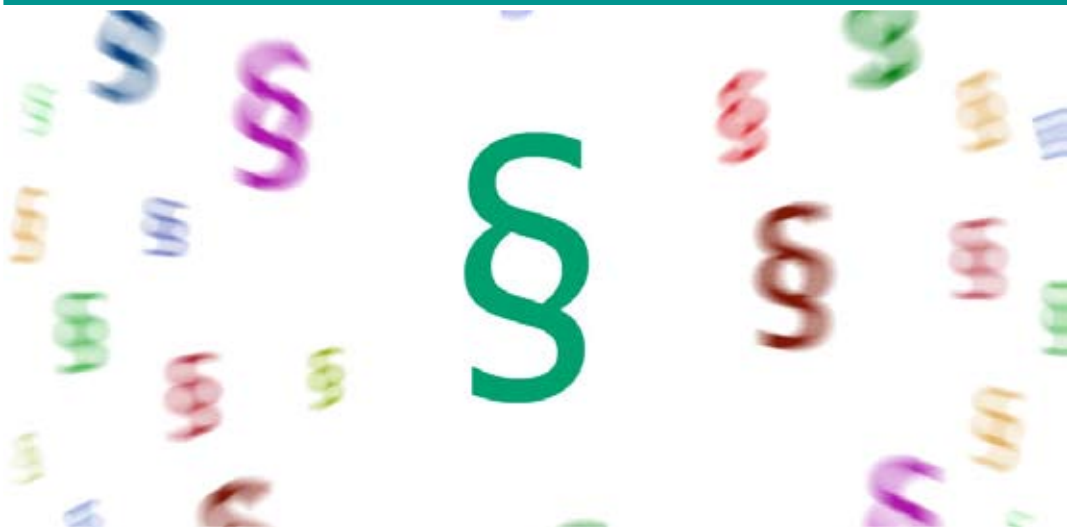
Ochrona dóbr osobistych i danych osobowych



Piotr Waglowski

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

PARP

WEB.GOV.PL
WSPIERAMY E-BIZNES

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

Autor:
Piotr Waglowski

Wydawca:

Polska Agencja Rozwoju Przedsiębiorczości (PARP)
ul. Pańska 81/83
00-834 Warszawa

www.parp.gov.pl

Skład:
Marcin May
PARP

Wydanie I

Publikacja bezpłatna

Publikacja powstała w ramach projektu „Uruchomienie wielofunkcyjnej platformy komunikacji internetowej wspierającej realizację działań 8.1 i 8.2 PO IG", realizowanego przez Polską Agencję Rozwoju Przedsiębiorczości, współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego.

Wspieramy e-biznes www.web.gov.pl

Spis treści

1. Dobra osobiste

Dobra osobiste przysługują wszystkim **osobom fizycznym**. Mają charakter niemajątkowy, nie mogą być przenoszone (są niezbywalne), nie można się ich zrzec, a gasną wraz ze śmiercią podmiotu uprawnionego. Kodeks cywilny wymienia pewien **przykładowy katalog** takich dóbr: zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Dobra te chronione są przez prawo cywilne niezależnie od ochrony przyznanej im na podstawie innych przepisów. Otwarty katalog dóbr osobistych powiększa się m.in. w wyniku orzecznictwa sądowego. Obejmuje - poza wskazanym katalogiem - również dobra osobiste związane ze sferą życia prywatnego, rodzinnego i strefą intymności. Jak stwierdził Sąd Najwyższy[1]: ochrona w tym zakresie może odnosić się do wypadków ujawnienia faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać. Dlatego właśnie prywatność jest dobrem osobistym człowieka.

Dobra osobiste **przysługują odpowiednio również osobom prawnym**. Sformułowanie „odpowiednio" oznacza, że osoby prawne nie są chronione dokładnie tak samo, jak osoby fizyczne. Osoba prawna nie ma np. wizerunku, które to pojęcie odpowiada - w pewnym uproszczeniu - temu, co można zarejestrować (wizerunek to prawie tyle, co zdjęcie, rysunek danej osoby fizycznej, czasem mowa o innych rodzajach wizerunku, np. w przypadku, gdy rejestrujemy czyjąś wypowiedź). Sąd Najwyższy uznał[2], że nie jest wizerunkiem osoby prawnej ani wizerunek miejsca jej siedziby ani wizerunki osób, wchodzących w skład jej organów, lub nawet całego zespołu i tym podobnych jej elementów (z osobna lub łącznie wziętych). Na podobnej zasadzie nie można mówić o zdrowiu osoby prawnej. W innym orzeczeniu sąd uznał[3], że dobra osobiste osób prawnych to „wartości niemajątkowe, dzięki którym osoba prawna może funkcjonować zgodnie ze swym zakresem działań".

Ochrona dóbr osobistych obejmuje zarówno ochronę w przypadku naruszenia dóbr, ale również w przypadku ich zagrożenia (w przypadku zagrożenia dóbr osobistych również można skorzystać z roszczeń przewidzianych przez Kodeks). Ochrona przysługuje jednak tylko w przypadku **zagrożenia lub naruszenia bezprawnego**. Istnieją pewne przesłanki, które wyłączają bezprawność. Można tu wymienić zgodę uprawnionego, działanie oparte na przepisie prawnym lub realizujące prawo podmiotowe, działanie w obronie uzasadnionego interesu społecznego Działanie zagrażające lub naruszające czyjeś dobra osobiste może również polegać na zaniechaniu. Jednocześnie należy pamiętać, że bezprawność czynu naruszającego dobro osobiste domniemywa się (w konsekwencji należy przyjąć, że ten, kto naruszył dane dobro osobiste, w przypadku sporu musi wykazać, że jego działanie nie było bezprawne).

