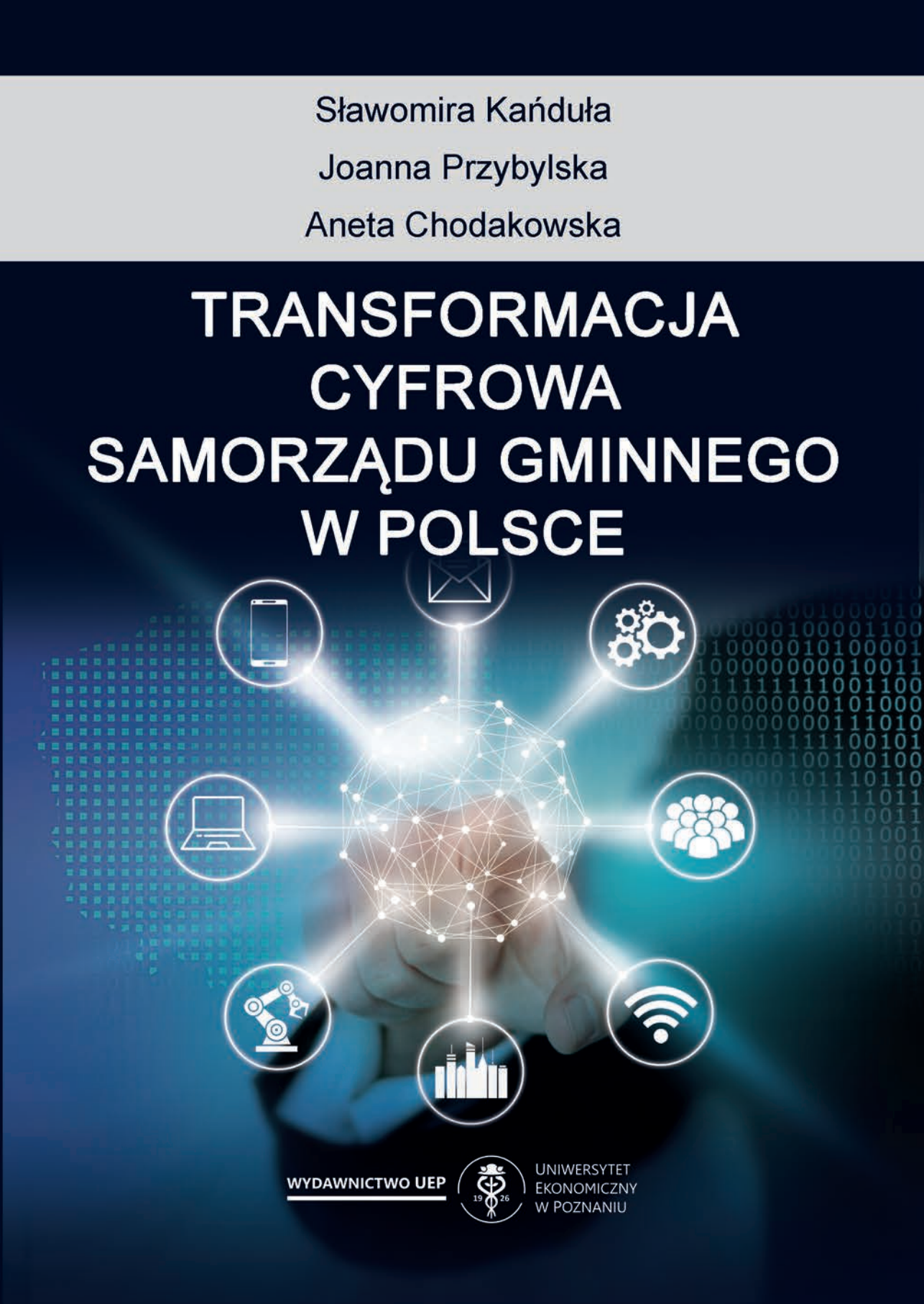
Sławomira Kańduła
Joanna Przybylska
Aneta Chodakowska

TRANSFORMACJA CYFROWA SAMORZĄDU GMINNEGO W POLSCE

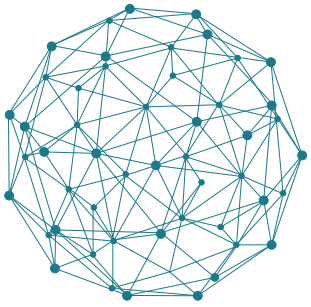


WYDAWNICTWO UEP
UNIWERSYTET EKONOMICZNY W POZNANIU

TRANSFORMACJA CYFROWA SAMORZĄDU GMINNEGO W POLSCE

Sławomira Kańduła
Joanna Przybylska
Aneta Chodakowska

TRANSFORMACJA CYFROWA SAMORZĄDU GMINNEGO W POLSCE



WYDAWNICTWO UEP
UNIWERSYTET EKONOMICZNY W POZNANIU

Poznań 2023

Sławomira Kańduła
Joanna Przybylska
Aneta Chodakowska

Badania ankietowe sfinansowano ze środków przyznanych w ramach programu Ministra Edukacji i Nauki pod nazwą „Regionalna Inicjatywa Doskonałości" w latach 2019–2023 nr projektu 004/RID/2018/19 kwota finansowania 3 000 000 zł

ISBN: 978-83-8211-165-1
e-ISBN: 978-83-8211-166-8
https://doi.org/10.18559/978-83-8211-166-8

Sugerowane cytowanie: Kańduła, S., Przybylska, J. i Chodakowska, A. (2023). Transformacja cyfrowa samorządu gminnego w Polsce. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. https://doi.org/10.18559/978-83-8211-166-8

WYDAWNICTWO UNIWERSYTETU EKONOMICZNEGO W POZNANIU
ul. Powstańców Wielkopolskich 16, 61-895 Poznań
tel. 61 854 31 54, 61 854 31 55
www.wydawnictwo.ue.poznan.pl, e-mail: wydawnictwo@ue.poznan.pl
adres do korespondencji: al. Niepodległości 10, 61-875 Poznań

Skład: Wydawnictwo eMPI²

Druk: Zakład Graficzny Uniwersytetu Ekonomicznego w Poznaniu
ul. Towarowa 53, 61-896 Poznań, tel. 61 854 38 06

SPIS TREŚCI

WSTĘP

Początek XXI wieku to okres dynamicznego rozwoju światowej gospodarki i dążenia do tzw. gospodarki 4.0. Gospodarka ta jest uogólnieniem koncepcji przemysłu 4.0, mają w niej zastosowanie nie tylko technologie ogólnego przeznaczenia, ale także technologie wspierające, np. internet rzeczy (*Internet of things* – IoT), systemy cyber-fizyczne, technologia mgły i chmury (*fog and cloud computing)*, sztuczna inteligencja *(artificial intelligence* – AI), analityka obliczeniowa wykorzystująca gigadane, robotyka, technologie addytywne (druk 3D), rozszerzona rzeczywistość. Główną siłą napędową rozwoju są więc obecnie technologie informacyjno-komunikacyjne (*information and communication technologies* – ICT). Technologie te decydują o charakterze współczesnej gospodarki, wyznaczają tempo jej przeobrażeń oraz umożliwiają efektywniejsze i szybsze gromadzenie, przetwarzanie, analizę i wykorzystanie danych oraz efektywniejsze zaspokajanie potrzeb publicznych.

Jeśli Polska chce być ważnym uczestnikiem tej gospodarki, musi spełniać wymagania stawiane przez konkurencyjne gospodarki, których cechami są: wysoki poziom rozwoju technologicznego, wysoka produktywność i dobra organizacja pracy. O sukcesie decydują nie tylko ludzie (poszczególne jednostki, pracodawcy, organizacje społeczne), ale także instytucje publiczne. Wszyscy powinni być gotowi na zmiany, doskonalić swoje umiejętności i być otwarci na wdrażanie nowych rozwiązań cybernetycznych.

W literaturze podkreśla się konieczność implementacji przez instytucje publiczne nowych technologii (Ojo, 2019). Należy się zastanowić nad rolą samorządu terytorialnego w tym zakresie (Dylewski i Kępa, 2009). Z jednej strony jest on podmiotem, który musi się dostosować do wyzwań światowej gospodarki i przeciwdziałać zagrożeniom związanym z „cyfrową transformacją". Z drugiej strony powinien wspierać kształtowanie konkurencyjności podmiotów gospodarczych zlokalizowanych na jego terenie i podnosić kompetencje cyfrowe mieszkańców. Wymusza to nowe spojrzenie na zakres zadań samorządu oraz sposób ich wykonywania, a także poszukiwanie nowych źródeł finansowania tych zadań.

W Polsce literatura przedmiotu na temat technologii informacyjno-komunikacyjnych w kontekście samorządu terytorialnego nie jest bogata. Szerzej opisany jest w zasadzie tylko wątek *smart city* (Sikora-Fernandez, 2018) i konieczności rozwoju e-administracji samorządowej (Cellary, 2019b). Badania diagnozujące stan gotowości jednostek samorządu terytorialnego (jst) do ich implementacji są albo wycinkowe (Jastrzębska, 2018), albo częściowo nieaktualne (Basikowska, 2011), albo pokazują e-administrację przez pryzmat obywatela (Wilk,

2014). Czynniki sukcesu i poziom wykorzystania technologii informacyjno-komunikacyjnych przez administrację publiczną w Polsce badał w zasadzie tylko zespół pod kierunkiem Ziemby (2018), z tym że kwestionariusz ankiety był skierowany zarówno do urzędów jednostek samorządu terytorialnego różnych szczebli, jak i do ministerstw i innych jednostek administracji państwowej[1].

Polscy autorzy podkreślają przede wszystkim korzyści, jakie niesie ze sobą informatyzacja i cyfryzacja gospodarki, podczas gdy w literaturze światowej zwraca się już uwagę na trudności z zastosowaniem nowych technologii i konieczność niwelowania negatywnych konsekwencji społecznych (np. pogłębienie nierówności) wynikających z zachodzących przemian. Na przykład zdaniem Ndou (2004) wiele prób innowacyjnego świadczenia usług kończy się niepowodzeniem z powodu słabego zrozumienia przez społeczeństwo, pracowników samorządowych i decydentów koncepcji, procesów i funkcji e-administracji. Jednym z czynników osłabiających zainteresowanie nowymi technologiami jest ograniczoność dochodów jednostek samorządowych (Perdał, 2014). Moon (2002), badając rozwój e-administracji w USA, pyta, czy ona rzeczywiście istnieje, czy też pozostaje w fazie deklaracji lub na początkowym etapie rozwoju. Postawienie takiego pytania polskim jednostkom samorządowym umożliwi wskazanie, czy podejście do gospodarki 4.0 różni się w zależności od tego, czy mamy do czynienia z państwami Europy Zachodniej czy Środkowo-Wschodniej, co sugeruje Ojo (2019).

Z przytoczonych wyżej względów autorki podjęły w monografii temat transformacji cyfrowej samorządu gminnego w Polsce. Tematyka ta jest ważna i aktualna, a jej znaczenie wzrosło w ostatnich latach, kiedy jednostki samorządowe zmuszone były, tak jak inne podmioty życia społeczno-gospodarczego, do funkcjonowania w warunkach pandemii COVID-19, która przyspieszyła procesy cyfryzacji różnych sfer ich działalności (Kańduła i Przybylska, 2022a). Rozważania zawarte w tej monografii są prowadzone z perspektywy samorządu gminnego – najniższego szczebla samorządu terytorialnego w Polsce. Wynika to z tego, że na organach samorządu tego szczebla spoczywa najwięcej zadań polegających na zaspokajaniu codziennych potrzeb obywateli o charakterze zbiorowym. Część zagadnień poruszonych w monografii ma charakter uniwersalny, tzn. można je odnieść też do powiatów i województw. W szczególności dotyczy to: możliwości wykorzystywania technologii informacyjno-komunikacyjnych do wspierania zrównoważonego rozwoju, źródeł finansowania transformacji cyfrowej samorządu

[1] Już po skierowaniu monografii do recenzji ukazały się raporty przygotowane przez zespół Obserwatorium Polityki Miejskiej Instytutu Rozwoju Miast i Regionów na temat zarządzania miastem z wykorzystaniem danych (Łachowski i in., 2022) oraz cyfryzacji urzędów miast (Miazga i in., 2022). Pierwszy raport był pokłosiem badań ankietowych przeprowadzonych od sierpnia do grudnia 2021 r. (poprzedzonych pilotażem), na populacji miast powyżej 5000 mieszkańców, a drugi – badań trwających od lipca do grudnia 2022 r. wśród tej samej kategorii miast.

terytorialnego, cyberbezpieczeństwa jako elementów kontroli zarządczej oraz cyberataków w działalności samorządu terytorialnego.

Celem monografii jest diagnoza dotycząca wykorzystywania przez gminy nowych technologii informacyjno-komunikacyjnych. Postawiono w niej tezę, że stopień zaawansowania gmin (mierzony liczbą wykorzystywanych nowych rozwiązań technologicznych) jest uzależniony od typu administracyjnego gminy oraz jej położenia.

Monografię podzielono na siedem rozdziałów. W pierwszym scharakteryzowano przejawy gospodarki 4.0, zwracając uwagę na technologie informacyjno-komunikacyjne konstytuujące tę gospodarkę, które mogą być wykorzystane w gminach. W tym rozdziale zdefiniowano pojęcie transformacji cyfrowej samorządu gminnego oraz podano przykłady wykorzystywania ICT w procesie zarządzania współczesnymi gminami, które chcą się rozwijać w duchu koncepcji *smart city* i *smart village*. Ze względu na mnogość dostępnych technologii, zróżnicowanie rozwiązań oferowanych przez dostawców oraz odwoływanie się do tych technologii w trakcie dyskusji wyników badań ankietowych w ostatnim rozdziale zrezygnowano z wyodrębniania punktu, w którym szczegółowo scharakteryzowano by te technologie. W rozdziale określono też uwarunkowania i bariery transformacji cyfrowej gmin.

Do uwarunkowań transformacji cyfrowej zaliczono m.in. dostęp do infrastruktury cyfrowej oraz umiejętność korzystania z niej, ale Polska ma w tej sferze duże braki (Miazga i in., 2022), można wręcz mówić o nierównościach cyfrowych na kilku poziomach. Nierówności te są przedmiotem rozważań w rozdziale drugim. Dyskutowane są w nim przyczyny, konsekwencje i ewolucja nierówności cyfrowych. Istnienie tych nierówności oddala Polskę od osiągnięcia celów zrównoważonego rozwoju, a przecież jednym z nich jest zmniejszenie nierówności w obrębie państwa i między państwami. Ambicją poszczególnych państw jest też uczynienie miast i osiedli ludzkich obszarami bezpiecznymi, stabilnymi, zrównoważonymi oraz sprzyjającymi włączeniu społecznemu. Uważamy, że w gospodarce 4.0 dostępne są narzędzia, które można wykorzystać do osiągnięcia celów tego rozwoju, w konsekwencji gminy wchodzą na ścieżkę transformacji cyfrowej, aby rozwijać się w sposób zrównoważony. W rozdziale trzecim scharakteryzowano więc cele zrównoważonego rozwoju, wyodrębniono nowy filar tego rozwoju i zasygnalizowano rolę gmin w tym rozwoju. Zwrócono też uwagę m.in. na rodzaje innowacji, ponieważ działania podejmowane w duchu *smart city* i *smart village* są innowacjami społecznymi, a transformacja cyfrowa samorządu gminnego, w tym urzędu gminy, może być traktowana jako innowacja organizacyjna.

W rozdziale pierwszym wskazano, że barierą transformacji cyfrowej jest brak środków finansowych. W czwartym rozdziale zaprezentowano więc źródła finansowania transformacji cyfrowej gmin. Podjęcie tego zagadnienia jest

konsekwencją studiów literatury, z której wynika, że bariera finansowa jest najważniejszą przeszkodą we wprowadzaniu nowych ICT (Norris i in., 2021). Taka konstatacja wypływa też z naszych wcześniejszych badań na temat cyberbezpieczeństwa w urzędach gmin (Chodakowska i in., 2022b). Pisanie o tych źródłach jest – z kilku powodów – zadaniem dość trudnym. Po pierwsze, źródeł tych jest dużo. Po drugie, brakuje czytelnej systematyki tych źródeł. W dokumentach Komisji Europejskiej, a w ślad za tym w regulacjach krajowych, pisząc o rozpatrywanych źródłach, używa się – niekiedy przypadkowo – określeń: fundusze, programy, instrumenty, inicjatywy, narzędzia. Po trzecie, według stanu na 31 grudnia 2022 r. nieznana jest ostateczna budowa programów operacyjnych, na podstawie których mogą być dzielone środki z funduszy Unii Europejskiej. Niemożliwe jest więc precyzyjne określenie, w której osi programu, w którym działaniu i poddziałaniu należy szukać środków. Po czwarte, szerokie opisywanie stanu z lat 2013–2020 miałoby jedynie walor historyczny, ponieważ – mimo że w 2022 r. jeszcze organizowano konkursy – wydatkowanie środków powinno nastąpić do czerwca 2023 r. Po piąte, instytucjami odpowiedzialnymi za wydatkowanie funduszy Unii Europejskiej zaplanowanych w programach operacyjnych są rozmaite podmioty (zagraniczne i krajowe różnych szczebli). Po szóste, według stanu na dzień 31 grudnia 2022 r. niejasne jest to, czy Polska otrzyma jakiekolwiek środki z budżetu UE, szczególnie z Funduszu Odbudowy UE, ze względu na nieporozumienia dotyczące spełniania bądź niespełniania przez Polskę warunków ich przyznania[2]. Mając to na uwadze, w rozdziale tym dokonano systematyki dostępnych źródeł finansowania transformacji cyfrowej oraz ogólnej charakterystyki funduszy zewnętrznych dostępnych w latach 2013–2021. Następnie przedstawiono cele, które Komisja Europejska chce osiągnąć, dystrybuując środki w latach 2022–2027. Scharakteryzowano też dwa nowe źródła (fundusze) oraz programy (inicjatywy) Komisji Europejskiej odnoszące się do transformacji cyfrowej. Wskazano też programy grantowe organizowane przez instytucje krajowe w latach 2020–2022.

Ważnym aspektem procesów transformacji cyfrowej są zagrożenia związane z przenoszeniem sfery realnej do świata cyfrowego. Za jedno z głównych zagrożeń autorki uważają cyberprzestępczość, która wymusza na jednostkach samorządu gminnego konieczność podejmowania działań w zakresie zapewnienia cyberbezpieczeństwa. W konsekwencji w rozdziale piątym pokazano cyberbezpieczeństwo jako element kontroli zarządczej w samorządzie gminnym, a w rozdziale szóstym scharakteryzowano rodzaje cyberataków na urzędy gmin. W tym miejscu odwołano się do niepublikowanych wyników badań przeprowadzonych przez autorki w 2020 r. W ostatnim rozdziale prezentowane są wyniki badań

[2] Chodzi o spełnianie warunków, w tym dotyczącego praworządności opisanych w specjalnym dokumencie (Rozporządzenie PEiR, 2020).

przeprowadzonych wśród gmin w styczniu 2022 r. na temat ich gotowości do funkcjonowania w gospodarce 4.0.

Monografię przygotowano na podstawie literatury przedmiotu, aktów prawnych i innych źródeł. Prezentowane są w niej także wyniki dwóch osobnych badań własnych. Oba badania ankietowe przeprowadzono metodą CAWI (*computer-assisted web interview*). Prośbę o wypełnienie elektronicznego arkusza ankiety wysłano do urzędów wszystkich gmin w Polsce na ich oficjalne skrzynki e-mailowe (do wiadomości dołączono aktywny link do ankiety). Badania zostały przeprowadzone w latach 2020–2022. Szczegółowe dane na temat respondentów zamieszczono w rozdziałach szóstym i siódmym.

Publikacja jest adresowana do wszystkich osób zainteresowanych problematyką samorządu gminnego. Treści w niej zawarte zainteresują zarówno pracowników naukowych zajmujących się tą tematyką, jak i tych odbiorców, którzy interesują się funkcjonowaniem samorządu gminnego we współczesnym, dynamicznie zmieniającym się świecie. Osadzenie problematyki działalności gmin w warunkach gospodarki 4.0 oraz przedstawienie założeń, warunków oraz ograniczeń i problemów związanych z wdrażaniem cyfrowych rozwiązań do działalności jednostek samorządowych sprawia, że prezentowane treści mają istotne znaczenie i charakteryzują się wysokim stopniem aktualności, szczególnie po pandemii COVID-19, która przyczyniła się do przyspieszania procesów cyfryzacji gospodarki. Z tego względu adresatami problematyki prezentowanej w monografii są również praktycy samorządowi, którzy już rozpoczęli lub w najbliższym czasie rozpoczną wdrażanie cyfrowych zmian w gminach, dostawcy usług cyfrowych dla jednostek samorządu terytorialnego oraz decydenci.

1

GMINY WOBEC WYZWAŃ GOSPODARKI 4.0

1.1. Zarys koncepcji gospodarki 4.0

Nie ma jednej, powszechnie akceptowanej definicji gospodarki 4.0. Najogólniej można stwierdzić, że jest to gospodarka, w której człowiek dysponuje dużą ilością danych (z internetu ludzi, internetu rzeczy, wirtualnej rzeczywistości) przesyłanych i przechowywanych za pośrednictwem nowych technologii i przetwarzanych za pomocą sztucznej inteligencji. Już w 1930 r. Keynes (2011) zauważył, że nowe technologie poprawiają wydajność i zmniejszają koszty produkcji towarów i usług w tempie wcześniej niespotykanym. Wiedza i innowacje zawsze odgrywały ważną rolę w rozwoju gospodarczym, ale na przełomie XX i XXI w. znaczenie tych czynników dla rozwoju zrównoważonego znacznie się zwiększyło. Peters i in. (2009) twierdzą, że w ciągu 20 lat ludzkość przeszła z gospodarki postindustrialnej do gospodarki informacyjnej, a następnie digitalnej i poprzez gospodarkę wiedzy do gospodarki kreatywnej, gospodarki cyfrowej czy gospodarki 4.0. Etapy rozwoju gospodarki zaprezentowano w tabeli 1.

Tabela 1. Etapy rozwoju gospodarki

Wyszczególnienie	**Etapy rozwoju gospodarki / transformacji gospodarki**			
Oznaczenie numeryczne	1.0	2.0	3.0	4.0
Nazwa gospodarki	techniczna	elektryczna	internetowa	cyfrowa
Główne cechy	– mechanizacja – energia parowa maszyny	– uprzemysłowienie – linie montażowe – produkcja masowa	– automatyzacja produkcji – komputery – elektronika	– systemy cybernetyczne – sieci – internet rzeczy – gigadane – technologia mgły i chmury – telefonia 5G
Umowna data rozpoczęcia	1784	1870	1969	1996

Źródło: opracowanie własne.

Pierwsza rewolucja przemysłowa polegała na przełomowym napędzaniu maszyn parą i wodą. Druga rewolucja była związana z szerokim zastosowaniem w przemyśle energii elektrycznej. Trzecia jest utożsamiana z automatyzacją procesów produkcyjnych, rozwojem środków telekomunikacji, elektroniki, systemów informatycznych i komputerów. Wyraźny rozwój technologii informacyjnych i telekomunikacyjnych jest z kolei utożsamiany z czwartą rewolucją przemysłową, do której wydaje się wprost odnosić pojęcie gospodarki cyfrowej i gospodarki 4.0.

Gospodarka 4.0 jest uogólnieniem koncepcji przemysłu 4.0. Terminu „przemysł 4.0" po raz pierwszy użyto w niemieckiej inicjatywie „Industrie 4.0", która w 2011 r. zgromadziła przedstawicieli świata biznesu, polityki i nauki. „Industrie 4.0" to nazwa nadana planowi zwiększenia konkurencyjności niemieckiej gospodarki. Plan został poparty przez rząd niemiecki, który umieścił go w programie rozwoju kraju, którego głównym celem jest osiągnięcie statusu światowego lidera w innowacyjnych technologiach (Kagermann, Lukas i Wahlster, 2011, cyt. za Bendkowski, 2017).

Zmiany technologiczne zachodzące we współczesnym świecie są nazywane czwartą rewolucją przemysłową. Jest to bezpośrednie nawiązanie do innych przełomowych zmian w życiu społeczno-gospodarczym ludzkości, takich jak: mechanizacja produkcji maszynami wodnymi i parowymi pod koniec XVIII w. (rewolucja 1.0), rozwój produkcji masowej dzięki maszynom napędzanym energią elektryczną i silnikami spalinowymi oraz podział pracy na przełomie XX i XXI w. (rewolucja 2.0) oraz wykorzystanie komputerów i kanałów komunikacji elektronicznej w niemal wszystkich dziedzinach życia społeczno-gospodarczego krajów (rewolucja 3.0, tzw. cyfryzacja gospodarki). Wszystko to jest tylko wstępem do zmian, które nas teraz czekają i które nazywamy czwartą rewolucją przemysłową lub nową gospodarką.

Dźwignią gospodarki 4.0 jest telefonia piątej generacji (5G)[3], która charakteryzuje się szybkością transmisji danych na poziomie minimum 1 Gb/s, opóźnieniem 1 ms oraz przepustowością powyżej 10 Gb/s (tabela 2).

Cechą gospodarki 4.0 jest gromadzenie i przetwarzanie masowych ilości danych, co jest określane mianem gromadzenia gigadanych (*big data*). Dane te mają być usługowo przetwarzane w chmurze obliczeniowej (*cloud computing*), przechowywane dzięki technologii łańcucha bloków (*blockchain*)[4] oraz analizowane z wykorzystaniem uczenia maszynowego (sztucznej inteligencji). W gospodarce 4.0 na szeroką skalę mają być też wykorzystane: mobilny internet, aplikacje w telefonach i smartwatchach, internet (wszech)rzeczy, druk 3D, roboty, drony, a w przyszłości komputery kwantowe.

[3] Trwają już prace nad technologią 6G.

[4] W praktyce częściej używa się nazwy angielskiej, dlatego w dalszej części książki posługujemy się określeniem *blockchain*.

Tabela 2. Charakterystyka telefonii 5G na tle technologii wcześniejszych generacji

Technologia	**GSM, CDMA, PDC, iDEN, wzmacniacz cyfrowy**	**CDMA 2000, UMTS, EDGE, HSPA**	**LTE, WiMAX, WiFi**	**Zunifikowany IP, integracja łączy szerokopasmowych LAN/WAN/PAN/WLAN, technologie oparte na modulacji OFDM**
Skrótowe oznaczenie	2G	3G	4G	5G
Czas powstania	1990	2004	2010	2018
Szybkość transmisji danych	50 Kb/s – 1 Mb/s	400 Kb/s – 4 Mb/s	2 Mb/s – 1 Gb/s	1 Gb/s i powyżej
Opóźnienie	629 ms	212 ms	98 ms	1 ms
Przepustowość	20 Kb/s – 40 Kb/s	1 Mb/s – 3 Mb/s	3 Mb/s – 5 Mb/s	powyżej 10 Mb/s

Źródło: opracowanie własne na podstawie (*Strategia*, 2020).

Koncepcja gospodarki 4.0 jest postrzegana jako źródło wielu możliwości, które mogą być impulsem rozwojowym dla polskiej gospodarki. Należą do nich (Dmowski i in., 2016):

– Lepsze zaspokojenie potrzeb konsumentów dzięki projektowaniu produktów na indywidualne zamówienia oraz produkcji małych partii produktów (masowa personalizacja).
– Wzrost produktywności – zastosowanie nowych technologii umożliwia optymalizację procesu produkcyjnego, skrócenie przestojów fabryk i urządzeń, lepszą alokację zasobów oraz tworzenie nowych produktów.
– Tworzenie nowych miejsc pracy o wysokiej wartości dodanej. Będą one skupione wokół automatyki i technologii informatycznych oraz nowych branż pokrewnych, takich jak współpraca robotów z ludźmi.
– Rozwój nowych branż, głównie dzięki dostawcom innowacyjnych rozwiązań teleinformatycznych oraz podmiotom, które mogą je zastosować w praktyce.
– Wzrost innowacyjności gospodarki, który umożliwi ekspansję technologii poza granice państwa.
– Wzrost atrakcyjności podmiotów gospodarczych i kraju w oczach inwestorów. To, co zwykle przyciąga inwestorów, to wysokie umiejętności potencjalnych pracowników oraz dynamicznie rozwijająca się innowacyjna gospodarka.
– Spadek kosztów produkcji wynikający z poprawy jakości produktów i zmniejszenia zapasów.

– Efektywne wykorzystanie materiałów i energii.
– Wzrost lojalności klientów, możliwy dzięki personalizacji oferty (duże dane mogą być wykorzystane do analizy behawioralnej klientów w punktach sprzedaży, np. na stacjach benzynowych).

Upowszechnienie się pojęcia gospodarki 4.0 wpłynęło na to, że również na poszczególne sfery gospodarki patrzy się przez pryzmat nowych technologii informacyjno-komunikacyjnych i poszukuje się możliwości zastosowania tych technologii w procesie produkcyjnym i usługowym. Coraz powszechniejsze są więc dyskusje np. o publicznym transporcie 4.0 (Tolkiehn i in., 2018), środowisku 4.0 (Colla i in., 2020), zdrowiu 4.0 (Ćwiklicki i in., 2021), samorządzie terytorialnym 4.0.

Dlaczego o gospodarce 4.0 należy mówić w kontekście samorządu terytorialnego, w tym gmin? Ewoluująca gospodarka i gwałtowny wzrost oczekiwań społeczeństw w związku z analizowanymi przemianami technologicznymi potęgują potrzebę uwzględnienia roli sektora finansów publicznych w adaptacji do zmieniającego się otoczenia. Jednostki samorządu terytorialnego, w tym gminy, razem z sektorem prywatnym dostarczają obywatelom różnych dóbr i usług. Rozwój technologii informacyjno-komunikacyjnych umożliwia świadczenie wielu usług administracyjnych w formie elektronicznej oraz zastosowania nowych rozwiązań w świadczeniu usług z zakresu oświaty, ochrony zdrowia, pomocy społecznej, kultury, transportu, gospodarowania odpadami, zagospodarowania przestrzennego itp. Skala udziału sektora finansów publicznych w zaspokajaniu potrzeb społecznych może budzić wątpliwości, choć mikroekonomiczne analizy efektywnego dostarczania dóbr wyjaśniają, dlaczego te, których konsumpcja nie jest konkurencyjna i jest niewykluczalna, powinny być produkowane publicznie (Rosen i Gayer, 2014). Do osiągnięcia konsensusu co do zakresu sektora finansów publicznych w gospodarce nadal jest potrzebne dokładne zbadanie i ustalenie, które szczeble władzy powinny odpowiadać za konkretne zadania. W tym miejscu pojawia się federalizm fiskalny, który – w swojej tradycyjnej odsłonie – bada funkcje różnych szczebli władzy i ich wzajemne oddziaływanie.

W swoim przełomowym artykule Tiebout (1956) rozpoczął szeroką dyskusję na temat zdecentralizowanej struktury rządu i wzrostu efektywności wynikającego z lokalnego dostarczania dóbr publicznych. Przeniesienie zadań publicznych na niższe szczeble władzy miało stworzyć quasi-rynkowy mechanizm, który mógłby wyeliminować problem nieefektywności alokacji i gapowicza. Ze względu na większą jednorodność preferencji społeczności lokalnych niż ogólnokrajowych istnieje prawdopodobieństwo skuteczniejszego zapewnienia im jednolitego poziomu (lokalnego) dobra publicznego. Musiał jednak zostać spełniony szereg warunków, aby proces ten zakończył się pełnym sukcesem. W świecie rzeczywistym czysto zdecentralizowany system nie jest pożądany, ponieważ nie

może maksymalizować dobrobytu społecznego ze względu na wady wynikające z kwestii równości (polityka redystrybucji) i wydajności (pozytywne i negatywne efekty zewnętrzne oraz ekonomia skali) (Rosen i Gayer, 2014). Badania i dyskusja na temat znaczenia decentralizacji doprowadziły do powstania dwóch generacji teorii federalizmu fiskalnego, które pomogły w osiągnięciu ogólnego porozumienia (Poniatowicz, 2018). W teorii federalizmu fiskalnego postuluje się, aby dobra i usługi publiczne były zapewniane przez najniższy szczebel władzy, który jest w stanie osiągnąć wyznaczone cele, ponieważ ten szczebel jest bardziej zorientowany na obywatela niż wyższy. Jednak dobra, których skutki uboczne wpływają na społeczeństwo całego kraju, powinny być produkowane na poziomie krajowym (Ostrom i in., 1961). W przypadku dóbr i usług, z którymi wiążą się efekty zewnętrzne, ale niemających zasięgu krajowego, zapewnienie to powinno być realizowane na poziomie regionalnym lub lokalnym (w celu internalizacji efektów zewnętrznych). Jednak dochody pochodzące z podatków lokalnych są zwykle niewystarczające do pokrycia wszystkich wydatków związanych z tymi zadaniami, a niższe szczeble samorządu terytorialnego są wspierane dotacjami z budżetu państwa (warunkowymi lub bezwarunkowymi) i budżetów innych jednostek samorządu terytorialnego (Oates, 1999; Rosen i Gayer, 2014).

Decentralizacja sprzyja eksperymentowaniu i wprowadzaniu innowacji dotyczących dostarczania dóbr i usług publicznych. Założenie o powodzeniu każdej decyzji podejmowanej przez sektor finansów publicznych jest raczej nieosiągalne, a błędne decyzje mogą powodować straty społeczne, moralne lub ekonomiczne, które uniemożliwiają maksymalizację dobrobytu społeczeństwa. Zanim nowe rozwiązanie zostanie wdrożone na poziomie całego państwa, można je przetestować na jednej jednostce samorządu terytorialnego niczym w laboratorium, by sprawdzić, czy płynące z niego korzyści krańcowe przewyższają koszty krańcowe. Jeśli tak, to rozwiązanie może zostać skopiowane i zastosowane w innych samorządach lub nawet na szczeblu centralnym, w zależności od specyfiki. Jeśli nie, to szkody wynikające ze złej decyzji ograniczają się tylko do tej jednostki samorządu, w którym została wdrożona. Niektóre dobra i usługi publiczne, które są dziś uważane za oczywiste, w rzeczywistości rozpoczęły się jako eksperymenty w zdecentralizowanych rządach. Na przykład system ubezpieczeń społecznych zaprojektowany w USA w okresie Wielkiego Kryzysu wynikał z wcześniejszych doświadczeń kilku stanów, które wdrożyły takie programy (Rosen i Gayer, 2014). W prężnie rozwijających się gospodarkach i w obliczu rozwoju technologicznego rozwiązanie, które na razie jest uznawane za innowacyjne, może w końcu stać się oczywiste i niezbędne dla wzrostu dobrobytu społeczeństwa.

To krótkie omówienie teorii federalizmu fiskalnego daje przegląd ról różnych szczebli władzy w dążeniu do maksymalizacji dobrobytu społecznego i podkreśla jego potencjał przy wdrażaniu innowacyjnych rozwiązań. W Polsce samorząd terytorialny od ponad 30 lat odgrywa ważną rolę w wykonywaniu zadań publicz-

nych. Technologie informacyjno-komunikacyjne wywołują zasadnicze zmiany w sposobie działania różnych podmiotów: producentów, usługodawców, klientów, całej gospodarki, a więc także jednostek samorządu terytorialnego, w tym gmin. Choć jednostki te mogą się wydawać organizacjami mniej skłonnymi – w porównaniu do szczebla centralnego – do wdrażania innowacyjnych rozwiązań i przeznaczania na nie dużej części swoich dochodów (Centrum, 2015), muszą dostosować się i współpracować w celu stworzenia wspólnej sieci i świadczenia nowoczesnych usług publicznych. Muszą też wejść na ścieżkę transformacji cyfrowej. Dalsze rozważania będziemy prowadzić w kontekście samorządu gminnego, ponieważ na gminach ciąży najwięcej zadań z zakresu bezpośredniego zaspokajania potrzeb publicznych. Rozważania te są jednak istotne także w odniesieniu do powiatów i województw (z uwzględnieniem specyfiki ich zadań).

1.2. Pojęcie transformacji cyfrowej samorządu gminnego[5]

Nie ma jednej, powszechnie akceptowalnej definicji transformacji cyfrowej. Wynika to z tego, że każdy podmiot ma inne oczekiwania i znajduje się na innym etapie „nasycenia" swej działalności technologiami. Prawdopodobnie pierwszy raz pojęcia cyfryzacji w znaczeniu zmian w otoczeniu będących następstwem coraz bardziej powszechnego stosowania nowych technologii użył Wachal, który blisko 50 lat temu pisał o cyfryzacji społeczeństwa *(digitalisation of society*) (Brennen i Kreiss, 2016).

