Anna Zalesińska

Ochrona sfery życia prywatnego w przestrzeni informatycznej

Wstęp

Technika cyfrowa za pośrednictwem technologii informacyjnych zapewnia możliwość sprawnego gromadzenia, przetwarzania i udostępniania informacji. Można zaryzykować stwierdzenie, że przenika ona do wszystkich dziedzin, stając się ich nieodłącznym składnikiem. Współcześnie komunikacja kształtuje świadomość oraz standardy nowoczesnego społeczeństwa, pełni funkcję integracyjną w aspekcie społecznym, gospodarczym i politycznym[1]. Czynnikiem, który umożliwia przenikanie się i splatanie systemów komunikacji (konwergencję), a w efekcie „stopienie się informatyki i telekomunikacji", jest Internet[2]. Jego ekspansywny rozwój otworzył przed ludzkością niezmierzone możliwości. Niestety, Internet ma też swoją „ciemną stronę" – równie fascynującą, co niebezpieczną. Dwie główne i immanentne cechy Internetu – eksterytorialność i anonimowość – wyznaczają granice wolności[3], dając jednocześnie szerokie spektrum możliwości. Właśnie tym cechom, a zwłaszcza swoistemu „mitowi anonimowości" Internet zawdzięcza swoją popularność. Niestety, tak samo jak w rzeczywistym świecie, także w wirtualnym wolność niesie

[1] Zob. A. Haręża, *Doktryna hakerów – mit czy rewolucja? Uwagi na temat natury informacji, entropii cyberprzestrzeni i postawy awangardy rewolucji postindustrialnej*, Prawo Mediów Elektronicznych, dodatek do Monitora Prawniczego, nr 2, 2006, s. 45. T. Globan-Klas wskazuje, że komunikacja za pośrednictwem elektronicznych mediów zmieniała relacje pomiędzy czasem, przestrzenią a komunikacją społeczną, a wręcz „unicestwiła zarówno czas, jak i przestrzeń w komunikowaniu się na odległość". Wskutek ewolucji tradycyjna komunikacja asynchroniczna jest zastępowana synchroniczną, zob. T. Globar-Klas, P. Sienkiewicz *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków, 1999, s. 10 i 19.

[2] Zob. J. Barta, R. Markiewicz, *Internet a prawo*, Kraków, 1998, s. 13.

[3] Zob.. K. Gienas, *Cyberprzestępczość*, Jurysta, nr 11, 2003, s. 9.

ze sobą wiele zagrożeń. W efekcie powstają warunki wprost doskonałe do rozwoju przestępczości komputerowej (cyberprzestępczości)[4].

Celem niniejszego opracowania jest ukazanie problematyki związanej z potencjalnymi zagrożeniami sfery życia prywatnego w przestrzeni informatycznej[5], a także określenie potencjalnych środków ochrony ukształtowanych na gruncie prawa publicznego i prywatnego.

1. Sfera życia prywatnego a prawa osobiste w Kodeksie cywilnym w kontekście zagrożeń związanych z rozwojem nowoczesnych technologii

Koncepcja prawnej ochrony sfery życia prywatnego człowieka ukształtowała się na gruncie doktryny amerykańskiej[6]. Dorobek doktryny

[4] Już sam problem znalezienia adekwatnej nazwy dla omawianego zjawiska budzi kontrowersje. Częstokroć używa się nazwy przestępstwo komputerowe, co jest zgodne z określeniami występującymi w języku innych państw, tj. *computer criminality* czy *Komputerkriminalität*. Używane jest także pojęcie „nadużycie komputerowe" (zob. T. Tomaszewski, *Kryminalistyczna problematyka przestępczości komputerowej*, Problemy Kryminalistyki, nr 143, 1980, s. 69). Natomiast jeden z największych autorytetów i pionierów w dziedzinie prawno-karnej analizy prawa nowych technologii K.J. Jakubki zaproponował definicję „przestępczości komputerowej", zgodnie z treścią której jest to zjawisko kryminologiczne, obejmujące wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz w całym systemie połączeń komputerowych, a także w sam sprzęt komputerowy oraz prawo do programu komputerowego (zob. K.J. Jakubski, *Przestępczość komputerowa – podział i definicja*, Przegląd Kryminalistyki, nr 2/7, 1997, s. 31). Dla potrzeb niniejszego opracowania przyjęte zostało pojęcie cyberprzestępstwo, zgodnie z terminologią zawartą w Konwencji Rady Europy o Cyberprzestępczości (*Council of Europe Convention on Cybercrime*, Budapeszt, 23 listopada 2001 r.).

[5] Pod tym pojęciem należy rozumieć wirtualną przestrzeń, w ramach której odbywa się komunikacja pomiędzy mediami cyfrowymi. Termin ten zbliżony jest znaczeniowo do „cyberprzestrzeni", która jednak tradycyjnie zaliczana jest do terminologii *sciencefinction*, gdzie służy do określenia „wirtualnej przestrzeni życiowej wygenerowanej przez komputer". Zob. W. Gibson, *Neuromancer*, Poznań, 1999; zob. także *Przestępczość w cyberprzestrzeni. Nowe formy specyficznej dla naszych czasów przestępczości komputerowej przekład*, za: Kriminalistik, 1996, 3, s. 194–198, oprac. Anna Henschke, [w:] Problemy Kryminalistyki, 1997, 215, s. 74–78

[6] Zob. S.D. Warren, L.D. Brandeis, *The Right to Privacy*, Harvard Law Review, 1890, 4, s. 193.

i judykatury amerykańskiej nie pozostał bez wpływu na europejski porządek prawny, w tym również na polskie regulacje.

