

Rozdział I. Zagadnienia ogólne

Ryszard Szostak

1. Standardy urzędowe informatyzacji

Postępująca informatyzacja administracji i w ogóle działalności publicznej trwa już od ponad 20 lat. Jej założenia są zbieżne z podstawowymi zasadami administracji obywatelskiej: otwartej, przejrzystej, rzetelnej, budzącej zaufanie oraz efektywnej w załatwianiu spraw publicznych. Elektronizacja czynności i procedur usprawnia bowiem oraz przyspiesza wydatnie załatwianie spraw oraz świadczenie usług publicznych, podnosi ich jakość z równoległym ograniczeniem uciążliwości biurokratycznych, w warunkach powszechnego dostępu do informacji¹. W dalszej perspektywie informatyzacja zapewnia integrację funkcjonalno-terytorialną administracji oraz współpracę zróżnicowanych struktur administracyjnych, a także bardziej skuteczną kontrolę ich funkcjonowania, nie licząc zwykłej koordynacji wewnętrznego obiegu dokumentów. W sferze zamówień publicznych już w końcu lat dziewięćdziesiątych sygnalizowano potrzebę usprawnień organizacyjno-proceduralnych i radykalnego ograniczenia przerostu uciążliwości biurokratycznych². Z czasem pełna elektronizacja procedur udzielania zamówień publicznych stała się jednym z założeń gruntownego ich reformowania. W szczególności już w dyrektywie ogólnej 2004/18/WE³ podkreślono, że z uwagi na postęp w technologiach informacyjnych i komunikacyjnych, zwłaszcza w celu zwiększenia efektywności przejrzystości procedur udzielania zamówień, środki elektronicznej

¹ Por. M. *Gonczar*, Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców, Warszawa 2009, s. 20 i n.

² Por. Zielona księga. Zamówienia publiczne w UE – w poszukiwaniu rozwiązań, Komunikat Komisji Europejskiej z 27 listopada 1996 r., COM (96) 583.

³ Dyrektywa 2004/14/WE Parlamentu Europejskiego i Rady z 31.3.2004 r. w sprawie koordynacji procedur udzielania zamówień publicznych na roboty budowlane, dostawy i usługi (Dz.Urz. UE L Nr 134, s. 114 ze zm.).

komunikacji powinny być traktowane na równi z tradycyjnymi środkami komunikowania i wymiany informacji (motyw 35 preambuły). Narzędzia elektroniczne dopuszczone do praktycznego zastosowania powinny być w jak największym stopniu kompatybilne z technologiami dopuszczonymi w innych państwach. Oszczędność czasu związaną z wdrażaniem nowych technik komunikacyjnych zalecano poświęcić na istotne skrócenie ustawowych terminów przewidzianych w prawie zamówień publicznych. Dyrektywy z 2004 r. nie spełniły jednak pokładanych nadziei w zakresie usprawnień proceduralnych i poprawy efektywności udzielania zamówień publicznych, zostały zastąpione nowymi dyrektywami z 2014 r. W świetle nowej dyrektywy ogólnej Parlamentu Europejskiego i Rady 2014/24/UE Parlamentu Europejskiego i Rady z 26.2.2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE⁴ sprawny obieg informacji w zamówieniach publicznych ma znaczenie fundamentalne, a przerosty biurokratyczne należy zwalczać środkami elektronicznego przetwarzania danych. Ochrona poufności zaś musi być proporcjonalna i adekwatna do potrzeb, nie może eliminować nikogo z dostępu do informacji o zamówieniach publicznych. To samo wynika z dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE z 26.2.2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającej dyrektywę 2014/17/WE⁵. W rezultacie doniosłe dla sprawności i przejrzystości zamówień publicznych elektroniczne środki przekazu informacji muszą stać się standardowymi środkami komunikacji.

Obowiązkowa elektroniczna zamawiającego do automatyzacji procedur, zwłaszcza w kierunku elektronicznego przetwarzania ofert, z przekroczeniem granic wyznaczonych w dyrektywie ogólnej⁶, ani tym bardziej do elektronicznej oceny ofert, a nawet do zautomatyzowanego obiegu komunikacji wewnętrznej po stronie zamawiającego (por. motywy 51–52 preambuły do dyrektywy 2014/24/UE). Nie wolno zatem eliminować lub ograniczać tradycyjnych kompetencji ewaluacyjnych komisji przetargowych ani nawet pojedynczych urzędników zajmujących się profesjonalną oceną ofert przetargowych. Poza tym trzeba stosować niedyskryminujące, ogólnie dostępne oraz interoperacyjne z produktami ICT środki elektro-

⁴ Dz.Urz. UE L Nr 94, s. 65 ze zm.