Pisząc o technologiach informacyjno-komunikacyjnych w kontekście samorządu gminnego, używa się różnych określeń, w tym: informatyzacja, cyfryzacja i transformacja cyfrowa. Określenia te różnią się, choć często są utożsamiane. Są one częściowo zbieżne z czterema etapami rewolucji cyfrowej administracji publicznej wyróżnionymi przez Janowskiego (2015). Autor ten wyodrębnił następujące fazy tej rewolucji: cyfryzację (wprowadzenie pierwszych rozwiązań ICT w jednostkach administracji), transformację (e-government, czyli wdrożenie rozwiązań ICT mających wpływ na zmiany organizacyjne i umiejętności pracowników), zaangażowanie (zastosowanie rozwiązań ICT, które wpływają na relacje wewnątrz organizacji oraz na stosunki z podmiotami zewnętrznymi) oraz kontekstualizację (wpływ wdrożonych rozwiązań ICT na sektory gospodarki i ludzi).

Informatyzacja to proces wyposażania administracji publicznej w komputery i systemy teleinformatyczne, a następnie proces przechodzenia z rejestrów papierowych na informatyczne oraz wykorzystywanie baz danych. Stanowi się o tym np. w Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności pod-

[5] Na podstawie (Kaczyńska i in., 2021).

miotów realizujących zadania publiczne. Efektem informatyzacji jest zmiana procesów z papierowych na elektroniczne, z tym, że jest ona często dokonywana powierzchownie, tzn. dokument można pobrać, a nawet wypełnić elektronicznie, ale trzeba go wydrukować i dostarczyć do urzędu. Taka powierzchowna informatyzacja oznacza tylko częściową zmianę formy procesu świadczenia usługi (Szczepaniak, 2021). Określenia cyfryzacja administracji (publicznej, w tym samorządowej) używa się do opisania procesu cyfryzacji usług publicznych, czyli całościowego świadczenia ich przez internet za pomocą różnych ICT. Usługi elektroniczne (e-usługi) powinny być coraz powszechniejsze i coraz bardziej zaawansowane, co oznacza np. ich udostępnianie nie tylko za pośrednictwem internetu stacjonarnego, ale również mobilnego. Usługi te powinny być też zintegrowane, z możliwością automatycznego pobierania (zaciągnięcia) danych dotyczących użytkownika lub sprawy będących już w posiadaniu urzędu[6] oraz dostępne w jednym miejscu w internecie i łatwe do wyszukania z poziomu głównej strony internetowej urzędu (Miazga i in., 2022). Tak rozumiana cyfryzacja „zakłada poprawę efektywności procesów, wprowadzanie automatyzacji tam, gdzie to możliwe" (Szczepaniak, 2021, s. 34).

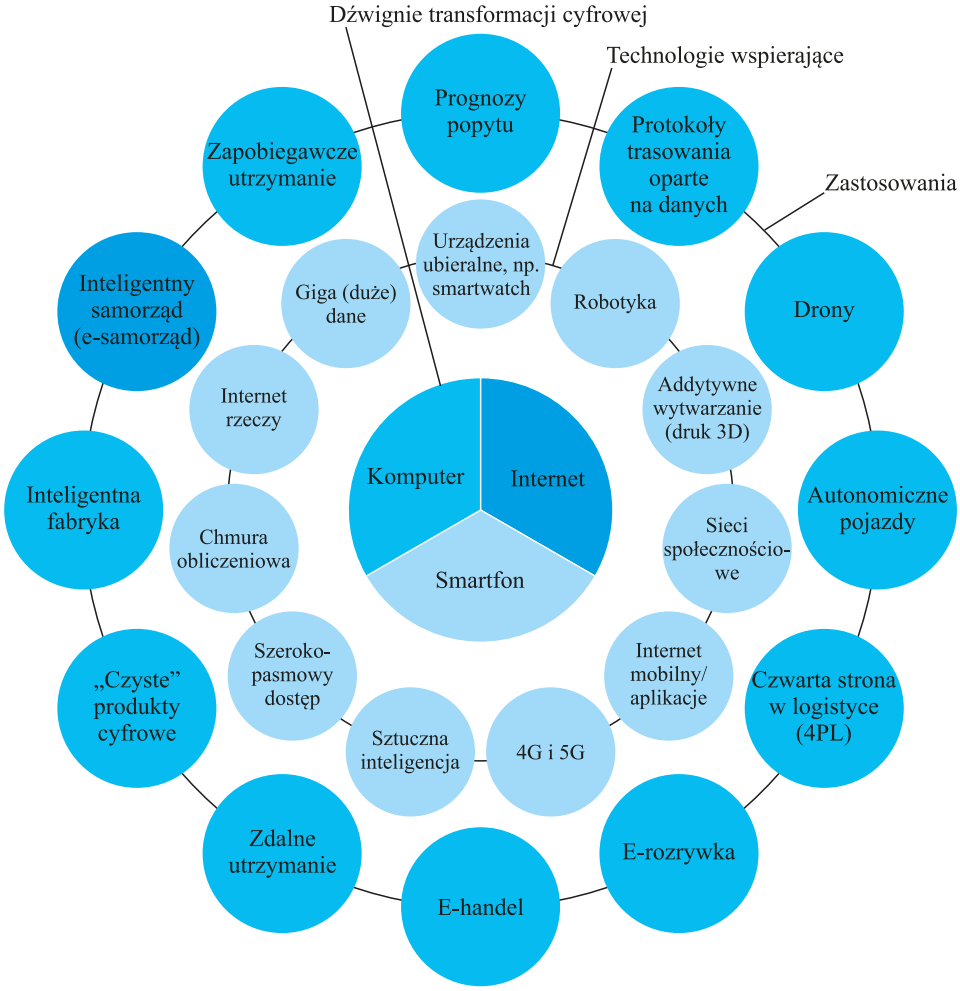
Najogólniej transformacją cyfrową samorządu gminnego można nazwać adaptację nowoczesnych technologii przez ten samorząd. Może ona się odnosić zarówno do stanu pożądanego (np. odpowiedniego nasycenia urzędu lub procesu świadczenia usług tymi technologiami), jak i do konkretnych działań podejmowanych od lat, aby stan ten został osiągnięty (Chaba, 2021). Można ją też zdefiniować jako zmianę, która powoduje, że technologia cyfrowa przenika wszystkie aspekty ludzkiego życia (Stolterman i Fors, 2004) bądź urzędu gminy czy wspólnoty lokalnej, lub jako proces zmian, których celem jest osiągnięcie pożądanego stopnia zaawansowania technologicznego albo bardziej ogólnie – jako trendy i skutki coraz bardziej intensywnego korzystania z ICT (Dufva i Dufva, 2019).

W literaturze spotyka się też szczegółowsze definicje, w których zwraca się uwagę na zmiany, jakie wywołuje tytułowa transformacja. Dla Liu i in. (2011) transformacją cyfrową jest taka przemiana organizacji, której efektem jest integracja technologii cyfrowych i procesów biznesowych. Jej efektem jest powstanie nowego modelu funkcjonowania danej jednostki, którego rdzeniem są ICT. W innej definicji zwraca się uwagę na to, że transformacja ta oznacza wykorzystanie technologii cyfrowych we wszystkich płaszczyznach działalności organizacji w celu istotnej poprawy wydajności lub zasięgu działania organizacji (*Digital transformation*, 2011). Transformacja ta oznacza też zmianę kultury danej organizacji, ponieważ wymaga od niej ciągłego kwestionowania *status quo*,

[6] Cellary (2022a, s. 42) wielokrotnie podkreślał, że nie powinno być tak, „aby od interesanta, który przedłożył dokumenty w jednym urzędzie, żądało się tych samych dokumentów w drugim, bo jeden urzędnik nie wie, czym dysponuje drugi urzędnik tego samego państwa, a często nawet tego samego urzędu, tylko innego wydziału".

eksperymentowania i radzenia sobie z porażką. Może się z nią wiązać zmiana dotychczasowej filozofii działania na rzecz stosunkowo nowych sposobów zarządzania, produkowania, świadczenia usług, komunikacji z odbiorcami (*Transformacja…*, 2022).

Transformacja cyfrowa nie jest nową technologią samą w sobie. Nie można by o niej jednak mówić, gdyby nie wymyślono technologii, produktów i usług, które umożliwiają dokonywanie innowacyjnych zmian w organizacjach (rysunek 1). Punktem wyjścia jest istnienie tzw. technologii ogólnego przeznaczenia: komputera, internetu i smartfona (Śledziewska i Włoch, 2020). Urządzenia



Rysunek 1. Podstawy transformacji cyfrowej, technologie wspierające i ich wybrane zastosowania

Źródło: (Kaczyńska i in., 2021).

te są wszechobecne w prawie wszystkich sektorach gospodarki i w życiu coraz większej liczby ludzi. Są one podstawą do rozwoju nowych urządzeń i innowacji, do których należy zaliczyć m.in.: sztuczną inteligencję, robotyzację, internet rzeczy, technologię chmury i mgły obliczeniowej, *blockchain*, a w przyszłości też komputery kwantowe. Ich istnienie jest impulsem do przejścia z gospodarki „starej" do gospodarki cyfrowej (*digital economy*), nazywanej też gospodarką elektroniczną (*e-economy*) i gospodarką sieciową (*network economy*) lub gospodarką cyfrową, a ostatnio gospodarką 4.0. Nie można jednak zapomnieć, że katalizatorem tej transformacji jest także popularyzacja mediów społecznościowych (Janicki i Goździewska-Nowicka, 2018). Gospodarka 4.0 nie jest prostą kontynuacją takiej cyfryzacji gospodarki, z jaką mieliśmy do czynienia w XX w. (Cellary, 2019a). W nowoczesnej, cyfrowej gospodarce funkcjonują jednostki, przedsiębiorstwa, władze państwowe i samorządowe.

Transformację cyfrową państwa można rozumieć jako przemianę sposobu działania organizacji publicznych wyrażającą się w głębokiej integracji technologii cyfrowych i procesów biznesowych tych jednostek, co prowadzi do wypracowania nowego modelu funkcjonowania państwa, którego rdzeniem są/będą zintegrowane systemy informatyczne. Docelowym efektem tej transformacji będzie „cyfrowe państwo" (*digital state*) (Sobczak, 2012, s. 265). W konsekwencji transformację cyfrową jednostki samorządu gminnego należy utożsamiać z całością zmian zachodzących w gminie, dotyczących usług, procesów, zasobów, kultury organizacyjnej samorządu oraz kompetencji, dokonywanych w celu (*Polityka…*, 2020):

– podnoszenia jakości usług publicznych,
– usprawnienia pracy urzędu (w wąskim znaczeniu) oraz urzędu i gminnych jednostek organizacyjnych (w szerszym znaczeniu),
– wsparcia procesów podejmowania decyzji strategicznych i operacyjnych,
– zwiększenia przejrzystości działania samorządu gminnego,
– angażowania mieszkańców w życie wspólnoty samorządowej.

Przemiany te są dokonywane za pomocą technologii informacyjno-komunikacyjnych z zamiarem osiągnięcia celów zrównoważonego rozwoju na szczeblu lokalnym. Transformacja cyfrowa samorządu gminnego powinna być wyrazem myślenia procesowego nastawionego na integrację wszystkich elementów tego samorządu: wydziałów urzędu, jednostek organizacyjnych, ludzi, rejestrów, zasobów informacyjnych oraz zawartych w nich danych (Szczepaniak, 2021). Transformacja cyfrowa tego samorządu jest więc wieloaspektowym procesem (w konsekwencji też długim), wymagającym koordynacji działań podejmowanych na różnych szczeblach administracji publicznej, w różnych wydziałach urzędu, w placówkach usługowych oraz koordynacji przyjmowanych rozwiązań. Wymaga ona również upowszechniania nowych technologii, podnoszenia kompetencji cyfrowych wszystkich stron procesu usługowego oraz zmian prawnych i orga-

nizacyjnych (Cellary, 2022a). Za Łukaszuk (2022, s. 309) kompetencje cyfrowe definiujemy jako szeroki pakiet umiejętności polegających nie tylko na znajomości obsługi komputera, urządzeń mobilnych i konkretnych programów oraz aplikacji, ale także jako umiejętności „weryfikacji oraz selekcji danych, uczenia się, świadomości i zagrożeń świata cyfrowego".

Transformacja cyfrowa jest sposobem dojścia do *e-government* i *e-governance* (Ganczar i Sytek, 2021), czyli – najogólniej – takich modeli funkcjonowania administracji publicznej, która jest przejrzysta dla obywateli (podmiotów gospodarczych i innych interesariuszy) (Matheus i in., 2021), otwarta na współpracę z nimi, gotowa do włączania ich w proces podejmowania decyzji i przyjazna.

Istotą transformacji cyfrowej jest doprowadzenie do tego, aby urząd gminy (w wąskim rozumieniu) oraz urząd i gminne placówki usługowe[7] (w szerszym ujęciu) były przyjazne dla obywateli, a określone technologie wspomagały świadczenie lokalnych usług publicznych. Przyjazny urząd należy tu rozumieć jako instytucję, w której obywatele i przedsiębiorcy mogą jak najwięcej spraw – z dowolnego miejsca, o dowolnym czasie – załatwić sami, bez udziału lub z minimalnym udziałem urzędnika. Analogicznie można zdefiniować przyjazną placówkę usługową.

Aby można było mówić o wejściu danej gminy na ścieżkę transformacji cyfrowej, muszą być spełnione przynajmniej następujące warunki podstawowe (Szczepaniak, 2021):

– elektroniczny obieg dokumentów jest podstawową formą ich procedowania,
– zostanie zinwentaryzowana infrastruktura w urzędzie, spisane zostaną wszystkie urządzenia będące w posiadaniu pracowników oraz ich stan,
– zostaną opisane wszystkie papierowe zasoby informacji (różnorodne rejestry publiczne), którym następnie zostanie nadana postać elektroniczna,
– nastąpi przegląd funkcjonalności istniejących elektronicznych rejestrów publicznych, np. spisów mieszkańców,
– właściwi pracownicy zostaną wyposażeniu w podpisy elektroniczne,
– będą przeprowadzone szkolenia pogłębiające kompetencje cyfrowe różnych grup pracowników,
– zostanie przyjęty system pracy na dokumentach współdzielonych w chmurze lub w systemie elektronicznego zarządzania dokumentacją,
– zostanie uzgodnione jednolite podejście do usług elektronicznych.

W cyfryzacji i transformacji cyfrowej samorządu gminnego upatruje się wielu korzyści. Przewiduje się, że (docelowo) wyeliminuje się dokumenty w wersji papierowej, a tym samym ograniczy się zbędne czynności: powielania, drukowania na każdym etapie, przesyłania tradycyjną pocztą, ręcznego rejestrowania,

[7] Mamy tu na myśli zarówno jednostki organizacyjne gminy, jak i spółki gminne.

archiwizowania i wyszukiwania dokumentów (Cellary, 2022a). Tym samym zmniejszy się presję na gospodarcze wykorzystywanie środowiska naturalnego (ograniczy się korzystanie z papieru) i obniży koszty. Eliminacja doprowadzi do poprawy efektywności i jakości funkcjonowania państwa, a w konsekwencji gospodarki i jakości życia obywateli. Przewiduje się, że elektroniczne załatwianie wielu spraw uprości pracę urzędników i poprawi jakość obsługi obywateli i innych interesariuszy. Elektroniczne świadczenie usług ułatwi też pozyskiwanie informacji zwrotnej o ich jakości (Guz, 2022). Wszystko to wpłynie na wzrost efektywności świadczenia lokalnych usług publicznych. Transformacja cyfrowa samorządu gminnego będzie też impulsem do uczenia się (podnoszenia kompetencji cyfrowych) samej organizacji, pracowników, obywateli i przedsiębiorców (Guz, 2022). W dalszej części pracy określenia cyfryzacja i transformacja cyfrowa będą używane zamiennie.

1.3. Polskie gminy w drodze do gospodarki 4.0[8]

W ostatnich latach o gminach (w szczególności miastach) przyszłości mówi się w kategorii „smart". Pojęcie *smart city* po raz pierwszy w literaturze pojawiło się stosunkowo niedawno, w 1992 r., jednak wówczas nie podjęto próby jego zdefiniowania. Autorzy Gibson, Kozmetzky i Smilor użyli go wtedy w kontekście inteligentnych budynków i biur (Korenik, 2019). Ich podejście było relatywnie wąskie, biorąc pod uwagę znaczenie tego terminu dzisiaj. W polskiej literaturze termin *smart city* używa się zamiennie z jego polskim odpowiednikiem, czyli inteligentne miasto. Ustalenie jego jednoznacznej, precyzyjnej definicji jest niełatwe ze względu na fakt, że jest to stosunkowo nowa idea. Przegląd wybranych definicji *smart city* sformułowanych przez badaczy przedmiotu, organizacje międzynarodowe oraz organy rządowe niektórych państw przedstawia tabela 3.

Z dokonanego przeglądu wynika, że *smart city* jest przedmiotem zainteresowania zarówno naukowców z licznych dziedzin nauki: między innymi ekonomii, urbanistyki, ekologii i socjologii, ważnych organizacji międzynarodowych, jak i podmiotów sektora publicznego i prywatnego. Niezależnie jednak od różnic interesów tych podmiotów definicje te mają wspólną cechę – charakteryzują *smart city* jako miasto społeczeństwa charakteryzującego się kreatywnym myśleniem, które w swoich codziennych działaniach umiejętnie wykorzystuje techniczne oraz technologiczne innowacje, bazując przede wszystkim na technologiach informacyjno-komunikacyjnych. Przy pomocy tych technologii miasta ze

[8] Na podstawie (Koszeluk, 2021).

Tabela 3. Przegląd definicji *smart city*

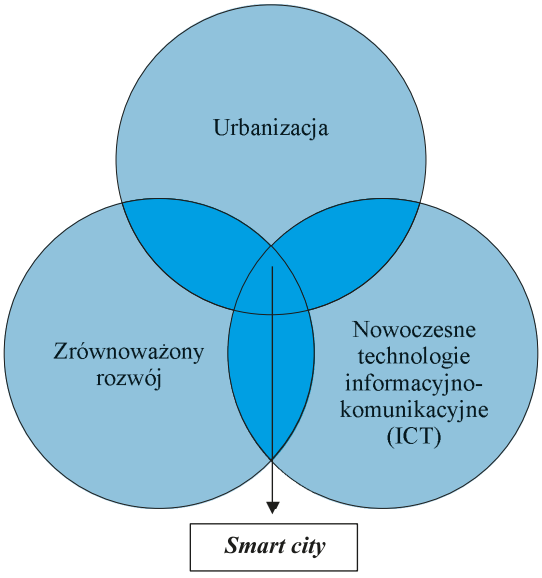
Źródło	Definicja
Definicje formułowane w literaturze	
Caragliu i in. (2011)	Miasto inwestujące w kapitał ludzki i społeczny oraz tradycyjną i nowoczesną infrastrukturę komunikacyjną (odpowiednio: transport i ICT[a]) w celu napędzania zrównoważonego rozwoju gospodarczego oraz podniesienia jakości życia, jednocześnie mądrze gospodarujące zasobami naturalnymi poprzez zarządzanie partycypacyjne
Batty (2012)	Miasto, w którym ICT jest połączone z tradycyjną infrastrukturą, skoordynowane i zintegrowane przy użyciu nowoczesnych technologii cyfrowych
Piro i in. (2013)	Środowisko miejskie, które – wspierane przez powszechne systemy ICT – jest w stanie zagwarantować swoim mieszkańcom zaawansowanie i innowacyjne usługi w celu poprawy jakości ich życia
Definicje organizacji międzynarodowych	
KE (b.d.)	*Smart city* jest miejscem, gdzie tradycyjne sieci oraz usługi stają się bardziej wydajne dzięki wykorzystaniu cyfrowych oraz telekomunikacyjnych technologii, przynosząc korzyści swoim mieszkańcom oraz biznesom
ONZ (2016)	*Smart city* wykorzystuje możliwości, jakie niesie ze sobą cyfryzacja, czysta energia oraz technologie, jak również innowacyjne technologie transportowe, tym samym dostarczając mieszkańcom przyjazne środowisku rozwiązania oraz stymulując proces zrównoważonego rozwoju poprzez polepszenie świadczonych przez nie usług
OECD (2019)	*Smart city* to całość inicjatyw oraz metod, które efektywnie wykorzystują cyfryzację w celu podniesienia dobrobytu mieszkańców oraz kreowania wydajniejszych, zrównoważonych oraz inkluzywnych usług i środowisk miejskich jako części kolektywnego procesu, angażującego licznych interesariuszy
Definicje organów rządowych wybranych państw	
Hiszpania (OECD, 2019)	Koncepcja *smart city* jest holistyczną ideą miast, które wykorzystują ICT, aby podnieść jakość życia mieszkańców oraz dostępność; zapewnia konsekwentne postępujący rozwój ekonomiczny, socjalny oraz środowiskowy. Umożliwia przekrojowe interakcje między mieszkańcami i miastami oraz dostosowuje się do ich potrzeb w czasie rzeczywistym, ekonomicznie oraz wydajnie jakościowo, zapewniając otwartość danych, a także rozwiązania i usługi ukierunkowane na mieszkańców
Wielka Brytania (OECD, 2019)	Koncepcja *smart city* nie jest statyczna i nie posiada wyczerpującej definicji. Jest procesem, szeregiem etapów, w którym miasto staje się coraz bardziej przyjazne do życia i elastyczne, tym samym reagujące szybciej na nowe wyzwania
Definicje podmiotów sektora prywatnego	
Smart Cities Council (2012)	*Smart city* gromadzi dane z urządzeń oraz sensorów wbudowanych w jezdnie, sieci energetyczne, budynki oraz inne elementy infrastruktury. Udostępnia te dane za pomocą inteligentnych systemów komunikacyjnych, zarówno przewodowych, jak i bezprzewodowych. Następnie wykorzystuje inteligentne oprogramowania do przetworzenia danych na wartościowe informacje oraz do tworzenia ulepszonych usług elektronicznych

cd. tabeli 3

Źródło	Definicja
International Business Machines Corporation (OECD, 2019)	Miasto, które optymalnie wykorzystuje wszystkie obecnie dostępne, wzajemnie ze sobą połączone informacje w celu lepszego zrozumienia oraz kontrolowania swoich działań, a także optymalizuje zużycie ograniczonych zasobów
CISCO (Falcober i Mitchell, 2012)	*Smart city* wdraża skalowalne rozwiązania, które wykorzystują ICT w celu podniesienia efektywności, redukcji kosztów oraz podniesienia jakości życia

[a] ICT – technologie informacyjno-komunikacyjne (*information and communication technologies*).

Źródło: opracowanie własne na podstawie (Caragliu i in., 2011; Estevez i in., 2016; OECD, 2019; Piro i in., 2013).



Rysunek 2. Idea *smart city*

Źródło: opracowanie własne na podstawie (Estevez i in., 2016).

zwiększoną efektywnością wykorzystują dostępne im zasoby w celu podniesienia jakości życia mieszkańców miasta i zagwarantowania jego zrównoważonego rozwoju (rysunek 2).

Smart city cechuje „dalekowzroczność". Miasto smart jest miastem przyszłości, które dobrze funkcjonuje w sferach gospodarki, kapitału ludzkiego, mobilności, środowiska i warunków życia oraz lokalnego zarządzania, zbudowanych na aktywnym działaniu i udziale świadomych, niezależnych, decydujących o sobie obywateli. Wykorzystuje możliwości płynące z cyfryzacji, czystej energii

i nowoczesnych technologii, zapewniając w ten sposób mieszkańcom wysoce efektywne rozwiązania, które są jednocześnie bardziej przyjazne środowisku (OECD, 2019).

Aby miasto było smart, musi wykorzystywać nowoczesne technologie informacyjno-komunikacyjne. Według UNESCO (2009) pod pojęciem tym należy rozumieć zbiór różnych narzędzi technologicznych oraz środków używanych do transmisji, przechowywania, przetwarzania i udostępniania oraz wymiany informacji. Zaliczane są do nich m.in. komputery, serwery oraz klastry obliczeniowe, ale także internet, telefonia mobilna oraz wszelkiego rodzaju sieci przewodowe i bezprzewodowe, oprogramowania oraz usługi informatyczne. Infrastruktura ICT, na której bazują miejskie rozwiązania smart, kategoryzując najprościej, składa się z (Malucha, 2018):

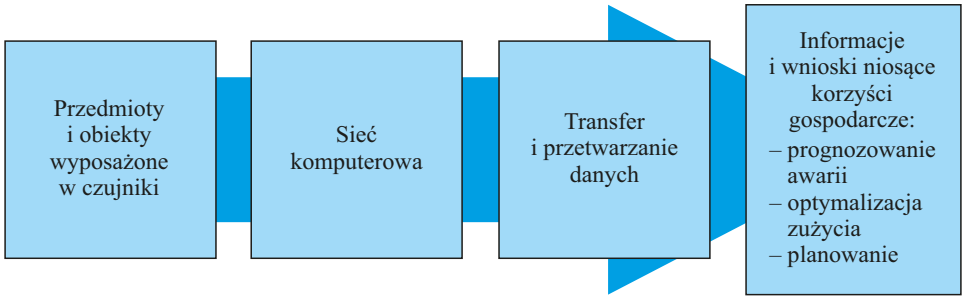
– obiektów wyposażonych w czujniki (odczytujące m.in. temperaturę, poziom wilgoci, drgania czy ruch), a także nadajniki służące do komunikacji, odbioru poleceń oraz przekazywania danych;
– systemów oraz urządzeń umożliwiających odbiór przekazanych do nich danych oraz ich przetwarzanie dla celów podejmowania decyzji (komputery, wszelkiego rodzaju urządzenia mobilne, czy chmury obliczeniowe);
– infrastruktury komunikacyjnej umożliwiającej transmisję danych pomiędzy obiektami (takich jak sieci WiFi, Bluetooth czy też NFC[9]).

Optymalizacja procesów miejskich z zakresie zarówno komunikacji miejskiej, jak i zużycia energii oraz wszelkiego rodzaju innych mediów wymaganych do prawidłowego funkcjonowania miasta jako całości jest powiązana z implementacją rozwiązań pozwalających na monitorowanie większości procesów i działań zachodzących w mieście. W celu zagwarantowania sprawności systemu monitorowania niezbędne jest wdrażanie i wykorzystywanie systemów zaawansowanych czujników umożliwiających zdalne odczyty, a także przekazywanie danych do systemów sterujących i monitorujących funkcjonowanie miasta (Chomiak-Orsa, 2016).

Taki „ekosystem", wewnątrz którego wyposażone w sensory urządzenia mogą się komunikować z komputerami, jest nazywany internetem rzeczy lub internetem (wszech)rzeczy. Umożliwia on otaczającym człowieka obiektom czynny udział w jego środowisku, między innymi poprzez udostępnianie użyt-

[9] Pojęcia NFC *(near field communication*) używa się do określenia sposobu (standardu) komunikacji bezprzewodowej wykorzystującej technologię zbliżeniową. Komunikacja ta polega na szybkim, automatycznym, czyli niewymagającym udziału człowieka „połączeniu" dwóch urządzeń po zbliżeniu ich na odległość kilku bądź kilkunastu centymetrów. Zbliżenie to umożliwia przepływ informacji pomiędzy tymi urządzeniami. Łączyć mogą się różne urządzenia, np. smartfon i terminal płatniczy. W tym przypadku, po jednorazowym włączeniu w telefonie funkcji NFC, możliwe jest dokonywanie płatności mobilnych za pomocą telefonu, bez konieczności posiadania przy sobie karty bankomatowej (Coskun i in., 2013).

kownikom w sieci informacji w sposób bezprzewodowy, przy wykorzystaniu tego samego protokołu IP łączącego sieć. Dzięki temu obiekty te (różne urządzenia i czujniki) mają możliwość rozpoznawania zdarzeń czy zmian następujących w ich otoczeniu, wymiany informacji i samodzielnego wszczęcia odpowiedniej akcji bądź reakcji bez konieczności interwencji człowieka (Grodner i in., 2016; IERC, 2015). Ideę funkcjonowania internetu rzeczy przedstawiono na rysunku 3.



Rysunek 3. Istota internetu rzeczy

Źródło: Opracowanie własne na podstawie (Malucha, 2018).

Internet rzeczy można zastosować w wielu sferach działalności gmin, szczególnie o charakterze miejskim. Oto przykłady jego wykorzystania (Rot, 2017; *Strategia…*, 2020):

– zbudowanie zintegrowanego systemu monitoringu wizyjnego;
– stworzenie systemu informującego w czasie rzeczywistym o liczbie wolnych miejsc parkingowych (lub wolnych do wypożyczenia rowerów, samochodów, hulajnóg) i ich rozmieszczeniu, czyli systemu inteligentnego transportu;
– pomiar temperatury, wilgotności powietrza i natężenia ruchu;
– stworzenie ogólnodostępnej strefy bezprzewodowego internetu;
– zdalne monitorowanie stopnia wypełnienia kontenerów na śmieci;
– zdalne monitorowanie poziomu i czystości wody w rzekach i zbiornikach wodnych;
– zdalne badanie czystości powietrza w różnych punktach gminy;
– zarządzanie siecią ciepłowniczą, gazową, wodną, energetyczną;
– zdalne monitorowanie zdrowia mieszkańców wyposażonych w inteligentne opaski;
– system płatności NFC w środkach transportu publicznego i w budynkach użyteczności publicznej;
– wielofunkcyjne karty miejskie dla mieszkańców.

Nowoczesne technologie informacyjno-komunikacyjne oraz internet rzeczy znajdują szerokie zastosowanie w *smart cities*. Po pierwsze, czujniki stanowią podstawowy element wszystkich systemów monitorowania czy sterowania. W ich kontekście coraz częściej używa się określenia inteligentne systemy sterowania, ze względu na ich autonomiczność oraz zdolność zdalnej kontroli, które pozwalają na zoptymalizowanie, np. zużycia danych mediów. Procesy zarządzania miastem, które są przez nie wspomagane, w znacznym stopniu przyczyniają się do zapobiegania degradacji środowiska, ale również minimalizacji zużycia zasobów naturalnych oraz zarządzania ich dystrybucją. Postęp technologiczny w tym zakresie umożliwia również minimalizację kosztów wynikających z odejścia od monitoringu klasycznego (np. liczników) na rzecz bezprzewodowego (Chomiak-Orsa, 2016).

Kolejną kategorią rozwiązań wykorzystujących ICT, mających istotny wpływ na kreowanie strategii *smart city*, jest zastosowanie narzędzi komunikacji zdalnej. W tej grupie można wyróżnić takie rozwiązania technologiczne, jak: chmury obliczeniowe (*cloud computing*), internet rzeczy, a także infrastruktura komunikacji bezprzewodowej 5G i LTE. Rozwiązania te mogą być wykorzystywane przede wszystkim do komunikacji dalekiego zasięgu, pozwalającej na przekazywanie oraz wymianę wielkich zbiorów danych.

Inną funkcjonalnością, mającą szczególne znaczenie podczas wdrażania koncepcji *smart city*, jest automatyzacja procesów zachodzących w mieście. Najważniejszymi technologiami wykorzystywanymi do komunikacji krótkiego zasięgu są RFID (*radio-frequency identification*) i NFC (*near-field communication*). Identyfikacja radiowa RFID znajduje zastosowanie w niemalże wszystkich systemach komunikacyjnych sieci miejskich. Wśród najpopularniejszych rozwiązań można wskazać inteligentne przystanki, parkingi, jak również systemy oświetlania. Z kolei technologia NFC pozwala na dwukierunkową wymianę informacji, co sprawia, że jest wykorzystywana do transferu danych pomiędzy urządzeniami (Chomiak-Orsa, 2016). W inteligentnych miastach technologie te znajdują zastosowanie w wielu dziedzinach (tabela 4). Niektóre z tych rozwiązań można też zastosować w inteligentnych wsiach.

Tabela 4. Przykłady zastosowania inteligentnych rozwiązań w wybranych sferach działalności samorządu gminnego w *smart city*

Bezpieczeństwo publiczne	Zdrowie[a]	Mobilność miejska	Gospodarka i mieszkalnictwo
predictive policing (śledztwa oparte na komputerowych prognozach)	telemedycyna	informacje o transporcie publicznym w czasie rzeczywistym	cyfrowe wydawanie licencji oraz zezwoleń dla przedsiębiorstw
mapowanie przestępczości[b] w czasie rzeczywistym	zdalne monitorowanie pacjenta	płatności mobilne w transporcie publicznym	programy przekwalifikowania oraz szkolenia online

cd. tabeli 4

Bezpieczeństwo publiczne	Zdrowie[a]	Mobilność miejska	Gospodarka i mieszkalnictwo
wykrywanie strzałów	akcesoria monitorujące styl życia	pojazdy autonomiczne	edukacja spersonalizowana
inteligentny monitoring	alerty pierwszej pomocy	inteligentna sygnalizacja świetlna	lokalne e-centrum kariery
optymalizacja czasu reakcji w sytuacji kryzysowej	informacje o jakości powietrza w czasie rzeczywistym	opłaty za kongestię transportową, p. wjazd do miasta	cyfrowe wydawanie zezwoleń na użytkowanie gruntów oraz budowę
systemy wczesnego ostrzegania przed zagrożeniami, np. porywistym wiatrem	monitorowanie rozprzestrzeniania chorób zakaźnych	transport publiczny na żądanie	otwarte bazy danych (katastry, ewidencje gruntów i budynków)
personal alert (alarmy bezpieczeństwa osobistego)	oparte na danych interwencje w zdrowie publiczne (np. dezynfekcja i higiena)	inteligentne parkowanie	
systemy bezpieczeństwa mieszkań	wyszukiwanie oraz umawianie wizyt lekarskich online	*carpooling* *car/bike sharing*	
inspekcje budynków oparte na analizie danych	zintegrowane systemy zarządzania przepływem pacjentów	*load pooling*[c] oraz inteligentne paczkomaty	
zarządzanie tłumem		zintegrowane informacje dla transportu multimodalnego[d]	
Energia	**Woda**	**Odpady**	**Partycypacja**
system automatyki budynkowej	monitorowanie zużycia wody	cyfrowe monitorowanie oraz płatności za wywóz odpadów	lokalne aplikacje dla mieszkańców
domowe zautomatyzowane systemy energetyczne	wykrywanie wycieków i ich kontrolowanie	optymalizacja trasy pojazdów do wywozu odpadów	lokalne platformy komunikacji
monitorowanie zużycia energii w domach	inteligentne systemy nawadniające zieleń gminną		cyfrowe usługi administracyjne
inteligentne oświetlenie uliczne	monitoring jakości wody		

[a] Niektóre z rozwiązań, np. umawianie wizyt lekarskich, wykraczają poza zadania polskich gmin, chyba że utworzyły i prowadzą podmiot leczniczy.
[b] Mapowanie, czyli wskazywanie miejsc popełnienia przestępstwa na podstawie materiałów źródłowych (np. nagrań z monitoringu lub pomiaru).
[c] Łącznie kilku dostaw od jednego odbiorcy.
[d] Przewóz towarów przy pomocy przynajmniej dwóch środków transportu.

Źródło: opracowanie własne na podstawie (OECD, 2019).

Poszukiwanie rozwiązań mających wspierać utrzymywanie równowagi pomiędzy cywilizacją a środowiskiem jest obiektywną potrzebą i ważnym zadaniem gmin. Znalezieniu tej równowagi sprzyjają ICT, które pozwalają na optymalizację różnych procesów zachodzących w mieście. Obecnie innowacyjne technologie informacyjno-komunikacyjne stanowią poniekąd determinantę kierunków rozwoju miast. Z drugiej strony mają one charakter swego rodzaju spoiny, stanowiąc elementarne narzędzie pozwalające na zaistnienie efektów synergii będących wynikiem korelacji wszystkich płaszczyzn funkcjonowania *smart city* (Chomiak-Orsa, 2016).

Bardzo ważnym elementem gospodarki 4.0 są dane. Administracja gminna potrzebuje więc narzędzi analitycznych i raportujących, których wykorzystanie umożliwi pracownikom szybki dostęp do danych, raportów, analiz i przełoży się na wzrost efektywności działania. Narzędzia takie są obejmowane mianem systemów inteligencji biznesowej (*business inteligence*). Umożliwiają one integrację danych z różnych systemów, w tym danych gromadzonych przez gminne jednostki organizacyjne (Hauke, 2017).

Gminy są także jednymi z podmiotów zobowiązanych do udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania (otwartych danych). Otwarte dane to takie informacje sektora publicznego, które są udostępniane lub przekazywane w postaci elektronicznej, bezwarunkowo lub z uwzględnieniem warunków wynikających z przepisów prawnych. Są to dane kompletne, aktualne, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego. Dane te są przeznaczone do bezpłatnego ponownego wykorzystywania na tych samych zasadach dla każdego użytkownika, bez konieczności potwierdzania tożsamości przez użytkownika (Ustawa, 2021).

Od 2022 r. jednostki administracji publicznej, w tym jednostki samorządu terytorialnego, mają możliwość wdrażania systemu elektronicznego zarządzania dokumentacją (EZD). System ten został wprowadzony w ramach projektu „EZD RP – elektroniczne zarządzanie dokumentacją w administracji publicznej" i jest udostępniany na zasadach niekomercyjnych zainteresowanym podmiotom administracji publicznej. System EZD jest narzędziem umożliwiającym kompleksowe dokumentowanie przebiegu załatwiania i rozstrzygania spraw w jednostkach. Wspomaga on również m.in.: tworzenie, obsługę i obieg dokumentów elektronicznych i papierowych (w tym korespondencji wpływającej i wychodzącej), zarządzanie aktami i dokumentami w aktach spraw (elektronicznymi i papierowymi), w tym ich udostępnianie i archiwizowanie oraz zarządzanie informacją. Poszczególne jednostki samorządowe samodzielnie decydują o wdrożeniu EZD (Podlaski Urząd, 2022).