Dobro osobiste powinno odpowiadać interesom przeciętnej jednostki ludzkiej i mieć charakter obiektywny, to znaczy, że przy ocenie naruszenia np. czci należy mieć na uwadze nie tylko subiektywne odczucie osoby żądającej ochrony prawnej, ale także obiektywną reakcję w opinii społeczeństwa[4].

1.1. Niezamknięty katalog dóbr osobistych w „społeczeństwie informacyjnym"

Praktycznie wszystkie z wymienionych w katalogu kodeksowym dóbr osobistych mogą być zagrożone lub naruszone w Internecie (być może tylko poza nietykalnością mieszkania). Umieszczenie migającej grafiki na forum internetowym, na którym często spotykają się osoby chore na epilepsje, może doprowadzić takie osoby do śmierci, a na pewno stanowi zagrożenie **zdrowia**. Wolność jest również rozumiana jako **wolność** od obawy i strachu, od użycia przemocy lub zrealizowania groźby przez inną osobę.

Poprzez publikację w Internecie może dojść do naruszenia czci (a więc zarówno dobrego imienia, jak i godności osobistej) - w takim przypadku dodatkowym wsparciem ochrony są przepisy prawa karnego, które przewidują karę za pomawianie w środkach masowego komunikowania się. można naruszyć również prawo do **nazwiska** (chociażby przez bezprawne umieszczenie takiego nazwiska w nazwie domenowej). W kontekście Internetu nowego znaczenia nabiera ochrona przyznawana **pseudonimowi**. Jak zauważył Sąd Najwyższy[5]: „nazwa użytkownika, którą posługuje się osoba korzystająca z serwisu internetowego, podlega ochronie prawnej na takiej podstawie, na jakiej ochronie podlega nazwisko, pseudonim lub firma". Naruszenie prawa do **wizerunku**, to np. opublikowanie czyjegoś zdjęcia bez jego zgody. Ochronę wizerunku dodatkowo wspierają przepisy prawa autorskiego: rozpowszechnianie wizerunku wymaga zgody osoby na nim przedstawionej, przy czym nie dotyczy to osób powszechnie znanych, lub stanowiących jedynie szczegół całości, takiej jak np. zgromadzenie.

1 *Wyrok Sądu Najwyższego z dnia 18 stycznia 1984 r., sygn. I CR 400/83, OSNC 1984/11/195*
2 *Wyrok Sądu Najwyższego - Izba Cywilna z dnia 25 maja 1977 r., sygn. I CR 159/77*
3 *Wyrok Sądu Apelacyjnego w Warszawie z dnia 19 grudnia 1995 r. sygn. IACR 1013/95*
4 *Wyrok Sądu Najwyższego z dnia 16 stycznia 1976 r., sygn. II CR 692/75, OSN 1976/11/251*
5 *Wyrok Sądu Najwyższego z dnia 11 marca 2008 r., sygn. IICSK539/07*

Wobec powyższych uwag warto odnotować jedno z pierwszych orzeczeń polskich sądów na temat stosowania tzw. linków. Jak zauważył Sąd Apelacyjny w Krakowie[6]: „Okoliczność, iż strona pozwana nie miała żadnego wpływu na zawartość witryn internetowych, do których odesłała użytkowników portalu, nie jest doniosła dla oceny jej odpowiedzialności za naruszenie dóbr osobistych powódki. Odpowiedzialność ta łączy się bowiem z zamieszczeniem na stronie portalu internetowego strony pozwanej odesłania (linku) do witryny, na której znajdował się wizerunek powódki oraz rekomendacją tej witryny przez stronę pozwaną, a nie z wprowadzeniem tej witryny do sieci internetowej i ukształtowaniem jej zawartości".

Oczywista wydaje się ochrona **korespondencji**, a nawet „komunikacji". Ochrona takiego dobra, w związku z coraz powszechniejszym wykorzystaniem Internetu, wydaje się coraz bardziej znacząca. Przeglądanie cudzej poczty elektronicznej, jej publikowanie w Internecie bez stosownego uprawnienia, może stanowić zagrożenie tego dobra osobistego, obok zagrożenia prywatności.

Warto pamiętać, że **twórczość** - sama w sobie - jest również chronionym przez prawo cywilne dobrem oso-bistym. W tym miejscu warto przywołać tezę Sądu Apelacyjnego w Warszawie[7], który stwierdził, że „dla prawno-autorskiej ochrony utworu nie ma znaczenia, w jaki sposób dokonujący naruszenia wszedł w jego posiadanie lub też, w jaki sposób utwór do niego dotarł, w szczególności nie ma znaczenia okoliczność, iż utwór, stanowiący przedmiot naruszenia dotarł do dokonującego naruszenia jako niezamawiana korespondencja przesyłana drogą elektroniczną, tak zwany spam". Ten konkretny spór dotyczył opublikowania przez redakcję nadesłanego do niej, a niezamówionego wcześniej utworu - wiersza. W tym samym orzeczeniu sąd uznał ochronę również takich twórców, którzy pozostają dla naruszającego ich prawa anonimowi: „Ochronie podlega twórca nie tylko powszechnie znany, którego utwory są publikowane w dużym nakładzie, lecz każdy, którego prawa do utworu zostały w jakikolwiek sposób naruszone, prawo autorskie nie dokonuje rozróżnień w zakresie ochrony w zależności od wartości utworu i uznania, jakim cieszy się autor". Ta teza może mieć istotne znaczenie dla tych wszystkich, którzy chcieliby wykorzystać „znalezione w Internecie" utwory, o których autorach nic nie wiedzą.

W przypadku osób fizycznych i osób prawnych można mówić o ochronie **firmy**, a więc takiego oznaczenia, pod którym działa przedsiębiorca. W przypadku osób fizycznych będzie to - co do zasady - imię i nazwisko, ewentualnie wraz z dodatkowymi oznaczeniami, takimi jak np. wskazanie na przedmiot działalności; w przypadku osób prawnych będzie to ich nazwa zawierająca również w sobie określenie formy prawnej. Zgodnie z orzecznictwem - „firma, pod którą prowadzi swoje przedsiębiorstwo dany podmiot, ma w stosunkach prawnych, w jakie wchodzi, takie znaczenie, jak dla osoby fizycznej przedstawia jej nazwisko"[8].