⁵ Dz.Urz. UE L Nr 94, s. 243 ze zm.

⁶ Wyjątkowo dopuszcza się zautomatyzowane przetwarzanie ofert w ramach licytacji elektronicznej, aukcji uzupełniającej oraz dynamicznego systemu dokonywania zakupów.

niczne, które są w powszechnym użyciu i nie ograniczają dostępu wykonawców do postępowania o udzielenie zamówienia. Wymagania komunikacyjne, charakterystyka narzędzi i formaty plików muszą być każdorazowo dostatecznie sprecyzowane w warunkach zamówienia (por. motyw 53 preambuły do dyrektywy 2014/24/UE). Wyjątki od nadrzędnej zasady powszechnej dostępności środków elektronicznych są dopuszczalne wyłącznie w przypadkach szczególnych, wskazanych enumeratywnie w dyrektywie, implementowanych w sposób zbliżony w poszczególnych państwach członkowskich. Także nieliczne odstępstwa od zastosowania formy elektronicznej w komunikacji pomiędzy zamawiającym-organizatorem a wykonawcami mogą być dopuszczalne jedynie w przypadkach ustawowo określonych, zdeterminowanych pośrednio dyrektywami.

Wprowadzenie do dyrektyw wymogu pełnej elektronicznej procedur udzielania zamówień publicznych poprzedzały akty przygotowawcze. Decydujący wpływ miała rezolucja Parlamentu Europejskiego z 25.10.2011 r. w sprawie modernizacji zamówień publicznych (2048/INI), a także komunikat Komisji z 20.4.2012 r. o strategii na rzecz e-Zamówień (COM 179)⁷. Według ogólnego art. 22 ust. 1 dyrektywy 2014/24/UE państwa członkowskie zapewniają, aby wszelka komunikacja i wymiana informacji, w szczególności elektroniczne składanie ofert, dokonywana była z wykorzystaniem środków komunikacji elektronicznej w rozumieniu dyrektywy. Na gruncie prawa polskiego odstępstwa od zasady elektronicznego przekazu informacji w sytuacjach szczególnych (na rzecz tradycyjnej pisemności) podaje art. 10c ZamPubU, z obowiązkiem uzasadnienia wyjątków w protokole postępowania. W odniesieniu do nieistotnych elementów procedury można zastosować wyjątkowo nawet ustny przekaz informacji (telefoniczny), jeśli jego treść zostanie następnie w sposób dostateczny udokumentowana (art. 22 ust. 2 dyrektywy 2014/24/UE), choć w ramach prawa polskiego nie doszło do konkretyzacji tych czynności. Szczegółowe wymagania dotyczące narzędzi i urządzeń do elektronicznego odbioru ofert, wniosków lub projektów konkursowych określono w załączniku Nr IV do dyrektywy 2014/24/UE⁸, które w znacznej mierze zostały odzwierciedlone w rozporządzeniu wykonawczym Prezesa Rady

⁷ Por. H. Talago-Sławoj, w: A. Sołtysińska, H. Talago-Sławoj, Europejskie prawo zamówień publicznych. Komentarz, Warszawa 2016, s. 284.

⁸ Chodzi w szczególności o spełnienie wymagań z zakresu: 1) tzw. rozliczalności czasu rzeczywistego przekazu informacji, 2) ochrony poufności, integralności i bezpieczeństwa danych oraz 3) zapewnienia kontroli nad odbiorem i przechowaniem danych, wyłącznie przez osoby uprawnione.

Ministrów z 27.6.2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych⁹. Podstawowe znaczenie ma obowiązek zachowania poufności i integralności ofert lub wniosków aż do momentu ich oficjalnego otwarcia, a także powinność prawidłowego ich przechowywania i archiwizacji. Jeśli poziom ryzyka uzasadnia wymóg zastosowania zaawansowanego podpisu elektronicznego, trzeba przestrzegać norm europejskich o kwalifikowanym certyfikacie do tego rodzaju podpisu wraz z obowiązującymi sposobami jego nieodpłatnej weryfikacji w trybie on-line. Wymagania informatyczne warunkujące ubieganie się przez wykonawcę o zamówienie publiczne mogą stanowić część składową specyfikacji istotnych warunków zamówienia albo przybrać formę załącznika do tego dokumentu, podobnie jak praktykowane od dawna udostępnienie projektu umowy finalnej. Według definicyjnego art. 2 pkt 13 dyrektywy 2014/24/UE wymagane przez zamawiającego „formaty” przedstawiania ofert lub innych oświadczeń mieszczą się w szerszym pojęciu „dokumentów zamówienia”.