Zdecydowanie mniej uwagi przywiązuje się do inteligentnego rozwoju innych obszarów niż miasta. Synowiec (2021) dokonała przeglądu literatury,

z którego wynika, że wsie budzą skojarzenia dalekie od postępu i (inteligentnego) rozwoju, tymczasem, jak przekonuje Shuldiner (2020), wspólnoty inne niż miasta, jako mniejsze i charakteryzujące się słabszą dynamiką zachodzących w nich zmian, a tym samym większą jednorodnością, z pewnością mogą spełniać kryteria przestrzeni przyszłości[10]. Można więc mówić o koncepcji *smart village* – inteligentnej wsi (inteligentnej wioski smartwsi)[11], która nawiązuje do idei *smart city* (tabela 5). Inteligentne wsie to te wiejskie społeczności lokalne, które „wykorzystują technologie cyfrowe[12] i innowacje w swoim codziennym życiu, poprawiając w ten sposób jego jakość, polepszając standard usług publicznych i lepiej wykorzystując zasoby lokalne" (Kalinowski i in., 2021, s. 14).

Tabela 5. Porównanie koncepcji *smart city* oraz *smart village*

Kryterium porównania	Koncepcja *smart city*	Koncepcja *smart village*
Geneza	– postęp technologiczny, rozwój gospodarki opartej na wiedzy i innowacjach, również presja na ochronę środowiska – wsparcie polityczne instytucji globalnych, w tym ONZ, UE i OECD umożliwiło dynamiczny rozwój koncepcji *smart city* – lata 90. XX w.	– potrzeba wzmocnienia żywotności, włączenia i konkurencyjności obszarów wiejskich UE, wyhamowania trendów depopulacyjnych i poprawy jakości życia – koncepcja i jej wdrażanie służy realizacji założeń strategii Europa 2020 oraz Deklaracji Cork 2.0 – powstała po 2017 r.
Podstawy teoretyczne	teorie: biegunów wzrostu, centrów i peryferii, teoria gron, teoria produktu podstawowego i nowa teoria handlu, koncepcja terytorialnych systemów produkcji, koncepcja środowiska innowacyjnego, teoria regionów uczących się, koncepcja inteligentnych specjalizacji	koncepcja zakorzenienia terytorialnego, teoria gron, teoria produktu podstawowego i nowa teoria handlu, koncepcja terytorialnych systemów produkcji, koncepcja środowiska innowacyjnego, teoria regionów uczących się, koncepcja inteligentnych specjalizacji, teoria biegunów wzrostu, centrów i peryferii
Szybkość zmian	bardzo szybkie dynamiczne zmiany, kierowane tempem zmian w rozwiązaniach ICT; *smart living*	wolniejsze tempo zmian; mniej radykalne zmiany; *slow life*

[10] Szewc (2020) także stoi na stanowisku, że wszystkie gminy oraz różne formy ich współpracy mogą podejmować działania zmierzające do urzeczywistnienia koncepcji *smart city*.

[11] W literaturze używa się zarówno określenia *smart villages* (inteligentne wioski), jak i *smart village* (inteligentna wieś). Pierwsze określenie jest popularniejsze.

[12] Technologie cyfrowe można traktować jako synonim technologii informacyjno-komunikacyjnych.

cd. tabeli 5

Kryterium porównania	Koncepcja *smart city*	Koncepcja *smart village*
Główne cele zmian	wzrost konkurencyjności terytorium, efektywności wykorzystania zasobów, zmniejszenie presji na środowisko, poprawa jakości życia poprzez zastosowanie postępu technologicznego	poprawa jakości życia, zatrzymanie ludności wiejskiej przed odpływem do miast, troska o lokalne dziedzictwo wsi, digitalizacja wsi, rozwój kapitału społecznego na wsi
Najważniejsze czynniki (katalizatory) zmian	technologia i wysoka jakość kapitału ludzkiego	kapitał terytorialny, lokalne dziedzictwo wsi, kapitał społeczny, innowacje technologiczne i społeczne umożliwiające włączenie społeczności wiejskich
Liderzy przemian	duże znaczenie prywatnych podmiotów stosujących nowe technologie, władz realizujących projekty partnerstwa publiczno-prywatnego	duże znaczenie lokalnych podmiotów, lokalnych liderów oraz inicjującej, aktywizującej i koordynującej roli władz lokalnych (w tym sołtysów i rady sołeckiej)
Główne dziedziny zastosowania	transport miejski, ochrona środowiska, wykorzystanie energii, gospodarka wodna i odpadowa, ochrona zdrowia, bezpieczeństwo publiczne	gastronomia, rękodzieło, turystyka, nowoczesne rozwiązania technologiczne dla rozwoju turystyki i ochrona środowiska (gospodarka wodna, gospodarka odpadami), transport, ochrona zdrowia i bezpieczeństwo, kultura
Specjalizacja	inteligentna specjalizacja (szczególnie działalność tematyczna, miasta tematyczne, np. miasta projektowania, miasta mediów, miasta sztuki, miasta filmu)	lokalne specjalizacje bazujące na unikalnym potencjale endogenicznym (lokalne produkty i usługi, tradycja i tożsamość miejsca), dziedzictwo kulturowe
Znaczenie współpracy/ partnerstwa terytorialnego	duże	duże (często obowiązkowym warunkiem rozwoju jest nawiązanie współpracy miejsko-wiejskiej)
Etap wdrażania	zaawansowany	początkowy pilotażowy
Główne bariery rozwoju	ograniczenia technologiczne, organizacyjne i finansowe; brak uczestnictwa i świadomości mieszkańców; brak akceptacji i identyfikacji z koncepcją inteligentnego rozwoju	brak uczestnictwa i świadomości mieszkańców, akceptacji i identyfikacji z koncepcją rozwoju inteligentnego, bariery technologiczne, organizacyjne i finansowe

Źródło: opracowanie własne na podstawie (Guzal-Dec, 2018, s. 40–41).

Nieco inna jest geneza obu koncepcji, częściowo rozbieżne są też ich podstawy teoretyczne. W obu koncepcjach „ważna jest technologia, podobnie jak inwestycje w infrastrukturę, rozwój biznesu, kapitał ludzki, potencjał i budowanie społeczeństwa obywatelskiego. Ważne jest również dobre zarządzanie i zaangażowanie obywateli" (Guzal-Dec, 2018, s. 33). W obu zwraca się też uwagę na umiejętności korzystania z kompetencji cyfrowych, dostęp do e-usług zdrowotnych i innych podstawowych usług, innowacyjne rozwiązania w zakresie ochrony środowiska. W przypadku *smart village* ważna jest też możliwość zastosowania ICT do: zwiększenia efektowności produkcji rolniczej i ułatwienia pracy, tworzenia gospodarki o obiegu zamkniętym w odniesieniu do odpadów rolniczych, dbania o środowisko naturalne, poprawy procesu świadczenia przez gminę usług z zakresu infrastruktury technicznej i społecznej, promocji lokalnych produktów, integracji mieszkańców. Tym samym umożliwią one czerpanie korzyści z inteligentnych specjalizacji w zakresie projektów rolno-spożywczych, turystyki, działalności kulturalnej itp. Nowe technologie mogą znaleźć zastosowanie zarówno w życiu mieszkańców wsi (np. montaż czujników informujących o nawodnieniu upraw, automatyzacja procesu karmienia zwierząt), jak i w działalności gmin. W tabeli 6 zestawiono przykłady zastosowania inteligentnych rozwiązań w duchu koncepcji *smart village* w polskich gminach wiejskich i miejsko-wiejskich.

W odróżnieniu od miast „społeczności zamieszkujące obszary wiejskie wykazują niższy poziom dostępu, ale też otwartości wobec korzystania z nowych technologii informacyjnych. Dlatego też wskazuje się na potrzebę zwiększenia innowacyjnego rozwoju obszarów wiejskich przy znaczącym udziale innowacji społecznych. To one winny być generatorem pozytywnych zmian skutkujących rozwojem kapitału ludzkiego i społecznego i przyczyniać się do skuteczniejszego wdrażania innowacji technologicznych na tych obszarach" (Guzal-Dec, 2018, s. 36).

Nowoczesne technologie wpływają na wzrost jakości życia zarówno w mieście, jak i na wsi, ponieważ, jak podkreślają Gevelt i Van Holmes (2015), w przypadku wsi wykorzystanie tych technologii w inicjatywach rozwoju obszarów wiejskich stwarza szansę świadczenia nowych usług i zwiększenia dochodów. W Polsce inteligentne rozwiązania są stopniowo wprowadzane we wspólnotach wiejskich. Pionierami tych przeobrażeń są m.in. gminy: Jarocin, Magnuszew, Michałowo, Morawica, Olsztynek, Ryczywół, Rzeczenica, Staszów, które obok innych 56 gmin wzięły udział w pierwszej edycji konkursu „Moja SMART wieś" zorganizowanego przez Instytut Rozwoju Wsi i Rolnictwa Polskiej Akademii Nauk (Kalinowski i in., 2021).

Tabela 6. Przykłady zastosowania inteligentnych rozwiązań w duchu koncepcji *smart village* w wybranych gminach wiejskich i miejsko-wiejskich[a]

Gmina, województwo	Nazwa inicjatywy, miejscowość	Sfera życia społeczno-gospodarczego, której dotyczy inicjatywa
Dragacz; kujawsko-pomorskie	Nie ciafrotać jeno robić! Wiejskie działania – miejskie inspiracje	dziedzictwo kulturowe, edukacja i ekologia
Jarocin; wielkopolskie	Doposażenie infrastruktury rekreacyjno-edukacyjnej nad stawem wiejskim w Łuszczanowie (Łuszczanów)	działania infrastrukturalne, prośrodowiskowe i na rzecz integracji mieszkańców
Michałowo; podlaskie	Nowy model hospicjum na terenach wiejskich (Michałowo)	ochrona zdrowia
Olsztynek; warmińsko-mazurskie	Ostoja Wioska 3,0 (Tomaszyn)	ekologiczne rolnictwa i inne działania na rzecz lokalnej społeczności (lokalne targi, biobazary)
Ryczywół; wielkopolskie	Hala widowiskowo-sportowa w Ryczywole. Jak to Ryczywół stał się smart (Ryczywół)	inwestycja infrastrukturalna z zakresu sportu i rekreacji, wykorzystująca nowe technologie
Staszów; świętokrzyskie	Moja smart wieś (Wiązownia Kolonia)	inicjatywy z różnych dziedzin, m.in. komunikacji z mieszkańcami, edukacji, kultury
Szubin; kujawsko-pomorskie	Centrum Astronomiczno-Kulturalno-Dydaktyczne (Niedźwiady)	inwestycja infrastrukturalna połączona z edukacyjną
Gostycyn; kujawsko-pomorskie	Górnicza Wioska kopalnią idei Smart Villages (Piła)	różne działania poprawiające jakość życia mieszkańców sołectwa, np: stworzenie ekomuzeum, opracowanie questa i skrytek geocachingu, utworzenie Przedsiębiorstwa Społecznego „Górnicza Wioska" Sp. z o.o., zbudowanie biologicznej oczyszczalni ścieków
Łomianki; mazowieckie	Moja Smart wieś Kiełpin – IDEA (Kiełpin)	montaż ławki z ogniwem fotowoltaicznym, za pomocą której można ładować smartfony; budowa hot spotu na placu zabaw

[a] Wybrano tylko smart inicjatywy bezpośrednio związane z zadaniami gmin. Szerzej na temat tych i innych rozwiązań podejmowanych w duchu *smart village* można przeczytać w podanych źródłach.

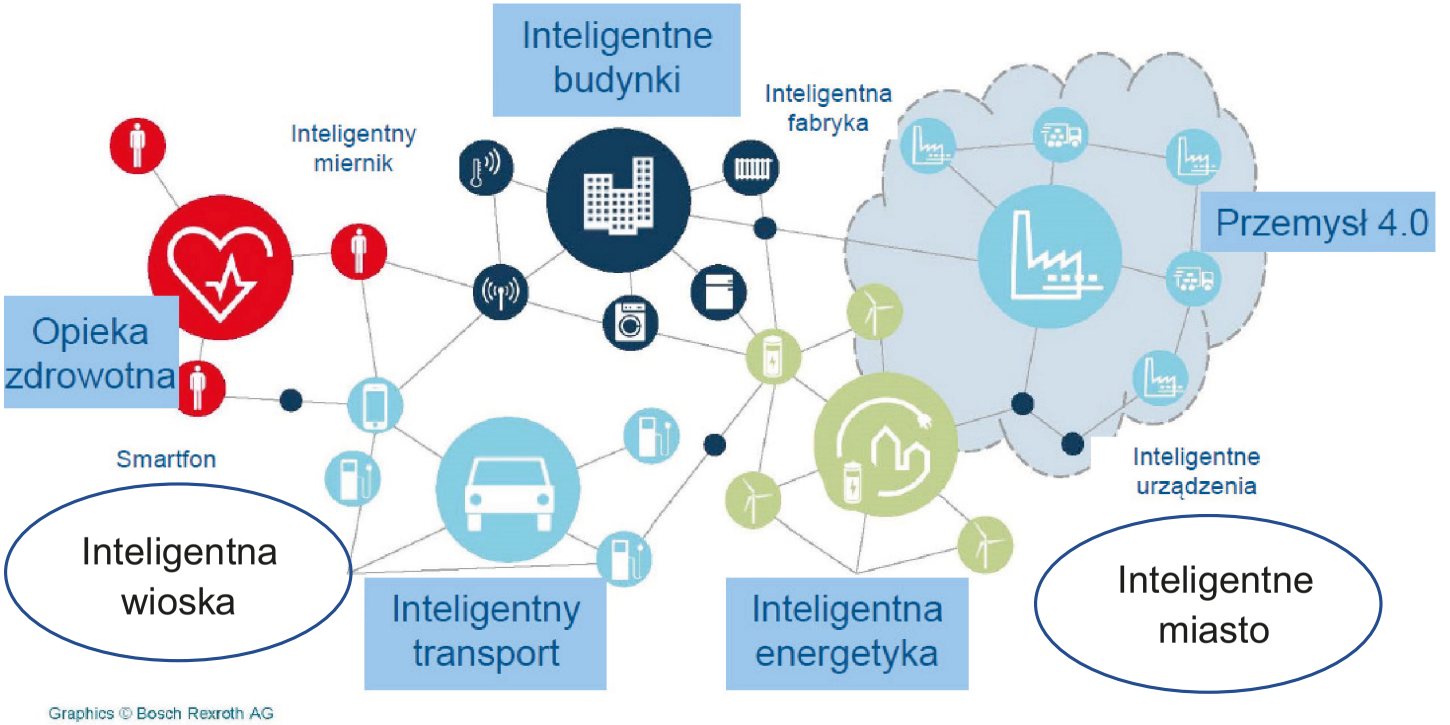
Źródło: opracowanie własne na podstawie (Kalinowski i in., 2021; Surowiec, 2021).

1.4. Wybrane aspekty wpływu nowych technologii na gospodarkę gmin

Efektem zastosowania nowych technologii będzie przekształcenie się „zwykłych" gmin w „gminy smart", co w uproszczeniu przedstawiono na rysunku 4. Gminy muszą próbować zrozumieć istotę gospodarki 4.0. Wydaje się, że można ją scharakteryzować następująco: gospodarka 4.0 jest to gospodarka danych, których źródłami są: mobilny internet ludzi, internet rzeczy oraz wirtualna i wzbogacona rzeczywistość. Te ogromne dane (gigadane) są przesyłane za pośrednictwem telefonii 5G, a gromadzone w chmurze obliczeniowej. Dane te są przetwarzane i analizowane przez sztuczną inteligencję. Wyniki analiz mają być wykorzystywane w procesie produkcji i świadczenia usług po to, aby zapewnić ich efektywność i doprowadzić do osiągnięcia celów zrównoważonego rozwoju. Nowe technologie doprowadziły do tego, że komunikacja następuje nie tylko pomiędzy ludźmi, ale też między maszynami oraz maszynami i ludźmi. Współistnienie ludzi i maszyn oraz wykorzystywanie w ich relacjach nowych technologii kreują zintegrowane środowisko (społeczne, gospodarcze) oparte na danych (Cellary, 2022b). Przed jednostkami samorządowymi jeszcze daleka droga, aby doprowadzić do połączenia wszystkiego ze wszystkim: urzędu gminy z gminnymi jednostkami organizacyjnymi i spółkami gminnymi oraz z mieszkańcami i podmiotami gospodarczymi. Wydaje się jednak, że transformacja cyfrowa każdej wspólnoty jest nieuchronna.

Wyzwania stojące przed gminami w związku z transformacją cyfrową można podzielić na: technologiczne, dotyczące kultury organizacyjnej urzędów gmin, związane ze świadomością i kompetencjami organów gmin, urzędników, mieszkańców i podmiotów współtworzących tkankę wspólnoty samorządowej oraz odnoszące się do funkcji pełnionych przez gminy, zakresu wykonywanych zadań, wykorzystywanych narzędzi oraz metod zaspokajania potrzeb mieszkańców i podmiotów gospodarczych.

W coraz większym stopniu gminy będą odchodzić od bezpośredniego wykonywania zadań (świadczenia usług) na rzecz pełnienia funkcji zarządczej, polegającej na ukierunkowywaniu rozwoju danej jednostki terytorialnej, na co wiele lat temu zwracała uwagę Wojtasiewicz (2004). Ukierunkowanie tego rozwoju będzie się odbywać poprzez uchwalanie strategii rozwoju (być może także strategii rozwoju cyfrowego), kojarzenie podmiotów gospodarczych ze start-upami i ośrodkami badawczymi, zapraszanie do gmin (miast) operatorów nowych usług, np. roweru miejskiego, hulajnóg elektrycznych, *carsharingu*. Strategie takie należy tworzyć, aby zminimalizować ryzyko wprowadzania w gminach rozwiązań sugerowanych przez dostawców nowych technologii,



Rysunek 4. Wizualizacja smartgminy

Źródło: opracowanie własne na podstawie (Cellary, 2019a).

ale niekoniecznie wynikających z analizy potrzeb społecznych[13]. Bezpośrednie funkcje wykonawcze będą ograniczane nie tylko w związku z realizacją postulatów nowego zarządzania publicznego[14] i *good governance*[15], ale także dlatego, że gminy i ich jednostki organizacyjne nie będą w stanie nadążyć za podmiotami prywatnymi we wprowadzaniu innowacyjnych metod zaspokajania potrzeb obywateli.

Punktem wyjścia do zmian zakresu zadań gmin musi być jasny podział zadań i kompetencji związanych z transformacją cyfrową pomiędzy organy władzy i administracji rządowej i samorządowej. W tej chwili taką dyskusję prowadzi się np. w odniesieniu do podziału zadań z zakresu zapewnienia cyberbezpieczeństwa przestrzeni publicznej (Chałubińska-Jentkiewicz, 2021; Kostrubiec, 2021). Już teraz zmienia się zakres świadczonych usług (Lipowicz, 2019; Szewc, 2020). Zgodnie z zasadą domniemania kompetencji na barki samorządu terytorialnego (gmin) spada upowszechnianie konwencjonalnych umiejętności posługiwania się komputerem, smartfonem, korzystania z aplikacji.

Nie mniej ważne jest określenie zakresu samodzielności gmin w stosowaniu nowych technologii. Zasadniczo gminy mają samodzielność w stanowieniu o wydatkach, w tym o formach organizacyjnych, w jakich są wykonywane ich zadania. Mogą więc wykorzystywać internet rzeczy do zdalnego odczytu liczników i montować czujniki na miejscach parkingowych po to, aby ustalić, czy są zajęte. W tym przypadku w przepisach prawnych określono cel, jaki mają osiągnąć gminy (zaspokojenie potrzeb z zakresu zaopatrzenia w wodę i transportu), a wybór sposobu dojścia do niego pozostawiono do dyspozycji usługodawcy. Niekiedy samodzielność wydatkowa może być dyskusyjna, np. wątpliwe jest, czy stworzenie miejskiego systemu wypożyczania rowerów mieści się w zadaniach gminy. Takie wątpliwości wynikają z tego, że prawo nie nadąża za rzeczywistością (Szewc, 2020). Czasami organy władzy i administracji rządowej

[13] Jak dotąd odrębne strategie transformacji cyfrowej opracowało i uchwaliło tylko kilka jednostek samorządu terytorialnego, w tym województwo mazowieckie i Warszawa.

[14] Jest to jeden z modeli zarządzania publicznego, który powstał w reakcji na wady biurokracji. Akcentuje się w nim konieczność odejścia od biurokratycznego myślenia i kierowania sprawami publicznymi za pomocą metod i technik zarządzania stosowanych w sektorze prywatnym. W koncepcji nowego zarządzania publicznego zwraca się uwagę np. na: osiąganie wyników, a nie proces wykonywania zadań, konieczność traktowania obywateli jak klientów, a nie petentów, włączanie sektora prywatnego w zaspokajanie potrzeb publicznych. Szerzej na ten temat np. (Krynicka, 2006).

[15] Jest to jeden z modeli zarządzania publicznego. Zwraca się w nim uwagę na konieczność poprawy jakości rządzenia, co nastąpi, jeżeli będą przestrzegane zasady: przejrzystości, partycypacji, praworządności, konsensusu, równości, efektywności, odpowiedzialności, spełniania potrzeb. Bardzo ważne jest przestrzeganie wszystkich zasad, bo doprowadzi to do dobrych rządów (dobrego rządzenia), które są cechą efektywnego państwa. Szerzej na ten temat np. (Dziemianowicz i in., 2018).

nakazują gminom wykonywanie zadań podnoszących jakość życia mieszkańców za pomocą ICT, np. (Szewc, 2020):

– stosowanie odpowiednich systemów teleinformatycznych,
– wnoszenie podań i korespondowania ze stronami drogą elektroniczną,
– udostępnianie informacji publicznej,
– transmitowanie na żywo obrad rady gminy i dokumentowania nagrań,
– prowadzenie działalności w zakresie telekomunikacji, w tym instalowanie sieci światłowodowych i oferowanie mieszkańcom dostępu do internetu.

Należałoby to tego dodać doręczanie korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego i publicznej usługi hybrydowej (Ustawa, 2020) oraz obowiązek opracowania planu zrównoważonego rozwoju publicznego transportu zbiorowego przez gminy liczące co najmniej 50 tys. mieszkańców, w którym określa się m.in. linie komunikacyjne, na których przewidywane jest wykorzystanie pojazdów elektrycznych lub pojazdów napędzanych gazem ziemnym, oraz planowany termin rozpoczęcia ich użytkowania (Ustawa, 2010). Uregulowania te bezpośrednio wpływają na sposób wykonywania zadań przez gminy. Można je co prawda ocenić jako ograniczające samodzielność gmin w stanowieniu o wydatkach (Kańduła, 2003), ale sprzyjają one upowszechnianiu nowych rozwiązań, a tym samym transformacji cyfrowej samorządu gminnego.

Konieczne jest dostosowanie oferty edukacyjnej szkół prowadzonych przez samorząd do oczekiwań rynku i tworzenie pozaszkolnych możliwości zdobycia pożądanych kwalifikacji. Niezbędne jest więc nawiązanie ściślejszych kontaktów między placówkami oświatowymi i podmiotami gospodarczymi (tworzenie klas patronackich, praktyki zawodowe), tak aby możliwe było kształcenie bezpośrednio na stanowisku pracy. Zdecydowała się na to np. gmina wiejska Tarnowo Podgórne z województwa wielkopolskiego, która utworzyła szkołę branżową (zawodową) i średnią – Zespół Szkół Technicznych. W szkole branżowej I stopnia uczniowie mogą się kształcić w zawodach: mechatronik, magazynier-logistyk, stolarz, tapicer, krawiec, elektromechanik. W technikum uczniowie mogą się kształcić w zawodach: technik informatyk, technik mechatronik, technik logistyk, technik robotyk, technik elektronik, technik procesów drukowania (*Zespół…*, 2021).

Rywalizacja o przyciągnięcie innowacyjnych podmiotów gospodarczych i dążenie do zatrzymania dotychczasowych inwestorów zaowocuje przejmowaniem przez gminy części kosztów na etapie powstawania inwestycji oraz kosztów ich eksploatacji (np. kosztów uzbrojenia terenów, kosztów budowy dróg dojazdowych i infrastruktury technicznej, ale także zapewnienia infrastruktury telefonii 5G). Ponoszone też będą inne wydatki na stymulowanie przedsiębiorczości i kreatywności oraz zasilenie kapitałowe instytucji otoczenia biznesu, np. agencji rozwoju lokalnego i regionalnego, ośrodków wspierania przedsiębiorczości,

inkubatorów przedsiębiorczości, centrów i parków technologicznych, funduszy poręczeniowo-kredytowych, start-upów. Należy się także spodziewać wzrostu wydatków budżetowych gmin na stypendia dla młodych ludzi, którzy tworzą innowacyjne rozwiązania, oraz wydatków na organizację maratonów projektowania (tzw. hakatonów), podczas których, przy wykorzystaniu otwartych baz danych jednostki samorządowej, tworzone są aplikacje mające na celu poprawę jakości życia w danej wspólnocie i usprawnienie komunikacji między społecznością a urzędem samorządowym (*Po raz trzeci…*, 2019). Dokonywane będą też wydatki na działalność informacyjną i promocyjną. Samorząd terytorialny musi bowiem informować o swoich e-usługach, edukować i motywować do korzystania z nich potencjalnych użytkowników.

Zmianie muszą ulec metody (modele) wykonywania zadań. Chodzi tu o konieczność wykonywania zadań związanych z transformacją cyfrową we współpracy. Niezbędna jest współpraca organów gmin (w szczególności wykonawczych), informatyków zatrudnionych w urzędach, kierowników wydziałów i jednostek organizacyjnych, samorządowych osób prawnych świadczących usługi oraz podmiotów oferujących nowe rozwiązania technologiczne. Powinni oni współpracować nie tylko ze sobą, ale także z podmiotami z podsektora rządowego. Współpraca może polegać na: wspólnym zakupie sprzętu komputerowego i oprogramowania, zakupie szkoleń, dostępu do internetu, zakupie usług magazynowania i przetwarzania danych w chmurze (Ziemba i in., 2015). Wymaga to zmiany mentalności w samorządzie terytorialnym, bo część samorządowców wciąż uważa, że każda jednostka samorządowa powinna dokonywać transformacji cyfrowej samodzielnie, w imię samodzielności i niezależności od organów państwa. Prowadzi to jednak do niepotrzebnego mnożenia wydatków publicznych i opóźnia pełną transformację cyfrową administracji publicznej. Niezbędne jest stworzenie platformy wymiany myśli, specyfikacji dokumentów przetargowych, produktów cyfrowych. Krokiem w dobrą stronę jest projekt „Linia współpracy rządu i samorządu 2016" (*Linia…*, b.d.).

Wykorzystywanie nowych technologii wpłynie też na kulturę organizacyjną gmin. W strukturach ich urzędów pojawią się komórki, biura lub wydziały zajmujące się różnymi aspektami nowych technologii. Ich przykładem jest Biuro Cyfryzacji i Cyberbezpieczeństwa w Urzędzie Miasta Poznania. Wójtowie (burmistrzowie, prezydenci) będą też powoływać swoich pomocników do spraw transformacji cyfrowej, w tym do spraw *smart city*. Takie stanowiska są już m.in. w Gdyni i we Wrocławiu. Należy się też spodziewać powoływania pełnomocników do spraw danych miejskich (Łachowski, 2021).

Trudno jest dzisiaj wartościować, które z tych zmian będą najistotniejsze, ale uważamy, że będą one impulsem rozwojowym nowoczesnych gmin miejskich, wiejskich i miejsko-wiejskich.

1.5. Uwarunkowania i bariery transformacji cyfrowej samorządu gminnego

Transformacja cyfrowa samorządu gminnego może być inicjatywą podejmowaną lokalnie, jednak nadanie jej „państwowego" charakteru nie tylko podnosi rangę tego procesu, ale też stwarza szansę uzyskania finansowego wsparcia ze strony organów władzy i administracji rządowej. Od kilku lat cyfryzacja jest priorytetem polskiego rządu, dlatego (nieistniejące już) Ministerstwo Cyfryzacji[16] określiło pięć podstawowych uwarunkowań (warunków wstępnych, zasad) tej transformacji (Chaba, 2021; MC, 2016).

Po pierwsze, administracja publiczna ma pełnić funkcję służebną wobec obywatela. Ma to polegać na zastępowaniu zagmatwanych i różnorodnych procedur elektronicznymi usługami charakteryzującymi się prostotą (krótkim i intuicyjnym procesem usługowym) i spójnością rozumianą jako standaryzacja usług (ta sama usługa lub podobna powinna być świadczona w ten sam sposób niezależnie od rodzaju usługodawcy). Prostotę tę ma zapewnić stosowanie nowoczesnych technologii. Warunek ten można spełnić na poziomie samorządu gminnego, w szczególności gdy decyzje (stanowiące i wykonawcze) podejmują osoby stosunkowo młode, legitymujące się wyższym wykształceniem, mające wysokie poparcie społeczne (Perdał, 2014).

Warunkiem zbudowania e-administracji publicznej jest zapewnienie obywatelom i przedsiębiorcom dostępu do sieci komputerowej o wysokiej przepustowości. Rozwój tej sieci jest drugim uwarunkowaniem transformacji, na który zwracają uwagę przedstawiciele rządu. Trzecim warunkiem jest stałe, niezależne od wieku, podnoszenie kompetencji cyfrowych adresatów usług elektronicznych i usługodawców. Następnym wymogiem transformacji cyfrowej jest przekonanie usługodawców i usługobiorców, że dostęp do sieci oraz usług publicznych jest bezpieczny, wszystkie dane są chronione, a transakcje są zabezpieczone przed cyberprzestępcami. Piątym warunkiem udanej transformacji cyfrowej administracji publicznej, w tym gminnej, jest zapewnienie łatwego dostępu do danych gromadzonych przez instytucje publiczne. Uwarunkowania te trzeba uzupełnić o jeszcze jedno, mianowicie transformacja cyfrowa samorządu gminnego nie będzie możliwa, jeżeli nie będą uchwalane i wprowadzane w życie przepisy prawne (Chaba, 2021), które będą stanowiły „ramy" tej transformacji i w których zostaną uregulowane zagadnienia dotyczące m.in. rodzajów ICT wykorzystywanych

[16] Ministerstwo Cyfryzacji było urzędem obsługującym ministra właściwego do spraw informatyzacji. Utworzono je 8 grudnia 2015 r., a zlikwidowano 7 października 2020 r. (Rozporządzenie RM, 2020). Dotychczasowych pracowników włączono w skład Kancelarii Prezesa Rady Ministrów. Powołano też Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

w sektorze finansów publicznych, sposobów korzystania z rożnych systemów, obowiązków samorządu gminnego z zakresu stwarzania warunków do rozwoju sieci i podnoszenia kompetencji cyfrowych, certyfikacji systemów zapewnienia bezpieczeństwa informacji, elektronicznego zarządzania dokumentami czy elektronicznego dostarczania korespondencji.

Okolicznością mającą wpływ na transformację cyfrową jest też pandemia COVID-19, która przyspieszyła tę transformację. Wcześniej w niektórych jednostkach debatowano nad celowością zastosowania nowych technologii, w innych ich wdrażanie trwało długo. Nieoczekiwanie pandemia sprawiła, że technologie cyfrowe udało się zastosować w ciągu tygodni, a nawet dni. Znalazły się dodatkowe środki finansowe nie tylko na działania podnoszące poziom bezpieczeństwa zdrowotnego mieszkańców (np. rozdawanie środków ochronnych, dezynfekcja miejsc publicznych), ale również na działania rozwojowe, które są wykorzystywane nawet po ustaniu pandemii. Chodzi tu o oferowanie usług, które pozwalają korzystać z urzędów i infrastruktury samorządowej w bezpieczny, zdalny sposób, oraz usług, które mają zmniejszyć nierówności społeczne między członkami wspólnoty samorządowej.

Wytyczne rządu dotyczące ograniczenia bezpośrednich kontaktów między ludźmi wpłynęły na wprowadzanie w urzędach rozwiązań umożliwiających zdalny dostęp interesariuszy do danych gromadzonych przez gminy, przeprowadzanie spotkań organów stanowiących w formie wideokonferencji, zwiększenie liczby usług świadczonych elektronicznie (Kańduła i Przybylska, 2022c; Miazga i in., 2022). Gdynia wykorzystywała możliwości sztucznej inteligencji i wprowadziła do systemu monitoringu miejskiego algorytm po to, aby lokalizować duże skupiska ludzi i móc zareagować, na przykład zwiększając częstotliwość dezynfekcji tych obszarów (Jurczak, 2020). W Koszalinie, Siemianowicach Śląskich oraz w Tarnowie w tym samym celu wykorzystywano drony (Łuczyn, 2020). Włodarze gmin zaczęli też intensywniej wykorzystywać media społecznościowe do informowania o liczbie zakażeń, podjętych działaniach, apelowania o przemyślanie zachowania itp. (Kańduła i Przybylska, 2022b).

W opinii autorek lockdown wywołany przez pandemię COVID-19 był niewątpliwie katalizatorem cyfryzacji części usług publicznych, jednak skala tych zmian jest stosunkowo niewielka. Warto zauważyć, że digitalizacja usług publicznych niesie bez wątpienia szereg korzyści dla mieszkańców, może jednak również prowadzić do wykluczenia cyfrowego osób, szczególnie mniej zamożnych i starszych.

Proces transformacji cyfrowej polskiej administracji publicznej postępuje, ale organy odpowiedzialne za tę transformację dostrzegają wiele barier (tabela 7), które utrudniają ten proces (Chaba, 2021; MC, 2019). Można je podzielić na bariery: instytucjonalne, techniczne, kadrowe, finansowe oraz inne.

Tabela 7. Bariery transformacji cyfrowej administracji publicznej w Polsce z punktu widzenia administracji rządowej

Grupa barier	Bariera/trudność
Instytucjonalne	brak jednolitego modelu współdziałania pomiędzy administracją państwową a jst, w tym w odniesieniu do wymiany sprawdzonych rozwiązań i dobrych praktyk czy wzajemnego świadczenia usług (jest tak nawet pomimo funkcjonowania przykładowo „linii współpracy" i rady użytkowników ePUAP, w której działają dwie stałe grupy współpracy między rządem i jst zajmujące się kwestiami organizacyjnymi oraz technicznymi dotyczącymi cyfryzacji)
	rozproszenie i brak skoordynowania w odniesieniu do zarządzania zasobami informatycznymi
	brak odpowiednich regulacji prawnych odnośnie do kwestii związanych z ochroną prywatności obywateli czy zakresem wykorzystywania tzw. danych wrażliwych, wynikający ze zbyt szybkiego rozwoju technologii cyfrowych, który wpływa m.in. na powstawanie luk prawnych w tym zakresie
Techniczne	brak interoperacyjności (spójności, połączenia) systemów i rejestrów publicznych wykluczający możliwość nawiązywania współpracy i wymiany informacji pomiędzy różnymi organami publicznymi
	powielanie znacznej części danych i ich ponowne, nieuzasadnione wykorzystywanie na różnych poziomach administracji publicznej, w tym regionalnym i lokalnym
	niedostateczna dbałość o jakość systemów informatycznych (może to wynikać zarówno z niedostatku kadr, środków, jak i braku świadomości), co przejawia się w braku ich certyfikacji, co potwierdzają badania (Chodakowska i in., 2022b)
	brak zapewnienia odpowiedniego bezpieczeństwa danych i informacji znajdujących się w rejestrach publicznych
Kadrowe	mała liczba specjalistów z zakresu ICT powodująca niemożność korzystania przez jst z ich usług
	brak odpowiednich kompetencji w jst, w tym w odniesieniu do projektowania, zamawiania, budowania i utrzymywania systemów informatycznych, co powoduje opóźnienia w ich wdrażaniu i niską jakość stosowania nowych rozwiązań
Finansowe	zbyt duże koszty budowy i utrzymywania systemów oraz rejestrów publicznych
	brak środków finansowych
Inne	stosunkowo niski poziom wykorzystania usług publicznych przez obywateli wynikający z braku odpowiednich kompetencji cyfrowych
	niska skłonność do współpracy (partnerstwa publiczno-publicznego) między jst, co skutkuje dublowaniem wydatków, koniecznością powtarzania procedur przetargowych

Źródło: opracowanie własne na podstawie (Chaba, 2021; MC, 2019).