Za A. Szpunarem można wskazać, że najogólniej prawo to można rozumieć jako dające generalną ochronę przed ingerencją osób nieuprawnionych w sferę życia prywatnego[7]. Niemniej w ramach zespołu wartości, które sfera ta obejmuje swoim zasięgiem, wyróżnia się przede wszystkim dobre imię, wizerunek, życie osobiste, wolność, tajemnicę danych osobowych, przeszłość danej osoby. Różnorodność wspomnianych wartości jest w dużej mierze uzależniona od poziomu rozwoju kulturalno-cywilizacyjnego państwa, a przede wszystkim preferowanych i akceptowanych w danym społeczeństwie wartości służących samorealizacji jednostki[8]. Truizmem jest twierdzić, że rozwój mediów, takich jak prasy, radia, filmu, telewizji, stwarza nowe możliwości naruszania tej kategorii dóbr i interesów jednostki. Ewolucja ta jest szczególnie zauważalna w dobie społeczeństwa informacyjnego. Jest to nowy typ społeczeństwa, kształtujący się w krajach postindustrialnych, w których rozwój technologii informatycznych osiągnął najszybsze tempo. Jednoznaczne zdefiniowanie tak złożonego pojęcia, jak społeczeństwo informacyjne, jest niezwykle skomplikowanym zagadnieniem[9]. Aczkolwiek założenie, że współczesne społeczeństwo opiera się na „informacji, wiedzy i telekomunikacji jako środkach produkcji i kształtowania warunków życia społecznego”[10], można uznać za aksjomat, które stanowi podstawę dla większości przyjętych konstrukcji definicji.

W kontekście zakreślonego obszaru badawczego koniecznym jest określenie katalogu dóbr osobistych, które w efekcie ekspansyw-

[7] Zob. A. Szpunar, *O ochronie sfery życia prywatnego*, Nowe Prawo, 1982, 3–4, s. 5 i n.

[8] Zob. K.K. Kubiński, *Ochrona życia prywatnego*, Ruch Prawniczy, Ekonomiczny i Socjologiczny, rok LV, 1993, z. 1, s. 61 i n.

[9] T. Globan-Klas, *Społeczeństwo informacyjne i jego teoretycy*, [w:] J. Lubacza (red.), *W drodze do społeczeństwa informacyjnego*, Warszawa 1999, s. 29–55.

[10] *Ibidem*, s. 48. Zob. M. Castells w trylogii *Wiek informacji: gospodarka, społeczeństwo, kultura* (1989), *Powstanie społeczeństwa sieciowego* (1996), *Siłą tożsamości* (1997), *Koniec Tysiąclecia* (1998). Ten wybitny ideolog jako pierwszy wskazał, że organizacyjną podstawą dla nowoczesnego modelu społeczeństwa jest właśnie sieć, tj. Internet.

nego rozwoju Internetu oraz ukształtowania się nowego typu społeczeństwa – informacyjnego – podlegają nowym rodzajom zagrożeń. Niewątpliwie zaliczyć do niego można takie wartości, jak tajemnica korespondencji, dobre imię, cześć, dobrą sławę, wizerunek oraz prawo do wolności.

1.1. Prawo do prywatności

Postulat wyodrębnienia prawa do prywatności jako samodzielnego dobra osobistego na gruncie polskiego prawa po raz pierwszy został podniesiony przez A. Kopffa[11]. Podstawowe znaczenie miało przyjęcie przez niego nadrzędnej konstrukcji jednolitego prawa osobistości. W obrębie tej nadrzędnej konstrukcji wyróżnił on prawo do ochrony życia prywatnego, zróżnicowane w zależności od sfer[12]. Koncepcja prawa do prywatności z trudem torowała sobie drogę w judykaturze. Dopiero w ostatnim dziesięcioleciu XX w. pojawiły się nowe impulsy zmierzające do ugruntowania koncepcji zakładającej istnienie odrębnego dobra osobistego w postaci sfery życia prywatnego. Nowelizacja art. 14 Ustawy z dnia 26 stycznia 1984 r. Prawo prasowe[13], wejście w życie Konstytucji RP[14] z 1997 r. oraz przystąpienie Polski do Europejskiej Konwencji Praw Człowieka ukierunkowały dalszy rozwój doktryny i judykatury w tym zakresie[15]. Obecnie za utrwalony należy uznać pogląd zgodnie, z którym życie prywatne należy włączyć do katalogu dóbr osobistych, mimo że nie zostało ono wyrażone *expressis verbis* w art. 23 k.c.[16]

---

[11] Zob. A. Kopff, *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, Studia cywilistyczne, 20, 1972, s. 3–40.

[12] Zob. A. Szpunar, *op. cit.*, s. 6.

[13] Dz.U. Nr 5, poz. 24.