Z organizacyjnego punktu widzenia na obszarze Rzeczypospolitej Polskiej podstawowe znaczenie ma InformPodPubIU z kilkoma aktami wykonawczymi. Reguluje ona w szczególności zasady ustalania minimalnych wymagań dla systemów teleinformatycznych oraz ich dostosowania do realizacji zadań publicznych, w tym kształtowanie krajowych ram interoperacyjności, sposobów wymiany informacji drogą elektroniczną, a także funkcjonowania elektronicznej platformy usług administracji publicznej (ePUAP). Podmiotowy zakres tej regulacji pokrywa się niemal w całości z zasięgiem prawa zamówień publicznych (por. art. 2 InformPodPubIU). Wyjątki dotyczą jednak zamawiających prywatnych, zwłaszcza wydatkujących środki publiczne na warunkach art. 3 ust. 1 pkt 5 ZamPubIU. Rozwiązania informatyczne przewidziane w prawie zamówień publicznych, a także w ElektrZamPubU stanowią *lex specialis* względem powołanych przepisów ogólnych o informatyzacji. Nieco na dalszym planie pozostają unormowania z ŚwiadUsłElektU, do której zresztą odsyła nawet sam art. 2 pkt 17 ZamPubIU przy definicji środków komunikacji elektronicznej. Ta ostatnia regulacja pozostaje jednak aktualna jedynie w zakresie definicji i pojęć podstawowych oraz obowiązków usługodawcy związanych ze świadczeniem usług drogą elektroniczną, skoro chodzi o usługi realizowane na odległość poprzez indywidualny przekaz danych, przesyłanych, otrzymanywanych lub przechowywanych za pomocą urzą-

⁹ Dz.U. z 2017 r. poz. 1320 ze zm.

dzeń do elektronicznego przetwarzania (włącznie z kompresją cyfrową) w całości nadawanych, odbieranych lub transmitowanych za pomocą sieci telekomunikacyjnych (przewodowych, światłowodowych, radiowych) w rozumieniu przepisów prawa telekomunikacyjnego (art. 2 pkt 4 ŚwiadUsłElektU)¹⁰. Usługodawca usług elektronicznych (potocznie zwanych internetowymi) to każda osoba, która chociażby ubocznie zajmuje się działalnością z zakresu świadczenia tego rodzaju usług. Takim usługodawcą jest również UZP w zakresie usług świadczonych za pośrednictwem działającej przy urzędzie platformy cyfrowej (e-usługi). Wiele powinności składających się na jego status wynika zatem właśnie z ŚwiadUsłElektU.

Środki komunikacji elektronicznej w sferze zamówień publicznych to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, w szczególności drogą poczty elektronicznej (art. 2 pkt 5 ŚwiadUsłElektU w zw. z art. 2 pkt 17 ZamPublU). Z kolei przez system teleinformatyczny rozumie się jednolicie (na gruncie obu powyższych regulacji) zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniających przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w ujęciu prawa telekomunikacyjnego¹¹, niekoniecznie komputerowego, lecz także funkcjonującego na innych zasadach elektronicznego przekazu informacji. Oznaczanie indywidualnego systemu teleinformatycznego umożliwiające porozumiewanie się za pomocą środków komunikacji elektronicznej nazywa się jednolicie adresem elektronicznym, natomiast oprogramowanie umożliwiające łączenie i wymianę danych w komunikacji między systemami nazywa się „interfejsowym”. Zasady wydawania certyfikatów kwalifikowanego podpisu elektronicznego oraz identyfikacji elektronicznej określa natomiast wprost rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE¹², a także uzupełniająca ustawa krajowa z 5.9.2016 r. o usługach zaufania publicz-

¹⁰ Więcej X. Konarski, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, Warszawa 2004, s. 8 i n.

¹¹ Według ustawy z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2018 r. poz. 1954 ze zm.).

¹² Dz.Urz. UE L Nr 257, s. 73.

nego oraz identyfikacji elektronicznej¹³. Doniosłe znaczenie ma ponadto rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)¹⁴ wraz z uzupełniającą ustawą z 10.5.2018 r. o ochronie danych osobowych¹⁵.