Osoby kierujące procesem tej transformacji w miastach także dostrzegają czynniki, które spowalniają adaptację ICT przez jst (tabela 8). Pogrupowano je, wyróżniając bariery: instytucjonalne, wdrożeniowe, ludzkie, techniczne i finansowe. Pomiędzy tymi barierami zachodzą określone zależności, niektóre z nich wynikają z innych. Na przykład niska skłonność do współpracy powoduje, że niektóre gminy samodzielnie wprowadzają określone rozwiązania (innowacje cyfrowe), co może wpływać na wzrost kosztów. W dalszej części opracowania odniesiono się do niektórych z tych barier. Bariery te powodują, że w inteligentnych miastach i wioskach powstają „silosy", co oznacza, że różne wydziały urzędu lub gminne placówki usługowe „zamykają się", wykonują własne, czasami sprzeczne z celami całej gminy zadania i nie dostrzegają korzyści płynących ze współpracy (Miazga i in., 2022).

Transformację utrudniają niejasne priorytety organów stanowiących i wykonawczych jst. Może to wynikać z tego, że często cyfryzacji lub jej braku

Tabela 8. Czynniki spowalniające transformację cyfrową samorządu gminnego

Grupa barier	Wyszczególnienie
Instytucjonalne	– niejasne priorytety organów jst – brak wizji, odwagi i zaangażowania liderów jst (wójtów, burmistrzów, prezydentów lub dyrektorów wydziałów) – brak podstaw prawnych transformacji cyfrowej (brak strategii transformacji cyfrowej) – brak współpracy między wydziałami i koordynacji wykonywanych przez nie działań – brak warunków do efektywnej pracy zespołowej – brak wsparcia ze strony liderów – nieodpowiednia struktura organizacyjna urzędów jst – brak pozwolenia ze strony przełożonych (i klientów) na błędy w trakcie transformacji cyfrowej – niewystarczająca zwinność (chęć zarządzania zmianą) urzędów jst – zmiany w organizacji i zarządzaniu nie nadążają za zmianą technologii – zmiany uwarunkowań prawnych i formalnych, np. reguł ochrony danych osobowych, lub dotyczących własności danych
Wdrożeniowe	– brak holistycznego spojrzenia na jst – braki w umiejętności zarządzania projektami – przyjmowanie nierealnych założeń projektowych – gwałtowana rewolucja zamiast stopniowej zmiany i racjonalnych wdrożeń – „wyspowe, punktowe" wdrażanie nowych rozwiązań oderwane od całego procesu świadczenia usługi – rozproszenie e-usług na różnych stronach/portalach urzędu – formalny, urzędowy sposób opisania e-usługi bez informacji jak „krok po kroku" przejść przez proces usługowy – pozorna transformacja cyfrowa („papierowe" e-usługi) – niewielka otwartość na nowe modele świadczenia usług – niewystarczające inwestycje w cyfryzację

cd. tabeli 8

Grupa barier	Wyszczególnienie
Ludzkie	– ograniczone zasoby kadrowe (brak programistów, specjalistów od cyberbezpieczeństwa) – niechęć pracowników do zmian – niewystarczające kompetencje władz gminy, pracowników samorządowych, mieszkańców i innych interesariuszy – niewystarczająca świadomość możliwości zastosowania ICT – niewielka otwartość na testowanie nowych rozwiązań – brak odbiorców usług w procesie projektowania – niewystarczające zaangażowanie mieszkańców jst (niechęć do testowania nowych rozwiązań i przekazywania merytorycznych opinii) – niewystarczające zaangażowanie interesariuszy zewnętrznych – niska świadomość mieszkańców na temat oferowanych usług cyfrowych – przeciążenie mieszkańców i innych interesariuszy wprowadzaniem nowych e-usług i ICT
Techniczne	– niedostosowanie technologii do potrzeb (inwestowanie „na wyrost" lub w rozwiązania, które nie będą mogły być ulepszane) – słabe zabezpieczenie serwerów – inwestowanie w „modne" rozwiązania (nieuzasadnione inwestycje w cyfrowe „gadżety") – niepełne wykorzystanie potencjału danych gromadzonych w jst (szczególnie w miastach) – brak standardów gromadzenia danych – niska interoperacyjność systemów i zbiorów danych – zależność jst od dostawców technologii
Finansowe	– wysokie koszty utrzymania infrastruktury służącej do gromadzenia gigadanych oraz ich analizy – brak wystarczających środków finansowych
Inne	– brak danych lub słaba jakość gromadzonych danych – problemy etyczne wynikające z gromadzenia danych (ograniczenie prywatności poprzez ciągłą inwigilację korzystających z usług) – zagrożenia bezpieczeństwa

Źródło: opracowanie własne na podstawie: (Ciupa, 2020, 2021; Guz, 2022; Matheus i in., 2021).

„nie widać". Z punktu widzenia części mieszkańców ważniejsze mogą być inwestycje w widoczną „gołym okiem" infrastrukturę techniczną i społeczną. Wójt i radni stają więc przed dylematem, czy w ogóle inwestować w nowoczesne technologie, a jeśli tak, to które z możliwych rozwiązań będzie najwłaściwsze dla wspólnoty, którą kierują. Wiąże się z tym brak wizji gminy w przyszłości oraz odwagi w wyznaczaniu kierunków jej rozwoju. Interesujące byłoby zbadanie, czy gminy opracowują strategie transformacji cyfrowej, w której określają jej zasady, a przynajmniej czy aktualizując strategie rozwoju, ujmują w nich „komponent" cyfrowy. Może to wpłynąć na brak wsparcia ze strony władz gminy osób, które chcą unowocześniać proces świadczenia

usług, oraz słabe zaangażowanie liderów lokalnych w zmianę (Miazga i in., 2022). Z dotychczasowych badań przeprowadzonych przez Obserwatorium Polityki Miejskiej Instytutu Rozwoju Miast i Regionów (IRMiR) wśród miast powyżej 5 tys. mieszkańców wynika, że 60% spośród uczestniczących w badaniu nie opracowało dokumentu strategicznego poświęconego transformacji cyfrowej (Miazga i in., 2022) lub jej wybranym elementom, np. zarządzaniu danymi (Łachowski i in., 2022). Jeżeli już zagadnienie transformacji cyfrowej się pojawia, to jest ono wpisane do „ogólnej" strategii jst. Brak dokumentu świadczy o tym, że do problematyki transformacji nie podchodzi się systemowo i długofalowo. Cyfryzacja gmin ma charakter „wyspowy", co oznacza, że wzrost stopnia stosowania nowych rozwiązań ICT następuje w sposób nieskoordynowany i przypadkowy (Miazga i in., 2022). Transformacja cyfrowa jest prowadzona fragmentarycznie, co oznacza, że rozwiązania cyfrowe pojawiają się albo tylko w urzędzie gminy, albo tylko w gminnych osobach prawnych lub jednostkach organizacyjnych, albo w niektórych wydziałach urzędu. Brakuje współpracy, wymiany informacji i koordynacji działań pomiędzy różnymi podmiotami gminnymi. Wynika to ze wspomnianego badania IRMiR, w którym wskazano, że tylko w co trzecim mieście wyznaczono osobę lub komórkę organizacyjną zajmującą się transformacją cyfrową w urzędzie, a w co siódmym – osobę lub komórkę odpowiedzialną za wprowadzenie rozwiązań z zakresu *smart city* (Miazga i in., 2022). Powoduje to, jak sądzimy, niepotrzebne dublowanie wydatków, np. na zakup nowych rozwiązań technologicznych, na zarządzanie nimi, na szkolenia, ale również traktowanie cyfryzacji jako „fanaberii", której nie trzeba poświęcać dużej uwagi.

Ciupa (2020) twierdzi, że poważną barierą omawianego procesu jest to, że zmiany organizacyjne i zarządcze w gminie nie nadążają za cyfryzacją. Jest to zarówno pochodną wcześniej wymienionych barier leżących po stronie jst, jak i tego, że niedoskonałe jest ustawodawstwo krajowe, które wymusza określony obieg dokumentów. Może to prowadzić do paradoksalnych sytuacji, że usługobiorca musi pobrać elektroniczny dokument z urzędu X po to, aby dołączyć go do wniosku składanego w placówce publicznej Y. Jest to związane z niewystarczającą zwinnością urzędu oraz brakiem pozwolenia na błędy (zarówno ze strony pracowników jst, liderów lokalnych, mieszkańców, jak i organów nadzoru i kontroli).

Kolejną grupę tworzą bariery pojawiające się na etapie implementacji nowych rozwiązań (bariery wdrożeniowe). Należy zwrócić tu uwagę na brak umiejętności holistycznego spojrzenia na gminę i zastanowienia się, w jaki sposób dany projekt wpłynie na jednostki organizacyjne gminy, gminne osoby prawne, ale również na mieszkańców, podmioty gospodarcze i innych interesariuszy, którzy mają korzystać z proponowanych rozwiązań.

W dalszym ciągu nie w każdej gminie prawidłowo zarządza się projektem (Ciupa, 2020; Guz, 2022). W związku z tym przyjmuje się nierealne założenia dotyczące np. przebiegu procesu cyfryzacji. Wiąże się to też z brakiem otwartości na zmianę modelu świadczenia lokalnej usługi publicznej. Warto sprawdzić, czy nie byłoby efektywniejsze wykonywanie danej e-usługi we współpracy między jst lub w formule partnerstwa publiczno-prywatnego.

Ciupa (2020) zwraca też uwagę na to, że gminy starają się finansować transformację cyfrową z zewnętrznych środków (w szczególności ze źródeł europejskich), które pojawiają się i muszą być wykorzystane w określonym czasie. W wielu gminach obserwuje się rewolucyjne, gwałtowne zmiany zamiast wprowadzania racjonalnych zmian w kilku etapach. Powstaje wtedy ryzyko, że gmina nie poświęci dostatecznie dużo czasu na zaplanowanie całego procesu. Należy zwrócić uwagę na to, że nawet jeżeli gminy oferują mieszkańcom e-usługi, to często są one zlokalizowane na różnych stronach, portalach urzędu. Mankamentem procesu usługowego jest brak możliwości wyszukania e-usługi z poziomu głównej strony internetowej urzędu oraz formalny, urzędowy sposób opisania e-usługi bez informacji, jak „krok po kroku" przejść przez proces usługowy (Miazga i in., 2022).

Trzeba też pamiętać, że sama elektronizacja dotychczas „papierowej" usługi[17], bez zmiany procesu jej świadczenia, nie jest transformacją cyfrową, lecz co najwyżej digitalizacją dokumentu. O transformacji można mówić wtedy, gdy przekłada się „papierowe" procedury na rozwiązania elektroniczne po to, aby zmienić (uprościć) proces świadczenia usług. Prawdopodobnie wiąże się to również z „wyspowymi" wdrożeniami nowych technologii w oderwaniu od zmiany procesu usługowego oraz w oderwaniu od zmian w innych jednostkach. Powoduje to powstanie „papierowych" e-usług, czyli takich, w których np. wniosek czy podanie można wypełnić elektronicznie, ale potem trzeba ten wniosek wydrukować i dostarczyć do urzędu, albo wniosek drukowany jest w urzędzie i następuje jego „papierowy" obieg.

Rozpatrując bariery transformacji cyfrowej jst, warto też wspomnieć o niewystarczających inwestycjach w cyfryzację. Wiąże się to z brakiem wizji gminy w przyszłości oraz traktowaniem tych inwestycji jako kosztu, a nie korzyści w perspektywie wielu lat, w tym o charakterze finansowym – wynikającym z oszczędności czasu, papieru, pracy urzędników. Przyczyną niewystarczających inwestycji jest brak środków finansowych, co potwierdzają badania przeprowadzone wśród gmin w Polsce w latach 2020–2022 (Chodakowska i in., 2022; Miazga i in., 2022).

Grupa barier personalnych pokrywa się częściowo z ograniczeniami wskazanymi przez stronę rządową. Można się spotkać z niedostatecznymi kom-

[17] Metafory tej użyto w kontekście tradycyjnej, osobistej wizyty w urzędzie, choć można ją też odnosić do wniosku/podania/listu przygotowanego na papierze.

petencjami władz lokalnych i pracowników samorządowych, na co wskazują zarówno badania krajowe (Chodakowska i in., 2022), jak i zagraniczne (Hatcher i in., 2020), ograniczone kompetencje wykonawców (podmiotów „instalujących" nowe technologie), jak i odbiorców usług (mieszkańców, podmiotów gospodarczych, szczególnie przedsiębiorców mikro i małych). W każdej z tych grup można się też spotkać z brakiem skłonności do korzystania z internetu, brakiem świadomości w odniesieniu do tego, jakie możliwości dają nam nowe technologie oraz z niechęcią do testowania (i późniejszego stosowania) tych technologii w codziennych kontaktach z administracją gminną. Obserwuje się też niechęć pracowników jst do zmian, co może być pochodną ich niskich kompetencji cyfrowych (Łachowski i in., 2022). Bolączką gmin jest także pomijanie interesariuszy (mieszkańców, przedsiębiorców) w pracach nad planowaniem nowej usługi, z czym wiąże się odwieczne pytanie, czy usługę oferuje się lub usprawnia dla samego usprawniania, czy też w taki sposób, aby była ona jak najprostsza, jak najbardziej dogodna dla obywatela. Bez udziału interesariuszy trudne będzie wychwycenie błędów i niedogodności na etapie pilotażu. Ponadto może to wpłynąć na brak zainteresowania odbiorców w korzystaniu z e-usługi, która pozostanie „martwa", więc efektywność jej świadczenia będzie niewielka.

Za Ciupą (2020) w grupie barier technicznych należy wskazać niedostosowanie technologii do rzeczywistych potrzeb urzędu i mieszkańców. Możne to być zarówno przygotowanie zbyt infantylnej usługi, jak i rozwiązania zbyt zaawansowanego. Istnieje też obawa, że powstanie swoista moda na niektóre rozwiązania technologiczne i gminy będą chciały mieć u siebie modne „gadżety". Tymczasem w transformacji cyfrowej nie chodzi o epatowanie nowoczesnością, lecz o usprawnienie działania gmin. Wspomniany autor twierdzi też, że transformacja cyfrowa nie jest jeszcze zaawansowana, ponieważ wprowadzane rozwiązania nie wykorzystują potencjału danych gromadzonych w różnych gminnych instytucjach, na co zwraca uwagę także zespół IRMiR (Łachowski i in., 2022). Jest to konsekwencją braku standardu, według którego dane te są gromadzone, oraz braku interoperacyjności[18] (współpracy, wymiany danych) różnych systemów gromadzenia danych. Należy też zwrócić uwagę na asymetrię informacji pomiędzy gminą a dostawcami ICT. Druga grupa, mająca większą wiedzę techniczną i technologiczną, może – kierując się maksymalizacją zysku, a nie dobrem wspólnym – „wymóc" na jst zakup określonej technologii. Warto

[18] Interoperacyjność to „zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych" (Ustawa, 2005).

tu dodać jeszcze jedną determinantę. Punktem wyjścia do transformacji cyfrowej jst są bowiem możliwości prostego i szybkiego komunikowania się z urzędami i instytucjami gminnymi (Tomaszewicz i Buko, 2015). Potrzebne są tu nie tylko świadomość, umiejętności, ale także sprzęt, a przede wszystkim sieć internetowa o dużej przepustowości.

PRZYCZYNY, KONSEKWENCJE I EWOLUCJA NIERÓWNOŚCI CYFROWYCH

2.1. Nierówności cyfrowe problemem XX i XXI wieku

Wszystkie zmiany niosą ze sobą ryzyko wystąpienia ich nierównomiernego wdrażania, powodującego w konsekwencji rożnego rodzaju nierówności socjoekonomiczne. Literatura przedmiotu obfituje w wiele pozycji w tym zakresie, które są przede wszystkim poświęcone badaniom nad nierównościami dochodowymi i majątkowymi analizowanymi już od początku XX w.[19] W ostatnich latach zarówno badacze, jak i decydenci na szczeblach lokalnym, krajowym oraz ponadnarodowym zwracają coraz większą uwagę na kwestię nierówności szans ekonomicznych (np. bezrobocia) czy społecznych (np. edukacji) (Bartak, 2019; KE, 2017b), ale też problemy wynikające z nierównomiernego powstawania i dostępu do sieci internetowej. Pod koniec XX w. internet postrzegano jako narzędzie, za pomocą którego dojdzie do poprawy sytuacji życiowej osób o najniższych dochodach, co w konsekwencji wpłynie na ograniczenie nierówności społecznych. Szansy tej upatrywano w obniżeniu kosztów i możliwości szybszego dotarcia do informacji i wiedzy. Sądzono, że wpłynie to na wyrównanie szans w dostępie do wykształcenia, lepszej pracy, większych dochodów (Anderson i in., 1997). Przypuszczano także, że internet przyczyni się do wzrostu konkurencyjności i demokratyzacji życia społecznego (KBN, 2003). W przeciwstawnym nurcie podawano w wątpliwość niwelowanie nierówności społecznych dzięki internetowi, co przyczyniło się do podjęcia wielu badań w tym zakresie, których analizę przeprowadzili m.in. DiMaggio i in. (2021) oraz Graham (2011). Po kilkudziesięciu latach od powstania internetu wiemy, że dostęp do niego umożliwił tworzenie ogromnego bogactwa w rekordowo krótkim czasie. Bogactwa, które w znacznej mierze zostało skoncentrowane wokół niewielkiej liczby osób, przedsiębiorstw i państw, co wpływa na powiększanie różnic w produktywności i wzroście gospodarczym między bogatymi a biednymi (UN, 2019), zamiast doprowadzać do ich ograniczenia.

[19] Między innymi Atkinson (1970), Costa iPérez-Duarte (2019), Przekota (2021).

2.2. Pierwszy poziom nierówności cyfrowych

Nierówności społeczne wynikające z postępu cyfrowego określono w literaturze mianem wykluczenia cyfrowego (*digital divide*) rozumianego jako różnica pomiędzy jednostkami, które mają dostęp do internetu i komputera, a jednostkami, które tego dostępu nie mają (Graham, 2011; Philips i in., 2010; van Dijk, 2006; Warschauer, 2004). Zjawisko to stało się przedmiotem badań zajmujących się wyjaśnieniem przestrzennego zróżnicowania na poziomie krajowym i lokalnym. Wykorzystując wskaźnik dostępu do sieci, zaobserwowano, że społeczeństwa państw rozwiniętych (określane również mianem hiperrozwiniętych cyfrowo) cieszą się znacznie większą dostępnością do internetu aniżeli społeczności państw najsłabiej rozwiniętych. W 2019 r. średnie wskaźniki kształtowały się odpowiednio na poziomach 87% i 19%; UN, 2019). W Unii Europejskiej zróżnicowanie w poziomie wykluczenia cyfrowego jest zdecydowanie mniejsze i z roku na rok maleje, jednak mimo to w 2021 r. sięgało około 15 pp. (tabela 9).

W latach 2019–2021 największy odsetek gospodarstw domowych mających dostęp do sieci odnotowano w Holandii (średnio 99%), natomiast najmniejszy – w Bułgarii (średnio 84%). W 2021 r. średnia unijna wskaźnika wyniosła 92% i była zbieżna z wartością analogicznego wskaźnika dla Polski. Warto jednak zaznaczyć, że dostępność do internetu w Polsce w 2021 r. uległa poprawie o około 5 pp. względem 2019 r. i była kontynuacją trendu wzrostowego z poprzednich lat. Na podstawie badań za lata 2002–2007 na 154 gospodarkach z całego świata Ayanso i in. (2013) podzielili je na dwie grupy – państwa liderów i państwa doganiające liderów. Autorzy wykazali, że zaledwie dziewięć państw zdołało zmienić swój status na lidera – cztery państwa z Azji (Bahrajn, Brunea Darussalam, Katar i Zjednoczone Emiraty Arabskie) oraz pięć państw z Europy (Bułgaria, Chorwacja, Łotwa, Litwa i Polska).

Zarówno wśród państw rozwiniętych, jak i państw słabo rozwiniętych, obserwuje się „linie podziału cyfrowego" – w skali regionalnej i lokalnej (Gómez Barroso i Pérez Martínez, 2004). Dostęp do internetu jest mniejszy w regionach wiejskich aniżeli w regionach miejskich, co świadczy o większym wykluczeniu cyfrowym osób zamieszkujących tereny wiejskie (Greenstein i Prince, 2006; UN, 2019). Townsend i in. (2013) argumentowali, że zwiększenie dostępu szerokopasmowego może zmniejszyć rosnący podział cyfrowy, społeczny i gospodarczy między obszarami wiejskimi i miejskimi. Choć łącze szerokopasmowe znacząco zyskuje na znaczeniu w opiece zdrowotnej, edukacji, dostępie do informacji, biznesie, usługach, administracji publicznej czy rekreacji, nie jest ono zapewniane w takim samym stopniu na obszarach wiejskich i w miastach. Analogiczne wnioski wynikają z analizy odsetka lokali mieszkalnych z dostępem do

Tabela 9. Odsetek gospodarstw domowych z dostępem do internetu w państwach UE w latach 2019–2021

Państwo	Lata		
	2019	2020	2021
UE-27	90	91	92
Austria	90	90	95
Belgia	90	91	92
Bułgaria	75	79	84
Chorwacja	81	85	86
Cypr	90	93	93
Czechy	87	88	89
Dania	95	95	96
Estonia	90	90	92
Finlandia	94	96	97
Francja	90	b.d.	93
Grecja	79	80	85
Hiszpania	91	95	96
Holandia	98	97	99
Irlandia	91	92	97
Litwa	82	82	87
Luksemburg	95	94	99
Łotwa	85	90	91
Malta	86	90	91
Niemcy	95	96	92
Polska	87	90	92
Portugalia	81	84	87
Rumunia	84	86	89
Słowacja	82	86	90
Słowenia	89	90	93
Szwecja	96	94	93
Węgry	86	88	91
Włochy	85	88	b.d.

Źródło: opracowanie własne na podstawie danych z bazy Eurostat.

internetu szerokopasmowego w Polsce w latach 2017–2020 na poziomie gmin[20] (tabela 10).

Tabela 10. Odsetek lokali mieszkalnych z dostępem do internetu szerokopasmowego na poziomie gmin w Polsce w latach 2017–2020 (w %)

Typ gmin / rok	2017	2018	2019	2020
Gminy miejskie	95	96	97	97
Gminy wiejskie	70	71	73	75
Gminy miejsko-wiejskie	81	82	84	84
Średnia[a]	82	83	85	86

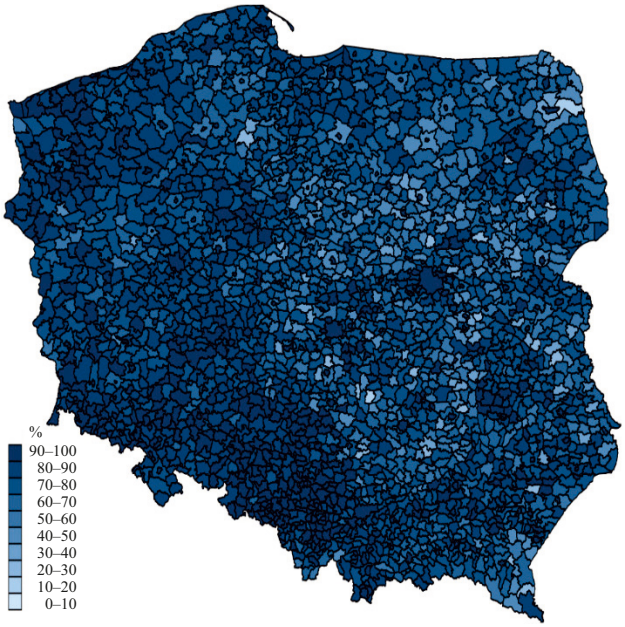
[a] Różnica między danymi publikowanymi przez Urząd Komunikacji Elektronicznej i Eurostat wynika z innej metodologii obliczania – w danych Eurostat jest także uwzględniony dostęp do internetu poprzez smartfona.

Źródło: opracowanie własne na podstawie danych Urzędu Komunikacji Elektronicznej.

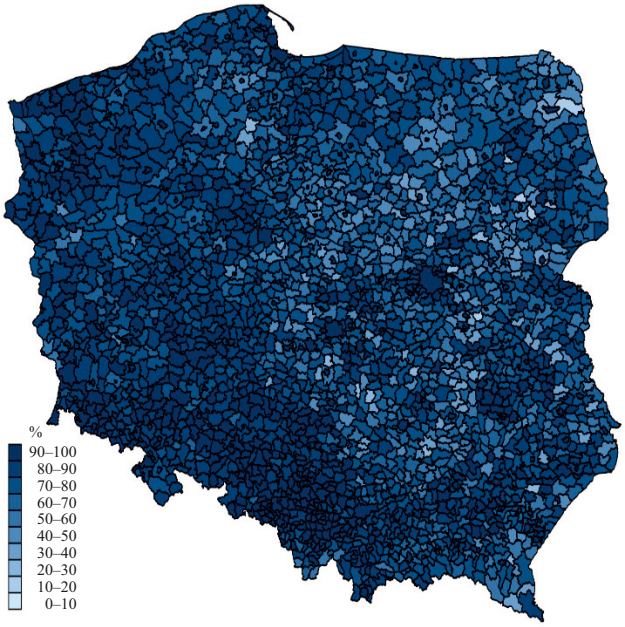
W badanych latach średnio ponad 95% mieszkańców gmin miejskich miało dostęp do szerokopasmowego internetu przy odchyleniu standardowym około 3,5 pp. Najwyższe wskaźniki, tj. powyżej 99,9%, odnotowano w gminach Kolno, Bukowno, Bielsk Podlaski, Starachowice, Pionki, Olsztyn, Lędziny, Hajnówka i Skarżysko-Kamienna. Natomiast najniższe, tj. między 42,8 a 50%, w gminach Sokołów Podlaski, Żory, Tczew i Obrzycko. W przypadku gmin miejsko-wiejskich średnio 83% lokali mieszkalnych miało dostęp do szerokopasmowego internetu, jednak przy większym odchyleniu standardowym aniżeli w przypadku gmin miejskich, bo wynoszącym około 11 pp. Wartości wskaźnika powyżej 99,9% odnotowano w gminach Kety, Brzeszcze, Zator i Suchedniów. Wśród gmin, których wskaźnik był najmniejszy i wyniósł poniżej 10 %, tj. między 2,3% a 9,8%, należy wskazać odpowiednio Kosów Lacki, Błażową, Szydłów i Tyczyn. Gminy wiejskie to z kolei jednostki ze średnio najniższym odsetkiem lokali mieszkalnych z dostępem do internetu wynoszącym 73%, co jest wynikiem o ponad 20 pp. niższym aniżeli w przypadku gmin miejskich. W grupie gmin wiejskich występowało największe zróżnicowanie w zakresie nierówności w dostępie do sieci (odchylenie standardowe wyniosło około 16%), jednak w latach 2017–2020 zaobserwowano średni największy przyrost wskaźnika. Warto jednak zauważyć, że aż 22 gminy mogły pochwalić się siecią internetową obejmującą ponad 99,9% mieszkańców, z czego sześć gmin (Lubenia, Chmielnik, Przeciszów, Radzanów, Klwów i Dynów) osiągnęło wartość 100%. Jednocześnie wartość wskaźnika dostępności do sieci dla 12 gmin wyniosła poniżej 10%, z czego w trzech gminach (Sokołów Podlaski, Jabłonna

[20] Zgodnie z podziałem administracyjnym gmin według stanu na 31 grudnia 2020 r. w Polsce funkcjonowały 302 gminy miejskie (wraz z miastami na prawach powiatu), 1533 gminy wiejskie oraz 642 gminy miejsko-wiejskie.

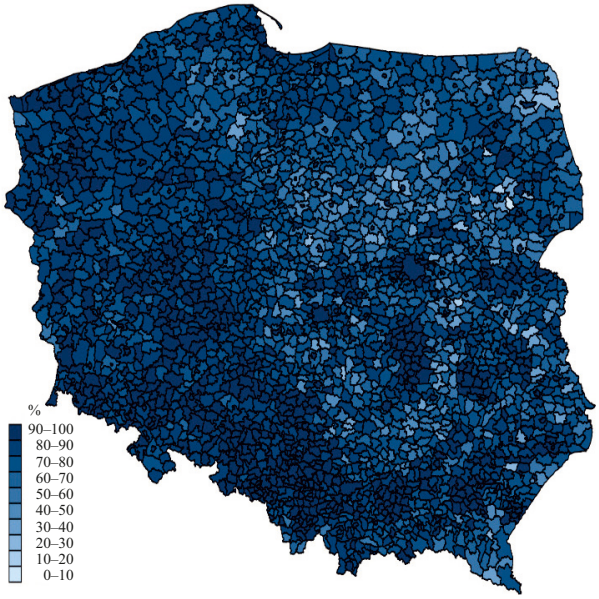
2017


%
90–100
80–90
70–80
60–70
50–60
40–50
30–40
20–30
10–20
0–10

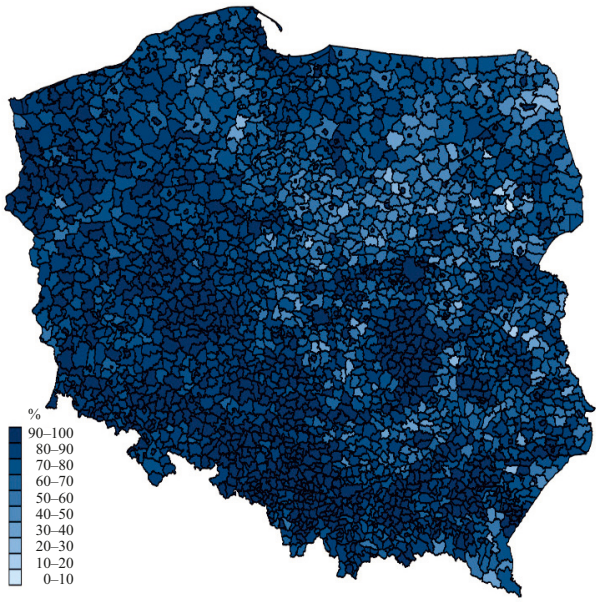
2018


%
90–100
80–90
70–80
60–70
50–60
40–50
30–40
20–30
10–20
0–10

2019



2020

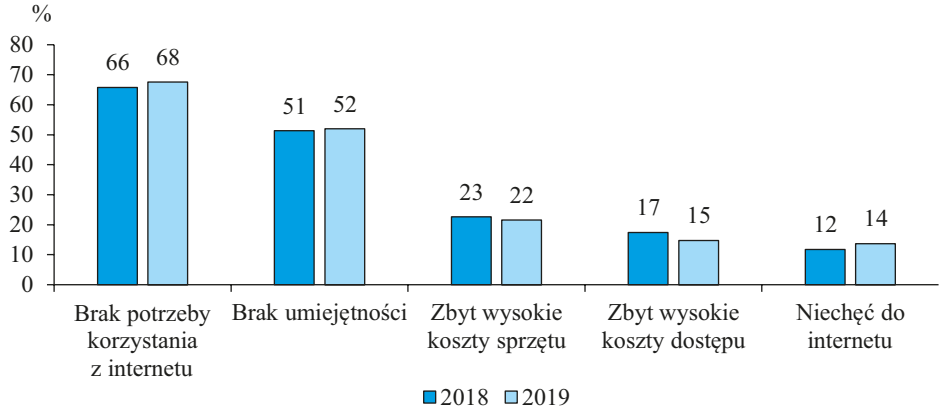


Rysunek 5. Odsetek lokali mieszkalnych z dostępem do szerokopasmowego internetu w gminach w latach 2017–2020

Źródło: opracowanie własne na podstawie danych Urzędu Komunikacji Elektronicznej i Głównego Urzędu Geodezji i Kartografii (Państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju, https://dane.gov.pl/pl/dataset/726,panstwowy-rejestr-granic-i-powierzchni-jednostek-podziaow-terytorialnych-kraju/resource/29515/table).

Lacka, Sterdyń) mniej niż 1% gospodarstw domowych miało dostęp do szerokopasmowego internetu.

Zróżnicowanie przestrzenne w odsetku lokali mieszkalnych z dostępem do szerokopasmowego internetu w polskich gminach w latach 2017–2020 prezentuje rysunek 5. Wnioski płynące z analizy danych oraz map są zbieżne z wynikami badań Gómeza Barroso i Péreza Martínez (2004), ponieważ można na nich dostrzec „linie podziału cyfrowego". Gminy południowo-zachodniej Polski mają średnio wyższe wskaźniki dostępu do szerokopasmowego internetu aniżeli gminy w Polsce północno-wschodniej. Mieszkańcy tej drugiej części Polski są zatem w większym stopniu zagrożeni wykluczeniem cyfrowym. Zauważyć można koncentrację zmiennej wokół dużych miast i obszarów z dużym zagęszczeniem ludności, co potwierdzają dane dotyczące większego wykluczenia cyfrowego na obszarach wiejskich. Należy jednak zwrócić uwagę na stopniowe zmniejszanie wykluczenia cyfrowego, zwłaszcza w gminach z województwa mazowieckiego. Główny Urząd Statystyczny w Polsce przeprowadził badanie, którego celem było zweryfikowanie przyczyn braku dostępności do internetu. Wyniki przedstawia rysunek 6.



Rysunek 6. Przyczyny braku dostępu do internetu w polskich gospodarstwach domowych

Źródło: opracowanie własne na podstawie (GUS, 2019).

W latach 2018–2019 ponad 2/3 ankietowanych uznało, że nie miało potrzeby korzystania z internetu. Brak potrzeby korzystania z internetu w rzeczywistości może wynikać z szeregu innych czynników, takich jak brak świadomości możliwości i korzyści, jakie daje dostęp do sieci (np. e-usługi, e-zakupy, samorozwój), ale też obawa przed nieznanym czy negatywne opinie lub doświadczenia – średnio 13% respondentów wyrażało niechęć do internetu. Połowa ankietowanych wskazała na brak umiejętności, ponad 20% – na zbyt wysokie koszty sprzętu

umożliwiającego korzystanie z internetu i niecałe 20% – na zbyt wysokie koszty dostępu do internetu.

Miara dostępności do internetu stała się pierwszym narzędziem do pomiaru wykluczenia cyfrowego, dzięki której możliwe stało się wyodrębnienie obszarów geograficznych zamieszkiwanych przez osoby wykluczone cyfrowo (DiMaggio i in., 2021). Tym samym problem dostępu do internetu jest obecnie uważany za pierwszy poziom nierówności cyfrowych (*first-level digital divide*).

2.3. Drugi i trzeci poziom nierówności cyfrowych

Wraz z nieustannym rozwojem sieci internetowej pojawiła się konieczność zbadania wykluczenia cyfrowego wykraczającego poza pomiar zorientowany jedynie na analizę wskaźnika dostępności do internetu – zwłaszcza w krajach rozwiniętych, gdzie problem ten został zminimalizowany (Ferreira i in., 2021). Argumentowano, że wykluczenie cyfrowe nie wynika tylko i wyłącznie z podziału na tych, którzy mają dostęp do sieci, i tych, którzy tego dostępu nie mają, ponieważ pomimo powszechnego dostępu do internetu w krajach rozwiniętych wykluczenie cyfrowe utrzymuje się w innych formach. Biorąc pod uwagę, że analiza pierwszego poziomu nie wystarczyła do całkowitego zrozumienia pojęcia wykluczenia cyfrowego, coraz więcej badaczy podjęło się wyodrębnienia jego kolejnych poziomów (Ferreira i in., 2021).

Hargittai (2002) zauważyła, że należało dokonać rozróżnienia nierówności w dostępie do internetu i nierówności w umiejętnościach korzystania z niego. Ten nowy poziom nierówności cyfrowych określono mianem nierówności uczestnictwa, ponieważ wskazuje na różnice między grupami ludzi w zakresie ich umiejętności niezbędnych do efektywnego korzystania z internetu. Określenie drugiego poziomu nierówności cyfrowych (*second-level digital divide*) było możliwe dzięki zauważeniu, że nawet przy równych poziomach dostępu ludzie z różnych klas i grup nie mają tych samych umiejętności i wiedzy, aby w ten sam sposób korzystać z zasobów cyfrowych, co prowadzi do różnych poziomów użytkowania (van Dijk, 2006). Mianowicie ze względu na różnice w umiejętnościach i wiedzy niektóre osoby czerpią z technologii znacznie więcej korzyści niż inne, co w konsekwencji prowadzi do pogłębiania nierówności cyfrowych (Zillien i Hargittai, 2009). Należy zatem zauważyć, że drugi poziom nierówności cyfrowych obejmuje zarówno różnice w umiejętnościach cyfrowych, jak i różnice w wykorzystywaniu zasobów internetu (Scheerder i in., 2017).

Doskonały przegląd badań nad czynnikami wpływającymi na drugi poziom nierówności cyfrowych przedstawili Scheerder i in. (2017). Według przeprowa-

dzonej metaanalizy najliczniejszą grupę determinant sprawdzonych przez autorów przeanalizowanych badań stanowiły czynniki socjodemograficzne i społeczno-ekonomiczne. Znacznie rzadziej analizowano przyczyny motywacyjne, osobowe czy kulturowe.