1.2. Prywatność

Dobrem osobistym, które nie jest przewidziane w katalogu kodeksowym, jest prywatność. Zasługuje ona na szczególne wyróżnienie w tym opracowaniu, ze względu na rozwój „społeczeństwa informacyjnego", którego członkowie zyskują coraz większe techniczne możliwości ingerowania w to dobro. Ochrona prawa do prywatności jest regulowana w sposób bardzo rozbudowany. Przepisy poświęcone prawu do prywatności znalazły się w umowach międzynarodowych dotyczących praw człowieka, np. w Europejskiej Konwencji Praw Człowieka, znalazły się również w prawie Unii Europejskiej, w Konstytucji Rzeczypospolitej Polskiej i szeregu ustaw szczegółowych, jak np. w prawie prasowym. Cywilnoprawnej ochronie prawa do prywatności, jako dobra osobistego człowieka, towarzyszy również administracyjno-prawna ochrona danych osobowych (której poświęcono oddzielny rozdział niniejszego opracowania). Wsparciem dla ochrony prywatności są również niektóre przepisy prawa karnego.

W zakresie prawa do prywatności, jako podstawowego prawa człowieka, warto odesłać do art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (Europejskiej Konwencji Praw Człowieka), z którego wynika, że każdemu przysługuje prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Jednocześnie przepis ten wprowadza zasadę, zgodnie z którą niedopuszczalna jest ingerencja władzy publicznej w korzystanie ze wspomnianego 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 prywatności może być więc ograniczone, ale po spełnieniu szeregu warunków.

Na tle tego przepisu zapadały już orzeczenia Europejskiego Trybunału Praw Człowieka, które warto przywołać w kontekście ochrony prywatności w „społeczeństwie informacyjnym". Trybunał uznał na przykład, że doszło do naruszenia art. 8 Konwencji w sprawie, w której chodziło o monitorowanie pracownicy jednej z brytyjskich uczelni (ustalono w trakcie procesu, że monitoring polegał m.in. na sprawdzaniu odwiedzanych przez skarżącą witryn internetowych, analizowano daty i czas odwiedzin tych witryn, monitorowano również aktywność związaną z wykorzystywaniem przez nią poczty elektronicznej)[9].

6 *Wyrok Sądu Apelacyjnego w Krakowie z dnia 20 lipca 2004 r., sygn. I ACa 564/04*
7 *Wyrok Sądu Apelacyjnego w Warszawie z dnia 14 marca 2006 r., sygn. VI ACa 1012/2005*
8 *Wyrok Sądu Apelacyjnego w Poznaniu z dnia 22 października 1991 r., sygn. I ACr 400/90*
9 *Wyrok Europejskiego Trybunału Praw Człowieka z dnia 3 kwietnia 2007 r. w sprawie Copland v. the United Kingdom (no. 62617/00)*

Przepisy Konstytucji RP przewidują szereg przepisów, które dotyczą prywatności. Przepisy te dają podstawę do dalszych regulacji tej kwestii w przepisach rangi ustawowej. Należy jednak pamiętać, że to właśnie w Konstytucji znalazło się prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, tam też znalazły się gwarancje wolności komunikowania się i ochrony tajemnicy takiego komunikowania, gwarancje wolności wyrażania poglądów oraz pozyskiwania i rozpowszechniania informacji, a także gwarancje ochrony konsumenta przed działaniami zagrażającymi jego prywatności.

Co odnotowano już w pierwszej części tego opracowania (por. rozdział 1.4) - w prawie Unii Europejskiej problematyka ochrony prywatności pojawia się również w szeregu aktów prawnych.

W konsekwencji rozlicznych regulacji dotyczących prawa do prywatności przepisy dotyczące tej sfery znalazły się również w przepisach rangi ustawowej, wśród których należy wymienić ustawę Prawo prasowe, ustawę Prawo telekomunikacyjne, ustawę o zwalczaniu nieuczciwej konkurencji, czy ustawę o świadczeniu usług drogą elektroniczną.

Prywatność jest dobrem osobistym człowieka i podlega ochronie na podstawie przepisów Kodeksu cywilnego. Ma to swoje uzasadnienie w ugruntowanym już orzecznictwie Sądu Najwyższego i innych sądów. Zgodnie z podstawowym dla tej problematyki orzeczeniem Sądu Najwyższego[10]: „Otwarty katalog dóbr osobistych (art. 23 i 24 kc) obejmuje także dobra osobiste związane ze sferą życia prywatnego, rodzinnego, ze sferą intymności. Ochrona w tym zakresie może odnosić się do wypadków ujawnienia faktów z życia osobistego i rodzinnego, nadużywania uzyskanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać".

Problematyka ochrony prywatności zaczyna również pojawiać się w orzeczeniach sądowych, które dotyczą szeroko pojętego „społeczeństwa informacyjnego". Wypada tu odnotować np. wyrok Sądu Apelacyjnego w Warszawie[11], który uznał, że przesyłanie krótkich wiadomości tekstowych (SMS) do byłego współpracownika, stanowiło w tej konkretnej sprawie naruszenie prawa do prywatności. W sprawie istotne było to, że wiadomości przesyłano w dłuższym czasie; chociaż abonent telefonu komórkowego domagał się zaprzestania takiego procederu, przesyłający nie spełnili tej prośby, wiadomości te miały charakter „mobilizujący do aktywności", chociaż osoba, która otrzymywała wiadomości (niektóre dochodziły o 5.00 czy 6.00 rano) nie współpracowała już wówczas z wysyłającym je podmiotem. Tego typu wyroki dają również podstawę do formułowania tezy, że na podstawie przepisów o ochronie dóbr osobistych, w szczególności prawa do prywatności, można walczyć ze zjawiskiem przesyłania niezamówionej korespondencji elektronicznej (czyli ze „spamem"; problematyce tej poświęcone będą również rozważania na gruncie przepisów o świadczeniu usług drogą elektroniczną w dalszej części niniejszego opracowania, por. rozdział 4.3.5).