[14] *Konstytucja Rzeczpospolitej Polskiej z dnia 02.04.1997 r.* (Dz.U. Nr 78, poz. 483)..

[15] Zob. M. Pazdan, [w:] K. Pietrzykowski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2008, s. 137–143.

[16] *Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny* (Dz.U. Nr 16, poz. 93). Zob. P. Sut, *Czy sfera intymności jest dobrem chronionym w prawie cywilnym?*, Palestra, 1995, 7–8, s. 51 i n.

Prawo do ochrony prywatności implikuje prawo do informacji po stronie jednostki, tj. do otrzymywania wiadomości o tym, gdzie i w jakim celu są przekazywane i przetwarzane dane jej dotyczące. Zastosowanie nowoczesnych systemów informatycznych umożliwiających elektroniczne przetwarzanie danych spowodowało powstanie nowych, nieznanych wcześniej zagrożeń dla prawa do prywatności. Możność kumulacji ogromnej ilości informacji o jednostce, szybkość ich gromadzenia i przekazywania za pomocą wcześniej nieznanych metod urealniają faktyczne niebezpieczeństwo ich zniekształcenia oraz łatwiejszą dostępność do zbiorów dla osób trzecich. Staje się to potencjalnie potężnym środkiem „wywierania presji na jednostkę, tworząc stan zagrożenia w rozmiarze wcześniej niewystępującym”[17].

1.2. Tajemnica korespondencji

Tajemnica korespondencji została wyróżniona *expressis verbis* w art. 23 k.c., a także w art. 49 Konstytucji RP, który gwarantuje wolność komunikowania się oraz jej ochronę. W doktrynie prawa cywilnego przyjmuje się możliwie szerokie rozumienie terminu korespondencja, tak by swoim zasięgiem objął on różne sposoby porozumiewania się, w tym także za pośrednictwem środków komunikacji elektronicznej. Ochrona przysługuje nie tylko adresatowi korespondencji, lecz również jej nadawcy (autorowi). Do naruszenie tajemnicy korespondencji może dojść wskutek różnych zachowań. Tytułem przykładu można wskazać bezprawne zapoznanie się z korespondencją zaadresowaną do innej osoby, w tym także wskutek uzyskania dostępu do systemu informatycznego, przejęcie i przywłaszczenie, a także zniszczenie cudzej korespondencji lub jej upublicznienie. W prawie polskim odrębnie została uregulowana tajemnica telekomunikacyjna (por. art. 159 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[18]).

---

[17] Zob. M. Safjan, *Prawo do ochrony – granice autonomii informacyjnej*, [w:] M. Wyrzykowski (red.), *Ochrona danych osobowych,* Warszawa, 1999, za: M. Mucha, *Obowiązki administracji publicznej w sferze dostępu do informacji*, Wrocław 2002, s. 150.

[18] Dz.U. Nr 171, poz. 1800 ze zm.

1.3. Dobre imię, cześć, dobra sława, wizerunek

Cześć człowieka jako dobro osobiste została wymieniona w art. 23 k.c. oraz w art. 47 Konstytucji RP. Pozostaje ona w ścisłej korelacji z dobrym imieniem oraz sławą, a także z wizerunkiem oraz głosem człowieka. Do naruszenia wymienionych dóbr osobistych może dojść w rozmaity sposób, w tym także za pośrednictwem środków komunikacji elektronicznej. W szczególności, jak już wskazano, rozwój techniki otwiera nowe możliwości naruszania sfery życia prywatnego, w tym zwłaszcza czci i dobrego imienia, często bezkarnie, wobec trudności ujawnienia sprawcy. Portale społecznościowe, fora dyskusyjne, strony internetowe dają sprawcy nowe obszary działalności, chroniąc jednocześnie jego personalia. Analogicznie sytuacja wygląda w przypadku rozpowszechniania wizerunku wbrew woli osoby na niej przedstawionej. Oprócz art. 23 i 24 k.c. ochrona wizerunku uregulowana jest również w Prawie prasowym oraz w Ustawie z dnia 4 lutego 1994 r. – Prawo autorskie[19]. Szczegółowe umówienie tak skomplikowanej materii wykraczałoby jednak poza ramy niniejszego opracowania.

Co istotne jednak, oceniając ewentualne naruszenie wskazanych dóbr osobistych w Internecie konieczne jest uwzględnienie specyfiki działania tego medium. Z jednej strony trzeba mieć na uwadze takie wartości, jak absolutna wolność słowa, anonimowość, brak jakiejkolwiek kontroli oraz masowy dostęp do umieszczonych danych, a z drugiej strony potrzebę zapewnienia należytej ochrony sfery życia prywatnego. W efekcie zasięg przekazu i masowość jego odbioru wymagają szczególnej ostrożności i wystrzegania się bezprawnego naruszania dóbr osobistych innych użytkowników[20] a ocena bezprawności powinna być również uwzględniać kontekst sytuacyjny[21].

---

[19] Dz.U. z 2006 r. Nr 90, poz. 631.

[20] Wyrok Sądu Najwyższego z dnia 07.09.1972 r., sygn. akt I CR 374/72, OSPiKA z 1974 r., poz. 28 oraz wyrok Sądu Najwyższego z dnia 29.06.1983 r., sygn. akt II CR 160/83, niepubl., SIP Legalis.

