


*Dominika Skoczylas\** <https://orcid.org/0000-0003-1231-8078>

## ADMINISTRACYJNOPRAWNE ASPEKTY INFORMATYZACJI SEKTORA OCHRONY ZDROWIA W POLSCE. E-ZDROWIE W DOBIE PANDEMII COVID-19

**Streszczenie.** Celem artykułu jest przedstawienie podstawowych rozwiązań prawnych w zakresie informatyzacji sektora ochrony zdrowia w Polsce. Artykuł w głównej mierze dotyczy administracyjnoprawnych aspektów związanych z wykorzystaniem technologii informacyjno-komunikacyjnych w dziedzinie ochrony zdrowia. Dokonano w nim przeglądu i oceny regulacji prawnych pojawiających się w sytuacji ekstraordynaryjnej, jaką jest pandemia COVID-19. Przedmiotem rozważań były kwestie prawne, społeczne i technologiczne wdrożenia nowych przepisów w czasie pandemii. Analiza tematu pozwoliła odpowiedzieć na pytania czy w dobie pandemii COVID-19 wzrosło zainteresowanie e-usługami medycznymi oraz czy ich świadczenie było efektywne i bezpieczne. Jak wynika z przeprowadzonej analizy, mamy do czynienia z tendencją wzrostową wykorzystywania środków komunikacji elektronicznej w sektorze ochrony zdrowia, stąd też jego informatyzacja jest procesem dynamicznym. Potwierdzono, że usługi medyczne powinny być dostosowane do potrzeb pacjentów (personalizacja usług) i bezpieczne, dlatego niezbędnym aspektem jest również wzmocnienie działań z zakresu cyberbezpieczeństwa świadczenia usług w sektorze ochrony zdrowia. Metody badawcze obejmują analizę podstawowych aktów prawa z wykorzystaniem literatury przedmiotu.

**Słowa kluczowe:** cyberbezpieczeństwo, e-zdrowie, informatyzacja, pandemia COVID-19, sektor ochrony zdrowia

## ADMINISTRATIVE-LEGAL ASPECTS OF INFORMATISATION OF THE HEALTH CARE SECTOR IN POLAND. E-HEALTH IN THE ERA OF COVID-19 PANDEMIC

**Abstract.** The aim of the article is to present basic legal solutions in the field of informatisation of the health care sector in Poland. The article mainly deals with administrative-legal aspects related to the use of information and communication technologies in the field of health care. It reviews and assesses the legal regulations emerging in an extraordinary situation, such as the COVID-19 pandemic. The subject of consideration was the legal, social and technological issues of implementing new regulations during the pandemic. The analysis of the topic made it possible to answer the questions of whether interest in medical e-services has increased in the era of the

---

\* Uniwersytet Szczeciński, [dominika.skoczylas@usz.edu.pl](mailto:dominika.skoczylas@usz.edu.pl)

COVID-19 pandemic and whether their provision has been effective and safe. According to the analysis, there is an increasing trend in the use of electronic means of communication in the health sector, hence its informatisation is a dynamic process. It was confirmed that medical services should be tailored to the needs of patients (personalisation of services) and secure, and therefore it is also necessary to strengthen cybersecurity measures for service provision in the health sector. Research methods include the analysis of basic legal acts with the use of the literature on the subject.