Wiek jest jednym z najważniejszych faktorów wpływających na kompetencje cyfrowe i sposób korzystania z internetu (Brandtzæg i in., 2011; Wasserman i Richmond-Abbott, 2005). Różnice pokoleniowe między starszymi a młodszymi użytkownikami internetu są widoczne w wielu badaniach. Starsi użytkownicy są grupą znacznie częściej wykluczoną cyfrowo – zarówno pod względem korzystania, jak i dostępności do internetu (Karahasanović i in., 2009). Potwierdzają to także wyniki analiz przeprowadzonych przez GUS (2019). Wynika z nich, że im młodsi respondenci, tym większy odsetek korzystających z sieci. Według badań Yuan i Jia (2021) starsi ludzie rzadziej korzystają z internetu, ponieważ są mniej zdolni do uczenia się i zapamiętywania nowych rzeczy niż osoby młodsze, a także boją się utraty pieniędzy przez m.in. zapomnienie kodu płatności, wprowadzenie niewłaściwej kwoty lub zostanie oszukanym przez innych. Z kolei Millward (2003) argumentuje, że dla osób starszych użyteczność internetu jest związana nie tylko z dostępnością do sieci. Brak umiejętności korzystania z internetu wśród osób starszych prowadzi bowiem do opinii, że technologie informacyjne i komunikacyjne są dla młodych, co powoduje utrzymywanie braku zainteresowania korzystaniem z internetu po stronie popytowej, a więc ze strony osób starszych. Wykluczenie cyfrowe osób starszych stało się szczególnie ważnym problemem od momentu wystąpienia pandemii COVID-19, która unaoczniła nierówny dostęp do technologii cyfrowych wśród ludzi w różnym wieku. Osoby starsze są bardziej narażone na wykluczenie cyfrowe i doświadczają barier w dostępie do towarów i usług, które coraz częściej można zamawiać online. Wykluczenie cyfrowe ogranicza możliwości aktywnego i zdrowego starzenia się, w tym udziału w życiu społecznym i gospodarczym (EKG, 2021). Wykorzystanie technologii informacyjnych i mediów społecznościowych w celach społecznych było bowiem ważne nie tylko w przypadku izolacji wynikającej z obostrzeń spowodowanych pandemią COVID-19, ale także w przypadku osób z ograniczoną mobilnością (Clark i Moloney, 2020). Wyzwaniem jest wzmocnienie pozycji osób starzejących się poprzez zapewnienie dostępu do technologii cyfrowych, jak i zwiększenie ich umiejętności cyfrowych. Należy zapewnić przyjazne i adekwatne do wieku usługi cyfrowe, a także etyczne i bezpieczne środowiska cyfrowe, które obejmują różnorodność starzejących się populacji. Technologie cyfrowe mogą pomagać w nauce nowych umiejętności, ułatwiać interakcje społeczne, wspierać niezależne i autonomiczne życie oraz usprawniać procesy zarządzania i świadczenia usług zdrowotnych i opieki społecznej, zwłaszcza dla starzejących się populacji (EKG, 2021). Problem starzejącego się społeczeństwa dotyczy już również Pol-

Tabela 11. Statystyki mediany wieku ludności w powiatach w Polsce w latach 2018–2020

Rok	Średnia	Odchylenie standardowe	Minimum	Maksimum
2018	40,33	1,82	3 4.00	47,00
2019	41,22	1,83	34,80	47,70
2020	41,58	1,83	35,10	48,00

Źródło: opracowanie własne na podstawie informacji Banku Danych Lokalnych (https://bdl.stat.gov.pl/bdl/start).

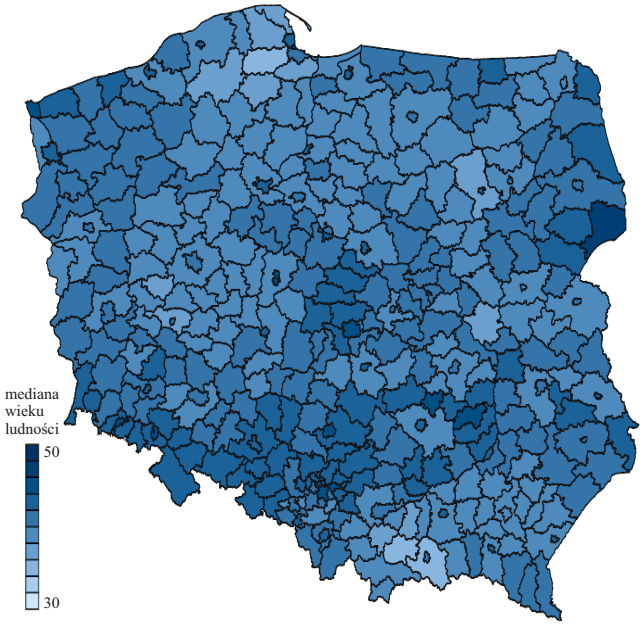
ski. Analizę przestrzenną mediany wieku ludności w polskich powiatach[21] w latach 2018–2020 przedstawia rysunek 7, a podstawowe statystyki tabela 11.

Średnia mediana wieku ludności w powiatach w Polsce wzrastała od 40,3 lat w 2018 r. do 41,6 lat w 2020 r. Najniższą wartość, tj. poniżej 37 lat, odnotowano w powiatach: kartuskim, limanowskim i nowosądeckim. Natomiast najwyższą medianą wieku, tj. powyżej 46 lat, charakteryzowały się powiaty: m. Jelenia Góra, hajnowski, m. Sopot. Nawiązując do wcześniejszej analizy przestrzennej odsetka lokali mieszkalnych z dostępem do internetu, w przypadku mediany wieku brak jest wyraźnych linii podziału. Powiaty z wyższą medianą są relatywnie równomiernie rozproszone na całym terytorium Polski, z pewną koncentracją w powiatach przy granicy zachodniej, północnej i wschodniej oraz w okolicy Śląska i w centrum Polski. Relatywnie wysokie różnice w wartościach skrajnych median wieku w poszczególnych powiatach, sięgające około 13 lat, mogą wskazywać na konieczność podjęcia działań i wdrożenia programów zmierzających do zmniejszenia wykluczenia cyfrowego nie tylko na poziomie krajowym, ale i na poziomie lokalnym, samorządowym.

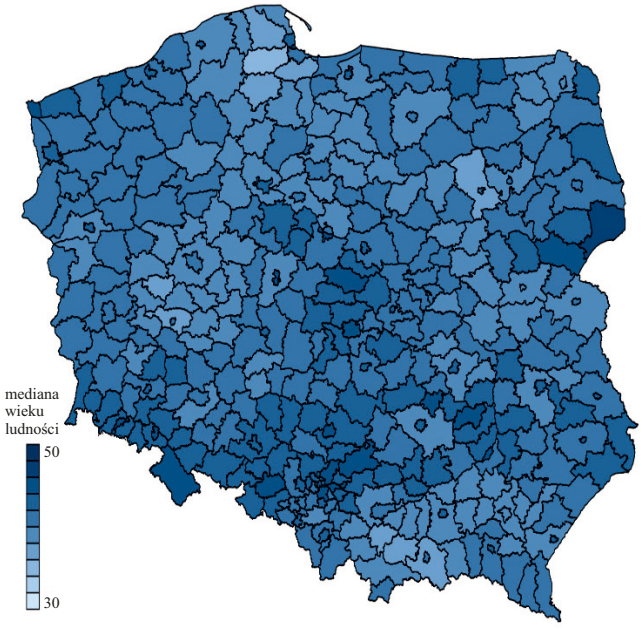
Drugim czynnikiem badanym w literaturze pod kątem wpływu na nierówności cyfrowe drugiego poziomu jest dochód. Ferreira i in. (2021) wskazali, że obszary silne gospodarczo i zamieszkiwane przez osoby o wysokim dochodzie są obszarami o lepszej dostępności do sieci. Ponadto dochód ma najsilniejszy potencjał wzajemnego związku przyczynowo-skutkowego: niskie dochody prowadzą do niekorzystania z internetu i zwiększania nierówności cyfrowych, co z kolei może prowadzić do niższych dochodów (Martin i Robinson, 2007). Według wcześniejszych badań (Zhang, 2013) koszt usług cyfrowych stanowi barierę dostępu zwłaszcza dla osób o niskich dochodach, a jej obniżenie skłoniłoby do zwiększenia częstotliwości korzystania z sieci. Ze względu na nieustanny rozwój technologii, spadek cen sprzętu i kosztu dostępu do sieci, dla krajów rozwijających się ważny jest wybór odpowiednich technologii cyfrowych i ich

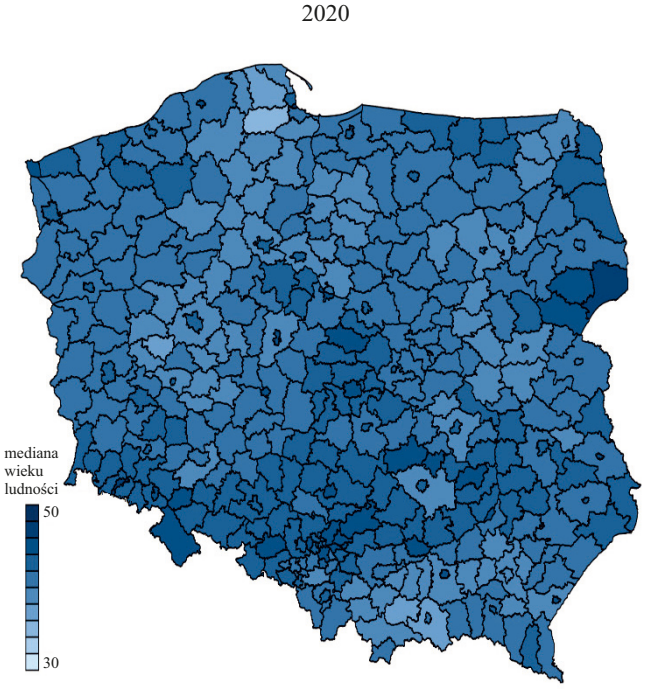
[21] Bank Danych Lokalnych publikuje dane na temat mediany wieku ludności na poziomie powiatów.

2017



2018





Rysunek 7. Mediana wieku ludności w powiatach w latach 2018–2020

Źródło: opracowanie własne na podstawie danych Banku Danych Lokalnych (https://bdl.stat.gov.pl/bdl/start) i Głównego Urzędu Geodezji i Kartografii (Państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju, https://dane.gov.pl/pl/dataset/726,panstwowy-rejestr-granic-i-powierzchni-jednostek-podziaow-terytorialnychkraju/resource/29515/table).

wdrożenie w odpowiednim czasie. Z punktu widzenia niwelowania nierówności społecznych spowodowanych wykluczeniem cyfrowym ważne jest równomierne wdrażanie technologii cyfrowych, by wiele osób mogło sobie na nie pozwolić i korzystać w sposób spełniający podstawowe wymagania.

Pandemia COVID-19 uwypukliła problem nierówności dochodowych wpływających na wykluczenie cyfrowe. Zmiana trybu nauczania w systemie oświaty ze stacjonarnego na zdalne spowodowała konieczność wyposażenia wszystkich uczniów w sprzęt odpowiedni do łączenia się z siecią i uczestnictwa w lekcjach online. Mimo relatywnie wysokiego odsetka lokali mieszkalnych z dostępem do internetu w Polsce okazało się, że liczba sprzętu komputerowego jest zbyt mała, by umożliwić w pełni wszystkim dzieciom naukę w trybie online. Problem wynikał m.in. z powodu potrzeby współdzielenia sprzętu z rodzeństwem czy rodzicami pracującymi zdalnie. Wynika stąd, że grupy uważane do czasu pandemii za wolne od wykluczenia cyfrowego zostały nim dotknięte (Federacja Konsumen-

tów, 2021), a sam wskaźnik dostępności do internetu faktycznie jest absolutnie niewystarczający do określenia nierówności cyfrowych. W badaniu przeprowadzonym w kwietniu 2020 r. przez Instytut Spraw Publicznych, Fundację Rozwoju Społeczeństwa Obywatelskiego oraz Fundację Orange dyrektorzy ponad 646 szkół podstawowych oraz ponadpodstawowych stwierdzili, że wykluczenie cyfrowe w największym stopniu negatywnie wpływa na edukację zdalną dzieci i młodzieży. Wskazali przede wszystkim na brak dostępu do właściwych urządzeń (81%), a także brak umiejętności obsługiwania tych urządzeń oraz oprogramowania (71%). Analogicznymi problemami zostali dotknięci także nauczyciele (Federacja Konsumentów, 2021).

Mimo rozwoju technologii, pojawiania się nowych urządzeń umożliwiających korzystanie z sieci (smartfony, tablety) koszt urządzeń pozostaje nadal relatywnie wysoki w przypadku gospodarstw domowych o najniższych dochodach (poniżej 2500 zł netto). Stanowią one największą grupę wśród gospodarstw domowych bez dostępu do internetu (Federacja Konsumentów, 2021). Zasadna jest zatem analiza wynagrodzeń w Polsce z uwzględnieniem aspektu przestrzennego. Dane statystyczne dotyczące średniego przeciętnego miesięcznego wynagrodzenia brutto w cenach z 2020 r. prezentuje tabela 12. W latach 2017–2020 średnia dla kraju wzrosła z poziomu 4108 zł do 4774 zł, a rozpiętość pomiędzy wartościami minimalnymi a maksymalnymi wyniosła średnio około 5 tys. zł brutto.

Tabela 12. Statystyki średniego przeciętnego miesięcznego wynagrodzenia brutto w cenach z 2020 r. w powiatach w Polsce w latach 2017–2020 (w zł)

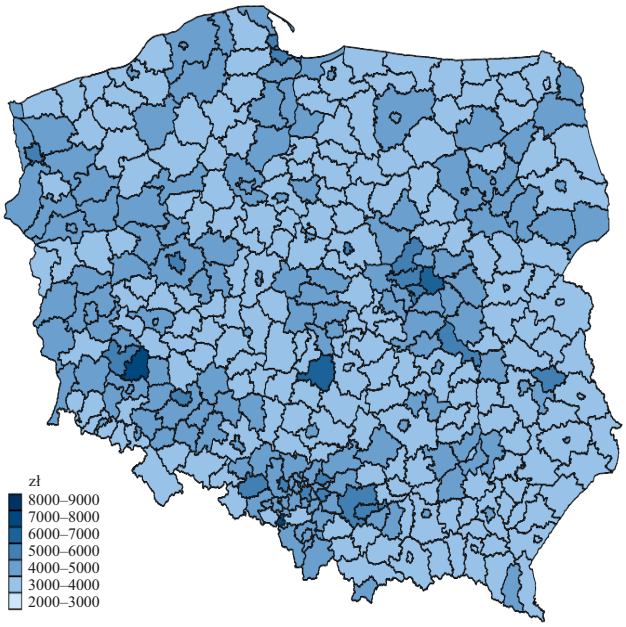
Rok	Średnia	Odchylenie standardowe	Minimum	Maksimum
2017	4108	549	3138	7968
2018	4305	584	3309	8441
2019	4545	600	3619	8637
2020	4774	581	3872	8920

Źródło: jak w tabeli 11.

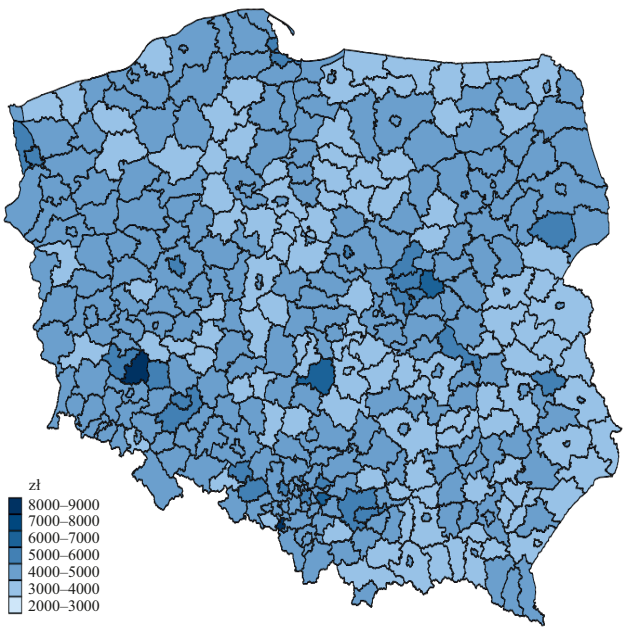
Oprócz standardowej analizy statystycznej warto przedstawić przestrzenne zróżnicowanie przeciętnego miesięcznego wynagrodzenia brutto w cenach realnych (baza = 2020) w powiatach w Polsce w latach 2017–2020 (rysunek 8).

Analizując średnie przeciętne miesięczne wynagrodzenie brutto w powiatach w latach 2017–2020, jako jednej z miar zagrożenia wykluczeniem cyfrowym, należy stwierdzić, że zróżnicowanie pomiędzy tymi jednostkami samorządu terytorialnego uległo zmniejszeniu. W 2018 r. koncentracja najwyższych wartości występowała głównie w dużych miastach i wokół nich i mimo utrzymania tej tendencji do 2020 r. w pozostałych powiatach zróżnicowanie zostało zmniej-

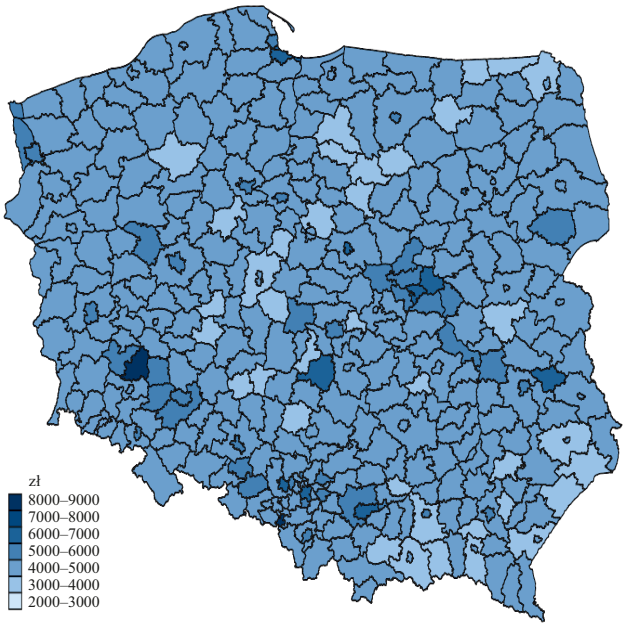
2017


zł
8000–9000
7000–8000
6000–7000
5000–6000
4000–5000
3000–4000
2000–3000

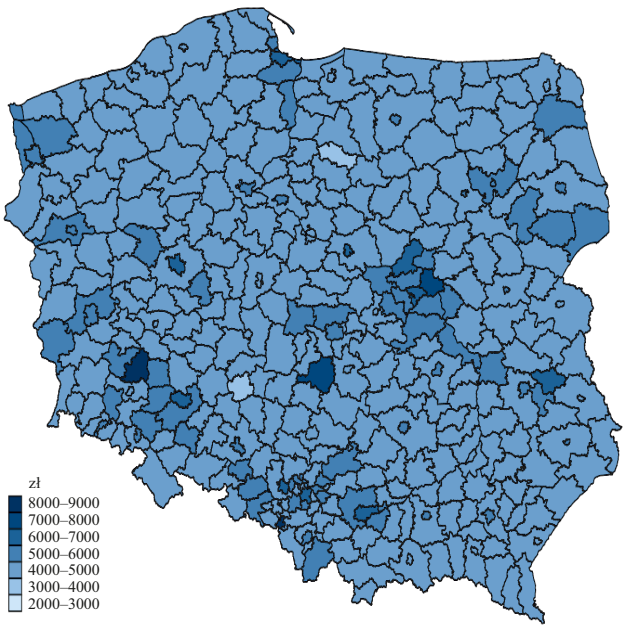
2018


zł
8000–9000
7000–8000
6000–7000
5000–6000
4000–5000
3000–4000
2000–3000

2019



2020

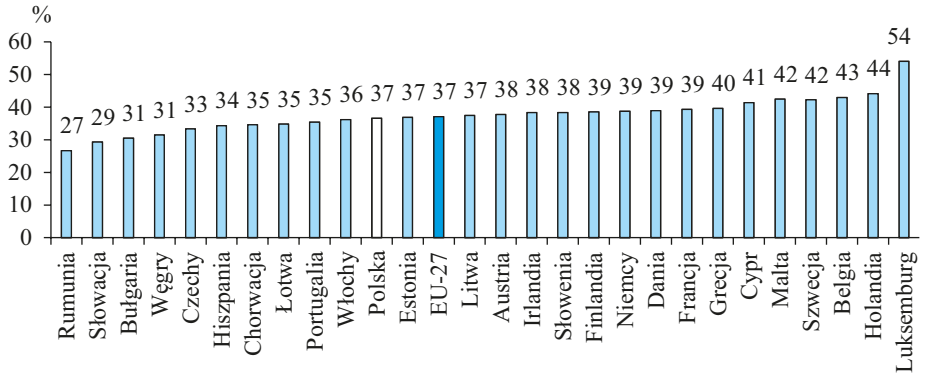


Rysunek 8. Średnie przeciętne miesięczne wynagrodzenie brutto w cenach realnych (baza = 2020) w powiatach w Polsce w latach 2017–2020

Źródło: jak rys. 7.

szone. Jednakże relatywnie duża rozpiętość między wartościami minimalnymi a maksymalnymi może potęgować wykluczenie cyfrowe, ponieważ koszty sprzętu i dostępu do internetu stanowią barierę przede wszystkim w gospodarstwach domowych w małych miastach i na obszarach wiejskich. Podjęcie dodatkowych działań zmierzających do zmniejszenia nierówności cyfrowych w poszczególnych regionach państwa z uwzględnieniem nierównomierności dochodów jest zatem bardzo ważne. Osoby o wysokich dochodach mają znacznie lepszy dostęp do technologii informacyjno-komunikacyjnych i są w stanie z nich korzystać, dzięki czemu biorą większy udział w życiu społecznym i politycznym niż ludzie obdarzeni jedynie niewielką ilością kapitału ekonomicznego (Fuchs, 2009).

Kolejną zmienną, często analizowaną w kontekście drugiego poziomu nierówności cyfrowych, jest status zatrudnienia. Jeszcze w latach 90. XX w. słaba umiejętność czytania i pisania nie stanowiły przeszkody w znalezieniu pracy, a kompetencje cyfrowe nie determinowały jej charakteru. Po ponad 30 latach transformacji i rozwijania technologii cyfrowych wiadomo, że wykluczenie cyfrowe prowadzi do ograniczenia możliwości zatrudnienia i rozwoju, a kompetencje cyfrowe i informacyjne są coraz bardziej pożądane. Istotną cechą współczesnego rynku pracy jest powiększająca się różnica między tymi, którzy posiadają umiejętności wymagane przez pracodawców, a tymi, którym ich brakuje (Bynner i Reder, 2010). Dostęp do internetu i kompetencje oraz umiejętności pozwalające na korzystanie z oprogramowania i sieci stał się niezwykle istotny w czasach pandemii COVID-19, ponieważ spowodowała ona zdecydowane rozpowszechnienie telepracy. Jeszcze przed pandemią ilość pracy, jaką można było wykonywać zdalnie, w wielu państwach była niewielka. Zmiana trybu pracy ze stacjonarnej na zdalną w wielu branżach i zawodach zapewniła ciągłość pracy milionom pracowników i tysiącom przedsiębiorstw w Unii Europejskiej. Ponadto pomogła zachować miejsca pracy, które w przeciwnym razie mogłyby zostać utracone. Według badań przeprowadzonych przez Sostero i in. (2021) kryzys społeczno-gospodarczy wywołany pandemią spowodował, że nagła konieczność dostosowania się do nowego rynku pracy dotyczyła co najmniej tylu osób, co wszystkie inne państwowe programy wsparcia dla bezrobotnych, wprowadzające okresowe dopłaty czy skracające wymiar czasu pracy. Powołani autorzy wykazali także, że gdyby nie gotowość i zdolność organizacji oraz przedsiębiorstw do błyskawicznego przystosowania się do pracy zdalnej, skutki kryzysu byłyby dużo bardziej poważne. Gdyby jednak praca zdalna w wielu sektorach nie była możliwa, restrykcje wprowadzane przez rządy wielu gospodarek rozwiniętych najprawdopodobniej nie byłyby tak duże, ale wiązałoby się to z większą liczbą zachorowań, zgonów i problemów już i tak nadwyrężonych systemów opieki zdrowotnej. Udział telepracy w zatrudnieniu w poszczególnych państwach Unii Europejskiej zaprezentowano na rysunek 9.



Rysunek 9. Udział telepracy w zatrudnieniu w państwach UE w 2018 roku

Źródło: opracowanie własne na podstawie danych z bazy Eurostat (https://ec.europa.eu/eurostat/web/main/data/database).

W czasie pandemii możliwości przejścia na pracę zdalną były znacznie większe w przypadku usług opartych na wiedzy. W państwach, w których zawody oparte na wiedzy stanowią większy odsetek wszystkich zawodów, istnieje większy odsetek miejsc pracy, którą można wykonywać zdalnie (Sostero i in., 2021). Najniższy zakres telepracy dotyczył Rumunii (27%) i wyniósł dwukrotnie mniej niż w Luksemburgu (54%). W Polsce 37% zatrudnienia było wykonywane z udziałem telepracy, co jest wartością zbliżoną do średniej wszystkich państw Unii Europejskiej. Najwyższy udział telepracy odnotowano w krajach skandynawskich i krajach Beneluksu, co według badań Sostero i in. (2021) korelowało w dużej mierze z rankingiem krajów według rozpowszechnienia telepracy przed wybuchem pandemii COVID-19. Najniższy udział telepracy w zatrudnieniu występuje w państwach Europy Wschodniej, a także w niektórych większych państwach członkowskich w Europie Południowej (np. we Włoszech i Hiszpanii).

Telepraca jest możliwa przede wszystkim w sektorze usług, będącym trzecim obok rolnictwa i przemysłu sektorem gospodarki narodowej. Usługi obejmują transport, łączność, handel, gospodarkę komunalną, ochronę zdrowia, oświatę, administrację, wymiar sprawiedliwości, instytucje finansowe i ubezpieczeniowe oraz pozostałe. Rola tego sektora wzrasta wraz z rozwojem gospodarczym państwa, a coraz większe znaczenie zyskują usługi oparte na wiedzy (Węgrzyn i Miłaszewicz, 2017). Jest to szczególnie istotne w kontekście drugiego poziomu wykluczenia cyfrowego. Z jednej strony osoby nieposiadające dostępu do internetu lub umiejętności korzystania z sieci i oprogramowania są wykluczone z możliwości świadczenia pracy zdalnej, szczególnie istotnej podczas pandemicznych obostrzeń, co w konsekwencji prowadzi do zmniejszenia dochodu. Z drugiej strony osoby zatrudnione w sektorze rolnictwa bądź prze-

mysłu mogą odczuwać większe konsekwencje w przypadku wprowadzanych obostrzeń pandemicznych, a jednocześnie mogą nie być dostatecznie zmotywowane, by uzyskać dostęp do sieci i zacząć z niej korzystać. Wydaje się zatem, że pracownicy większości działów sektora usług są w mniejszym stopniu narażeni na wykluczenie cyfrowe i jego szeroko pojęte konsekwencje. Mimo systematycznego wzrostu udziału sektora usług w polskiej gospodarce można dostrzec zróżnicowanie przestrzenne w zakresie odsetka ludności zatrudnionej w tym sektorze (rysunek 10).

Zróżnicowanie przestrzenne udziału osób zatrudnionych w usługach jest zauważalne we wszystkich prezentowanych latach (2017–2020), co jest konsekwencją selektywnego rozwoju usług w Polsce (Ilnicki, 2009). Wysoki odsetek jest charakterystyczny przede wszystkim dla miast na prawach powiatu i trochę niższy dla sąsiadujących z nimi powiatów. Można także zaobserwować linie podziału geograficznego – odsetek ludności pracującej w usługach jest wyższy w powiatach południowej Polski, zachodniej i północnej, a niższy w powiatach centralnej i wschodniej Polski. Podstawowe statystyki przedstawia tabela 13. Średnia wartość odsetka osób zatrudnionych w usługach w powiatach w Polsce wyniosła 43% we wszystkich analizowanych latach. Najniższą wartość, tj. poniżej 18%, odnotowano w powiatach: łomżyńskim, skierniewickim, zamojskim i suwalskim. Natomiast najwyższą, tj. powyżej 85%, w m. Warszawie i m. Sopot. Należy jednak zwrócić uwagę na dużą rozpiętość wartości skrajnych (około 70 pp.), co biorąc pod uwagę wcześniejsze rozważania w kontekście wykluczenia cyfrowego, może się przyczyniać do potęgowania nierówności.

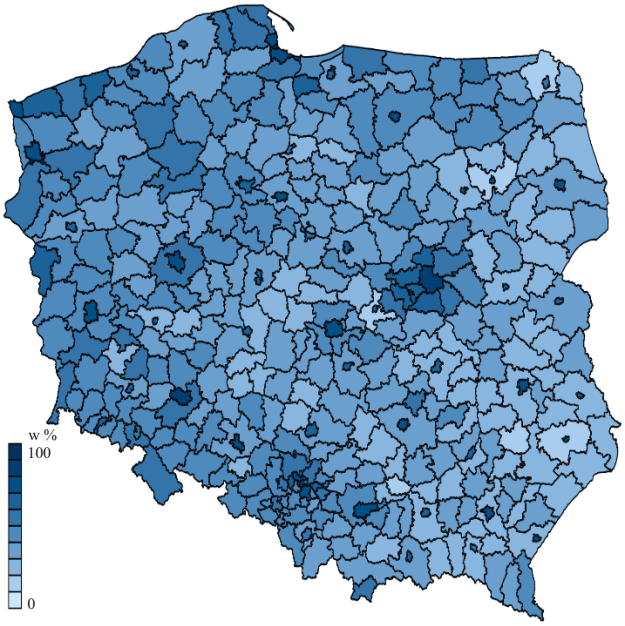
Tabela 13. Statystyki odsetka ludności zatrudnionej w sektorze usług w powiatach w latach 2017–2020 (w %)

Rok	Średnia	Odchylenie standardowe	Minimum	Maksimum
2017	43	15	17	87
2018	43	15	17	86
2019	43	15	16	86
2020	43	15	16	87

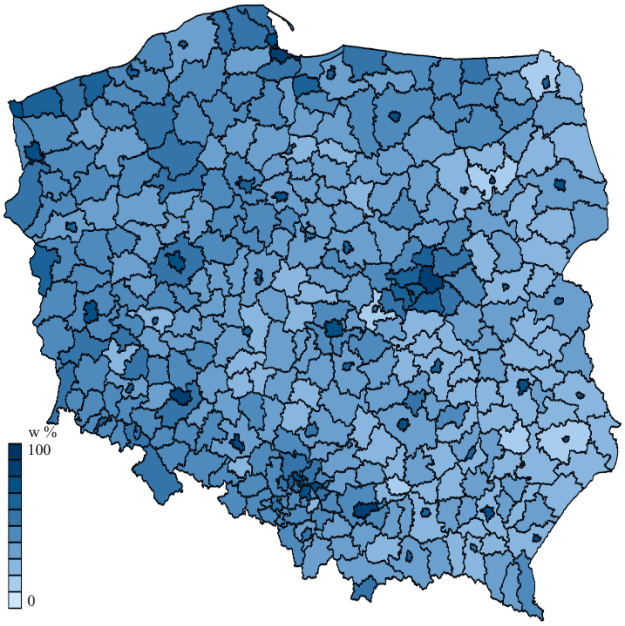
Źródło: jak w tabeli 11.

Nie tylko rodzaj wykonywanej pracy ma znaczenie w kontekście wykluczenia cyfrowego, ale i sam fakt zatrudnienia. Z badań GUS (2019, 2021) wynika, że najwyższy odsetek internautów stanowią studenci, a następnie osoby aktywne zawodowo. Znacznie rzadziej z internetu korzystają bezrobotni, a najmniej – emeryci i osoby bierne zawodowo. Osoby bezrobotne i bierne zawodowo są zatem znacznie bardziej narażone na wykluczenie cyfrowe, co niesie ze sobą

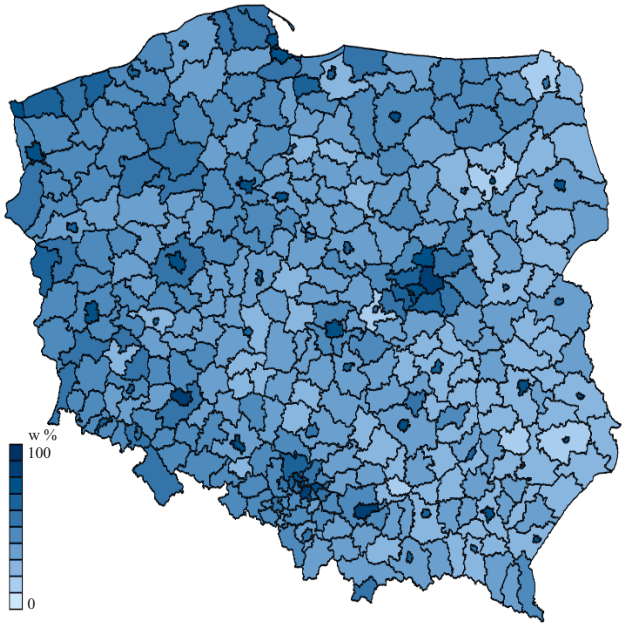
2017



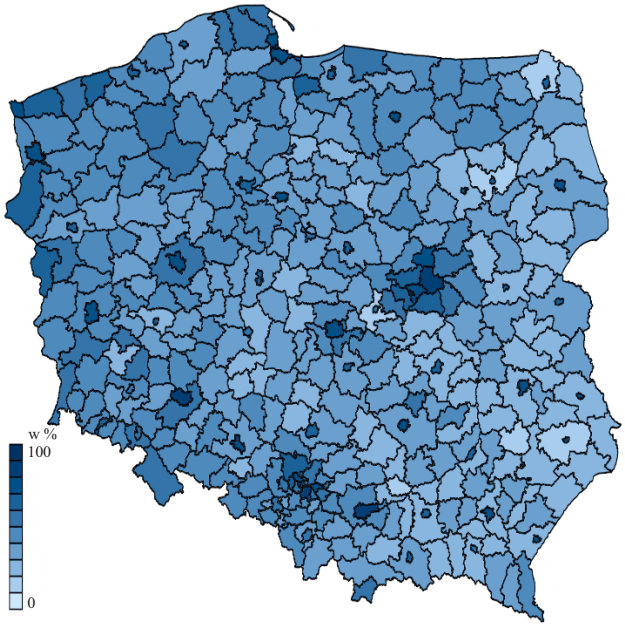
2018



2019



2020



Rysunek 10. Odsetek ludności zatrudnionej w sektorze usług w powiatach w latach 2017–2020

Źródło: jak rys. 7.

dalsze konsekwencje socjoekonomiczne. Aby przedstawić i dokonać analizy przestrzennej (rysunek 11) tych osób, wykorzystano dane na temat liczby pracujących na 1000 ludności w wieku produkcyjnym w polskich gminach. Wartość na poziomie 230 informuje, że spośród 1000 osób w wieku produkcyjnym w danej gminie 230 osób było zatrudnionych, a 770 osób pozostawało bez pracy i były to osoby zarówno bezrobotne, jak i bierne zawodowo. Wybór zmiennej jest podyktowany brakiem dostępności danych o bezrobotnych i biernych zawodowych na poziomie gmin.

Podobnie jak w przypadku udziału osób zatrudnionych w usługach najwyższym wskaźnikiem liczby pracujących przypadających na 1000 ludności w wieku produkcyjnym charakteryzują się miasta na prawach powiatu i, przeważne, sąsiadujące z nimi gminy. Linie podziału geograficznego są mniej wyraźne, jednak pozwalają dostrzec większą wartość wskaźnika w gminach Polski południowej i zachodniej, a niższy w przypadku gmin Polski centralnej i wschodniej.

Podstawowe statystyki przedstawia tabela 14. Średnia wartość liczby pracujących na 1000 ludności w wieku produkcyjnym w gminach w Polsce w latach 2017–2020 wyniosła 230 w 2017 i wzrosła do 242 w 2020 r. W badanym okresie najniższą wartość, tj. zera osób pracujących na 1000 mieszkańców, odnotowano aż w 40 gminach – w jednej gminie miejskiej, 35 gminach wiejskich i czterech gminach miejsko-wiejskich. Najwyższą liczbę osób pracujących, tj. powyżej 1000 ludności, odnotowano w 17 gminach, a w Kleszczowie były to wartości maksymalne. Gminy, na których terenie liczba pracujących jest większa aniżeli liczba osób w wieku produkcyjnym, są miejscem zatrudnienia dla osób spoza tego obszaru. Są one zatem szczególnie ważne z punktu widzenia sytuacji społeczno-gospodarczej regionu, ponieważ stanowią rynek pracy o znaczeniu ponadlokalnym. Znaczące różnice między gminami mogą potęgować przestrzenne nierówności cyfrowe w społeczeństwie.

