób ubiegających się o zatrudnienie jak i pracowników.

Zgoda na przetwarzanie danych osobowych na tle zagadnień prawa pracy

Przechodząc do omówienia podstaw prawnych przetwarzania danych osobowych wykorzystywanych w procesie rekrutacji ważnym elementem jest art. 6 ust. 1 lit. a RODO. Zgodnie z nim osoba, której dane dotyczą wyraża zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. Kluczowym aspektem jest również forma wyrażenia zgody zgodnie z art. 4 pkt 11 RODO musi być ona dobrowolna i stanowić konkretne, wyrażone w sposób świadomy i jednoznaczny okazanie woli. Warto podkreślić, że zgoda może być udzielona w formie oświadczenia lub wyraźnego działania potwierdzającego. Art. 9 ust. 2 lit. a RODO dotyczy natomiast sytuacji, gdy osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie swoich danych osobowych w jednym lub kilku konkretnych celach. Przykładowe formułowanie zgody może obejmować aspekty dotyczące kolejnych naborów pracowniczych lub przetwarzania szczególnych kategorii danych, o których mowa w art. 9 ust. 1 RODO. W odniesieniu do informacji zawartych w Krajowym Rejestrze Karnym art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 o Krajowym Rejestrze Karnym uprawnia pracodawców do uzyskiwania informacji o osobach, których dane osobowe zgromadzone zostały w Rejestrze. Prawo to przysługuje w zakresie niezbędnym dla zatrudnienia pracownika podlegającego wymogowi niekaralności lub korzystania z pełni praw publicznych. W kontekście poszukiwania informacji o kandydatach do pracy na portalach społecznościowych "background screening" czy potwierdzania informacji zawartych w referencjach należy uwzględnić art. 22^1 § 3 Kodeksu pracy. Udostępnienie pracodawcy danych osobowych odbywa się poprzez oświadczenie osoby, której dane dotyczą. Podsumowując, przepisy takie jak art. 6 RODO, art. 23 ustawy o ochronie danych osobowych, art. 9 RODO czy art. 22^1 § 3 kodeksu pracy stanowią fundamenty prawne, które regulują proces rekrutacji w tym przetwarzanie danych osobowych kandydatów. Ważne jest zrozumienie tych regulacji oraz ich skutków w kontekście działań pracodawcy podczas rekrutacji. Należy także wskazać ,że przy przeprowadzaniu procedur rekrutacyjnych istotne znaczenie mają także art. 22^1 Kodeksu pracy wskazujący jakich danych w powszechnym procesie rekrutacji może oczekiwać pracodawca od osoby ubiegającej się o zatrudnienie. Znaczenie posiadają także art. 22^{1a} i 22^{1b} Kodeksu pracy.

Dane osobowe gromadzone w procesie rekrutacji

Rozważając tematykę zakresu danych osobowych zbieranych od kandydatów w procesie rekrutacyjnym należy wskazać, iż pracodawca ma prawo żądać od osoby starającej się o zatrudnienie określonych informacji niezbędnych do zawarcia umowy o pracę. Wymienione dane obejmują: imię (imiona) i nazwisko, datę urodzenia, dane kontaktowe wskazane przez kandydata oraz szczegóły dotyczące wykształcenia i historii zatrudnienia. Pracodawca może również oczekiwać informacji o kwalifikacjach zawodowych i przebiegu dotychczasowej kariery zawodowej, jednakże tylko w przypadku, gdy są one niezbędne do wykonywania określonej pracy lub na danym stanowisku. Warto zauważyć, że decyzja o udostępnieniu dodatkowych informacji, takich jak adres do korespondencji, adres poczty elektronicznej lub numer telefonu należy do samodzielnej decyzji kandydata. Imiona rodziców oraz adres zamieszkania nie mogą być zbierane przez pracodawcę w ramach procesu rekrutacyjnego. Ponadto wszelkie inne dane osobowe, których pozyskanie jest pożądane przez pracodawcę podlegają wyrażeniu zgody przez kandydata. Odmowa udzielenia zgody lub jej późniejsze wycofanie nie może prowadzić do negatywnego traktowania kandydata w kontekście zatrudnienia ani nie może być przyczyną odmowy zatrudnienia. W kontekście tematyki danych osobowych, których pracodawca może oczekiwać od kandydata na pracownika ważne jest uwzględnienie obowiązujących przepisów prawa. Przy rozważaniach na ten temat należy uwzględnić zarówno art. 22^1 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U.) jak i postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Wedle obowiązujących regulacji pracodawca może oczekiwać od kandydata na pracownika konkretnych danych osobowych. Są to informacje identyfikacyjne, takie jak imię i nazwisko, data urodzenia, dane kontaktowe, a także szczegóły dotyczące wykształcenia i przebiegu dotychczasowego zatrudnienia. Warto podkreślić, że pracodawca może także oczekiwać nowych informacji, takich jak adres do korespondencji, adres poczty elektronicznej lub numer telefonu, jednak tak jak już wskazano ich udostępnienie zależy od decyzji samego kandydata. Ponadto poruszając kwestie natury doktrynalnej należy zaznaczyć, że w kontekście ogólnego rozporządzenia o ochronie danych, istnieje możliwość wprowadzenia bardziej szczegółowych przepisów dotyczących przetwarzania danych osobowych pracowników. Przykładowo, państwa członkowskie mogą zawrzeć w swoich przepisach lub porozumieniach zbiorowych szczegółowe regulacje dotyczące celów

przetwarzania danych w związku z zatrudnieniem uwzględniając kwestie rekrutacyjne, zarządzania, bezpieczeństwa w miejscu pracy i zakończenia stosunku pracy. Warto również podkreślić, że postanowienia ogólnego rozporządzenia o ochronie danych są skuteczne bezpośrednio w państwach członkowskich od 25.05.2018 r. co oznacza, że mają pierwszeństwo przed krajowym prawem bez potrzeby implementacji. W związku z tym każde państwo członkowskie ma obowiązek powiadomienia Komisji Europejskiej o przepisach przyjętych w ramach art. 88 ust. 1 RODO dotyczących szczegółowych przepisów ochrony danych pracowników. W obszarze akwizycji danych w trakcie procedury rekrutacyjnej istotne są przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO), w szczególności art. 5, który definiuje zasady przetwarzania danych osobowych. Warto zwrócić uwagę na zasadę „zgodności z prawem, rzetelności i przejrzystości" zgodnie , z którą dane osobowe powinny być przetwarzane zgodnie z prawem, rzetelnie i transparentnie dla osób, których dane dotyczą (art. 5 ust. 1 lit. a RODO). Kolejną ważną zasadą stosowaną w procesie przetwarzania danych osobowych jest zasada „ograniczenia celu" nakazująca zbieranie danych osobowych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach, a następnie zakaz przetwarzania danych w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b RODO). Dodatkowo zasada „minimalizacji danych" wymaga zgody na przetwarzanie jedynie tych informacji, które są adekwatne, stosowne i ograniczone do niezbędnego minimum dla określonych celów (art. 5 ust. 1 lit. c RODO). Aspekt zgodności z prawem (art. 5 ust. 1 lit. a RODO) znajduje dalsze rozwiązanie w art. 6 RODO. Przepis ten stanowi, że przetwarzanie danych jest zgodne z prawem, jeżeli spełnione jest co najmniej jedno z wymienionych w nim kryteriów.

Przechodząc do analizy pozyskiwania danych potencjalnych pracowników przez pracodawców w procesie rekrutacji istotne jest ponowne odwołanie się do art. 22^1 § 1 Kodeksu pracy wyznaczającego jakich danych pracodawca ma prawo obligatoryjnie oczekiwać od osoby biorącej udział w rekrutacji. Nawiązując stosunek pracy pracodawca wedle wskazanego przepisu (art. 22^1 KP) ma prawo żądać danych osobowych obejmujących : imię i nazwisko , datę urodzenia , miejsce zamieszania, wykształcenie, przebieg dotychczasowego zatrudnienia . Katalog danych jakich pracodawca może oczekiwać zmienia się wraz z uzyskaniem statusu pracownika przez osobę wcześniej ubiegającą się o zatrudnienie. Od pracowników pracodawca może oczekiwać innych danych osobowych oraz innych danych niezbędnych dla ustalenia uprawnień ze stosunku pracy (np. dane dot. dzieci pracownika, numer rachunku płatniczego). Zgodnie z art. 22^1 § 1 KP pracodawca wyłącznie w sytuacjach, gdy jest to niezbędne do wykonywania pracy określonego

rodzaju lub na określonym stanowisku może dodatkowo żądać informacji dotyczących wykształcenia, kwalifikacji zawodowych oraz przebiegu dotychczasowego zatrudnienia. Należy zatem zauważyć, że żądanie fotografii od kandydata do pracy oraz informacji o stanie cywilnym wykracza poza uprawnienia pracodawcy. Trzeba jednak pamiętać, że jeśli ogłoszenie o pracę nie zawiera takich wymagań, a osoba kandydująca umieściła takie dane w swojej aplikacji z własnej inicjatywy to należy uznać, iż zrobiła to dobrowolnie (dane są przetwarzane na podstawie zgody aplikującego). Po nawiązaniu stosunku pracy pracodawca żąda od pracownika danych dotyczących jego wykształcenia i przebiegu dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania na etapie ubiegania się przez pracownika o zatrudnienie. Ponadto pracodawca jest uprawniony do uzyskania od pracownika innych danych osobowych niż wyżej określone, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Zgodnie z art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (tekst jedn. Dz.U. z 2023 r. poz. 159) pracodawcy przysługuje prawo do uzyskania informacji o osobach, których dane zgromadzone zostały w KRK w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej. W związku z tym kandydat do pracy nie ma obowiązku przedstawienia informacji z KRK, a pracodawca nie może tego od niego wymagać ani sam pozyskać takich danych, chyba że przymiot niekaralności byłby ustawowym wymogiem świadczenia pracy na danym stanowisku czy też wykonywania danego zawodu. Kandydaci na pracowników odrzuceni w procesie rekrutacji przez pracodawcę z uwagi na brak udostępnienia danych osobowych, do zbierania których pracodawca nie był uprawniony (np. stan cywilny, zdjęcie) mogą dochodzić od pracodawcy odszkodowania z tytułu dyskryminacji na podstawie art. 183d KP. Wśród innych środków prawnych przysługujących takim osobom rozważyć można również pozew o naruszenie dóbr osobistych, a także złożenie zawiadomienia o podejrzeniu popełnienia przestępstwa określonego w art. 107 ust. 1 ustawy z 10.05.2018 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2019 r. poz. 1781).

W kontekście regulacji prawnych tego procesu warto zwrócić jednak także uwagę na art. 22^{1a} § 1 Kodeksu pracy, który wprowadza możliwość uzyskania zgody od kandydata na przetwarzanie innych danych niż te wymienione w art. 22^{1} § 1 Kodeksu pracy. Istotną rolę odgrywa również art. 22^{1b} § 1 Kodeksu pracy. Precyzuje on, że zgoda osoby ubiegającej się o zatrudnienie może stanowić

podstawę przetwarzania danych szczególnych kategorii takich jak informacje o stanie zdrowia jedynie w przypadku, gdy przekazanie tych danych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Artykuł ten odnosi się do pozyskiwania przez rekrutującego danych szczególnej kategorii jakimi są dane wrażliwe.

Zgoda na przetwarzanie danych osobowych – forma jej udzielenia w procesie rekrutacji

W procesie rekrutacji istotnym warunkiem umożliwiającym legalne przetwarzanie danych osobowych zawartych w dokumentach takich jak Curriculum Vitae (CV) czy list motywacyjny jest wyrażenie przez kandydata zgody na przetwarzanie tych informacji przez pracodawcę. Działanie to stanowi kluczowy element umożliwiający prawidłowe i zgodne z przepisami prawa korzystanie z przekazanych przez kandydata dokumentów. Postanowienia dotyczące zgody na przetwarzanie danych osobowych są zgodne z uregulowaniami zawartymi w rozporządzeniu 2016/679 o ochronie danych (RODO). Warto zaznaczyć, że zgodnie z przepisami RODO wyrażenie zgody na przetwarzanie danych musi odpowiadać określonym kryteriom. Mowa tutaj o charakterze dobrowolnym, precyzyjnie określonym, świadomym i jednoznacznym wyrażeniu woli osoby, której dane dotyczą. Zazwyczaj dokonuje się tego w formie pisemnej lub elektronicznej. Zgoda musi być wyrażona w sposób jednoznaczny, potwierdzający konkretne działanie, które manifestuje dobrowolne, świadome i jednoznaczne przyzwolenie na przetwarzanie danych osobowych w ściśle określonym celu lub celach. Istotne jest, aby milczenie domyślne zaznaczenie pól czy brak działań nie było interpretowane jako wyrażenie zgody. W przypadku przetwarzania danych dla różnych celów konieczne jest uzyskanie zgody na wszystkie związane z nimi operacje. Aby wyrażenie zgody było świadome osoba, której dane dotyczą powinna posiadać informacje dotyczące tożsamości administratora danych oraz celów przetwarzania. Minimalna ilość informacji na temat procesu przetwarzania danych, które należy przekazać obejmuje identyfikację administratora i zamierzone cele przetwarzania. Tym samym osoba wyrażająca zgodę posiada pełną świadomość i zrozumienie procesu, któremu się poddaje.

Odnośnie procesu rekrutacyjnego istotne jest, aby kandydaci byli pouczani o konieczności udzielenia zgody na przetwarzanie ich danych osobowych. Stanowi to warunek umożliwiający pracodawcy legalne korzystanie z dokumentów aplikacyjnych takich jak CV i list motywacyjny. Zgoda winna być zawarta

zarówno w CV, jak i liście motywacyjnym co pozwala na kompleksowe przetwarzanie danych w ramach procesu rekrutacyjnego.

Usunięcie danych osobowych kandydata na pracownika zebranych w rekrutacji

Okres retencji danych aplikanta na stanowisko pracy powinien być dostosowany do zasad przetwarzania danych oraz z góry ustalony przez administratora. Z reguły pracodawca winien niezwłocznie po zakończeniu procesu rekrutacji trwale usunąć dane osobowe kandydata, na przykład poprzez zniszczenie lub zwrot, jeżeli nie doszło do zawarcia umowy o pracę. Wyjątkiem od tej zasady mogą być sytuacje, w których istnieją inne legalne podstawy umożliwiające administratorowi dalsze przetwarzanie tych danych. Warto podkreślić, że szczegółowe cele przetwarzania danych powinny być klarowne, uzasadnione i precyzyjnie określone już w chwili ich pozyskiwania. Dlatego też ewentualne przedłużenie okresu przechowywania danych zawartych w aplikacji kandydata powinno stanowić raczej wyjątek niż regułę usuwania danych oraz być szczególnie uzasadnione.

Dane administratora danych osobowych udzielane kandydatom na pracownika – obowiązek informacyjny

W procesie rekrutacyjnym nakłada się na pracodawcę obowiązek precyzyjnego, zrozumiałego i łatwo dostępnego informowania kandydata o różnych aspektach -obowiązek informacyjny . Należy dostarczyć mu jasnych danych, takich jak pełna nazwa i adres siedziby firmy, dane kontaktowe inspektora ochrony danych w przypadku jego wyznaczenia, a także cel przetwarzania danych i podstawy prawnej tego procesu, znaną w chwili pozyskiwania informacji. Istotnym elementem jest ujawnienie odbiorców danych lub ich kategorii, planów ewentualnego transgranicznego przetwarzania danych (o ile to ma zastosowanie), okresu w jakim dane będą przetwarzane bądź kryteriów ustalania tego okresu. Przysługujące kandydatowi prawa są równie ważne, takie jak żądanie dostępu do danych, uzyskanie ich kopii, poprawa, usunięcie czy ograniczenie przetwarzania. Kandydat powinien być świadomy prawa do odwołania zgody w każdej chwili, nie wpływając negatywnie na zgodność z prawem wcześniejszego przetwarzania na podstawie udzielonej zgody. Ponadto informacja o możliwości złożenia skargi do organu nadzorczego jest kluczowa. Kwestia dobrowolności lub obowiązku udzielenia danych, a także konsekwencji ich ewentualnego wstrzymania powinna

być jasno przedstawiona. Obowiązek dostarczenia informacji można zrealizować między innymi poprzez treść ogłoszenia o pracy, bezpośrednie przekazanie informacji po otrzymaniu CV kandydata, a także w formie automatycznej odpowiedzi podczas komunikacji za pośrednictwem poczty elektronicznej. Ryzyka wynikające z nieprawidłowego przetwarzania danych osobowych w kontekście procesu rekrutacji obejmują naruszenie prywatności poprzez nieadekwatne gromadzenie, przechowywanie lub udostępnianie informacji kandydatów. Ponadto istnieje potencjalne zagrożenie dyskryminacji, gdyż nieodpowiednie wykorzystanie danych może prowadzić do nierównego traktowania na podstawie cech osobowych, takich jak wiek, płeć czy orientacja seksualna. Aspekt bezpieczeństwa danych jest również istotny, gdyż brak właściwego zabezpieczenia informacji może prowadzić do wycieku, narażając kandydatów na ryzyko kradzieży tożsamości lub innych form nadużyć. Wszystkie powyżej wskazane kwestie mieszczą się w pojęciu obowiązku informacyjnego, który stanowi niezbędny element prawidłowego procesu przetwarzania danych osobowych.

Zbieranie danych biometrycznych w procesie rekrutacji

W odniesieniu do poruszanej tematyki istotnym wydaje się także poruszenie kwestii danych biometrycznych stanowiących szczególną kategorię danych osobowych , których wykorzystywanie stanowi ważną kwestię w procesie rekrutacji. Zgodnie z art. 4 pkt. 14 Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO) termin "dane biometryczne" odnosi się do informacji osobistych, które wynikają z przeprowadzenia specjalnego procesu technicznego i dotyczą cech fizycznych, fizjologicznych lub behawioralnych konkretnej osoby. Takie dane umożliwiają lub potwierdzają jednoznaczną identyfikację jednostki przykładowo poprzez wizerunek twarzy lub informacje daktyloskopijne. Dane biometryczne obejmują wszelkie informacje osobiste związane m.in. z kodem DNA, wizerunkiem twarzy, układem linii papilarnych czy tęczówką oka. Pracodawca może przetwarzać zdjęcie kandydata, które ten załączył w CV, jeżeli jest to konieczne do celów procesu rekrutacji. Zdjęcie zamieszczone przez aplikującego w CV wedle mojej opinii stanowi dane biometryczne zgodnie z rozumieniem RODO, gdyż obejmuje informacje umożliwiające jednoznaczną identyfikację danej osoby - wizerunek twarzy. Pracodawca może przetwarzać zdjęcie kandydata w procesie rekrutacji na podstawie prawnie uzasadnionego interesu, jeżeli jest to niezbędne dla oceny kwalifikacji lub spełnienia innych wymagań związanych z danym stanowiskiem pracy. Preferowaną praktyką zapewniającą niewątpliwą

zgodność z przepisami dotyczącymi ochrony danych osobowych jest uzyskanie wcześniej wspomnianej zgody od kandydata. Od osób ubiegających się o zatrudnienie można żądać załączenia zdjęcia do CV tylko wtedy, gdy jest to uzasadnione i konieczne dla celów rekrutacji. Jednakże praktyka ta może być uważana za potencjalnie dyskryminacyjną, dlatego pracodawca powinien starannie rozważyć czy żądanie zdjęcia jest niezbędne do oceny kwalifikacji kandydata i czy nie narusza zasad równego traktowania. Dyskryminacja w procesie rekrutacji, co do ochrony danych osobowych zidentyfikowana jest w przypadku podejmowania decyzji rekrutacyjnych przez pracodawcę opartych na kryteriach nieuzasadnionych lub nielegalnych, co skutkuje naruszeniem zasad równego traktowania kandydatów. Szereg aspektów ilustruje różne formy dyskryminacji w tym kontekście m.in wymaganie nieuzasadnionych informacji od kandydatów takich jak załączanie zdjęć może być interpretowane jako działanie dyskryminacyjne. Uzależnianie decyzji rekrutacyjnych od danych biometrycznych na przykład wizerunku twarzy, bez uzasadnionego związku z wymaganiami stanowiska może prowadzić do naruszenia zasad ochrony danych osobowych oraz wprowadzania dyskryminacyjnych praktyk rekrutacyjnych. Przedstawione działania stanowią potencjalne naruszenia zasad ochrony danych osobowych narażając pracodawcę na konsekwencje prawne, w tym na kary finansowe oraz utratę zaufania społecznego. Z tego powodu pracodawcy zobowiązani są do stosowania uczciwych i transparentnych praktyk rekrutacyjnych, eliminując wszelkie przejawy dyskryminacji i przestrzegając norm ochrony danych osobowych.

Podsumowanie – Ochrona Danych Osobowych w Procesie Rekrutacji

Reasumując ochrona danych osobowych stanowi nieodłączny element procesu rekrutacyjnego . Jest to wąska i często niedoceniana gałąź prawa nieodłącznie sprzężona w omawianym kontekście z prawem pracy , a także prawem administracyjnym oraz cywilnym w szczególności w zakresie kar za niewłaściwe przeważanie danych dla podmiotów nimi administrujących . Procedura ochrony danych osobowych kandydatów ubiegających się o zatrudnienie jest bardzo złożona , co przedstawiają wcześniejsze rozważania w tym zakresie wskazujące zaledwie główne kwestie w tym zakresie . Wobec czego należy wysnuć wniosek ,iż niewątpliwie owa złożoność tego procesu stanowi jedno z wielu wyzwań jakie stoją przed ochroną danych osobowych przetwarzanych w procesie rekrutacji. Prawidłowe przetwarzanie danych osobowych nie jest łatwe zwłaszcza ,iż sam proces

rekrutacji można podzielić na różne etapy – zbieranie , przetwarzanie, przechowywanie danych -. Biorąc pod uwagę ten wewnętrzny podział samego procesu w stosunku ,do którego na każdym jego etapie po części mają zastosowanie odrębne przepisy mu dedykowane w kontekście należytej ochrony danych oraz zaangażowanie wielu osób w procesie rekrutacji (pracodawcy pełniącego rolę administratora danych bądź też ewentualnie podmiotów zewnętrznych pełniących te funkcję oraz oczywiście pracowników potencjalnego pracodawcy zaangażowanych w rekrutacje na vacat) zarządzanie danymi osobowymi w rekrutacji jest tak trudne i skomplikowane. Jednakże należy pamiętać ,że jest to kluczowy proces mający na celu zapewnienie ochrony prywatności osób poszukujących zatrudnienia. Wyzwaniem stojącym po stronie pracodawcy jest także właściwe poinformowanie kandydatów o przetwarzaniu ich danych osobowych jest to element , który nie tylko stanowi wymóg prawa, ale również taka kwestia, która zadecyduje o tym ,że dana osoba zdecyduje się wziąć udział w rekrutacji na dane stanowisko . Jest to istotny punkt z uwagi na wzrastającą w świadomości społeczeństwa wartość danych osobowych , które w XXI wieku stanowią jedną z najważniejszych walut. Zagrożeniem dla przetwarzanych danych są oczywiście wszelkiego rodzaju wycieki danych czy ataki cybernetyczne mające na celu pozyskanie tak cennych informacji . Wobec czego nieodzownym obowiązkiem administratora danych osobowych jest należyte ich zabezpieczenie, aby nie dopuścić np. do kradzieży tożsamości bądź też innych form nadużyć.

Kończąc wywód należy wskazać na istotę chęci i świadomości samego kandydata ubiegającego się o zatrudnienie , gdyż z prezentowanych w analizie przepisów prawnych wynika jednoznacznie ,że co do zasady poza szczególnymi wypadkami objętymi w przepisach dotyczących ochrony danych osobowych to właśnie jego świadoma zgoda stanowi podstawę przetwarzania danych i to w szczególności tych sklasyfikowanych jako wrażliwe. Ustawodawca chcąc chronić jego prawo do prywatności określił katalog danych jakich może żądać pracodawca od osoby ubiegającej się o pracę ,co w kontekście polskich regulacji w szczególności ujmuje art. 22^1 Kodeksu pracy. Ma to za zadanie ochronić pracownika przed dyskryminacją , która mogłaby zostać wywołana żądaniem przedstawienia na poczet rekrutacji danych odnoszących się do stanu cywilnego , religii czy przekonań politycznych.

Uwadze należy poddać fakt ,iż wyzwania związane z ochroną danych osobowych w kontekście procesu rekrutacji nakładają obowiązek nieustannego dostosowywania praktyk rekrutacyjnych do dynamicznych zmian w przepisach, technologii oraz oczekiwaniach społecznych, a efektywne kierowanie tymi aspektami

stanowi kluczowy element w utrzymaniu zaufania zarówno ze strony kandydatów oraz ogółu społeczeństwa.

Bibliografia

Jaśkowski K., Maniewska E.
2023 *Kodeks pracy. Komentarz*, Wydanie 13, Wolters Kluwer.

Urząd Ochrony Danych Osobowych (UODO)
2018 *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, https://orka.sejm.gov.pl/BOP_info.nsf/0/43826AB057FD-3661C125832E00368D2F/%24File/Poradnik%20dotycz%C3%84%E2%80%A6cy%20zatrudnienia.pdf.

Weronika Anna Łowicka

Uniwersytet Mikołaja Kopernika w Toruniu

Studentka

SYGNALISTA – NOWA OCHRONA JAKO WYZWANIE DLA REGULACJI PRAWNEJ

> Szkoła, praca, organizacje obywatelskie i systemy polityczne nie pozwalają ludziom robić wszystkiego, co naprawdę potrafią. (...) ludzka zdolność do współpracy jest o wiele większa i bardziej złożona niż to, na co pozwalają instytucje (Sennett 2013).

DEMASKUJĄCY NARUSZENIE CZYLI SYGNALISTA

Na sam początek należy odróżnić zgłaszanie nieprawidłowości jako sygnalista a jako donosiciel. Donos jest jawnym lub anonimowym zgłoszeniem, które oskarża osobę lub instytucję do podmiotu, który posiada uprawnienia wobec oskarżonego. Ważne jest tu podkreślenie osobistej korzyści donosiciela jako konsekwencji tego działania. Sygnalista natomiast nie zgłasza by skorzystać, ale by skorzystało jego otoczenie. Najważniejszą wstępną przesłanką zgłaszającego jest dobra wiara w działaniu, które ma na celu poprawę sytuacji w danej organizacji. Brzmi jak świetlana idea utopijnego świata, ponieważ wydawać by się mogło, że każdym kieruje jednak osobista pobudka. Jednak czy fundament tego pomysłu jest nowy?

Sygnaliści istnieją od dawna. Pierwszymi udokumentowanymi sygnalistami byli marynarze w 1777 roku w Stanach Zjednoczonych (Stranger 2019). Dziesięciu amerykańskich marynarzy zgłosiło zachowanie Eska Hopkinsa – swojego komandora w marynarce kontynentalnej. Spisali to w formie petycji do Kongresu Kontynalnego. Zareagowano na to zgłoszenie i wsparto oficerów poprzez

zwolnienie Hopkinsa, ten jednak pozwał marynarzy o zniesławienie w wyniku czego dwoje z nich zostało aresztowanych. I tutaj ponownie Kongres wsparł marynarzy otaczając ich ochroną, która była odpowiednia dla współczesnego sygnalisty. Również to w Ameryce po raz pierwszy użyto określenia whistleblower. W 1971 r. termin ten dzięki Ralphowi Naderowi[1] wprowadzony został do obiegu, ale początkowo definiowano go dla każdego zgłaszanego naruszenia niezależnie od motywu, dopiero z czasem przypisano go wyłącznie do osoby zgłaszającej naruszenie w dobrej wierze.

Jaka jest więc ciągle kreująca się sylwetka sygnalisty? Dyrektywa 2019/1937 daje początek współczesnej kreacji tej osoby. Wskazuje, że osoby pracujące dla organizacji publicznej lub prywatnej są pierwszymi, które będą mogły naocznie, bądź z dostarczonych im informacji wykryć naruszenie w tej organizacji dla niej szkodliwe. Sygnalistą będzie więc każdy kto miał związek z organizacją w kontekście związanym z pracą[2]. Będzie to więc pracownik, pracownik tymczasowy, osoba świadcząca pracę na innej podstawie niż stosunek pracy, ale również przyszły pracownik (w rekrutacji) czy były pracownik. Będzie to również przedsiębiorca zaangażowany w prace organizacji, akcjonariusz wspólnik czy członek organu, a także osoba świadcząca pracę pod nadzorem i kierownictwem. Według Ustawy z dnia 14 czerwca 2024 r. polska regulacja objęła również funkcjonariusza oraz żołnierza. Nie jest to jednak regulacja obejmująca tylko osoby, które otrzymują pieniądze od organizacji. Będzie to również stażysta, wolontariusz czy praktykant, którzy nie będą otrzymywać wynagrodzenia[3]. Sygnalistą może być każdy z nas. Mamy pełne prawo i obowiązek zgłoszenia naruszenia prawa w miejscu pracy. Sygnalista to nie jest jednak stanowisko, ani funkcja - jest to status który uzyskujemy po dokonaniu zgłoszenia naruszenia prawa.

W konkluzji jest to osoba fizyczna, która kanałem zewnętrznym lub wewnętrznym zgłasza naruszenie albo ujawnia publicznie informacje na temat naruszeń uzyskane w kontekście związanym z pracą. Zostanie sygnalistą wymaga jednak by przekazywano informacje w dobrej wierze, by były one prawdziwe w momencie zgłoszenia, by spełniały zakres przedmiotowy przepisów ustawy oraz aby doszło do samego zgłoszenia lub ujawnienia. Zgodnie z ustawą podmiot

[1] Amerykański polityk i aktywista społeczny, który stanął na czele pierwszego współczesnego ruchu konsumenckiego i objechał kraj z wykładami oraz organizował grupy społeczne, których celem była walka z niedbałością i żądzą zysku wielkich korporacji.

[2] Przeszłe, obecne lub przyszłe działania związane z wykonywaniem pracy na podstawie stosunku pracy lub innego stosunku prawnego. Są to wszelkie informacje, które mogą być korzystne dla polepszenia funkcjonowania organizacji poprzez możliwość podjęcia działania następczego po otrzymaniu zgłoszenia od sygnalisty.

[3] Dz.U. 2024 poz. 928.

może jednak w procedurze wewnętrznej rozszerzyć katalog przedmiotowych dokonywanych naruszeń prawa. Wtedy jednostka uzyskuje pełnoprawną ochronę wynikającą z tytułu regulacji normatywnej. Takiej ochronie mogą podlegać również osoby z nią związane tj. osoba, która pomogła w dokonaniu zgłoszenia, osoba trzecia powiązana z sygnalistą np. żona/mąż, ale również prowadząca z nią wspólne gospodarstwo domowe, podmioty prawne stanowiące własność, zatrudniające lub inaczej połączone z sygnalistą w kontekście związanym z pracą.

FORMY ZGŁASZANIA NARUSZEŃ W USTAWIE Z DNIA 14 CZERWCA 2024 R. O OCHRONIE SYGNALISTÓW

Najważniejszą kwestią przed samym wyborem formy zgłoszenia naruszenia istotne jest, że polskim projekt ustawy o ochronie sygnalistów posługuje się katalogiem w zakresie przedmiotowym. Jest to wzorowane na dyrektywie 2019/1937 UE.

> ***Art. 3.*** *1. Naruszeniem prawa jest działanie lub zaniechanie niezgodne z prawem lub mające na celu obejście prawa dotyczące:*
> 1) korupcji;
> 2) zamówień publicznych;
> 3) usług, produktów i rynków finansowych;
> 4) przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;
> 5) bezpieczeństwa produktów i ich zgodności z wymogami;
> 6) bezpieczeństwa transportu;
> 7) ochrony środowiska;
> 8) ochrony radiologicznej i bezpieczeństwa jądrowego;
> 9) bezpieczeństwa żywności i pasz;
> 10) zdrowia i dobrostanu zwierząt;
> 11) zdrowia publicznego;
> 12) ochrony konsumentów;
> 13) ochrony prywatności i danych osobowych;
> 14) bezpieczeństwa sieci i systemów teleinformatycznych;
> 15) interesów finansowych Skarbu Państwa Rzeczypospolitej Polskiej, jednostki samorządu terytorialnego oraz Unii Europejskiej;
> 16) rynku wewnętrznego Unii Europejskiej, w tym publicznoprawnych zasad konkurencji i pomocy państwa oraz opodatkowania osób prawnych.
> 17) konstytucyjnych wolności i praw człowieka i obywatela – występujące w stosunkach jednostki z organami władzy publicznej i niezwiązane z dziedzinami wskazanymi w pkt 1–16
>
> 2. Podmiot prawny może dodatkowo w ramach procedury zgłoszeń wewnętrznych przewidzieć możliwość zgłaszania informacji o naruszeniach dotyczących obowiązujących w tym podmiocie prawnym regulacji wewnętrznych lub standardów etycznych, które zostały ustanowione przez podmiot prawny na podstawie przepisów prawa powszechnie obowiązującego i pozostają z nimi zgodne[4].

[4] Dz.U. 2024 poz. 928.

Pojawiły się głosy, że powinniśmy w tym miejscu znaleźć katalog otwarty[5] - jak wtedy jednak wykluczono by naruszenia, które projekt wprost wskazuje? Sygnalistą nie może być bowiem osoba fizyczna posiadająca informacje w zakresie danych objętych przepisami o ochronie informacji niejawnych, tajemnicą zawodów medycznych oraz prawniczych, tajemnicą narady sędziowskiej oraz związanymi z poszczególnymi etapami postępowania karnego. Ustawa pozostawia jednak możliwość poszerzenia tego katalogu wyłącznie w ramach procedury wewnętrznej.

Czas przejść do najważniejszego pytania- Jak mogę dokonać zgłoszenia?

Sygnalista ma do wyboru trzy formy zgłoszenia: może przekazać informacje o naruszeniu poprzez kanał wewnętrzny, który zapewnia mu jego organizacja, może przekazać informacje o nieprawidłowościach w regulacjach poprzez kanał zewnętrzny oraz dokonać ujawnienia publicznego.

Kanał wewnętrzny zapewnia podmiot publiczny lub prywatny, który może podejmować działania w kontekście związanym z pracą czyli w praktyce każdy. Ustanowiono jednak próg minimalny dla tego obowiązku- podmiot prawny, dla którego według stanu na dzień 1 stycznia lub 1 lipca wykonuje pracę zarobkową co najmniej 50 osób. Liczymy te osoby poprzez pracowników w przeliczeniu na pełne etaty oraz inne osoby świadczące pracę na innej podstawie niż stosunek pracy za wynagrodzeniem. Zauważamy, że choć osoby dokonujące czynności na rzecz podmiotu obejmuje zakres ochrony sygnalisty to nie są one wliczane do ilości osób fizycznych ustanawiających obowiązek utworzenia kanału zgłoszeń wewnętrznych. Pojawiają się również dwa odrębne wyjątki, ponieważ próg nie będzie miał zastosowania do podmiotów prawnych, które wykonują działalność w zakresie usług, produktów i rynków finansowych oraz przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, bezpieczeństwa transportu i ochrony środowiska, objętych innymi aktami prawnymi UE, ponieważ są one zobowiązane niezależnie od progu oraz do jednostek samorządu terytorialnego obszaru gminy lub powiatu, które liczą mniej niż 10 000 mieszkańców, ponieważ będą one zwolnione z obowiązku.

Projekt ustawy przewiduje jednak możliwość ustalenia wspólnej procedury zgłoszeń[6] dla jednostek samorządu terytorialnego w ramach wspólnej obsługi zgłoszeń. W zakresie wspólnej procedury zgłoszeń JST muszą dokonać ustalenia procedury zgłoszeń w ramach wspólnej obsługi, która jest możliwa na podstawie przepisów samorządowych. Obowiązkowo muszą zapewnić jej odrębność

[5] Instytut Spraw Obywatelskich.

[6] Regulowana przepisami o samorządzie gminnym, powiatowym, wojewódzkim.

i niezależność procedury i podejmowania działań następczych. Można określić, że wszelkie wykonawcze podmioty JST posiadają obowiązek utworzenia takiego rozwiązania.

Pracodawca zapewnia system zgłaszania w swoim zakładzie pracy jeżeli został na niego nałożony ustawowy obowiązek ustanowienia kanałów zgłaszania naruszeń. Powinien w przeciągu siedmiu dni odpowiedzieć, że otrzymał zgłoszenie, a w terminie trzech miesięcy zakończyć działania następcze związane z sygnalizowaną informacją. W przypadku gdyby nie przeprowadził odpowiednich czynności osoba zgłaszająca może skierować swoją informację do zgłoszenia zewnętrznego. Zgłoszenia zewnętrznego sygnalista może jednak dokonać z pominięciem zgłoszenia wewnętrznego, pomimo iż jest ono zalecane.