1.3. Ochrona dóbr osobistych

Przepisy przewidują zarówno niemajątkowe środki ochrony dóbr osobistych, jak i majątkowe środki ochrony. Do niemajątkowych środków ochrony można zaliczyć np. roszczenie o zaniechanie działania zagrażającego dobrom osobistym (o ile nie jest ono bezprawne). Będzie nim również możliwość żądania dopełnienia czynności potrzebnych do usunięcia skutków naruszenia (w szczególności: stosowne co do treści i formy oświadczenie, ale nie tylko, gdyż można sobie wyobrazić, że w przypadku naruszeń w Internecie takim dopełnieniem czynności będzie np. umieszczenie na serwerze specjalnego przygotowanego pliku zawierającego instrukcje dla wyszukiwarek internetowych, by usunęły dany zasób internetowy z wyników wyszukiwania). Kodeks cywilny przewiduje również inne możliwości stosowania niemajątkowych środków ochrony, do których można zaliczyć np. powództwo o ustalenie bezprawności naruszenia.

Wśród majątkowych środków ochrony należy wymienić - przykładowo - możliwość przyznania zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. Poszkodowany może domagać się również odszkodowania na zasadach ogólnych przewidzianych w Kodeksie cywilnym, a to w sytuacji, gdy wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa.

Obok przepisów znajdujących się w Kodeksie cywilnym również inne przepisy zawierają dodatkowe środki ochrony dóbr osobistych (np. omówiona wcześniej ustawa o prawie autorskim i prawach pokrewnych).

Warto w tym miejscu przywołać pewne rozstrzygnięcia, które dotyczyły naruszenia dóbr osobistych w działalności prasowej. Sąd Najwyższy uznał m.in., że również w stosunku do wydawcy można kierować roszczenia niemajątkowe, związane z naruszeniem dobra osobistego w materiale prasowym, a podstawą takich roszczeń będą przepisy Kodeksu cywilnego[12]. W innym rozstrzygnięciu Sąd Najwyższy uznał[13], że „powołanie się na publikację lub wypowiedź innej osoby może - w okolicznościach konkretnej sprawy - okazać się niewystarczające do odparcia zarzutu braku bezprawności naruszenia dóbr osobistych".

10 Wyrok Sądu Najwyższego - Izba Cywilna i Administracyjna z dnia 18 stycznia 1984 r., sygn. I CR 400/83, OSNCP 1984/11 poz. 195

11 Wyrok Sądu Apelacyjnego w Warszawie z 2007 roku, sygn. I ACa 584/06

12 Uchwała Sądu Najwyższego - Izba Cywilna z dnia 7 grudnia 1993 r., sygn. III CZP 160/93

13 Wyrok Sądu Najwyższego - Izba Cywilna z dnia 28 maja 1999 r., sygn. I CKN 16/98

Wreszcie wypada przywołać rozstrzygnięcie, które zapadło na gruncie przepisów Prawa prasowego, które również dotyczy dóbr osobistych. Oto Sąd Apelacyjny w Katowicach stwierdził[14], że „media zobowiązane są do respektowania takich wartości, jakimi są dobra osobiste człowieka. Wolność słowa nie oznacza bowiem dowolności korzystania z niej. Barierę dla dowolności korzystania z wolności słowa stanowi art. 12 Prawa prasowego, zobowiązujący dziennikarzy do zachowania szczególnej staranności i rzetelności przy zbieraniu i wykorzystaniu materiałów prasowych, zwłaszcza sprawdzenia zgodności uzyskanych wiadomości lub podania ich źródła". Tego typu orzeczeń dotyczących funkcjonowania mediów jest niezwykle dużo, a powyżej przywołano jedynie kilka, by zobrazować doniosłość i różnorodność form ochrony dóbr osobistych.

2. Ochrona danych osobowych

Problematyka ochrony danych osobowych regulowana jest w Polsce przepisami Konstytucji RP (m.in. w zakresie prawa do prywatności), ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (w przypadku tej ustawy należy szczególnie zwrócić uwagę na szereg aktów wykonawczych, które mają istotne znaczenie ze względu na dopełnienie obowiązków wynikających z ochrony danych osobowych), ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, przepisami szeregu ustaw szczegółowych. Na poziomie Unii Europejskiej m.in. w takich aktach prawnych, jak Dyrektywa 95/46/EC Parlamentu Europejskiego oraz Rady z 24 października 1995 roku o ochronie osób w związku z przetwarzaniem danych osobowych oraz o swobodnym przepływie takich danych, Dyrektywa 97/66/EC Parlamentu Europejskiego oraz Rady z 15 grudnia 1997 roku regulująca przetwarzanie danych osobowych oraz ochronę prywatności w sektorze telekomunikacyjnym czy Dyrektywa Parlamentu Europejskiego i Rady nr 2002/58/WE z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej (Dyrektywa o prywatności i łączności elektronicznej).

Jeśli chodzi o normy konstytucyjne, to obok ochrony prawnej życia prywatnego oraz o decydowaniu o swoim życiu osobistym, Konstytucja stanowi, że obowiązek ujawnienia danych dotyczących konkretnej osoby musi wynikać z ustawy, a organy władzy publicznej mogą przetwarzać jedynie takie dane osobowe, które są niezbędne w demokratycznym państwie prawnym. Konstytucja daje jednocześnie obywatelowi prawo dostępu do dotyczących go danych, sprostowania lub usunięcia dotyczących go danych nieprawdziwych, niepełnych lub zebranych w sposób niezgodny z przepisami ustawy.