**Keywords:** cybersecurity, e-health, informatisation, COVID-19 pandemic, health sector

## 1. WPROWADZENIE

Organy administracji publicznej, właściwe podmioty czy instytucje są odpowiedzialne za realizację zadań publicznych. Zakłady administracyjne zapewniają ciągłe i bezpośrednie świadczenie usług w takich dziedzinach jak: oświata, kultura, opieka i pomoc społeczna czy ochrona zdrowia (Spasowska-Czarny 2012, 133–134). Wysoka jakość usług publicznych jest jednym z mierników prawidłowo i skutecznie działającej administracji. Niemniej jednak współcześnie, ze względu na potrzeby społeczeństwa oraz postęp technologiczny, obserwuje się dynamiczny rozwój regulacji prawnych dotyczących modernizacji w zakresie świadczenia usług publicznych na odległość. Kluczowe znaczenie ma w tym przypadku polityka prowadzona przez Unię Europejską, która postuluje „proces adaptacji nowoczesnych metod i narzędzi zarządzania zadaniami publicznymi” (Kobylińska 2013, 132). W omawianym zakresie chodzi przede wszystkim o wdrożenie szczególnych, wysokich standardów informatyzacji zadań publicznych. Ukierunkowanie działań administracji na potrzeby obywateli w zakresie zastosowania nowych technologii w usługach publicznych jest nierozzerwalnie związane z tzw. funkcją administracji świadczącej. Dodać bowiem należy, że administracja publiczna angażuje się w działania uwarunkowane przez zmieniające się okoliczności społeczno-gospodarcze, determinanty postępu cywilizacyjnego (Bukowska 2017, 131–133). Wprowadzenie nowego sposobu zarządzania sprawami publicznymi (administracja elektroniczna i usługi elektroniczne) wymagało zmian o charakterze organizacyjno-prawnym, w tym przeobrażenia struktur, dostosowania organizacji do nowych form działania. Pojawiły się zatem specjalne regulacje prawne w kluczowych sektorach usług publicznych. Wraz ze zmianą stylu zarządzania, konieczne było wzmocnienie kompetencji cyfrowych podmiotów odpowiedzialnych za efektywne działanie sektora, a także wyposażenie w odpowiednie środki materialne, w tym zwiększenie wydatków na realizację usług w pełnym zakresie (zakup sprzętu, oprogramowania, zabezpieczeń systemowych).

Kluczowe zmiany objęły sektor ochrony zdrowia, pod kątem planowania i koordynacji działań związanych z jego informatyzacją, tworzenia transparentnych i bezpiecznych systemów informacyjnych, popularyzacji usług on-line w zakresie e-zdrowia czy telemedycyny. Oczywiście pozytywnie należy ocenić także zorientowanie usług na pacjenta, ochronę danych i personalizację usług medycznych.

Można powiedzieć, że informatyzacja systemu ochrony zdrowia w znaczącym stopniu realizuje postulat dostępności do świadczeń zdrowotnych. Niezaprzeczalnie „ochrona zdrowia jest obszarem strategicznym państwa i wymaga systemowego podejścia do zarządzania tym obszarem dla urzeczywistnienia sprawności systemu” (Rogowska 2019, 222). Aczkolwiek należy zauważyć, że pełna informatyzacja sektora ochrony zdrowia jest procesem jeszcze nieukończonym. Ponadto, istnieje wiele problemów związanych ze świadczeniem usług i bezpieczeństwem systemów informacyjnych, które dostrzeżono m.in. w dobie pandemii COVID-19. W tym czasie konieczne było również wprowadzenie regulacji prawnych, umożliwiających realizację usług medycznych. Ocena powyższego wymaga przedstawienia rozwiązań prawnych odnoszących się bezpośrednio do informatyzacji sektora ochrony zdrowia (także tych, które powstały w czasie pandemii).

## 2. INFORMATYZACJA, TECHNOLOGIE INFORMACYJNO-KOMUNIKACYJNE

Bez wątplenia informatyzacja przyczyniła się do usprawnienia świadczenia usług publicznych na odległość<sup>1</sup>. Przetwarzanie i transmisja danych za pomocą sieci telekomunikacyjnej ułatwiły i przyspieszyły realizację zadań publicznych, przy jednoczesnym zachowaniu transparentności działań podmiotów administrujących. Informatyzacja pozwala zwiększyć efektywność i poprawić jakość świadczenia usług publicznych. Dlatego tak istotne są zdolność sektora publicznego (do którego zalicza się także sektor ochrony zdrowia) do szybkiego wprowadzenia zmian w odniesieniu do nowych warunków społeczno-gospodarczych oraz wykorzystywanie innowacyjnych rozwiązań w organizacji i przeciwdziałanie wykluczeniu cyfrowemu (Jastrzębska 2018, 46). Aleksandra Monarcha-Matlak wskazuje na szczególne zalety komunikacji elektronicznej, wśród których wymienia m.in. równoczesność, pojemność i zintegrowanie przekazu czy wielopłaszczyznowość. Ponadto zauważa różnorodność rozwiązań technicznych i narzędzi teleinformatycznych służących porozumiewaniu się na odległość i pojawianie się coraz to nowszych form e-kontaktów (Monarcha-Matlak 2022, 269). Nowe technologie nie są obce także sektorowi ochrony zdrowia.