Jak działa zgłoszenie zewnętrzne? W zakresie zewnętrznego zgłoszenia przekazujemy informację o naruszeniu prawa do Rzecznika Praw Obywatelskich[7] albo organu publicznego. Początkowo organem odpowiedzialnym miała być Państwowa Inspekcja Pracy, ale zrezygnowano z tego rozwiązania w kolejnych projektach. Przez organ publiczny rozumiemy natomiast naczelne i centralne organy jednostek samorządu terytorialnego oraz inne wykonujące z mocy prawa zadania z zakresu administracji publicznej. Jako sygnalista mogę obawiać się dokonać zgłoszenia do własnej organizacji pomimo ścisłej regulacji o zakazie działań odwetowych.

Obie powyższe formy mogą jednak okazać się niewystarczające. Co wtedy? Pozostaje ostatnia, trzecia droga tj. ujawnienie publiczne. Jest to podanie informacji o naruszeniu prawa lub jej uzasadnionego podejrzenia do ogólnej wiadomości publicznej. Błędnie rozumie się przez to jako podanie do prasy, a ustawodawca w najnowszym projekcie ustawy jasno określił, że jeżeli przekazanie informacji o naruszeniu prawa następuje bezpośrednio do pracy to nie stosuje się przepisów o ochronie sygnalisty tylko ustawę o prawie prasowym. Przykładem takiego ujawnienia jest przykładowo rozesłanie maila do osób trzecich o naruszeniu. Nie doprecyzowano jednak jaki jest próg aby ustalić- czy to już jest ujawnienie publiczne czy jeszcze nie – Czy ujawnienie publiczne zaczyna się od dziesięciu osób czy od pięćdziesięciu? Na ten moment niestety nie wiemy, możliwe że dookreśli to dopiero praktyka.

Sygnalista aby podlegać ochronie w zakresie ujawnienia publicznego musi spełnić ustawowe kryteria. Musi dokonać zgłoszenia wewnętrznego, a następnie

[7] Projekt polskiej ustawy 26.02.2024 r.; We wcześniejszych projektach tą instytucją miała być Państwowa Inspekcja Pracy, ale odstąpiono od tego pomysłu ze względu na rozgraniczenie z donosem, charakter instytucji oraz rodzaj procedury.

zewnętrznego i w terminie nie zostaną podjęte działania odpowiednie do naruszenia lub przy takiej samej sytuacji z pominięciem zgłoszenia wewnętrznego dokona zgłoszenia zewnętrznego. Są to jednak przesłanki wzruszalne, ponieważ ochrona będzie zapewniona również w przypadku gdy istnieje uzasadniona podstawa, że ujawnianie naruszenie może stanowić oczywiste bądź bezpośrednie zagrożenie dla interesu publicznego lub gdy zgłoszenie zewnętrze spowoduje działania odwetowe, ukrycie lub zniszczenie dowodów, zmowę lub udział organu publicznego.

Pracodawca kiedy zakończy się okres vacatio legis Ustawy o ochronie sygnalistów będzie zobowiązany zapewnić w firmie, sądzie, jednostce samorządu terytorialnego czy szpitalu odpowiednią procedurę wewnętrzną zgłaszania naruszeń – tak aby każda z trzech form była dostępna i bezpieczna.

NOWE OBOWIĄZKI DLA PRACODAWCÓW I PRACOWNIKÓW

O sygnaliście mówi się coraz częściej i coraz bardziej szczegółowo. Jest to procedura, która ma umożliwić pracodawcy, ale również pracownikom zapobieganie naruszeniom w organizacji. Oznacza to jednak zmiany i dostosowanie się do precyzyjnych wymogów ustawowych w zakresie organizacji publicznych i prywatnych. Pierwsze projekty przewidywały miesięczny okres vacatio legis na wdrożenie wewnętrznej procedury zgłoszeń. Ku korzyści podmiotów prawnych został on przedłużony do trzech miesięcy[8], ale w świetle konieczności ingerencji w strukturę organizacji warto podjąć działania wcześniej.

Głównym obowiązkiem pracodawcy jako podmiotu prawnego jest ustalenie wewnętrznego kanału i procedury, która umożliwi pracownikowi zgłaszanie naruszeń, a jeżeli takie zgłoszenia się pojawią również podjęcie działań następczych. Tak, procedura musi przede wszystkim wskazywać na osobę wyznaczoną do obsługi zgłoszeń czyli jednostkę organizacyjną lub osobę, która na podstawie upoważnienia będzie posiadała dostęp do zgłaszanych nieprawidłowości i podejmie działania następcze. Taka osoba ma obowiązek poinformować, że odczytano zgłoszenie w terminie siedmiu dni od jego otrzymania, chyba że zgłoszenia dokonano anonimowo i nie wiemy komu właściwie odpowiedzieć. Następnie rozwiązuje sprawę w terminie trzech miesięcy od otrzymania informacji lub od udzielenia odpowiedzi o otrzymaniu zgłoszenia. Osoba obsługująca zgłoszenia nie będzie oczywiście podejmowała żadnych działań jeżeli okaże się, że zgłoszenie

[8] Okres trzymiesięczny przewidziany jest dla kanału wewnętrznego, natomiast dla kanału zewnętrznego przewidziano okres sześciu miesięcy.

było bezzasadne[9] - kiedy jest za mało szczegółów lub jest to informacja powielona bez nowych istotnych dodatków. Jeżeli pracodawca posiada już przygotowaną dokumentacje i chciałby wdrożyć na już procedurę wewnętrzną to nie jest to wystarczające. Ważnym aspektem jest konsultacja z zakładową organizacją związkową, jeżeli jest ich kilka to z zakładowymi organizacjami związkowymi, a jeżeli ich nie ma to z przedstawicielem pracowników. Ustawa o związkach zawodowych wskazuje, że tryb konsultacji przewidziany jest w poszczególnych regulacjach prawnych. Dla procedury sygnalistycznej takie konsultacje muszą trwać nie krócej niż 5 dni i nie dłużej niż 10 dni od dnia przedstawienia przez podmiot projektu procedury wewnętrznej. Nie posiadamy jednak informacji czy taka opinia jest wiążąca, także zakładamy iż jest ona niezbędna, ale niewiążąca.

Pracodawca, który pomimo posiadania obowiązku ustanowienia procedury zgłoszeń wewnętrznych, nie ustala wbrew regulacją prawnym tej procedury lub ustala ją nieprawidłowo, podlega karze grzywny.

Sygnalista uzyska z tytułu nowych regulacji dodatkowe możliwości i ochronę, ale tym samym społecznie będzie się od niego wymagać uszanowania tej doniosłej roli. Oczekiwać się będzie, że dokona on zgłoszenia, które zauważy w miejscu pracy. Może ono być związane zarówno z niewłaściwym wykonywaniem obowiązków przez poszczególnych pracowników jak i ogólnymi tendencjami w organizacji. Obowiązkiem osoby zgłaszającej jest działanie w dobrej wierze ku polepszeniu swojego środowiska pracy i nie działając w kierunku szkody.

DZIAŁANIA ODWETOWE

Są to wszelkie bezpośrednie lub pośrednie działania lub zaniechania w kontekście związanym z pracą, które jest wynikiem dokonania zgłoszenia lub ujawnienia publicznego, i które narusza lub może naruszyć prawa sygnalisty i wyrządzić mu nieuzasadnioną szkodę. Jako działanie odwetowe traktujemy również groźbę lub próbę zastosowania środków wyrządzających szkodę. Jednak nie wszelkie działania podejmowane wobec sygnalisty będą odwetowe. Zdarzają się przypadki gdy prześladowanie danej osoby pojawiło się wcześniej i to właśnie było przedmiotem zgłoszenia. Działanie odwetowe tak samo jak zgłoszenie musi być związane z pracą, z przyszłą, obecną lub przeszłą relacją pracownik a pracodawca. Jest to działanie lub zaniechanie naruszające prawa zgłaszającego lub wyrządzające zgłaszającemu szkodę. Czynności takie to odmowa nawiązania stosunku

[9] Niemożliwe do weryfikacji i podjęcia działań następczych.

pracy, wypowiedzenie stosunku pracy, obniżenie wynagrodzenia za prace, wstrzymanie nagród, awansów, przymus, zastraszanie, wykluczenie i wszelkie inne niesprawiedliwe traktowanie powodujące szkodę materialną i niematerialną[10].

Należałoby w zakresie prawa pracy spojrzeć na kodeksowy zakaz dyskryminacji[11], który stanowi, że pracownicy powinni być równo traktowani w zakresie relacji stosunku pracy: nawiązywania, rozwiązania, warunków zatrudnienia, awansowania, dostępu do szkoleń. Pracodawca przy tym obszarze nie może różnicować sytuacji ze względu na płeć, wiek, rasę, niepełnosprawność, religię, przekonania polityczne, pochodzenie etniczne, wyznaniowe, orientacje seksualną, wymiar godzinowy pracy. Kodeks pracy reguluje również pojęcie mobbingu[12] w pracy. Każdy pracodawca jest zobowiązany przeciwdziałać uporczywemu i długotrwałemu nękaniu lub zastraszaniu pracownika, które wywołuje szkodę u pracownika.

Teraz jak odróżnić działania odwetowe a dyskryminacje a mobbing? Pojawiły się w debatach społecznych głosy, że będzie problem z ustaleniem granic pomiędzy tymi pojęciami. Wszystkie polegają na działaniu lub zaniechaniu, powodują szkodę dla konkretnej osoby lub ogółu organizacji, są nieprawidłowościami, powinny być zwalczane i nietolerowane. Nie widzę jednak podstaw dla omyłek, gdyż mamy w każdym trzech pojęć odpowiedni wyróżnik. Mobbing jest uporczywy i długotrwały, nie posiada podstawy w konkretnym działaniu osoby lub organizacji, która go doświadcza. Dyskryminacja również nie posiada impulsu do powstania i jest to obowiązek równego traktowania w środowisku pracy, a katalog jest bardzo szeroki. Działania odwetowe natomiast nie są obowiązkiem jak dyskryminacja, są niepożądane jak mobbing ale nie muszą być długotrwałe. Ponad to jako jedyne znajdują ugruntowane w dokonanym zgłoszeniu lub ujawnieniu – dopiero gdy zdarzą się po jednym z nich możemy je tak określić. Upraszczając moglibyśmy przyjąć chronologię, że najpierw występuje zakaz dyskryminacji jako obowiązek, następnie jeżeli obowiązek zostanie złamany i trwa to pojawia się mobbing , a jeżeli sygnalista dokona zgłoszenia i pojawią się nowe, odrębne od mobbingu działania lub zaniechania na jego szkodę to mamy odwet.

[10] Dz.U. 2024 poz. 928.
[11] Art. 18 (3a) , Dz.U. 1974 nr 24 poz. 141.
[12] Art. 94 (3) Mobbing, Dz.U. 1974 nr 24 poz. 141.

SYGNALISTA A OCHRONA DANYCH OSOBOWYCH

Ochrona danych osobowych jest podstawą ochrony sygnalisty. Dane osobowe sygnalisty to wszelkie dane przetwarzane w związku z przyjęciem zgłoszenia lub podjęcia działań następczych. Odpowiednio zabezpieczone i poufne, nie podlegające ujawnieniu nieupoważnionym osobom. Dane są odpowiednio zabezpieczane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r.. Poufność tożsamości osoby zgłaszającej naruszenie powinno być zapewnione poprzez odpowiednie rozwiązania techniczne i organizacyjne, aby chronić nie tylko zgłaszającego, ale również dane osób wymienionych w tym zgłoszeniu[13]. Dostęp powinna mieć ograniczona liczba osób, a dokładniej głównie wspomniany już wcześniej koordynator czyli osoba/osoby wyznaczone do obsługi zgłoszeń na postawie pisemnego upoważnienia. Są one zobowiązane do zachowania tajemnicy posiadanych informacji, również po cofnięciu upoważnienia. Polski projekt ustawy[14] stanowi, że kto wbrew regulacją ujawnia dane sygnalisty, osoby z nią powiązanej lub osoby, która pomogła w dokonaniu sygnalizacji naruszenia to podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do roku. Bardzo dobrym rozwiązaniem jest anonimizacja[15] danych sygnalisty przykładowo gdy przekazujemy informacje osobom odpowiedzialnym za wykonanie działań następczych albo kiedy raportujemy naruszenia. Wszelkie jednak dodatkowe zabezpieczenia mogą być przez nas zastosowane jedynie, kiedy nie wpływa to na weryfikację zgłoszenia i wykonanie czynności następczych. Aby ochrona funkcjonowała prawidłowo należy ująć w regulaminach i procedurach dotyczących przyjmowania i obsługi zgłoszeń stosowne zapisy tzw. Klauzule informacyjne. Obecnie podstawą dla przetwarzania danych sygnalisty jest prawnie uzasadniony interes administratora[16], nawet jeżeli jest to zgodne z dyrektywą UE, kiedy pojawi się polska ustawa to będzie to już wynikało z obowiązku prawnego ciążącego na części przedsiębiorców. Podmiot prawny zapewnia ochronę nie tylko sygnaliście, ale również osobom, których to zgłoszenie dotyczyło czy świadków lub współpracowników zdarzenia, na każdym etapie rozpatrywania naruszenia. Potencjalną podstawą przetwarzania naruszeń gdzie mogą być zawarte i dane zwykłe jak i wrażliwe jest głownie art. 6 RODO[17], który obejmie zgodę na ujawnienie tożsamości, obowiązki administratora, działania w zakresie

[13] Naruszających, świadków, współsprawców, źródła informacji.
[14] Projekt ustawy 26.02.2024 r.
[15] Uniemożliwienie zidentyfikowania określonej osoby.
[16] Art. 6 u. 1 lit. f Dz.U. 2018 poz. 1000.
[17] Dz.U. 2018 poz. 1000.

interesu publicznego, ale również art. 9 RODO ze względu na dane wrażliwe kiedy przetwarzanie danych niezbędne w celu ważnych interesów publicznych oraz art. 10 RODO o przetwarzaniu danych o wyrokach skazujących, czynów zabronionych lub powiązanych. Jest to podstawa postępowania zarówno w zakresie kanału wewnętrznego jak i zewnętrznego. W zakresie w jakim sygnalista godzi się na ujawnienie swojej tożsamości, to zgodnie z RODO jest to podstawa przetwarzania jego danych. W zakresie działań następczych zbyt wczesne ujawnienie danych osób związanych ze sprawą może doprowadzić do zniweczenia celu prowadzonego postępowania na co wskazuje dyrektywa UE 2019/1937 stanowiąc, że procedury dotyczące działań następczych związanych ze zgłoszeniami naruszeń prawa Unii w dziedzinach objętych zakresem jej stosowania służą osiągnięciu ważnego celu leżącego w ogólnym interesie Unii i państw członkowskich w rozumieniu art. 23 ust.1 lit. e) RODO, gdyż celem jest poprawa praw i polityk Unii. Podstawa gwarancji poufności danych określa dyrektywa o osobie zgłaszających naruszenia, która zapewnia że aby tożsamość sygnalisty nie została ujawniona to danej tej osoby nie mogą być przekazane bez jej zgody żadnej nieuprawnionej do rozpatrywania zgłoszenia osobie. Tutaj działamy w zakresie zgody sygnalisty, zapewnienia poufności osobie wskazanej w naruszeniu i jej zgody, obowiązku zachowania tajemnicy zawodowej i umowy powierzenia przetwarzania danych osobowych.

SYGNALISTA A PRAWO PRASOWE

Dyrektywa 2019/1937 UE nie daje podstaw aby spod ochrony prawnej wyłączyć osoby zgłaszające naruszenia do mediów- polski projekt ustawy wyłącza jednak taką możliwość. Ujawnienie publiczne to co prawda przekazanie działania lub zaniechania będącego naruszeniem w zakresie zamkniętego katalogu, ale nie polega na wykorzystaniu prasy, telewizji. Jak już wyżej wspomniano -wprost wyłączono przepisem projektu ochronę dla osoby, która będzie ze swoimi informacjami podległa regulacją ustawy z 26 stycznia 1984 r. Prawo prasowe[18]. Wskazuje ono, że w przypadku przekazania naruszenia do prasy dziennikarz ma obowiązek dochowania poufności danych osobowych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze oraz innych osób, które przekazując informacje zastrzegły niechęć ujawniania ich danych. To wyłączenie i kierowanie się ochroną na podstawie powyższej

[18] Art. 15 ust. 2 pkt. 1, Dz.U.2018.0.1914 t.j.

regulacji z Prawa prasowego stało się utrudnieniem przy projektach polskiej ustawy ze względu na dialog z opinią społeczną. M.in.. Fundacja im. Stefana Batorego[19] czy Instytut Spraw Publicznych[20] wskazały, iż wyłączenie prasy z polskiego projektu ustawy o ochronie sygnalistów jest niezgodne z dyrektywą UE, ponieważ może to doprowadzić do sytuacji, że osoba zgłaszające nie będzie mogła skorzystać z asekuracji przewidzianej w projekcie, a tym samym obniża poziom ubezpieczenia swoich danych osobowych, tym bardziej, że sama dyrektywa 2019/1937 nie daje podstaw, żeby takiego wyłączenia w przepisach krajowych dokonać.

CZY POLSKA JEST GOTOWA NA NOWĄ REGULACJĘ?

Przede wszystkim ciągle pojawiającym się pytaniem jest – Kiedy w Polsce pojawi się ustawa o ochronie sygnalistów? Dyrektywa Parlamentu Europejskiego i Rady UE 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii powinna być zgodnie z prawem unijnym wdrożona przez państwo członkowskie w określonym czasie. 17 grudnia 2021 r. minął dla Polski czas implementacji. Kolejny termin wyznaczono nam na 17 grudnia 2023 r. i również nie został dotrzymany. Wydaje się, że prace nad przepisami dotyczącymi ochrony osób zgłaszających nabierają rozpędu. Mimo to Trybunał Sprawiedliwości wypowiedział się negatywnie w kwestii ociągania się w zakresie wdrożenia regulacji w naszym kraju. Skargę na Polskę wniosła Komisja Europejska. Polska argumentowała, że opóźnienia wynikły ze zbyt szerokiego zakresu regulacji dyrektywy 1937/2019, pandemii COVID-19 oraz napływu uchodźców ze względu na agresję na Ukrainę. TSUE odrzuciło argumenty Polski, zauważono, że polskie argumenty dotyczyły wszystkich krajów Unii Europejskiej. Reszta krajów UE poradziła sobie to mimo przeszkód z implementacją dyrektywy na grunt prawa krajowego. Polska w wyniku została zobowiązana do zapłacenia siedmiu milionów euro ryczałtu kary i czterdziestu tysięcy kary dziennie do dnia, aż ustawa się pojawi[21].

Sygnalista wymaga odpowiedniego, wcześniejszego przygotowania. Pojawiają się głosy, że kiedy ustawa w końcu się pojawi to kraj nie będzie gotowy na tą regulacje. Obawia się o zrozumienia zakresu przedmiotowego i podmiotowego, przeszkolenie organizacji, zmieszczenie się w czasie vacatio legis, nadużywanie ochrony o zgłaszaniu naruszeń, nie mówiąc już, że dalej nie wyjaśniono

[19] Organizacja pozarządowa o statusie organizacji pożytku publicznego. Głównym celem jej działalności jest udzielanie dotacji organizacją podejmującym działania na rzecz dobra publicznego.
[20] Pozarządowy i niezależny ośrodek analityczno- badawczy.
[21] Wyrok TSUE z 26.04.2024 r.

szczegółowych praktycznych aspektów pracy Rzecznika Praw Obywatelskich w zakresie przyjmowania zgłoszeń zewnętrznych[22].

Po długotrwałej legislacji dnia 24 czerwca 2024 r. w Dzienniku Ustaw została ogłoszona Ustawa z dnia 14 czerwca 2024r. o ochronie sygnalistów i aktualnie jest w okresie vacatio legis- obawy co do niej na ten moment pozostają niezmienne[23].

Na szczęście pojawia się coraz więcej specjalistów w tym zakresie, którzy chętnie przeszkalają wszelkie podmioty prawne, które tego potrzebują. Szkolenia są nieodłącznym elementem towarzyszącym wdrażaniu nowych narzędzi w miejscu pracy. Celem jest zapoznanie organizacji w zakresie ochrony z Dyrektywy Parlamentu Europejskiego i Rady UE 2019/1937 z 23 października 2019 r, możliwych rozwiązań kanału zgłoszeniowego czy pomoc przy procedurze wewnętrznej. Korzyści szkolenia to świadomość aktualnego stanu prawnego z unijnej dyrektywy oraz polskiego projektu ustawy, powszechne zrozumienie komu przysługuje ustawowa ochrona, uświadomienie celu procedur tj. przeciwdziałanie działaniom odwetowym, zwiększenie zaufania do procedury wewnątrz środowiska pracy, usprawnienie mechanizmu ochrony wizerunku podmiotu.

Warto, żeby szkolić nie tylko podmioty, ale ogół społeczeństwa, który na rozwiązanie służące polepszeniu społeczeństwa działa jako zawistne działanie na niekorzyść osoby trzeciej.

BIBLIOGRAFIA

Akty prawne

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, (Dz.U. 1974 nr 24 poz. 141).

Ustawa z dnia 26 stycznia 1984 r., Prawo prasowe, (Dz.U.2018.0.1914 t.j.).

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

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

Projekt polskiej ustawy o ochronie sygnalistów z 26.02.2024 r.

[22] Stan opisywany na marzec 2024r.
[23] Stan opisywany na lipiec 2024 r.

Literatura

Arcimowicz J. i inni
2018 *Skarżypyty, donosiciele, sygnaliści?: studium socjologiczno-prawne,* Instytut Stosowanych Nauk Społecznych UW.

Baran B., Ożóg M.
2021 *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Wolters Kluwer Polska.

Baran-Wesołowska B.
2024 *Zgłaszanie nieprawidłowości. Whistleblowing w praktyce,* Wolters Kluwer Polska.

Gąsecka A.
2021 *Ochrona sygnalistów. Nowe obowiązki pracodawców*, Wiedza i Praktyka.

Jabłoński M., Radziszewski T., Wasiak D., Wygoda K.
2022 *Sygnalista a ochrona danych osobowych – wybrane zagadnienia systemowe,* Wydawnictwo Adam Marszałek.

Sennett R.
2013 *Razem. Rytuały, zalety i zasady współpracy,* Spectrum.

Stranger A.
2019 *Whistleblowers: Honesty in America from Washington to Trump*, Yale University Press

mgr **DOMINIKA FILIPEK**
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Absolwentka

ZAKRES PROCEDUR OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH PRZEZ OSOBY UPOWAŻNIONE W PRZEDSIĘBIORSTWIE

WPROWADZENIE

Procedury ochrony danych osobowych przetwarzanych przez osoby upoważnione w przedsiębiorstwie stanowią kluczowy element zapewnienia zgodności z przepisami o ochronie danych oraz umożliwienia odpowiedzialnego i bezpiecznego gospodarowania informacjami prywatnymi. Celem artykułu jest w szczególności zbadanie procedur ochrony danych osobowych w kontekście osób upoważnionych w przedsiębiorstwie, koncentrując się na kluczowych zagadnieniach, takich jak cele, zasady oraz wyzwania związane z tym obszarem.

Ochrona danych osobowych przez osoby upoważnione ma szczególne znaczenie w kontekście regulacji takich jak: 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 (dalej jako: „Ogólne Rozporządzenie o Ochronie Danych w Unii Europejskiej" lub „RODO"). Wdrażanie odpowiednich procedur staje się fundamentalne dla przedsiębiorstw, ponieważ osoby upoważnione mają dostęp do wrażliwych informacji, co wymaga szczególnej ostrożności i przestrzegania ścisłych zasad ochrony danych.

Centralnym aspektem procedur ochrony danych osobowych jest zapewnienie przestrzegania zasad transparentności, uczciwości i legalności przetwarzania danych. Osoby upoważnione są zobowiązane do przestrzegania tych zasad

podczas gromadzenia, przetwarzania i przechowywania informacji osobowych. Ich działania powinny być zgodne z politykami oraz procedurami zapewniania bezpieczeństwa danych określonymi przez przedsiębiorstwo.

Edukacja i szkolenia pracowników mają również istotny wpływ na skuteczność procedur ochrony danych osobowych. Wdrożenie kompleksowych programów szkoleniowych, które podkreślają znaczenie ochrony danych, ich bezpiecznego przetwarzania i zachowania poufności jest niezbędne dla zwiększenia świadomości pracowników na temat konsekwencji naruszeń związanych z ochroną danych.

Niezwykle ważnym elementem procedur ochrony danych osobowych jest także ciągłe monitorowanie działań osób upoważnionych w zakresie przetwarzania informacji. Regularne audyty wewnętrzne pozwalają na ocenę zgodności z przepisami oraz identyfikację ewentualnych luk w procedurach ochrony danych. Działanie te umożliwia wdrożenie szybkich reakcji i poprawek w przypadku wykrycia problemów.

Zgodnie z przepisami RODO, osoby upoważnione mają obowiązek współpracy z organem nadzorczym ds. ochrony danych osobowych. W razie jakichkolwiek wątpliwości czy incydentów związanych z przetwarzaniem danych, ich aktywna kooperacja z organem nadzorczym jest kluczowa dla zapewnienia zgodności z prawem oraz skutecznej reakcji na ewentualne zagrożenia.

Skuteczne procedury ochrony danych osobowych w przedsiębiorstwie, w kontekście osób upoważnionych, wymagają nieustannego doskonalenia, edukacji pracowników oraz monitorowania zmian w przepisach dotyczących ochrony danych. Ich właściwe wdrożenie stanowi kluczową kwestię w kontekście zapewnienia zaufania klientów, partnerów biznesowych oraz całego społeczeństwa do sposobu, w jaki organizacje zarządzają i chronią dane osobowe, jednocześnie przestrzegając najwyższych standardów bezpieczeństwa i zgodności prawnej.

Wszystkie te elementy, czyli wypracowanie odpowiednich procedur, edukacja pracowników, monitorowanie i audytowanie działań oraz współpraca z organem nadzorczym, łącznie stanowią kompleksową strategię ochrony danych osobowych przetwarzanych przez osoby upoważnione w przedsiębiorstwie. Ich właściwe wdrożenie przekłada się nie tylko na zgodność z przepisami, ale również na budowanie zaufania, co ma kluczowe znaczenie dla długoterminowego sukcesu organizacji w dobie coraz większego znaczenia ochrony danych osobowych.

Artykuł uwzględnia stan prawny obowiązujący w dniu 1 marca 2024 r.

PODSTAWOWE DEFINICJE

- ***„dane osobowe"*** – zgodnie z art. 4 pkt 1 RODO, oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („*osobie, której dane dotyczą*"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- ***„przetwarzanie"*** **–** zgodnie z art. 4 pkt 2 RODO, oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- ***„podmiot przetwarzający"*** **–** zgodnie z art. 4 pkt 8 RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
- ***„odbiorca"*** – zgodnie z art. 4 pkt 9 RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
- ***„przedsiębiorca"*** – zgodnie z art. 4 pkt 18 RODO, oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.

OBOWIĄZEK USTANOWIENIA PROCEDUR OCHRONY DANYCH OSOBOWYCH

W obliczu coraz większego znaczenia danych osobowych w dzisiejszym świecie cyfrowym, obowiązek ustanowienia skutecznych procedur ochrony danych osobowych przez przedsiębiorstwa stał się kwestią kluczową. Przedsiębiorstwa jako podmioty przetwarzające dane osobowe, mają zatem obowiązek ustanowienia skutecznych procedur ochrony tych danych (Sagan-Jeżowska 2018, s. 120-122).

Istotnym elementem procedur ochrony danych jest określenie zakresu danych osobowych, do których mają dostęp osoby upoważnione. Jest to niezwykle istotne, ponieważ pozwala to na kontrolę przepływu danych wewnątrz przedsiębiorstwa oraz minimalizuje ryzyko nieuprawnionego dostępu do danych. W tym kontekście ważne jest także zastosowanie zasad minimalizacji danych, co oznacza przetwarzanie tylko niezbędnych informacji, które są konieczne do osiągnięcia określonych celów.

W zakresie obowiązku ustanowienia procedur ochrony danych osobowych niezwykłą wagę mają przepisy RODO. Art. 24 RODO precyzuje, że administratorzy danych osobowych mają obowiązek stosować odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni poziom bezpieczeństwa. W praktyce oznacza to, że przedsiębiorstwa muszą opracować kompleksowe procedury, które będą skutecznie chronić dane osobowe przed nieuprawnionym dostępem, utratą, zniszczeniem czy nieautoryzowanym ujawnieniem (Wyka i Mielczarek 2019, s. 120-126).

Podstawowe wymagania, jakie nakłada art. 24 RODO na administratorów danych osobowych, to:

- ocena ryzyka;
- zastosowanie adekwatnych środków ochrony danych osobowych;
- monitorowanie i aktualizowanie środków ochrony danych osobowych;
- dokumentacja procedur ochrony danych osobowych.

W związku z powyższym, należy zarówno podkreślić znaczenie dokumentowania procedur ochrony danych. Artykuł 30 RODO nakłada na przedsiębiorstwa obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, co obejmuje opis stosowanych procedur ochrony. Ma to na celu zapewnienie przejrzystości i odpowiedzialności w zakresie przetwarzania danych osobowych. Prowadzenie rejestru czynności przetwarzania danych pomaga administratorom

danych oraz podmiotom przetwarzającym kontrolować i dokumentować procesy przetwarzania, co jest kluczowe dla zapewnienia zgodności z przepisami prawa oraz ochrony danych osobowych. Powyższy przepis nakłada na administratorów danych osobowych oraz osoby upoważnione obowiązek prowadzenia rejestru czynności przetwarzania danych (Sagan-Jeżowska 2018, s. 123-125). Rejestr ten powinien zawierać szereg istotnych informacji dotyczących przetwarzania danych osobowych m.in. informacje identyfikacyjne, cele przetwarzania, opis kategorii odbiorców oraz okres przechowywania danych.

Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (dalej: „TSUE") potwierdza wagę obowiązku ustanowienia procedur ochrony danych osobowych. W jednej z kluczowych spraw – Wyrok TSUE z dnia 10 lipca 2018 r., C-25/17 - TSUE podkreślił, że przedsiębiorstwa mają obowiązek wdrożyć skuteczne środki ochrony danych w celu zapewnienia zgodności z przepisami RODO i ochrony praw jednostek. Sprawa ta dotyczyła konkretnie monitorowania przez pracodawcę Deutsche Bank SAE zlokalizowanego w Hiszpanii, działań pracowników w miejscu pracy poprzez zainstalowanie kamer w miejscach ogólnodostępnych. Federación de Servicios de Comisiones Obreras (CCOO), hiszpański związek zawodowy, wnioskował o zaniechanie monitorowania przez bank oraz o uznanie tego działania za naruszenie prywatności pracowników. TSUE w swojej decyzji wydał wyrok, który miał znaczący wpływ na interpretację przepisów dotyczących ochrony danych osobowych w miejscu pracy. Trybunał stwierdził, że monitorowanie pracowników za pomocą kamer w miejscach ogólnodostępnych może stanowić naruszenie ich praw do prywatności, co potwierdzało konieczność zachowania równowagi między interesami pracodawcy a prawami pracowników. Decyzja ta miała dalekosiężne konsekwencje dla praktyk monitorowania pracowników przez pracodawców w całej Unii Europejskiej. W wyroku TSUE podkreślił, że aby monitorowanie było zgodne z prawem, musi być ono konieczne i proporcjonalne do celu, a pracownik musi być w pełni poinformowany o fakcie monitorowania oraz jego zakresie.

Podsumowując, obowiązek ustanowienia skutecznych procedur ochrony danych osobowych jest niezwykle istotny z perspektywy zgodności z RODO oraz ochrony danych osobowych. Wdrożenie i przestrzeganie tych procedur jest kluczowe dla zapewnienia bezpieczeństwa danych oraz zachowania zaufania klientów i partnerów biznesowych.

WDRAŻANIE PROCEDUR OCHRONY DANYCH OSOBOWYCH

Wdrożenie procedur ochrony danych osobowych to proces kompleksowy, wymagający zaangażowania zarówno kadry kierowniczej, jak i pracowników na różnych szczeblach organizacyjnych. Przeprowadzenie skutecznego wdrożenia procedur wymaga przede wszystkim edukacji pracowników oraz regularnych audytów.

W zakresie powyższego zagadnienia, niezbędną podstawę stanowi art. 5 RODO, który charakteryzuje fundamentalne zasady przetwarzania danych osobowych, które muszą być przestrzegane przez wszystkie podmioty odpowiedzialne za ich przetwarzanie (Litwiński 2009, s. 30-35).

Do powyższej wspomnianych zasad można zaliczyć:

- **zasada legalności, rzetelności i przejrzystości** - dane osobowe muszą być przetwarzane w sposób legalny, czyli zgodny z przepisami prawa. Podmiot przetwarzający musi działać w sposób rzetelny, a przetwarzanie danych musi być prowadzone w sposób przejrzysty dla osoby, której dane dotyczą;
- **zasada celowości ograniczonej** - dane osobowe mogą być zbierane i przetwarzane jedynie w celach określonych, jasnych i zgodnych z prawem. Oznacza to, że dane mogą być wykorzystywane tylko do konkretnych celów, o których osoba, której dane dotyczą, została poinformowana;
- **zasada dokładności danych -** dane osobowe powinny być dokładne i aktualne, a w przypadku konieczności - uaktualniane. Podmioty przetwarzające są zobowiązane do podjęcia odpowiednich środków, aby zapewnić poprawność i kompleksowość danych;
- **zasada minimalizacji danych -** zgodnie z tą zasadą, dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne w stosunku do celów, w których są przetwarzane. Podmiot przetwarzający nie powinien gromadzić ani przechowywać danych w większym zakresie, niż jest to konieczne;
- **zasada ograniczenia przechowywania danych -** dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osób jedynie przez okres niezbędny do realizacji celów, w których są przetwarzane. Po upływie tego okresu dane powinny być usuwane lub anonimizowane.

- **zasada integralności i poufności -** podmioty przetwarzające mają obowiązek zapewnić odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed nieuprawnionym lub nielegalnym przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem danych

Konkretyzacja powyższych zasad została uwzględniona w art. 32 RODO, który stanowi podstawowy punkt odniesienia w zakresie wdrażania procedur ochrony danych. Zgodnie z tym przepisem, administratorzy danych oraz podmioty przetwarzające muszą wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni poziom bezpieczeństwa danych osobowych. Proces wdrażania procedur ochrony danych rozpoczyna się od oceny ryzyka, zgodnie z wymogami art. 32 ust. 1 lit. a RODO. Administratorzy danych powinni przeprowadzić szczegółową ocenę ryzyka związanego z przetwarzaniem danych osobowych i na tej podstawie określić niezbędne środki ochrony (Mostowik 2022, s. 123-126).

Warto również zauważyć, że art. 32 RODO szczegółowo określa, jakie środki techniczne i organizacyjne należy zastosować w celu zapewnienia bezpieczeństwa danych osobowych. Obejmuje to m.in. szyfrowanie danych, regularne testowanie, weryfikację oraz monitorowanie, a także przywracanie dostępności danych po incydentach. Powyższy przepis ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych oraz ochronę przed potencjalnymi zagrożeniami związanymi z ich przetwarzaniem. Przestrzeganie tych wymogów jest kluczowe dla zgodności z przepisami prawa oraz dla zachowania zaufania klientów i partnerów biznesowych (Sakowska-Baryła 2020, s. 67-69).

Powyższe stanowisko zostało przykładowo potwierdzone w Wyroku Wojewódzkiego Sądu Administracyjnego (dalej: „**WSA**") w Warszawie z dnia 1 lipca 2022 r. sygn. II SA/Wa 3211/21, w którym WSA, stwierdził, że *„(…) Stosownie zaś do treści art. 32 ust. 1 RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. W myśl art. 32 ust. 2 RODO, administrator oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób*

przetwarzanych. Przepis art. 32 RODO stanowi konkretyzację, wskazanej w art. 5 ust. 1 lit. f) RODO, zasady integralności i poufności, zgodnie z którą dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.(…) Należy zwrócić uwagę, że RODO wprowadziło podejście, w którym zarządzanie ryzykiem jest fundamentem działań związanych z ochroną danych osobowych i ma charakter ciągłego procesu. Podmioty przetwarzające dane osobowe zobligowane są do zapewnienia wdrażania organizacyjnych i technicznych środków bezpieczeństwa, jak również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Oznacza to, że koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych".