Do realizacji zadań publicznych używa się wyłącznie systemów teleinformatycznych spełniających minimalne wymagania ustalone normatywnie, w tym zapewniających interoperacyjność (współpracę i spójność) między-systemową na zasadach określonych w krajowych ramach interoperacyjności. Przy wymianie informacji poza administracją publiczną system komputerowy powinien spełniać dodatkowo wymagania zapewniające równe traktowanie rozwiązań informatycznych. Zamawiający-organizator publikuje w Biuletynie Informacji Publicznej (BIP) lub udostępnia w inny sposób zestawienie stosowanych w oprogramowaniu interfejsowym struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących (art. 13 ust. 2 pkt 2 lit. a InformPublU). W zamówieniach publicznych obowiązują jeszcze dodatkowe wymagania szczególne z art. 10a–10f ZamPublU, rozwinięte na mocy ElektrZamPubR. Każdy nowo utworzony system teleinformatyczny wymaga przeprowadzania odpowiednich testów akceptacyjnych, o charakterze weryfikacyjnym. Może być zainstalowany wyłącznie na podstawie z góry opracowanego projektu informatycznego zastosowania publicznego, określającego szczegółowe dyspozycje organizacyjno-techniczne, gwarantujące jego sprawność i niezawodność. Minimalne wymagania zapewniają wymianę informacji z innymi systemami, natomiast interoperacyjność polega na zdolności do współdziałania z zastosowaniem właściwych rozwiązań do gromadzenia i przekazywania informacji na rzecz wzajemnie korzystnych efektów. Szczegółowe rozwiązania zawiera KRIR. Interoperacyjność osiąga się przez:

- 1) ujednolicenie polegające na zastosowaniu kompatybilnych norm, standardów i procedur;

¹³ Dz.U. z 2016 r. poz. 1579 ze zm.

¹⁴ Dz.Urz. UE L Nr 119, s. 1.

¹⁵ Dz.U. z 2018 r. poz. 1000 ze zm.

- 2) wymiennosc umożliwiającą zastąpienie w razie potrzeby produktu lub procesu innym, bez zakłócenia wymiany informacji;
- 3) zgodność jako przydatność produktu (procesu) do wspólnego użytkowania.

Zastosowanie któregokolwiek z tych rozwiązań zależy *in casu* od właściwości indywidualnych systemu i oceny ryzyka. Minimalne wymagania dla systemów informatycznych dotyczą w szczególności:

- 1) wymagań techniczno-informatycznych sprzętu i oprogramowania;
- 2) formatów danych w zakresie udostępniania informacji (wskazanych w załączniku 2 KRIR);
- 3) sposobu kodowania dokumentów (w standardzie unicode UTF-8);
- 4) formatów danych w zakresie udostępniania dokumentów (wskazane w załącznikach 3–4 KRIR);
- 5) zachowania poufności i bezpieczeństwa transmisji oraz przechowywania danych, a także
- 6) tzw. rozliczalności operacji polegającej na odpowiednim ich dokumentowaniu (por. standardy z § 20–21 KRIR).

Za zbadanie osiągnięcia właściwego stopnia interoperacyjności przez system teleinformatyczny odpowiada twórca oprogramowania interfejsowego w trybie art. 21 InformPodPublU. Kontrola urzędowa interoperacyjności ma charakter administracyjny.

Do utworzenia i nadzorowania elektronicznej platformy usług administracji publicznej (ePUAP) ustawa zobowiązała ministra właściwego do spraw informatyzacji. Platforma funkcjonuje centralnie w postaci specjalnego systemu teleinformatycznego, w ramach którego instytucje publiczne udostępniają swoje usługi za pośrednictwem tzw. punktów dostępowych w sieci internetowej. Obok zapewnienia zwykłej komunikacji usługą o dużej doniosłości praktycznej jest możliwość utworzenia tzw. profilu zaufanego ePUAP, pozwalającego użytkownikowi platformy na opatrzenie dokumentów tworzonych i przesyłanych z wykorzystaniem ePUAP w podpis elektroniczny, potwierdzony profilem zaufanym (tzw. podpis zaufany), wskazującym jednoznacznie na określoną osobę i jej konto oraz na czas dokonania tego podpisu (art. 20ad–20c InformPodPublU)¹⁶. Podpisu powyższego nie wolno jednak utożsamiać z kwalifikowanym podpisem elektronicznym o wyższym poziomie zaufania, choć nie ma przeszkód, aby ePUAP spełnił rolę kanału prze-

¹⁶ Szczegółową regulację zawiera rozporządzenie Ministra Cyfryzacji z 10.9.2018 r. w sprawie profilu zaufanego i podpisu zaufanego (Dz.U. z 2018 r. poz. 1760).

syłowego dla dokumentów opatrzonych podpisem kwalifikowanym zamiast tzw. podpisem zaufanym potwierdzanym w zwykłym trybie profilem zaufanym. W celu wymiany informacji drogą elektroniczną podmioty publiczne zakładają ogólnie dostępne elektroniczne skrzynki podawcze, spełniające normatywnie ustalone (minimalne) warunki organizacyjno-techniczne doręczania dokumentów¹⁷. Jest to ogólnie dostępny środek komunikacji elektronicznej służący do przekazywania dokumentów elektronicznych z wykorzystaniem ePUAP. Może być stosowany w zamówieniach publicznych, lecz oczywiście na warunkach prawa zamówień publicznych oraz ElektrZamPubR.