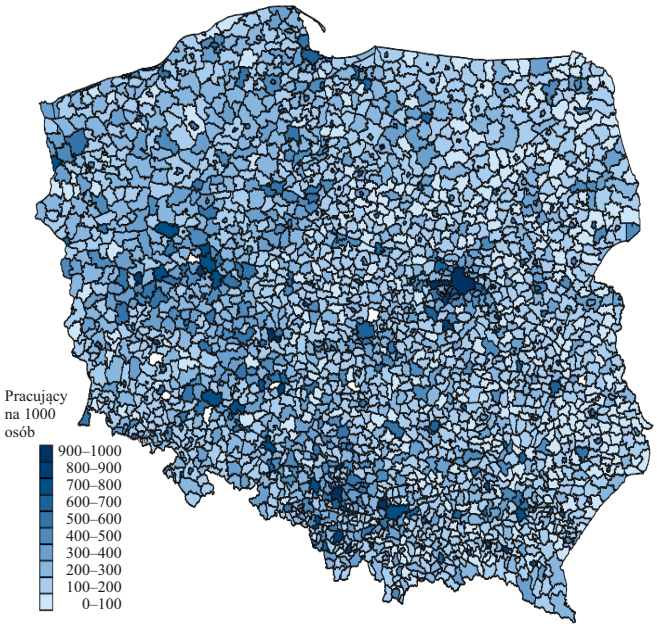
Galperin i Arcidiacono (2021) przeanalizowali status zatrudnienia jako determinantę nierówności cyfrowych ze szczególnym naciskiem na różnice wynikające z płci pracowników. Autorzy argumentowali, że rodzaje zawodów wykonywanych przez kobiety i mężczyzn wiążą się z różnymi możliwościami dostępu

Tabela 14. Statystyki liczby pracujących na 1000 ludności w wieku produkcyjnym w gminach w latach 2017–2020

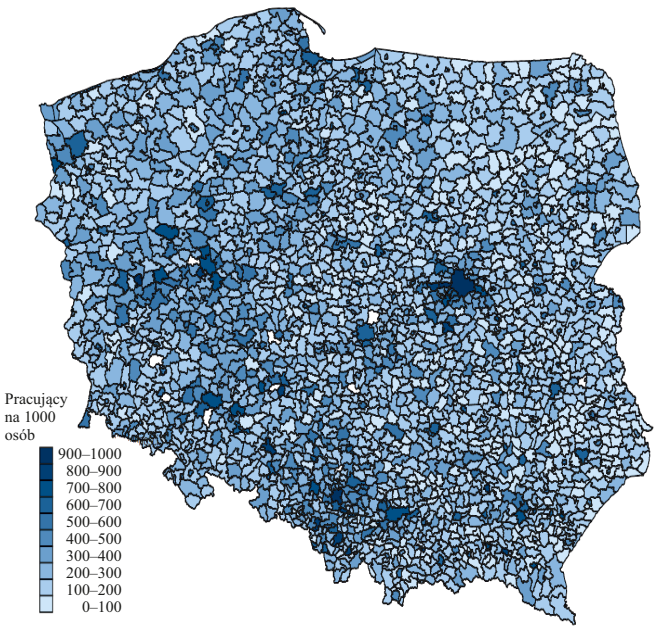
Rok	Średnia	Odchylenie standardowe	Minimum	Maksimum
2017	230	191	0	4335
2018	237	195	0	4308
2019	242	199	0	4167
2020	242	199	0	3973

Źródło: jak w tabeli 11.

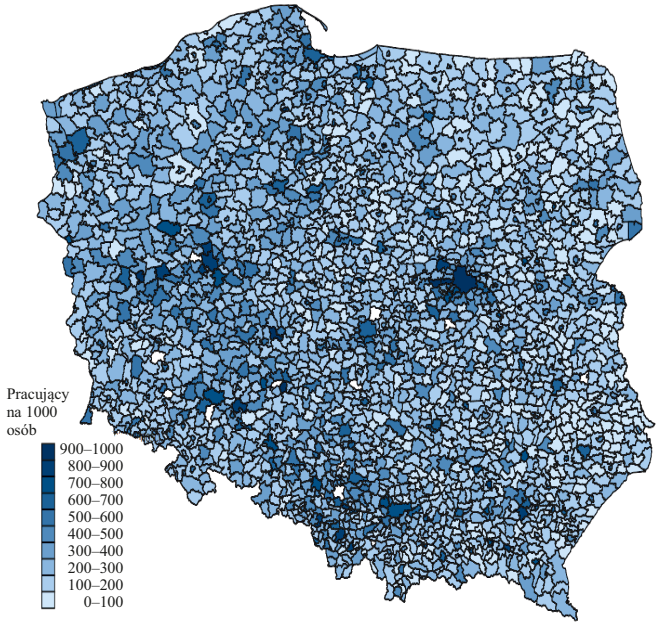
2017


Pracujący
na 1000
osób
900–1000
800–900
700–800
600–700
500–600
400–500
300–400
200–300
100–200
0–100

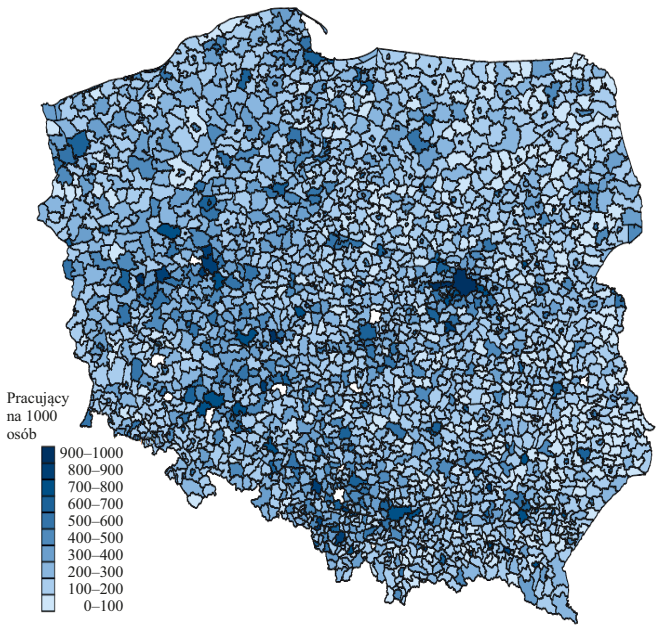
2018


Pracujący
na 1000
osób
900–1000
800–900
700–800
600–700
500–600
400–500
300–400
200–300
100–200
0–100

2019



2020



Rysunek 11. Liczba pracujących na 1000 osób w wieku produkcyjnym w gminach w Polsce w latach 2017–2020

Źródło: jak rys. 7.

do internetu i rozwijania umiejętności cyfrowych, które przyczyniają się do ogólnego wzrostu korzystania z sieci. Wyniki badań przeprowadzone na czterech państwa Ameryki Łacińskiej (Ekwadorze, Gwatemali, Meksyku i Peru) wykazały, że różnice w rodzaju zatrudnienia między kobietami i mężczyznami są znacznie ważniejszym czynnikiem wpływającym na różnice między płciami w korzystaniu z internetu aniżeli dochód, wiek czy wykształcenie osób z obu płci. Ponadto korelacja między zatrudnieniem a korzystaniem z internetu jest silniejsza wśród kobiet niż mężczyzn. Wynika to z charakteru sektorów, w których zwykle pracują kobiety. Wykorzystanie technologii informacyjno-komunikacyjnych jest bowiem większe np. w usługach związanych z oświatą i ochroną zdrowia aniżeli w sektorach przemysłowym czy rolniczym. Szacunki dokonane przez autorów sugerują, że gdyby odsetek kobiet i mężczyzn zatrudnionych w danych sektorach był równy, luka cyfrowa między płciami w badanych państwach zmniejszyłaby się o co najmniej jedną czwartą.

Wśród czynników determinujących drugi poziom wykluczenia cyfrowego płeć jest od wielu lat relatywnie często analizowaną zmienną. Mimo to na początku XXI w. wyniki badań były jeszcze niejednoznaczne. Hilbert (2011) wskazał, że przyczyną odmiennych zdań w dyskusji na temat dostępu kobiet do cyfrowych technologii informacyjno-komunikacyjnych i przede wszystkim korzystania z nich były dwa poglądy: z jednej strony twierdzono, że kobiety są raczej technofobiczne, a mężczyźni są znacznie lepszymi użytkownikami narzędzi cyfrowych, natomiast z drugiej strony uważano, że kobiety entuzjastycznie podchodzą do komunikacji cyfrowej. Wyniki badań przeprowadzonych przez Hilberta (2011) na przykładzie państw rozwijających się z Ameryki Łacińskiej i Afryki dowiodły, że w przypadku kobiet ich niższe kompetencje cyfrowe i mniejsze wykorzystywanie ICT są bezpośrednim wynikiem niesprzyjających warunków w zakresie zatrudnienia, edukacji i dochodów. Analogiczne wnioski z badań uzyskali wcześniej Wasserman i Richmond-Abbott (2005). Jednak po skontrolowaniu tych zmiennych przez Hilberta (2011) okazało się, że kobiety są bardziej aktywnymi użytkownikami narzędzi cyfrowych niż mężczyźni. W Polsce badania na temat społeczeństwa informacyjnego z uwzględnieniem nierówności płci przeprowadził Główny Urząd Statystyczny (GUS, 2019). Wynika z nich, że zróżnicowanie ogólnych umiejętności cyfrowych ze względu na płeć jest niewielkie, jednak dostrzeżono dwie prawidłowości: większy odsetek kobiet niż mężczyzn charakteryzuje się niskimi umiejętnościami cyfrowymi, jednak w przypadku umiejętności określonych jako podstawowe i ponadpodstawowe zależność była odwrotna. Podobne wyniki uzyskano w przypadku analizy umiejętności związanych z komunikowaniem się przez internet oraz w przypadku cyfrowych umiejętności związanych z oprogramowaniem. W zakresie cyfrowych umiejętności informacyjnych to również mężczyźni stanowili większy odsetek osób charakteryzujących się ponadpodstawowym poziomem. W kon-

tekście przedstawionych wyników warto zaprezentować przestrzenne zróżnicowanie wskaźnika feminizacji, odzwierciedlającego liczbę kobiet przypadającą na 100 mężczyzn w gminach w Polsce (rysunek 12).

Podobnie jak w przypadku poprzednio analizowanych przestrzennie zmiennych koncentracja wysokiego współczynnika feminizacji jest dostrzegalna przede wszystkim w miastach na prawach powiatu i gminach ościennych. Brak jest natomiast jednoznacznych linii podziału geograficznego.

Statystyki przedstawione w tabeli 15 wskazują, że w latach 2018–2020 średnia wartość współczynnika feminizacji dla wszystkich gmin w Polsce wyniosła 102 kobiety na 100 mężczyzn. Najniższe wartości, tj. poniżej 90, odnotowano w gminach Paprotnia, Gzy, Goszczyn, Młynarze oraz Turośl i są one gminami wiejskimi. Natomiast najwyższe, tj. powyżej 115, w gminach Puławy, Łęczyca, Zgierz, Komprachcice, Lublin, Pabianice, m. Warszawa, Polanica Zdrój, Łódź oraz Ciechocinek, które poza gminą Komprachcice, będącą gminą wiejską, są gminami miejskimi.

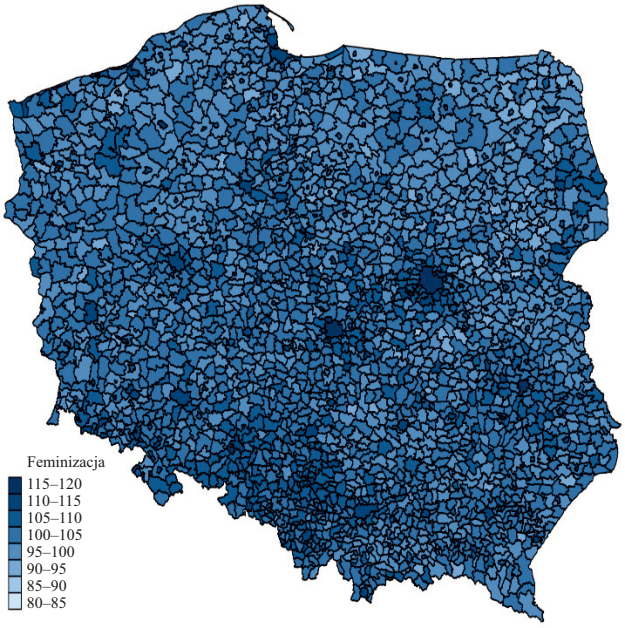
Tabela 15. Statystyki wskaźnika feminizacji w gminach w latach 2017–2020

Rok	Średnia	Odchylenie standardowe	Minimum	Maksimum
2017	102	5	87	120
2018	102	5	87	120
2019	102	5	87	120
2020	102	5	86	120

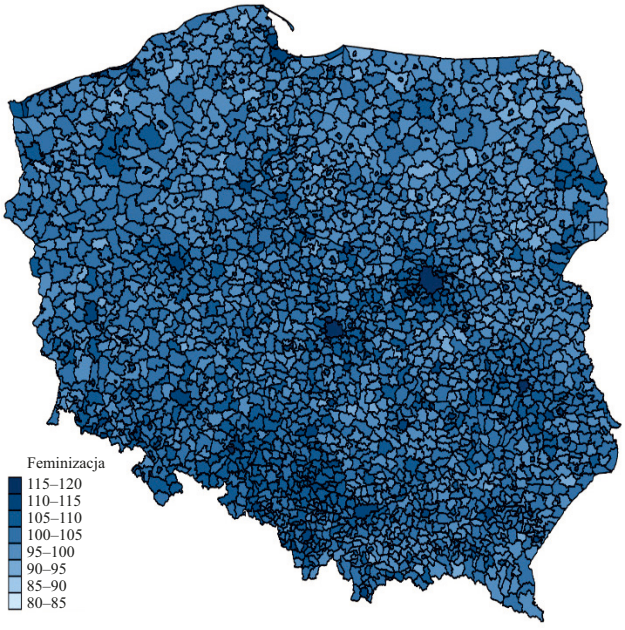
Źródło: jak w tabeli 11.

Analizy drugiego poziomu nierówności cyfrowych są poświęcone różnorodnym czynnikom, które determinują umiejętności cyfrowe oraz sposoby korzystania z internetu, jednak nie uwzględniają skutków tych różnic. Na rzeczywistych konsekwencjach wynikających z różnych poziomów dostępu i wykorzystania zasobów cyfrowych skupiają się analizy trzeciego poziomu nierówności cyfrowych (*third-level digital divide*) (Scheerder i in., 2017). Wyodrębnienie nowego poziomu było konieczne ze względu na to, że badania dotyczące pierwszego i drugiego poziomu nierówności cyfrowych często nie pozwalały na określenie i wyjaśnienie jej społecznych, kulturowych, gospodarczych, politycznych i terytorialnych skutków (Ferreira i in., 2021). Efektem badań nad trzecim poziomem rozpatrywanych nierówności jest podział użytkowników internetu na tych, którzy wykorzystują go do prostych zastosowań (np. wysłania wiadomości tekstowej, wyszukania informacji, załatwienia sprawy urzędowej) oraz tych, którzy mają umiejętności pozwalające nie tylko na „konsumowanie" technologii informacyjnej, ale także na współtworzenie przekazywanych treści i kreowa-

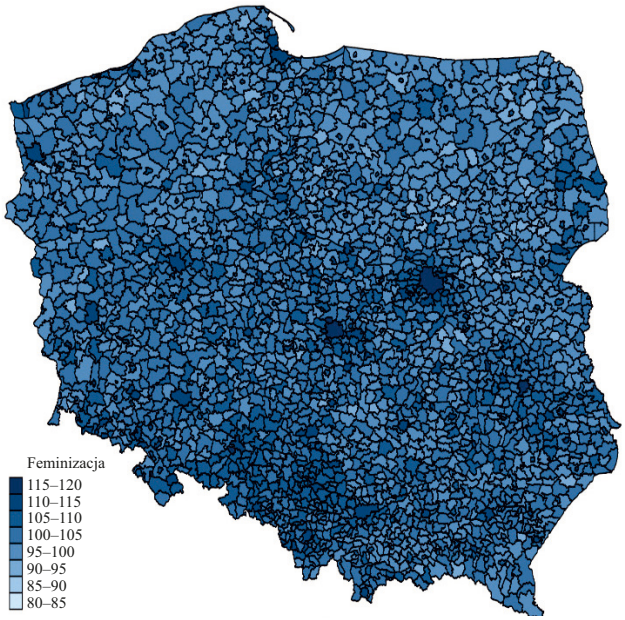
2017


Feminizacja
115–120
110–115
105–110
100–105
95–100
90–95
85–90
80–85

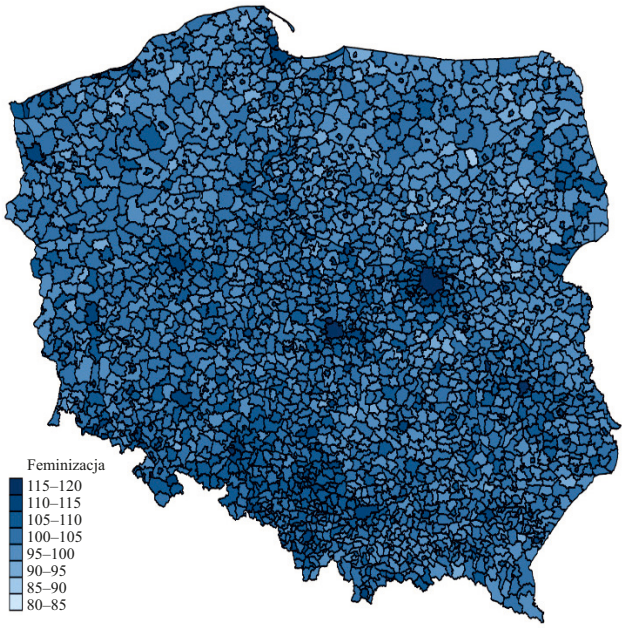
2018


Feminizacja
115–120
110–115
105–110
100–105
95–100
90–95
85–90
80–85

2019



2020



Rysunek 12. Wskaźnik feminizacji w gminach w Polsce w latach 2017–2020

Źródło: jak rys. 7.

nie nowych rozwiązań (Nielsen, 2006). Trzeci poziom nierówności cyfrowych dotyczy też dysproporcji w korzyściach z użytkowania z internetu wśród osób o podobnym profilu wykorzystywania sieci i z podobnym poziomem dostępu do technologii informacyjno-komunikacyjnych oraz infrastruktury internetowej (van Deursen i Helsper, 2015). Obserwuje się zarówno skutki pozytywne, jak i negatywne, takie jak cyberprzestępczość, nienawiść i dezinformacja w mediach społecznościowych, uzależnienie od internetu czy gier (van Dijk, 2020).

3

TRANSFORMACJA CYFROWA GMIN WARUNKIEM ICH ZRÓWNOWAŻONEGO ROZWOJU

3.1. Cele zrównoważonego rozwoju

Samorząd terytorialny odgrywa bardzo ważną rolę w zmniejszaniu nierówności społecznych, a także technologicznych, ponieważ zrównoważony rozwój rozpoczyna się w skali mikro, najbliżej obywateli i ich problemów. O zrównoważonym rozwoju dyskutuje się od lat 80. XX w. Koncepcja ta zrodziła się z konieczności ochrony środowiska przed negatywnymi efektami zewnętrznymi gwałtownego rozwoju gospodarki kapitalistycznej w kilku ostatnich dekadach. Idea zrównoważonego rozwoju jest odpowiedzią na niebezpieczeństwa, jakie pociąga za sobą rozwój gospodarek, szczególnie w krajach wysoko rozwiniętych. Problemy, które zapoczątkowały tę koncepcję, to m.in.: degradacja środowiska, wyczerpywanie się zasobów naturalnych, intensywny przyrost liczby ludności, powiększające się zróżnicowanie między gospodarkami wysoko i słabo rozwiniętymi. Termin zrównoważony rozwój został rozpowszechniony w 1987 r. w raporcie Światowej Komisji ds. Środowiska i Rozwoju zwanym raportem Brundtlanda. Zapisano w nim, że zrównoważony rozwój jest to „rozwój, który spełnia potrzeby teraźniejszości, bez uszczerbku dla zdolności przyszłych pokoleń do zaspokojenia ich własnych potrzeb (UN, 1987).

Hawken (1994) twierdził, że zrównoważony rozwój to stan ekonomiczny, w którym wymagania stawiane przez ludzi i gospodarkę można zaspokoić bez uszczerbku dla środowiska naturalnego, z którego korzysta obecne, a będzie korzystać następne pokolenie. Ideę tę można wyrazić następującymi słowami: zostaw świat lepszy niż go zastałeś, nie bierz więcej niż potrzebujesz, staraj się nie szkodzić życiu ani środowisku naturalnemu, a jeśli to zrobisz, to zadośćuczyń swemu działaniu.

W późniejszych publikacjach definicja ta była rozszerzana i uściślana, ale mimo to zrównoważonego rozwoju (SD) nie udało się precyzyjnie zdefiniować. Obszerny przegląd literatury na ten temat można znaleźć w artykule Mensah (2019), a dyskusję na temat zasadności nowego spojrzenia na zrównoważony

rozwój w warunkach pandemii COVID-19 w artykule Hakovirta i Denuwara (2020).

Zazwyczaj wyróżnia się trzy filary zrównoważonego rozwoju, którymi są (Moldan i in., 2012; Purvis i in., 2019):

– gospodarka (ekonomia),
– społeczeństwo,
– środowisko,

ale niektórzy autorzy wyodrębniają też filar czwarty, którym jest kultura (Makrakis i in., 2012) lub zdrowie.

Szczegółowe cele zrównoważonego rozwoju do 2030 r., które zostały wskazane przez ONZ w 2015 r. w rezolucji „Przekształcamy nasz świat: Agenda na rzecz zrównoważonego rozwoju 2030 (UN, 2020) odnoszą się do gospodarki, społeczeństwa i środowiska (tabela 16).

Tabela 16. Cele zrównoważonego rozwoju

Grupy celów	Cele specjalne
Cele gospodarcze	Cel 8. Promowanie trwałego, sprzyjającego włączeniu społecznemu i zrównoważonego wzrostu gospodarczego, pełnego i produktywnego zatrudnienia oraz godnej pracy dla wszystkich Cel 9. Budowanie odpornej infrastruktury, promowanie zrównoważonej industrializacji sprzyjającej włączeniu społecznemu oraz wspieranie innowacji Cel 10. Zmniejszenie nierówności w krajach i między nimi Cel 12. Zapewnienie zrównoważonych wzorców konsumpcji i produkcji
Cele społeczne	Cel 1. Wyeliminowanie ubóstwa we wszystkich jego formach na całym świecie Cel 2. Wyeliminowanie głodu, osiągnięcie bezpieczeństwa żywnościowego i lepszego odżywiania oraz promowanie zrównoważonego rolnictwa Cel 3. Zapewnienie zdrowego życia i promowanie dobrego samopoczucia wśród wszystkich ludzi w każdym wieku Cel 4. Zapewnienie włączającej i sprawiedliwej edukacji wysokiej jakości oraz promowanie możliwości uczenia się przez całe życie dla wszystkich Cel 5. Osiągnięcie równość płci i wzmocnienie pozycji wszystkich kobiet i dziewcząt Cel 7. Zapewnienie wszystkim dostępu do niedrogiej, niezawodnej, zrównoważonej i nowoczesnej energii Cel 11. Sprawienie, by miasta i osiedla ludzkie były przyjazne, bezpieczne, odporne i zrównoważone Cel 16. Promowanie pokojowego i integracyjnego społeczeństwa na rzecz zrównoważonego rozwoju, zapewnienie wszystkim dostępu do wymiaru sprawiedliwości oraz budowanie skutecznych, odpowiedzialnych i integracyjnych instytucji na wszystkich poziomach

cd. tabeli 16

Grupy celów	Cele specjalne
Cele środowiskowe	Cel 6. Zapewnienie wszystkim dostępności do wody i gospodarki sanitarnej oraz zrównoważone zarządzanie nimi Cel 13. Podjęcie pilnych działań w celu przeciwdziałania zmianom klimatu i ich skutkom Cel 14. Ochrona i zrównoważone wykorzystanie oceanów, mórz i zasobów morskich dla zrównoważonego rozwoju Cel 15. Ochrona, przywracanie i promowanie zrównoważonego użytkowania ekosystemów lądowych, zrównoważone zarządzanie lasami, zwalczanie pustynnienia oraz powstrzymanie i odwrócenie degradacji gleby oraz powstrzymanie utraty różnorodności biologicznej
Cel ogólny	Cel 17. Wzmocnienie środków realizacji i ożywienie Globalnego Partnerstwa na rzecz Zrównoważonego Rozwoju

Źródło: opracowanie własne na podstawie (Schoenmaker, 2017).

Wszystkie cele są ze sobą powiązane. Biorąc pod uwagę tematykę niniejszej monografii, warto zwrócić uwagę przede wszystkim na cele 4, 9, 10, 11 i 17. Państwa powinny dążyć do zapewnienia do 2030 r. wszystkim dziewczętom i chłopcom dostępu do nieodpłatnej, sprawiedliwej i dobrej jakości edukacji przedszkolnej, na poziomie podstawowym i ponadpodstawowym oraz wyższym. Należy tworzyć nowe i poprawić stan już istniejących placówek edukacyjnych, które powinny uwzględniać potrzeby dzieci, osób niepełnosprawnych, zarówno chłopców jak i dziewcząt, a także zapewnić bezpieczne, wolne od przemocy środowisko nauczania dla wszystkich. Ponadto należy znacząco zwiększyć liczbę wykwalifikowanych nauczycieli. W celu 9 zapisano budowę stabilnej infrastruktury, promocję zrównoważonego przemysłu oraz wsparcie innowacyjności, które są warunkiem rozwoju technologicznego, a tym samym transformacji cyfrowej gospodarki. Cel 10 dotyczy m.in. promowania integracji społecznej, gospodarczej i politycznej wszystkich ludzi, bez względu na wiek, płeć, niepełnosprawność, rasę, pochodzenie etniczne, narodowość, religię lub status. W celu 11 podkreśla się m.in. konieczność wzmocnienia wysiłków na rzecz ochrony i zabezpieczenia światowego dziedzictwa kulturowego i przyrodniczego. Cel 17 odnosi się m.in. do konieczności zwiększenia wykorzystania technologii kluczowych dla rozwoju, w szczególności technologii informacyjnych i komunikacyjnych. Ponadto zapisano w nim konieczność dążenia do osiągania celów zrównoważonego rozwoju poprzez współpracę podmiotów publicznych, nawiązywanie współpracy między podmiotami publicznymi i prywatnymi oraz z udziałem społeczeństwa obywatelskiego. Aktywizacja społeczności jest niezbędna do odkrycia tożsamości lokalnej i nawiązania więzi społecznych, aby działać w intencji dobra wspólnego. Najlepszym sposobem na zapewnienie udziału społeczeństwa w działaniach na rzecz zrównoważonego

rozwoju jest decentralizacja zadań administracji publicznej i publicznych zasobów finansowych. Należy też promować inicjatywy obywatelskie, wzmacniać rolę organizacji społecznych i bezpośredniego udziału mieszkańców w podejmowaniu decyzji (Schoenmaker, 2017).

Koncepcja zrównoważonego rozwoju stała się na tyle powszechna, że poszczególne kraje, w tym Polska, starają się uwzględnić jej aspekty ekonomiczne, środowiskowe i społeczne. W zależności od tego, jak rozwinięty jest kraj, zrównoważony rozwój może przybierać różne formy, a wymienionych 17 celów może być osiąganych w różnym stopniu, z różnym natężeniem i za pomocą różnych instrumentów. Niemniej panuje powszechna zgoda, że bez zrównoważonego rozwoju zasoby naturalne zostaną nieodwracalnie wyczerpane, a to może uniemożliwić życie na Ziemi naszym dzieciom i wnukom (Hayward i Garvin, 2010).

Gospodarka (ekonomia) odgrywa ważną rolę w koncepcji zrównoważonego rozwoju. Po pierwsze, wynika to z tego, że rozwój przemysłu prowadzi do niekiedy nieodwracalnego zniszczenia środowiska, a po drugie, rozwój gospodarczy generuje wypracowywanie środków finansowych, które są przeznaczane na osiąganie poszczególnych celów tego rozwoju. W skali lokalnej gospodarką zajmują się jednostki samorządu terytorialnego. Ich transformacja cyfrowa może ułatwić osiągnięcie postulatów zrównoważonego rozwoju, ponieważ ICT są fundamentem zrównoważonego rozwoju (Ziemba, 2018).

3.2. Rodzaje innowacji w procesie zrównoważonego rozwoju

Nie ma rozwoju bez innowacji. Gospodarka 4.0 jest interakcją techniki, gospodarki i społeczeństwa, dlatego stwarza możliwości dalszego rozwoju gospodarczego i społecznego. Barber (2014) twierdził, że technologia jest kluczem do zrównoważonego rozwoju. Dzięki internetowi edukacja, nauka na szczeblu akademickim, kultura, handel, finanse, administracja, inne usługi mogą się równolegle rozwijać w nowej, wirtualnej rzeczywistości. Mamy więc do czynienia z: e-handlem, e-usługami, e-edukacją, e-zdrowiem, e-administracją, e-państwem, e-samorządem terytorialnym. Ich powstanie nie byłoby możliwe, gdyby człowiek nie wprowadzał innowacji do wszystkich sfer życia społeczno-gospodarczego.

Innowacje i innowacyjność gospodarki są złożonymi i różnie rozumianymi kategoriami ekonomicznymi. Najogólniej innowacja oznacza wprowadzenie czegoś nowego, np. nowego sposobu świadczenia usług na rzecz mieszkańców, a innowacyjność – stworzenie warunków, aby mogły być kreowane innowacje. To uruchomienie mechanizmów, które są zdolne do tworzenia nowych i dosko-

nalenia istniejących dóbr, poprzez wprowadzanie zmian w procesie technologicznym, metodach zarządzania organizacją wynikających z postępu wiedzy i dostępu do coraz to nowych osiągnięć naukowych (Marciniak, 2010). Oznacza to szybki rozwój tych dziedzin, które tradycyjnie są uważane za kreatywne (media), i tych, w których innowacje są pożądane (opieka zdrowotna, edukacja) (Peters i in., 2012).

W zależności od sposobu powstawania innowacji można je podzielić na zamknięte (*closed innovation*) i otwarte (o*pen innovation)*. Pierwsze są tworzone przez organizacje we własnym zakresie, wprowadzają je pracownicy tych organizacji. Otwarte innowacje powstają we współpracy danej organizacji z partnerami zewnętrznymi. Łączenie wewnętrznych i zewnętrznych pomysłów przyspiesza powstawanie innowacji (Chesbrough, 2003).

Innowacje można też podzielić na: produktowe, technologiczne (procesowe), organizacyjne i rynkowe (Penc, 1999). Wyróżnia się też innowacje marketingowe (OECD i Eurostat, 2005), oszczędne (*frugal innovation*), ekoinnowacje oraz innowacje społeczne (Szczepańska, 2017). Pierwsze odnoszą się do towarów i usług, a sprowadzają się do udoskonalania już istniejącego produktu lub wytwarzania nowego produktu. Innowacje technologiczne odnoszą się do zmian w stosowanych metodach wytwarzania, usprawniających produkcję oraz zwiększających jej efektywność. Innowacje organizacyjne zmieniają system zarządzania danym podmiotem i organizację procesu produkcji. Innowacje rynkowe są ukierunkowane na zaspokojenie potrzeb konsumentów, a marketingowe polegają na wypracowaniu nowych rozwiązań w zakresie metod sprzedaży, wzornictwa i opakowania, metod ustalania cel, metod promocji i reklamy. Innowacje oszczędne to nowe rozwiązania powstające początkowo w krajach rozwijających się. Nie bazują one na przeprojektowanych innowacjach zachodnich, ale są od nowa zaprojektowanymi produktami, usługami lub rozwiązaniami organizacyjnymi dopasowanymi do potrzeb klienta i ograniczeń zasobowych. Innowacje te polegają na wykorzystaniu minimum zasobów i istniejących możliwości do rozwiązania problemu lub wykonania ważnego zadania szybciej i taniej, ale przy zachowaniu rozsądnej jakości. Istotą innowacji oszczędnych jest masowa użyteczność i przystępność cenowa (Rao, 2013). Ze względu na swą istotę powinny się nimi zainteresować jednostki samorządu terytorialnego. Innowacje te mogłyby być przydatne w ochronie zdrowia, edukacji, ochronie środowiska, polityce społecznej. Wpisują się więc one w koncepcję rozwoju zrównoważonego. Z koncepcją tą powiązane są też ekoinnowacje, czyli wszystkie innowacje, które prowadzą do osiągnięcia zrównoważonego rozwoju przez ograniczenie negatywnego oddziaływania działalności produkcyjnej na środowisko, zwiększenie odporności przyrody na obciążenia lub zapewnienie większej skuteczności i odpowiedzialności w zakresie korzystania z zasobów naturalnych (Kemp i Pearson, 2007).

Z punktu widzenia problematyki monografii warto też wspomnieć o innowacjach społecznych. Innowacją społeczną jest każde nowe rozwiązanie (usługa, produkt, strategia, model działania, forma organizacji, proces), które odpowiada na potrzeby społeczne bardziej efektywnie niż rozwiązania dotychczasowe. Innowacją społeczną będzie zarówno zaspokajanie potrzeb społecznych (np. z zakresu warunków pracy, edukacji, ochrony zdrowia) w nowy sposób, jak i stymulowanie innowacyjnych wydarzeń o charakterze społecznym (np. rozwój metod otwartego oprogramowania) (Kroik i Skonieczny, 2013). W węższym znaczeniu innowacją społeczną jest tylko to rozwiązanie, które powstaje samoistnie, oddolnie, z inicjatywy określonych osób lub ich organizacji (Szczepańska, 2017). Niezależnie od definicji specyfika tych innowacji polega na tym, że prowadzą do zmian korzystnych dla człowieka i całego społeczeństwa. Ponieważ społeczeństwo jest jednym z filarów zrównoważonego rozwoju, innowacje te są ważne z punktu widzenia dążenia do zrównoważonego rozwoju. Innowacje społeczne odgrywają ważną rolę w tych dziedzinach życia społeczno-gospodarczego, w których inne rodzaje innowacji zawodzą, są przestarzałe lub nie pozwalają na właściwe wykorzystywanie pojawiających się w otoczeniu możliwości (Mulgan i in., 2007). Innowacje te pojawiają się m.in. w edukacji (Loogma i in., 2012), ochronie zdrowia (Beinare i McCarthy, 2012), kulturze (Tremblay i Pilati, 2013), usługach publicznych (Teets, 2012), ochronie środowiska (Maruyama i in., 2007) czy finansach publicznych (Philips i in., 2010). Wielu autorów wskazuje na możliwości wykorzystania innowacji społecznych w wymienionych dziedzinach. Na przykład Raufflet (2009) twierdzi, że innowacje społeczne mogą się przyczyniać do nabywania i uaktualniania wiedzy w celu lepszego zaspokajania potrzeb społecznych. Część autorów pokazuje, że innowacje te można wykorzystać do promowania zmian społecznych, np. aby zmniejszyć przemoc wobec kobiet (Sullivan, 2003) lub pomóc chorym osobom bezdomnym (Calsyn, 2003), do poprawy zdrowia i pomocy społecznej (Heales i Green, 2017). Tak rozumiane innowacje społeczne stają się zatem sposobem na poprawę jakości życia obywateli, będącą rezultatem ich wdrożenia (Mulgan, 2006; Pol i Ville, 2009), a tym samym na zmniejszenie nierówności wewnątrz państwa oraz między poszczególnymi państwami, co przybliżyłoby ludzkość do wypełnienia kilku celów zrównoważonego rozwoju.

Współczesny konsument dóbr publicznych i prywatnych wręcz domaga się innowacji. W podmiotach sektora finansów publicznych działania innowacyjne nie są takie dynamiczne jak w sektorze prywatnym, ale pandemia COVID-19 przyczyniła się do tego, że nawet administracja publiczna nie tylko zaczęła postrzegać innowacje jako ważny czynnik zrównoważonego rozwoju, ale zaczęła też na dużą skalę przyswajać sobie innowacje (podobnie jak obywatele) i rozpowszechniać je. Obywatel oczekuje od administracji publicznej oraz podmiotów usługowych dóbr, które będą rozwijały jego wiedzę, poszerzały zaintere-

sowania, umożliwiały załatwienie spraw urzędowych online, podtrzymywały jego przynależność do grupy. Co istotne, zdaniem Bella to właśnie innowacje wykorzystujące technologie cyfrowe powodują największe zmiany społeczne, a zwolennicy determinizmu technologicznego, którego jest przedstawicielem, twierdzą, że odpowiednie rozwiązania techniczne mogą rozwiązać problemy społeczne, a tym samym, że problemy społeczne można opisać językiem techniki (Dobrowolski, 2005).