Wdrażanie skutecznych procedur ochrony danych osobowych jest niezbędnym krokiem dla przedsiębiorstw w kontekście zapewnienia zgodności z RODO oraz ochrony danych osobowych ich klientów i pracowników. Proces ten obejmuje ocenę ryzyka, wdrożenie odpowiednich środków technicznych i organizacyjnych, szkolenia pracowników oraz regularne audyty i monitorowanie działań. Przestrzeganie tych kroków jest kluczowe dla zapewnienia skutecznej ochrony danych osobowych i zgodności z przepisami prawa (Litwiński 2009, s. 45-50).

ROLA OSÓB UPOWAŻNIONYCH W PRZEDSIĘBIORSTWIE W ZAKRESIE REALIZACJI PROCEDUR OCHRONY DANYCH OSOBOWYCH

Osoby upoważnione odgrywają kluczową rolę w realizacji procedur ochrony danych osobowych. Ich zadaniem jest nie tylko przetwarzanie danych zgodnie z obowiązującymi przepisami, ale także monitorowanie działań w zakresie ochrony danych oraz reagowanie na ewentualne naruszenia (Sakowska-Baryła 2020, s. 67-69).

Artykuł 29 RODO nakłada na administratora danych obowiązek wyznaczenia osób odpowiedzialnych za nadzór nad przestrzeganiem RODO w przedsiębiorstwie. Osoby te, zwane upoważnionymi, mają za zadanie nadzorowanie wdrażania i przestrzegania procedur ochrony danych osobowych oraz zapewnienie, że

działania przedsiębiorstwa są zgodne z przepisami RODO. Główną rolą osób upoważnionych jest zapewnienie, że działania przedsiębiorstwa w zakresie ochrony danych osobowych są zgodne z przepisami prawa oraz z zasadami RODO. To właśnie im powierza się nadzór nad wdrażaniem i przestrzeganiem procedur ochrony danych oraz podejmowanie działań w celu zapobiegania ewentualnym incydentom związanym z naruszeniem ochrony danych (Grzelak 2019, s. 154-158).

Osoby upoważnione mają również istotne zadania związane z zarządzaniem ryzykiem. Ich rola obejmuje udział w procesie oceny ryzyka związanego z przetwarzaniem danych osobowych, co pozwala na identyfikację potencjalnych zagrożeń oraz określenie skutecznych środków zapobiegawczych (Fajgielski 2019, s. 92-95).

Dodatkowo, osoby upoważnione mają obowiązek monitorowania przestrzegania przepisów o ochronie danych w przedsiębiorstwie oraz zapewnienie odpowiedniego przeszkolenia pracowników w zakresie zasad ochrony danych. Są one również punktem kontaktowym dla organów nadzorczych oraz osób, których dane dotyczą, w sprawach związanych z przetwarzaniem danych osobowych.

Drugim istotnym aspektem roli osób upoważnionych jest reprezentowanie przedsiębiorstwa w kontaktach z organami nadzorczymi oraz osobami, których dane dotyczą. Osoby upoważnione pełnią funkcję punktu kontaktowego dla organów nadzorczych, takich jak Prezes Urzędu Ochrony Danych Osobowych oraz dla osób, których dane są przetwarzane. W związku z tym, osoby te są odpowiedzialne za komunikację z organami nadzorczymi w przypadku ewentualnych kontroli oraz za udzielanie odpowiedzi na żądania i skargi osób, których dane są przetwarzane (Litwiński 2009, s. 30-35).

Kolejnym istotnym aspektem roli osób upoważnionych jest szkolenie pracowników w zakresie przestrzegania zasad ochrony danych oraz monitorowanie wykonywania tych zasad w praktyce. Osoby upoważnione są odpowiedzialne za edukację pracowników w zakresie przetwarzania danych osobowych, zapewnienie świadomości zasad ochrony danych oraz monitorowanie czy pracownicy przestrzegają tych zasad w codziennej praktyce działania przedsiębiorstwa (Fajgielski 2019, s.78-80).

Przykładowo w Decyzji Prezesa Urzędu Ochrony Danych Osobowych z dnia 16 kwietnia 2019 r. ZSPU.440.131.2019 odwołano się do sytuacji przekazania danych na rzecz profesjonalnego pełnomocnika: *„(…) W sytuacji przekazania danych na rzecz profesjonalnego pełnomocnika reprezentującego interesy mocodawcy mamy do czynienia z przetwarzaniem danych przez pełnomocnika*

działającego w imieniu administratora danych osobowych, w granicach przyznanego mu umocowania i nie we własnych celach, lecz dla realizacji celów administratora danych. Działanie radcy prawnego znajduje również swe oparcie w art. 29 RODO, zgodnie z którym podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Zauważyć przy tym należy, iż zgodnie z art. 3 ust. 1 ustawy z dnia 6 lipca 1982 r. o radcach prawnych (Dz.U. z 2018 r. poz. 2115 ze zm.) radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej".

W powyższym przypadku mamy do czynienia z przetwarzaniem danych przez pełnomocnika działającego w imieniu administratora danych osobowych, w granicach przyznanego mu umocowania i nie we własnych celach, lecz dla realizacji celów administratora danych. Działanie radcy prawnego / adwokata znajduje również swe oparcie w art. 29 RODO, zgodnie z którym podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego (Mostowik 2022, s. 89-92).

Podsumowując, role osób upoważnionych w przedsiębiorstwie w zakresie realizacji procedur ochrony danych osobowych są kluczowe dla skutecznego zarządzania ochroną danych oraz zapewnienia zgodności z przepisami prawa. Osoby te mają istotny wpływ na kształtowanie kultury ochrony danych w przedsiębiorstwie, dbając o przestrzeganie zasad ochrony danych, reprezentując przedsiębiorstwo w kontaktach z organami nadzorczymi oraz dbając o świadomość pracowników w zakresie przetwarzania danych osobowych. Dlatego też, właściwe wyznaczenie, wsparcie i zaufanie dla osób upoważnionych stanowią kluczowe elementy skutecznej polityki ochrony danych w przedsiębiorstwie (Wyka i Mielczarek 2019, s. 134-137).

PODSUMOWANIE

Reasumując, rola osób upoważnionych w przedsiębiorstwie w zakresie realizacji procedur ochrony danych osobowych *de lege lata* stanowi istotny element skutecznej polityki ochrony danych. Ich funkcje obejmują nadzór nad wdrożeniem i przestrzeganiem procedur, zarządzanie ryzykiem, szkolenie pracowników oraz reprezentowanie przedsiębiorstwa w kontaktach z organami nadzorczymi

i osobami, których dane dotyczą. Ich rola nie ogranicza się jedynie do nadzoru, ale obejmuje także aktywne działania mające na celu zapewnienie zgodności z przepisami prawa oraz ochronę danych osobowych.

Przez podejmowane działania osoby upoważnione przyczyniają się do kształtowania kultury ochrony danych w przedsiębiorstwie oraz zapewnienia świadomości pracowników w zakresie przetwarzania danych osobowych. Ich zaangażowanie w monitorowanie przestrzegania przepisów o ochronie danych, udzielanie wsparcia w kontaktach z organami nadzorczymi oraz zapewnienie przeszkolenia pracowników *de lege lata* jest niezbędne dla skutecznej ochrony danych osobowych. Wdrożenie i przestrzeganie procedur ochrony danych wymaga zrozumienia roli osób upoważnionych oraz zapewnienia im odpowiedniego wsparcia i zaufania ze strony kierownictwa przedsiębiorstwa.

Wydane orzeczenia, takie jak przykładowo sprawa C-25/17 TSUE, potwierdzają istotną rolę osób upoważnionych oraz kluczową konieczność przestrzegania przepisów RODO w kontekście ochrony danych osobowych. Decyzje te stanowią wytyczne dla przedsiębiorstw, wskazując na konieczność zachowania równowagi między interesami pracodawcy a prawami pracowników oraz konieczność przestrzegania zasad ochrony danych osobowych w miejscu pracy.

Wdrożenie skutecznych procedur ochrony danych osobowych oraz zapewnienie odpowiedniego szkolenia dla osób upoważnionych może być wyzwaniem szczególnie dla małych i średnich przedsiębiorstw, które często dysponują ograniczonymi zasobami. W przedstawionym zakresie niezbędne byłoby *de lege ferenda* wprowadzenie specjalnych programów wsparcia finansowego lub szkoleniowego dla tych przedsiębiorstw mogłoby ułatwić im przestrzeganie przepisów dotyczących ochrony danych.

Wdrożenie powyższych sugestii *de lege ferenda* mogłoby przyczynić się do dalszego usprawnienia procesu ochrony danych osobowych w przedsiębiorstwach oraz lepszego przestrzegania przepisów RODO, co przyczyniłoby się do większej skuteczności ochrony danych osobowych.

Podsumowując, rola osób upoważnionych w przedsiębiorstwie w zakresie realizacji procedur ochrony danych osobowych jest kluczowa dla zapewnienia zgodności z przepisami prawa oraz skutecznej ochrony danych osobowych. Ich działania mają istotny wpływ na kulturę ochrony danych w przedsiębiorstwie i stanowią fundament skutecznej polityki ochrony danych. Dlatego też, należy im zapewnić odpowiednie wsparcie oraz zaufanie, aby mogły efektywnie pełnić swoje funkcje i przyczyniać się do ochrony danych osobowych w przedsiębiorstwie.

BIBLIOGRAFIA

Akty prawne:

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2023, poz. 775 ze zm.).

Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2023 r., poz. 1634 ze zm.).

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.

rzecznictwo:

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 10 lipca 2018 r., C-25/17, LEX nr 2600148.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 lipca 2022 r. sygn. II SA/Wa 3211/21, LEX nr 3413537.

Decyzje:

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 16 kwietnia 2019 r. ZSPU.440.131.2019, LEX nr 3285044.

Literatura

Fajgielski P.
2019 *Prawo ochrony danych osobowych. Zarys wykładu,* Warszawa.

Grzelak A.
2019 *Ochrona danych osobowych w sądach i prokuraturze*, Warszawa.

Mostowik M.
2022 *Ochrona danych osobowych w internecie rzeczy w prawie UE,* Warszawa.

Litwiński P.
2009 *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa.

Sagan-Jeżowska A.
2018 *Ochrona danych osobowych w małej i średniej firmie. Kontrola poprawności wdrożenia RODO. Metodyka, procedury, wzory*, Warszawa.

Sagan-Jeżowska A.
2018 *Klauzule RODO, Wzory klauzul z praktycznym komentarzem*, Warszawa.

Sakowska-Baryła M.
2020 *Ochrona danych osobowych w warunkach pracy zdalnej*, Warszawa.

Wyka T., Mielczarek M.A.
2019 *Administrator i inspektor ochrony danych osobowych*, [w:] red. Wyka T., Mielczarek M.A., Warszawa.

Patrycja Rzepecka

Uniwersytet Marii Curie-Skłodowskiej

Studentka

OUTSOURCING DANYCH OSOBOWYCH – SZANSA CZY ZAGROŻENIE DLA PRZEDSIĘBIORCY?

WPROWADZENIE

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. L. z 2016 r. Nr 119, str. 1 z późn. zm.), w dalszej części nazywane jako RODO, weszło w życie 25 maja 2018 roku. Od tamtej pory minęło już prawie sześć lat, co pozwala na dokonanie pewnego przeglądu dotychczasowego stosowania i podsumowania tego, co udało się wypracować przez ten okres.

W kontekście *outsourcingu* przede wszystkim można wyróżnić podmioty, które mogą stanowić podmioty zewnętrzne, a administrator powierza im odpowiednie dane, czyli podmiot przetwarzający (tzw. procesor), subprocesor, a także podmiot o szczególnych i kompletnie odrębnym charakterze - inspektor danych osobowych stanowiący swoistego odbiorcę danych osobowych. Jednocześnie należy wskazać, że wejście w życie RODO pozwoliło na wyróżnienie podstawowych zasad dotyczących przetwarzania danych osobowych, do których odnosić się będą wszelkie uregulowania. Konkretnie chodzi o art. 5 ust. 1 rozporządzenia, które bezpośrednio na nie wskazują - zasada legalności, przejrzystości, celowości, minimalizacji danych, poprawności, integralności i poufności, rozliczalności. Stanowią one dyrektywy interpretacyjne, które pozwalają na odpowiednią

interpretację przepisów RODO, a co za tym idzie - często mają one wpływ na postrzeganie obowiązków administratora, a także innych podmiotów, o których będzie mowa w niniejszym artykule. Pełnią rolę regulacyjną, ponieważ posiadają charakter normatywny, ale stanowią również dyrektywy interpretacyjne i pewnych wytycznych legislacyjnych. Należy jednak wskazać, że możliwe jest ich ograniczenia na gruncie art. 23 RODO, co wskazuje na fakt, że nie mają one charakteru absolutnego.

Przejawiają się one w szczególności w relacjach między administratorem, czyli głównym podmiotem, który przetwarza dane, a pozostałymi podmiotami mającymi dokonywać na nich operacji, czy też przeprowadzać ich kontrolę. Jako, że obecnie większość przedsiębiorców korzysta z usług zewnętrznych przedsiębiorstw, to stanowią one pewne wyznaczniki odnoszące się do relacji między wspomnianymi podmiotami - a przede wszystkim oddziałują one na ich obowiązki, co będzie można zaobserwować.

OUTSOURCING DANYCH OSOBOWYCH: DEFINICJE I KLUCZOWE POJĘCIA

Oceniając zjawisko *outsourcingu* danych osobowych w pierwszej kolejności poznać definicje, będące w tym przypadku kluczowe. Sam *outsourcing* z języka angielskiego znaczy zlecanie usług firmie zewnętrznej, co najlepiej obrazuje z czym mamy do czynienia, gdyż wskazuje na istnienie podmiotu trzeciego - niezwiązanego z przedsiębiorcą. Jednocześnie, same rozważania na temat outsourcingu w doktrynie prawniczej zwykle dotyczą prawa bankowego, co nie oznacza, że nie można mówić o nim w innych kontekstach. Jak wskazuje Sąd Najwyższy "Outsourcing można zdefiniować jako przedsięwzięcie polegające na wydzieleniu ze struktury organizacyjnej przedsiębiorstwa macierzystego realizowanych przez nie funkcji i przekazanie do realizacji innym podmiotom gospodarczym"[1]. Podobne definicje przewijają się już na przestrzeni lat, a A. Krasuski już w 2010 r. trafnie interpretował samo zjawisko - "Z przytoczonych powyżej różnych definicji outsourcingu wynika, że jest to proces składający się na szereg czynności, których celem jest delegacja obowiązków lub uprawnień jednego przedsiębiorcy drugiemu przedsiębiorcy, za wynagrodzeniem, w sposób sformalizowany, tj. na podstawie zawartej umowy" (Krasuski 2010, roz. 1 pkt 1).

[1] Postanowienie SN z 13.04.2021 r., I USK 6/21, LEX nr 3159922. - samo postanowienie dotyczy outsourcingu pracowniczego, co jednak nie oznacza, że nie można zastosować go do innych dziedzin, gdyż Sąd Najwyższy przytacza w nim ogólną definicję outsourcingu.

Wobec powyższego, z pewnością możemy stwierdzić, że samo pojęcie outsourcingu obejmuje zlecanie zewnętrznemu podmiotowi wykonywania określonych funkcji realizowanych przez przedsiębiorcę na podstawie określonej umowy i za odpowiednim wynagrodzeniem.

Przy określaniu obowiązków w zakresie dokonywania przetwarzania danych oraz ich udostępniania podmiotom trzecim należy wskazać również na samo pojęcie danych osobowych. Ich definicja jest określona w art. 4 pkt 1 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/WE, czyli tzw. ogólne rozporządzenie o ochronie danych (dalej określane jako: RODO). Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (,,osobie, której dane dotyczą''); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Jak widać, zakres obejmujący to pojęcie jest wyjątkowo szeroki, a co za tym idzie - konieczne jest zachowanie szczególnych obowiązków ze strony podmiotów będących w posiadaniu tego typu danych. Nie sposób nie wspomnieć również czym jest przetwarzanie, które tak naprawdę jest kluczowym pojęciem, gdy mowa o stosowaniu outsourcingu danych osobowych. Definicja została też wskazana w rozporządzeniu RODO jako operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[2]. Sama konstrukcja przepisu wskazuje na wyliczenie poszczególnych działań, jakie można z danych dokonywać, a zatem nie ma charakteru zamkniętego.

Jednocześnie, na gruncie RODO pojawiają się różne określenia podmiotów - administrator, podmiot przetwarzający, subprocesor czy też inspektor ochrony danych osobowych. Należy wskazać, że administrator to osoba fizyczna

[2] Art. 4 pkt 2 RODO.

lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania). Można zatem zauważyć, że administrator stanowi podstawową jednostkę, która dysponuje danymi - ustala sposoby ich przetwarzania, określa cele dokonywanych z nimi czynności, a także na nim ciążą obowiązki dotyczące ich przechowywania, pozyskiwania, dokonywania ogólnie rozumianego przetwarzania.

Jednym z najważniejszych obowiązków administratora jest wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem oraz aby móc to wykazać. Jednocześnie, środki powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Oprócz tego, jeśli administrator sam uzna, że proporcjonalnym byłoby wprowadzenie polityki ochrony danych, to może to zrobić, a samo rozporządzenie nie określa minimalnego zakresu takich dokumentów. Administrator może również stosować zatwierdzone kodeksy postępowania lub zatwierdzony mechanizm certyfikacji, co ma służyć udowodnieniu, że spełnia on ciążące na nim obowiązki.

Jednakże administrator nie musi samodzielnie nimi zarządzać, na co wskazują również motywy zawarte w RODO, które niejednokrotnie odwołują się do pojęcia podmiotu przetwarzającego, subprocesora, czy też inspektora danych osobowych. Jak zostało wcześniej wskazane najważniejszymi podmiotami, które mogą stanowią podmioty zewnętrzne, a administrator powierza im odpowiednie dane są podmiot przetwarzający (tzw. procesor), subprocesor, a także podmiot o szczególnych i kompletnie odrębnym charakterze - inspektor danych osobowych (mogący być określany tzw. odbiorcą). W celu dokładnego omówienia zależności oraz podejmowania się *outsourcingu*, w pierwszej kolejności należy dokonać analizy poszczególnych relacji między administratorem, a każdym z podmiotów.

ADMINISTRATOR A PODMIOT PRZETWARZAJĄCY

Podmiot przetwarzający zdefiniowany został jako osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora[3]. Co znaczące, podmiot przetwarzający jest niezależny

[3] Art. 4 pkt. 8 RODO.

w stosunku do administratora danych, a zatem dochodzi tu do zjawiska *outsourcingu*. Oznacza to, że następuje powierzenie dokonywania niektórych operacji przetwarzania danych osobowych przez administratora danych od zewnętrznej organizacji. Jednakże, następuje w przytoczonej definicji pewne zastrzeżenie w postaci dokonywania przetwarzania w imieniu administratora. Tym samym należy wskazać, że to właśnie administrator ustala cele i sposoby przetwarzania danych, więc podmiot przetwarzający może tego dokonywać jedynie w celach przez niego wskazanych. W razie realizacji własnych celów przetwarzania danych przez podmiot przetwarzający dojdzie do naruszenia zasad ochrony i przetwarzania danych osobowych, a co za tym idzie możliwa jest odpowiedzialność odszkodowawcza. Przykładem podmiotu przetwarzającego jest chociażby biuro księgowe, które przetwarza dane osobowe pracowników, czy też kontrahentów na zlecenie oraz w imieniu danego podmiotu tj. administratora. W tym przypadku konkretnym celem przetwarzania są niezbędne czynności związane z prowadzeniem rachunkowości oraz wypłacaniem wynagrodzeń.

W kwestii podmiotu przetwarzającego należy wskazać na istniejące uregulowania zawarte w RODO, gdyż samo rozporządzenie szeroko się do niego odnosi. W motywie 81 rozporządzenia można odnaleźć szczególne zamiary prawodawcy unijnego, które można uznać za uzasadnione. Na gruncie wspomnianego motywu można wywnioskować, że w przypadku, gdy przedsiębiorca (będący administratorem) decyduje się na wybór zewnętrznego podmiotu (podmiotu przetwarzającego) ma on obowiązek sprawdzić i zweryfikować, czy dany podmiot zapewnia wystarczające gwarancje - w szczególności, jeśli chodzi o wiedzę fachową, wiarygodność i zasoby, kwestie wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Jednocześnie, analogicznie jak w przypadku wskazania obowiązków administratora, również w przypadku podmiotu przetwarzającego stosowanie przez podmiot zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Jednocześnie w motywach niejednokrotnie używane jest sformułowanie "administrator i podmiot przetwarzający" niejako je rozdzielając i traktując ich osobno. Można z tego powodu wnioskować, że podmiot przetwarzający (podobnie jak administrator) musi samodzielnie aktualizować swojego polityki ochrony danych, realizować i ulepszać środki techniczne pozwalające na zapewnienie danym osobowym odpowiedniego poziomu bezpieczeństwa, a zatem obejmuje go obowiązek nałożony przez art. 32 RODO, gdzie określono odpowiednie zabezpieczenia do ryzyka

związanego z dokonywaniem przetwarzania. Niejednokrotnie kwestia odpowiedniego dobrania podmiotu będącego później podmiotem przetwarzającym przewija się również w decyzjach Prezesa Urzędu Ochrony Danych Osobowych. Jak wskazuje Prezes UODO - "Decyzja komu administrator miałby powierzyć przetwarzanie danych osobowych nie może być podejmowana bezpodstawnie. Konsekwencje podjęcia pochopnej decyzji, braku odpowiedniej formy czy treści umowy powierzenia, lub zaniedbania obowiązku ciągłej weryfikacji przez administratora gwarancji, o których mowa w art. 28 ust. 1 rozporządzenia 2016/679, mogą bowiem dotknąć bezpośrednio osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu. Tymczasem, stosując przepisy rozporządzenia 2016/679, należy mieć na uwadze, że celem tego rozporządzenia (wyrażonym w art. 1 ust. 2) jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych oraz że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych (zdanie pierwsze motywu 1 preambuły). W przypadku jakichkolwiek wątpliwości np. co do wykonania obowiązków przez administratorów - nie tylko w sytuacji, gdy doszło do naruszenia ochrony danych osobowych, ale też przy podejmowaniu decyzji dotyczących powierzenia przetwarzania danych osobowych innym podmiotom - należy w pierwszej kolejności brać pod uwagę te wartości. Ochronie tych praw służą konsekwentnie wymagania stawiane w art. 28 ust. 1, 3 i 9 rozporządzenia 2016/679, stąd ich naruszenie musi wiązać się z odpowiednią do konkretnych okoliczności reakcją organu nadzorczego"[4].

Szczegółowe uregulowania można odnaleźć w art. 28 RODO, gdzie wskazano już m.in. minimalny zakres obowiązków podmiotu przetwarzającego, który powinien zostać określony w umowie lub innym instrumencie prawnym. Wobec tego należy wskazać, że zalicza się do tego:

1. przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie administratora, w tym przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny - mogące stanowić fragment umowy powierzenia lub odrębnego dokumentu;

[4] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 7 września 2022 r., znak: DKN.5131.29.2022

2. zapewnienie, aby osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy poprzez np. odebranie stosownych oświadczeń oraz poinformowanie takich osób o obowiązkach i odpowiedzialności za naruszenie tajemnicy, jednocześnie należy wskazywać, iż dotyczy to nie tylko powierzonych do przetwarzaniach danych, ale też szczegóły stosunku łączącego strony, co wynika z wytycznych Komisji Europejskiej;
3. podejmowanie wszelkich środków dotyczące zapewnienia bezpieczeństwa przetwarzania poprzez np. przekazania procesorowi opisu operacji przetwarzania i celów w zakresie bezpieczeństwa
4. przestrzeganie warunków korzystania z usług tzw. subprocesora (o czym dalej);
5. w miarę możliwości pomoc administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
6. w miarę możliwości pomoc administratorowi wywiązać się z obowiązków dotyczących bezpieczeństwa przetwarzania danych osobowych, zgłaszania naruszeń organowi nadzorczemu, zawiadamianiu osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, dokonywanie oceny skutków dla ochrony danych, dokonywanie konsultacji z organem nadzorczym w przypadku przetwarzania o wysokim ryzyku;
7. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora dokonuje usunięcia lub zwrócenia mu wszelkich danych osobowych oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
8. udostępnianie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków wynikających z RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzenie audytów (w tym inspekcji) i przystąpienia się do nich.

Jak wskazuje dr Litwiński (2021, art. 28, Nb 9) w praktyce takie sprawdzenie, czy dany podmiot spełnia odpowiednie wymagania następuje w drodze kwestionariusza pytań, które dotyczą kwestii stosowania odpowiednich środków

technicznych i organizacyjnych zapewniających zgodność działań podmiotu przetwarzającego z przepisami RODO. Należy również zaznaczyć, że przy zawieraniu umowy powierzenia z podmiotem przetwarzającym nie ma obowiązku prowadzenia audytu stosowanych przez procesora środków, o czym również orzekł PUODO w uzasadnieniu decyzji z 17 grudnia 2020 r.[5] Wobec tego, już na etapie przed zawarciem umowy administrator ma obowiązek dowiedzieć się, jakich zabezpieczeń używa potencjalny kontrahent np. jak zabezpieczona jest dokumentacja, istnienie polityki ochrony danych, ustalenie osób odpowiedzialnych za bezpieczeństwo, czy też w ramach powierzenia dochodzić będzie do przekazywania danych poza Europejski Obszar Gospodarczy (EOG), a jeżeli tak, to w oparciu o jakie gwarancje zabezpieczeń. Naruszenie tego obowiązku może skutkować nałożeniem kary przez PUODO, na co również wskazują wydane decyzje - "Samo podpisanie umowy powierzenia przetwarzania danych osobowych bez dokonania odpowiedniej oceny podmiotu przetwarzającego nie może być uznane jako realizacja obowiązku przeprowadzenia postępowania weryfikującego podmiot przetwarzający pod kątem spełnienia przez niego wymogów rozporządzenia 2016/679. Z obowiązku przeprowadzenia takiej oceny nie zwalnia również fakt wieloletniej współpracy i korzystania z usług danego podmiotu przetwarzającego przed dniem 25 maja 2018 r., tj. przed rozpoczęciem stosowania rozporządzenia 2016/679. W przedmiotowej sprawie Administrator takiej weryfikacji nie przeprowadził, poprzestał jedynie na pozytywnej ocenie podmiotu przetwarzającego, będącej efektem dotychczasowej współpracy, podczas której, jak wyjaśnił, nie dochodziło do incydentów bezpieczeństwa. Konsekwencją braku dokonania tej oceny jest jednak naruszenie przez Fortum wymogu określonego w art. 28 ust. 1 rozporządzenia 2016/679"[6].

Po pierwsze, możliwe są dwie podstawy dla powierzenia danych osobowych - tj. umowa lub inny instrument prawny, który podlega prawu Unii lub prawu państwa członkowskiego i który wiąże podmiot przetwarzający i administratora (co w szczególności dotyczy organów i podmiotów ze strefy prawa publicznego - np. porozumienie administracyjne, ogólne warunki ubezpieczenia etc.)

Jeśli chodzi o umowę powierzenia, w doktrynie najczęściej wskazuje się na jej postać umowy o świadczenie usług, do której stosuje się przepisy

[5] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 22 kwietnia 2021 r., DKN.5130.3114.2020

[6] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 19 stycznia 2022 r., znak DKN.5130.2215.2020

kodeksu cywilnego o zleceniu (Litwiński 2021, art. 28, Nb 4). Jak wskazuje również motyw 81 RODO Przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Administrator i podmiot przetwarzający mogą postanowić skorzystać z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez Komisję albo które zostały przyjęte przez organ nadzorczy zgodnie z mechanizmem spójności, a następnie przyjęte przez Komisję. Na gruncie takiego stanowiska prawodawcy unijnego, można wskazać podstawowe elementy umowy powierzenia które muszą się znaleźć, aby była ona prawidłowa i zgodna z rozporządzeniem, a są nimi:

1. przedmiot i czas trwania przetwarzania;
2. charakter i cel przetwarzania;
3. rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;
4. obowiązki i prawa administratora.

Ponadto, umowa może również zawierać kwestie dotyczące przeprowadzania audytu, inspekcji, czy też przekazywania danych do państwa spoza obszaru EOG.

W przypadku formy wskazanej umowy, może być ona zawarta w postaci załącznika do umowy o świadczenie usług, czy też być integralną częścią umowy. Jest to kwestia nieuregulowana przez rozporządzenie, a co za tym idzie - stanowi to wolę stron. Jednakże, umowa powinna być zawarta w formie pisemnej, w tym możliwa jest droga elektroniczna. Główną rolą wskazanej umowy jest zapewnienie pewności w warunkach konkretnego stosunku prawnego przetwarzania danych, że operacje wykonywane na danych osobowych są rzeczywiście wykonywane przez podmiot do tego uprawniony, rzeczywiście w zakresie objętym powierzeniem i rzeczywiście z poszanowaniem zasad przetwarzania danych ustalonych w umowie (Litwiński 2021, art. 28, Nb 5). W przypadku formy ustnej jest to ryzykowne, gdyż z punktu widzenia prawa cywilnego pozostaje ważna, ale może rodzić odpowiedzialność na gruncie prawa administracyjnego, czy też niemożliwości późniejszego wykazania poszczególnych obowiązków stron umowy, bądź innych kwestii, które powinny być w umowie o powierzeniu zawarte.

W umowie o powierzeniu przetwarzania może również zawierać możliwość powierzenia przetwarzania tzw. subprocesorowi, czyli innego podmiotu przetwarzającego w zakresie wykonywania czynności przetwarzania powierzonych pierwotnie przez administratora podmiotowi. Jednakże, nie zostało to uregulowane w RODO, ale samo pojęcie subprocesora pojawia się w Wytycznych 07/2020 wydanych przez Europejskiego Rzecznika Ochrony Danych. W takiej sytuacji przewidziane są warunki dopuszczalności podpowierzenia, czyli uprzednia szczegółowa pisemna zgoda administratora i uprzednia ogólna zgoda administratora. Jednak, należy wyraźnie zaznaczyć, że podmiot przetwarzający musi zostać wcześniej poinformowany o zamierzonym dokonaniu podpowierzenia. Pozwala to na wyrażenie sprzeciwu przez administratora - w zakresie ogólnego zawarcia umowy podpowierzenia, czy też zgody na konkretnego subprocesora. Taka zgoda również powinna zostać udokumentowana dla ewentualnych celów dowodowych. Jednocześnie, należy wskazać, że odpowiedzialność za dobór subprocesora ciąży na procesorze względem administratora.

Wobec powyższych uregulowań, należy wskazać jak wygląda odpowiedzialność podmiotu przetwarzającego na zlecenie. Podstawową kwestią jest fakt, iż odpowiedzialność podmiotu przetwarzającego nie jest ograniczona do odpowiedzialności cywilnej z tytułu niewykonania lub nienależytego wykonania umowy (w przypadku umów cywilnoprawnych), lecz dotyczy również odpowiedzialności za niezgodne z prawem przetwarzanie danych (obszar prawa administracyjnego), a także odpowiedzialności karnej na gruncie ustawy z 10.5.2018 r. o ochronie danych osobowych (Pyka 2020, s. 14). Również motyw 146 RODO wskazuje na szerokie rozumienie pojęcia "szkoda", które według polskich realiów może obejmować zarówno szkodę majątkową, jak i niemajątkową. W zakresie odszkodowania można stwierdzić, że osoba poszkodowana będzie mogła domagać się zarówno *damnum emergens,* jak i *lucrum cessans*. Zatem, w przypadku wielości podmiotów tj. występowania administratora i podmiotu przetwarzającego, osoba poszkodowana będzie mogła dochodzić odszkodowania wobec administratora oraz podmiotu przetwarzającego, które będą odpowiadać solidarnie w ramach odpowiedzialności deliktowej. Z kolei odpowiedzialność deliktowa wynika z art. 82 ust. 1 RODO, które nie odnosi się do stosunku między administratorem lub podmiotem przetwarzającym, a osobą poszkodowaną, z której miałaby wynikać odpowiedzialność kontraktowa.

W tym miejscu należy wyraźnie zaznaczyć, że najszerszy zakres odpowiedzialności ciąży na administratorze. Dlatego, to przede wszystkim on odpowiada za wybór odpowiedniego podmiotu, a także przeprowadzanie jego weryfikacji

w trakcie trwania umowy. Z tego względu, podmiot przetwarzający może ponosić odpowiedzialność wyłącznie w sytuacji, gdy nie dopełnił obowiązków nałożonych bezpośrednio na niego w przepisach RODO lub działał poza lub wbrew zgodnym z prawem poleceniom administratora ewentualnie kiedy działał w sferze własnej dyskrecji, poza zakresem ustaleń z administratorem. Jednakże, istnieją przesłanki egzoneracyjne tj. wyłączające okoliczności naprawienia zaistniałej szkody przez administratora lub podmiot przetwarzający. Należy do nich chociażby brak zawinienia w zdarzeniu, które stało się przyczyną powstania szkody, co obejmuje zarówno winę umyślną, jak i nieumyślną. Przejawem takiej okoliczności będzie również wykazanie przez administratora, czyli przedsiębiorcę, dochowanie należytej staranności w wyborze i uregulowaniach umownych z podmiotem profesjonalnym, któremu administrator zlecił wykonanie określonych czynności. Jeśli chodzi o podmiot przetwarzający, to zgodnie z art. 82 ust. 2 RODO, nie powstanie, gdy:

1. przepisy RODO nie nakładały na podmiot przetwarzający bezpośrednio obowiązków, których niewykonanie lub nienależyte wykonanie spowodowało szkodę
2. podmiot przetwarzający działał zgodnie z (zgodnymi z prawem) instrukcjami administratora;
3. podmiot przetwarzający działał poza lub wbrew instrukcjom administratora, ale instrukcje te były niezgodne z prawem.

Z tego względu należy zaznaczyć, że szczególne znaczenie mają instrukcje (czy też polecenia) wydawane przez administratora, a także określenie jego szczegółowych obowiązków. W tym miejscu należy wspomnieć, iż możliwe jest dochodzenie roszczeń regresowych, które wynikałyby z zobowiązania solidarnego powstałego w wyniku odpowiedzialności deliktowej. Jednakże ograniczają się one do części, za którą dany podmiot ponosi odpowiedzialność, co wynika bezpośrednio z art. 82 ust. 5 RODO.

Ponadto, możliwe jest również poniesienie odpowiedzialności administracyjnej w wyniku decyzji Prezesa Urzędu Ochrony Danych Osobowych. Administracyjne kary pieniężne są nakładane w zależności od okoliczności każdego indywidualnego przypadku i możliwe jest również złagodzenie tej odpowiedzialności np. poprzez dążenie do naprawienia szkody. Taka okoliczność została wskazana przez Naczelny Sąd Administracyjny, który uznał, że "Posłużenie się podmiotem profesjonalnie trudniącym się doradztwem w zakresie informatyki w celu usunięcia skutków naruszenia nie zwalnia administratora z odpowiedzialności

administracyjnej, aczkolwiek ma wpływ na zakres jego odpowiedzialności”[7]. Również sam motyw 150 preambuły wskazuje, iż przy nakładaniu administracyjnych kar pieniężnych organ nadzorczy powinien określać indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, z należytym uwzględnieniem w szczególności charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub w celu zminimalizowania tych konsekwencji.

ADMINISTRATOR A OSOBA DZIAŁAJĄCA Z UPOWAŻNIENIA ADMINISTRATORA LUB PODMIOTU PRZETWARZAJĄCEGO

Zgodnie z art. 29 RODO podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Jednak, pomimo użycia sformułowania “upoważnienie” można uznać, że należy tę kwestię rozpatrywać w kategoriach funkcjonalnych tj. nie na podstawie udzielania formalnego upoważnienia, a kontroli ze strony odpowiedniego podmiotu. W tym przypadku następuje wyraźna różnica w stosunku do podmiotu przetwarzającego - konkretnie chodzi o dostęp do danych osobowych. Przykładem tego typu upoważnienia może być przekazanie danych osobowych profesjonalnemu pełnomocnikowi reprezentującego interesy mocodawcy w granicach udzielonego umocowania i dla realizacji celów administratora danych[8].