Elektroniczne skrzynki podawcze, których adresy powinny być podane w BIP, umożliwiają bezpośrednie doręczanie dokumentów elektronicznych, zgodnych pod względem struktury z wzorami urzędowymi, dostępnymi w centralnym repozytorium ePUAP, lub z zastosowaniem formularzy powiązanych bezpośrednio z tymi skrzynkami. Do całego procesu obsługi doręczeń wykorzystuje się bezpieczny kanał komunikacji zgodny z aktualną technologią internetową, ustaloną przez krajową lub europejską jednostkę normalizacyjną¹⁸. Doręczenie dokumentu elektronicznego może być potwierdzone automatycznie (zwrotnie na adres jego nadania), zwłaszcza opatrzonego podpisem kwalifikowanym albo tzw. podpisem zaufanym ePUAP. Nie wyklucza się jednak tradycyjnej formy potwierdzenia odbioru. Także druga strona (wykonawca) poświadcza odpowiednio odbiór dokumentu elektronicznego nadanego pod uprzednio wskazany adres elektroniczny. Dokumenty elektroniczne udostępnia się z zachowaniem ich integralności, o ile zostały podpisane podpisem elektronicznym, którego ważność w chwili składania może być zweryfikowana przez odbiorcę. W przeciwnym wypadku sporządza się jedynie kopię podpisaną podpisem elektronicznym; na kopię składa się pełna treść udostępnianego dokumentu (oryginału), elementy informacyjne oraz stosowny podpis.

Ustanowienie administratora (inspektora) systemu teleinformatycznego w instytucji sektora publicznego nie jest ustawowo wymagane, jednak w praktyce spotyka się takie stanowisko, zwłaszcza w większych jednostkach. Wyjątkowo z mocy przepisów odrębnych konieczne jest wyodrębnienie funkcji administratora odpowiedzialnego za przetwarzanie (elektroniczne) i ochronę danych osobowych (niekiedy także inspektora nadzorującego),

¹⁷ Por. rozporządzenie Prezesa Rady Ministrów z 14.9.2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 r. poz. 180).

¹⁸ Standardy ogólne podają dyspozycje § 4–5 rozporządzenia powołanego w przypisie poprzednim.

a także inspektora do spraw bezpieczeństwa teleinformatycznego, w związku z ochroną informacji niejawnych. Działający na ogół fakultatywnie „administrator” zapewnia sprawne funkcjonowanie systemu pod względem techniczno-organizacyjnym oraz nadzoruje przestrzeganie zasad prawidłowego jego wykorzystania. Na ogólnych zasadach można mu powierzyć szczególne uprawnienia w zakresie kontroli (monitoringu) personelu.

Efektywne funkcjonowanie komputera wraz z przynależnym sprzętem, a tym bardziej całego systemu komputerowego, zapewnia sterujący program komputerowy (zazwyczaj kilka programów działających w sprzężeniu, nazywanych łącznie oprogramowaniem), który jednak nie został zdefiniowany ustawowo, podobnie zresztą jak wiele innych dóbr intelektualnych. Zdefiniowanie rozwiązań składających się na program komputerowy pozostawiono zatem doktrynie i orzecznictwu. Z mocy przepisów art. 74 ust. 1 PrAut programy komputerowe podlegają ochronie prawnoautorskiej tak jak utwory literackie. Nie wynika z tego bynajmniej, że przynależą one do tej właśnie kategorii utworów, jedynie zasady samej ochrony są zbliżone. Podobnie przepis art. 278 KK, przewidujący odpowiedzialność karną za uzyskanie programu komputerowego bez zgody osoby uprawnionej w celu osiągnięcia korzyści majątkowej, nie określa bliżej przedmiotu przestępstwa. Z braku przepisów odrębnych niemożliwe jest także jakiegokolwiek sensowne odesłanie, co uchybia wyrażnie konstytucyjnej zasadzie dostatecznej określoności czynu zabronionego, skoro pojęcie programu komputerowego nie jest znane powszechnie. W doktrynie dominuje opisowe ujęcie programu komputerowego. Tak jak każdy inny program działania stanowi on zestaw wytycznych, instrukcji lub poleceń przesądzających o układzie (sekwencji) zamierzonych czynności, realizowanych w zasadzie w sposób automatyczny. W piśmiennictwie sięga się najczęściej do prostej definicji zaczerpniętej z prawa japońskiego lub amerykańskiego, w świetle której program komputerowy to kombinacja instrukcji i poleceń powodujących pożądane działanie komputera w celu osiągnięcia określonych rezultatów¹⁹. Z systemowego punktu widzenia program komputerowy stanowi dzieło *sui generis*, zbliżone do dzieła naukowego, co uzasadnia szczególną