Dostępność, efektywność i kompatybilność publicznych usług elektronicznych nie byłaby możliwa bez zmian systemowych i wdrożenia nowoczesnych technologii informacyjno-komunikacyjnych tzw. ICT (z ang. *Information and*

---

<sup>1</sup> Przez świadczenie usługi drogą elektroniczną, zgodnie z art. 2 pkt 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344) należy rozumieć wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

*Communication Technologies*). Chodziło o wprowadzenie takich rozwiązań technologicznych (sprzętu, oprogramowania, infrastruktury teleinformatycznej), które zapewnią przetwarzanie danych (komunikację) i świadczenie usług na odległość (Sibiga 2011, 3). Takie czynniki jak interoperacyjność, cyfrowość oraz transgraniczność przemawiają za szerokim zastosowaniem ICT w kluczowych dla sektora publicznego e-usługach. Bezspornie, istotą informatyzacji jest wzajemna, powszechna, swobodna wymiana danych i świadczenie usług, masowy i interaktywny charakter komunikatu, pełne usieciowienie oraz zapewnienie bezpiecznego i równego dostępu do e-zasobów (Skoczylas 2021, 234–235). W sektorze ochrony zdrowia ICT służą zarówno świadczeniu usług (np. telemedycyna), umożliwiając przygotowanie, udostępnianie, gromadzenie dokumentacji (np. obieg elektronicznej dokumentacji medycznej, e-recepty, e-skierowania, e-zwolnienia). W sytuacjach nadzwyczajnych mogą (i faktycznie są, co można było zauważyć w czasie pandemii COVID-19) okazać się jedyną formą kontaktu z placówką medyczną.

W toku rozważań o informatyzacji sektora publicznego należy uznać, że istotną rolę w zakresie prawidłowego sposobu realizacji zadań publicznych pełnią organy administracji publicznej (podmioty administrujące). Administracyjnoprawne aspekty informatyzacji odnoszą się do ustalenia zasad e-zarządzania i świadczenia e-usług, co jest zadaniem podmiotów posiadających władztwo administracyjne. Nie ulega wątpliwości, że przedmiotowy cel może być spełniony wyłącznie wtedy, gdy będą obowiązywały odpowiednie regulacje prawne określające standardy działania, tj. warunki konieczne do informatyzacji sektora publicznego w skali makro. W polskim porządku prawnym jednym z najważniejszych aktów w tym zakresie jest ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r., poz. 57 ze zm.), która określa m.in. tak kluczowe kwestie jak ustalanie minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych oraz dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi, Krajowych Ram Interoperacyjności systemów teleinformatycznych czy funkcjonowanie ePUAP. Równocześnie nie można pominąć rozwiązań zawartych w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r., poz. 1797). Identyfikacja elektroniczna jest jednym z podstawowych czynników wpływających na skuteczność, ale także bezpieczeństwo świadczenia e-usług. Koncepcja niezbędności regulacji prawnych i realizacji zadań *stricto* decyzyjnych, tj. formalnych, wymaga zorientowania na potrzeby obywateli. Kolejno zaś należy uwzględnić postęp technologiczny i zapewnić takie środki teleinformatyczne, za pomocą których e-usługi będą świadczone w sposób efektywny, całościowy, a przede wszystkim bezpieczny. Ze względu na uwagi poczynione powyżej, szczególnego znaczenia nabiera materia administracyjnoprawnych aspektów informatyzacji sektora ochrony zdrowia. W krajowym porządku prawnym istnieją bowiem specyficzne rozwiązania prawne w zakresie zastosowania ICT w tym segmencie życia publicznego.

### 3. REGULACJE PRAWNE W ZAKRESIE INFORMATYZACJI OCHRONY ZDROWIA W POLSCE

Ochrona zdrowia stanowi wartość konstytucyjną. Art. 68 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm.) wyznacza władzom publicznym zadania w zakresie zapewnienia równego dostępu do świadczeń publicznej opieki zdrowotnej. Wskazano w nim również rolę administracji publicznej w kontekście zapewnienia szczególnej opieki zdrowotnej dzieciom, kobietom ciężarnym, osobom niepełnosprawnym i osobom w podeszłym wieku. Warto przy tym – biorąc pod uwagę okoliczność wystąpienia pandemii COVID-19, podkreślić aktualizację obowiązków organów w zakresie zwalczania chorób epidemicznych. Informatyzacja sektora ochrony zdrowia, stanowiąca kiedyś rewolucyjne rozwiązanie, obecnie traktowana jest jako element konieczny funkcjonowania służby zdrowia. Wymieniane są bowiem liczne korzyści zastosowania ICT w ramach zw. technologii e-zdrowie, która „obejmuje różnorodne zastosowania systemów informatycznych i telekomunikacyjnych do realizacji usług mających kontekst zdrowotny lub medyczny” (Duplaga 2010, 48).