Jednocześnie, należy wskazać, że osoba upoważniona może zostać pociągnięta do odpowiedzialności nie tylko cywilnej, ale również karnej. W przypadku art. 107 ustawy o ochronie danych osobowych - “Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch”. Wobec czego, istnieją dwie przesłanki odpowiedzialności karnej - w przypadku, gdy niedopuszczalne jest przetwarzanie danych lub istnieje brak uprawnienia do przetwarzania.

[7] Wyrok Naczelnego Sądu Administracyjnego z dnia 6 grudnia 2023 r., sygn. akt III OSK 2931/21
[8] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 16 kwietnia 2019 r., znak ZSPU.440.131.2019

ADMINISTRATOR A ODBIORCA W POSTACI ZEWNĘTRZNEGO INSPEKTORA DANYCH OSOBOWYCH

Odbiorca ma charakter szczególnie szeroki, gdyż jest on osobą fizyczną lub prawną, organem publicznym, jednostką lub innym podmiotem, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z tym że nie są organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego o tj. chociażby organy podatkowe, organy celne, organy ścigania. Dlatego, odbiorcą danych może być właśnie podmiot przetwarzający, subprocesor, ale także - zewnętrzny inspektor ochrony danych.

W tym miejscu należy zaznaczyć, że wyznaczenie inspektora danych osobowych jest obowiązkowe w przypadkach określonych w art. 37 ust. 1 RODO, co obejmuje m.in. obowiązek wyznaczenia IOD w przypadku przetwarzania przez organ lub podmiot publiczny, bądź gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, a także gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych dotyczących wyroków skazujących i czynów zabronionych. Wobec tego, podmioty powinny ustalać, czy podlegają pod obowiązek wyznaczenia inspektora ochrony danych, czy też nie - a w takim przypadku, czy inspektor byłby przydatny w danym środowisku. Należy mieć również na względzie motyw 97 zawarty w preambule rozporządzenia w sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. Tacy inspektorzy ochrony danych - bez względu na to, czy są pracownikami administratora - powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny[9].

Powołanie takiego inspektora obejmuje nie tylko administratora, ale także podmiot przetwarzający. Dlatego, kwestie jego dotyczące odnoszą się zarówno wobec jednego, jak i drugiego podmiotu. Jednocześnie, należy wskazać,

[9] Motyw 97 z preambuły RODO.

że w rozporządzeniu wyraźnie zaznaczono, iż inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług, co wyraźnie umożliwia *outsourcing* tej funkcji.

Pomimo, iż w przypadku zewnętrznego IOD dokonuje się udostępnienia danych osobowych, administrator, czy też podmiot przetwarzający nie dokonuje tego w formie umowy powierzenia przetwarzania danych osobowych. W tym przypadku, kluczową różnicą jest fakt, iż w przypadku umowy powierzenia dochodzi do posługiwania się zewnętrznym podmiotem do realizacji zadań administratora związanych z przetwarzaniem danych, a sam podmiot przetwarzający ma obowiązek stosować się do zaleceń i instrukcji administratora. W przypadku umowy z zewnętrznym inspektorem konieczne jest zagwarantowanie podstawowych założeń zawartych w RODO, a przede wszystkim - jego niezależność. Z tego względu IOD nie otrzymuje takich zaleceń, czy też rekomendacji, a musi być wybrany na podstawie kryterium profesjonalizmu i wiedzy w zakresie ochrony danych osobowych. Samo powierzenie IOD danych osobowych tak naprawdę wynika z przepisów prawa, co potwierdzają chociażby obowiązki nałożone na administratora i podmiot przetwarzający w zakresie wspierania inspektora w wykonywanych przez niego zadaniach poprzez np. zapewnienie mu dostępu do danych osobowych i operacji przetwarzania. Z kolei, IOD obowiązany jest do zachowania tajemnicy i poufności co do wykonywanych zadań zgodnie z prawem UE lub prawem państwa członkowskiego. Co ważne, przedmiotem świadczenia w umowie w zewnętrznym IOD jest wykonywanie zadań wskazanych w rozporządzeniu, ale możliwe jest także powierzeniu mu zadań z zakresu nadzoru nad systemem ochrony danych osobowych. Jednak, jak wskazywane jest na stronie UODO - warto pamiętać, że możliwość wykonywania przez osobę, z którą zawierana jest umowa o świadczenie usług, zadań innych niż określone w RODO ograniczona jest zakazem występowania w tym zakresie konfliktu interesów (art. 38 ust. 6 RODO)[10]. Jednakże, niezależność inspektora danych nie oznacza, że nie można poddać go audytowi. Biorąc pod uwagę obowiązki ciążące na administratorze, to dochowanie należytej staranności również w dobraniu odpowiedniego inspektora ochrony danych jest pożądane, jednak z poszanowaniem jego niezależności oraz zakazu wydawania poleceń odnośnie zadań IOD.

Jednocześnie, co należy podkreślić pomimo wyznaczenia inspektora ochrony danych osobowych odpowiedzialność ponosi administrator. Wobec tego,

[10] https://uodo.gov.pl/pl/495/2412 [dostęp: 17.03.2024].

należy stwierdzić, że inspektor zobowiązany jest wykonywać swoje obowiązki z należytym uwzględnieniem ryzyka (art. 39 ust. 2 RODO), a zatem należy odnosić się do ogólnych miar staranności wykonywania zadań przez inspektora. W przypadku zewnętrznego inspektora, odpowiedzialność będzie miała charakter odpowiedzialności kontraktowej. Jednak, inspektor posiadałby możliwość uchylenia się od odpowiedzialności pod warunkiem wykazania dochowania tej należytej staranności i wykazania, że nie zostały dokonane uchybienia ze strony jego jako usługobiorcy. Co ważne, na inspektora nie można jednak nałożyć administracyjnych kar pieniężnych, a odpowiedzialność za zaniedbania inspektora może ponosić przedsiębiorca na gruncie art. 83 ust. 4 lit. a RODO, który stanowi, iż naruszenie w zakresie wykonywania zadań inspektora ochrony danych może skutkować nałożeniem administracyjnej kary pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

SZANSE I ZAGROŻENIA

Wobec powyższego należy jednoznacznie stwierdzić, że każde z rozwiązań ma swoje wady i zalety, co jednak nie oznacza, że nie można korzystać z *outsourcingu*. Należy wskazać, że podstawowymi możliwościami, które zyskują przedsiębiorstwa po oddelegowaniu części zadań do podmiotów przetwarzających jest chociażby zwiększenie wydajności, gdyż pozwala to skoncentrować się na podstawowych działaniach biznesowych. Dzięki temu, przedsiębiorcy mają również dostęp do nowych technologii, co poprawia sposoby zarządzania, a także daje możliwość korzystania z szerokiej gamy specjalistów z różnych dziedzin. Podobnie, w ramach *outsourcingu* funkcji inspektora danych osobowych możliwe jest zapewnienie odpowiedniego poziomu bezpieczeństwa, czy też nawet czasem zmniejszenie ryzyka związanego z naruszeniem przepisów dotyczących ochrony danych osobowych. Dzięki oddelegowaniu tej funkcji, przedsiębiorcy nie muszą samodzielnie zatrudniać odpowiednich specjalistów z tej dziedziny w ramach własnej infrastruktury, co pozwala również na zmniejszenie kosztów.

Jednakże, zasadniczym zagrożeniem jest kontrola nad zewnętrznym podmiotem, co tyczy się zarówno podmiotu przetwarzającego, jak i zewnętrznego IOD (z uwzględnieniem jego niezależności). Przedsiębiorca musi przeprowadzić odpowiednie działania, które pozwolą mu na dokonanie oceny, czy dany podmiot spełnia warunki przewidziane w rozporządzeniu, a także w trakcie trwania umowy poprzez audyty, czy też inspekcję. Z tego względu tak ważny jest

odpowiedni dobór specjalistów, stworzenie umowy zabezpieczającej interesy administratora-przedsiębiorcy i zwrócenie uwagi na powyższe kwestie, gdyż często mogą być decydujące w zakresie nawiązania umowy z konkretnym podmiotem i może zostać poddane kontroli w razie ewentualnego naruszenia. Często pojawia się również argument ewentualnego ryzyka reputacyjnego w razie naruszenia przepisów dotyczących ochrony danych osobowych, co może wiązać się z koniecznością ochrony swoich dóbr osobistych.

PODSUMOWANIE

Wobec powyższego, można stwierdzić, że *outsourcing* danych osobowych zdecydowanie może korzystnie wpłynąć na rozwój przedsiębiorstwa, a także umożliwia efektywniejsze realizowanie poszczególnych funkcji. Jednakże, przedsiębiorca musi być świadomy swoich obowiązków, a także powinien zachować i podejmować odpowiednie środki ostrożności w celu zminimalizowania ryzyka. Tym samym należy ponownie podkreślić, iż istotny w całym procesie jest dokonanie starannej selekcji i nadzoru, aby zapewnić zgodność z przepisami i ochronę danych osobowych w zakresie działania podmiotów zewnętrznych, które nimi dysponują.

BIBLIOGRAFIA

Akty prawne

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

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. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Literatura

Krasuski A.
2010 *Outsourcing danych osobowych w działalności przedsiębiorstw*, Warszawa.

Litwiński P. (red.)
2021 *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*.

Pyka A.
2020 *Powierzenie przetwarzania danych osobowych w świetle ogólnego rozporządzenia o ochronie danych*, „Prawo Mediów Elektronicznych", nr 1.

Nerka A.
2017 Powołanie inspektora ochrony danych jako przejaw społecznej odpowiedzialności biznesu, „Annales. Etyka w życiu gospodarczym", nr 20/3.

Morawski F.
2019 *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według Ogólnego Rozporządzenia o Ochronie Danych Osobowych*, „Acta Iuris Stetinensis", nr 26 (2).

Orzecznictwo i decyzje administracyjne

Postanowienie SN z 13.04.2021 r., I USK 6/21, LEX nr 3159922.

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 7 września 2022 r., znak: DKN.5131.29.2022.

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 22 kwietnia 2021 r., DKN.5130.3114.2020.

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 19 stycznia 2022 r., znak DKN.5130.2215.2020.

Wyrok Naczelnego Sądu Administracyjnego z dnia 6 grudnia 2023 r., sygn. akt III OSK 2931/21.

Źródła internetowe:

https://uodo.gov.pl/pl/495/2412 [dostęp:17.03.2024].

https://uodo.gov.pl/pl/495/2364 [dostęp: 17.03.2024].

https://uodo.gov.pl/pl/495/2410 [dostęp: 17.03.2024].

https://www.parp.gov.pl/component/content/article/84730:inspektor-ochrony-danych-w-przedsiebiorstwie-zadania-i-odpowiedzialnosc [dostęp: 17.03.2024].

https://www.parp.gov.pl/component/content/article/80756:administrator-procesor-odbiorca-kto-jest-kim-w-systemie-ochrony-danych-osobowych [dostęp: 17.03.2024].

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_pl [dostęp: 17.03.2024].

Joanna Walkowiak
Uniwersytet Warszawski
Studentka

PRZEDSIĘBIORCA Z PAŃSTWA TRZECIEGO A UNIJNE PRAWO OCHRONY DANYCH – SZANSE I WYZWANIA EKSTERYTORIALNEGO ZASTOSOWANIA RODO

WSTĘP

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 (*RODO*, *Rozporządzenie*) to jeden z najbardziej rozpoznawalnych w przestrzeni publicznej aktów prawa unijnego ostatnich lat. Jest to to pierwsza tak kompleksowa regulacja prawa ochrony danych, która opiera się na fundamentalnym założeniu, że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych (*motyw 1 Rozporządzenia*). Nie ma oczywiście wątpliwości, że przepisy Rozporządzenia bezpośrednio obowiązują przedsiębiorców na terenie Unii Europejskiej (*UE, Unia*). Jako obywatele UE mamy z nim do czynienia na co dzień, podpisując klauzule informacyjne przy załatwianiu codziennych spraw, czy robiąc zakupy w internecie. Nie jest jednak oczywiste ani powszechnie wiadome, że RODO przewiduje szeroki zakres zastosowania eksterytorialnego; mówiąc najprościej – że jego zastosowanie sięga daleko poza granice UE. Natomiast to właśnie stanowi jedną z głównych innowacji odróżniających RODO od dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie

ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (*Dyrektywa 95/46/WE*). Niniejszy artykuł omówi rozwój eksterytorialnego stosowania RODO, pozytywne aspekty przyjętych rozwiązań, ale także trudności i wyzwania, które wiążą się z tak daleko idącym stosowaniem RODO poza granicami Unii.

ZAKRES TERYTORIALNY STOSOWANIA RODO W PORÓWNANIU DO DYREKTYWY 95/46/WE

Eksterytorialny zakres zastosowania RODO

Art. 3.1 RODO przewiduje jego zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii. Art. 3.2 RODO przewiduje także sytuacje, w których RODO może być stosowane eksterytorialnie, tj. do podmiotów, które nie mają swojej siedziby na terytorium UE. Zgodnie z przywołanym przepisem, Rozporządzenie stosuje się do przetwarzania danych osobowych osób przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli: a) czynności przetwarzania wiążą się z oferowaniem im towarów lub usług w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty (*art. 3.2.a RODO*); lub b) monitorowaniem ich zachowania, jeśli ma ono miejsce w Unii (*art. 3.2.b RODO*). Rozporządzenie ma także zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, gdzie zgodnie z regułami mnar. prawa publicznego stosuje się prawo państwa członkowskiego (*art. 3.3 RODO*). O ile druga z podanych podstaw zastosowania RODO do jednostek poza Unią nie jest zbyt kontrowersyjna, to art. 3.2 RODO stanowi *novum* wobec Dyrektywy 95/46/WE (Van Alsenoy 2017, s. 77, 89). Zakres terytorialny wyznaczany przez art. 3.2.a RODO ustanawia tzw. zasadę targetowania, zgodnie z którą RODO obejmuje swoim zasięgiem podmioty, które poprzez swoje zachowanie rynkowe pokazują, że chcą działać i być obecne na rynku unijnym (de Her i Czerniawski 2016, s. 242).

Rozwój zakresu terytorialnego i eksterytorialnego zastosowania europejskiego prawa ochrony danych osobowych

Dyrektywa 95/46/WE, nie przewidywała tak szerokiego zakresu stosowania poza terytorium UE. Zgodnie z art. 4, znajdowała zastosowanie do przetwarzania danych osobowych w związku z prowadzoną przez administratora danych działalności gospodarczej poza Unią (czyli przewidywała swoje eksterytorialne zastosowanie) wtedy, gdy prawo unijne obowiązywało w tym miejscu na mocy prawa międzynarodowego publicznego (*art. 4.1.b*), oraz w przypadku, gdy do przetwarzania danych był wykorzystywany był sprzęt znajdujący się na terytorium UE (*art. 4.1.c*). Tak sformułowane podstawy zastosowania dyrektywy ograniczały jej eksterytorialne ambicje do miejsca, gdzie działalność gospodarcza faktycznie była prowadzona. Polska wersja językowa posługuje się sformułowaniem 'prowadzenie działalności gospodarczej' w miejsce angielskiego zwrotu 'establishment', które można również rozumieć jako 'organizację', 'siedzibę', 'ośrodek prowadzenia działalności gospodarczej'.

Niemniej, w trakcie obowiązywania Dyrektywy 95/46/WE okazało się, że dla osiągnięcia jej celu konieczna jest rozszerzająca interpretacja (Greeze 2019, s. 109). Celowościowej wykładni TSUE dokonał m. in. w licznych wyrokach, w których za każdym razem podkreślał, że celem ustawodawcy unijnego było zakreślenie szerokiego zakresu terytorialnego zastosowania dyrektywy. W sprawie C-131/12 (*Google Spain przeciwko APED*), TSUE opowiedział się za rozszerzającą wykładnią sformułowania 'prowadzenia działalności gospodarczej' – kluczowego dla właściwego określenia zakresu terytorialnego zastosowania RODO. Trybunał zwrócił w nim uwagę, że forma prawna prowadzenia działalności jest w rzeczywistości nieistotna, a decydujące znaczenie powinno mieć „efektywne i rzeczywiste prowadzenie działań poprzez stabilne rozwiązania organizacyjne", przez co dyrektywa objęła swoim zakresem także mniej oczywiste ośrodki oraz formy prawne prowadzenia działalności gospodarczej, jak filie, oddziały itp. Ponadto, w sprawie C-230/14 (*Weltimmo s. r. o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság*) TSUE uznał, że art. 4.a Dyrektywy zezwala na zastosowanie przepisów dotyczących ochrony danych osobowych państwa członkowskiego innego niż to, gdzie zarejestrowany jest administrator danych, jeżeli to w tym państwie prowadzi faktyczną i rzeczywistą działalność, i w związku z nią dokonuje przetwarzania danych osobowych. Rozszerzony zakres terytorialny zastosowania RODO potwierdza wobec tego decyzję prawodawcy unijnego i TSUE, podjęte jeszcze

w czasie obowiązywania dyrektywy 95/46/WE (Wskazówki 3/2018 2020, 4; Van Alsenoy 2017, s. 77).

Na zawarte bezpośrednio w przepisach rozszerzenie zakresu terytorialnego w stosunku do dyrektywy 95/46/WE złożyło się wiele czynników. Poza orzecznictwem TSUE, które dążyło do rozszerzającej wykładni dyrektywy, niebagatelne znaczenie miał rozwój cyberprzestrzeni, możliwości komunikacji na odległość i powszechność korzystania z Internetu (Svantesson 2015, 226, 230; Simmons i Huvley 2022, s. 617). Obecnie zauważa się, że niewiele zagadnień jest równie kontrowersyjnych jak jurysdykcja w przestrzeni internetowej (Svantesson 2015, s. 226). W naturalny sposób, korzystanie z Internetu wiąże się z przetwarzaniem ogromnych ilości danych. Nic też nie wskazuje na to, aby tendencja do korzystania w życiu codziennym z internetu przestała rosnąć, przeciwnie – pandemia COVID-19 przyspieszyła przenoszenie się coraz to nowych sfer życia w przestrzeń internetową. Wymiana danych na odległość oznacza, że nie obowiązują granice terytorialne, a zmiany technologiczne przyczyniają się do tego, że poszerzanie granic obowiązywania prawa danego państwa poza jego terytorium jest debatowane w skali globalnej. Niektórzy autorzy postulują, że zważywszy na sytuację, przed jaką stawia nas internet, wskazanie 'targetowania' jako podstawy jurysdykcyjnej jest jedynym wyjściem i drogą do zapewnienia ochrony danych, które przepływają w ramach korzystania z niego (Lutzi 2017, 703–05). Art. 3 RODO wpisuje się także w globalną tendencję do rozszerzenia zakresu terytorialnego prawa ochrony danych osobowych (Azzi 2018, s. 126), widoczną m.in. we wzroście spraw rozstrzyganych przez sądy powszechne, które dotyczą właśnie konfliktu jurysdykcyjnego w sprawach z zakresu ochrony danych (Daskal, 2018, s. 727).

WPŁYW SZEROKIEGO UREGULOWANIA ZAKRESU TERYTORIALNEGO NA SYTUACJĘ PRZEDSIĘBIORCÓW Z PAŃSTW TRZECICH

Omówiony powyżej zakres terytorialny, ze względu na bezprecedensowe obejmowanie spółek znajdujących się w państwach poza obszarem Unii i w żaden sposób z nią nie powiązanych, wywołuje kontrowersje. Może także powodować uzasadnione problemy i wątpliwości dotyczące jego zastosowania w praktyce, z jednej strony utrudniając wejście na rynek unijny podmiotom zagranicznym, a z drugiej strony – budzi uzasadnione wątpliwości, jak stosowanie prawa unijnego za granicą miałoby wyglądać w praktyce. Skuteczność art. 3.2 RODO, który w praktyce ma przyczynić się do faktycznego przestrzegania Rozporządzenia

przez podmioty z państw trzecich, nie jest więc przesądzona; wydaje się, że nie będzie to zadanie proste do zrealizowania.

Szeroki i nieostry zakres terytorialny może powodować trudności w interpretacji przesłanek stosowania RODO

Jednoznaczne uregulowanie terytorialnego zakresu obowiązywania RODO oraz możliwości oceny, czy RODO obejmuje dany podmiot zagraniczny, trudno przecenić. Niestety, sposób, w jaki został sformułowany art. 3 RODO – w szczególności art. 3.2.a, zawierający wspomnianą *targeting principle* – spotyka się z krytyką ze strony doktryny (Tene i Wolf 2013, s. 109; de Hert i Czerniawski 2016, s. 243; Svantesson 2015, s. 234). Zgodnie z art. 3.2.a, jak zostało zarysowane na wstępie, RODO stosuje się do przetwarzania danych osobowych osób przebywających w UE przez administratora lub podmiot przetwarzający, jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom w UE lub monitorowaniem ich zachowania, jeśli dochodzi do niego w UE. Przepis ten sformułowano głównie na potrzeby handlu elektronicznego, aby zapewnić konsumentom w UE ochronę ich danych osobowych w środowisku internetowym.

Wielu autorów zauważa, że *targeting principle* jest wyjątkowo nieostra, a firmy zagraniczne nie mogą być do końca pewne, czy RODO je wiąże, czy jednak nie (Mannion 2021, s. 692). Pojawiały się także postulaty zastąpienia tej zasady inną (Tene i Wolf 2013, s. 10) lub zmodyfikowania brzmienia artykułu (de Hart i Czerniawski, 2016, s. 243). Krytyka wynika z kilku czynników. Przede wszystkim, targetowania podmiotów znajdujących się w Unii jest trudne do stwierdzenia, jeżeli dana firma działa globalne, a strona internetowa, poprzez którą sprzedaje swoje produkty, sporządzona jest z myślą o kliencie międzynarodowym. W takiej sytuacji sam fakt, że strona sporządzona jest w językach unijnych (angielski, francuski, niemiecki czy hiszpański to języki powszechnie używane na świecie, nie tylko w Unii), a za oferowane produkty można płacić w euro, nie zawsze musi jeszcze świadczyć o świadomym 'targetowaniu'. W sytuacjach granicznych może to być trudne do ustalenia, ponieważ globalne działanie firmy nie wyklucza tego, że jednocześnie implementuje ona strategie mające na celu dotarcie do klientów w UE. Trudno jest jednak oceniać, czy zachodzi targetowania, gdy oceny dokonuje się *in abstracto*.

Kluczowym aspektem, który należy wziąć pod uwagę przy ocenie, czy kryterium z art. 3.2.a RODO jest spełnione, jest wobec tego właśnie 'targetowanie'. Liczy się to, czy można ustalić intencję administratora danych, aby produkty

czy usługi były oferowane, w tym także za darmo, podmiotom znajdującym się w UE (Wskazówki 3/2018, 2020, s. 17). Konieczność istnienia takiej właśnie intencji ze strony podmiotu targetującego potwierdza motyw 23. rozporządzenia (Van Alsenoy 2017, s. 86). Zgodnie z nim, „aby stwierdzić, czy administrator lub podmiot przetwarzający oferują towary lub usługi znajdującym się w Unii osobom, których dane dotyczą, należy ustalić, czy jest oczywiste, że administrator lub podmiot przetwarzający planują oferować usługi osobom, których dane dotyczą, w co najmniej jednym państwie członkowskim Unii". O ile kryteria, według których należy stwierdzić, czy do takiego targetowania dochodzi są niejasne, ustawodawca unijny próbował naprawić legislacyjne niedociągnięcia, precyzując zakres zastosowania przepisu oraz właściwy sposób jego interpretacji w motywach dyrektywy. W praktyce jednak, skoro o istnieniu bądź nie intencji decyduje się *ad casum* i jest to decyzja cokolwiek uznaniowa, nie ma pewności, czy takie sformułowanie znajdujące się w motywach rozporządzenia stanie się istotną wskazówką interpretacyjną. Wydaje się, że o ile może ono nakierować interpretację przepisu na właściwe tory, to stwierdzenie w konkretnym przypadku, czy RODO stosuje się na podstawie art. 3.2.a, czy nie, może wciąż nastręczać trudności.

Ponadto, na podstawie art. 3.2.a., Rozporządzenie ma zastosowanie w przypadku 'targetowania' podmiotów znajdujących się w Unii niezależnie od tego, jakie jest ich obywatelstwo. Tak samo nie jest ono zależne od rodzaju ich powiązania z UE; np. nie jest uwarunkowane tym, czy mają w Unii swoje stałe miejsce zamieszkania, czy są tam zameldowane etc. Może się więc okazać, że także spółka z państwa trzeciego, oferująca usługi z myślą o grupie osób niemających obywatelstwa unijnego – np. nakierowana na pomoc migrantom znajdującym się w Unii czasowo – będzie zobligowana do przestrzegania RODO. Takie rozwiązanie może się okazać dla niektórych firm zaskakujące, skoro na pierwszy rzut oka wydaje się, że ich działanie nie ma praktycznie żadnego związku z Unią.

Mimo prób wyłożenia kryteriów zastosowania art. 3.2.a w motywach, a także w dokumentach takich jak *guidelines* (Wskazówki 3/2018 2020), doktryna opisuje przypadki pograniczne, w których stwierdzenie, czy RODO wiąże daną spółkę, będzie utrudnione, albo wyniki takiego badania będą mało satysfakcjonujące. De Hert oraz Czerniawski posługują się przykładem, gdzie osoba fizyczna w UE zarezerwowała hotel w USA za pośrednictwem amerykańskiego internetowego biura podróży. Zgodnie z reżimem unijnego prawa ochrony danych, to biuro podróży podlega pod przepisy RODO (de Hert i Czerniawski 2016, s. 239). Powstaje jednak pytanie, czy takie rozwiązanie jest słuszne. Nie należy też tracić z pola widzenia, że art. 3.2a RODO powstał w dużej mierze z myślą z uwagi

na rozwój platform *e-commerce* oraz innych internetowych platform. Przywołani autorzy słusznie zwracają uwagę na fakt, że użytkownik, szczególnie w Interencie, cieszy się ogromnym wyborem dostępnych platform, dóbr i usług, i jeśli któraś z nich nie spełnia jego oczekiwań w zakresie ochrony danych, może bez przeszkód zrezygnować z korzystania z niej.

Eksterytorialne stosowanie budzi wątpliwości związane z legitymacją UE do regulowania sytuacji przedsiębiorców z państw trzecich, jurysdykcją i egzekwowaniem prawa (*law enforcement*)

Tak szeroki zakres eksterytorialny zastosowania RODO może być kontrowersyjny także z perspektywy jego zgodności z podstawowymi zasadami prawa publicznego. Faktycznie, konflikt jurysdykcyjny, pokazujący trudności wynikające z prób dopasowania eksterytorialnego prawa ochrony danych do międzynarodowego prawa publicznego, stanowi jedną z najbardziej kontrowersyjnych materii RODO (Svantesson 2015, s. 226). Chociaż można spotkać się z poglądem, że „idea jurysdykcji opartej na zasadzie terytorialności jest relatywnie nowa" (Ford 1999, s. 243), to na zasadzie terytorialności i możliwości decydowania o obowiązującym prawie na danym terytorium oparta jest obecna idea państwa i suwerenności państwowej, co znalazło wyraz m. in. w słynnej sprawie Lotus (Greze 2019, s. 114; Priamesti i Afriansyiah 2020, s. 84). Pomysł rozszerzania zakresu terytorialnego poza państwo, na terenie którego dany organ władzy lub organizacja ma prawo działać przez prawo danych osobowych, jest jednak nowatorski. Niektórzy uznają go za wskazany w dobie internetu, skoro przestrzeń digitalna zaciera fizyczne granice między państwami i pozwala na nieograniczone transgraniczne kontakty, a co za tym idzie, transgraniczny przepływ danych (Schultz 2008, s. 816-819). Debata ogniskuje się wobec tego właśnie wokół zagadnienia, czy eksterytorialne prawo ochrony danych nie ogranicza – choćby potencjalnie – suwerenności państwa oraz możliwości państwa do samodzielnego regulowania swojego prawa (de Hert i Czerniawski 2016, p. 240).

Zagadnienie eksterytorialnego zastosowania prawa ochrony danych jest tym bardziej istotne, że takie przepisy pojawiają się nie tylko w europejskim porządku prawnym. Choć jest to w prawie pewne *novum*, aby zakres obowiązywania aktu prawnego wykraczał tak dalece poza terytorium państwa, które go wprowadza, podobne przepisy można już również w aktach prawnych innych państw, w tym reżimów niedemokratycznych (Edoardo i Fabbrini 2021, s. 15). Im więcej porządków prawnych będzie wprowadzać zasady stosowania eksterytorialnego,

tym częściej może dochodzić do sytuacji, gdy dwie różne regulacje – o odmiennej treści i zakresie obowiązków administratorów i podmiotów przetwarzających dane – będą coraz częściej ze sobą konkurować. To może mieć w praktyce zdecydowanie negatywne skutki dla pewności prawa oraz dla zapewnienia skuteczności przepisów przewidujących eksterytorialne obowiązywania i stosowanie prawa. Sprawy, w których takie kwestie wymagają rozstrzygnięcia, nie istnieją jedynie w próżni i pojawiają się już w sądach. Przykładowo, w sprawie *Google Inc. v. Equustek Solutions Inc.* rozstrzygniętej w 2017 r. przez Kanadyjski Sąd Najwyższy, sąd wydał przeciwko Google nakaz obejmujący swoim zakresem działanie platformy nie tylko w Kanadzie, ale *de facto* na całym świecie (Edoardo i Fabbrini 2021, s. 13, *Google Inc. v. Equustek Solutions Inc.*). Sąd zdecydował, że taka decyzja nie stanowiłaby pogwałcenia prawa, skoro większość państw przestrzega wolności słowa i chroni prawa autorskie (*Google Inc. v. Equustek Solutions Inc.*, para. 44-45). O ile sprawa dotyczyła naruszeń IP, nie ulega wątpliwości, że podobna mogłaby pojawić się w kontekście konkretnych obowiązków i uprawnień osób, których dane dotyczą. Gdyby dotyczyła zagadnień bardziej kontrowersyjnych i nieimplementowanych na skalę międzynarodową, jak np. prawa do bycia zapomnianym (Edoardo i Fabbrini 2021, s. 14-15), zgodność takiego rozstrzygnięcia z prawem publicznym byłaby co najmniej wątpliwa.

Bardzo podobna sprawa zawisła już zresztą przed TSUE pod sygnaturą C-507/17 i została prawomocnie rozstrzygnięta (*Google LLC, następca prawny Google Inc., przeciwko Commission nationale de l'informatique et des libertés (CNIL)*. Trybunał musiał udzielić odpowiedzi na pytanie, jaki jest właściwy zakres terytorialny nakazu usunięcia linków ze storny interentowej na żądanie osoby, której dane w linku dotyczyly (tzw. geo-blokowania), wydanego przez sąd krajowy. Podstawami rozstrzygnięcia była zarówno dyrektywa 95/46/WE, jak i przepisy RODO (art. 17, regulujący „prawo do bycia zapomnianym"). TSUE postanowił w niej, że operator wyszukiwarki jest obowiązany do usunięcia owych linków nie ze wszystkich wersji swojej wyszukiwarki, ale z tych wersji wyszukiwarki, które odpowiadają wszystkim państwom członkowskim. TSUE zadecydował, że operator wyszukiwarki ma obowiązek usunięcia niezgodnych z przepisami RODO linków nie ze wszystkich wersji swojej wyszukiwarki, ale tylko z tych, które odpowiadają państwom członkowskim. Widać więc, że TSUE wyraźnie ogranicza zakres obowiązywania RODO jedynie do śladów obecności i działania podmiotu z państwa trzeciego na terytorium UE. W kontekście rozpatrywanego zakresu terytorialnego, Trybunał oparł swoje orzeczenie na art. 4 ust. 1 lit. a) dyrektywy 95/46 oraz z art. 3 ust. 1 RODO, dlatego nie odpowiada ono

dokładnie zagadnieniu obejmowania przedsiębiorców z państw trzecich europejskim prawem ochrony danych. Może być jednak pomocne dla stwierdzenia, jak daleko, w opinii Trybunału, sięga zdolność do wywierania wpływu na podmioty znajdujące się w innych państwach. Jak stwierdził Rzecznik Generalny Maciej Szpunar w opinii, której wnioski w tym zakresie zostały zaaprobowane przez TSUE „usuwanie linków powinno zostać przeprowadzone nie na poziomie krajowym (…) ale na poziomie Unii Europejskiej" (Opinia Rzecznika Genralnego 2019, para. 75). Widać więc poszanowanie wskazówek związanych z zasadą targetowania. W konsekwencji, chociaż nie zawsze wyznacza ona zakres terytorialny precyzyjnie, nie pozwala go ekstrapolować bez ograniczeń.

Poza teoretycznymi rozważaniami, jak daleko w dobie internetu i rozwijającej się cyberprzestrzeni sięgać mogą granice terytorialnego zasięgu prawa publicznego, taka regulacja może powodować także problemy praktyczne. Niewątpliwie, eksterytorialne zastosowanie RODO będzie w dużej mierze dotyczyć podmiotów, które i tak są związane swoim krajowym prawem ochrony danych osobowych. Nie da się jednak łatwo rozstrzygnąć, które z tych regulacji będą właściwe i co należy robić, jeśli będą ze sobą sprzeczne. Niektórzy zwracają uwagę, że ryzyko konfliktu jurysdykcyjnego może prowadzić do pogwałcenia gwarancji procesowych, takich jak *ne bis in idem*, jeżeli jeden podmiot (administrator danych lub podmiot przetwarzający) będzie poddany dwóm konkurującym jurysdykcjom (de Hert i Czerniawski, 2016, s. 241). Jest to stanowisko zdecydowanie niepozbawione słuszności. W praktyce, nawet jeśli administratora lub procesora danych będzie w teorii obowiązywało kilka różnych reżimów prawa ochrony danych, istnieje ryzyko wydania dwóch decyzji lub nałożenia kar przez dwa niezależnie działające organy.

Na marginesie, warto zwrócić uwagę na jeszcze jeden problem – mianowicie, że faktyczne wyegzekwowanie przestrzegania przepisów uda się raczej tylko organom krajowym. Jeśli zgodzić się, że w niektórych sytuacjach eksterytorialne zastosowanie prawa ochrony danych osobowych jest pożądane, jak zapewnić skuteczne przestrzeganie i egzekwowanie prawa ochrony danych osobowych w państwach trzecich. Oczywiście, w niektórych państwach wykonywanie przez spółki obowiązków nałożonych przez RODO jest skutecznie egzekwowane. Potwierdza to między innymi decyzję angielskiego sądu, która zapadła w sprawie AggregateIQ Data Services Ltd przeciwko UK's Information Commissioner's Office (Pramesti i Afriansyah 2020, s. 88). W tym wyroku sąd uznał, że spółka, której siedziba nie znajduje się w UE, i tak musi zachować zgodność z przepisami RODO. Zapewnienie spójności i egzekwowanie przepisów unijnych poza granicami UE jest

więc znacznie łatwiejsze, jeśli UE i państwo, w którym dochodzi do naruszenia – a więc, gdzie zgodność z RODO będzie ostatecznie egzekwowana – łączą wspólne interesy (Höglund 2018, s. 36) oraz wspólne podejście do prawa ochrony danych. Z dużym prawdopodobieństwem eksterytorialne zastosowanie RODO będzie więc najbardziej skuteczne tam, gdzie jego cel jest uznawany za słuszny, a zarówno legislacja krajowa, jak i regulacje wewnątrzkorporacyjne są z nim zbieżne. W państwach, w których organy krajowe nie mają takich kompetencji i nie działają tak, jak przewidują przepisy unijne, będzie to jednak trudne zadanie.

W praktyce, trudnością dla przedsiębiorcy może być konieczność dostosowania się jednocześnie do RODO oraz do krajowego porządku ochrony danych. Zagraniczne porządki ochrony danych nie są kompatybilne z RODO, szczególnie że obecnie zapewnia ono najwyższy poziom ochrony i jest najbardziej wymagającą dla administratorów i podmiotów przetwarzających regulacją z zakresu ochrony danych osobowych. Podobnie, uzasadnieniem dla rozszerzania zakresu stosowania RODO poza granice UE nie jest międzynarodowy zwyczaj oraz ponadnarodowe standardy wypracowane w zakresie ochrony danych osobowych (Azzi 2018, s. 145), które są znacznie mniej rygorystyczne. Ponadto, podczas gdy RODO oparte jest na generalnej zasadzie konieczności ochrony danych osób fizycznych, a ochrona danych została wpisana w porządek ochrony praw fundamentalnych, inne państwa w nakreślaniu wymogów ochrony danych kierują się raczej względami ekonomicznymi (patrz pkt. *Propozycje rozwiązań praktycznych*).