¹⁹ Por. zwłaszcza: S. Sołtyśński, Ochrona prawna programów komputerowych, w: Problemy kodyfikacji prawa cywilnego. Księga pamiątkowa ku czci Profesora Zbigniewa Radwańskiego, Poznań 1990, s. 384 i n.; J. Barta, R. Markiewicz, Główne problemy prawa komputerowego, Warszawa 1993, s. 66 i n.; R. Gola, Programy komputerowe w prawie cywilnym i podatkowym – zagadnienia praktyczne, Gdańsk 2007, s. 12; J. Barta, R. Markiewicz, Prawo autorskie, Warszawa 2016, s. 298 i n.; K. Gienas, w: Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, (red. A. Ferenc-Szydelko), Warszawa 2016, s. 358 i n.

ochronę rozwiązań nim objętych. Może być udostępniony na nośniku materialnym lub w drodze elektronicznej.

W zakresie ochrony prawnoautorskiej jednakowo doniosłe są zarówno tekstowe, jak i nietekstowe elementy programu. Do tych drugich należą przede wszystkim rozwiązania organizujące wewnętrzne funkcjonowanie samego programu, zapewniające pośrednio jego pożądane rezultaty. Podstawowe znaczenie ma tzw. system operacyjny, związany z elementami pozatekstowymi, występujący zazwyczaj w postaci kilku programów ze sobą sprzężonych, umożliwiający prawidłową współpracę zainstalowanych programów z komputerem (jako maszyną) i sprzętem towarzyszącym, a także z innymi programami (aplikacjami) użytkowymi. Są też programy o funkcjach pomocniczych, które nazywa się „narzędziowymi”. Każdy program cechuje się określonym językiem programowania, który jednak, tak jak inne idee, nie podlega ochronie²⁰. Język to podstawa tworzenia programu, a jednocześnie sposób przekazywania instrukcji i poleceń dla komputera. Języków programowania jest wiele, a wybór konkretnego należy do programisty²¹. Forma wyrażenia programu też nie jest jednakowa, w szczególności liczy się tzw. kod źródłowy utrwalony w przyjętym języku programowania, w postaci ciągu znaków wskazujących na określone instrukcje lub polecenia (komendy), który podlega przetworzeniu na kod maszynowy (w formie zero-jedynkowej), wyrażający się określonymi impulsami elektrycznymi przetwarzanymi przez procesor, w sposób „zrozumiały” dla komputera²². Ten drugi po zapisaniu w pamięci RAM komputera staje się jego częścią składową. Kody źródłowe, a także sam projekt programu, jak również dokumentacja przeznaczona dla użytkownika są objęte ochroną prawnoautorską, bez względu na zastosowanie: czysto biurokratyczne czy też w zakresie obsługi strony internetowej. Rozwiązywanie problemów z użyciem komputera odbywa się za pomocą algorytmów, które tworzą odpowiednie ciągi instrukcyjne, w zależności od rodzaju zadania. Pod względem przedmiotowym należą one do najważniejszych elementów tworzących program lub oprogramowanie. Algorytm wyraża się zbiorem instruk-

²⁰ Por. wyr. TSUE z 2.5.2012 r., C-406/10, *SAS Institute Inc. przeciwko World Programming Ltd.*, Legalis.

²¹ Jako pierwszy w administracji publicznej stosowano „FORTRAN” (1957), którego z czasem zastępowano „Cobolem” (1960).