Innowacyjność, dostępność oraz automatyzacja usług to podstawowe czynniki, które przemawiają za szerokim zastosowaniem ICT w sektorze ochrony zdrowia. Warto zadać pytanie, czy realizację chociażby części świadczeń przy użyciu nowych technologii należy ocenić pozytywnie. Pojawiają się tutaj trzy perspektywy przedmiotowej oceny, *stricte* administracyjnoprawna (określenie zasad świadczenia e-usług, skutków prawnych podejmowanych działań), społeczna (ułatwienia w dostępie do świadczeń) i technologiczna (wykorzystanie ICT jako bezpiecznego narzędzia wspierającego proces leczenia). W odniesieniu do pierwszej z nich, skonstatować należy, że chodzi o wdrożenie kompleksowych regulacji prawnych, a także takie zorganizowanie struktur, które umożliwią skuteczną realizację usług medycznych na odległość, określą wprost kompetencje organów, podmiotów odpowiedzialnych za funkcjonowanie sektora (m.in. placówek medycznych). Warto wspomnieć chociażby takie akty prawne jak: ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentystry (t.j. Dz.U. z 2023 r., poz. 1516 ze zm.), ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz.U. z 2022 r., poz. 2561 ze zm.), ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2023 r., poz. 1545), ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2022 r., poz. 1555 ze zm.) czy ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (t.j. Dz.U. z 2022 r., poz. 2527).

W celu realizacji określonych zadań publicznych w sektorze ochrony zdrowia, potrzebna jest również wykwalifikowana kadra pracowników, posiadająca stosowne kompetencje cyfrowe, co jest niezwykle istotne, w przypadku m.in.

elektronicznego obiegu dokumentacji medycznej czy korzystania z telemedycyny. Zmiany o *stricte* administracyjnym charakterze pozwalają obniżyć koszty leczenia i diagnostyki, usprawnić proces leczenia (w tym kontrolę realizacji świadczeń), zminimalizować nadużycia np. w kwestii refundacji czy rozliczeń, wprowadzić alternatywne sposoby leczenia, usprawnić dostęp do dokumentacji medycznej czy podnieść kwalifikacje personelu medycznego. W świetle powyższych rozważań, bezpośrednim skutkiem będzie poprawa dostępności i jakości świadczeń zdrowotnych (Batko 2012, 97–98). Należy zwrócić uwagę na to, że obecnie zgodnie z art. 4 ustawy o podstawowej opiece zdrowotnej, koordynacja opieki zdrowotnej nad świadczeniobiorcą w systemie ochrony zdrowia ma ściśle „informatyzowany charakter”. Istnieje także szeroki katalog elektronicznej dokumentacji medycznej, do której należy zaliczyć m.in. e-recepty, e-skierowania, e-zwolnienia, ale też inne dokumenty umieszczone w systemach informacji<sup>2</sup>. Aleksandra Klich słusznie zauważa wady i zalety prowadzenia dokumentacji w formie elektronicznej. Za korzystne uznaje możliwość co do zasady nieograniczonego dostępu do dokumentacji medycznej (pacjentów i podmiotów leczniczych), kompleksowość i wyższą jakość udzielania świadczeń zdrowotnych (profilaktyka, diagnostyka, leczenie), automatyzację tworzenia dokumentacji medycznej (rzetelny i transparenty sposób sporządzania dokumentacji), wdrożenie innowacyjnych rozwiązań – Internetu Rzeczy w usługach medycznych. Należy zgodzić się z Autorką, że efektywne zastosowanie ICT w sektorze ochrony zdrowia wymaga zapewnienia bezpieczeństwa przetwarzania danych w systemach teleinformatycznych, co wiąże się z ochroną prywatności pacjentów (Klich 2017, 357–358).