Wypełnianie obowiązków nakładane przez RODO oraz utrudnienia, jakie mogą napotkać podmioty zagraniczne w związku z wdrożeniem RODO

Jeśli przedsiębiorcę obowiązują przepisy RODO, wiąże się to z licznymi obowiązkami informacyjnymi wobec podmiotów, których dane są przetwarzane, koniecznością utrzymywania odpowiednich standardów przetwarzania oraz przechowywania danych. Wdrożenie RODO niesie za sobą znaczące koszty i wymaga zaimplementowanie określonych rozwiązania technicznych, na co firmy spoza Europy mogą nie być przygotowane. Jak zwraca uwagę doktryna, o ile promowanie inwestycji w lepsze zabezpieczenia i systemy ochrony danych samo w sobie jest wskazane, to jednak pozostaje kontrowersyjne, czy prawo unijne może nakładać na przedsiębiorców zagranicznych takie obowiązki, i wymuszać na nich ponoszenie takich kosztów (Rosentau 2018, s. 39). Zwraca się uwagę na to, że dla rynków *e-commerce* z państw rozwijających się, takich jak kraje afrykańskie, obowiązki nakładane przez RODO mogą stanowić znaczącą barierę do wejścia

na rynek europejski (Mannion 2021, s. 688). Dla firm z takich państw problemem może być mała dostępność *know-how* w zakresie implementacji prawa ochrony danych osobowych oraz niewielki budżet, jakie mogą one przeznaczyć na wdrożenie systemu ochrony danych zgodnego z wymogami europejskiej regulacji. Takie ograniczenia dotyczą szczególnie małych i średnich przedsiębiorstw, które działają na rynku unijnym nieregularnie (Svantesson 2015, s. 230).

Z drugiej strony, w sektorach i firmach, które dysponują większym budżetem i są nastawione na działania globalne, RODO wywiera duży wpływ. Przykładowo, zauważalnie oddziałuje ono na regulacje ochrony danych w firmach amerykańskich, nawet „pomimo wysiłków podejmowanych przez Stany Zjednoczone w celu ochrony przed unijnym prawem ochrony danych poprzez umowy dwustronne, eksterytorialne skutki RODO pokazują, że jest odwrotnie, a prawo to miało znaczący wpływ na wiele sektorów amerykańskiego społeczeństwa" (Jovanovic 2020, s. 39). W tym kontekście istotne jest także, że globalne korporacje – nawet jeśli w państwie siedziby nie obowiązuje prawo o standardach tak wymagających jak RODO – mogą wprowadzać reguły oparte na Rozporządzeniu jako zalecenia wewnątrzkorporacyjne. W ten sposób chcą np. przekonać do siebie konsumentów i dostosować się do ich oczekiwań (Jovanovic 2020, s. 52). Takie rozwiązania wymagają jednak odpowiedniego budżetu i prawnych oraz technologicznych rozwiązań, na które wiele podmiotów z biedniejszych państw nie może sobie pozwolić.

Różnica w pozycji przedsiębiorców unijnych a przedsiębiorców z państw trzecich

Pozycja przedsiębiorców z państw trzecich oraz przedsiębiorców unijnych w świetle RODO nie jest jednak identyczna. Najistotniejsza z różnic polega na tym, że jedynie przedsiębiorcom unijnym przysługuje ułatwienie w postaci tzw. *one-stop shop* (Tene i Wolf 2013, s. 8), która polega na tym, że przedsiębiorca unijny – niezależnie od tego, na terenie ilu państw w UE działa – podlega jedynie jednemu organowi nadzorczemu, ustalanemu wg kryterium siedziby. *One-stop shop* to element mechanizmu współpracy i spójności RODO, jednak znajduje on zastosowanie jedynie do administratorów i podmiotów przetwarzających posiadających jednostkę lub jednostki organizacyjne na terytorium Unii Europejskiej (Wskazówki 3/2018 2020, s. 13). Jest on niewątpliwie ułatwieniem, szczególnie w przypadku, gdy dany podmiot działa na obszarze kilku państw na terenie UE.

Propozycje rozwiązań praktycznych

De facto, najpewniejszym rozwiązaniem problemów powodowanych przez niejasny zakres terytorialny RODO jest przyjmowanie wewnętrznych regulacji naśladujących je przez spółki znajdujące się poza Unią, ale działające na jej terenie. W ten sposób, spółka, niezależnie od tego, czy i w którym momencie obejmuje ją zakres terytorialny zastosowania RODO, przestrzega przepisów. Niemniej, obecnie nie istnieje międzynarodowa praktyka lub standard ochrony danych osobowych, a zgodnie z danymi aktualnymi na rok. 2021, ok. 15% państw świata nie wprowadziło żadnych krajowych przepisów w tym zakresie (UNCTAD).

W doktrynie postulowany jest też rozwój ponadnarodowego prawa ochrony danych (Edoardo C., Fabbrini F., 2021) ze względu na to, że porządki krajowe (szczególnie z różnych państw, reprezentujących różne kultury prawne – np. europejski, chiński, rosyjski) są niekompatybilne i mają na celu ochronę różnych, często niespójnych ze sobą interesów. Dla przykładu, w Chinach prawo ochrony danych i regulacje podejmowane w tym zakresie motywowane są raczej względami bezpieczeństwa państwa, a nie przekonaniem o konieczności praw jednostki (Vatanparast 2020, s. 17). Ze względu na odmienne podstawy aksjologiczne, nie jest pewne, że zapewniana przez różne porządki prawne ochrona danych będzie w każdym wypadku spójna. Z tego też powodu, chociaż porządek ponadnarodowy byłby rozwiązaniem optymalnym ze względów praktycznych, to jednak różnice pomiędzy interesami poszczególnych państw mogą okazać się nie do pogodzenia. Obecnie nie ma podstaw do przypuszczania, że – nawet jeśli RODO stanowi „światowe źródło inspiracji" (Ryngaert C. i Taylor M. 2020, s. 9) – to zostanie w całej rozciągłości przyjęte przez państwa spoza zachodniego kręgu kulturowego. Postulować można raczej wypracowanie pewnego minimalnego standardu, który mógłby zapewnić, że pewne rudymentarne wymogi ochrony danych będą spełnione wszędzie.

PODSUMOWANIE

Zwiększona działalność przedsiębiorców w przestrzeni internetowej – rozwój *e-commerce*, możliwość zakupu coraz większej ilości dóbr i usług przez internet – stanowi przyczynę rozszerzania zakresu terytorialnego aktów prawa regulujących tę sferę. Zakres zastosowania RODO jest próbą odpowiedzi na wyzwania współczesności, która zmierza w dobrym kierunku, ale w praktyce nie stanowi rozwiązania idealnego.

Ocena regulacji

Rozwiązanie wprowadzone przez Rozporządzenie zapewnia oczywiście szerszą ochronę danych osób znajdujących się na terenie Unii Europejskiej, gwarantując, że ich dane przetwarzane przez podmioty znajdujące się poza UE wciąż będą podlegać ochronie. Biorąc pod uwagę, że dane osób znajdujących się na terenie UE przetwarzane są codziennie przez podmioty z całego świata, jedynie objęcie przedsiębiorców zagranicznych zakresem RODO zapewnia pełną ochronę tych danych. Z drugiej strony, z perspektywy przedsiębiorców zagranicznych potencjalnie objętych zakresem zastosowania RODO, sytuacja nie jest tak oczywista. Nie negując konieczności ochrony danych osobowych podmiotów unijnych niezależnie od tego, czy przetwarza je spółka unijna, czy poza UE, konieczność przestrzegania RODO może okazać się dużą dla przedsiębiorcy zagranicznego. Spółki z państw rozwijających się mogą mieć trudności: prawne, finansowe i techniczne, z wdrożeniem RODO. Takie ograniczenia mogą poważnie zniechęcać je do wejścia na rynek unijny (Curtiss 2016, 227). Trudności związane z koniecznością wdrożenia regulacji są tym większe, gdyż kryteria zastosowania eksterytorialnego nie są wystarczająco jasne, a wobec tego spółka może nie mieć pewności, czy jej obowiązkiem jest wdrożenie RODO, czy jednak nie musi tego robić. Jest to istotne także z perspektywy oceny możliwości nakładania na spółkę sankcji za nieprzestrzeganie tych regulacji, w tym kar finansowych, które osiągają w UE znaczne wysokości.

Postulaty *de lege ferenda* oraz przyszły rozwój eksterytorialnego prawa ochrony danych

Przepisy o ochronie danych osobowych powinny być przejrzyste i dostępne dla przedsiębiorców z różnych państw świata. Wzmożona pomocy we wdrożeniu RODO przedsiębiorcom zagranicznym (np. *one-stop shop* dla wszystkich, większa dostępność informacji co do wymogów stawianych przez RODO, bardziej klarowne przepisy w zakresie zastosowania terytorialnego, szczególnie oparte o ostrzej zarysowane kryteria) przełożyłaby się na jego lepsze stosowanie w praktyce, a przez to – także na wyższy poziom ochrony danych osobowych podmiotów na terenie UE. Należy przychylić się także do postulatu dalszego wypracowywania międzynarodowych standardów zakresie przynajmniej minimalnych gwarancji ochrony danych. Minimalny poziom ochrony, choć nie zapewni pełnej kompatybilności z RODO, w praktyce może mieć ogromne znaczenie –

szczególnie zważywszy na praktyczne i prawne trudności wiążące się z egzekucją przestrzegania RODO przez podmioty zagraniczne.

BIBLIOGRAFIA

Orzecznictwo

AggregateIQ Data Services Ltd (AIQ) przeciwko UK's Information Commissioner's Office (ICO).

C-131/12, Google Spain przeciwko APED [2014] ECLI:EU:C:2014:317.

C-230/14, Weltimmo s. r. o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECLI:EU:C:2015:639.

C-507/17, Google LLC, następca prawny Google Inc., przeciwko Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772.

C-585/08 i C-144/09 (sprawy połączone), Peter Pammer v Reederei Karl Schlüter GmbH & Co KG oraz Hotel Alpenhof GesmbH przeciwko Oliverowi Hellerowi [2010] ECLI:EU:C:2010:740.

Supreme Court of Canada, Google Inc. v. Equustek Solutions Inc. [2017] 2017 SCC 34.

Yahoo! Inc. v. LICRA and UEJF, 433 F.3d 1199 (9th Cir. 2006).

Literatura

Azzi A.
2018 *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, „Journal of Intellectual Property, Information Technology & Electronical Commerce Law" nr 9/2.

Curtiss T.
2016 *Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies,* „Washington Journal of Law, Technology & Arts", nr 12.

Daskal J.
2018 *Google Inc. v. Equustek Solutions Inc.*, „American Journal of International Law", nr 112.

de Hert P., Czerniawski M.
2016 *Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context*, „International Data Privacy Law", nr 6/3.

Edoardo C., Fabbrini F.
2020 *EU Data Protection Law between Extraterritoriality and Sovereignty,* [w:] *Data Protection Beyond Borders*, red. F. Fabbrini, E. Celeste, J. Quinn.

Ford R. T.
1999 *Law's Territory (A History of Jurisdiction)*, „Michigan Law Review", nr 97.

Greze B.
2019 *The Extra-Territorial Enforcement of the GDPR: a Genuine Issue and the Quest for Alternatives*, „International Data Privacy Law", nr 9/2.

Höglund W.
2019 *Exporting Data Protection Law. The Extraterritorial Reach of the GDPR.*

Jovanovic S.
2020 *Governing the Internet: The Extraterritorial Effects of the General Data Protection Regulation.*

Lutzi T.
2017 *Internet Cases in EU Private International Law: Developing a Coherent Approach International and Comparative,* „Law Quarterly", nr 66 (3).

Mannion C.
2021 *Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets*, „Vanderbilt Law Review", nr 53.

Pramesti I., Afriansyah A.
2020 *Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia 3rd International Conference on Law and Governance (ICLAVE 2019)*, Atlantis Press.

Rosentau M.
2018 *The General Data Protection Regulation and its Violation of EU Treaties*, „Juridica International", nr 27.

Ryngaert C., Taylor M.
2020 *The GDPR As Global Data Protection Regulation?*, „American Journal of International Law", nr 114.

Schultz T.
2008 *Carving up the Internet: Jurisdiction, Legal Orders and the Private/Public International Law Interface*, „European Journal of International Law", nr 19 (4).

Simmons B. A., Hulvey R. A.
2022 *Cyberborders: Exercising State Sovereignty Online*, „Temple Law Review", nr 95.

Svantesson D. J. B.
2015 *Extraterritoriality and Targeting in EU Data Privacy Law: the Weak Spot Undermining the Regulation*, „International Data Privacy Law", nr 5 (4).

Tene O., Wolf C.
2013 *Overextended: Jurisdiction and Applicable Law Under the EU General Data Protection Regulation*, Future of Privacy Forum White Paper.

Thorhauer N.
2015 *Conflicts of Jurisdiction in Crossborder Criminal Cases in the Area of Freedom, Security, and Justice Risks and Opportunities from an Individual Rights-Oriented Perspective*, „New Journal of European Criminal Law", nr 6.

Van Alsenoy B.
2017 *Reconciling the (Extra) Territorial Reach of the GDPR with Public International Law*, [w:] *Data Protection and Privacy under Pressure. Transatlantic Tensions, EU Surveillance, and Big Data*, red. Vermeulen G., Lievens E., Maklu-Publishers Antwerp.

Vatanparast R.
2020 *Data governance and the Elasticity of Sovereignty*, „Brooklyn Journal of International Law", nr 46.

Źródła internetowe

Goldman E.
2017 *US Court Protects Google From Canadian Court's Delisting Order–Google v. Equustek*, https://blog.ericgoldman.org/archives/2017/11/us-court

-protects-google-from-canadian-courts-delisting-order-google-v-equustek.htm, [dostęp 10.03.2024].

Opinia Rzecznika Generalnego

2019 *Opinia Rzecznika Generalnego Macieja Szpunara przedstawiona w dniu 10 stycznia 2019 r. (1), Sprawa C-507/17 Google LLC, która wstąpiła w prawa Google Inc. przeciwko Commission nationale de l'informatique et des libertés (CNIL), przy udziale Wikimedia Foundation Inc. Fondation pour la liberté de la presse, Microsoft Corp., Reporters Committee for Freedom of the Press i in., Article 19 i in., Internet Freedom Foundation i in., Défenseur des droits [wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Conseil d'État (rada państwa, Francja)]*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=209688&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=142762, [dostęp: 12.03.2024].

United Nations Conference on Trade and Development (UNCTAD)

2021 *Data Protection and Privacy Legislation Worldwide*, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, [dostęp: 10.03.2024].

OLGA SŁOMIŃSKA

TRANSFER DANYCH OSOBOWYCH W TRANSGRANICZNYCH PRZEJĘCIACH SPÓŁEK

WSTĘP

Celem niniejszej pracy jest analiza zagadnień prawnych dotyczących transferu danych osobowych w kontekście transakcji przejęć o wymiarze transgranicznym. Współcześnie, obserwowalny wzrost liczby produktów sieciowych przyczynił się do zwiększenia ilości danych i ich potencjalnej wartości zarówno dla przedsiębiorców, jak i konsumentów, sprzyjając konkurencyjności i innowacyjności oraz zapewniając zrównoważony wzrost gospodarczy[1]. Nadto, jako że coraz więcej przedsiębiorców działa globalnie, czy to poprzez rozwijanie działalności poza granicami kraju, świadczenie usług internetowych bądź prowadzenie handlu elektronicznego, przechowywanie i przekazywanie danych nabiera często charakteru międzynarodowego (Juliussen, Kozyri, Johansen, Rui 2023, s. 2). W odpowiedzi na to prawodawca unijny, podążając za ogólną tendencją ustawodawczą do stałego zwiększania poziomu ochrony prywatności, pochylił się nad kwestią zapewnienia bezpieczeństwa danych osobowych w kontekście transgranicznych transakcji przejęć. Dane objęte tą ochroną mają szeroki zakres, mogą dotyczyć w szczególności pracowników, kontrahentów czy klientów stron transakcji i pozostają wobec tego w sferze zainteresowania wielu jednostek powiązanych z działalnością danej spółki. W tym zmieniającym się krajobrazie wyłoniła się potrzeba regulacji, która zapewni osobom fizycznym odpowiedni poziom prywatności, nie zniechęcając jednocześnie potencjalnych zagranicznych inwestorów

[1] Motywy rozporządzenia PE i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych).

i nie wstrzymując korzystnych dla gospodarki transferów o wymiarze międzynarodowym poprzez zbyt uciążliwe i zbiurokratyzowane procedury ochrony danych.

W tym kontekście szczególne znaczenie dla przedsiębiorców nabrało rozporządzenie PE i Rady z 27 kwietnia 2016 r. 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych („Rozporządzenie"), które uregulowało większość kwestii związanych z przekazywaniem danych do państw z, a także spoza Europejskiego Obszaru Gospodarczego („EOG"). W porównaniu do obowiązującej wcześniej Dyrektywy 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, która utraciła moc z dniem 25 maja 2018 roku, Rozporządzenie zdaje się jeszcze skuteczniej harmonizować rozwiązania unijne w zakresie ochrony danych osobowych. Obejmuje ono szerszy krąg możliwych scenariuszy i precyzyjniej określa przesłanki legalnego dokonania czynności transferowych (Akintunde 2017, s. 33). Dzięki temu zapewnia ono jeszcze większą przewidywalność, a tym samym możliwość oceny ryzyka transakcyjnego, zarówno w relacjach biznesowych zamykających się w granicach Unii Europejskiej, jak i z inwestorami z krajów trzecich. W zakresie danych funkcjonujących w gospodarce cyfrowej jego postanowienia uzupełniać będzie rozporządzenie PE i Rady 13 grudnia 2023 r. 2023/2854 w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania, które jednak stosowane będzie dopiero od 12 września 2025 roku.

Przez wzgląd na możliwe komplikacje wynikające z głębokich różnic w środowiskach regulacyjnych państw EOG oraz państw spoza tego obszaru, a także wysokie kary pieniężne, jakie mogą zostać nałożone na przedsiębiorców przekazujących dane bez odpowiedniej podstawy prawnej, w Rozporządzeniu rozwinięto szereg rozwiązań pozwalających na ograniczenie ryzyk transakcyjnych związanych z ochroną danych osobowych omówionych w dalszej części pracy, w tym w szczególności wprowadzenie ogólnego zakazu przekazywania zgromadzonych danych osobowych do innych podmiotów, wskazanie katalogu przesłanek wyłącznie na podstawie których możliwy jest transfer danych oraz wprowadzenie dodatkowych wymogów w przypadku transakcji z udziałem podmiotów trzecich, jak wprowadzenie wiążących reguł korporacyjnych, standardowych klauzul umownych, kodeksów postępowania oraz mechanizmów certyfikacji. Niniejszy artykuł zmierza do oceny, na ile przewidziane mechanizmy pozwalają na poszanowanie standardów unijnych w dziedzinie ochrony danych osobowych w transakcjach

o międzynarodowym elemencie, a także czy na jakimś polu potrzebna jest zmiana legislacyjna celem dalszego zmniejszania występujących ryzyk.

Metodami badawczymi przyjętymi na potrzeby niniejszej pracy jest przede wszystkim metoda dogmatyczna, opierająca się na analizie treści obowiązującego prawa unijnego, a także skupiającej się wokół niego literaturze i orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej oraz polskiego sądownictwa powszechnego. Przedmiot zainteresowania stanowić będą przede wszystkim te regulacje z dziedziny ochrony danych osobowych, które mogą znaleźć zastosowanie w przypadku przejęć spółek, a w szczególności zbycia aktywów przedsiębiorstwa. Przyjęta metoda uzasadnia systematykę pracy, w której kolejne rozdziały wyodrębnione zostały według różnych środowisk regulacyjnych uzależnionych od pochodzenia zaangażowanych w transakcję podmiotów bądź to z Unii Europejskiej bądź państw trzecich. Metoda ta uzupełniona zostanie wnioskami z praktyki stosowania prawa w krajach unijnych. Przedmiotowe regulacje zostaną więc omówione w szerszym kontekście bieżących praktyk rynkowych, tak by ocenić na ile odpowiadają one rzeczywistym potrzebom podmiotów gospodarczych, a na ile jawi się potrzeba zmian w ustawodawstwie unijnym.

ZNACZENIE OCHRONY DANYCH OSOBOWYCH NA TLE PRZEJĘĆ SPÓŁEK

Sprzedaż udziałów w spółce

Wpierw należy podkreślić, iż pod pojęciem przejęć spółek można rozumieć techniki integracji podmiotów gospodarczych, polegające albo na bezpośrednim przeniesieniu własności lub innego tytułu prawnego do przedsiębiorstwa (transakcja asset deal), albo na nabyciu udziałów lub akcji w spółce uprawnionej do przedsiębiorstwa (transakcja *share deal*) (Keler 2021). Rozróżnienie to determinuje zakres obowiązków na tle przepisów o ochronie danych osobowych. W przypadku sprzedaży udziałów następuje przeniesienie własności nad spółką, która jest właścicielem danych niezbędnych do dalszego prowadzenia działalności gospodarczej i które spółka ta zobowiązana jest zachować na mocy prawa. Oznacza to, że w przypadku przejęcia poprzez sprzedaż udziałów dane pozostają w spółce docelowej i administratorem danych pozostaje ten sam podmiot, a jedynie zmienia się jego struktura własnościowa (Molle, Pfarr 2022, s. 4). Sądy krajowe potwierdzają, iż obowiązki na tle Rozporządzenia nie aktualizują się, gdy formalnie zmiana administratora danych nie następuje (Gambini, Stefanini

2017). Transakcje typu *share deal* co do zasady pozostają więc bez wpływu na obowiązki wynikające z ochrony danych osobowych, chyba że w stosunkach zobowiązaniowych wprowadzone zostały szczególne klauzule nakładające na podmiot przejmowany określone obowiązki notyfikacyjne. Ten rodzaj transakcji kwalifikowanych pod pojęciem fuzji i przejęć pozostaje więc poza zakresem dalszych rozważań.

Sprzedaż aktywów spółki

Inaczej kształtuje się otoczenie regulacyjne w przypadku transakcji sprzedaży aktywów, wśród których kluczowe miejsce zajmować mogą dane osobowe. Przy okazji tego rodzaju transakcji dochodzi do zmiany właściciela samych składników majątkowych konstytuujących przedsiębiorstwo lub jego zorganizowaną część (Paryś 2019). Wraz z przenoszeniem poszczególnych składników przedsiębiorstwa, w tym, zgodnie z art. 55^1 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny („k.c."), rzeczy ruchomych i nieruchomych, umów oraz wszelkich ksiąg i dokumentów związanych z prowadzeniem działalności gospodarczej, na które składać się mogą dane o stronach objętych nimi czynności prawnych, naturalnie dochodzi do przekazania innemu podmiotowi znacznej ilości danych osobowych. Również i wszelkiego rodzaju bazy danych zawierające dane osobowe kwalifikowane są jako zbiory poufne, które podlegają specjalnemu reżimowi ochrony w przypadku ich przekazywania[2]. Co więcej, choć załoga spółki *de lege* nie stanowi składniku przedsiębiorstwa zgodnie z k.c., a jej los prawny określa w prawie polskim odrębny art. 23^1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Morek 2023), w transakcjach typu *asset deal* co do zasady następuje przejście zakładu pracy lub jego części na nowego pracodawcę (Zielińska-Barłożek, Libiszewski, Dąbrowska 2017, s. 34), a w konsekwencji i przeniesienie wszystkich danych osobowych dotyczących kadry zarządzającej oraz pracowników spółki na nowego właściciela przedsiębiorstwa.

Dla wielu współczesnych przedsiębiorców gromadzenie i wymiana danych osobowych są wręcz podstawą ich działalności, w obliczu czego przyszłemu właścicielowi szczególnie zależy na nabyciu tych danych do spółki celowej w sposób całościowy, bezpieczny i w poszanowaniu dla praw osób trzecich (Funk 2017, s. 56). Wobec tego w transakcjach sprzedaży aktywów, ze względu na złożoność ich przedmiotu, przeniesienie aktywów oraz powiązanych z nimi danych

[2] Postanowienie Sądu Antymonopolowego z dnia 15 maja 1996 r., XVII Amz 1/96.

osobowych powinno być szczegółowo określone w umowie sprzedaży przedsiębiorstwa (Molle, Pfarr 2022, s. 4). Na gruncie polskiego prawa, zgodnie z art. 55^2 k.c., czynność prawna mająca za przedmiot przedsiębiorstwo obejmuje wszystko, co wchodzi w skład przedsiębiorstwa, chyba że co innego wynika z treści czynności prawnej albo z przepisów szczególnych. Oznacza to, że o ile nie uzgodniono inaczej, transakcja typu *asset deal* obejmie wszystkie aktywa przedsiębiorstwa i powiązane z nimi dane. Dzięki temu, o ile strony zamierzają objąć czynnością wszystkie składniki przedsiębiorstwa, nie muszą ich indywidualnie wyszczególniać w umowie[3]. Jeśli jednak chcą, aby określone grupy danych osobowych powiązane ze składnikami majątku przedsiębiorstwa pozostały u podmiotu sprzedającego, a nie przeszły na nowego właściciela, powinny one zostać wprost wskazane w umowie sprzedaży (Molle, Pfarr 2022, s. 5). Jest to jednak możliwe tylko o tyle, o ile ich wykluczenie nie przeszkodzi w kontynuowaniu działalności gospodarczej spółki w oparciu o otrzymaną część przedsiębiorstwa (Kuźmicka-Sulikowska 2023).

PRZEKAZYWANIE DANYCH OSOBOWYCH DO INNEGO PAŃSTWA W UNII EUROPEJSKIEJ

Podstawy przekazywania danych

Przekazanie danych osobowych do podmiotu przejmującego każdorazowo wymaga podstawy prawnej, która w zależności od okoliczności i zakresu transakcji opierać się może o różne modele. Art. 6 ust. 1 Rozporządzenia wskazuje, jakie rozwiązania można przyjąć, aby zapewnić zgodność z prawem przekazania danych. Choć katalog ten jest znacznie szerszy, przypadki, które zastosowanie znaleźć mogą dla transakcji objętych niniejszym artykułem zostały ujęte w punkcie a), b) i f) przepisu. Wśród nich wyróżnić można sytuację, gdy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych, gdy przetwarzanie jest niezbędne do wykonania umowy, bądź gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów. Wskazane przesłanki mają charakter samoistny, niezależny i równoważny (Piwowarczyk 2019, s. 112), żadnej z opcji nie jest więc prawnie przyznany szczególny priorytet. Ponadto wystarczająco jest, aby podmiot przekazujący dane spełnił co najmniej jeden z tych warunków, by prawidłowo przekazać dane do podmiotu

[3] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 17 maja 2017 r., I ACa 410/17.

nabywającego przedsiębiorstwo (Lubasz, Chomiczewski 2018). Należy omówić z osobna każdy z nich.

Zgoda osoby, której dane dotyczą

Pierwszym z przypadków jest gdy osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Pojęcie zgody zostało zdefiniowane w art. 4 pkt 11 Rozporządzenia, zgodnie z którym jest to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Oświadczenie dotyczące zgody powinno jasno wskazywać cel i zakres przetwarzania oraz podmiot, którego dotyczy, a także w sposób niebudzący wątpliwości wskazywać na udzielenie zgody (Fajgielski 2022, Nb 7). Nie jest tu wymagana określona forma prawna, dopuszcza się nawet złożenie jej *per facta concludentia* (Fajgielski 2022, Nb 7). W motywie 43 preambuły Rozporządzenia zaznaczono jednocześnie, iż zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne. W tym kontekście wskazuje się, iż indywidulane odnoszenie zgody do poszczególnych operacji przetwarzania będzie wymagane w sytuacjach wyjątkowych, uzasadnionych okolicznościami takimi jak udostępnianie danych innym podmiotom (Fajgielski 2022, Nb 10), co znalazłoby zastosowanie w przypadku zbycia przedsiębiorstwa na rzecz podmiotu trzeciego.

Uzyskanie zgody na przetwarzanie danych wydaje się najprostszym rozwiązaniem, jako że zasadniczo nie budzi ono wątpliwości interpretacyjnych i nie wymaga dalszej argumentacji ze strony beneficjenta zgody. Jednak szerokie grono podmiotów, do których należałoby się zwrócić oraz równie szeroki zakres przetwarzania, jaki należałoby w niej wskazać, czynią to rozwiązanie wysoce niepraktycznym i raczej niestosowanym przy transakcjach przejęć. Trudność wynika również z faktu, iż uprzednia zbiorcza zgoda na przetwarzanie zazwyczaj zwykle nie spełnia wymogów Rozporządzenia (Molle, Pfarr 2022, s. 4). Dla wielu komentatorów podejście to jest niezasadne i nie uwzględnia rozmaitych relacji łączących podmioty administrujące danymi z podmiotami, których dane te dotyczą (Tene, Wolf 2013, s. 8). W praktyce gospodarczej obserwowana jest więc tendencja do wyrażania zgód z góry na całą serię umów wchodzących w skład określonych transakcji, tak by uniknąć zbędnych formalności prawnych i technicznych oraz kosztów (Lazaro, Metayer 2015, s. 808). Podnosi się bowiem, iż w takich

sytuacjach ryzyko dla podmiotów chronionych jest minimalne, a zgodę można by wyinterpretować w sposób dorozumiany (Lazaro, Metayer 2015, s. 808). Dążąc jednak do zachowania pełnej zgodności z intencją ustawodawcy, zgoda na przetwarzanie przeważnie stosowana jest tylko wtedy, gdy dotyczy jedynie kilku osób fizycznych, między innymi największych kontrahentów, których zgoda jest wymagana w celu przeniesienia zawartych z nimi umów gospodarczych na nabywcę, bądź w przypadku tzw. danych wrażliwych, dla których przekazywania zgoda jest każdorazowo wymagana przez art. 9 ust. 2 lit. a) Rozporządzenia (Ilan 2016, Nb 8).

Zawarcie lub wykonanie umowy

Drugim z przypadków jest gdy przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Jak zauważa się w literaturze, do wykonania umowy, w szczególności przenoszących własność nad przedsiębiorstwem, może być niezbędne przekazanie danych innemu administratorowi, co samo w sobie stanowić może podstawę udostępniania danych, podobnie jak wspomniana wcześniej zgoda (Fajgielski 2022, Nb 18). Podstawa ta obejmuje wszystkie etapy transakcji, zaczynając od wstępnych rozmów i negocjacji, a kończąc na rozliczeniach po zawarciu umowy (Mendyk 2019, s. 190). Zawierają się w tym zarówno działania zmierzające do zawarcia umowy, realizację wzajemnych zobowiązań stron umowy oraz dochodzenie roszczeń z tytułu niewykonania bądź nienależytego wykonania umowy (Fajgielski 2022, Nb 17). Zakres danych, jakie są wymagane, zależy od charakteru oraz znaczenia umowy[4]. Niekiedy wystarczające są podstawowe informacje identyfikujące osobę, której dane dotyczą, na potrzeby powołania stron umowy czy zaadresowania pisma, w innych zaś przypadkach zakres danych potrzebnych do wykonania umowy może być szerszy i obejmować różnorodne dane osobowe (Fajgielski 2022, Nb 17). Najczęściej właśnie ta przesłanka stanowić będzie podstawę do przekazywania danych w ramach transakcji (Fritsche, Mann, Wehlage 2022, Nb 3). Choć jej zastosowanie wydaje się potencjalnie problematyczne już na etapie *due dilligence*, stosunkowo łatwo jest uzasadnić przekazywanie danych, gdy wynika ono z konkretnej umowy sprzedaży przedsiębiorstwa, do której wykonania zmierzają strony.

Uzasadnione interesy administratora danych

[4] Wyrok Naszelnego Sądu Administracyjnego z 19 grudnia 2001 r., II SA 2869/00.

Trzecim z przypadków jest gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych. Klauzula ta nazywana jest w skrócie „klauzulą prawnie uzasadnionych interesów" (Fajgielski 2022, Nb 28). Zamierzeniem prawodawcy unijnego było to, by pomimo braku wystąpienia innych podstaw możliwe było dokonanie przekazania w celu realizacji szczególnego, prawnie usprawiedliwionego celu (Fajgielski 2022, Nb 29). W przypadku przejęć spółek interesem podmiotów przetwarzających są interesy ekonomiczne stron w przeprowadzeniu transakcji (Neumeier 2020, s. 291). Choć przesłanka ta, ze względu na swoją elastyczność, wydaje się najprostsza do zastosowania, w rzeczywistości nakłada ona na podmiot przekazujący dużą odpowiedzialność w kwestii uzasadnienia celu przetwarzania oraz jego wpływu na osoby fizyczne, a także równowagi między tymi aspektami[5].

Rozporządzenie nie określa, co należy rozumieć pod pojęciem interesu administratora, można więc go rozumieć jako każdą korzyść, którą może on uzyskać (Puyraimond 2019, s. 14), w tym, *lege non distinguente*, sprzedaż składników majątkowych. Przykładowo, w motywie 48 preambuły Rozporządzenia wskazano, że administratorzy, którzy są częścią grupy przedsiębiorstw mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach tej grupy dla wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników. Podobnie wskazuje się, iż sprzedaż przedsiębiorstwa może stanowić uzasadniony interes dla przekazania danych podmiotom trzecim, szczególnie w zakresie w jakim obejmuje dane niewrażliwe (Nauwelaerts 2004, s. 41). W praktyce transakcyjnej podstawa ta powoływana jest powszechnie dla uzasadnienia przekazywania danych na etapie *due dilligence*, chroniąc interesy stron, którym zależy na zbudowaniu przyszłych relacji w oparciu o wiarygodne i precyzyjne dane (Fritsche, Mann, Wehlage 2022, Nb 2). Jednocześnie nie są na nie nałożone zbyt daleko idące obowiązki formalne, co jest o tyle sprzyjające, że strony nie wiedzą jeszcze, czy dojdzie do przeprowadzenia transakcji i faktycznego przekazania aktywów, a co za tym idzie przyjęcia na siebie konkretnych zobowiązań prawnych .

Nie można jednak pominąć wyjątku, zgodnie z którym podstawa ta nie można zostać zastosowana, jeżeli występują pewne nadrzędne interesy lub

[5] Information Commissioner's Office, UK GDPR guidance and resources: When can we rely on legitimate interests?, Cheshire 2024, s. 7.

podstawowe prawa i wolności osoby, której dane dotyczą. W praktyce przejęć każdorazowo dojdzie do pewnego rodzaju konfliktu interesów, w którym sprzedającemu i kupującemu zależy na jak najrzetelniejszym i najwiarygodniejszym przedstawieniu przedsiębiorstwa celowego w zamiarze zamknięcia transakcji na celnie określonych warunkach, natomiast klientom, kontrahentom i pracownikom sprzedającego na tym, by ich dane były ujawniane podmiotom trzecim jak najrzadziej, w jak najmniejszym zakresie i w jak najbezpieczniejszy sposób. Należy tu zaznaczyć, że w praktyce orzeczniczej sądów europejskich i krajowych interesy niemajątkowe, w tym możliwe interesy zainteresowanych osób fizycznych, generalnie uznawane są za przeważające nad interesami natury czysto majątkowej (Puyraimond 2019, s. 18). W obliczu powyższego, choć powołanie się na tą przesłankę wykazuje dużą łatwość, równie łatwo może zostać ona obalona przez zaangażowane osoby fizyczne, narażając strony transakcji na kary grzywny oraz inne konsekwencje prawne związane z przekazywaniem danych bez właściwej podstawy prawnej.