²² Kod źródłowy, zrozumiały dla człowieka, nie nadaje się do bezpośredniego przetwarzania przez procesor, dlatego za pomocą specjalnego programu – zwanego kompilatorem – podlega przetłumaczeniu na kod maszynowy i zapisaniu w postaci binarnej w pamięci operacyjnej komputera.

cji przeznaczonych do wykonania (przepisem), obejmujących ciąg logicznie uporządkowanych działań, niezbędnych do rozwiązania konkretnego zadania (sposób postępowania prowadzącego do rozwiązania problemu)²³. Wykonanie finalne programu w wersji binarnej polega bowiem na odpowiednim działaniu procesora, realizującego kolejne instrukcje programu, aż do jego zakończenia. Algorytmy jako zbiory idei nie podlegają ochronie. Ostatni z ważniejszych elementów programu komputerowego to interfejs, kształtujący relacje w układzie użytkownik–komputer, umożliwiający efektywną komunikację z komputerem. W praktyce najczęściej spotyka się interfejsy z wizualizacją graficzną w postaci tzw. okna programu, które jednak ze względu na swoje standardowe właściwości (brak oryginalności) nie podlegają ochronie²⁴, choć *in casu* nie można zupełnie wykluczać elementów twórczych²⁵. Odwoływanie się bowiem do standardów technicznych przy tworzeniu oprogramowania ogranicza kreatywność i stopień oryginalności, uszczuplając automatycznie zakres ochrony. Obok interfejsu użytkownika występują jeszcze interfejsy o charakterze wewnętrznym, zapewniające niezakłóconą komunikację pomiędzy systemem operacyjnym a oprogramowaniem użytkowym (tzw. interoperacyjność wewnętrzną). Oba rodzaje interfejsów uznawane są powszechnie za odrębne elementy oprogramowania.

W świetle przepisów art. 74 PrAut ochrona programu komputerowego obejmuje wszystkie formy jego wyrażenia z wyjątkiem idei i zasad będących podstawą któregokolwiek z elementów programu. Pośród praw osobistych twórca najważniejsze znaczenie ma autorstwo. Z pozostałych praw osobistych przysługujących standardowo twórcom wyłączono – z uwagi na specyfikę – prawo do zachowania integralności utworu, decydowania o jego upublicznieniu oraz do nadzoru nad korzystaniem z programu (art. 77 PrAut). Podstawowe znaczenie mają zatem prawa majątkowe, związane z korzystaniem z programu przez legalnego nabywcę na podstawie umowy licencyjnej lub wyjątkowo o przeniesienie praw, których zakres także został ograniczony ustawowo. Zgodnie bowiem z art. 74 ust. 4 PrAut aktualne są tylko: prawo do niezbędnego zwielokrotnienia programu, prawo do tłumaczenia prowadzącego do stworzenia utworu zależnego, przystosowania, zmiany lub innej modyfikacji

²³ Por. J. Barta, R. Markiewicz, Główne problemy, s. 77 i n., oraz R. Golat, Programy komputerowe, s. 20.

²⁴ Tak TSUE w wyr. z 22.12.2010 r., C-393/09, *Bezpečnostní softwarová asociace*, EU:C:2010:816.

²⁵ Więcej R. Golat, Programy komputerowe, s. 20 i n.; J. Barta, R. Markiewicz, Prawo autorskie, s. 298 i n., oraz K. Gienas, w: Ustawa, s. 363 i n.

użytecznej programu oraz prawo do jego rozpowszechnienia, w tym użyczenia lub najmu. Jeśli jednak program stworzony został przez pracownika w ramach obowiązków pracowniczych, prawa majątkowe przysługują pracodawcy, chyba że z umowy wynika co innego. Możliwości naruszania majątkowych praw autorskich do programu komputerowego w praktyce są o wiele szersze niż w odniesieniu do innych utworów. Już zwyczajna eksploatacja programu łączy się z ryzykiem jego niedozwolonego kopiowania, zwłaszcza z ryzykiem niedopuszczalnego zainstalowania na większej liczbie urządzeń, niż wynika to z licencji. Tymczasem zwykle korzystanie z programu obejmuje jedynie katalog czynności wyróżnionych ustawowo. Zgodnie z art. 75 PrAut można sporządzić niezbędną kopię zapasową, obserwować, badać i testować funkcjonowanie programu, zwielokrotnić kod w wymiarze niezbędnym do współdziałania z innymi programami lub zapewniać jego tłumaczenie itd. Forma tzw. dozwolonego użytku osobisto-prywatnego bez potrzeby upoważnienia (art. 23 PrAut) została natomiast wykluczona całkowicie, nie wspominając o wyłączeniu tradycyjnego prawa do doraźnego zwielokrotnienia dzieł intelektualnych na użytek szkół, bibliotek, archiwów i muzeów, a nawet w celach ściśle publicznych, w tym dla ochrony bezpieczeństwa powszechnego (por. art. 77 PrAut).