[21] Wyrok Sądu Najwyższego z dnia 23.05.2003 r., sygn. akt IV CKN 1076/00, OSNC z 2003 r., nr 9, poz. 121.

1.4. Prawo do wolności

Na gruncie doktryny prawa cywilnego ukształtowały się dwie koncepcje dotyczące rozumienia wolności jako dobra osobistego. Według S. Grzybowskiego „wolność" należy rozumieć wąsko jako fizyczną swobodę ruchu[22]. Natomiast według A. Szpunara termin ten powinno się rozumieć szeroko, jako ochronę przed jakimikolwiek naciskami, które krepują swobodne dysponowanie wartościami osobistymi[23]. W przypadku szerokiego rozumienia słowa „wolność" do naruszenia tego prawa na gruncie środków komunikacji elektronicznej może dojść w skutek wysyłania niezamówionej korespondencji (tzw. SPAM) oraz poprzez tzw. profilowanie, tj. tworzenie profili osobowych na podstawie danych uzyskanych przez śledzenie działań konkretnej osoby w Internecie[24]. Pierwszy czyn penalizowany jest na gruncie Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[25] (art. 24), natomiast w przypadku profilowania poszkodowany może dochodzić ochrony wyłącznie na gruncie prawa cywilnego.

1.5. Dane osobowe

Na odrębną wzmiankę zasługuje kwestia ochrony danych osobowych. W literaturze przedmiotu prezentowane są odmienne stanowiska w kwestii wyróżnienia danych osobowych jako odrębnego dobra osobistego. Za takim poglądem opowiada się m.in. A. Bierć[26]. Zgodnie z odmienną koncepcją dane osobowe stanowią tylko szczególną postać prawo do prywatności[27]. Najszerszą akceptację zyskał jednak trzeci pogląd wypracowany przez tzw. szkołę krakowską (J. Barta, M. Markiewicz,

---

[22] S. Grzybowski, *Ochrona dóbr osobistych według przepisów ogólnych prawa cywilnego*, Warszawa, 1957, s. 84.

[23] A. Szpunar, *Ochrona dóbr osobistych*, Warszawa, 1970, s. 126.

[24] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków, 1998, s. 28.

[25] Dz.U. Nr 144, poz. 1204.

[26] Zob. A. Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne*, [w:] Wyrzykowski (red.), *op. cit.*, s. 112.

[27] Zob. A. Mendis, *Prawna ochrona danych osobowych*, Warszawa, 1995, s. 14 i n.

P. Fajgielski[28]), w myśl którego pomiędzy ochroną prawa do prywatności (na płaszczyźnie prawa konstytucyjnego i cywilnego) a ochroną danych osobowych (dostrzeganą w Konstytucji RP i regulowaną Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[29] (dalej: OchrDanOsU) zachodzi stosunek krzyżowania się. Są to przy tym reżimy od siebie niezależne. W praktyce mogą się więc zdarzyć sytuacje, gdy przetwarzanie danych nie zostanie uznane za naruszenie prawa do prywatności[30].

W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio w rozumieniu przeciętnego odbiorcy, zwłaszcza przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Natomiast jeżeli wykorzystanie takiej informacji wymagałoby nadmiernych kosztów, czasu lub działań, nie uważa się jej za umożliwiającą określenie tożsamości osoby[31]. Przyjęta konstrukcja zapewnia szerokie rozumienie tego określenia, obejmują wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[32], tzn. w sytuacji, gdy administrator danych

---

[28] Zob. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 179.

[29] Dz.U., Nr 133, poz. 883. Ustawa ta implementowała do polskiego porządku prawnego Dyrektywę Parlamentu Europejskiego i Rady Unii Europejskiej nr 95/46/WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych oraz Dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej nr 2002/58/WE z 12 lipca 2002 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Dyrektywy te zostały wydane w celu stworzenia generalnych ram ochrony danych osobowych w całej Wspólnocie Europejskiej oraz zapewnienia odpowiedniego poziomu ochrony prywatności w ramach wspólnotowego rynku usług telekomunikacyjnych i central telefonicznych.

[30] Zob. M. Pazdan [w:] K. Pietrzykowski (red.), *op. cit.*, s. 142–143.

[31] Zob. art. 6 OchrDanOsU.

[32] Zob. J. Barta, M. Markiewicz, *Ochrona danych osobowych*, Kraków 2002, s. 283.

może bez nadmiernych nakładów powiązać typy informacji z konkretną osobą[33]. Przybliżenia wymaga również zakres podmiotowy OchrDanOsU. Prawo do ochrony danych osobowych zostało przyznane wyłącznie osobie fizycznej, a nie każdemu podmiotowi prawa. Aczkolwiek nie w każdych okolicznościach będzie zapewniona ochrona informacji dotyczącej jednostki. Danym będącym informacją publiczną w rozumieniu Ustawy o dostępie do informacji publicznej[34] bądź też zawartym w Ewidencji Działalności Gospodarczej[35] nie będzie przysługiwać ochrona na podstawie komentowanej ustawy.