Zakres przekazywanych danych

Mając na względzie powyższe podstawy przetwarzania nie można zapomnieć, iż zgodnie z art. 5 ust. 1 lit. c) Rozporządzenia, zakres przekazywanych danych powinien pozostać adekwatny, stosowny i ograniczony do tego, co niezbędne do celów przekazywania. Mając na uwadze powyższe, w zależności od tego na jakim etapie znajduje się transakcja, inny zakres danych może podlegać przekazaniu. Inne dane okażą się więc niezbędne dla celów sporządzania dokumentacji transakcyjnej, a inne dla zamknięcia transakcji. Przykładowo, potencjalny nabywca nie potrzebuje już na etapie badania *due dilligence* dostępu do wszelkich baz klientów, w tym informacji o dostawcach, klientach czy pracownikach spółki celowej, chyba że są one kluczowe dla podjęcia decyzji o zakupie. Strony powinny więc uzgodnić wpierw, jaka dokumentacja rzeczywiście pozostają relewantna dla ustalenia warunków transakcji, tak by uniknąć często nieproporcjonalnej ilości pracy związanych z ich redakcją, a następnie poddać przekazywane dokumenty procesom anonimizacji czy pseudonomizacji w zakresie danych osobowych (Segain, Thomas-Sertillanges 2018, s. 50; Neumeier 2020, s. 297). W ten sposób zakres przekazywanych danych może zostać ograniczony do minimum, zaś kupujący zachowuje możliwość zapoznania się z kluczową dokumentacją przedsiębiorstwa, co godzi postanowienia Rozporządzenia chroniące prywatność osób fizycznych z możliwością realnej oceny kondycji spółki przejmowanej.

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTWA SPOZA UNII EUROPEJSKIEJ

Dodatkowe przesłanki przekazywania danych

Jak już zaznaczono, w ostatnich latach zaobserwować można postępujące procesy globalizacyjne, które obejmują również aktywność gospodarczą. W ramach tych procesów spółki coraz częściej rozszerzają swoją działalność o nowe obszary w innych państwach, również poza Unią Europejską, przejmując zagraniczne spółki lub przedsiębiorstwa i tworząc rozbudowane struktury organizacyjne. Coraz częściej dochodzi więc do sytuacji, w której przedsiębiorca prowadzi działalność nawet i na kilku kontynentach, co pociąga za sobą konieczność transferu danych osobowych między jednostkami organizacyjnymi ulokowanymi na poszczególnych terytoriach (Fajgielski 2022, Nb 5). Potwierdzają to badania, zgodnie z którymi w ostatnich latach aż ponad 70% spółek założonych w Unii Europejskiej przekazuje dane do państw trzecich[6]. Współcześnie więc kwestia transferu danych poza obszar EOG pozostaje praktycznie nierozłączna z każdym przedsięwzięciem gospodarczym natury transgranicznej.

W przypadku transakcji zbycia aktywów do krajów poza EOG, prócz wymogu wskazania ważnej podstawy prawnej do transferu, na spółki zostały nałożone również dalej idące ograniczenia i obowiązki. Ta przezorność ustawodawcy unijnego wynika przede wszystkim z narastających w ostatnich latach obaw odnośnie poszanowania praw obywateli Unii Europejskiej w przypadku, gdy ich dane są przekazywane lub przetwarzane przez państwa spoza jej obszaru, o innych standardach bezpieczeństwa i ochrony prywatności, między innymi w związku z coraz częstszymi przypadkami nadużycia danych przez spółki działające w przestrzeni internetowej (Kuner 2023, s. 1). Dążąc do pogodzenia interesów osób fizycznych oraz podmiotów prowadzących działalność gospodarczą, w Rozporządzeniu, podobnie jak na gruncie poprzednio obowiązującej dyrektywy, przyjęto metodę regulacji, zgodnie z którą przekazywanie danych poza EOG jest generalnie zakazane, choć przewidziane są od tego wyjątki (Vrbljanac 2018 , s. 352). W przypadku gdy nie została wydana decyzja stwierdzająca odpowiedni poziom ochrony danych w odniesieniu do danego kraju trzeciego, warunki te można spełnić w drodze wdrożenia różnych przewidzianych środków prawnych,

[6] Statista, *Share of companies that transfer data from EU to other countries in 2021,* https://www.statista.com/statistics/1172995/data-transfer-from-the-eu [dostęp: 01.03.2024].

w tym wprowadzenia wiążących reguł korporacyjnych, standardowych klauzul umownych, kodeksów postępowania, mechanizmów certyfikacji.

Wiążące reguły korporacyjne

Pierwszym przypadkiem jest wprowadzenie wiążących reguł korporacyjnych na podstawie art. 47 Rozporządzenia. Zgodnie z definicją z art. 4 pkt 20 Rozporządzenia wiążące reguły korporacyjne to polityki ochrony danych osobowych stosowane przy jednorazowym lub wielokrotnym przekazaniu danych osobowych podmiotowi w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą. Polityki przyjmowane są wewnętrznie przez międzynarodowe koncerny w celu jednolitego przestrzegania zasad ochrony danych przez podmioty zależne we wszystkich krajach (Drobek 2018, Nb 1). Z tego względu rozwiązanie to będzie najskuteczniejsze w przypadku transakcji ze spółkami wchodzącymi w skład tych samych struktur korporacyjnych i zasadniczo nie znajdzie zastosowania do transferów do podmiotów spoza grupy (Öztürk 2022, s. 19). Należy jednak podkreślić, iż ze względu na swoją strukturę, złożoność i wysokie koszty, w praktyce wiążące reguły korporacyjne są prawie wyłącznie wykorzystywane przez duże międzynarodowe korporacje działające w wielu jurysdykcjach (McCann, Patel, Ruiz 2020, s. 7), w tym największe instytucje finansowe, koncerny przemysłowe, telekomunikacyjne, firmy sektora farmaceutycznego czy IT (Rojszczak 2019).

Zgodnie z kryteriami zatwierdzenia wskazanymi w art. 47 ust. 1 Rozporządzenia, reguły te muszą być prawnie wiążące oraz mieć zastosowanie i być egzekwowane przez każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w tym ich pracowników. Wiążące reguły korporacyjne muszą również wyraźnie przyznawać osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych (Drobek 2018, Nb 4). Wiążący charakter reguł może być osiągnięty w szczególności poprzez jednostronne zobowiązania, o ile w danym systemie będzie to prawnie skuteczne, zawarcie umowy wewnątrzgrupowej, której postanowienia nakładać będą na członków odpowiednie obowiązki, bądź zastosowanie innych instrumentów, które umożliwią osiągnięcie podobnych skutków prawnych (Drobek 2018, Nb 4). Przedmiotem oceny ze strony organu nadzoru nie jest jednak pojedyncza umowa łącząca dwie strony, ale zestaw wszelkich właściwych w tej dziedzinie dokumentów korporacyjnych wiążących i stosowanych w obrębie określonej grupy kapitałowej (Rojszczak 2019).

Jeżeli dane przekazywane są pomiędzy odrębnymi grupami przedsiębiorstw, z których każda posiada już posiada własne wiążące reguły korporacyjne, zatwierdzone przez odpowiednie organy nadzorcze, nie jest wymagane ponowne przeprowadzenie procedury autoryzacji na operacje transferu danych pomiędzy nimi (Karwala 2018, Nb 9).

Standardowe klauzule umowne

Drugim przypadkiem jest posłużenie się standardowymi klauzulami umownymi przyjętymi lub zatwierdzonymi przez Komisję. Mechanizm ten bazuje na doświadczeniach wypracowanych na forum innych organizacji międzynarodowych, takich jak Międzynarodowa Izba Handlowa, Organizacja Współpracy Gospodarczej i Rozwoju czy Rada Europy (Fisher, Karwala 2007, s. 16). W dniu 4 czerwca 2021 r. Komisja wydała zmodernizowane standardowe klauzule umowne dotyczące przekazywania danych przez ich administratorów z Unii Europejskiej do państw poza nią. Zgodnie z motywem 10 tej decyzji, standardowe klauzule umowne określone w załączniku łączą klauzule ogólne z podejściem modułowym, aby uwzględnić różne scenariusze przekazywania danych i złożoność współczesnych łańcuchów przetwarzania, w oparciu o to między jakimi podmiotami następuje przekazywanie. Oprócz klauzul ogólnych podmioty przetwarzające powinni wybrać moduł mający zastosowanie do ich sytuacji, aby dostosować obowiązki spoczywające na nich na mocy standardowych klauzul umownych do roli i obowiązków, jakie pełnią w związku z przedmiotowym przetwarzaniem danych.

Standardowe klauzule umowne mogą być oddzielnym dokumentem lub mogą zostać włączone do umowy głównej między stronami transakcji, z poszanowaniem dla zachowania ich treści określonej w akcie prawnym (Szurmak 2023, Nb 8). Rozwiązanie to jest uważane za jedno z najbardziej efektywnych metod przekazywania danych poza EOG dla każdego rodzaju transakcji, ponieważ nie wymaga od stron ani złożonych działań autorskich ani dalszych procedur autoryzacyjnych (Vrbljanac 2018, s. 345), ograniczając ponoszone przez nie koszty około-transakcyjne i sprowadzając się jedynie do zidentyfikowania właściwego modelu transferu danych. Zapewnia mu to cenioną na rynku przewidywalność, przejrzystość oraz dostępność (Cory, Dick 2020, Nb 4). Potwierdzają to wyniki badań, zgodnie z którymi w ostatnich latach konsekwentnie standardowe klauzule umowne pozostają najpopularniejszym wśród przedsiębiorców sposobem na transfer danych do krajów spoza EOG (Öztürk 2022, s. 16).

Kodeks postępowania

Trzecim przypadkiem jest zatwierdzenie kodeksu postępowania na podstawie art. 40 Rozporządzenia, wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Pojęcie „kodeks postępowania" nie zostało zdefiniowane w Rozporządzeniu, choć przepis art. 40 ust. 1 wskazuje, iż są to dokumenty, które mają pomóc we właściwym stosowaniu Rozporządzenia. Nie stanowią one jednak aktów prawa powszechnie obowiązującego, mają charakter tzw. samoregulacji, a więc dobrowolnych zobowiązań podmiotów, które przyjmują dany kodeks postępowania (Fajgielski 2022, Nb 4). Z reguły kodeksy postępowań mają charakter niewiążącego instrumentu o znaczeniu głównie informacyjnym, jednakże pod rządami Rozporządzenia podmioty, które je przyjmują, jednocześnie zobowiązują się do stosowania i podlegają wszelkim konsekwencjom w przypadku naruszenia postanowień kodeksu (Góral, Makowski 2018, Nb 3). Spośród możliwych rozwiązań, nie obserwuje się raczej praktycznych przykładów stosowania kodeksów postępowania dla celów transferu danych osobowych, w tym transferów na potrzeby zbycia przedsiębiorstwa do państwa trzeciego.

Mechanizm certyfikacji

Czwartym przypadkiem jest zatwierdzenie mechanizmu certyfikacji zgodnie z art. 42 Rozporządzenia wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Choć Rozporządzenie nie wprowadza definicji certyfikacji, zgodnie z normami Międzynarodowej Organizacji Normalizacyjnej w Genewie (ISO), oznacza ona poświadczenie przez niezależny podmiot, wydane w formie pisemnego zapewnienia, że dany produkt, usługa lub system spełniają określone wymagania, np. odpowiednie normy prawne lub techniczne (Drobek, Makowski 2018, Nb 2). Ich przedmiotem może być zarówno pojedyncza operacja transferu, jak i zestaw operacji[7]. Zastosowane mechanizmy certyfikacji muszą być uzupełnione o przyjęte przez podmioty przetwarzające w drodze umowy lub innego prawnego instrumentu wiążące i możliwe do wyegzekwowania zobowiązania

[7] European Data Protection Board, Guidelines 07/2022 on certification as a tool for transfers, Bruksela 2022, s. 9.

(Drobek, Makowski 2018, Nb 3). Może to nastąpić w drodze umowy wiążącej podmiot przekazujący z podmiotem docelowym, zarówno już istniejącej jak i zawartej odrębnie na potrzeby uregulowania kwestii przekazywania danych, co zdaje się być najpowszechniejszym rozwiązaniem, ale i innych instrumentów wywierających zbliżone skutki[8].

W różnych państwach europejskich to właśnie organy ochrony danych osobowych prowadzą programy certyfikacyjne, choć możliwe jest również powierzenia tego zdania specjalnym podmiotom certyfikującym (Drobek, Makowski 2018, Nb 6). Chociaż uzyskanie certyfikatu przez podmiot nabywający właściwie gwarantuje zgodność z prawem transferu i znacznie zwiększa bezpieczeństwo transakcji, przechodzenie przez złożoną procedurę jego uzyskania na potrzeby pojedynczej transakcji wydaje się zbyt dużym zaangażowaniem w porównaniu do pozostałych metod przewidzianych w Rozporządzeniu. Z drugiej jednak strony może ona przynosić długofalowe korzyści dla posiadającego go podmiotu, budując wizerunek przedsiębiorcy w oparciu o poszanowanie dla standardów unijnych i przekładając się na większe zaufanie wśród przyszłych kontrahentów, zarówno na potrzeby kolejnych transakcji, jak i bieżącej działalności gospodarczej.

Decyzja wykonawcza

W poszczególnych przypadkach, działając na podstawie art. 45 ust. 3 Rozporządzenia Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że w oparciu o wszechstronną analizę porządku prawnego państwa trzeciego, państwo to daje gwarancje zapewniające stopień ochrony „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii Europejskiej. Wówczas przekazywanie danych na potrzeby transakcji może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Za Trybunałem Sprawiedliwości należy podkreślić, iż nie oznacza to konieczności stwierdzenia identycznego stopnia ochrony pod względem środków, jakie państwo trzecie stosuje, o ile w praktyce skutecznie zapewniają one odpowiedni stopień ochrony, tj. czy biorąc pod uwagę istotę prawa do prywatności oraz jego skuteczne wprowadzenie w życie, egzekwowanie i nadzór nad jego przestrzeganiem, dany zagraniczny system zapewnia jako całość wymagany stopień ochrony[9]. Okresowo przeprowadza się w takim państwie

[8] Ibidem, s. 16.

[9] Wyrok Trybunału Sprawiedliwości z dnia 7 października 2015 r. w sprawie C-362/14, Maximilian Schrems/Data Protection Commissioner.

przegląd uwzględniający wszelkie mające znaczenia zmiany, a także, gdy ma to zastosowanie, wskazany zostaje właściwy organ lub organy nadzorcze.

Tytułem przykładu, w odniesieniu do przekazywania danych z Unii Europejskiej do Stanów Zjednoczonych Komisja Europejska przyjęła decyzję wykonawczą 2023/1795 z dnia 10 lipca 2023 r., stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA. Czyniąc to, Komisja zdecydowała, że Stany Zjednoczone zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z Unii Europejskiej do organizacji w Stanach Zjednoczonych, które są ujęte w "Wykazie ram prywatności danych", prowadzonym i udostępnianym publicznie przez Departament Handlu Stanów Zjednoczonych, zgodnie z załącznikiem I do decyzji (Talus 2023, s. 1). Zmiana ta była wysoce oczekiwana przez spółki amerykańskie, które często polegały na transatlantyckich transferach danych osobowych, nie tylko w ramach inwestycji zagranicznych, ale i w celu prowadzenia działalności internetowej, czy współpracy z podmiotami zależnymi lub powiązanymi w krajach europejskich (Cogan 2023, s. 348). Podobnie postąpiono w przypadku Japonii w decyzji z dnia 23 stycznia 2019 r., Zjednoczonego Królestwa w decyzji z dnia 28 czerwca 2021 r. oraz Republiki Korei w decyzji z dnia 17 grudnia 2021 r. Dla spółek planujących transakcję oznacza to, że pomimo transferu do jednego z powyższych państw trzecich nie będą musiały spełniać dodatkowych wymogów administracyjnych (McCann, Patel, Ruiz 2020, s. 6).

WNIOSKI

Analiza przytoczonych postanowień Rozporządzenia stanowiących kontynuację, a niekiedy i rozbudowanie rozwiązań przyjętych już wcześniej na gruncie obowiązującej do 2018 roku dyrektywy unijnej prowadzi do wniosku, iż obejmują one bardzo szeroki zakres możliwych konfiguracji podmiotowych i przedmiotowych składających się na operacje transferowe natury ponadnarodowej. Mając na uwadze spodziewany dalszy wzrost globalizacji oraz rozwoju technologii bazujących na wszelkich kategoriach danych, można oczekiwać, iż przepisy te będą dalej dostosowywane, tak by zapewnić zainteresowanym podmiotom należyty poziom ochrony prywatności niezależnie od tego, w jakim kraju się znajduje i z jakimi przedsiębiorstwami wchodzi w interakcję. Fakt iż najchętniej wybieranym przez podmioty handlowe rozwiązaniem pozostaje stosowanie standardowych klauzul umownych sugeruje, iż preferowane są metody najsilniej ujednolicone i wymagające jak najmniejszej ingerencji i zaangażowania czasowego oraz

finansowego ze strony tych podmiotów, które mogą wobec tego skupić się na istotniejszych dla nich kwestiach ich bieżącej działalności. Pozwala to również założyć, iż to ta metoda poddawana będzie zmianom w pierwszej kolejności poprzez aktualizację treści klauzul.

Należy pamiętać, iż niezależnie od mechanizmów ochronnych przewidzianych w Rozporządzeniu, strony transakcji mogą zapewnić sobie zgodność z przepisami ochrony danych osobowych stosując wykształcone przez inne podmioty gospodarcze praktyki rynkowe, tak by dodatkowo zminimalizować ryzyko poniesienia bezpośrednich strat finansowych bądź utraty renomy w przypadku zajścia jakichkolwiek niezamierzonych naruszeń. W kontekście transakcji zbycia przedsiębiorstwa szczególną rolę zajmuje to przeprowadzanie na etapie planowania transakcji dokładnego badania *due dilligence* obejmującego procedury ochrony danych osobowych w dotychczasowej spółce, w tym narzędzi oraz systemów przechowywania i przetwarzania danych, którego wyniki odzwierciedlenie znajdą w treści umowy zbycia przedsiębiorstwa (Funk 2017, s. 56). Ponadto, powszechną praktyką jest zawieranie w umowie standardowych oświadczeń i zapewnień dotyczących przestrzegania przepisów o ochronie danych, które będą chroniły nabywcę w przypadku, gdy pewne przypadki nieprawidłowości nie zostaną wykryte nawet w ramach tych szczegółowych badań (Villedieu, Hanriot 2019, Nb 8).

W zależności od wyników badań *due dilligence* i zidentyfikowanego poziomu ryzyka strony mogą również zastosować należyte zabezpieczenia umowne, tak by zminimalizować zagrożenie pociągnięcia ich do odpowiedzialności za naruszenie przepisów ochrony danych osobowych. Naruszenia bowiem mogą zostać wykryte już po przejęciu spółki, a na gruncie prawa polskiego na podstawie art. 55^4 k.c. nabywca przedsiębiorstwa jest odpowiedzialny solidarnie ze zbywcą za jego zobowiązania związane z prowadzeniem przedsiębiorstwa. Poziom wprowadzonych do umowy zabezpieczeń, w tym wysokość możliwych kar, uzależnić mogą między innymi od branży, w jakiej działa dany podmiot (największe koszty w rezultacie naruszeń danych osobowych obserwuje się w sektorze ochrony zdrowia, finansowym i farmaceutycznym), czy państwa pochodzenia danego podmiotu (znacznie wyższe straty finansowe w związku z tymi naruszeniami odnotowywane są w Stanach Zjednoczonych, krajach Azji Środkowej i Kandzie niż w przypadku podmiotów działających w Unii Europejskiej)[10]. Wyniki badania mogą również przełożyć się na przyjęty sposób ustalenia ceny zakupu czy jej wysokość kwotową.

[10] International Business Machines Corporation, Cost of Data Breach Report 2023, s. 12-13.

Artykuł ten nie wyczerpuje wszystkich kwestii związanych z ochroną danych osobowych. Poza podstawą prawną przekazywania oraz dodatkowymi przesłankami w przypadku transferów poza unijnych, strony powinny mieć również na względzie sam sposób przekazywania danych osobowych na cele transakcji. Muszą w szczególności zadbać, by systemy, za pomocą których dane są przekazywane, w tym stosowane powszechnie *Virtual Data Rooms*, zapewniały bezpieczeństwo przechowanych w nich danych, mając przy tym na uwadze, że sam dostawca systemu jest podmiotem przetwarzającym dane, z którym należy zawrzeć umowę o przetwarzaniu (Neumeier 2020, s. 294). Na każdym etapie konieczne jest działanie z zachowaniem należytej staranności wymaganej przez podmioty profesjonalne, uwzględniającej wdrożenie odpowiednich środków technicznych i organizacyjnych (Sakowska-Baryła 2017, s. 878), które pozwolą na przeprowadzenie transferu w pełnej zgodności z prawem unijnym. Pozostaje to jednak materiałem na dalsze publikacje, które, w obliczu postępujących rozwiązań technologicznych i narzędzi automatyzacji towarzyszącym transakcjom handlowym wymagać będą stałej aktualizacji. Niewątpliwie towarzyszyć im będą zmiany regulacji prawnych próbujących nadążyć za coraz to nowszymi ryzykami grożącymi prywatności zawikłanych w nie osób fizycznych.

BIBLIOGRAFIA

Akty prawne

Motywy rozporządzenia PE i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych).

Orzecznictwo

Postanowienie Sądu Antymonopolowego z dnia 15 maja 1996 r., XVII Amz 1/96.

Wyrok Naszelnego Sądu Administracyjnego z 19 grudnia 2001 r., II SA 2869/00.

Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 17 maja 2017 r., I ACa 410/17.

Wyrok Trybunału Sprawiedliwości z dnia 7 października 2015 r. w sprawie C-362/14, Maximilian Schrems/Data Protection Commissioner.

Literatura

Akintunde S. E.
2017 *An Analysis of the General Data Protection Regulation (EU) 2016/679*, Lapland.

Cogan J. K.
2023 *The United States and the European Union Begin Implementation of the European Union-U.S. Data Privacy Framework*, „American Journal of International Law", nr 117/2.

Cory N., Dick E., Castro D.
2020 *The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade*, [w:] I*nformation Technology & Innovation Foundation,* Waszyngton.

Drobek P.
2018 *Komentarz do art. 47* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* red. E. Bielak-Jomaa, D. Lubasz, Warszawa.

Drobek P., Makowski P.
2018 *Komentarz do art. 42*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* red. E. Bielak-Jomaa, D. Lubasz, Warszawa.

European Data Protection Board, Guidelines 07/2022 on certification as a tool for transfers, Bruksela 2022.

Fajgielski P.
2022 [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa.

Fisher B., Karwala D.
2007 *Umowy transferowe jako instrument przekazywania danych osobowych do państw trzecich*, „Przegląd Prawa Handlowego", nr 10.

Fritsche S., Mann C., Wehlage K. K.
2022 *Corporate Transactions and the GDPR: Data Protection Obstacles in Due Dilligence and Asset Deals,* Hamburg.

Funk C.
2017 *Datenschutz in der M&A-Transaktion,* „*Kölner Schrift zum Wirtschaftsrecht*", nr 8(1-2).

Gambini L., Stefanini E.
2017 *New Consent for Processing Sensitive Data Not Needed After Change of Data Controller: Data Protection Thoughts and M&A*, Portolano Cavallo Studio Legale.

Góral U., Makowski P.
2018 Komentarz do art. 40, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa.

Ilan D.
2016 *Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities*, Harvard Law School Forum on Corporate Governance, Cambridge.

Information Commissioner's Office, UK GDPR guidance and resources: When can we rely on legitimate interests?, Cheshire 2024.

International Business Machines Corporation, Cost of Data Breach Report 2023.

Juliussen B. A., Kozyri E., Johansen D., Rui J. P.
2013 *The Third Country Problem under the GDPR: Enhancing Protection of Data Transfers with Technology*, „International Data Privacy Law", nr 13/3.

Karwala D.
2018 *Wiążące reguły korporacyjne – pojęcie, istota i korzyści z ich stosowania*, Warszawa.

Keler G.
2021 *Badanie due diligence w transakcjach fuzji i przejęć. Znaczenie i skutki prawne,* Warszawa.

Kuner C.
2023 *Protecting EU Data Outside EU Borders under the GDPR*, Kluwer Law International, Haga.

Kuźmicka-Sulikowska J.
2023 *Komentarz do art. 55(2)*, [w:] *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Warszawa.

Lazaro C., Le Metayer D.
2015 *Le consentement au traitement des données personnelles. Perspective comparative sur l'autonomie du sujet*, „La Revue juridique Thémis de l'Université de Montréal", nr 48-3.

Lubasz D., Chomiczewski W.
2018 *Komentarz do art. 6*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa.

McCann D., Patel O., Ruiz J.
2020 *The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision*, Londyn.

Mendyk B.
2019 *Wybrane problemy związane z wdrażaniem RODO: Podstawy przetwarzania danych*, „Życie Weterynaryjne", 94/3.

Molle A., Pfarr M. C.
2022 *Data Assets in M&A Transactions*, Berlin.

Morek R.
2023 *Komentarz do art. 55(1)*, [w:] *Kodeks cywilny. Komentarz*, red. K. Osajda, W. Borysiak, Warszawa.

Nauwelaerts W.
2004 *How EU data privacy affects due diligence*, IFLR, Londyn.

Neumeier N.
2020 *Datenschutzrechtliche Millionengeldbußen bedrohen die M&A Branche*, [w:] *Legal Revolutionary: Rechstmagazin in der digitalen Wirtschaft,* Frankfurt nad Menem.

Neumeier N.
2020 *Datenschutzrechtliche Millionengeldbußen bedrohen die M&A Branche*, [w:] *Legal Revolutionary: Rechstmagazin in der digitalen Wirtschaft,* Frankfurt nad Menem.

Paryś W.
2019 *Zakup a inne sposoby uzyskania własności przedsiębiorstwa lub jego zorganizowanej części*, [w:] *Nabycie przedsiębiorstwa lub jego zorganizowanej części: Praktyczne ujęcie prawne, bilansowe oraz podatkowe*, red. J. Jurasz Warszawa.

Piwowarczyk M.
2019 *Podstawy Prawne przetwarzania danych osobowych przez instytucje finansowe w przypadku braku zawarcia umowy*, „Folia Iuridica Universitatis Wratislaviensis", nr 8/1.

Puyraimond J. F.
2019 *L'intérêt légitime du responsable du traitement dans le RGPD: in cauda venenum?, „Droit de la consommation – DCCR*".

Rojszczak M.
2019 *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa.

Sakowska-Baryła M.
2017 *Przetwarzanie danych osobowych przez podmioty publiczne*, „Kontrola państwowa", nr 62/6.

Segain H., Thomas-Sertillanges J. B.
2018 *Opérations de M&A et protection des données personnelles: identifier et minimiser les risques*, „Fusions & Acquisitions Magazine", nr 5.

Szurmak P.
2023 *Zawieranie nowych standardowych klauzul umownych – praktyczne problemy*, Warszawa.

Talus A.
2023 *Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023*, Bruksela.

Tene O., Wolf C.,
2013 *The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent*, The Future of Privacy Forum, Waszyngton.

Villedieu A. L., Hanriot M.
2019 *La protection des données personnelles dans les opérations de fusion-acquisition,* CMS Francis Lefebvre Publications.

Vrbljanac D.
2018 *Personal Data Transfer to Third Countries – Disrupting the Even Flow*, „Athens Journal of Law", nr 4(4).

Zielińska-Barłożek I., Libiszewski K., Dąbrowska A.
2017 *Praktyczny przewodnik prawny po transakcjach fuzji i przejęć,* Warszawa.

Öztürk Ö.
2022 *Data Transfers out of the European Economic Area*, "Social Science Research Network".

Źródła internetowe

Statista, *Share of companies that transfer data from EU to other countries in 2021,* https://www.statista.com/statistics/1172995/data-transfer-from-the-eu [dostęp: 01.03.2024].

Karolina Kamila Gajewska

Uniwersytet Mikołaja Kopernika

Studentka

WPŁYW RODO NA FUNKCJONOWANIE PLIKÓW COOKIES

WPROWADZENIE

Wejście w życie 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 wywołało niemałe poruszenie. Zakres podmiotowy RODO obejmuje administratorów danych, podmioty przetwarzające dane oraz osoby, których dane dotyczą. Ponadto zasięg rozporządzenia ma charakter eksterytorialny, co oznacza, że przepisy mają zastosowanie także do podmiotów spoza Unii Europejskiej, o ile przetwarzają dane osób fizyczny zamieszkały na terenie państw UE. Akt prawny narzucił szereg zmian, a także wprowadził wiele nowości dotyczących ochrony danych osobowych na kilku płaszczyznach. Największa reorganizacja nastąpiła w obszarze prawa pracy i prawa bankowego, w związku z czym adaptacja nowych przepisów w świecie wirtualnym nie zyskała dużej popularności. W rezultacie, wciąż duża ilość internautów nie wie jak powinna wyglądać skuteczna ochrona danych osobowych w cyberprzestrzeni. Niestety nieświadomość użytkowników nie stanowi jedynego problemu. Problematyka ochrony danych osobowych w internecie jest bardziej złożona, ponieważ liczba sytuacji, w których dochodzi do naruszeń przepisów przez dostawców usług telekomunikacyjnych ciągle rośnie.

Głównym założeniem tej publikacji jest uzmysłowienie osobom korzystającym ze stron internetowych skali problemu poprzez ukazanie w jak szybki i prosty sposób oddają dostęp nieznanym usługodawcą do swoich danych osobowych, a także pokazanie jak powinna wyglądać witryna internetowa zgodna z założeniami RODO.

DEFINICJE

Dane osobowe, przetwarzanie

Na samym początku jednakże warto zwrócić uwagę, co dokładnie kryje się pod pojęciem danych osobowych. Zgodnie z art 4 pkt. 1 rozporządzenia, "dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[1]. Zatem jakiekolwiek informacje mogą być uznane za dane osobowe, gdy odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby. Dane osobowe obejmują informacje dotyczące prywatnego życia osoby (w tym działalności zawodowej), a także życia publicznego. Warto zauważyć, że RODO nie odnosi się do przetwarzania informacji anonimowych.

Należy podkreślić, iż każdy ma prawo do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania[2]. Ciekawym aspektem, jest to, iż prawo do ochrony danych osobowych nie jest prawem nieograniczonym. Zgodnie z art. 52 pkt.1 Karty praw podstawowych Unii Europejskiej wszelkie ograniczenia

[1] 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. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

[2] Karta praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 z późn. zm.).

w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Z pojęciem "dane osobowe" często występuje słowo "przetwarzanie", które oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[3]. Jednakże, nie wszystkie dane osobowe mogą być przetwarzane. Zgodnie z art. 9 pkt. 1 Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby[4]. Mimo to, rozporządzenie przewiduje pewne odstępstwa, które umożliwiają także przetwarzanie danych osobowych szczególnej kategorii. Między innymi należy do nich wyraźna zgoda osoby na przetwarzanie tych danych, czy też objęcie przetwarzaniem danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

Pliki cookies, polityka plików cookies, polityka prywatności

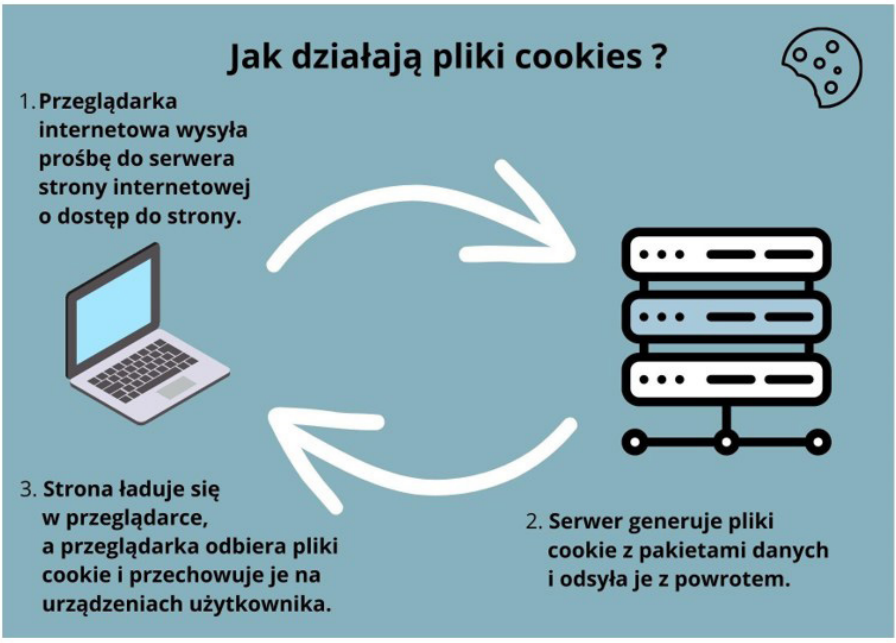
W pierwszej kolejności trzeba zauważyć, iż są to trzy zupełnie różne pojęcia i nie należy ich ze sobą mylić, a przede wszystkim nie wolno używać tego nazewnictwa zamiennie.

Pliki cookies, czyli ciasteczka to małe pliki, które są umieszczone na urządzeniu użytkownika przez przeglądarkę internetową. Przechowują one informacje o preferencjach użytkownika, które odnotowywane są na podstawie odwiedzanych przez niego stron internetowych. Ciasteczka mogą pełnić różne funkcje, takie jak zwiększenie komfortu korzystania z przeglądarki, ponieważ między innymi umożliwiają kontynuowanie sesji oraz optymalizację działania strony,

[3] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.
[4] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

a także są odpowiedzialne za dostarczanie spersonalizowanych reklam. Mogłoby się wydawać, że stanowią bardzo ważny i pomocny instrument. Jednakże, należy spojrzeć na to z innej perspektywy, ponieważ aby pliki cookies spełniały swoją podstawową rolę, potrzebują danych o użytkownikach. Dopóki internauta świadomie wyraża zgodę na taki proces i przysługuje mu prawo do odmowy to jest to zgodne z prawem, niestety niekoniecznie w każdym przypadku tak to wygląda. Kwestia dotycząca plików cookies zostały uregulowana w art. 173 ustawy Prawo telekomunikacyjne. Natomiast w przypadku ciasteczek, które wykorzystują dane osobowe oprócz przepisów Prawa telekomunikacyjnego należy też brać pod uwagę przepisy dotyczące ochrony danych osobowych, czyli tzw. RODO[5].

Polityka plików cookies to nic innego jak dokument, który określające zasady korzystania z plików cookies na stronie internetowej. Udostępnienia tego dokumentu przez właściciela strony internetowej jest jego obowiązkiem. Polityka cookies zazwyczaj zawiera informacje na temat rodzaju plików cookies używanych przez stronę, celu ich wykorzystania, czasu przechowywania oraz sposobu zarządzania nimi przez użytkowników.



Rysunek 1. Jak działają pliki cookies?
Źródło: *Opracowanie własne*

[5] Cookies – jak wdrożyć je zgodnie z prawem?, Creativa Legal, https://creativa.legal/cookies-jak-wdrozyc-je-zgodnie-z-prawem/, [dostęp: 10.02.2024].

Natomiast polityka prywatności zazwyczaj stanowi oddzielny dokument, który informuje o tym, jakie dane osobowe są zbierane i w jaki sposób są one wykorzystywane. Dodatkowo, polityka prywatności powinna także określić sposób w jaki użytkownik może zmienić, bądź też usunąć przekazane dane osobowe. Polityka prywatności ma kluczowe znaczenie dla budowania zaufania pomiędzy użytkownikiem a administratorem danych i często jest wymagana przez przepisy i regulacje prawne dotyczące prywatności.

WYMOGI DOTYCZĄCE FUNKCJONOWANIA PLIKÓW COOKIES

Aby strona internetowa prawidłowo przetwarzała dane osobowe i odpowiadała normom prawnym narzuconym przez unijne rozporządzenie o ochronie danych osobowych musi spełnić szereg wymogów, które zostały poniżej omówione krok po kroku. Podmiotem, który odpowiada za zgodne z prawem przetwarzanie danych jest administrator strony. Zgodnie z art. 4 "administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania[6].

Baner

Baner jest pierwszą rzeczą, która powinna pojawić się natychmiast po wejściu w witrynę internetową, która przetwarza dane. To nic innego jak panel informacyjny, który powinien być umiejscowiony w widocznym dla użytkownika miejscu, a także być zaprojektowany w sposób przejrzysty i łatwy do zauważenia przez każdego internautę. Kolory powinny być stonowane, a treść komunikatu nie może być skomplikowana. Niedopuszczalne jest stosowanie małych, nieczytelnych banerów. Baner przede wszystkim powinien zawierać:

- jasny komunikat, o tym, że strona używa plików cookies
- odnośnik do polityki cookies
- odnośnik do polityki prywatności

[6] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

- możliwość zarządzania ustawieniami cookies
- możliwość wyrażenia zgody, bądź odmowy na przetwarzanie plików cookies.

Ponadto projekt baneru powinien być także dostosowany do różnych rozmiarów ekranu, tak aby był łatwo zauważalny na każdym urządzeniu, niezależnie czy jest to komputer, tablet czy też smartfon. Zmiana ustawień dotycząca plików cookies także powinna być możliwa z samego banera, bez wymogu przechodzenia do nowej karty.