Zakres przedmiotowy informatyzacji zamówień publicznych powinien być kompleksowy. Początkowo implementację dyrektyw europejskich w zakresie pełnej elektronicznej przewidywano w okresie najpóźniej do 18.10.2018 r.²⁶ W wyniku nowelizacji ustawy z 22.6.2016 r. o zmianie ustawy – Prawo zamówień publicznych oraz niektórych innych ustaw²⁷ (art. 15) termin ten, w odniesieniu do zamówień małej wartości poniżej europejskiego progu kwotowego (aktualnie do 144 tys. euro, w odniesieniu do zamówień samorządowych 210 tys. euro, a w przypadku zamówień budowlanych – 5548 tys. euro), odroczone jednak do 1.1.2020 r.²⁸ W uzasadnieniu podano, że umożliwi to lepsze przygotowanie się drobnych przedsiębiorców do korzystania z formy elektronicznej, zwłaszcza z zastosowaniem kwalifikowanego podpisu elektronicznego, a wielu zamawiającym wydłuży czas na wdrożenie narzędzi elektronicznych niezbędnych do obsługi procedur udzielania zamówień publicznych, tym bardziej że dyrektywy europejskie w zakresie elektronicznej

²⁶ Więcej o tym *E. Kisiel, D. Konicz, M. Ordysińska*, Elektroniczna zamówień publicznych w praktyce, Wrocław 2018, s. 17 i n.

²⁷ Dz.U. z 2016 r. poz. 1020 ze zm.

²⁸ Por. art. 2 ustawy z 20.7.2018 r. zmieniająca ustawę – Prawo zamówień publicznych oraz ustawę o zmianie ustawy – Prawo zamówień publicznych oraz niektóre inne ustawy (Dz.U. z 2018 r. poz. 1603).

zamówień małej wartości nie mają charakteru bezwzględnie wiążącego. Towarzyszyła temu obawa co do skutków przejściowego ograniczenia konkurencyjności postępowań w zamówieniach mniejszej wartości. Ponadto złączono nieco wymogi elektronizacji obligatoryjnej w odniesieniu do zamówień większej wartości, a mianowicie zastosowanie kwalifikowanego podpisu elektronicznego przewidziano jedynie dla składania ofert lub wniosków o dopuszczenie do postępowania oraz oświadczeń towarzyszących, o których mowa w art. 25a ZamPublU, w szczególności dla jednolitego europejskiego dokumentu zamówienia oraz oświadczenia wykonawcy o powołaniu się na potencjał podwykonawcy, natomiast w pozostałym zakresie dopuszcza się zwykłą formę elektroniczną. Nadal fakultatywne znaczenie ma elektronizacja drobnych zamówień publicznych, wyłączonych spod reżimu ustawowego, o wartości poniżej 30 tys. euro. W pierwszej kolejności liczy się oczywiście informatyzacja procedur udzielania zamówień większej wartości, co wynika zresztą wprost z dyspozycji dyrektyw europejskich z 2014 r., poświęconych tym zamówieniom. W sferze umów o zamówienia publiczne, zwłaszcza w odniesieniu do zasad ich wykonywania, panuje większa swoboda, a zastosowanie formy elektronicznej pozostaje zasadniczo fakultatywne, przy pełnym poszanowaniu autonomicznej woli stron transakcji. Przewiduje się jednak parę wyjątków, a w szczególności e-fakturowanie rozliczenia finansowego transakcji oraz sprawozdawczość elektroniczną o udzielonych zamówieniach.

W okresie przejściowym (do końca 2019 r.) komunikacja między zamawiającym a wykonawcami w postępowaniach o udzielanie zamówień mniejszej wartości odbywa się zgodnie z wyborem zamawiającego: za pośrednictwem operatora pocztowego, osobiście, za pośrednictwem posłańca, faksu lub przy użyciu środków komunikacji elektronicznej w rozumieniu ŚwiadUsłElektU (art. 18a ZmPrZamPubl16). Nie dotyczy to jednak zamówień udzielanych przez centralnych zamawiających, podlegających pełnej elektronizacji, już od 18.10.2018 r., bez względu na szacunkową wartość zamówienia. Wybrany przez zamawiającego sposób przekazywania oświadczeń, wniosków, zawiadomień oraz informacji nie może ograniczać konkurencji. Jeżeli zaś komunikacja odbywa się drogą elektroniczną lub za pomocą faksu, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt otrzymania wiadomości. Tylko wyjątkowo same oferty lub wnioski o dopuszczenie do udziału w postępowaniu, a także oświadczenia, o których mowa w art. 25a ZamPublU, składa się pod rygorem nieważności w formie pisemnej, albo – za zgodą zamawiającego – w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.