Natomiast każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, jest zbiorem danych[36]. Jest on obok zbioru ewidencyjnego jedną z dopuszczalnych przez ustawę postaci przetwarzania danych. Jeżeli dane osobowe są przetwarzane za pomocą systemu informatycznego to zgodnie z koncepcją przyjętą przez E. Drozda domniemanie faktyczne przemawia wówczas za uznaniem, że są one przetwarzane właśnie w zbiorze danych, gdyż już standardowe oprogramowanie umożliwia do nich dostęp według wielu kryteriów. W konsekwencji również domniemanie to dotyczy przetwarzania danych na stronie internetowej[37]. Jednakże OchrDanOsU znajdzie zastosowanie również w przypadku przetwarzania danych w systemach informatycznych poza zbiorem danych. Pod pojęciem przetwarzanie danych należy rozumieć 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[38]. Wskazane przez ustawodawcę przykładowe

---

[33] Zob. A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2006, s. 51.

[34] Dz. U. Nr 112, poz. 1198.

[35] Prowadzonej docelowo na podstawie Ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2010 r. Nr 220, poz. 1447 – t.j.).

[36] Zob. art. 7 pkt 1 OchrDanOsU.

[37] Zob. A. Drozd, *op. cit.*, s. 57. Zbiór ewidencyjny przetwarzany jest najczęściej ręcznie, natomiast zbiór danych automatycznie.

[38] Zob. art. 7 pkt 2 OchrDanOsU.

operacje na danych zostały uporządkowane w nieprzypadkowej kolejności, gdyż o przetwarzaniu danych można mówić począwszy od zbierania danych, a skończywszy na ich usunięciu. Użycie zwrotu „zwłaszcza" podkreśla, że choć w systemach informatycznych nie zawsze możliwe jest wyróżnienie poszczególnych operacji, dane osobowe i tak podlegają ochronie[39].

2. System środków ochrony sfery życia prywatnego w cyberprzestrzeni

2.1. Cywilnoprawne środki ochrony

Niewątpliwie do prywatnej sfery życia należy zaliczyć, jak już wskazano, przede wszystkim fakty dotyczące stosunków jednostki z najbliższym otoczeniem, spokój psychiczny *sensu stricto*, a także dane należące do sfery życia intymnego, takie jak stan zdrowia, przeszłość, życie seksualne. Uruchomienie mechanizmów ochrony cywilnoprawnej następuję w momencie przekroczenia wyznaczonej przez przepisy prawa, zasady współżycia społecznego oraz zgodę dysponenta ostrożności[40]. Na gruncie prawa cywilnego można wyróżnić niemajątkowe (art. 24 k.c.) oraz majątkowe (art. 448 k.c.) środki ochrony prawnej.

Regulacje zawarte w art. 23 i 24 k.c. kreują system instrumentów prawnych chroniących dobra osobiste, pod pojęciem których należy rozumieć wartości o charakterze niemajątkowym, ściśle związane z osobą ludzką, decydujące o jej bycie, pozycji w społeczeństwie, a będące wyrazem jej odrębności psychicznej i fizycznej oraz moż-

[39] Przykładowo, dostarczanie wiadomości tekstowych abonentom sieci telefonii komórkowej za pomocą SMS (usługa przesyłania krótkich wiadomości tekstowych w cyfrowych sieciach telefonii komórkowej) na zlecenie podmiotu zewnętrznego jest przetwarzaniem danych osobowych, pomimo że pozostają oni anonimowi dla zleceniodawcy. Zob. wyrok NSA z 10 sierpnia 2005 r., OSK 1856/04, z krytyczną glosą P. Szkudlarka, Gazeta Sądowa, nr 1, 2006.

[40] Zob. E. Woch, *Sfera życia prywatnego i jej ochrona przed naruszeniem w Cyberprzestrzeni*, [w:] R. Skubisz (red.), *Internet 2000. Prawo – ekonomia – kultura*, Lublin, 2000, s. 74.

liwości twórczych, uznane powszechnie w społeczeństwie i uznane przez dany system[41].

Niemajątkowa ochrona dóbr osobistych została uzależniona od dwóch podstawowych przesłanek, tj. od zagrożenia lub naruszenia dóbr osobistych ujmowanego w kategoriach obiektywnych faktów oraz bezprawności, co do której ustawodawca wprowadził domniemanie. Pod pojęciem bezprawności według A. Ciska należy rozumieć pewną obiektywną wadliwość przedmiotową, która polega na obiektywnej sprzeczności określonego zachowania, z pewnymi regułami postępowania, wyznaczonymi zarówno przez normy prawne, jak i przez szeroko rozumiane zasady współżycia społecznego, które swym zakresem mogą obejmować różne reguły postępowania[42]. Nie każde jednak zachowanie prawa podmiotowego danej osoby powinno zostać uznane za bezprawne, albowiem w konkretnych okolicznościach wkroczenie w sferę cudzych dóbr osobistych może mieścić się w granicach wyłączających domniemanie z art. 24 k.c. Do takich kategorii należy działanie w ramach porządku prawnego, realizacja własnego prawa podmiotowego, działanie w granicach wyznaczonych przez przepisy prawa, zgodna uprawnionego, obrona interesu indywidualnego lub społecznego zasługującego na ochronę bądź wręcz przeciwnie brak zasługującego na ochronę interesu[43].