3.3. Piąty filar zrównoważonego rozwoju – integracja cyfrowa

Problematyka rozwoju zrównoważonego jest szeroka i wielowątkowa. W niezwykle obszernej literaturze przedmiotu najczęściej wyróżniane są trzy filary zrównoważonego rozwoju – hasłowo nazywane: gospodarka (ekonomia), społeczeństwo i środowisko. Filary te oznaczają, że u podstaw idei zrównoważonego rozwoju leży jednoczesne zintegrowanie działań człowieka w wymienionych obszarach. Gospodarka (ekonomia) odgrywa ważną rolę w koncepcji zrównoważonego rozwoju. Po pierwsze, wynika to z tego, że rozwój przemysłu prowadzi do niekiedy nieodwracalnego zniszczenia środowiska, a po drugie, rozwój gospodarczy generuje wypracowywanie środków finansowych, które są przeznaczane na osiąganie poszczególnych celów tego rozwoju. Myśląc o zrównoważonym rozwoju społecznym, należy „stawiać" człowieka w centrum. Wszystkie działania powinny być przeprowadzane z poszanowaniem godności ludzkiej i prawa równego dostępu do dóbr publicznych. Pozbawianie kogokolwiek dostępu do tych dóbr, np. ze względu na wiek, niepełnosprawność, miejsce zamieszkania, umiejętności cyfrowe lub wysokość wynagrodzenia, jest sprzeczne z koncepcją zrównoważonego rozwoju. Nowe technologie stwarzają wszystkim szansę na pełniejszy udział w życiu społecznym i gospodarczym. Wiele działań podejmowanych przez gminy jest zgodnych z tym filarem, np. oferowanie usługi elektronicznego, a nawet zdalnego dostępu do księgozbioru w bibliotece lub organizowanie kursów obsługi komputera i smartfona dla seniorów.

Zrównoważony rozwój środowiskowy (ekologiczny) wymaga ochrony środowiska, w tym zasobów naturalnych. Obywatele, podmioty gospodarcze, państwa powinny świadomie korzystać z wody, energii i używać odnawialnych źródeł energii. Należy unikać uszkodzenia ekosystemu, a może się to ziścić wtedy, jeżeli eksploatacja złóż nieodnawialnych zostanie zastąpiona wytwarzaniem surowców odnawialnych. W tym filarze postuluje się także zmniejszenie emisji do gleby, wody i powietrza szkodliwych substancji. W przypadku gmin działaniami wspierającymi

zrównoważony rozwój środowiskowy jest np. wymiana taboru komunikacji miejskiej na elektryczny i wodorowy, przeprowadzanie termomodernizacji budynków, dofinansowywanie wymiany pieców węglowych, montaż oszczędnościowego oświetlenia ulicznego. Nowe technologie mogą wspierać te działania, np. montaż czujników na lampach pozwoli na ich włączanie dopiero, gdy się ściemni.

Niektórzy autorzy wyodrębniają też filar czwarty, którym jest kultura (Sabatini, 2019; Hawkes, 2001) lub zdrowie. Kultura jest niezbędna do rozwoju społecznego, ale w świecie, który walczy ze skutkami pandemii COVID-19, uzasadnione jest wprowadzenie następnego filaru zrównoważonego rozwoju: zdrowia człowieka (zdrowia publicznego). Co prawda ONZ wymienia zdrowie wśród szczegółowych celów tego rozwoju, ale jego oddzielenie od innych celów sugeruje, że jest to jeden z wielu, a nie zasadniczy warunek przetrwania ludzkości i zrównoważonego rozwoju ludzkości. Za potraktowaniem zdrowia jako osobnego filara zrównoważonego rozwoju przemawia to, że nie jest już ono tylko kwestią demograficzną lub indywidualną, ale, co pokazała pandemia z lat 2019–2022, ma zasadnicze znaczenie z punktu widzenia zrównoważonego rozwoju wszystkich państw na świecie (Hakovirta i Denuwara, 2020).

Pamiętając o wyzwaniach, z jakimi przyszło się mierzyć społeczeństwu w warunkach pandemii COVID-19, oraz biorąc pod uwagę funkcjonowanie społeczeństwa w gospodarce 4.0, autorki opowiadają się za traktowaniem zdrowia jako czwartego filaru zrównoważonego rozwoju oraz proponują filar piąty – *digital inclusion*. Koncepcja pięciu filarów zrównoważonego rozwoju została przedstawiona na rysunek 13.

Rysunek 13. Pięć filarów zrównoważonego rozwoju w społeczeństwie postcovidowym

Źródło: opracowanie własne.

Piąty filar – integracja cyfrowa – jest związany z niwelowaniem nierówności w rozwoju cyfrowym społeczeństwa. Nierówności te tradycyjnie rozpatruje się w dwóch wymiarach. Pierwszym z nich jest dostęp do internetu, w tym w szczególności do internetu szerokopasmowego, oraz dostęp do sprzętu komputerowego. Drugim wymiarem są umiejętności cyfrowe. Wykluczenie w tym wymiarze jest rozumiane jako brak możliwości zdobycia, utrzymania lub uaktualnienia zdolności związanych z technologiami informacyjno-komunikacyjnymi. W kontekście gospodarki 4.0 można również mówić o trzecim wymiarze nierówności w rozwoju cyfrowym, który łączy dwa pierwsze: nierównościach w umiejętności wykorzystania technologii w określonym celu, czyli tworzenia wartości dodanej przy wykorzystaniu posiadanego sprzętu i umiejętności (Arendt, 2013), co zostało szerzej opisane w poprzednim rozdziale monografii. Jak podkreśla van Dijk (2013), powyższy model charakteryzuje się kumulacyjnością i rekursywnością. Poszczególne wymiary *digital exclusion* następują kolejno po sobie, a proces powtarza się w miarę pojawiania się nowych technologii. Co ważne, dopiero zmniejszenie nierówności w dwóch pierwszych płaszczyznach umożliwia podejmowanie działań, które będą zmierzały do niwelowania nierówności na trzeciej płaszczyźnie. Dysproporcje lub braki w którejkolwiek z trzech wymienionych wcześniej płaszczyzn prowadzą do wykluczenia cyfrowego, którego istnienie z kolei zaburza zrównoważony rozwój społeczeństwa. Dysproporcje te są poważną barierą rozwoju miast oraz istotnym czynnikiem stagnacji obszarów wiejskich.

Z badań zaprezentowanych w poprzednim rozdziale wynika, że część polskiego społeczeństwa jest wykluczona cyfrowo. Jest to zarówno wykluczenie „motywacyjne", przez które rozumiemy niechęć wobec nowych technologii wynikającą z: braku wiary we własne możliwości, braku motywacji do zapoznania się z nowoczesnymi technologiami oraz lęku przed nowościami, jak również wykluczenie „materialne", które oznacza brak możliwości zakupu urządzeń, oprogramowania i usług dostępu do internetu. Wynika z tego, że w polskim społeczeństwie występują nierówności w rozwoju cyfrowym w wymiarze pierwszym i drugim. Bariery, jakie powstają na tym etapie rozwoju, uniemożliwiają dalszy rozwój, kompetencji cyfrowych. Wykluczeniem cyfrowym są zagrożeni szczególnie ludzie starsi, mieszkańcy terenów wiejskich oraz ludzie o niższym statusie majątkowym. Pandemia COVID-19 wyraźnie uwypukliła te różnice.

3.4. Znaczenie samorządu gminnego w zrównoważonym rozwoju cyfrowym

O zrównoważonym rozwoju można mówić nie tylko w skali makroekonomicznej, ale także w skali lokalnej, z perspektywy miasta i gminy, zgodnie ze stwierdzeniem „myśl globalnie, działaj lokalnie". Co prawda na zrównoważony rozwój gminy wpływają czynniki zewnętrzne, niezależne od władz lokalnych, np. stabilność sytuacji społeczno-gospodarczej na szczeblu regionu i całego państwa, ale nie bez znaczenia są tu także czynniki wewnętrzne, które powinny zapewnić stabilność wszystkich podmiotów tworzących wspólnotę lokalną (podmiotów gospodarczych, organizacji pozarządowych, mieszkańców). Podstawowe potrzeby mieszkańców o charakterze zbiorowym są zaspokajane przez samorząd lokalny. W konsekwencji gmina jest centrum życia społecznego i lokalnej gospodarki, jest ośrodkiem edukacji dzieci i młodzieży oraz upowszechniania kultury i pielęgnowania tradycji. Gminy odgrywają też ważną rolę w udzielaniu wsparcia osobom starszym i poszkodowanym przez los. Są one też odpowiedzialne za rozbudowę sieci infrastruktury technicznej (ulic, chodników, wodociągów, kanalizacji) oraz ochronę środowiska. Można więc przyjąć, że gmina jest najniższym poziomem, na którym powinno się rozwiązywać problemy towarzyszące ludzkości.

Samorząd terytorialny może część swoich zadań wykonywać w sposób tradycyjny, może też wprowadzać nowe rozwiązania, dostosowując się do sytuacji wynikającej np. z pandemii COVID-19, wojny w Ukrainie, kryzysu energetycznego i potrzeb mieszkańców. Pandemia pokazała anachronizm w świadczeniu usług publicznych, w tym z zakresu oświaty, kultury i pomocy społecznej. Uświadomiła wszystkim, że obecne metody nauczania są niedostosowane do możliwości technologicznych, oczekiwań młodych ludzi i wymagań rynku pracy. Funkcjonowanie w warunkach pandemii przyczyniło się do sprawniejszego wprowadzania różnego rodzaju innowacji społecznych oraz innowacji oszczędnych. Do nowych, elektronicznych kanałów świadczenia usług z zakresu oświaty, kultury i pomocy społecznej można zaliczyć: telefonię analogową, telefonię cyfrową (w tym telefonię internetową), telefonię komórkową (w tym także krótkie telefoniczne wiadomości tekstowe, czyli tzw. SMS-y), komunikatory elektroniczne, pocztę elektroniczną oraz różne rodzaje aplikacji i formularzy elektronicznych.

Pandemia spowodowała, że wszyscy musieliśmy się stać cyfrowymi innowatorami, w przeciwnym razie pozostalibyśmy na marginesie procesów: konsumpcji, produkcji, świadczenia usług. Jaka jest rola samorządu w cyfrowej transformacji edukacji? Po pierwsze, zapewnienie odpowiedniej infrastruktury i wsparcia, po drugie, pomoc w dostępie do sprzętu, po trzecie, zapewnienie wsparcia dla nauczycieli i dyrektorów oraz po czwarte, zapewnienie wsparcia

psychologicznego. Dzięki programowi Innowacyjna edukacja Rzeszów szybko odnalazł się w nowej rzeczywistości wynikającej z zamknięcia szkół. Na wprowadzenie nowych rozwiązań gotowy był nie tylko samorząd, ale także uczniowie, dyrektorzy i nauczyciele, którzy przeszli odpowiednie szkolenia z wykorzystania tych narzędzi na długo przed oficjalnym zamknięciem szkół. W dalszym ciągu pracownicy miasta pomagają w poznawaniu tajników Office 365 (można się kontaktować telefonicznie, mejlowo i przez komunikatory). Pomimo dobrego przygotowania Rzeszowa i Gdańska do nauczania z wykorzystaniem technologii cyfrowych przejście na tryb zdalny rodziło wiele problemów, które trudno było rozwiązać w krótkim czasie. Internet może doskonale wspierać edukację, ale technologia może też być elementem wykluczenia społecznego. Nie wszyscy mają komputer, tablet czy smartfon na wyłączność, dostęp do szybkiego internetu bez limitu przesyłania danych, miejsce do swobodnej pracy czy nauki. Słabsze łącze lub brak kamery internetowej oznacza, że uczniowie nie mogą uczestniczyć w zdalnych lekcjach na równych zasadach z innymi. Największym wyzwaniem było więc zapewnienie wszystkim potrzebującym uczniom i nauczycielom dostępu do sprzętu (laptopów, tabletów czy smartfonów). Oba miasta pozyskiwały dodatkowe środki od sponsorów, ubiegały się o dotacje z budżetu państwa oraz pośredniczyły w przekazywaniu sprzętu bezpośrednio od podmiotów gospodarczych do uczniów. Następnym problemem były niewystarczające kompetencje cyfrowe niektórych uczniów i nauczycieli, co groziło wykluczeniem z procesu edukacyjnego dużej liczby uczniów. W większości przypadków uczniowie szybko się zaadaptowali, bo albo już doskonale poruszają się w wirtualnym świecie, albo szybko wchłaniają nowinki technologiczne (*Rzeszowski projekt…*, b.d.).

Nauczanie z wykorzystaniem technologii wymaga zmiany nastawienia, zmiany metod kształcenia i zdobycia nowych kompetencji w zakresie prowadzenia zajęć. Rzeszów miał już wcześniej przeszkolonych nauczycieli, Gdańsk wspiera ich za pośrednictwem funkcjonującej od kilku lat Gdańskiej Platformy Edukacyjnej. Umożliwia ona korzystanie z elektronicznych systemów oceniania, e-maili służbowych dla nauczycieli i dyrektorów, ponadto pozwala prowadzić zdalne zajęcia lub telekonferencje. Nie wszyscy nauczyciele znali to narzędzie, dlatego z inicjatywy gminy utworzono kanał na YouTube: EduStandardGDN TV, na którym umieszczano tutoriale nagrywane przez nauczycieli i dyrektorów z gdańskich szkół i placówek edukacyjnych, pokazujące zasady wykorzystania narzędzi dostępnych w na platformie (Felis, 2011). Utworzono też zamknięte grupy w mediach społecznościowych dostępne dla tych dyrektorów i nauczycieli. Uczestnictwo w dyskusji grup, które są moderowane przez przedstawicieli miasta, stwarza przestrzeń do wymiany doświadczeń i pomysłów związanych z nauczaniem zdalnym (*Gdańska Platforma…*, b.d.).

Czas pandemii zmienił rodzaje usług z zakresu pomocy społecznej oraz sposób ich świadczenia. W tym okresie niektóre jednostki samorządowe

(np. Wrocław) zdecydowały się na wykorzystanie aplikacji Dobre Wsparcie, która umożliwia nowoczesne zarządzanie usługami opiekuńczymi. Aplikacja została stworzona przez Fundację Nauka dla Środowiska z Koszalina we współpracy z partnerami społecznymi. Prace nad nią były dofinansowane ze środków Europejskiego Funduszu Społecznego zarządzanego przez Urząd Marszałkowski w Szczecinie. Aplikacja Dobre Wsparcie określana jest jako „Uber oferujący sąsiedzkie usługi opiekuńcze". Pozwala ona na zdiagnozowanie rzeczywistego zapotrzebowania na usługi, tym samym pozwala obniżyć koszty usług opiekuńczych w gminie i odpowiada na wyzwania przyszłości (bo wykorzystuje nowe technologie, np. sygnał GPS do lokalizacji potrzebującego). System jest autonomiczny, łączy lokalnych użytkowników (gminy, ośrodki pomocy, opiekunów, poradnie i rodziny). W czasie pandemii COVID-19 narzędzie mogło być wykorzystywane w kierowaniu pracą sztabów kryzysowych, instytucji zarządzających pomocą społeczną, pracownikami służb medycznych i wolontariuszami. Osoby pracujące w terenie dostają poprzez aplikację zadania do wykonania oraz informacje, gdzie, komu i kiedy mają pomóc. Wykonanie zadań potwierdzają „odhaczeniem" ich w programie. W systemie osoba zarządzająca ma podgląd do lokalizacji pracowników, wolontariuszy i podopiecznych. Narzędzie to było pomocne również dla służb kontrolujących przestrzeganie kwarantanny domowej. W 2019 r. aplikacja ta zwyciężyła w konkursie Komisji Europejskiej Regio-Stars na najbardziej innowacyjne projekty unijne. Projekt otrzymał wyróżnienie w kategorii obejmującej zwalczanie nierówności i ubóstwa. W obliczu pandemii twórcy aplikacji udostępnili ją zainteresowanym gminom nieodpłatnie (*Dobre wsparcie*, b.d.). Przedstawione rozwiązanie, wdrożone na poziomie lokalnym i odnoszące sukcesy, być może stało się impulsem do stworzenia aplikacji zaproponowanej przez rząd Kwarantanna Domowa, ułatwiającej i usprawniającej przeprowadzanie obowiązkowej kwarantanny domowej (*Aplikacja…*, b.d.).

W maju 2020 r. w Poznaniu uruchomiono nową usługę pod nazwą Telefon Porad Cyfrowych, która polega na tym, że trzy razy w tygodniu pracownik Centrum Inicjatyw Senioralnych udziela seniorom porad z zakresu nowych technologii. Wsparcie obejmuje rozwiązywanie problemów z komputerem, tabletem, smartfonem czy aparatem fotograficznym. Konsultant informuje m.in., jak wysłać e-mail, zgrać zdjęcia z telefonu, pobrać z internetu aplikacje i programy umożliwiające bezpłatne rozmowy i wideorozmowy, założyć konto na Facebooku, wyszukać w internecie strony z ofertą aktywnego i ciekawego spędzenia czasu. Działania te mają przeciwdziałać wykluczeniu cyfrowemu seniorów, szczególnie w czasie pandemii, kiedy brak wiedzy na temat nowych technologii utrudniał kontakt z bliską osobą i dostęp do informacji (*Telefon…*, b.d.).

Również w kulturze pojawiły się inne, dotąd niestosowane przez gminy rozwiązania. W Toruniu widowisko plenerowe Skyway Festiwal odbywało się dotąd w przestrzeni miasta, a polegało na tym, że na budynkach miasta wyświetlane

były instalacje świetlne. W 2020 r. festiwal został przeniesiony na teren lotniska. Wykorzystano mechanizm *drive-thru*, co pozwoliło na zachowanie odpowiedniej odległości pomiędzy widzami festiwalu. Publiczność przejechała wzdłuż instalacji we wnętrzu własnego samochodu (*Świetlne…*, b.d.). Umożliwiło to uczestniczenie w kulturze bez narażania się na bezpośredni kontakt z innymi ludźmi. Następna innowacja miała na celu zmniejszenie nierówności społecznych i zapobieganie wykluczeniu osób starszych niemających dostępu do internetu. Mieszkańcy Katowic w wieku powyżej 65. roku oraz osoby niepełnosprawne mogą zamówić książkę lub audiobook z biblioteki z dowozem do domu, a potem w ten sam sposób ją oddać. Na potrzeby realizacji tego zadania zakupiono i w specjalny sposób oznakowano samochód bagażowy (Bednarek, 2020).

Przytoczone przykłady innowacji potwierdzają, że samorząd gminny często stanowi swego rodzaju laboratorium do testowania nowych rozwiązań[22], również w zakresie innowacji technologicznych, które, jeśli okażą się sukcesem, stanowią wzorzec do naśladowania bądź są bezpośrednio wdrażane na poziomie centralnym, w całym kraju.

Świadczenie usług w wymieniony sposób ma sporo zalet, ale napotyka też wiele barier. Bariery te można podzielić na leżące po stronie usługobiorcy oraz leżące po stronie usługodawcy. Można też wyróżnić bariery techniczne, które odnoszą się do obu stron procesu usługowego. Do barier leżących po stronie usługobiorcy można zaliczyć: brak chęci lub motywacji do korzystania z usług online, brak szeroko rozumianych umiejętności cyfrowych. Wśród barier leżących po stronie usługodawcy można wskazać: brak aktywności, brak pomysłu na to, w jaki sposób przejść na usługi online. W grupie barier technicznych należy wskazać przede wszystkim takie, jak: brak lub niezadowalająca jakość sprzętu, brak niezbędnych aplikacji (czasami wynikająca z ich odpłatności), brak dostępu do szerokopasmowego internetu lub jego słaba jakość. Na specyficzne przeszkody, które utrudniają świadczenie usług edukacyjnych w formule online, wskazuje Baszyński (2020).

Badania pilotażowe przeprowadzone przez Kańdułę i Przybylską (2022b) po pierwszych trzech miesiącach pandemii COVID-19 wykazały wyraźne różnice w poszczególnych obszarach wdrażania innowacji społecznych. Na taką sytuację, zdaniem autorek, wpływ miały głównie dwa czynniki. Pierwszym z nich był charakter zadań realizowanych przez samorząd – w obszarach zadań obligatoryjnych można było zaobserwować szybsze tempo wprowadzania nowych, innowacyjnych rozwiązań świadczenia usług niż w obszarach związanych z realizacją zadań fakultatywnych. Przy braku obligatoryjności usług część gmin zrezygno-

[22] Innowacje pojawiają się też na innych szczeblach samorządu terytorialnego. Na przykład Urząd Marszałkowski Województwa Małopolskiego w Krakowie, wykorzystując własne zasoby, stworzył elektroniczne narzędzie do zarządzania regionalnym programem operacyjnym na lata 2014–2020, tzw. system e-RPO (Guz, 2022).

wała z ich świadczenia podczas lockdownu, a stosunkowo niewielka grupa podjęła starania zmierzające do wprowadzenia do oferty usług online. Drugim czynnikiem wpływającym na tempo digitalizacji usług świadczonych przez jednostki samorządu terytorialnego była dostępność zewnętrznych źródeł finansowania tego typu działań. Digitalizacja następowała szybciej w obszarach, w których były dostępne dodatkowe środki finansowe przeznaczone na realizację działań w tym zakresie.

Autorki uważają, że piątym, niezbędnym filarem zrównoważonego rozwoju jest *digital inclusion*. Jednak realizacja celów wpisujących się w ten filar – zapewnienie dostępności sprzętu oraz rozwijanie umiejętności cyfrowych społeczeństwa – w dużej mierze spoczywa na samorządzie gminnym, który będąc najbliżej swoich mieszkańców, jest w stanie najszybciej i najrzetelniej zidentyfikować braki i nierówności w tym zakresie oraz zainicjować działania zmierzające do ich usunięcia. Dopiero zapewnienie zrównoważonego rozwoju na szczeblu lokalnym pozwala na realizację tej idei na szczeblu regionalnym, narodowym i globalnym.

4

ŹRÓDŁA FINANSOWANIA TRANSFORMACJI CYFROWEJ GMIN

4.1. Systematyka źródeł finansowania zadań gmin

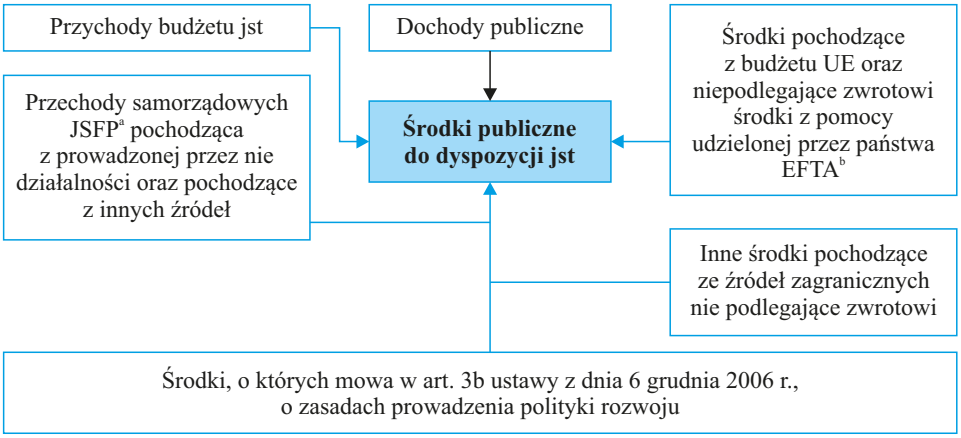
Jedną z cech samorządu terytorialnego jest możliwość samodzielnego prowadzenia gospodarki finansowej na podstawie własnego budżetu oraz wyposażenie w dochody własne i obce, których wysokość powinna być dostosowana do zakresu zadań. Samorząd ten powinien mieć też dostęp do rynku kapitałowego, na którym mógłby pozyskiwać zwrotne źródła finansowania zadań (Europejska karta, 1994). Wstąpienie Polski do Unii Europejskiej (UE) otwarło też możliwość ubiegania się o środki pochodzące z budżetu UE oraz o niepodlegające zwrotowi środki z pomocy udzielanej przez państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA).

Źródła finansowania działalności jednostek samorządu terytorialnego (jst) mogą być grupowane według różnych kryteriów. Można je dzielić, biorąc pod uwagę np. ustawę o finansach publicznych z 2009 r. oraz kryteria: ekonomiczne (prawne), zwrotności i źródła pochodzenia środków. Według przepisów prawnych źródła finansowania działalności jst w Polsce są nazywane środkami publicznymi. Można wyróżnić kilka grup tych środków (rysunek 14).

W Konstytucji RP zapisano, że dochodami jst są dochody własne, subwencja ogólna i dotacje celowe. Dochody jst można klasyfikować według różnych kryteriów. Najczęściej spotykany i najbardziej kontrowersyjny jest ich podział na dochody własne i obce (zwane także pozostałymi, uzupełniającymi, wyrównawczymi).

W skład dochodów własnych jst wchodzą:

- podatki i opłaty (niekiedy wyróżnia się też grupę dopłat), choć te pierwsze tylko na szczeblu gmin,
- dochody z majątku samorządowego,
- inne dochody spełniające kryteria zaliczenia ich do dochodów własnych lub przyporządkowane do tej kategorii na podstawie przepisów prawnych.



[a] Jednostki sektora finansów publicznych.
[b] Państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu.

Rysunek 14. Grupy środków publicznych do dyspozycji jednostek samorządu terytorialnego

Źródło: opracowanie własne na podstawie (Ustawa, 2009).

Natomiast dochody obce obejmują: udziały w dochodach budżetu państwa[23] (w podatkach państwowych), subwencję ogólną i dotacje celowe. O przeznaczeniu środków pozyskanych w formie dochodów własnych, udziałów (w podatku dochodowym od osób fizycznych oraz udziału w podatku dochodowym od osób prawnych) oraz subwencji decyduje rada gminy (Kotlińska, 2011). Charakter celowy mają natomiast dotacje celowe, które mogą pochodzić z różnych źródeł: budżetu państwa, budżetów innych jednostek samorządu terytorialnego, państwowych funduszy celowych, osób prawnych zaliczanych do sektora finansów publicznych (np. Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej), funduszy będących w dyspozycji Banku Gospodarstwa Krajowego oraz ze źródeł zagranicznych. Niekiedy dotacje są obligatoryjnymi (np. na finansowanie zadań zleconych), a innym razem fakultatywnymi (np. dotacje z funduszy UE, niektóre dotacje z budżetu państwa na dofinansowanie zadań własnych) źródłami dochodów. Ponadto niekiedy zaliczane są do dochodów obcych, a niekiedy do dochodów własnych (np. dotacje z budżetów innych jst oraz z funduszy celowych). Co więcej, zdarza się, że dotacje formalnie są nazywane „środkami na dofinansowanie własnych inwestycji gmin, powiatów (związków gmin, związków powiatowo-gminnych, związków powiatów), samorządów województw, pozyskanymi z innych źródeł". Tak się dzieje w przypadku udzielania dotacji ze środków różnych programów rządowych, za których dystrybucję odpowie-

[23] Systematyka ta może wywoływać kontrowersje. Na ten temat piszą m.in. Kotlińska (2009) oraz Patrzałek i in. (2022).

dzialny jest Bank Gospodarstwa Krajowego, np. rządowego funduszu inwestycji lokalnych. Takie dotacje są zaliczane do dochodów własnych jst pomimo ich celowego przeznaczenia i pochodzenia spoza terenu działania tych jednostek. Taka praktyka nie sprzyja przejrzystości finansów publicznych.

Co do zasady dochody jst pochodzące z poszczególnych tytułów nie mogą być przeznaczane na finansowanie konkretnych wydatków, chyba że odrębna ustawa stanowi inaczej. Celowe przeznaczenie mają niektóre opłaty, dotacje celowe oraz środki z budżetu UE i z innych źródeł zagranicznych niepodlegające zwrotowi. Ostatnia wymieniona grupa jest szczególnym rodzajem dochodów jst. Nazwanie ich „środkami" (a nie dochodami) wynika ze specyfiki ich planowania i ewidencjonowania oraz dysponowania nimi i ich rozliczania.

Wymienione grupy dochodów są przeznaczane przede wszystkim na finansowanie wydatków bieżących, a więc w ograniczonym zakresie można je przeznaczyć na finansowanie działań składających się na transformację cyfrową gmin. Finansowanie wydatków inwestycyjnych wymusza sięganie po nadzwyczajne źródła zasilania finansowego, którymi są pożyczki, kredyty i emisja obligacji (Surówka i Owsiak, 2018). W budżetach jst pojawiają się więc przychody publiczne. Obejmują one środki publiczne pochodzące (najogólniej) ze źródeł zwrotnych: ze sprzedaży papierów wartościowych, z prywatyzacji majątku jst, z otrzymanych pożyczek i kredytów, ze spłat pożyczek i kredytów udzielonych ze środków publicznych, z innych operacji finansowych (w tym wolne środki, o których jest mowa w art. 217 ustawy o finansach publicznych z 2009 r.). Pożyczki mogą pochodzić ze źródeł krajowych i zagranicznych, ze źródeł publicznych i prywatnych. Filipiak i Dylewski (2021) twierdzą, że w portfelu instrumentów dłużnych gmin i innych jst „coraz częściej będą się pojawiać instrumenty związane z realizacją celu przejścia na gospodarkę neutralną dla klimatu", ponieważ takie zalecenia wypływają z dokumentów strategicznych UE. Jeżeli tak będzie w rzeczywistości, to należy się spodziewać także wzrostu długu na skutek zaciągania pożyczek na finansowanie transformacji cyfrowej gmin, choć – w dalszym ciągu – wśród dostępnych źródeł finansowania przeważają dotacje. Dług może jednak narastać w związku z koniecznością zgromadzenia wkładu własnego przy korzystaniu z funduszy europejskich. Zadania z zakresu transformacji cyfrowej mogą być też finansowane przez gminy w formule partnerstwa publiczno-prywatnego.

Źródła finansowania działalności gmin mogą być też dzielone według kryterium zwrotności. W tym ujęciu wyróżnia się:

– źródła bezzwrotne (dochody własne, subwencję, dotacje z budżetu państwa i innych źródeł, z tym z funduszy UE);
– źródła zwrotne (kredyty, pożyczki, w tym z funduszy UE).

Klasyfikując źródła finansowania działalności gmin, można też dokonać ich podziału z punktu widzenia źródła pochodzenia środków. Wyodrębnia się wtedy źródła:

– krajowe (wewnętrzne), np. dochody własne, dochody otrzymywane z budżetu państwa, dotacje z państwowych funduszy celowych, dotacje z innych źródeł krajowych, w tym od spółek Skarbu Państwa, darowizny, kredyty i pożyczki zaciągnięte na rynku krajowym[24];
– zagraniczne (zewnętrzne), np. dotacje i pożyczki z budżetu UE, dotacje z innych źródeł niepodlegających zwrotowi, np. z środków Europejskiej Agencji Kosmicznej, kredyty i pożyczki zaciągnięte zagranicą.

Wszystkie krajowe źródła środków publicznych mogą być wykorzystane do finansowania działań składających się na transformację cyfrową gmin. Wydaje się jednak, że w warunkach niewystarczalności dochodów do sfinansowania nawet obligatoryjnych zadań o charakterze bieżącym priorytetowe znaczenie należy przypisać środkom z budżetu Unii Europejskiej i z innych źródeł zagranicznych niepodlegających zwrotowi. Z tego względu w monografii pominięto charakterystykę dochodów własnych gmin oraz tych dochodów obcych, których otrzymanie nie wymaga udziału gminy w postępowaniu konkursowym (np. subwencji). Pominięto także problematykę instrumentów rynku finansowego, ponieważ możliwości ich wykorzystania w gospodarce finansowej gmin są szeroko omówione w literaturze (Patrzałek i in., 2022), a ponadto rynek ten jak dotąd nie oferuje specjalnych instrumentów, które mogłyby zostać wykorzystane na finansowanie zadań z zakresu transformacji cyfrowej. W następnym punkcie zostaną zasygnalizowane tylko te krajowe źródła środków, których celem jest (do)finansowanie działań z zakresu transformacji cyfrowej jst. Są to: państwowy fundusz celowy (Fundusz Szerokopasmowy) oraz środki Polskiego Funduszu Rozwoju S.A. (PFR).

Członkostwo Polski w UE otworzyło przed jst możliwość finansowania zadań bieżących i inwestycyjnych z bezzwrotnych i zwrotnych środków pochodzących z budżetu UE oraz z innych źródeł zagranicznych. Dochody budżetu UE są dystrybuowane pomiędzy różne podmioty i w formie rozmaitych instrumentów (funduszy, programów, inicjatyw). Dystrybucja środków z funduszy unijnych jest zdecentralizowana – zajmują się nią państwa członkowskie UE. Część środków z budżetu UE, zwanych programami Komisji Europejskiej (KE), jest też dzielona centralnie, tzn. zajmuje się tym wymieniona komisja.

Nie pretendując do dokonania pełnej systematyki instrumentów, za których pośrednictwem UE dystrybuuje środki pomiędzy państwa członkowskie, można wyodrębnić ich następujące grupy:

[24] W gminach wiejskich i miejsko-wiejskich działania z zakresu *smart villages* mogą być finansowane ze środków gromadzonych w funduszu sołeckim, który jest formą budżetu obywatelskiego (Ustawa, 2014).

– źródła tradycyjne, czyli fundusze UE, przede wszystkim Europejski Fundusz Rozwoju Regionalnego, a w odniesieniu do *smart village* – Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich;
– nowe źródła (fundusze) – Fundusz na rzecz Sprawiedliwej Transformacji (nowy fundusz UE) oraz Instrument na rzecz Odbudowy i Zwiększania Odporności[25] (instrument tymczasowy);
– instrumenty terytorialne, w tym tradycyjne: Rozwój Lokalny Kierowany przez Społeczność (RLKS) i Zintegrowane Inwestycje Terytorialne (ZIT) oraz nowy – Inny Instrument Terytorialny (IIT);
– programy (inicjatywy) Komisji Europejskiej[26], np.: Cyfrowa Europa, Horyzont Europa, Kreatywna Europa, CEF („Łącząc Europę"), REACT-EU, Wi-Fi4EU[27].

Przyjęto, że tradycyjnymi źródłami (funduszami, instrumentami i inicjatywami) są te, z których jst mogły korzystać w perspektywie finansowej 2014–2020 i w latach wcześniejszych, natomiast nowymi źródłami są te, które utworzono w związku z dążeniem do osiągnięcia celów UE wyznaczonych na lata 2021–2027 i późniejsze, oraz te, które utworzono na określony czas w związku z koniecznością złagodzenia społecznych i gospodarczych negatywnych konsekwencji pandemii COVID-19, w szczególności w celu zwiększenia odporności państw UE na wahania cyklu koniunkturalnego oraz przygotowania ich do wyzwań związanych z troską o środowisko naturalne i możliwości, jakie wiążą się z rozwojem ICT.

W dalszych punktach tego rozdziału zasygnalizowano historyczne już możliwości ubiegania się o dofinansowanie zadań ze środków funduszy zaplanowanych do wykorzystania w latach 2014–2020. Programy operacyjne będące podstawą do ubiegania się o dofinansowanie działań z zakresu transformacji

[25] Instrument ten jest specyficzny, ponieważ w założeniu jest rozwiązaniem tymczasowym. Ze środków tego instrumentu finansowane są reformy i inwestycje w państwach członkowskich UE od początku pandemii w lutym 2020 r. do 31 grudnia 2026 r. (instrument powołano 19 lutego 2021 r.). Specyficzne jest też źródło jego finansowania – aby sfinansować odbudowę państw po pandemii, Komisja Europejska – w imieniu UE – zaciągnęła zobowiązania na rynku kapitałowym (KE, b.d., *Instrument*).

[26] Zdaniem Kornberger-Sokołowskiej, Zdanukiewicz i Cieślaka (2010) inicjatywy wspólnotowe to działania podejmowane przez instytucje unijne w celu wsparcia osiągania celów UE. Wiatrak (2004) definiuje je jako programy bezzwrotnej pomocy oferowane państwom członkowskim UE. Wsparcie przyznawane jest na te działania, które są istotne nie tylko dla danego państwa, ale też dla UE jako całości. Inicjatywy są finansowane z funduszy UE oraz z budżetów państw uczestniczących w inicjatywie. Inicjatywa może być wykonywana w trakcie jednego okresu programowania, może też obowiązywać w latach następnych (ustanawiane są kolejne edycje tych programów).

[27] Pominięto programy, które były dostępne w latach 2014–2020 i wcześniejszych. Warto jednak pamiętać, że niektóre programy obowiązujące w latach 2021–2027 są kontynuacją wcześniejszych inicjatyw. Na przykład programem Horyzont Europa zastąpiono program Horyzont 2020.

cyfrowej jst ze środków z budżetu UE w kontekście perspektywy finansowej na lata 2021–2027 zostały zaprezentowane w punkcie czwartym tego rozdziału. Poprzedzono go przedstawieniem celów UE związanych z cyfryzacją gospodarek państw członkowskich. Scharakteryzowano również programy zarządzane bezpośrednio przez Komisję Europejską. Omawiając potencjalne źródła finansowania transformacji cyfrowej gmin, wyodrębniono punkt pt. Programy grantowe finansowane ze źródeł zagranicznych. Jest to zabieg celowy. Jednostki samorządu terytorialnego mogą się bowiem ubiegać o środki unijne w różny sposób: (1) składając wnioski o dofinansowanie zadań ze środków ujętych w krajowych i regionalnych planach operacyjnych; (2) przystępując do konkursów organizowanych przez Komisję Europejską lub inne instytucje unijne; (3) uczestnicząc w konkursach organizowanych przez podmioty sektora finansów publicznych (ministerstwa, agencje rządowe, państwowe osoby prawne), publicznego (np. Polski Fundusz Rozwoju S.A.) lub sektora prywatnego. Źródłem środków przeznaczanych na granty dzielone przez podmioty z trzeciej grupy mogą być np. Europejski Fundusz Rozwoju Regionalnego bądź program REACT UE.