Zgoda

Zgodnie z art. 4 pkt. 1 rozporządzenia "zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych[7]. Oznacza to, iż wyrażenie zgody musi nastąpić przez wyraźne aktywne i świadome działanie użytkownika. Zamknięcie baneru nie może zostać uznane za akceptację plików cookies. Ponadto, użytkownik w każdym momencie powinien mieć możliwość rezygnacji, czyli cofnięcia zgody. Opcja ta powinna być łatwo dostępna do znalezienia przez internautę, natomiast sama strona powinna co jakiś czas prosić o odnowienie zgody. Poza samą zgodą, użytkownik powinien mieć prawo do odrzucenia wszystkich plików cookies, a także możliwość wyboru poszczególnych plików cookies, na które wyraża zgodę. Wszystkie trzy opcje powinny być bezpośrednio dostępne z poziomu baneru, natomiast ich kolorystyka taka sama, aby nie wpływać na wybór użytkownika. Co ważne, użytkownik musi zostać poinformowany i poproszony o zgodę zanim pliki cookies zaczną faktycznie działać.

Lista partnerów

Odnośnik do listy partnerów również powinien być dostępny i znajdować się na banerze. Po kliknięciu w odpowiedni link, użytkownikowi powinno ukazać się pełne zestawienie dostawców, którzy biorą udział w przetwarzaniu danych osobowych. Celem listy jest pełne ukazanie wszystkich podmiotów, które są zaangażowane w zbieranie danych podczas korzystania z konkretnej strony internetowej. Poza nazwą poszczególnych podmiotów, powinny znaleźć się informacje

[7] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

takie jak: rodzaj, cel i funkcja zbierania danych, długość ich magazynowania. Dodatkowo powininen znajdować się odnośnik do polityki prywatnośći każdego z partnerów.

Polityka prywatności

Polityka prywatności powinna stanowić łatwo dostępny dokument. Odnośnik do tego dokumentu powinien znajdować się na banerze, bądź w widocznym miejscu na głównej stronie. Polityka prywatności powinna być czytelna i napisana prostym językiem. Istotne jest, aby w razie jakichkolwiek zmian, dokument zawierający politykę prywatności został zaktualizowany.

Dokument ten, powinien szczegółowo opisywać prawa użytkownika w zakresie danych osobowych takie jak:

- prawo do informacji jakie dane są przetwarzane
- prawo do dostępu do przetwarzanych przez dany podmiot danych o użytkowniku
- prawo do zmiany konkretnych danych osobowych
- prawo do żądania usunięcia przetwarzanych danych osobowych
- prawo do ograniczenia przetwarzania danych osobowych
- prawo do wycofania zgody na przetwarzanie danych osobowych.

Kolejnym elementem zawartym w polityce prywatności powinna być informacja o danych osobowych, które są zbierane o użytkowniku. Każda kategoria danych powinna zawierać szczegółowy opis, jakie konkretnie dane są zbierane np. nazwa profilu, adres e-mail, hasło itp. wraz ze wskazaniem, w którym momencie dane te są pobierane. Administrator danych powinien także poinformować o celach przetwarzania łącznie z określeniem podstawy prawnej oraz kategorii danych osobowych wykorzystywanych w tym celu.

W polityce prywatności również powinna znaleźć się informacja o tym, w jaki sposób i dlaczego udostępniane są dane użytkowników podmiotom trzecim. Zgodnie z rozporządzeniem "strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe[8]. Dodatkowo powinna zostać wskazana kategoria podmiotów trzecich,

[8] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

ich nazwa, a także kategorie danych, które zostały tym podmiotom przekazane oraz powód tego działania. W przypadku transferu danych do innych krajów, administrator danych ma obowiązek zawarcia takiej informacji.

Następny aspekt, który powinien zostać poruszony w polityce prywatności to okres przechowywania danych. Według art. 5 ust.1 lit. e rozporządzenia RODO, dane osobowe mogą być przechowywane przez przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Administrator ma obowiązek ustalić i podać do wiadomości konkretny okres czasu, a zatem określony w miesiącach, bądź latach. Natomiast przepis wyklucza możliwość użycia sformułowania niedookreślonego między innymi takiego jak "bezterminowo". Ustawodawca pozwala na dłuższe przechowywanie danych, lecz wciąż nie na nieograniczone w czasie, jeżeli będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych[9].

Jak wiadomo, administrator przetwarzając dane osobowe jest także odpowiedzialny za ich bezpieczeństwo. W związku z tym, administrator w dokumencie powinien szczegółowo opisać jakie środki bezpieczeństwa są przez niego stosowane w celu ochrony danych osobowych przed nieuprawnionym dostępem, utratą czy zniszczeniem.

Ostatnim punktem, który powinien znaleźć się w polityce prywatności jest kontakt do administratora danych, z którego może skorzystać użytkownik w razie pojawienia się jakichkolwiek pytań.

Polityka plików cookies

Polityka plików cookies może stanowić odrębny dokument, bądź być połączona z polityką prywatności. Celem dokumentu jest wyjaśnienie, jakie skutki niesie za sobą wyrażenie zgody przez użytkownika na stosowanie plików cookies. W pierwszej kolejności, polityka plików cookies powinna zawierać wyjaśnienie czym właściwie pliki cookies są. Administrator danych ma obowiązek także poinformować, w jaki sposób wykorzystuje pliki wraz ze wskazaniem jaką kategorię plików stosuje i w jakim celu. Wyróżniamy kilka rodzajów plików cookies. Przede wszystkim występuje podział na niezbędne i funkcjonalne pliki cookies. Niezbędne to te, bez których strona nie może prawidłowo funkcjonować, a w związku z tym użytkownik nie ma możliwości ich modyfikacji. Zupełnie

[9] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

odwrotnie jest z funkcjonalnymi plikami cookies, które występują jedynie w celu zwiększenia jakości działania strony poprzez zapamiętanie preferencji użytkownika. Natomiast ze względu na okres czasu można wyodrębnić trwałe i sesyjne pliki cookies. Cookies sesyjne to małe pliki, które są zapisywane na urządzeniu użytkownika podczas przeglądania strony internetowej. Te pliki cookie służą do przechowywania informacji tymczasowych i zapewniają spersonalizowane przeglądanie. W przeciwieństwie do trwałych plików cookie, pliki cookie sesji są automatycznie usuwane po zamknięciu przeglądarki[10]. Pliki cookies pochodzące od innych dostawców niż administratora strony określane są mianem plików cookies osób trzecich. Najczęściej pochodzą one od reklamodawców.

Podobnie jak w przypadku polityki prywatności, jakakolwiek aktualizacja polityki plików cookies musi zostać natychmiast udostępniona użytkownikowi. Ponadto użytkownik powinien z łatwością znaleźć informację o okresie magazynowania danych i sposobie ich usuwania po upłynięciu odpowiedniego terminu.W polityce, administrator powinien zawrzeć także punkt odnoszący się do zmiany, bądź też wycofania zgody. Instrukcja dotycząca zarządzania plikami cookies powinna być napisana prostym językiem. Podobnie, jak w przypadku polityki prywatności, należy podać dane do kontaktu z inspektorem danych w razie jakichkolwiek pytań ze strony użytkownika.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Środki ochrony danych osobowych zostały przewidziane w rozporządzeniu. Zgodnie z art. 77 ust. 1 RODO: Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie[11]. W związku z tym, jeśli dane są przetwarzane w sposób nieprawidłowy, bądź też bez uzyskania zgody, użytkownik może złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych, który pełni rolę organu nadzorczego w Polsce.

[10] *Co to są pliki cookie i jakie są ich rodzaje?*, Tecnobits, https://tecnobits.com/pl/Co-to-s%C4%85-pliki-cookie-i-jakie-s%C4%85-ich-rodzaje%3F/, dostęp: 14.02.2024].

[11] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

Procedura złożenia skargi

Uprawnionym do wniesienia skargi jest osoba fizyczna, której dane osobowe zostały naruszone. Złożenie skargi może nastąpić na piśmie, bądź też przez internet. Istnieje też możliwość złożenia skargi ustnie do protokołu w siedzibie Urzędu Ochrony Danych Osobowych po wcześniejszym umówieniu na konkretną godzinę[12]. Wniesienie skargi nie jest obarczone żadnym terminem, oznacza to, że uruchomienie procesu może nastąpić w każdym momencie, a cała procedura jest bezpłatna.

Zgodnie z Kodeksem postępowania administracyjnego, Prezes Urzędu Ochrony Danych Osobowych powinien załatwić skargę bez zbędnej zwłoki, nie później jednak niż w ciągu miesiąca. Natomiast w przypadku bardziej skomplikowanej sprawy, powinna ona zostać rozstrzygnięta nie później niż w terminie dwóch miesięcy od dnia jej wszczęcia. Po zbadaniu sprawy i rozpatrzeniu zasadności skargi, Prezes UODO wydaje decyzję administracyjną, w której może uwzględnić żądanie strony albo uznać je za oczywiście bezzasadne. Zarówno skarżącemu, jak i administratorowi danych przysługuje prawo do wniesienia odwołania od wydanej decyzji do sądu administracyjnego. Odwołanie powinno zostać wniesione w terminie 30 dni od daty doręczenia stronie decyzji za pośrednictwem organu, który wydał orzeczenie[13].

Kary za nieprzestrzeganie

W przypadku wykrycia nieprawidłowości Prezes Urzędu Ochrony Danych Osobowych ma prawo nałożyć na podmiot karę administracyjną. Zgodnie z art. 83 RODO: Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

12 *Opis procedury: Zabezpieczenie danych osobowych przed nieuprawnionym ujawnieniem*, Biznes.gov.pl, https://www.biznes.gov.pl/pl/opisy-procedur/-/proc/891, [dostęp: 11.02.2024].

13 *Nieprawidłowe przetwarzanie danych osobowych – jak wnieść skargę?, Poradnik Przedsiębiorcy,* https://poradnikprzedsiebiorcy.pl/-nieprawidlowe-przetwarzanie-danych-osobowych-jak-wniesc-skarge#:~:text=Wniesienie%20skargi%20na%20nieprawid%C5%82owe%20przetwarzanie%20danych,do%20Prezesa%20Urz%C4%99du%20Ochrony%20Danych%20Osobowych.&text=Wniesienie%20skargi%20na%20nieprawid%C5%82owe,Urz%C4%99du%20Ochrony%20Danych%20Osobowych.&text=na%20nieprawid%C5%82owe%20przetwarzanie%20danych,-do%20Prezesa%20Urz%C4%99du%20Ochrony, [dostęp: 09.02.2024].

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,
- umyślny lub nieumyślny charakter naruszenia,
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych przez nich wdrożonych,
- wszelkie wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego,
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków,
- kategorie danych osobowych, których dotyczyło naruszenie,
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie,
- jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie uprawnienia naprawcze, a jak tak czy podmiot się do nich zastosował,
- stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji,
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty[14].

Maksymalna wysokość kary administracyjnej wynosi 20 000 000 euro, natomiast gdy podmiotem naruszającym ochronę danych osobowych jest przedsiębiorstwo to kara może wynieść do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

PODSUMOWANIE

Obecnie ochrona danych osobowych odgrywa bardzo istotną kwestią i jest jedną z najważniejszych, zarazem najtrudniejszych wyzwań współczesnej cyfrowej

[14] Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.

rzeczywistości. W związku z tym, podnoszenie świadomości poprzez edukację użytkowników stanowi konieczny element do zagwarantowania bezpiecznego korzystania z wirtualnego świata. Dogłębne wyjaśnienie, a w rezultacie zrozumienie przez odbiorcę podstawowych pojęć tj. cookies, polityka cookies oraz polityka plików prywatności, a dodatkowo wyobrażenie o procesie przetwarzaniu danych da możliwość powzięcia indywidualnej decyzji i wyrażenie, bądź odmówienia zgody na ten proces.

Wprowadzenie Rozporządzenia o Ochronie Danych Osobowych (RODO) można określić mianem przełomowego momentu, który spowodował narzucenie konkretnych regulacji na administratorów danych. Od tej pory, każda strona internetowa, przetwarzająca dane osobowe musi być zgodna z europejskimi standardami, a jakiekolwiek odstępstwa mogą zostać ukarane wysokimi sankcjami finansowymi. Warto jednakże zaznaczyć, że dążenie do zachowania prywatności i ochrony danych osobowych użytkowników jest nie tylko wymogiem prawnym, ale również moralnym obowiązkiem każdej instytucji działającej w przestrzeni cyfrowej.

Bezpieczeństwo danych osobowych to fundament zaufania użytkowników do usług online oraz klucz do utrzymania zdrowej i transparentnej relacji między użytkownikami a dostawcami usług internetowych. Dlatego też ciągłe edukowanie użytkowników na temat ich praw i obowiązków w zakresie ochrony danych osobowych jest niezmiernie istotne dla budowania lepszego świata internetowego, gdzie zaufanie będzie odgrywać pierwszorzędną rolę.

BIBLIOGRAFIA

Akty prawne

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34).

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. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Karta praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 z późn. zm.).

Źródła internetowe

Cookies – jak wdrożyć je zgodnie z prawem?, Creativa Legal, https://creativa.legal/cookies-jak-wdrozyc-je-zgodnie-z-prawem/, [dostęp: 10.02.2024].

CookieYes - GDPR & CCPA Cookie Consent Solution, CookieYes, https://www.cookieyes.com/, [dostęp: 10.02.2024].

Nieprawidłowe przetwarzanie danych osobowych – jak wnieść skargę?, Poradnik Przedsiębiorcy, https://poradnikprzedsiebiorcy.pl/-nieprawidlowe-przetwarzanie-danych-osobowych-jak-wniesc-skarge#:~:text=Wniesienie%20skargi%20na%20nieprawid%C5%82owe%20przetwarzanie%20danych,do%20Prezesa%20Urz%C4%99du%20Ochrony%20Danych%20Osobowych.&text=Wniesienie%20skargi%20na%20nieprawid%C5%82owe,Urz%C4%99du%20Ochrony%20Danych%20Osobowych.&text=na%20nieprawid%C5%82owe%20przetwarzanie%20danych,do%20Prezesa%20Urz%C4%99du%20Ochrony, [dostęp: 09.02.2024].

Opis procedury: Zabezpieczenie danych osobowych przed nieuprawnionym ujawnieniem, Biznes.gov.pl, https://www.biznes.gov.pl/pl/opisy-procedur/-/proc/891, [dostęp: 11.02.2024].

Co to są pliki cookie i jakie są ich rodzaje?, Tecnobits, https://tecnobits.com/pl/Co-to-s%C4%85-pliki-cookie-i-jakie-s%C4%85-ich-rodzaje%3F/, dostęp: 14.02.2024].

mgr **Klaudia Łachowska-Jarecka**

Uniwersytet im. Adama Mickiewicza w Poznaniu

Absolwentka

STOSOWANIE SZTUCZNEJ INTELIGENCJI W PROCESIE AUTOMATYCZNEGO ROZPOZNAWANIA TWARZY – WYBRANE ZAGADNIENIA PRAWNE

Wprowadzenie

Ostatnie kilkadziesiąt lat stanowiło dynamiczny rozwój nowych technologii. Zwiększenie ich wykorzystania dostrzegalne jest w wielu aspektach życia społecznego. Dużą popularność zdobyły w ostatnich latach w szczególności metody weryfikacji osób bazujące na biometrii, czyli sposobie dokonywania identyfikacji w oparciu o indywidualne cechy fizyczne danego podmiotu (Zaborska 2019, s. 97-106). Niezmienność, unikalność oraz brak możliwości replikacji tych cech powoduje, iż dokonywana w oparciu o nie identyfikacja jest bezpieczniejsza oraz skuteczniejsza (Krasuski 2018, s. 118; Kapczyński 2009, s. 11).

Dostrzegając, iż metody identyfikacji oparte na posiadaniu określonej wiedzy (znajomość kodu PIN, hasła) czy okazaniu konkretnego przedmiotu (karta dostępu, klucz) są często niewystarczające, dąży się do zastąpienia ich przez metody nowocześniejsze i obarczone mniejszym prawdopodobieństwem wystąpienia błędu, do jakich zaliczyć można właśnie biometrię (Zaborska 2019, s. 97-106; Łachowska 2021; Gutowska 2004, s. 69; Gutfeter i Pacut 2016, s. 79).

Jedną z popularniejszych w ostatnich latach metod uwierzytelniających opierających się na tej technologii jest automatyczne rozpoznawanie twarzy (Fajgielski 2021; Tiszbierek 2013, s. 1227-1235). Choć stosowanie tego

rozwiązania ułatwia codzienne funkcjonowanie (np. poprzez umożliwienie odblokowania urządzenia elektronicznego bez użycia rąk), to nie pozostaje ono jednak irrelewantne dla podstawowych praw i wolności jednostek, w szczególności ochrony prywatności. Obok głosów podkreślających duży potencjał w rozwoju tej technologii (Michałowicz 2021, s. 81; Fajgielski 2021), przez wiele lat pojawiały się również głosy sceptyczne, wskazujące na zagrożenia wynikające ze stosowania tej metody (Fajgielski 2021; Tiszbierek 2013, s. 1227-1235), postulujące konieczność zintensyfikowania prac legislacyjnych i uregulowania prawnego zastosowania technologii opartych o działanie sztucznej inteligencji (Michałowicz 2021, s. 82).

Technologia automatycznego rozpoznawania twarzy – geneza, specyfika i zastosowanie

Geneza

Choć technologia rozpoznawania twarzy zyskała znaczącą popularność dopiero w ostatnich latach, to znana jest zdecydowanie dłużej. Już w latach 60. XX w. rozpoczęto badania nad technologią umożliwiającą rozpoznanie ludzkiej twarzy i podjęto pierwsze próby stworzenia komputera, który w oparciu o załadowany obraz zidentyfikowałby ludzką twarz (Nilsson 2009, s. 172). System ten jednak znacząco różnił się od obecnie znanego nam modelu automatycznego rozpoznawania twarzy opartego na sztucznej inteligencji. Dokonywane pomiary bazowały na danych wprowadzonych ręcznie przez człowieka (współrzędnych określonych cech twarzy takich jak wewnętrzny i zewnętrzny kącik oka, środek źrenicy), w oparciu o które komputer dokonywał obliczeń i automatycznie porównywał wyniki analizy załadowanego zdjęcia ze zdjęciem występującym w bazie, w ten sposób dopasowując otrzymane rekordy (Nilsson 2009, s. 172).

Kolejne próby stworzenia systemu rozpoznawania twarzy polegały na ulepszeniu dotychczasowych rozwiązań poprzez wyeliminowanie etapu ręcznego wpisywania współrzędnych twarzy na rzecz automatycznego rozpoznania cech anatomicznych człowieka, w szczególności analizy i rozpoznania linii profilu, jednak i ten system nie był pozbawiony błędów (Tiszbierek 2013, s. 1227-1235; Nilsson 2009, s. 172).

Swoisty przełom w zakresie badań nad technologią automatycznego rozpoznawania twarzy nastąpił na początku lat dwutysięcznych. Choć dotychczas wypracowane techniki były dostępne na rynku komercyjnym już w latach 90. XX w.,

to oparte były wyłącznie na analizie zdjęć. Dopiero nowe tysiąclecie przyniosło rozwiązania nowocześniejsze, pozwalające na detekcję twarzy w czasie rzeczywistym (algorytm Viola Jones) w oparciu o uczenie maszynowe, które znane jest nam współcześnie (Yamaguchi 2012, s. 29).

Sposób działania

Proces rozpoznawania twarzy jest procesem złożonym, opierającym się na kilku usystematyzowanych etapach.

Pierwszy z nich stanowi detekcja obiektu. Dochodzi wówczas do wykrycia na obszarze poddanym analizie twarzy i wyodrębnienie jej z tła, na którym się znajduje (Li i Jain 2005, s. 1).

Następnie wykryty obszar poddaje się normalizacji i segmentacji – procesowi mającemu na celu zlokalizowanie poszczególnych elementów twarzy (usta, nos, oczy) i ich ustandaryzowanie pod kątem geometrycznym (normalizacja geometryczna) oraz wyrównanie właściwości obrazu takich jak cienie, oświetlenie czy skala szarości (normalizacja fotometryczna) (Yamaguchi 2012, s. 2).

Działanie to umożliwia przeprowadzenie kolejnego etapu, jakim jest ekstrakcja, czyli wyodrębnienie z analizowanego obszaru określonych indywidulanych cech. Wyróżnienie elementów właściwych danemu człowiekowi, odróżniających go od innych ludzi, pozwala dokonać szczegółowej analizy w oparciu o utworzone wektory cech twarzy (Yamaguchi 2012, s. 3).

To na ich podstawie, w ostatnim – czwartym etapie – system dokonuje porównania utworzonych podczas analizy wektorów z wektorami cech twarzy już istniejącymi w bazie, powstałymi w oparciu o analizę innych wizerunków (Tiszbierek 2013, s. 1227-1235*;* Li i Jain 2005, s. 3). Jeśli są one tożsame dochodzi do identyfikacji osoby w oparciu o przeprowadzoną analizę.

Choć dla zdrowego człowieka rozpoznanie oraz zidentyfikowanie ludzkiej twarzy nie stanowią większej trudności, z punktu widzenia rozwiązań technologicznych zadanie to nie jest tak proste.

W pierwszej kolejności należy zwrócić uwagę na jakość materiału poddawanego analizie. Niejednokrotnie zdarza się, że panujące warunki techniczne utrudniają przeprowadzanie analizy – już nieodpowiedni kąt padania światła może zaburzyć cały proces, uniemożliwiając rozpoznanie analizowanego obiektu i dopasowanie go do materiału dostępnego w bazie.

Ostatnie doświadczenia życia w czasie pandemii i obowiązek noszenia maseczek ochronnych zakrywających znaczną cześć twarzy pokazały, że również

w takiej sytuacji może dojść do nieefektywnego rezultatu przeprowadzanego procesu. Niemniej należy podkreślić, iż dostawcy tej usługi starają się podążać z duchem czasu i na bieżąco eliminować potencjalne przeszkody, tak by zwiększyć skuteczność i użyteczność tej technologii umożliwiając jej szerokie zastosowanie.

Wybrane zastosowania technologii automatycznego rozpoznawania twarzy

Technologia automatycznego rozpoznawania twarzy występuje zarówno w sektorze prywatnym, jak i publicznym. Jej dostępność, skuteczność oraz bezpieczeństwo spowodowały szerokie zainteresowanie jej wykorzystania w codziennym życiu.

Jednym z najpopularniejszych metod jej wykorzystania są smartfony i możliwość odblokowania telefonu w oparciu o identyfikację twarz jego właściciela (Fajgielski 2021). Zastosowanie tej technologii w tym obszarze stanowi odpowiedź na oczekiwania użytkowników końcowych, którzy w szybki i bezpieczny sposób chcą móc korzystać ze swoich urządzeń. Technologia automatycznego rozpoznawania twarzy gwarantuje nie tylko wysoki poziom bezpieczeństwa (praktycznie brak możliwości odblokowania przez inna osobę), ale i wygodę – w odróżnieniu od innej popularnej metody biometrycznej, jaką jest odcisk palca, technologia rozpoznawania twarzy nie wymaga dodatkowego angażowania rąk użytkownika.

Ciekawym, ale i powodującym szeroką dyskusję, jest rozwiązanie postulowane przez International Air Transport Association (IATA) – One ID. Głównym celem stosowania tej metody jest usprawnienie systemu obsługi pasażerów w portach lotniczych (IATA a; b), poprzez umożliwienie pasażerom posługiwania się identyfikatorem biometrycznym (np. w zakresie rozpoznania rysów twarzy).

Rozwiązanie to zostało już wdrożone przez niektóre linie i porty lotnicze, które zaczęły oferować przeprowadzenie odprawy za pośrednictwem metody automatycznego rozpoznania twarzy (Euronews 2023)[1]. Zainteresowani skorzystaniem z tej metody pasażerowie, mogą wgrać do systemu przewoźnika swoje zdjęcie i dane oraz wyrazić zgodę na przeprowadzenie odprawy za pośrednictwem technologii automatycznego rozpoznawania twarzy. Lotniska wyposażone zostały w odpowiednie systemy – dedykowane bramki z kamerami, które w czasie rzeczywistym identyfikują pasażerów przez nie przechodzących z wcześniej udostępnionymi w bazie wizerunkami. Jak oszacowano dzięki zastosowaniu tej technologii

[1] Wśród portów lotniczych oferujących tę usługę znajdują się lotniska w Hamburgu, Atlancie, Detroit, Dubaju, Tokio, Lyonie czy Fort Lauderdale na Florydzie.

proces odprawy stał się płynniejszy i – co ważne z perspektywy pasażerów – wygodniejszy. Stanowi to też wyjście naprzeciw oczekiwaniom podróżnych – jak wykazał przeprowadzony przez IATA Global Passenger Survey aż 73% potencjalnych podróżnych zadeklarowała chęć udostępniania swoich danych biometrycznych w celu korzystania z tego rozwiązania (IATA 2021).

Technologia rozpoznawania twarzy znajduje też zastosowanie w sektorze publicznym. Doskonałym tego przykładem może być wykorzystanie technologii rozpoznania twarzy przez organy ścigania. Metoda ta umożliwia zidentyfikowanie wśród tłumu ludzi twarzy przestępcy, poprzez dopasowanie pobranego materiału do materiału już znajdującego się w bazie (Szostek 2021; Kucharska 2019, s. 20–21; Business Insider 2018). Co ciekawe, technologia ta znajduje na świecie zastosowanie nie tylko w celu ścigania przestępców, ale i np. identyfikowania przechodniów niestosujących się do zasad ruchu drogowego poprzez przekraczanie ulicy na czerwonym świetle (Business Insider 2018). Choć sam pomysł wykorzystania technologii w służbie społeczeństwu nie wzbudza kontrowersji, tak sposób w jaki jest został zastosowany już tak. Kontrola zachowań obywateli pozbawia ich bowiem jakiejkolwiek anonimowości i prawa do prywatności, a w efekcie może prowadzić do ostracyzmu społecznego i publicznej stygmatyzacji.

Również polski ustawodawca dążył do zautomatyzowania procesów weryfikacji petentów w sektorze publicznym. Doskonałym tego przykładem są trwające prace nad ustawą Prawo komunikacji elektronicznej, w której jednym z proponowanych rozwiązań jest umożliwienie zdalnej identyfikacji abonenta przy zawieraniu umowy, poprzez podanie swoich danych elektronicznie, w trakcie wideokonferencji (art. 297 ust. 2 lit. d). Zgodnie z projektem ustawy identyfikacja odbywać się ma poprzez porównanie okazanego przez abonenta wizerunku zawartego w dowodzie tożsamości wraz jednoczesnym udostępnieniem swojego wizerunku w trakcie transmisji audiowizualnej. Choć w projekcie ustawy nie sprecyzowano, czy proces identyfikacji odbywać się będzie w sposób zautomatyzowany, to wskazano, iż „wideokonferencja może odbywać się z wykorzystaniem automatycznej analizy danych lub przez porównanie danych, o których mowa w przepisie przez osobę fizyczną działającą w imieniu przedsiębiorcy telekomunikacyjnego", co otwiera możliwość stosowania w procesie identyfikacji technologii automatycznego rozpoznawania twarzy. Rozwiązanie to stanowi wyjście naprzeciw oczekiwaniom przedsiębiorcom i samym konsumentom, którzy dzięki projektowanym zmianom będą mogli bez wychodzenia z domu rozpocząć korzystanie z usług elektronicznych.

Regulacje prawne – RODO

Regulacje prawne dotyczące danych biometrycznych

W związku z wykorzystaniem technologii automatycznego rozpoznawania twarzy ma miejsce przetwarzanie danych osobowych, bowiem technologia ta zakłada, że na danych osobowych, a dokładniej na danych biometrycznych, będą wykonywane określone operacje.

Obecnie kwestie te reguluje rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych, RODO). Jest to regulacja ogólna i znajduje, co do zasady, zastosowanie do wszelkich sytuacji, gdy ma miejsce przetwarzanie danych osobowych biometrycznych, także procesie automatycznego rozpoznawania twarzy.

RODO nie znajduje jednak zastosowania, jeśli coś innego wynika z jego materialnego zakresu stosowania lub z przepisów szczególnych (Fajgielski 2021). Do tych ostatnich zaliczyć należy ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości, która stanowi implementację dyrektywy 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 postepowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW. Ustawa ta określa, jak należy chronić dane osobowe, gdy ma miejsce automatyczne rozpoznawanie twarzy w ramach monitoringu wizyjnego miejsc i wydarzeń publicznych przez organy ścigania (Fajgielski 2021).

Definicja danych biometrycznych

Zgodnie z art. 4 pkt 14 RODO dane biometryczne 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. Warto przy tym zwrócić uwagę na wskazówkę

interpretacyjną wskazaną w motywie 51 RODO, zgodnie z którą fotografie są objęte definicją danych biometrycznych tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.

Za cechy danych biometrycznych uznać należy ich uniwersalny charakter (występują u każdego człowieka), unikalność (odróżniają ludzi od siebie) oraz trwałość (co do zasady pozostają z człowiekiem przez całe jego życie) (Chomiczewski i in. 2018). Warto przy tym zwrócić uwagę, iż za dane biometryczne można uznać fotografię twarzy tylko w sytuacji, gdy zdjęcie jest poddawane specjalne przetwarzaniu, które ma na celu identyfikacje osoby lub weryfikacje jej tożsamości (a zatem nie każde zdjęcie z wizerunkiem twarzy to dane biometryczne) (Fajgielski 2021). Dane te uznaje się za szczególne kategorie danych osobowych, co wiąże się ze szczególnymi zasadami przetwarzania danych biometrycznych wskazanym w art. 9 RODO.

Podobną definicją danych biometrycznych posłużył się też polski prawodawca, który w art. 4 ust. 2 ustawy o zwalczaniu przestępczości wskazał, iż danymi biometrycznym są dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, w tym wizerunek twarzy lub dane daktyloskopijne, które zostały uzyskane wskutek specjalnego przetwarzania technicznego.

Zasady przetwarzania danych biometrycznych

Zgodnie z ogólną zasadą dot. szczególnych kategorii danych osobowych wskazaną w art. 9 ust. 1 RODO oraz art. 14 ust. 1 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości zabrania się przetwarzania danych osobowych danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej. Jednakże od wspomnianego zakazu zostały ustanowione pewne wyjątki, o których mowa w art. 9 ust. 2 RODO oraz art. 14 ust. 2 wymienionej wyżej ustawy, jednak z uwagi na przedmiot i zakres stosowania obu aktów różnią się one między sobą.

W przypadku RODO wyjątkiem przemawiającym na rzecz przetwarzania danych osobowych w związku z automatycznym rozpoznawaniem twarzy jest wyraźna zgoda osoby, której dane dotyczą, na przetwarzanie tych danych (art. 9 ust. 2 lit a) RODO). W związku z tym administrator powinien spełnić wymagania dotyczące zgody wynikające z art. 7 RODO. W pierwszej kolejności administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę

na przetwarzanie swoich danych osobowych. Co więcej, zgoda powinna być uzewnętrzniona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Poza tym oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być przedstawione jasnym i prostym językiem oraz nie powinno zawierać nieuczciwych warunków. Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

Z kolei zgodnie z art. 14 ust. 2 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości dopuszcza się przetwarzanie danych biometrycznych, jeżeli przepisy prawa zezwalają na ich przetwarzanie lub jest to niezbędne dla ochrony życia lub zdrowia lub interesów osoby, której dane dotyczą, lub innej osoby, lub dane takie zostały upublicznione przez osobę, której dotyczą. Jednakże ustawodawca nie transponował we wspomnianym przepisie przesłanki określonej w art. 10 dyrektywy, tj. bezwzględnej niezbędności przetwarzania oraz stosownych zabezpieczeń dla praw i wolności osoby, której dane dotyczą, zwłaszcza w zakresie dostępu do takich danych, okresu ich przetwarzania czy ograniczania ich dalszego przetwarzania.

Kierunek zmian regulacji prawnych

Rozporządzenie w sprawie sztucznej inteligencji

Wobec szybkiego rozwoju technologii opartej o sztuczną inteligencję i jednoczesnym braku szczegółowej regulacji odpowiadającej wyzwaniom, które wiążą się z coraz szerszym stosowaniem AI, prawodawca europejski podjął prace i przyjął Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ws. ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (Artificial Intelligence Act). Jest to pierwsza tak kompleksowa regulacja prawna ustanawiająca zharmonizowane przepisy dotyczące sztucznej inteligencji.

Główne założenia rozporządzenia opierają się na stworzeniu jednolitych ram prawnych, umożliwiających wykorzystywanie pojawiających się rozwiązań

technologicznych opartych na sztucznej inteligencji z zapewnieniem poszanowania praw podstawowych i wartości oraz bezpieczeństwa, przy jednoczesnym umożliwieniu rozwoju jednolitego rynku, a tym samym utrzymaniu wiodącej pozycji UE w zakresie wdrażania nowych technologii i zapewnieniu wzrostu dobrostanu społecznego.

Choć wyraźnie podkreślono – zarówno już w uzasadnieniu projektu, jak i w samych motywach rozporządzenia – korzyści wynikające ze stosowania AI (a wobec tego potrzebę jej dalszego rozwijania i wykorzystywania), akcentuje ono równie wyraźnie zagrożenia wynikające ze stosowania nowych rozwiązań dla podstawowych praw jednostek.

Szczególną uwagę zwraca się na przetwarzanie danych przez technologie dokonujące identyfikacji biometrycznej. Rozporządzenie definiuje identyfikację biometryczną jako „zautomatyzowane rozpoznawanie fizycznych, fizjologicznych, behawioralnych i psychologicznych cech ludzkich, w celu ustalenia tożsamości osoby fizycznej przez porównanie danych biometrycznych tej osoby z danymi biometrycznymi osób fizycznych przechowywanych w bazie danych".

Tak jak w projekcie rozporządzenia, podobnie w przyjętej treści dokumentu rozróżniono systemy zdalnej identyfikacji biometrycznej działające „w czasie rzeczywistym" (pobranie, porównanie i identyfikacja zachodzą natychmiast, niemal natychmiast lub w każdym razie bez znacznego opóźnienia) od tych działających „post factum" (porównanie i identyfikacja następują ze znacznym opóźnieniem od momentu pobrania danych).

Zważywszy na bardziej dotkliwy dla praw i wolności charakter identyfikacji „w czasie rzeczywistym", w art. 5 ust. 1 lit. h) rozporządzenia wprowadzono zakaz wykorzystywania tego systemu w przestrzeni publicznej do celów ścigania przestępstw, przewidując jednocześnie trzy wyjątki od tej zasady:

1. ukierunkowanego poszukiwania konkretnych ofiar uprowadzeń, handlu ludźmi lub wykorzystywania seksualnego ludzi, a także poszukiwania osób zaginionych;
2. zapobiegnięcia konkretnemu, istotnemu i bezpośredniemu zagrożeniu życia lub bezpieczeństwa fizycznego osób fizycznych lub rzeczywistemu i aktualnemu lub rzeczywistemu i dającemu się przewidzieć zagrożeniu atakiem terrorystycznym;
3. lokalizowania lub identyfikowania osoby podejrzanej o popełnienie przestępstwa w celu prowadzenia postępowania przygotowawczego lub ścigania lub wykonania kar w odniesieniu do przestępstw, o których

mowa w załączniku II, podlegających w danym państwie członkowskim karze pozbawienia wolności lub środkowi polegającemu na pozbawieniu wolności przez okres, którego górna granica wynosi co najmniej cztery lata.

Uprawnienie do zastosowania któregokolwiek z wyjątków wskazanych w art. 5 ust. 2 lit. h) powinno być poprzedzone oceną ryzyka – analizą okoliczności konieczności zastosowania tej metody, jak i oceny konsekwencji wykorzystania systemu dla praw i wolności jednostek. Dodatkowym ograniczeniem w zakresie możliwości zastosowania któregokolwiek z wyjątków wskazanych w art. 5 ust. 1 lit. h) jest konieczność uzyskania uprzedniej (w uzasadnionych przypadkach także następczej – tj. wniosek o takie zezwolenie powinien zostać złożony bez zbędnej zwłoki, najpóźniej w ciągu 24 godzin) zgody właściwego organu państwa członkowskiego, w którym ma nastąpić wykorzystanie.