W przypadku, gdy zostaną spełnione wskazane przesłanki i nie zaistnieje żadna okoliczność wyłączająca bezprawność poszkodowany na podstawie art. 24 k.c. może domagać się zaniechania działania, a w przypadku, gdy dojdzie do naruszenia, można domagać się usunięcia skutków naruszenia dóbr osobistych oraz zadośćuczynienia pieniężnego lub zapłaty określonej sumy pieniężnej na wskazany cel społeczny. W przypadku działań prewencyjnych osoba pokrzywdzona może żądać zaniechania tylko określonego działania. Natomiast, gdy dojdzie do naruszenia dóbr osobistych w Internecie, konieczne staje się

---

[41] Tak A. Cisek, *Dobra osobiste i ich niemajątkowa ochrona w Kodeksie Cywilnym*, Wrocław 1989 (Acta Universitatis Wratislaviensis, No 1016, Prawo CLXVII), s. 39.

[42] *Ibidem*, s. 69.

[43] Zob. S. Grzybowski, *op. cit.*, s. 115 i n.

nadto wykazanie zaistnienia realnej obawy dalszych naruszeń[44]. Jak już wskazano w sytuacji, gdy naruszenie określonej wartości stanie się faktem dokonanym, można żądać usunięcia skutków naruszenia. Treść żądania powinna być dostosowana do charakteru i rodzaju naruszenia dobra osobistego[45]. Poszkodowany może więc domagać się usunięcia stanu naruszenia jego dobra lub podjęcia czynności zmierzających do usunięcia skutków naruszenia, wśród których wyróżnia się takie, które zmierzają tylko do usatysfakcjonowania pokrzywdzonego i takie, które za pośrednictwem mass mediów mają dotrzeć do osób trzecich[46]. W przypadku, gdy do naruszenia dóbr osobistych dochodzi w Internecie przy użyciu publikacji prasowej, aktualizują się instrumenty prawne zagwarantowanego w ramach Prawa prasowego (art. 32 ust. 1). Poszkodowany może żądać umieszczenia sprostowania lub odpowiedzi na łamach danego czasopisma, a gdy redaktor odmówi może on wystąpić do sądu w celu realizacji roszczenia. Wskazać jednak należy, że jak wskazał Sąd Najwyższy korzystanie z ochrony na gruncie Prawa prasowego nie pozbawia poszkodowanego roszczeń z Kodeksu cywilnego, gdyż wzajemna relacja przepisów oparta jest na ich kumulatywnym zbiegu[47].

Środkiem ochrony dóbr osobistych jest również powództwo oparte na art. 189 k.p.c. Podnosi się, iż uzyskanie wyroku ustalającego „niekiedy wystarczy, aby zapobiec dalszym jego naruszeniom albo aby uchylić niebezpieczeństwo dokonania naruszeń"[48].

Przepis art. 24 § 1 zd. 3 k.c. odsyła natomiast *de facto* do art. 445 i 448 k.c. Tym samym możliwym jest zasądzenie zadośćuczynienia pieniężnego za doznaną krzywdę lub na wskazany przez niego cel społeczny. Przepis art. 24 § 2 k.c. stanowi także, że jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa,

---

[44] Por. S. Dmowski, S. Rudnicki, *Komentarz do Kodeksu cywilnego. Księga I. Część ogólna*, Warszawa, 2006, s. 70.

[45] Uchwała Sądu Najwyższego z dnia 30.12.1971 r., sygn. akt III CZP 87/71, OSN 1972, Nr 6, poz. 104.

[46] J. Panowicz-Lipska, *Majątkowa ochrona dóbr osobistych*, Warszawa 1975, s. 5.

[47] Wyrok Sądu Najwyższego z dnia 08.02.1990 t., sygn. akt II CR 1303/89, OSN z 1991 r., poz. 108.

[48] M. Pazdan, *op. cit.*, s. 166–169.

poszkodowany może żądać jej naprawienia na zasadach ogólnych. Nie wystarczy wówczas spełnienie przesłanek ochrony z art. 24 § 1 k.c., lecz muszą być równocześnie spełnione przesłanki, od których zależy odpowiedzialność odszkodowawcza. Tym samym nie jest wykluczona kumulacja roszczeń odszkodowawczych zarówno z roszczeniami opartymi na przepisie art. 24 § 1 k.c., jak i z żądaniem zadośćuczynienia pieniężnego na podstawie art. 445 lub 448 k.c. lub z żądaniem zapłaty stosownej kwoty na cel społeczny na podstawie art. 448 k.c.[49]

2.2. Rozwiązania karnoprawne

Ochrona sfery życia prywatnego na gruncie prawa karnego jest ograniczona do enumeratywnie wymienionych w Kodeksie karnym[50] dóbr osobistym, których naruszenie wolą ustawodawcy zostało spenalizowane. W efekcie wyczerpanie znamion określonych w art. 212–216 oraz 267 k.k. będzie powodować odpowiedzialność karną sprawcy, jeżeli nie zaistnieją okoliczności wyłączające winę lub bezprawność. W efekcie w ramach prawa karnego chronione są takie dobra osobiste jak tajemnica korespondencji oraz dobre imię, cześć, godność i wizerunek.