Kolejna perspektywa wiąże się z oczekiwaniami pacjentów, a jednocześnie z ułatwieniami w zakresie dostępu do świadczeń. Z raportu Głównego Urzędu Statystycznego za 2020 r. (Główny Urząd Statystyczny 2022, 60–61) wynika, że coraz częściej korzystamy z Internetu w celu realizacji świadczeń medycznych. Polacy chętnie rezerwują wizyty lekarskie, sprawdzają wyniki badań czy dostępność produktów leczniczych online. Niewątpliwie pandemia COVID-19 spowodowała wzrost zainteresowania ICT w usługach medycznych. Z analizy GUS wynika m.in., że w 2020 r. 34,2% członków gospodarstw domowych wykorzystywało Internet w celu uzyskania informacji o chorobach oraz sposobach leczenia, a 31,0% poszukiwało danych na temat zdrowego stylu życia. Z kolei 22,4% badanych sprawdzało opinie na temat lekarzy, a 9,2% skorzystało z Internetu w celu zakupienia produktu leczniczego. Na wizytę lub badanie przez stronę internetową w czwartym kwartale 2020 umówiło się 4,9% respondentów, telefonicznie – 36,2%. Zatem kolejnym z administracyjnoprawnych skutków

---

<sup>2</sup> Wyróżnia się m.in. System Informacji Medycznej, dziedziczne systemy teleinformatyczne np. System Rejestru Usług Medycznych Narodowego Funduszu Zdrowia, System Monitorowania Dostępności do Świadczeń Opieki Zdrowotnej, System Obsługi List Refundacyjnych czy rejestry medyczne. Zob. art. 5 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

informatyzacji sektora ochrony zdrowia będzie wdrożenie zasad administracji świadczącej, promującej zaangażowanie pacjenta w bezpośredni monitoring świadczeń zdrowotnych i umożliwiającej kompleksowy zakres realizacji świadczeń medycznych online.

Powyższe wiąże się z trzecią perspektywą technologiczną (wykorzystanie ICT jako bezpiecznego narzędzia wspierającego proces leczenia). Efektywność działań, oprócz regulacji prawnych i uwarunkowań społecznych, wymaga również wprowadzenia odpowiedniej polityki bezpieczeństwa świadczeń medycznych. Tutaj pod uwagę należy wziąć przede wszystkim cyberbezpieczeństwo usług medycznych, ochronę prywatności (danych osobowych pacjentów) oraz poufność dokumentacji medycznej. Wyzwania a zarazem konieczność wprowadzenia zmian w zakresie aktualnej polityki bezpieczeństwa e-zdrowia i świadczenia usług na odległość zauważono w dobie pandemii COVID-19.

#### 4. SYTUACJA EKSTRAORDYNARYJNA – PANDEMIA COVID-19 EFEKTYWNOŚĆ I CYBERBEZPIECZEŃSTWO SEKTORA OCHRONY ZDROWIA

W obrębie administracyjnoprawnych skutków informatyzacji należy zwrócić uwagę na szczególne rozwiązania wprowadzone w ekstraordynaryjnej sytuacji, jaką była pandemia COVID-19. Rozważania wymagają kwestie prawne, społeczne i technologiczne wdrożenia nowych przepisów w czasie pandemii. Istotnie, na co wskazują chociażby przedstawione wcześniej analizy statystyczne GUS, w dobie pandemii COVID-19 wzrosło zainteresowanie e-usługami medycznymi, pojawiły się jednak problemy z bezpieczeństwem czy dostępnością do e-usług. W związku ze znaczną liczbą zakażeń wirusem SARS-CoV-2, od 2020 r. zdecydowano się wprowadzić (często *ad hoc*) zmiany w zakresie funkcjonowania kluczowych sektorów życia publicznego, m.in. w organizacji służby zdrowia (Pyrzyńska i Skoczylas 2020, 227). W istocie służba zdrowia musiała przyjąć określone standardy działania i metody w walce z poważnym kryzysem zdrowotnym. Wzorem rozwiązań międzynarodowych krajowe organy władzy publicznej wprowadziły m.in. ograniczenia w przemieszczaniu się, podróżowaniu, zakaz zgromadzeń, pracę i naukę w formie online, a w kwestiach *stricto* medycznych – obowiązek odbycia kwarantanny, noszenia maseczek ochronnych, wdrożono także program szczepień przeciwko COVID-19 (Robakowski, Synowec 2020, 92–93).