Zgodnie z motywem 54, z uwagi na techniczne niedoskonałości stosowanych systemów, jak również szczególny charakter danych biometrycznych (unikalność) ich przetwarzanie może powodować dotkliwe skutki w postaci dyskryminacji osób fizycznych. Jednocześnie z kategorii systemów wysokiego ryzyka wyłączono te systemy AI, które weryfikują tożsamość konkretnej osoby w celu uzyskania dostępu, uruchomienia urządzenia bądź dostania się do pomieszczeń.

Ocena przyjętego rozwiązania i postulaty *de lege ferenda*

Choć samo dążenie i podejmowanie działań prawodawczych do uregulowania stosowania technologii rozpoznawania twarzy zasługuje na uznanie, tak przyjęte rozporządzenie może wzbudzać wiele zastrzeżeń i wątpliwości.

W pierwszej kolejności zwrócić należy uwagę, iż zaproponowane w rozporządzeniu rozróżnienie na identyfikację w czasie rzeczywistym oraz post factum, wydaje się być błędem. Każda bowiem ze wskazanych metod jednakowo może wywierać wpływ na prawa i wolności jednostek, w szczególności w zakresie swobodnego podejmowania decyzji o swojej aktywności w przestrzeni publicznej (Michałowicz 2021, s. 90). Ponadto już samo dokonanie oceny, czy dany system dokonuje identyfikacji w czasie rzeczywistym czy też post factum może być trudne. W rozporządzeniu posłużono się bowiem wyrażeniami generalnymi i nieostrymi („natychmiast", „niemal natychmiast", „bez znacznego opóźnienia", „znaczne opóźnienie"), w związku z czym rozgraniczenie tych dwóch sposobów identyfikacji może być problematyczne i prowadzić do nadużyć.

Zwraca się także uwagę, iż ogólny zakaz przetwarzania danych biometrycznych w czasie rzeczywistym (z enumeratywnie wskazanymi wyjątkami) wyrażony w art. 5 ust. 1 lit. h) rozporządzenia jest niewystarczający – dotyczy on bowiem wyłącznie podmiotów publicznych, całkowicie pomijając podmioty prywatne, dla których stosowanie technologii identyfikacji twarzy na gruncie rozporządzenia jest dozwolone (Michałowicz 2021, s. 91). Zważywszy na fakt, iż podmioty prywatne coraz częściej decydują się na stosowanie tej metody weryfikacji w celach komercyjnych[2], zaproponowane rozwiązanie nie odpowiada aktualnym potrzebom i nie zwiększa poziomu ochrony wolności i praw jednostek, co w kontekście szczególnego charakteru przetwarzanych danych, budzi znaczące kontrowersje. Sam cel przetwarzania (publiczny lub prywatny) pozostaje bowiem bez znaczenia w obliczu inwazyjności takiego rozwiązania i ewentualnych skutków jego działania. W szczególności pod uwagę należy wziąć podatność na wadliwość takich systemów (co zresztą zostało podkreślone w motywie 54 rozporządzenia), a w efekcie – możliwe dotkliwe konsekwencje występujące po stronie osoby fizycznej, które mogą okazać się trudne do odwrócenia.

Wobec powyższego należy przychylić i nieustannie wspierać glosy postulujące wprowadzenie całkowitego zakazu stosowania technologii automatycznego rozpoznawania twarzy bez różnicowania na organy władzy publicznej i jednostki prywatne. Mając na uwadze przydatność tej metody weryfikacji w niektórych przypadkach, zasadnym byłoby dopuszczenie stosowania tej technologii w enumeratywnie i konkretnie wskazanych przypadkach, co z pewnością ograniczyłoby negatywny wpływ na prawa jednostek, w szczególności tak fundamentalne prawo jak prawo do prywatności.

Ważnym głosem w dyskusji dotyczącej możliwości stosowania technologii automatycznego rozpoznawania twarzy pozostaje wspólna opinia Europejskiej Rady Ochrony Danych Osobowych i Europejskiego Inspektora Ochrony Danych Osobowych (Wspólna opinia EROD-EIOD 5/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji z dnia 18 czerwca 2021 r.), w której zaakcentowano obawy związane z dopuszczalnością zdalnej identyfikacji biometrycznej. Wobec tego organy te wezwały do wprowadzenia ogólnego zakazu wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania jakichkolwiek cech ludzkich w przestrzeni publicznej (Wspólna opinia EROD-EIOD 5/2021, s. 13). Co więcej w opinii zalecono również

[2] Doskonałym przykładem są wspomniane wcześniej porty lotnicze stosujące technologię automatycznego rozpoznawania twarzy do przeprowadzenia procesu odprawy.

ustanowienie zakazu – zarówno w sektorze publicznym, jak i prywatnym – stosowania systemów sztucznej inteligencji, których trafność nie została udowodniona, bądź które stoją w bezpośredniej sprzeczności z podstawowymi wartościami UE (Wspólna opinia EROD-EIOD 5/2021, s. 14).

Podsumowanie

Szybki rozwój nowych technologii bazujących na działaniu sztucznej inteligencji bez wątpienia jest zjawiskiem pozytywnym i pożądanym, przynoszącym korzyści społeczno-ekonomiczne, a sama technologia automatycznego rozpoznawania twarzy może ułatwiać nasze życie. Z drugiej jednak strony, z uwagi na szczególny charakter danych poddawanych przetwarzaniu, niejednokrotnie brak świadomości i realnej kontroli nad tym procesem, a także wysokie ryzyko naruszenia podstawowych praw i wolności człowieka, wzbudza ono kontrowersje[3].

Wobec tego należy pozytywnie ocenić działania prawodawcy unijnego, które doprowadziły do uregulowania tej materii. Wydaje się jednak, że prawo powinno nie tylko odpowiadać na pojawiające się nowe rozwiązania technologiczne, ale nawet być o krok przed nimi. Zaproponowane i przyjęte w rozporządzeniu rozwiązania wydają się w tym kontekście niewystarczające i, w mojej ocenie, mogą sprzyjać utracie kontroli nie tylko nad naszymi danymi, lecz życiem w ogóle.

Z tego też powodu należy wciąż postulować wprowadzenie ogólnego zakazu stosowania technologii automatycznego przetwarzania twarzy, dopuszczając jednak konkretne wyjątki od tej zasady, uwzględniające poszanowanie prawa do prywatności każdego z nas. Wyłącznie zapewnienie podwyższonych standardów ochrony i restrykcyjne podejście do przetwarzania naszych danych biometrycznych, uwzględniające proporcjonalność stosowanych metod identyfikacji do celów przetwarzania danych, może uchronić nas przed wystąpieniem negatywnych skutków takich działań, niejednokrotnie trudnych do odwrócenia.

[3] Problem ten bardzo dobrze obrazuje dyskusja dotycząca planów umożliwienia stosowania rozpoznawania twarzy w szeregu technologii nadzoru w Irlandii, w tym w kamerach CCTV i kamerach policyjnych oraz w systemach automatycznego rozpoznawania tablic rejestracyjnych. Irlandzka Rada Swobód Obywatelskich (The Irish Council for Civil Liberties) rozpoczęła kampanię, w której zachęca ludzi, by również napisali do ministra, że nie zgadzają się na przechwytywanie i przetwarzanie danych przez system nadzoru FRT. Rada przyłącza się do innych organizacji pozarządowych z całego świata, domagając się wprowadzenia szerszego zakazu stosowania tej technologii w miejscach publicznych: https://www.biometricupdate.com/202206/real-time-facial-recognition-surveillance-planned-in-ireland-moratorium-demanded; Wątpliwości związane z technologią automatycznego rozpoznawania twarzy pojawiają się także w Polsce. Już w 2020 r. Fundacja Panoptykon zorganizowała kampanię społeczną mającą na celu zebranie podpisów pod petycją nt. zakazu stosowania biometrycznych technologii nadzoru w przestrzeni publicznej, więcej: https://panoptykon.org/odzyskaj-swoja-twarz.

Bibliografia

Akty prawne

Projekt ustawy – Prawo komunikacji elektronicznej, UC7.

Stanowisko Parlamentu Europejskiego przyjęte w pierwszym czytaniu w dniu 13 marca 2024 r. w celu przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/... ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji i zmieniającego rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), P9_TC1-COD(2021)0106.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)

Wspólna opinia EROD-EIOD 5/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji z dnia 18 czerwca 2021 r.

Monografia wieloautorska

Chomiczewski W. i in.

2018 *Art. 4 pkt 14 RODO. Dane biometryczne,* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa.

Fajgielski P.

2021 Część II *Nowe technologie z perspektywy prawa publicznego,* [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa.

Gutfeter W., Pacut A.

2016 *Człowiek w systemie biometrycznym*, [w:] *Dokumenty a prawo,* red. M. Tomaszewska-Michalak, T. Tomaszewski, Warszawa.

Gutowska D.
2004 *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, „Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej", nr 20.

Jain A.K., Li S. Z.
2005 *1. Introduction*, [w:] *Handbook of Face Recognition*, red. S. Z. Li, A. K. Jain, Nowy Jork.

Kapczyński A.
2009 *Technologie biometryczne*, [w:] *Biometria w bankowości i administracji publicznej*, red. R. Kaszubski, Warszawa.

Krasuski A.
2018 *Ochrona danych osobowych na podstawie RODO*, Warszawa.

Kucharska E.
2019 *BriefCam – jeden system, wiele mozliwości*, „Stołeczny Magazyn Policyjny", nr 12.

Łachowska K.
2021 *3. Dane szczególnej kategorii na gruncie RODO,* [w:] *Ochrona danych osobowych w prawie publicznym*, red. M. Jędrzejczak, Warszawa.

Michałowicz A.
2021 *Przetwarzanie danych biometrycznych a ochrona jednostek - analiza wybranych zagadnień na tle ogólnego rozporządzenia o ochronie danych i projektu aktu w sprawie sztucznej inteligencji*, „IKAR", nr 6.

Nilsson N. J.
2009 *The Quest for Artificial Intelligence*, Cambridge.

Szostek D.
2021 *LegalTech w organach ścigania,* [w:] *LegalTech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym,* red. D. Szostek, Warszawa.

Tiszbierek A.
2013 *Komputerowe systemy automatycznej klasyfikacji i rozpoznawania twarzy*, Opole.

Yamaguchi O.
2012 *Face Recognition Technology, and Its Real-World Application* [w:] *Perception and Machine Intelligence: First Indo-Japan Conference,* red. K. Pal Sankar i inni, Kalkuta.

Zaborska S.
2019 *Legal Regulation of the Protection of Biometric Data under the GDPR*, „Studia Iuridica Lublinensia", nr 2.

Źródła internetowe

IATA
a *One ID*, https://www.iata.org/en/programs/passenger/one-id/ [dostęp: 01.03.2024].
b *One ID and standarization of identity management solutions*, https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/one-id-standarization-identity-management-solutions_3pagedoc.pdf [dostęp: 01.03.2024].
2021 *Global Passenger Survey (GPS)*, https://www.iata.org/en/publications/store/global-passenger-survey/ [dostęp: 01.03.2024].

Euronews
2023 *This German airport could be the first to offer face-scanning technology for all passengers*, https://www.euronews.com/travel/2023/10/27/this-german-airport-could-be-the-first-to-offer-face-scanning-technology-for-all-passenger [dostęp: 01.03.2024].

Business Insider
2018 *Rozpozna twarz i wyśle smsa – Chińczycy znaleźli sposób na przechodzenie "na czerwonym"*, https://businessinsider.com.pl/technologie/rozpozna-twarz-i-wysle-smsa-chinczycy-znalezli-sposob-na-przechodzenie-na-czerwonym/624sp0v [dostęp: 01.03.2024].

SZYMON DONARSKI

Uniwersytet Mikołaja Kopernika w Toruniu

Student

KOLEBKA DLA NARUSZEŃ, CZYLI POZYSKIWANIE I PRZETWARZANIE DANYCH PRZEZ PLATFORMĘ TIKTOK

WPROWADZENIE

W dobie cyfryzacji i ciągłego, dynamicznego rozwoju przestrzeni wirtualnej powstała łatwa w obsłudze i szeroka przestrzeń do rozrywki, a także marketingu i zarobku. Sam w sobie internet oraz stricte połączone z nim platformy, które bez dostępu do tzw. sieci nie mają większego sensu i zastosowania. Platformy takie jak Facebook, Instagram, Twitter czy w ostatnich latach zyskujący na znaczeniu i wiodący prymat, szczególnie wśród młodzieży TikTok stanowią idealną przestrzeń do rozwoju naruszeń prawa, przykładowo dóbr osobistych i majątkowych, praw autorskich i pokrewnych oraz danych osobowych. Niniejsze opracowanie bierze pod lupę jedynie fragment tak rozległego problemu i dotyczy szczegółowej analizy naruszenia danych osobowych na platformie TikTok.

CZYM JEST TIKTOK?

W celu uzyskania dokładnego zarysu sytuacji warto wspomnieć czym właściwie jest platforma TikTok. Aplikacja została stworzona przez chińskie przedsiębiorstwo ByteDance we wrześniu 2016 r. Aplikacja od samego początku cieszyła się popularnością i dużym zasięgiem, a w pierwszym kwartale 2022 r. okazała się być najczęściej pobieraną aplikacją na świecie, o czym poinformowano w raporcie Q1 2022: *Store Intelligence Data Digest firmy SensorTower* (Brejza 2022,

s. 53-54).

W ciągu ostatnich kilku lat możliwości upowszechniania wizerunku na dużą skalę, a także w zakresie globalnym znacznie się rozwinęły, głównym faktorem tego zjawiska jest Internet i odpowiednie platformy społecznościowe, w tym omawiany TikTok. Zapewnia on użytkownikom możliwość publikacji różnych treści różnych według własnego uznania i w praktyce nieograniczonej tematyce. Zazwyczaj na TikToku pojawiają się krótkie, maksymalnie dziesięciominutowe filmiki. Współcześnie wizerunek to marka osobista, która jest wykorzystywana w celach komercyjnych (Bodanka 2022, s.12).

Z popularnością platformy i rekordowym wzrostem liczby użytkowników, wzrosło też ryzyko naruszenia wizerunku i szeroko rozumianych danych osobowych. Każda osoba, która jest zainteresowana utworzeniem profilu na TikToku musi się zarejestrować, a tym samym podać wymagane o sobie informacje. Niektóre z danych mogą stanowić dane wrażliwe zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (dalej jako „RODO")[1]. Pojawia się więc szereg poważnych pytań, m.in. czy podane dane osobowe są odpowiednio chronione? Czy TikTok działa zgodnie z RODO?

POLITYKA PRYWATNOŚCI PLATFORMY TIKTOK

Według dostępnych informacji Tik Tok jest aplikacją gromadzącą najwięcej danych osobowych i informacji na temat swoich użytkowników. Najaktualniejsza wersja dokumentu dotyczącego polityki prywatności platformy pochodzi z 19 listopada 2023 r.[2] Ze wstępu ww. dokumentu użytkownik dowiaduje się, że ma on zastosowanie do danych osobowych przetwarzanych przez TikTok w związku z aplikacjami TikTok, witrynami internetowymi, oprogramowaniem i powiązanymi usługami. Z kolei administratorem danych w zależności od miejsca zamieszkania użytkownika jest TikTok Technology Limited, spółka irlandzka („TikTok Ireland"), oraz TikTok Information Technologies UK Limited („TikTok UK"), spółka brytyjska. Wymienione spółki są współadministratorami wszelkich informacji przetwarzanych w związku z prowadzoną na TikToku

[1] 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. L. z 2016 r. Nr 119, str. 1 z późn. zm.) (dalej jako „RODO")

[2] TikTok Technology Limited 2023.

polityką prywatności.

TikTok gromadzi tzw. informacje użytkownika czy też może bardziej adekwatnie nazwane dane osobowe na trzy sposoby: informacje podane przez użytkownika, informacje zebrane automatycznie oraz informacje pochodzące z innych źródeł (TikTok Technology Limited 2023). W zakresie danych podawanych przez użytkownika (m.in. przy zakładaniu konta) możemy wymienić: datę urodzenia, nazwę użytkownika, adres e-mail, numer telefonu oraz hasło oraz w zakresie woli użytkownika zdjęcie profilowe, gdyż nie jest to element konieczny. TikTok gromadzi także dane w zakresie publikowanych na portalu treści m.in. są to zdjęcia, filmy. Dodatkowo gromadzeniu podlegają także kontakty znajdujące się na urządzeniu z którego korzysta użytkownik, warunkiem jest oczywiście wyrażenie zgody na zaimportowanie ich do aplikacji (Podolski 2023) oraz automatycznie zbierane informacje o przybliżonej lokalizacji (np. kraj, miasto) na podstawie jego danych pozyskiwanych z np. Karty SIM czy adresu IP (TikTok Technology Limited 2023).

TRANSGRANICZNE PRZEKAZYWANIE DANYCH OSOBOWYCH PRZEZ PLATFORMĘ TIKTOK

Polityka prywatności, przetwarzanie danych pozyskiwanych przez platformę TikTok i szereg naruszeń w różnych dziedzinach prawa od dłuższego czasu martwi wiele osób i budzi kontrowersje, m.in. z powodu obawy, że dane osobowe użytkowników mogą być udostępniane pracownikom innych oddziałów serwisu na świecie, w tym przede wszystkim w Chinach. Niedawno okazało się, były to słuszne obawy, bowiem wraz z wejściem w życie nowej polityki prywatności platformy TikTok, która w zakresie najważniejszych informacji została omówiona w powyższym akapicie opracowania, na jaw wyszło, że owe dane rzeczywiście przekazywane są przez platformę m.in. do oddziału w Chinach. W samej polityce prywatności zostało to ujęte w dość nieoczywisty sposób, gdyż nie zostało to określone wprost. W dokumencie pod zakładką „Nasza Grupa korporacyjna" (dalej jako „Grupa korporacyjna") użytkownik może dowiedzieć się, że „*jako podmiot o zasięgu globalnym Platforma korzysta ze wsparcia szeregu jednostek należących do grupy korporacyjnej*" i w tym celu podmioty te przetwarzają informacje podane przez użytkownika, informacje zebrane automatycznie oraz informacje pochodzące z innych źródeł. Dopiero po wejściu w szczegóły odesłań i linków znajdujące się w wymienionej zakładce Użytkownik może dowiedzieć się, że podmioty należące do Grupy korporacyjnej to m.in. Chiny, Malezja, Brazylia czy Singapur.

Podmioty uzyskują zdalny dostęp do danych osobowych Użytkowników. Przedstawiciele Platformy wychodząc na przeciw obawom korzystających uspokajają, że chodzi jedynie o dostosowanie algorytmów aplikacji do preferencji Użytkowników, niemniej takie zapisy Polityki prywatności budzą uzasadnione wątpliwości co do ich zgodności z RODO (Podolski 2023).

Jak stanowi preambuła RODO[3] transgraniczne przekazywanie danych osobowych poza obszar Unii Europejskiej jest kwestią bardzo ryzykowną, bowiem może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać swojego prawa do ochrony danych osobowych, w szczególności w zakresie ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem informacji. Warto dodać, że transfer danych poza Unię Europejską (dalej jako „UE") nie jest prostą sprawą, bowiem podstawą prawną dla transferów danych poza UE mogą być standardowe klauzule umowne, wiążące reguły korporacyjne lub decyzje o odpowiednim poziomie ochrony wydane przez Komisję Europejską. Po stronie TikToka spoczywa obowiązek do zapewnienia, że każda z tych podstaw prawnych jest należycie przestrzegana i że dane użytkowników są odpowiednio chronione przed nieautoryzowanym dostępem[4]. W kontekście stricte przekazywania danych osobowych Użytkowników Platformy do Chin, a także enumeratywnie wymienionych wymogów postawionych przez UE w akcie RODO nie wszystkie przesłanki są spełnione przez platformę, aby transfer dany był w pełni swobodny i legalny. W zakresie standardowych klauzul umownych, czyli klauzul, zatwierdzonych przez Komisję Europejską, które mają na celu zapewnienie, że dane przekazywane poza granice UE są chronione w sposób porównywalny do wymogów, jakie przewiduje RODO[5], TikTok stosuje standardowe klauzule umowne do przekazywania danych do krajów trzecich, w tym do Chin. Także w zakresie wiążących reguł korporacyjnych, przekazywanie danych w ramach grupy firm ByteDance, czyli właściciela TikToka są stosowane - są to wewnętrzne zasady ochrony danych osobowych stosowanymi przez grupy przedsiębiorstw międzynarodowych, które winny być zatwierdzone przez odpowiedni organ ochrony danych[6]. Niezgodność pojawia się dopiero na etapie ogólnym - decyzji o odpowiednim poziomie ochrony, który w tym aspekcie wydaje się być najbardziej kluczowy, bowiem dotyczy kwestii gwarancji bezpieczeństwa transferowanych danych, a z tym tożsamego bezpieczeństwa Użytkowników. Decyzyjność w tym

[3] RODO, preambuła pkt (116).
[4] https://gdprlocal.com/cross-border-data-transfers-post-gdpr/.
[5] RODO, preambuła pkt (81).
[6] RODO, preambuła pkt (108).

temacie przypada Komisji Europejskiej, która musi uznać, że dany kraj jest w stanie zapewnić odpowiedni poziom ochrony danych, a samo przekazywanie danych do tego kraju jest dozwolone. Chiny nie znajdują się na liście krajów z decyzją stwierdzającą adekwatność ochrony, dlatego TikTok musi polegać na innych mechanizmach zabezpieczających, a sam transfer budzi obawy i kontrowersje.

Organy Unii Europejskiej nie pozostają obojętni na obawy Użytkowników Platformy. Parlament Europejski oraz inne organy nadzorujące ochronę danych osobowych, takie jak Europejski Inspektor Ochrony Danych, apelowali o podjęcie działań w zakresie kwestii przetwarzania przez Platformę danych osobowych i zgodności z prawem, przede wszystkim z RODO. Doprowadziło to do wszczęcia w 2022 r. kilku postępowań kontrolnych (European Commission for Internal Market 2022).

OCHRONA DANYCH OSOBOWYCH DZIECI

TikTok jako platforma, której głównym założeniem jest kreacja przez Użytkowników krótkich filmików z podłożonym dźwiękiem czy też różnego rodzaju kontentu skupia w swoim obszarze wiele młodych osób. Często użytkownikami TikTok są osoby, które fałszywie oświadczają, że ukończyły 13 rok życia i tworzą swój profil oraz biorą aktywny udział w tworzeniu społeczności TikToka. Na oficjalnej stronie Platformy dostępny jest dokument dotyczący bezpieczeństwo i dobra osób niepełnoletnich (TikTok Technology Limited 2024), który został wydany i obowiązuje od 17 kwietnia 2024 r.. Z dokumentu wynika, że Platforma jest mocno zaangażowana w zapewnienie bezpieczeństwa Użytkownikom, a pierwszą zasadą jest to, że Użytkownik musi spełnić wymóg minimalnego wieku, jeśli chce korzystać z aplikacji. Aby mieć konto na Platformie, wymagane jest ukończenie co najmniej 13 roku życia, z zastrzeżeniem, że w niektórych regionach obowiązują dodatkowe ograniczenia wiekowe oparte na prawie lokalnym. W praktyce jednak weryfikacja wieku osób korzystających z aplikacji jest znikoma, dopiero w momencie zgłoszenia przez innego z Użytkowników TikTok zablokuje konto osoby, która nie spełnia wymogu minimalnego wieku. TikTok zablokuje także nieodpowiednie treści zarówno dla młodszych, jak i pełnoletnich Użytkowników. Do ograniczeń treści powyżej 18 roku życia należą m.in.: zaburzenia odżywiania i postrzeganie własnego ciała, nagość i ekspozycja ciała, hazard i różnego rodzaju używki. W praktyce jednak często treści tego typu i tak są udostępniane i promowane przez Użytkowników, którzy obchodzą system weryfikacji TikToka lub zwyczajnie reakcja administratorów Platformy jest zbyt późna, a treści docierają

do małoletnich Użytkowników.

TikTok dopuścił się nieprawidłowej praktyki w zakresie przetwarzania danych osobowych dzieci, co zostało wykryte przez irlandzki organ nadzorczy a także poskutkowało wydaniem wiążącej decyzji przez Europejską Radę Ochrony Danych (dalej jako „EROD"). Naruszenia te miały miejsce w okresie od 31 lipca do 31 grudnia 2020 r. i dotyczyły powyżej opisanej niekonsekwencji w wprowadzonych przez TikToka narzędzi weryfikacji wieku. EROD we wspomnianej decyzji wyraziła poważne wątpliwości co do skuteczności mechanizmu weryfikacji wieku wprowadzonego przez TikToka. Stwierdzono m.in., że zastosowana „bramka wiekowa", która została wprowadzona w celu uniemożliwienie Użytkownikom w wieku poniżej 13 roku życia dostęp do Platformy, była niedostatecznie weryfikowana, co w rezultacie było łatwo obejść, a środki stosowane po uzyskaniu przez użytkowników dostępu do TikToka nie były stosowane wystarczająco systematycznie[7].

TikTok w tym samym okresie czasu naruszył także jedną z fundamentalnych zasad przetwarzania danych osobowych - zasadę rzetelności RODO przy przetwarzaniu danych osobowych dotyczących dzieci w wieku od 13 do 17 lat. EROD oraz irlandzki organ nadzoru również zajęli stanowisko w tej sprawie. Zgodnie z zasadą rzetelności[8] *dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty w odniesieniu do osoby, której dane dotyczą.* Co to oznacza w praktyce? Oznacza to, że dane osobowe powinny być przetwarzane w sposób przejrzysty, czyli osoby, których dane dotyczą, muszą być informowane o tym, w jaki sposób ich dane będą przetwarzane, kto będzie administratorem danych oraz w jakim celu są one pozyskiwane. Zgodnie z tą zasadą dane osobowe nie mogą być przetwarzane w sposób, który mógłby wprowadzać osoby, których dotyczą, w błąd ani nie mogą być zbierane w sposób podstępny lub nieuczciwy, a stricte samo przetwarzanie danych osobowych musi być zgodne z obowiązującymi przepisami prawa[9].

W zakresie naruszenia wykrytego przez irlandzki organ nadzorczy, naruszenie dotyczyło praktyk polegających na stosowaniu powiadomień typu pop-up tj.: okienka rejestracji oraz okienka publikowania wideo. W wyniku analizy dokonanej przez EROD stwierdzono, że w przypadku obu tych okien, opcje nie były przedstawiane użytkownikowi w sposób obiektywny i neutralny. W oknie

[7] https://www.edpb.europa.eu/news/news/2023/following-edpb-decision-tiktok-ordered-eliminate-unfair-design-practices-concerning_pl

[8] Art. 5 ust. 1 lit. a RODO

[9] Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

rejestracyjnym sugerowano małoletnim wybór konta publicznego poprzez kliknięcie prawego przycisku oznaczonego jako „*Pomiń*", co znacząco wpływało później na prywatność małoletniego na Platformie, przykładowo przez udostępnianie komentarzy do stworzonych wideo. Małoletni byli także w sposób podprogowy nakłaniani, aby zamiast jaśniejszego przycisku „*Anuluj*" kliknąć przycisk „*Opublikuj teraz*", był on bowiem wyświetlany pogrubionym, ciemniejszym tekstem umieszczonym po prawej stronie. Oznaczenie swojego tiktoka jako prywatny, było znacznie bardziej skomplikowane, należało najpierw wybrać opcję „*Anuluj*", a następnie poszukać ustawień prywatności, aby przejść na tzw. konto prywatne. Platforma zatem zachęcała małoletnich Użytkowników do wyboru domyślnych ustawień publicznych, utrudniając im dokonywanie wyborów korzystnych dla ochrony ich danych osobowych. Zgodnie ze stanowiskiem EROD administratorzy nie powinni utrudniać osobom, których dane dotyczą, dostosowania ustawień prywatności i ograniczenia przetwarzania ich danych osobowych. Decyzja została przyjęta przez irlandzki organ ochrony danych, a oprócz upomnienia i nakazu zapewnienia zgodności z przepisami, irlandzki organ ochrony danych nałożył na TikToka karę pieniężną w wysokości 345 mln euro. TikTok Technology (Dublin, Irlandia) 10 października 2023 r. wniósł skargę przeciwko EROD. Strona skarżąca zażądała stwierdzenie nieważności wiążącej decyzji nr 2/2023 z dnia 2 sierpnia 2023 r. w przedmiocie sporu przedłożonego przez Irish SA w odniesieniu do TikTok Technology Limited i obciążenie strony pozwanej kosztami postępowania[10].

WYCIEK DANYCH OSOBOWYCH KLIENTÓW PORTALU PANDABUY.COM

TikTok jako platforma o bardzo dużej popularności, która z roku na rok zyskuje większe grono odbiorców i zasięg o charakterze globalnym pośrednio przyczynia się do rozprzestrzeniania naruszeń prawa. Internet niejednokrotnie obiegały różnego rodzaju treści, które nie powinny nigdy być przeznaczone do wglądu publicznego. Jednym z miejsc, o globalnym zasięgu jest właśnie Platforma TikTok, gdzie poufna informacja może zostać rozprzestrzeniona do bardzo szerokiego grona odbiorców zaledwie w kilka minut. Przykładem pośredniego przyczynienia się do naruszenia prawa danych osobowych może być wyciek danych osobowych klientów portalu pandabuy.com (dalej jako „pandabuy")

29 kwietnia 2024 r. Mirosław Wróblewski, Prezes UODO zawiadomił

[10] (Dz. U. UE. C. z 2023 r. poz. 782).

Prokuraturę Rejonową Warszawa Śródmieście-Północ o podejrzeniu popełnienia przestępstwa przez sprawców publikacji danych polskich klientów platformy sprzedażowej pandabuy[11]. Pandabuy to platforma e-commerce specjalizująca się w pośrednictwie zakupów z chińskich serwisów. Strona działa jako pośrednik, pomagając użytkownikom spoza Chin w zakupie produktów, które mogą być trudne do zdobycia bez znajomości języka chińskiego czy chińskich metod płatności. Dane osobowe klientów platformy wyciekły z serwisu i zostały opublikowane w zagregowanych formach na innych stronach i portalach internetowych w tym w głównej mierze na TikToku. Najprawdopodobniej informacja ta zdobyła tak gwałtowny rozgłos na TikToku ze względu na to, że często kupującymi były osoby należące do młodszego pokolenia, niekiedy osoby, które w internecie kreują wizerunek zamożnych, z kolei platforma pandabuy nie sprowadzała z Chin produktów wysokiej jakości. Zakres danych objętych wyciekiem był szeroki i obejmował: imiona i nazwiska, adresy e-mail, numery telefonów, identyfikatory użytkowników, adresy IP, hasła, adresy dostaw, dane dotyczące zamówień i płatności. Wyciek tych danych był nie tylko naruszeniem i skutkiem nieodpowiedniego przechowywania i bezpieczeństwa danych, ale rzeczywiście stworzył zagrożenie dla użytkowników serwisu, bowiem dane te posłużyły autorom strony „lista-drillowcow.pl", utworzonej 7 kwietnia, do stworzenia interaktywnej mapy Polski, na której zamieścili informacje odnoszące się do polskich klientów tego serwisu, tj. m. in. ich imiona i nazwiska oraz adresy dostawy.

W ocenie Prezesa UODO przetwarzanie danych osobowych polskich klientów oraz publikacja na stronach internetowych, przez osoby administrujące tymi stronami odbywało się bez podstawy prawnej. Tym samym naruszony został przepis art. 107 ust. 1 RODO. Zgodnie z tym artykułem: *kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch*[12].

CZY INFLUENCERZY MUSZĄ STOSOWAĆ RODO?

Ściśle powiązanym zjawiskiem z Platformą TikTok jest fakt obecności na niej specyficznego typu Użytkowników - influencerów. Influencerzy to twórcy, którzy należą raczej do osób popularnych i opiniotwórczych w sieci - jak sama

[11] Urząd Ochrony Danych Osobowych, Prezes UODO zawiadomił prokuraturę o wycieku danych osobowych klientów portalu pandabuy.com.
[12] Art. 107 ust.1 RODO.

etymologia tego słowa wskazuje, z języka angielskiego „*influence*" oznacza wpływ. Bycie influencerem to z możliwości kreowania uproszczonego, krótkiego i chwytliwego przekazu, przy bardzo ograniczonych kosztach jego produkcji i rozpowszechniania, co z kolei świetnie sprawdza się na TikToku, gdzie przekaz i komunikacja odbywa się za pośrednictwem krótkich nagrań (Modzelewski 2023, s. 158). Działalność influencerów często polega na pośredniczeniu pomiędzy marką a konsumentem, co może stanowić formę ukrytej reklamy (Grzybczyk 2020, s. 172). Działalność influencerów jest działalnością odpłatną, a co za tym idzie wielu z nich ma swoje firmy i w rozumieniu przepisów prawa jest przedsiębiorcą, a w związku z tym jest on zobowiązany do przestrzegania postanowień RODO. Jak w przypadku każdej działalności możliwe jest dopuszczenie się naruszeń przepisów RODO oraz wycieku danych osobowych, na szczeblu inflfluencer - odbiorca oraz na szczeblu influencer - zlecający. W wypadku stwierdzenia, że działalność influencera narusza postanowienia RODO osoba pokrzywdzona ma prawo wszczęcia postępowania przed Urzędem Ochrony Danych Osobowych (dalej jako „UODO") (Podolski 2023).

PODSUMOWANIE

TikTok jako platforma o globalnym zasięgu, skupiająca w swoim obszarze miliardy użytkowników jest swoistą kolebką dla naruszeń różnych dziedzin prawa w tym również prawa ochrony danych osobowych. Przetwarzanie danych, a także ich bezpieczeństwo dalej budzi i najprawdopodobniej będzie budzić kontrowersje i będzie stałym tematem kontroli organów unijnych. Platforma jest odpowiedzialna bezpośrednio za naruszenia RODO czy to w zakresie przetwarzania i bezpieczeństwa danych osobowych, poprzez niejasną Politykę prywatności, jak i przekazywanie danych osobowych do administratorów w Chinach, mimo wyraźnego braku pozytywnej decyzji Komisji Europejskiej stwierdzającej adekwatność ochrony danych, czy też w zakresie ochrony danych osobowych dzieci, co wzbudziło szczególne obawy w irlandzkim organie nadzoru.

Szczególnym aspektem jest fakt, że TikTok przyczynia się również do pośredniego naruszenia przetwarzania i bezpieczeństwa danych osobowych jako Platforma, która stanowi narzędzie pracy dla infuencerów oraz skupia w swoim obrębie duże grono internautów, którzy korzystając z możliwości szybkiego i dalekosiężnego przekazywania informacji może w dalszym ciągu doprowadzać do wszelkiego wycieku danych osobowych, a tym samym stanowić zagrożenie dla osób, do których owe dane należą.

BIBLIOGRAFIA

Akty prawne

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. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Literatura

Bodanka O.
2022 *Naruszenie wizerunku przy wykorzystaniu technologii deepfake – analiza prawna i praktyczna.* „Opolskie Studia Administracyjno-Prawne".

Brejza K.
2022 *TikTok jako współczesne źródło wiedzy,* BiBliotheca Nostra.

European Commission for Internal Market
2022 *China's access to TikTok data of EU citizens.*

Grzybczyk K.
2020 *Rozrywki XXI wieku a prawo własności intelektualnej.*

Modzelewski B.
2023 *Współczesne wyzwania z zakresu praw własności intelektualnej w dobie przesileń cywilizacyjnych. Zagadnienia wybrane na kanwie doświadczeń prawnych Stanów Zjednoczonych Ameryki Północnej.*

Podolski K.
2023 *TikTok, a RODO.*

2023 *Zgłoszenie influencer do UOKiK.*

TikTok Technology Limited
2023 *Polityka prywatności.*
2024 *Bezpieczeństwo i dobro osób niepełnoletnich.*

Urząd Ochrony Danych Osobowych

2024 *Prezes UODO zawiadomił prokuraturę o wycieku danych osobowych klientów portalu pandabuy.com.*

Źródła internetowe

https://rkrodo.pl/tik-tok-a-rodo/#Jakie_dane_osobowe_i_informacje_przetwarza_Tik_Tok [dostęp: 01.03.2024].

https://www.edpb.europa.eu/news/news/2023/following-edpb-decision-tiktok-ordered-eliminate-unfair-design-practices-concerning_pl [dostęp: 01.03.2024].

Lex, Skarga wniesiona w dniu 10 października 2023 r. - TikTok Technology/ Europejska Rada Ochrony Danych, (Dz. U. UE. C. z 2023 r. poz. 782). [dostęp: 01.03.2024].

ISBN: 978-83-67959-67-4