Przepis art. 267 k.k. obejmuje enumeratywnie wymienione działania przestępne, tj. uzyskanie bezprawnego dostępu do informacji oraz uzyskanie dostępu do systemu informatycznego (*hacking*), naruszenie tajemnicy korespondencji (*sniffing*), a także ujawnienie informacji o innej osobie. Choć w art. 267 § 1 k.k. nie użyto pojęcia „komunikowanie się" ani „korespondencja", przestępstwo ujęte w tym przepisie nazwać też możemy naruszeniem tajemnicy komunikowania się lub tradycyjnie tajemnicy korespondencji[51]. Bezpośrednim przedmiotem ochrony art. 267 § 1 k.k. jest szeroko rozumiane prawo do dysponowania informacją, mające charakter prawa podmiotowego[52]. Tym samym

[49] *Ibidem*, s. 168.

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

[51] Zob. B. Kunicka-Michalska [w:] A. Wąsek, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Komentarz do art. 222–316*, t. 2, Warszawa, 2010, s. 684 i n.

[52] Wyrok Sądu Najwyższego z 20.01.2003 r., sygn. akt I KZP 43/02, OSNKW, nr 1–2, poz. 5.

przedmiotem czynu jest odpowiednio w § 1 dostęp do informacji nieprzeznaczonej dla sprawcy, w § 2 dostęp do systemu informatycznego do którego sprawca nie ma dostępu, w § 3 użycie urządzenia technicznego w celu uzyskania informacji, do której nie jest sprawca uprawniony, a w § 4 informacja uzyskana w sposób określony w poprzednich paragrafach. Czyn zabroniony określony w art. 267 k.k. jest przestępstwem umyślnym, które może być pożenione z zamiarem bezpośrednim lub ewentualnym. Jest to przestępstwo ścigane na wniosek pokrzywdzonego (art. 257 § 5 k.k.).

Natomiast art. 212 k.k. penalizuje zachowania, które wskutek naruszenia dobrego imienia, czci, godności lub wizerunku prowadzić będą do zniesławienia pokrzywdzonego. Jest to przestępstwo ścigane z oskarżenia prywatnego. Przedmiotem ochrony jest właśnie dobre imię, cześć oraz honor poszkodowanego. Czyn ten popełnia każdy, kto pomawia wymienione w nim podmioty, tj. osoby fizyczne, grupy osób, instytucje prawne, osoby prawne oraz tzw. ustawowe osoby prawne (art. 33^1 k.c.). Pomówienie może być dokonane zarówno niepublicznie, jak i publicznie, w tym również za pomocą środków komunikowania się (art. 212 § 2 k.k.). Jest to przestępstwo formalne, gdyż wystarczy sama potencjalna możliwość poniesienia przez pokrzywdzonego szkód moralnych, tj. poniżenia w opinii publicznej lub narażenia na utratę zaufania. Pomówienie jest przestępstwem umyślnym, które można popełnić w zamiarze bezpośrednim lub ewentualnym. Nie stanowi zniesławienia krytyka postępowania lub właściwości osób, jeśli jest dokonywana w ramach tzw. dozwolonej krytyki (art. 213 k.k.)[53]. Przestępstwo zniesławienia jest w dużej mierze podobne do innego przestępstwa określonego w rozdziale XXVII, tj. przestępstwa znieważenia, określonego w art. 216 k.k. Znieważanie może jednak dotyczyć wyłącznie człowieka, zachowanie sprawcy musi być obraźliwe, w przeciwieństwie do zniesławienia zniewaga nie musi być uczyniona w konkretnej wypowiedzi (może być to określony gest lub wizerunek) i musi być skierowana bezpośrednio lub pośrednio do osoby znieważanej. Tutaj również ściganie odbywa się wyłącznie z oskarżenia prywatnego (art. 216 § 5 k.k.).

[53] J. Wojciechowski, [w:] A. Wąsek, R. Zawłocki (red.), *op. cit.*, s. 1298 i n.

2.3. System ochrony związany z przetwarzaniem danych osobowych

Celem zapewnienia ochrony danym osobowym jest umożliwienie realizacji prawnie chronionego interesu jednostki do zachowania prywatności i intymności, szczególnie w dobie postępującej komputeryzacji życia. Faktem jest, że zapewnienie odpowiedniego poziomu ochrony danych osobowych jest koniecznością. Ochrona ta jednak nie powinna mieć charakteru bezwzględnego i dopuszczać możliwość udostępniania danych osobowych i ich przetwarzania pod pewnymi warunkami.

W prawie polskim przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyraziła na to zgodę (chyba że chodzi o usunięcie dotyczących jej danych), jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa oraz do wykonania określonych prawem zadań realizowanych dla dobra publicznego i dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą[54]. Jak już wspomniano, elektroniczna forma przetwarzania danych implikuje powstanie pewnych konsekwencji, który nie występują w ramach formy tradycyjnej. Faktem jest, że nowoczesne środki gromadzenia i przesyłu informacji powodują powstanie zupełnie nowego wymiaru i jakości przetwarzanych danych., co wymaga zastosowania nieco innych standardów oraz procedur postępowania, by zapewnić odpowiednio poziom bezpieczeństwa i integralno-

[54] Zob. art. 23 ust. 1 OchrDanOsU. W przepisie tym wskazany jest jeszcze jeden przypadek, tj. gdy jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, który zostały celowo pominięty przez autorkę, gdyż wykracza poza zakres tematyczny pracy. Zasady przetwarzania danych są ograniczone przez art. 27 ust. 2 OchrDanOsU, który zawiera enumeratywny katalog wyjątków od całkowitego zakazu przetwarzania danych szczególnie wrażliwych, tzn. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

ści danych[55]. Stąd ustawodawca ustanawia wymóg odpowiedniego zabezpieczenia danych w systemie informatycznym. Rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem[56].