Wobec wzrastającej skali zachorowań wprowadzono ustawę z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t.j. Dz.U. z 2023 r., poz. 1327 ze zm.). Określono, m.in., że w przypadku braku dostępności do lekarza uprawnionego do przeprowadzenia badania wstępnego lub kontrolnego, badanie takie może przeprowadzić i wydać odpowiednie orzeczenie lekarskie inny lekarz (art. 12a

ust. 3 specustawy), przedłużono ważność orzeczeń lekarskich funkcjonariuszy publicznych (art. 31k specustawy) i orzeczeń lekarskich wydanych w ramach wstępnych, okresowych i kontrolnych badań lekarskich (art. 31m specustawy). Specustawa wpłynęła na zmiany innych ustaw dotyczących funkcjonowania sektora ochrony zdrowia. Kwestie prawne objęły wprowadzenie rozwiązań mobilnych, za pomocą których możliwe było zlokalizowanie miejsca pobytu chorego i potencjalnego kontaktu z innymi osobami. W dobie pandemii zwiększył się dostęp do specjalistycznych usług medycznych, popularność zyskała telemedycyna. Zastosowanie technologii teledywidualnych należy ocenić pozytywnie ze względu na możliwość zdalnego prowadzenia procesu leczenia pacjenta w jego domu (użycie specjalistycznych urządzeń) czy zachowanie stałej komunikacji z pacjentem w ramach opieki skoordynowanej – konsultacji na odległość (Kwiatkowska 2022, 163).

W odniesieniu do uwarunkowań społecznych i technologicznych, podmioty służby zdrowia (przez placówki medyczne – lekarzy podstawowej opieki zdrowotnej, laboratoria do powiatowych stacji sanitarno-epidemiologicznych i do stacji wojewódzkich) przekazywały informacje o zakażeniach, hospitalizacjach, ozdrowieniach i zgonach spowodowanych koronawirusem. Miało to oczywiście swój wydźwięk epidemiologiczny, ale również statystyczny (Golinowska i Zabdyr-Jamroz 2020, 11). Z kolei kwestie *stricte* technologiczne dotyczyły głównie wykorzystania ICT w ramach elektronicznego obiegu dokumentów, ale także zintegrowania działań na polu świadczenia usług medycznych. Na pytanie czy w dobie pandemii COVID-19 wzrosło zainteresowanie e-usługami medycznymi – należy odpowiedzieć zdecydowanie twierdząco. Nałożono wiele nowych obowiązków na podmioty wchodzące w skład sektora ochrony zdrowia, w związku z koniecznością świadczeń usług na odległość. Wzrosła liczba pacjentów, którym pomoc mogła zostać udzielona online (czy telefonicznie), zaangażowania wymagało również wprowadzenie szczepień ochronnych (funkcjonowanie infolinii szczepień). Czy natomiast świadczenie usług zdrowotnych w czasie pandemii było efektywne i bezpieczne? Odpowiedź nie jest jednoznaczna, albowiem usługi medyczne co do zasady były spersonalizowane, natomiast kwarantanna negatywnie wpłynęła na zdrowie fizyczne i psychiczne szczególnie osób starszych i poddanych długotrwałej izolacji/kwarantannie (Sokół-Szawłowska 2021, 58). Wystąpiły problemy z dostępem do e-usług (bariery, wykluczenie cyfrowe). Zawodne okazały się także niektóre rozwiązania teleinformatyczne. Oprócz zakłóceń w ciągłości świadczenia usług dostrzeżono następujące zagrożenia: nieuprawnione udostępnienie czy modyfikację danych wrażliwych, ataki typu phishing, incydenty hakerskie, instalowanie złośliwych oprogramowań czy działania o charakterze cyberprzestępczym, a nawet cyberterrorystycznym. Powyższe jest wynikiem słabości systemów zabezpieczających (infrastruktury teleinformatycznej), niedostatecznych umiejętności cyfrowych kadry medycznej i administracyjnej oraz nieodpowiednich procedur



i mechanizmów zwalczania cyberzagrożeń i incydentów istniejących w organizacji (Makuch, Guziak 2020, 91–92).