2.1. Ustawa o ochronie danych osobowych i akty wykonawcze

Ustawa o ochronie danych osobowych reguluje: zasady postępowania przy przetwarzaniu danych osobowych, prawa osób fizycznych, których dane są lub mogą być przetwarzane, wprowadza też zasady zabezpieczania przetwarzanych danych osobowych, procedurę rejestracji zbiorów danych osobowych, procedurę przekazywania danych osobowych do państw trzecich oraz sankcje karne związane z naruszeniami prawa o ochronie danych osobowych. Ustawa również ustanawia Generalnego Inspektora Danych Osobowych[15] jako naczelny organ ochrony danych osobowych oraz określa jego kompetencje.

Do ustawy o ochronie danych osobowych wydano również akty wykonawcze, które należy uwzględnić przy analizowaniu obowiązków i praw wynikających z ustawy:

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[16],
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych[17],
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[18],
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych[19].

14 Wyrok Sądu Apelacyjnego w Katowicach z dnia 4 listopada 1999 r., sygn. I ACa 536/99
15 http://www.giodo.gov.pl
16 Dz. U. z 2004 r. Nr 100 poz. 1024
17 Dz. U. z 2006 r. Nr 203 poz. 1494
18 Dz. U. z 2004 r. Nr 100 poz. 1025
19 Dz. U. z 2004 r. Nr 94 poz. 923

Poza ustawą o ochronie danych osobowych i omówioną już wcześniej regulacją Kodeksu cywilnego, dotyczącą ochrony dóbr osobistych, przepisy związane z ochroną danych osobowych znalazły się również w innych aktach prawnych. Istotne jest jednak to, że - zgodnie z ustawą o ochronie danych osobowych - w przypadku, gdy przepisy szczególne przewidują ochronę idącą dalej, niż wynika to z treści ustawy, należy stosować te właśnie przepisy szczególne.

2.2. Pojęcie danych osobowych

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zgodnie z ustawą o ochronie danych osobowych osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości konkretnej osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Danymi osobowymi będą zarówno dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i dane, które są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia, pomimo że nie pozwalają na jej natychmiastową identyfikację. Daną osobową będzie taka informacja, która pozwala na ustalenie tożsamości danej osoby, bez nadzwyczajnego wysiłku i nakładów, zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł. Danymi osobowymi nie będą pojedyncze informacje o dużym stopniu ogólności. W zależności od współwystępowania z innymi informacjami, informacja o dużym stopniu ogólności będzie stanowić daną osobową, gdy zostanie zestawiona z innymi dodatkowymi informacjami, które prowadzą do identyfikacji konkretnej osoby. Pojedynczą informacją, która stanowi dane osobowe, jest np. numer PESEL.

W jednej z decyzji, które dotyczyły danych udostępnionych przez użytkowników serwisu internetowego nasza-klasa.pl, a które dotyczyły skarżącego, Generalny Inspektor Ochrony Danych Osobowych zakwestionował[20] uznanie za dane osobowe informacji o imieniu i nazwisku skarżącego, w połączeniu z informacjami o nazwie i adresie szkoły podstawowej oraz oznaczeniu klasy, do której uczęszczał, wraz z jego wizerunkiem z 1978/1979 roku, stwierdzając: „analiza przedstawionego stanu faktycznego prowadzi jednak do wniosku, że potencjalna możliwość powiązania ww. sekwencji informacji o skarżącym z nim obecnie wymaga zaangażowania niewspółmiernych kosztów, czasu lub działań. Warto przy tym zwrócić uwagę, że imię i nazwisko skarżącego zostało przypisane do jego wizerunku sprzed lat przez osobę trzecią, w formie komentarza do fotografii i w tym sensie informacja ta nie ma charakteru obiektywnego". GIODO publikuje w ramach prowadzonego przez siebie serwisu internetowego również orzeczenia sądów, które dotyczyły wydanych przez niego wcześniej decyzji, a także inne materiały, pozwalające na interpretację ustawy.

Dane osobowe można podzielić na **dane osobowe zwykłe i dane osobowe wrażliwe**. Przepisy ustawy o ochronie danych osobowych wprowadzają w stosunku do pewnych kategorii danych zakaz ich przetwarzania (chociaż przewidują jednocześnie zamkniętą listę sytuacji, w których takie przetwarzanie będzie dopuszczalne). Katalog danych wrażliwych jest katalogiem zamkniętym i obejmuje on:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniową, partyjną lub związkową,
- dane o stanie zdrowia,
- kodzie genetycznym,
- nałogach,
- życiu seksualnym,
- dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

2.3. Przetwarzanie danych

Ustawa definiuje pojęcie **przetwarzania danych osobowych**, które rozumie jako jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Ustawa nie definiuje poszczególnych form przetwarzania danych (z jednym wyjątkiem), w związku z czym należy w stosunku do nich stosować właściwe definicje słownikowe. Wyjątkową formą przetwarzania danych jest **usuwanie danych**. Usuwanie danych jest jedyną formą przetwarzania, która nie wymaga wyrażenia zgody przez osobę, której dane dotyczą. Usuwanie danych to:

- zniszczenie danych osobowych, tzn. - w zależności od nośnika, na jakim dane zostały utrwalone - zniszczenie samego nośnika, albo w przypadku nośników stosowanych w systemach informatycznych, usunięcie znajdującego się na nich zapisu,
- modyfikacja w stopniu uniemożliwiającym identyfikację osoby, której te dane dotyczą, czyli

20 Decyzja GIODO z dnia 3 września 2008 roku, sygn. DOLiS/DEC515/08/22857

sprowadzenie danych do postaci, w której określenie tożsamości osoby fizycznej wymagałaby nadmiernych kosztów, czasu i działań.