Wskazać należy również, że wszystkie zadania, którymi obciąża się administratorów bezpieczeństwa informacji, są realizowane w ramach posiadanych środków, a ich skuteczność jest uzależniona od należytego wypełniania nałożonych obowiązków przez wszystkie podmioty mające dostęp do systemu informatycznego[57].

Zakończenie

Prawo cywilne chroni niewątpliwie wszelkie dobra przed wszelkiego rodzaju zagrożeniami pochodzącymi nie tylko od ludzi, ale także od jednostek organizacyjnych. Natomiast katalog dóbr osobistych chronionych przez prawo karne jest węższy i ma charakter zamknięty. Nadto prawo cywilne może również pełnić funkcję prewencyjną, dzięki instrumentom z art. 24 k.c., a wydany przez sąd cywilny wyrok zakazujący działań zagrażających lub naruszających dobra osobiste działa na przyszłość. Ważkim argumentem jest również fakt, iż na gruncie prawa cywilnego wystarczającym jest wykazanie bezprawności naruszania, w sytuacji, gdy prawo karne wymaga zawinienia. Niewątpliwie z uwagi na krótkie okresy przedawnienia w prawie karnym, ochrona cywilnoprawna oparta na art. 24 k.c. również jest pełniejsza, gdyż roszczenia te nie przedawniają się, a skutków prawnych nie zlikwiduje ustawa amnestyjna lub

[55] M. Jabłoński, K. Wygoda, *Ochrona danych osobowych w prawie polskim*, [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003, s. 137.

[56] Niezbędne minimum środków i procedur zabezpieczających wskazano w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 80, poz. 522).

[57] M. Jabłoński, K. Wygoda, *op. cit.*, s. 146.

warunkowe umorzenie postępowania, jak to jest na gruncie postępowania karnego. Wydaje się, że ciężar ochrony dóbr osobistych w coraz większym zakresie będzie jednak spoczywał na prawie cywilnym, którego elastyczne instrumenty mogą sprostać szerokiemu spektrum zagrożeń istniejących we współczesnym świecie.

Jednakże w kontekście omawianych rozwiązań prawnych wskazać należy, iż skuteczność ochrony szeroko rozumianej sfery życia prywatnego w dużej mierze należy od zakresu edukacji oraz świadomości istnienia zagrożeń. W związku z powyższym zaznajomienie się z nowymi technologiami stało się nie tylko społecznym obowiązkiem, lecz jak pisze U. Meinberg nabrało wręcz „egzystencjalnego znaczenia”[58]. Społeczeństwo powinno być odpowiednio przystosowane do zachodzących przemian. Wiele osób widzi jednak szansę w technice, czyli różnego rodzajach zabezpieczeniach, takich jak programy antywirusowe czy też systemy haseł. Ochrona te jednak bez wystarczającego poziomu świadomości użytkowników może się okazać jednak niewystarczająca, gdyż to właśnie człowiek jest najsłabszym ogniwem bezpieczeństwa informatycznego[59]. Niezależnie od technicznego zaawansowania szkodliwych programów, cyberprzestępcy często próbują wykorzystać ludzkie słabości, by rozprzestrzeniać swoje metody, czemu mają służyć różne ukształtowane w ramach inżynierii społecznej (tzw. socjotechniki). W efekcie bardzo ważną rolę odgrywa tzw. świadomość społeczeństwa informacyjnego, czyli świadomość roli wiedzy i technologii informatycznych w życiu społeczeństw, dostrzeganie niebezpieczeństw związanych z tymi procesami oraz przezwyciężanie negatywnych efektów rozwoju świadomości informatycznej, która jest powiązana z rolą informatyzacji życia we wszystkich dziedzinach[60].

[58] Zob. U. Meinberg, *Wpływ nowych technologii informacji na społeczeństwo i człowieka*, [w:] A. Kieras, M.S. Szczepański, U. Żydek-Bednarczyk, *Internet – społeczeństwo informacyjne – kultura*, Tychy 2006, s. 14.

[59] Tytułem przykładu można wskazać nienależyte przechowywanie haseł dostępowych, tworzenie zbyt prostych haseł, otwieranie załączników w sytuacji, gdy nie znamy nadawcy, ujawnienie swoich danych osobowych.

[60] L.W. Zacher, *Rewolucja informacyjna i społeczeństwo*, Warszawa, 1997, za: M.S. Szczepański, R. Geisler. *Budowa społeczeństwa informacyjnego. Wyzwania dla województwa śląskiego*, [w:] A. Kieras, M. S. Szczepański, U. Żydek-Bednarczyk, *op. cit.*, s. 146.