Ochrona zdrowia należy do usług, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej państwa<sup>3</sup>. Dlatego też *de lege ferenda* dobrym zabiegiem byłoby wprowadzenie optymalnej polityki cyberbezpieczeństwa w poszczególnych segmentach świadczenia e-usług medycznych. Proponuje się, aby odpowiedzialnymi za wdrożenie polityki cyberbezpieczeństwa w ramach technologii e-zdrowie były placówki medyczne (dyrektorzy placówek), którzy w porozumieniu z przedstawicielami Ministerstwa Zdrowia i pracownikami placówki stworzyliby wspólną strategię umożliwiającą ograniczenie negatywnych skutków incydentów i cyberzagrożeń. W tym celu należałoby również podjąć współpracę z sektorem IT.

## 5. PODSUMOWANIE

Reasumując, informatyzacja sektora ochrony zdrowia jest zjawiskiem dynamicznym. Rozwój ICT wpłynął na zmiany w świadczeniu usług medycznych, zarówno pod kątem organizacyjno-prawnym, jak i społecznym. W wyniku przeprowadzonej analizy wskazano, że administracyjnoprawne aspekty informatyzacji ochrony zdrowia przynoszą wymierne skutki nie tylko w powstaniu licznych regulacji prawnych, ale również w kwestii poprawy jakości świadczenia e-usług i ich personalizacji, a także wzrostu kompetencji cyfrowych administracji i pracowników służby zdrowia. Przedstawiona w artykule analiza statystyczna Głównego Urzędu Statystycznego potwierdza, że mamy do czynienia z tendencją wzrostową wykorzystywania ICT w sektorze ochrony zdrowia.

Co do zasady pozytywnie należy ocenić prawotwórcze działania organów administracji publicznej w dobie pandemii COVID-19. Trzeba przyznać, że w tym czasie wzrosło zainteresowanie e-usługami medycznymi (co stanowiło najczęściej jedyną możliwość kontaktu ze służbą zdrowia), natomiast nie zawsze ich realizacja była efektywna i bezpieczna. Tym samym niezbędne jest wzmocnienie działań z zakresu cyberbezpieczeństwa i weryfikacja świadczenia e-usług z kilku perspektyw, o których była mowa powyżej, tj. administracyjnoprawnej (skonkretyzowanie zasad świadczenia e-usług i skutków prawnych podejmowanych działań), społecznej (ograniczenie barier, wykluczenia cyfrowego) i technologicznej (w szczególności pod kątem cyberbezpieczeństwa). *De lege ferenda* proponuje się wprowadzenie polityki cyberbezpieczeństwa w poszczególnych segmentach świadczenia e-usług medycznych za której wdrożenie odpowiedzialne byłyby wszystkie podmioty mające wpływ na funkcjonowanie służby zdrowia z Ministrem Zdrowia i dyrektorami

---

<sup>3</sup> Zob. Załącznik nr 1 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913).

placówek medycznych na czele. Polityka cyberbezpieczeństwa mogłaby poprawić zarówno jakość świadczenia usług – tj. „umożliwić ciągłą realizację e-usług o wysokim standardzie” (Skoczylas 2022, 329), jak i ograniczyć negatywne skutki cyberzagrożeń.