Ustawę o ochronie danych osobowych stosuje się do danych osobowych, które są lub mogą być przetwarzane w **zbiorach danych**. Wyjątkiem jest przetwarzanie danych osobowych nieznajdujących się w zbiorze, jeśli przetwarzanie ma miejsce w systemie informatycznym (pewne wyjątki przewiduje również ustawa o świadczeniu usług drogą elektroniczną). Zbiorem danych w rozumieniu ustawy jest „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie".

Zbiór danych podlega **zgłoszeniu celem rejestracji** w Biurze Generalnego Inspektora Ochrony Danych Osobowych z wyjątkami, które wprost wynikają z przepisów ustawy[21]. Takim wyjątkiem objęty jest m.in. zbiór danych osobowych przetwarzanych w związku z zatrudnieniem u administratora danych (tj. zbiorów obecnych i byłych pracowników, a także kandydatów do pracy) oraz świadczeniem administratorowi danych usług na podstawie umów cywilnoprawnych (np. na podstawie umowy zlecenia, umowy o dzieło). Przepisy zwalniające z obowiązku rejestracji zbiorów nie zwalniają administratora z innych obowiązków, takich jak np. stosowanie wymaganych prawem środków bezpieczeństwa związanych z przetwarzaniem danych, oraz obowiązków informacyjnych.

Z przetwarzaniem danych związane jest również pojęcie **administratora danych**, czyli m.in. organu, jednostki organizacyjnej, a także niektórych innych podmiotów wymienionych w ustawie, które decydują o celach i środkach przetwarzania danych. Administratorem danych osobowych wykorzystywanych w zakresie działalności prowadzonej przez przedsiębiorcę jest sam przedsiębiorca, a nie jego organy, czy osoby fizyczne zasiadające w organach przedsiębiorcy. Administratorem danych jest w szczególności spółka z ograniczoną odpowiedzialnością, spółka akcyjna, spółka jawna oraz spółka komandytowa. W przypadku działalności gospodarczej prowadzonej przez osobę fizyczną, administratorem danych jest osoba prowadząca działalność gospodarczą. Pozostaje ona administratorem danych nawet w przypadku wyznaczenia osoby odpowiedzialnej za przetwarzanie danych osobowych. W przypadku powierzenia danych celem ich przetwarzania podmiotowi zewnętrznemu, administratorem danych pozostaje podmiot przekazujący te dane i ciążą na nim w dalszym ciągu, pomimo powierzenia danych, wszystkie obowiązki wynikające z ustawy.

Jedną z przesłanek pozwalających na przetwarzanie danych, jest **zgoda osoby, której dane dotyczą**. Zgody na przetwarzanie danych osobowych nie wolno domniemywać lub dorozumiewać z oświadczeń woli o innej treści. Przetwarzanie danych osobowych jest dopuszczalne jedynie wtedy, gdy osoba, której te dane dotyczą, wyrazi na to zgodę (wyjątkiem jest przetwarzanie danych osobowych polegające na usunięciu dotyczących jej danych). Z treści oświadczenia woli o wyrażeniu zgody na przetwarzanie danych osobowych powinno wynikać, iż wyrażający zgodę z pełną świadomością godzi się na to, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażenie zgody na przetwarzanie danych może obejmować również przetwarzanie w przyszłości, o ile cel przetwarzania nie ulegnie zmianie. Zgoda na przetwarzanie danych, wyrażona w formie pisemnej przez osobę, której dane dotyczą, stanowi jedną z przesłanek umożliwiających przetwarzanie danych „wrażliwych".

2.4. Obowiązek informacyjny

Poinformowanie o fakcie przetwarzania danych osobowych jest jednym z obowiązków ciążących na podmiocie przetwarzającym dane osobowe (administratorze danych). Dane ulegające przetwarzaniu mogą zostać pozyskane przez administratora danych w dwojaki sposób - bezpośrednio od osoby, której dane dotyczą oraz od podmiotu trzeciego. Jeśli przetwarzane dane nie pochodzą bezpośrednio od osoby, której dotyczą, podmiot przetwarzający dane (administrator danych) jest dodatkowo obowiązany poinformować o źródle (pochodzeniu) przetwarzanych danych.

Obowiązek informacyjny powstaje w chwili gromadzenia danych osobowych. Oznacza to, że bezpośrednio po utrwaleniu danych przez podmiot przetwarzający, osobie, której dane dotyczą, przysługuje uprawnienie do uzyskania informacji na temat nazwy i siedziby podmiotu przetwarzającego dane, celu zbierania danych i jego zakresie, prawach osoby związanych z przetwarzaniem, tj. prawie dostępu do danych oraz prawie do ich poprawiania, a także o dobrowolności lub obowiązku podania danych (w przypadku istnienia obowiązku podania danych należy wskazać podstawę prawną istnienia takiego obowiązku). W przypadku pozyskania danych nie od osoby, której dane dotyczą, także o źródle, z którego dane zostały pozyskane. Niedopełnienie obowiązku informacyjnego może być podstawą do wniesienia przez osobę, która nie uzyskała informacji w powyższym zakresie, skargi do Generalnego Inspektora Ochrony Danych Osobowych.

Zakres obowiązku informacyjnego zawiera ponadto zobowiązanie administratora danych do udzielenia informacji dotyczących zasad przetwarzania danych osobowych. Informacji takich administrator danych udziela na wniosek osoby, której dane są przetwarzane. Zobowiązanie to wynika z prawa osób, których

21 Z obowiązku zgłoszenia zwolnieni są administratorzy zbiorów danych wyliczonych w treści przepisu art. 43 ust. 1 ustawy o ochronie danych osobowych.

dane są przetwarzane, do kontroli przetwarzania tych danych. Administrator, w ciągu 30 dni od daty złożenia wniosku przez osobę, której dane są przetwarzane, musi udzielić odpowiedzi, zawierającej informacje o: istnieniu zbioru danych osobowych, administratorze danych - w zakresie jego nazwy i siedziby (w przypadku osoby fizycznej - imienia i nazwiska oraz adresu zamieszkania), celu, zakresie i sposobie przetwarzania danych zawartych w zbiorze, dacie rozpoczęcia przetwarzania danych dotyczących wnioskującej osoby, treści tych danych, podane w zrozumiałej formie, źródle tych danych (z wyjątkiem obowiązywania administratora tajemnicy ustawowej w tym zakresie), udostępnianiu tych danych, a w szczególności o odbiorcach lub kategorii odbiorców, którym dane są udostępniane. Niedopełnienie obowiązku informacyjnego może powodować odpowiedzialność administracyjno-prawną przed Generalnym Inspektorem Ochrony Danych Osobowych oraz karną.

2.5. Zagadnienia organizacyjne i techniczne przetwarzania danych

Administrator danych obowiązany jest zastosować środki techniczne i organizacyjne, które, w zależności od kategorii przetwarzanych danych oraz zagrożeń, zapewnią odpowiednią ochronę przetwarzanym danym. Administrator danych prowadzi dokumentację, opisującą sposób przetwarzania danych oraz środki podjęte w celu ich ochrony. W szczególności, administrator danych powinien zabezpieczyć dane przed:

- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- przetwarzaniem z naruszeniem ustawy,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby upoważnione przez administratora danych. Administrator obowiązany jest prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych. Ma również obowiązek zapewnienia kontroli nad tym, kto, kiedy i jakie dane wprowadził do systemu przetwarzającego dane osobowe oraz komu są one przekazywane.

Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, na dokumentację, prowadzoną przez administratora danych, opisującą sposób przetwarzania danych oraz środki podjęte w celu ich ochrony, składa się: polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

Polityka bezpieczeństwa powinna obejmować swoim zakresem wszystkie aspekty zabezpieczania danych osobowych (zarówno dane przetwarzane w systemach informatycznych, jak i w sposób tradycyjny). W ramach przygotowania polityki bezpieczeństwa administrator powinien przypisać poszczególnym osobom zakres obowiązków związanych z przetwarzaniem danych osobowych, oraz określić: zasoby danych osobowych, procesy istotne dla ciągłości funkcjonowania administratora danych (związane z przetwarzaniem danych osobowych), zagrożenia mające wpływ na zabezpieczanie przetwarzanych danych, podatność systemu informatycznego na zagrożenia, mechanizmy zabezpieczania przetwarzania danych osobowych (w systemie informatycznym i poza takim systemem), ryzyko po wdrożeniu mechanizmów zabezpieczających. Polityka bezpieczeństwa przetwarzania danych osobowych powinna zawierać m.in. określenie obszaru przetwarzania danych osobowych poprzez przygotowanie wykazu budynków, pomieszczeń, części pomieszczeń, w których dane te są przetwarzane (niezależnie od tego, czy przetwarzanie prowadzone jest w sposób tradycyjny, czy też w systemie informatycznym), wykaz zbiorów danych osobowych oraz wskazanie programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych oraz wzajemne ich powiązania, sposób przepływu danych pomiędzy poszczególnymi systemami, określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia danym poufności, integralności oraz rozliczalności (tzn. możliwości przypisania działań podmiotu w sposób jednoznaczny wyłącznie temu podmiotowi).

Instrukcją zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, można m.in. określić procedury przyznawania użytkownikowi identyfikatora w systemie informatycznym lub przyznania uprawnień do przetwarzania informacji, metody i środki uwierzytelniania użytkowników takiego systemu, procedury tworzenia kopii zapasowych, itp. Instrukcja może również zawierać procedurę postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego, przetwarzającego dane osobowe.

Wskazaną wyżej dokumentację prowadzi (w formie pisemnej) oraz wdraża administrator danych. Przez wdrożenie należy rozumieć opublikowanie dokumentacji i zapoznanie z nią osób upoważnionych do przetwarzania danych osobowych oraz osób, mogących mieć wpływ na bezpieczeństwo przetwarzanych danych. Administrator danych powinien również zorganizować szkolenia dla osób upoważnionych do przetwarzania danych osobowych, które swoim zakresem obejmowałyby kwestie zawarte w polityce bezpieczeństwa i instrukcji.

2.6. Poziomy bezpieczeństwa przetwarzania danych

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, wprowadza 3 poziomy środków bezpieczeństwa przetwarzania danych w systemach informatycznych.

Poziom podstawowy stosuje się, gdy w systemie informatycznym nie przetwarza się danych „wrażliwych", a także, gdy żadne z urządzeń należących do systemu nie jest połączone z siecią publiczną. W takim systemie stosuje się następujące środki bezpieczeństwa:

- obszar, w którym przetwarza się dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych; osoby nieuprawnione mogą przebywać w tym obszarze jedynie za zgodą administratora danych lub w obecności osoby upoważnionej,
- system informatyczny przetwarzający dane osobowe wyposażony jest w mechanizm kontroli dostępu do tych danych,
- system informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
- identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,
- w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni; hasło składa się co najmniej z 6 znaków,
- dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych; kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem i usuwa niezwłocznie po ustaniu ich użyteczności.

Jeśli w systemie przetwarza się dane „wrażliwe", ale nadal żadne z urządzeń należących do systemu nie jest połączone z siecią publiczną, wówczas mamy do czynienia z **poziomem podwyższonym**, w którym należy zastosować, obok środków przewidzianych dla systemu podstawowego, również następujące środki:

- hasło uwierzytelniające użytkownika powinno składać się z co najmniej 8 znaków,
- urządzenia i nośniki zawierające dane wrażliwe zabezpiecza się w sposób gwarantujący ich integralność i poufność.