## BIBLIOGRAFIA

- Batko, Kornelia. 2012. „Wykorzystanie technologii informacyjno-komunikacyjnych w transformacji organizacji z sektora ochrony zdrowia – koncepcja e-zdrowie”. W *Technologie informacyjne w transformacji współczesnej gospodarki*. Seria: *Zeszyty Naukowe Wydziałowe Uniwersytetu Ekonomicznego w Katowicach. Studia Ekonomiczne*. Red. Celina M. Olszak, Ewa Ziemba. 95–113. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.
- Bukowska, Joanna. 2017. „Funkcje administracji publicznej”. W *Nauka administracji*. Red. Zbigniew Cieślak. 121–137. Warszawa: Wolters Kluwer.
- Duplaga, Mariusz. 2010. „Znaczenie technologii e-zdrowia w rozwoju innowacyjnego modelu świadczenia usług w ochronie zdrowia”. *Zdrowie Publiczne i Zarządzanie* 2 (VIII): 47–55.
- Główny Urząd Statystyczny. 2022. „Analizy statystyczne. Ochrona zdrowia w gospodarstwach domowych w 2020 r.” Warszawa, Kraków. <https://stat.gov.pl/obszary-tematyczne/zdrowie/zdrowie/ochrona-zdrowia-w-gospodarstwach-domowych-w-2020-r-,2,7.html> (dostęp: 14.11.2022).
- Golinowska, Stanisława. Zabdyr-Jamroz, Michał. 2020. „Zarządzanie kryzysem zdrowotnym w pierwszym półroczu pandemii COVID-19. Analiza porównawcza na podstawie opinii ekspertów z wybranych krajów”. *Zdrowie Publiczne i Zarządzanie* 18(1): 1–31.
- Jastrzębska, Karolina. 2018. *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*. Warszawa: CeDeWu.
- Klich, Aleksandra. 2017. „Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej”. *Ekonomiczne Problemy Usług* 126(2): 351–360.
- Kobylińska, Urszula. 2013. „Mierniki sprawności usług publicznych”. *Współczesne Zarządzanie* 2: 131–140.
- Kwiatkowska, Ewa. M. 2022. „Cyfryzacja ochrony zdrowia a konieczność wprowadzania nowych rozwiązań prawnych”. *Krytyka Prawa. Niezależne studia nad prawem* 14(1): 154–170.
- Makuch, Julia. Guziak, Matusz. 2020. „Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych”. *Rocznik Bezpieczeństwa Międzynarodowego* 14(2): 86–102.
- Monarcha-Matlak, Aleksandra. 2022. „Komunikacja elektroniczna, prawo komunikacji elektronicznej, Europejski kodeks łączności elektronicznej i ich wpływ na rozwój jurysdykcji administracyjnej”. W *Kierunki rozwoju jurysdykcji administracyjnej*. Red. Marek Szewczyk, Lucyna Staniszevska, Maciej Kruś. 267–276. Warszawa: Wolters Kluwer.
- Pyrzyńska, Agata. Skoczylas, Dominika. 2020. „Elections during COVID-19 Pandemic in the Light of Democratic Values and International Standards of Human Rights Protection”. *European Research Studies Journal* XXIII, special issue 2: 226–246.
- Robakowski, Piotr. Synowec, Joanna. 2020. „Polityka zdrowotna RP – co zmieniło się w dobie COVID 19?”. *Studia Polityczne* 48(3): 85–106.
- Rogowska, Klaudia. 2019. „Ochrona zdrowia jako strategiczny obszar zarządzania państwa”. *Nierówności Społeczne a Wzrost Gospodarczy* 59(3): 212–225.
- Sibiga, Grzegorz. 2011. „Informatyzacja administracji publicznej w Polsce”. *Edukacja Prawnicza* 3: 3–7.

- Skoczylas, Dominika. 2021. „Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku”. W *Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonałości warsztatu naukowca*. Red. Michał Staniszewski, Henryk A. Kretek. 233–243. Gliwice: Wydawnictwo Politechniki Śląskiej.
- Skoczylas, Dominika. 2022. „Rozwój teleinformatyczny państw Europy Wschodniej w kontekście cyberbezpieczeństwa. Zagrożenia a ochrona cyberprzestrzeni – wybrane zagadnienia”. *Prawo i Więź* 3(41): 328–344.
- Sokół-Szawłowska, Marlena. 2021. „Wpływ kwarantanny na zdrowie psychiczne podczas pandemii COVID-19”. *Psychiatria* 18(1): 57–62.
- Spasowska-Czarny, Hanna. 2012. „Zakład publiczny a przedsiębiorstwo państwowe: kryteria rozróżnienia w poglądach doktryny prawa administracyjnego”. *Studia Iuridica Lublinensia* 18: 133–140.

### Akty prawne

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 ze zm.).
- Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentystry (t.j. Dz.U. z 2023 r., poz. 1516 ze zm.).
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 344).
- Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz.U. z 2022 r., poz. 2561 ze zm.).
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r., poz. 57 ze zm.).
- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2023 r., poz. 1545).
- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2022 r., poz. 1555 ze zm.).
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r., poz. 1797).
- Ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (t.j. Dz.U. z 2022 r., poz. 2527).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913).
- Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t.j. Dz.U. z 2023 r., poz. 1327 ze zm.).