Poziom wysoki stosuje się, gdy przynajmniej jedno z urządzeń systemu informatycznego przetwarzające dane osobowe jest połączone z siecią publiczną. Przy takim poziomie bezpieczeństwa należy zastosować takie środki, które stosuje się przy poziomie podstawowym oraz podwyższonym, a także:

- system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
- w przypadku zastosowania logicznych zabezpieczeń, obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych,
- administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

2.7. Dane osobowe w niektórych innych aktach prawnych

Przepisy dotyczące ochrony danych osobowych znajdują się również w wielu różnych ustawach odrębnych. Poniższy wybór nie wyczerpuje listy takich ustaw, a zaprezentowany jest jedynie przykładowo.

Ustawa z dnia 26 czerwca 1974 r. **Kodeks pracy** przewiduje, że pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia. Pracodawca ma prawo żądać od pracownika podania również innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy. Ma prawo żądać również podania numeru PESEL pracownika. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa powyżej. Pracodawca może żądać podania innych jeszcze danych osobowych, jeżeli obowiązek ich podania wynika

z odrębnych przepisów.

Ustawa z dnia z dnia 18 lipca 2002 r. **o świadczeniu usług drogą elektroniczną** posługuje się definicją „danych osobowych" w brzmieniu ustalonym przez ustawę o ochronie danych osobowych, natomiast do przetwarzania tych danych wymaga stosowania własnych przepisów. Pierwszą różnicą, mającą charakter obostrzenia w stosunku do zasad przewidzianych w ustawie o ochronie danych osobowych jest objęcie (przez ustawę o świadczeniu usług drogą elektroniczną) ochroną przetwarzania danych niezależnie od faktu, czy przetwarzanie dokonywane jest w ramach zbioru danych. Celem, w jakim usługodawca może przetwarzać dane osobowe usługobiorcy, jest nawiązanie, ukształtowanie treści, zmiana lub rozwiązanie stosunku prawnego z usługobiorcą, natomiast danymi osobowymi, jakie usługodawca może przetwarzać, są: nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL lub - gdy ten numer nie został nadany -numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, jeżeli jest inny niż adres zameldowania na pobyt stały, dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy.

Przetwarzanie przez usługodawcę innych danych osobowych jest dopuszczalne, o ile dane te są niezbędne do dokonania innej niż wskazane czynności prawnej lub do realizacji umowy. W takim przypadku usługodawca ma obowiązek oznaczyć te dane jako niezbędne do realizacji wymienionych celów. Ponadto możliwe jest przetwarzanie przez usługodawcę danych osobowych, które nie są niezbędne do świadczenia usług, o ile usługobiorca wyrazi na to zgodę. Obowiązek informacyjny usługodawcy w rozumieniu ustawy o świadczeniu usług drogą elektroniczną polega na zapewnieniu usługobiorcy stałego i łatwego dostępu, za pomocą systemu teleinformatycznego używanego przez usługobiorcę, do informacji o:

- możliwości korzystania z usługi świadczonej drogą elektroniczną anonimowo lub z wykorzystaniem pseudonimu (usługodawca nie może zestawiać danych osobowych usługobiorcy z przybranym przez niego pseudonimem),
- udostępnianych przez usługodawcę środkach technicznych, zapobiegających pozyskiwanie i modyfikowanie przez osoby nieuprawnione, danych osobowych przesyłanych drogą elektroniczną,
- podmiocie, któremu powierza przetwarzanie danych, ich zakresie i zamierzonym terminie przekazania, jeżeli usługodawca zawarł z tym podmiotem umowę o powierzenie do przetwarzania takich danych jak nazwisko i imiona usługobiorcy, numer ewidencyjny PESEL lub - gdy ten numer nie został nadany - numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres, ale również dane służące do weryfikacji podpisu elektronicznego usługobiorcy.

Ustawa z dnia 6 września 2001 r. **o dostępie do informacji publicznej** jest aktem prawnym wyłączającym stosowanie przepisów Ustawy o ochronie danych osobowych w stosunku do określonych podmiotów. Zgodnie z ustawą o dostępie do informacji publicznej, do udostępniania informacji publicznej obowiązane są władze publiczne i inne podmioty wykonujące zadania publiczne. Ustawa wymienia w art. 4 ust. 1 listę podmiotów obowiązanych szczególnie do udostępniania informacji o charakterze publicznym, wśród których znajdują się m. in.: podmioty reprezentujące, zgodnie z odrębnymi przepisami, Skarb Państwa oraz podmioty reprezentujące państwowe osoby prawne albo osoby prawne samorządu terytorialnego oraz podmioty reprezentujące inne państwowe jednostki organizacyjne albo jednostki organizacyjne samorządu terytorialnego, podmioty reprezentujące inne osoby lub jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym, oraz osoby prawne, w których Skarb Państwa, jednostki samorządu terytorialnego lub samorządu gospodarczego albo zawodowego mają pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów.

W stosunku do osób sprawujących funkcje publiczne - w zakresie informacji mających związek z ich pełnieniem - nie obowiązuje ograniczenie prawa do informacji publicznej ze względu na prywatność osoby fizycznej. W tym sensie przepisy ustawy o ochronie danych osobowych nie stanowią podstawy do odmowy udzielania informacji na temat takich osób.

Ustawa z dnia 16 lipca 2004 r. **Prawo telekomunikacyjne** reguluje m.in. kwestię przetwarzania danych osobowych przez dostawców powszechnie dostępnych usług telekomunikacyjnych, stwierdzając, iż „treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „przetwarzaniem", dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania" oraz wymieniając katalog danych osobowych, do przetwarzania których dostawca powszechnie dostępnych usług telekomunikacyjnych jest uprawniony.

Ustawa z dnia 6 lipca 2001 r. **o usługach detektywistycznych** stwierdza m.in., że detektyw nie może powierzyć przetwarzania danych osobowych innemu podmiotowi, co stanowi pewne ograniczenie stosowania przepisów ustawy o ochronie danych osobowych. W stosunku do detektywów wyłączono również stosowanie niektórych przepisów ustawy o ochronie danych osobowych, które dotyczą w szczególności „obowiązku informacyjnego".