W pracy pominięto charakterystykę instrumentów terytorialnych, zarówno tradycyjnych, jak i instrumentu nowego. Jest to zabieg celowy, ponieważ instrumenty te nie są odrębnymi źródłami finansowania rozwoju, lecz formą zachęty jst do podejmowania współpracy w procesie planowania i finansowania rozwoju lokalnego. W konsekwencji beneficjenci ubiegający się o środki z instrumentów terytorialnych muszą tworzyć zinstytucjonalizowane partnerstwo[28]. Mogą się oni ubiegać o dofinansowanie zadań przyczyniających się do osiągnięcia wszystkich celów polityki spójności UE, o których będzie mowa w punkcie 4.3), w tym z zakresu: przedsiębiorczości, środowiska i transformacji cyfrowej (MFiPR, 2022c).

4.2. Źródła krajowe

Warunkiem rozwoju usług elektronicznych i podnoszenia kompetencji cyfrowych obywateli jest dostęp do internetu. Inwestycje z tym związane mogą być finansowane ze środków państwowego funduszu celowego – Funduszu Szerokopasmowego, którego dysponentem jest minister właściwy do spraw informatyzacji (Ustawa, 2010a). Środki tego funduszu przeznacza się na: (1) działania wspierające rozwój szybkich sieci telekomunikacyjnych poprzez dofinansowanie lub udzielanie pożyczek na budowę lub przebudowę tych sieci oraz wykonywanie przyłączy telekomunikacyjnych do lokalizacji użytkownika końcowego;

[28] Może to być np. stowarzyszenie gmin i związek komunalny.

(2) działania mające na celu pobudzenie popytu użytkowników końcowych na usługi związane z szerokopasmowym dostępem do internetu poprzez dofinansowanie zakupu usług telekomunikacyjnych, zakupu urządzeń multimedialnych oraz organizacji szkoleń rozwijających kompetencje cyfrowe lub udziału w tych szkoleniach oraz (3) koszty związane z obsługą funduszu. Pierwszy nabór wniosków trwał w okresie od 27.05 do 27.06.2022 r. Do podziału było 20 mln zł. Maksymalna kwota dofinansowania wynosiła 5 mln zł, co mogło odpowiadać 80% wartości wydatków kwalifikowalnych projektu. Planowano wyłonić czterech zwycięzców konkursu („Cyfryzacja", 2022).

Na projekty związane z nowymi technologiami można otrzymać dofinansowanie m.in. od Polskiego Funduszu Rozwoju spółki akcyjnej Skarbu Państwa, który udziela pożyczek oraz obejmuje akcje i udziały w spółkach. Fundusz przygotował program PFR dla miast, którego celem jest wsparcie w rozwoju polskich inteligentnych miast przyszłości. Zakłada się, że rozwiązania składające się na inteligentne miasta ułatwią załatwianie codziennych spraw ich mieszkańcom i efektywne zarządzanie infrastrukturą lokalną, a tym samym poprawią jakość życia (Polski Fundusz Rozwoju, b.d.).

Oferta PFR dla jst obejmuje nie tylko instrumenty finansowe. Realizując swoje statutowe cele w październiku 2022 r., PFR stworzył platformę elektroniczną pod nazwą „Giełda Miejskich Technologii", która jest wirtualnym miejscem spotkań gmin z dostawcami technologii mogącymi być wykorzystywanymi w procesie świadczenia usług lokalnych. Na platformie publikowane są informacje na temat rozwiązań technologicznych dostosowanych do specyfiki działalności administracyjnej gmin i procesu świadczenia przez nie usług. Gminy mogą wybrać interesujące je rozwiązanie, porównać z innymi oraz wystąpić o mikrogrant w kwocie do 50 tys. złotych na testowanie wybranego rozwiązania. Podmioty współpracujące z PFR służą pomocą w wyborze najkorzystniejszego rozwiązania. Na platformie są publikowane elektroniczne kursy dotyczące tego, które rozwiązania technologiczne można zastosować w różnych sferach działalności gmin, i na których przetestowanie można otrzymać dofinansowanie.

W pierwszym konkursie, który zorganizowano w październiku 2022 r., złożono 76 wniosków, a granty na łączną kwotę 275 tys. zł otrzymało sześć gmin (*Giełda…*, b.d.):

- Kowary na stworzenie elektronicznego zarządzania dokumentacją,
- Miejsce Piastowe na stworzenie elektronicznych deklaracji na podatki lokalne,
- Nowe Skalmierzyce na portal komunikacji online,
- Pruszcz Gdański na system zarządzania infrastrukturą drogową,
- Rybnik na przygotowanie wirtualnej karty mieszkańca,
- Świdnica na opracowanie mapy potencjału solarnego.

4.3. Ogólna charakterystyka źródeł finansowania transformacji cyfrowej gmin z tradycyjnych funduszy UE dostępnych do końca perspektywy finansowej 2014–2020

Rozwój gospodarki cyfrowej jest jednym z priorytetów UE, dlatego Komisja Europejska przygotowała kilkanaście instrumentów, o których środki mogą się ubiegać różne podmioty z państw członkowskich UE, w tym jst. Niektóre z tych instrumentów są finansowane z funduszy UE instrumentami polityki spójności. Do najważniejszych funduszy należy zaliczyć (Głąbicka i Grewiński, 2005): Europejski Fundusz Rozwoju Regionalnego (EFRR), Europejski Fundusz Społeczny (EFS) oraz Fundusz Spójności. Stosunkowo nowym – zaproponowanym w 2019 r. – funduszem jest Fundusz na rzecz Sprawiedliwej Transformacji (FST).

Wykorzystanie funduszy UE jest możliwe na podstawie tzw. programów operacyjnych, czyli dokumentów przygotowywanych przez poszczególne państwa członkowskie UE, w których zapisuje się najważniejsze priorytety i ogólne zasady przyznawania środków z funduszy UE. W tabeli 17 zestawiono nazwy tych programów obowiązujące w Polsce w latach 2007–2020. Do perspektywy trwającej od 2021 r. odniesiono się w dalszej części rozdziału.

Tabela 17. Programy operacyjne, na podstawie których przyznawano środki finansowe z funduszy UE w latach 2007–2020

Perspektywa finansowa	
2007–2013	**2014–2020**
program operacyjny Innowacyjna Gospodarka (POIG)	program operacyjny Inteligentny Rozwój (POIR)
program operacyjny Polska Cyfrowa (POPC)	
program operacyjny Infrastruktura i Środowisko (POIŚ)	
program operacyjny Rozwój Polski Wschodniej	program operacyjny Polska Wschodnia
program operacyjny Kapitał Ludzki	program operacyjny Wiedza Edukacja Rozwój
program operacyjny Pomoc Techniczna	
16 regionalnych programów operacyjnych	

Źródło: opracowanie własne na podstawie (Gwizda i in., 2014; Szymańska, 2019).

Szczegółowe omówienie tych dokumentów wykracza poza ramy tej książki i nie jest uzasadnione ze względu na finalizowanie projektów dofinansowywanych na podstawie zawartych w nich wytycznych. Mając na uwadze przedmiot tego opracowania, warto zwrócić uwagę na trzy programy. W latach 2007–2013

ważnym dokumentem był program operacyjny Innowacyjna Gospodarka, na którego podstawie przyznawano środki na zadania wspierające innowacyjność od technologicznej poprzez produktową, usługową do marketingowej włącznie, co miało się przełożyć na bardziej efektywną współpracę nauki, technologii oraz gospodarki.

W latach 2014–2020 wymieniony dokument został zastąpiony przez dwa nowe programy – program operacyjny Polska Cyfrowa (POPC) oraz program operacyjny Inteligentny Rozwój (POIR). Środki wypłacane na podstawie drugiego z tych dokumentów również były przeznaczane na stymulowanie innowacji, ale poprzez wspieranie projektów od ich początkowej fazy (powstania pomysłu) aż do fazy końcowej (całkowitej realizacji), czego skutkiem miał być wzrost potencjału gospodarki (Gwizda i in., 2014).

Nowym dokumentem był POPC. Środki ujęte w tym programie miały się przyczyniać do rozwoju obszarów informacyjno-komunikacyjnych i wzmocnić cyfryzację Polski. Ze środków przyznawanych na jego podstawie finansowano przede wszystkim upowszechnianie dostępu do szybkiego internetu, wzrost efektywności pracy urzędów poprzez e-usługi publiczne, ułatwienie dostępu do danych oraz ich upublicznienie w Centralnym Repozytorium Informacji Publicznej. Co więcej, istotna dla celów POPC w perspektywie lat 2014–2020 była też aktywizacja cyfrowa społeczeństwa poprzez e-integrację oraz e-aktywizację wspierające kompetencje cyfrowe, które przyczyniają się do rozwoju potencjału programistów, a tym samym tworzenia nowoczesnych rozwiązań cyfrowych dla administracji i całej gospodarki (Gwizda i in., 2014).

4.4. Priorytety Unii Europejskiej wyznacznikiem źródeł i kierunków finansowania transformacji cyfrowej gmin po 2020 roku

Jednym z priorytetów Komisji Europejskiej na lata 2021–2027 jest cyfryzacja, czyli rozwijanie ogólnodostępnej edukacji cyfrowej o wysokiej jakości oraz rozwijanie potencjału cyfrowego gospodarek państw członkowskich Unii Europejskiej. Komisja Europejska zakłada, że w latach 20. XXI w. nastąpi dynamiczny rozwój społeczeństwa i gospodarki UE. Impulsem tego rozwoju mają być technologie informacyjno-komunikacyjne.

Dążenie do unowocześnienia społeczeństw i gospodarek UE zostało uwypuklone poprzez opracowanie tzw. Europejskiego Kompasu Cyfrowego do 2030 r., w którym określono cztery kierunki transformacji cyfrowej oraz docelowe (do 2030 r.) mierniki osiągnięcia założonych celów (tabela 18).

Tabela 18. „Cyfrowe" cele UE do osiągnięcia do 2030 roku

Umiejętności	– specjaliści w dziedzinie ICT: 20 mln specjalistów oraz większa równowaga płci w zawodzie – podstawowe umiejętności cyfrowe: min. 80% ludności mającej podstawowe umiejętności cyfrowe
Bezpieczna i zrównoważona infrastruktura cyfrowa	– łączność: gigabit dla każdego, 5G wszędzie – najlepszej jakości półprzewodniki: dwukrotnie większy udział UE w światowej produkcji półprzewodników – dane – rozwiązania brzegowe i chmurowe: 10 tys. bezpiecznych węzłów brzegowych[a], neutralnych dla klimatu – przetwarzanie danych: pierwszy komputer z przyspieszeniem kwantowym
Transformacja cyfrowa przedsiębiorstw	– wykorzystanie technologii: 75% przedsiębiorstw w UE powinno korzystać z chmury, sztucznej inteligencji, dużych zbiorów danych – innowatorzy: rozwój scale-upów i finansowanie, aby podwoić liczbę tzw. jednorożców[b] w UE – opóźnienia w rozwoju technologicznym: ponad 90% małych i średnich przedsiębiorstw powinno osiągnąć co najmniej podstawowy poziom wykorzystania technologii cyfrowych
Cyfryzacja usług publicznych	– najważniejsze usługi publiczne: 100% online – e-zdrowie: 100% obywateli z dostępem do dokumentacji medycznej w formie elektronicznej – tożsamość cyfrowa: 80% obywateli korzystających z cyfrowego dowodu tożsamości

[a] Węzeł brzegowy jest to komputer, który działa jako portal użytkownika końcowego (lub „brama") do celów komunikacji z innymi węzłami w klastrach obliczeniowych, w których wiele komputerów korzysta z tych samych elementów systemu oprogramowania.

[b] Jednorożce oznaczają: (1) zrealizowanego jednorożca, tj. przedsiębiorstwo założone po 1990 r., którego pierwsza oferta publiczna lub sprzedaż na rzecz inwestora branżowego przyniosła powyżej 1 mld USD oraz (2) niezrealizowanego jednorożca, tj. przedsiębiorstwo, które w ostatniej rundzie prywatnego finansowania kapitału wysokiego ryzyka wyceniono na co najmniej 1 mld USD (tzn. wyceny nie potwierdzono w transakcji wtórnej)

Źródło: opracowanie własne na podstawie (*Cyfrowa dekada…*, b.d.).

Zakłada się, że do 2030 r. zostaną osiągnięte cele wymienione w tabeli 18 oraz zostanie podniesiony stopień cyfryzacji społeczeństwa i gospodarek Unii Europejskiej. Założenia zawarte w unijnym „kompasie" cyfrowym znalazły odzwierciedlenie w celach polityki spójności UE na lata 2021–2027, a w konsekwencji także w tzw. umowie partnerstwa, czyli dokumencie, w którym zapisuje się uzgodnione między Komisją Europejską a państwem członkowskim kierunki wydatkowania środków finansowych przeznaczonych na politykę spójności UE.

W zasadzie wszystkie cele polityki spójności na lata 2021–2027 odnoszą się w pewnym stopniu do cyfryzacji, ponieważ wyzwania, które leżały u podstaw ich wyznaczania, mogą być osiągane z wykorzystaniem ICT. Jednak spośród 19 celów szczegółowych przedstawionych w tabeli 19 wprost do cyfryzacji

Tabela 19. Cele polityki spójności UE na lata 2021–2027 i dziedziny wsparcia

Cel	Dziedziny (obszary) wsparcia przyjęte w polskiej Umowie partnerstwa
Cel 1: Bardziej konkurencyjna i inteligentna Europa	1. Wzrost znaczenia badań i innowacji oraz wykorzystanie zaawansowanych technologii 2. Wzmocnienie potencjału przedsiębiorstw i administracji publicznej na rzecz nowoczesnej gospodarki 3. Wzmacnianie łączności cyfrowej
Cel 2: Bardziej przyjazna dla środowiska niskoemisyjna Europa	2.1. Efektywność energetyczna 2.2. Wsparcie infrastruktury energetycznej i inteligentnych rozwiązań 2.3. Wsparcie produkcji energii ze źródeł odnawialnych 2.4. Przystosowanie do zmian klimatu 2.5. Gospodarka odpadowa i efektywne wykorzystanie zasobów 2.6. Zrównoważona gospodarka wodna i ściekowa 2.7. Ochrona dziedzictwa przyrodniczego i różnorodności biologicznej 2.8. Transport niskoemisyjny i mobilność miejska
Cel 3: Lepiej połączona Europa	3.1. Transport 3.2. Cyfryzacja
Cel 4: Europa o silniejszym wymiarze społecznym	4.1. Rynek pracy, zasoby ludzkie 4.2. Edukacja, kształcenie, umiejętności 4.3. Włączenie i integracja społeczna 4.4. Ochrona zdrowia 4.5. Kultura i turystyka
Cel 5: Europa bliżej obywateli	5.1. Europa bliżej obywateli
Cel 6: Łagodzenie skutków transformacji w kierunku gospodarki neutralnej dla klimatu	6.1. Europa w drodze ku gospodarce neutralnej dla klimatu

Źródło: opracowanie własne na postawie (*Projekt…*, 2021).

nawiązują cele 1.2 – wzmocnienie potencjału przedsiębiorstw i administracji publicznej na rzecz nowoczesnej gospodarki – oraz 3.2. – cyfryzacja.

W Umowie partnerstwa zapisano, że Polska otrzyma na inwestycje ponad 72,2 mld euro z dotychczasowych funduszy UE, a dodatkowo 3,8 mld euro z nowego źródła – Funduszu na rzecz Sprawiedliwej Transformacji (*Fundusze…*, b.d.). Należy go traktować jako uzupełniające – względem EFRR i EFS – źródło finansowania projektów wykonywanych na obszarach borykających się z dużymi wyzwaniami społeczno-gospodarczymi w związku z dążeniem UE do osiągnięcia do 2050 r. neutralności klimatycznej kojarzonej z hasłem Europejski Zielony Ład. Głównym celem FST jest dywersyfikacja gospodarcza obszarów, które zostały najmocniej dotknięte skutkami klimatycznej transformacji, łago-

dzenie tych skutków poprzez finansowanie modernizacji lokalnej gospodarki oraz wspieranie zatrudnienia. W tym celu ze środków FST będą finansowane inwestycje z zakresu: łączności cyfrowej, czystych technologii energetycznych, redukcji emisji, regeneracji obszarów przemysłowych, przekwalifikowania pracowników. Podstawą do ubiegania się o te środki będą krajowe i regionalne dokumenty – tzw. programy.

W tabeli 20 zestawiono cele polityki spójności UE z funduszami, z których finansowane będą działania przyczyniające się do osiągnięcia celów UE, oraz z nazwami programów. Władze jst oraz pracownicy samorządowi powinni znać źródła finansowania zadań oraz dokumenty planistyczne, w których zapisuje się cele UE, sposoby ich osiągania oraz źródła ich finansowania. Przygotowując wniosek o dofinansowania ze środków UE, jst musi wskazać, jaki cel UE zostanie osiągnięty dzięki wykonaniu zadania, o którego dofinansowanie się ubiega. Konieczne jest wskazanie podstawy prawnej (w tym nazwy programu) ubiegania się o dofinansowanie.

Tabela 20. Źródła finansowania celów polityki spójności UE na lata 2021–2027 oraz nazwy krajowych programów

Cel polityki spójności	Źródło finansowania (nazwa funduszu)	Rodzaj dokumentu (programu)
Cel 1	Europejski Fundusz Rozwoju Regionalnego (EFRR)	Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG)
		Fundusze Europejskie na Rozwój Cyfrowy (FERC)
		Fundusze Europejskie dla Polski Wschodniej (FEPW)
		16 regionalnych programów
Cel 2	– Fundusz Spójności (FS) – Europejski Fundusz Rozwoju Regionalnego (EFRR) – Europejski Fundusz Morski, Rybacki i Akwakultury	Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko (FEnIKS)
		Fundusze Europejskie dla Polski Wschodniej (FEPW)
		Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG)
		Fundusze Europejskie dla Rybactwa
		16 regionalnych programów
Cel 3	– Fundusz Spójności (FS) – Europejski Fundusz Rozwoju Regionalnego (EFRR)	Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko (FEnIKS)
		Fundusze Europejskie dla Polski wschodniej (FEPW)
		16 regionalnych programów

cd. tabeli 20

Cel polityki spójności	Źródło finansowania (nazwa funduszu)	Rodzaj dokumentu (programu)
Cel 4	– Europejski Fundusz Rozwoju Regionalnego (EFRR) – Europejski Fundusz Społeczny (EFS)	Fundusze Europejskie dla Rozwoju Społecznego (FERS)
		Fundusze Europejskie dla Polski Wschodniej (FEPW)
		Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko (FEnIKS)
		Fundusze Europejskie Pomoc Żywnościowa
		16 regionalnych programów
Cel 5	– Europejski Fundusz Rozwoju Regionalnego (EFRR) – Europejski Fundusz Morski, Rybacki i Akwakultury	Fundusze Europejskie dla Rybactwa
		16 regionalnych programów
Cel 6	Fundusz na rzecz Sprawiedliwej Transformacji	Program Fundusze Europejskie na rzecz Sprawiedliwej Transformacji Krajowy Plan Odbudowy i Zwiększania Odporności (tzw. KPO)

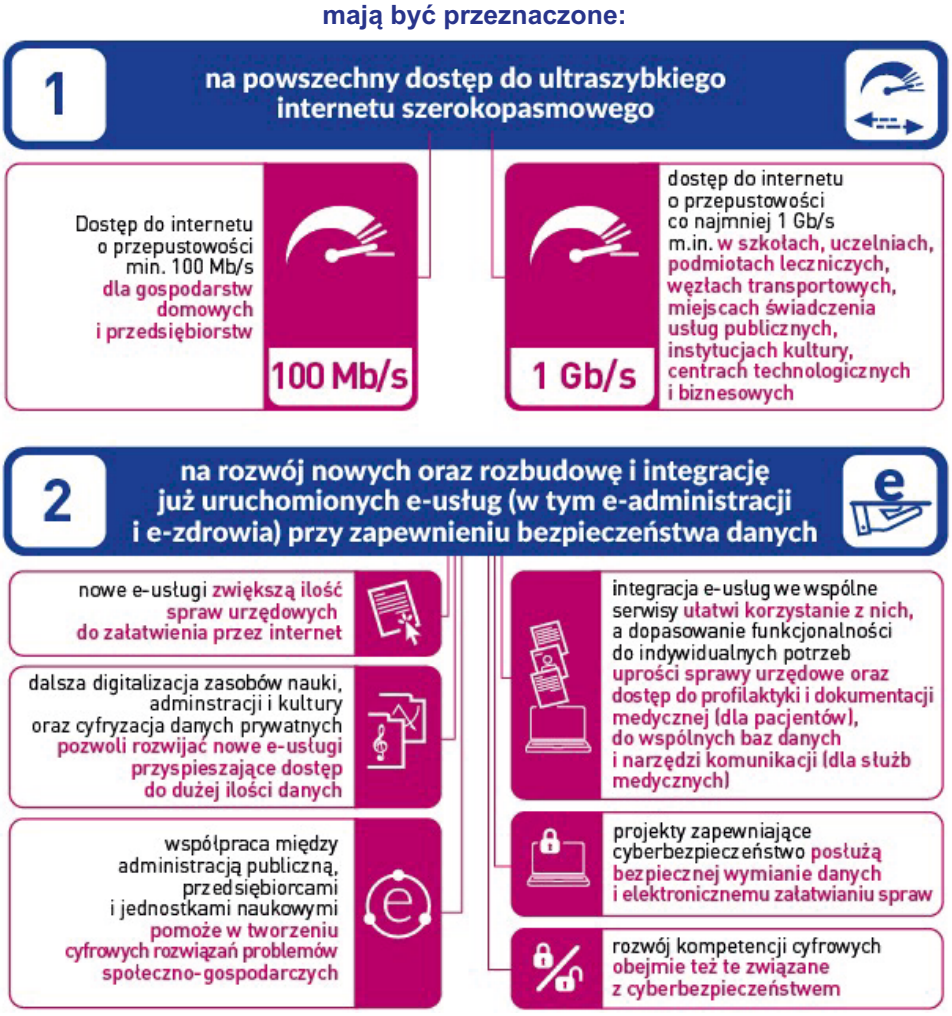
Źródło: opracowanie własne na podstawie (*Projekt…*, 2021).

4.5. Możliwości finansowania transformacji cyfrowej gmin ze środków Unii Europejskiej w latach 2021–2027

4.5.1. Europejski Fundusz Rozwoju Regionalnego i program operacyjny Fundusze Europejskie na Rozwój Cyfrowy 2021–2027

Głównym źródłem finansowania cyfryzacji samorządu terytorialnego jest zaliczony do źródeł tradycyjnych Europejski Fundusz Rozwoju Regionalnego, a podstawowym dokumentem, w którym określono rodzaje dofinansowanych zadań, jest program Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) (*Fundusze…*, 2022). O dofinansowanie podejmowanych przez siebie zadań będą mogły się ubiegać różne podmioty: przedsiębiorcy, organizacje pozarządowe, urzędy jst, szkoły, instytucje kultury, podmioty lecznicze. W tym miejscu zostaną scharakteryzowane najważniejsze rodzaje zadań jst, które mogą byś sfinansowane ze środków dzielonych na podstawie tego dokumentu.

Celem programu FERC jest wsparcie transformacji cyfrowej Polski. Przewidziano w nim dofinansowanie przedsięwzięć, które zapewnią (rysunek 15): szeroki dostęp do bardzo szybkiego internetu, efektywne i przyjazne użytkownikom zaawansowane e-usługi publiczne, skuteczne działanie krajowego systemu cyberbezpieczeństwa, dostęp do otwartych danych (z możliwością ich dalszego wykorzystywania), wsparcie rozwoju umiejętności cyfrowych Polaków. Przedsięwzięcia



Rysunek 15. Ogólna charakterystyka rodzajów projektów finansowanych ze środków programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027

Źródło: https://www.funduszeeuropejskie.gov.pl/strony/wiadomosci/polska-rewolucja-cyfrowa-trwa-wez-w-niej--udzial/

te powinny zintensyfikować współpracę międzysektorową na rzecz rozwiązywania problemów społeczno-gospodarczych przy pomocy ICT.

Zakres interwencji programu FERC wpisuje się w działania wskazane w europejskich i krajowych dokumentach strategicznych odnoszących się do transformacji cyfrowej. Są to następujące dokumenty:

– Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie[5],
– Europejska strategia w zakresie danych,
– Strategia UE w zakresie unii bezpieczeństwa,
– Strategia na rzecz odpowiedzialnego rozwoju do roku 2020 (z perspektywą do 2030 r.),
– Krajowa strategia rozwoju regionalnego 2030,
– Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

W programie FERC przewidziano środki na dofinansowanie w formie dotacji przedsięwzięć, które wychodzą naprzeciw wyzwaniom współczesnej gospodarki wskazanych w krajowych dokumentach: Narodowym Planie Szerokopasmowym, Programie zintegrowanej informatyzacji państwa oraz Programie otwierania danych na lata 2021–2027.

W tabeli 21 przedstawiono budowę programu FERC (zestawiono priorytety i kierunki wsparcia).

Tabela 21. Budowa programu operacyjnego Fundusze Europejskie na Rozwój Cyfrowy na lata 2021–2027

Priorytety programu FERC	Cele szczegółowe	Spodziewany efekt
Priorytet 1. Zwiększenie dostępu do bardzo (ultra) szybkiego internetu szerokopasmowego	1.1. Zwiększenie dostępu do bardzo (ultra) szybkiego internetu szerokopasmowego	udoskonalenie łączności cyfrowej
Priorytet 2. Zaawansowane usługi cyfrowe	2.1. Wysoka jakość i dostępność e-usług publicznych 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa 2.3. Cyfrowa dostępność i ponowne wykorzystanie informacji 2.4. Współpraca międzysektorowa na rzecz cyfrowych rozwiązań problemów społeczno-gospodarczych 2.5. Wsparcie umiejętności cyfrowych	czerpanie korzyści z cyfryzacji przez obywateli, przedsiębiorstwa, organizacje badawczych i instytucje publiczne

cd. tabeli 21

Priorytety programu FERC	Cele szczegółowe	Spodziewany efekt
Priorytet 3. Pomoc techniczna		podniesienie kompetencji beneficjentów programu FERC, w tym potencjalnych, dotyczących przygotowania dokumentacji projektowej oraz beneficjentów i instytucji systemu wdrażania (w zakresie przygotowania i rozliczania wniosków o płatność)

Źródło: opracowanie własne na podstawie (*Fundusze…*, 2022).

Z punktu widzenia samorządu terytorialnego szczególnie ważny jest priorytet II. Ze środków zaplanowanych na „Zaawansowane usługi cyfrowe" będą dofinansowywane projekty o charakterze ogólnopolskim, których efekty będą mogły być wykorzystane przez jst. Zaplanowano tu środki na: poprawę jakości e-usług publicznych i ich rozwój, w tym standaryzację. Ponadto środki będą udostępniane na projekty przyczyniające się do rozwoju krajowego systemu cyberbezpieczeństwa. Celem tych działań będzie poprawa odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych w najważniejszych podmiotach publicznych. Część środków zostanie przeznaczona na projekty zwiększające dostęp społeczeństwa do otwartych danych publicznych (zasobów kultury, nauki i administracji), w tym w czasie rzeczywistym. Środki w tym priorytecie będą mogły być przeznaczane także na wspólne międzysektorowe projekty, które będą wykorzystywać nowe technologie do rozwiązywania problemów społeczno-gospodarczych. Środki te będą też przeznaczane na podnoszenie kompetencji pracowników sektora finansów publicznych. Finansowane mają być szkolenia z zakresu cyfryzacji gospodarki, możliwości wykorzystywania ICT w procesie świadczenia usług, cyberbezpieczeństwa.

Scharakteryzowany fundusz nie jest jedynym funduszem unijnym, z którego można finansować zadania składające się na transformację cyfrową gmin w latach 2021–2027. W zależności od tego, jakie rozwiązanie miałoby zostać sfinansowane, gminy mogą składać wnioski o dofinansowanie z innych krajowych programów oraz z odpowiedniego programu regionalnego (wojewódzkiego). W tabeli 22 zestawiono przykładowe projekty i potencjalne źródła ich finansowania.

Tabela 22. Przykłady działań z zakresu transformacji cyfrowej gmin i potencjalne źródła ich finansowania

Przykłady projektów	Potencjalne zagraniczne źródło finansowania (nazwa programu)
– Utworzenie klubu rozwoju cyfrowego – ośrodka aktywizacji cyfrowej społeczności lokalnej – Poprawa dostępności cyfrowej – Powołanie asystenta rozwoju kompetencji cyfrowych – Stworzenie systemu gromadzenia danych – Cyfryzacja systemu oświaty	– Fundusze Europejskie na Rozwój Cyfrowy – Fundusze Europejskie dla Rozwoju Społecznego 2021–2027 – 16 regionalnych programów
– Montaż urządzeń zwiększających „cyfryzację" budynków użyteczności publicznej – Tworzenie cyfrowych systemów transportu miejskiego – Budowa kompleksowych rozwiązań chroniących system transportu i jego infrastrukturę przed cyberzagrożeniami – Tworzenie cyfrowych narzędzi zarządzania systemami elektroenergetycznymi – Cyfryzacja placówek podstawowej opieki zdrowotnej, w tym prowadzonych przez jst, i rozwój telemedycyny – Podnoszenie kompetencji kadr, w tym pracowników samorządowych instytucji kultury – Edukacja cyfrowa dorosłych – Upowszechnienie usług kulturalnych dostępnych online	– Fundusze Europejskie na Rozwój Cyfrowy – Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko 2021–2027 – 16 regionalnych programów

Uwzględniono jedynie programy operacyjne finansowane ze źródeł tradycyjnych.

Źródło: opracowanie własne na podstawie (MFiPR, 2022a, 2022b).

4.5.2. Instrument na rzecz Odbudowy i Zwiększania Odporności oraz Krajowy Plan Odbudowy i Zwiększania Odporności

Ważnym źródłem finansowania transformacji cyfrowej jst ma być Instrument na rzecz Odbudowy i Zwiększania Odporności (*Recovery and Resilience Facility – RRF*). Ten zasób środków został wygospodarowany przez UE w związku z koniecznością odbudowy unijnej gospodarki po kryzysie wywołanym pandemią COVID-19. Jest on elementem unijnego planu odbudowy *Next Generation EU* (Rozporządzenie PEiR, 2021). Wsparcie z tego źródła ma charakter dodatkowy w stosunku do środków wypłacanych z innych funduszy i programów unijnych, w związku z tym musi być z nimi spójne i skoordynowane. Zbieżność ta

jest widoczna m.in. w tzw. obszarach wsparcia. Zgodnie z celami UE 42,7% środków zostanie przeznaczonych na cele klimatyczne, a 20,85% na transformację cyfrową.

Wsparcie przyjmie postać dotacji oraz preferencyjnych pożyczek. Polska ma otrzymać 35,962 mld euro (około 158,5 mld zł), w tym 23,850 mld euro (około 106,9 mld zł) w formie dotacji oraz 12,112 mld euro (około 51,6 mld zł) w formie pożyczek, których spłata ma potrwać co najwyżej do 2058 r. Warunkiem koniecznym umożliwiającym otrzymanie przez Polskę środków finansowych z RRF było przygotowanie Krajowego Planu Odbudowy i Zwiększania Odporności (zwanego w skrócie KPO) i przyjęcie go przez Radę UE[8]. Otrzymanie środków musi poprzedzić podpisanie umowy z Komisją Europejską na tzw. część grantową oraz umowy na część pożyczkową. Horyzont czasowy realizacji dokumentu to okres od 1 lutego 2020 r. do 31 sierpnia 2026 r.

Na rysunku 16 przedstawiono podział środków ujętych w KPO na formę prawną (dotacja, pożyczka) oraz obszary wsparcia (komponenty KPO). Środki mają być przeznaczone na takie zadania, które przyczynią się do stymulowania gospodarki, inwestycji, wzrostu gospodarczego oraz zatrudnienia. Dofinansowane będą te działania, które rząd uznał za najważniejsze z punktu widzenia konieczności odbudowy gospodarki po pandemii COVID-19, oraz te, które tworzą podstawę budowy gospodarki odpornej na kolejne kryzysy. Według postanowień zawartych w KPO odbudowa polskiej gospodarki po kryzysie wywołanym pandemią COVID-19 ma się odbywać według pięciu głównych filarów (priorytetów) (*Krajowy Plan*…, 2021):

– odporność i konkurencyjność gospodarki,
– zielona energia i zmniejszenie energochłonności,
– transformacja cyfrowa,
– efektywność, dostępność i jakość systemu ochrony zdrowia,
– zielona, inteligentna mobilność.

W KPO przewidziano też środki na poprawę jakości instytucji i warunków jego realizacji, czyli na tzw. pomoc techniczną.

Cele, które rząd zamierza osiągnąć, dystrybuując środki na podstawie KPO, pokrywają się w większości z celami FERC, gdyż są to: wsparcie infrastruktury łączności, e-usług, kompetencji cyfrowych oraz cyberbezpieczeństwa. Dodano do nich cyfrową edukację i wykorzystanie rozwiązań technologii przełomowych. Na rysunkach 17 i 18 przedstawiono cele, które Polska chce osiągnąć, finansując inwestycje z zakresu transformacji cyfrowej z dotacji i pożyczek udzielanych ze środków Instrumentu na rzecz Odbudowy i Zwiększania Odporności.

Rysunek 16. Podział środków Krajowego Planu Odbudowy na tzw. obszary wsparcia (komponenty)

Źródło: (*Krajowy Plan…*, 2021).

Podsumowanie komponentu: **„Transformacja cyfrowa”**
Obszar/zakres polityki: cyfryzacja
Wyzwanie: zapewnienie rozwoju infrastruktury łączności cyfrowej oraz rozwiązań w zakresie e-usług, wykorzystania potencjału technologii przełomowych, cyfrowej edukacji, wzrostu kompetencji cyfrowych społeczeństwa, a także cyberbezpieczeństwa
Cel: Wzmocnienie przemian cyfrowych w sektorze publicznym, społeczeństwie i gospodarce
Cele szczegółowe:
C1: Poprawa dostępu do szybkiego internetu
Reformy: C1. 1. Zapewnienie powszechnego dostępu do szybkiego internetu – rozwój infrastruktury sieciowej
Inwestycje C1. 1.1. Zapewnienie dostępu do bardzo szybkiego internetu na obszarach białych plam
C2: Rozwój e-usług i ich konsolidacja, tworzenie warunków dla zastosowań przełomowych technologii cyfrowych w sektorze publicznym, gospodarce i społeczeństwie oraz usprawnienie komunikacji między instytucjami publicznymi, obywatelami i biznesem
Reformy: C2.1. Zwiększenie skali zastosowań rozwiązań cyfrowych w sferze publicznej, gospodarce i społeczeństwie
Inwestycje: C2. 1.1. E-usługi publiczne, rozwiązania IT usprawniające funkcjonowanie administracji i sektorów gospodarki oraz technologie przełomowe w sektorze publicznym, gospodarce i społeczeństwie C2 1.2. Wyrównanie poziomu wyposażenia szkół w przenośne urządzenia multimedialne C2 1.3. E-kompetencje
C3. Wzrost bezpieczeństwa w cyberprzestrzeni, zabezpieczenie infrastruktury przetwarzania danych oraz cyfryzacja infrastruktury służb odpowiedzialnych za bezpieczeństwo
Reformy: C3.1. Zwiększenie cyberbezpieczeństwa systemów informacyjnych, wzmocnienie infrastruktury przetwarzania danych
Inwestycje: C3.1.1. Cyberbezpieczeństwo – CyberPL oraz infrastruktura przetwarzania danych i dostarczania usług cyfrowych
Wpływa na realizację następujących celów zrównoważonego rozwoju: 
Szacowany koszt: 2796 mln euro

Rysunek 17. Cele, które mają być osiągnięte w związku z finansowaniem transformacji cyfrowej w formie dotacji przyznawanych na podstawie KPO

Źródło: (*Krajowy Plan…*, 2021).

Podsumowanie komponentu: **„Transformacja cyfrowa”**
Obszar/zakres polityki: cyfryzacja
Wyzwanie: zapewnienie rozwoju infrastruktury łączności cyfrowej oraz rozwiązań w zakresie e-usług, wykorzystania potencjału technologii przełomowych, cyfrowej edukacji, wzrostu kompetencji cyfrowych społeczeństwa, a także cyberbezpieczeństwa
Cel: Wzmocnienie przemian cyfrowych w sektorze publicznym, społeczeństwie i gospodarce
Cele szczegółowe:
C1: Poprawa dostępu do szybkiego internetu
Reformy: C1. 2. Podniesienie poziomu dostępności i wykorzystania nowoczesnej łączności przewodowej i bezprzewodowej na potrzeby społeczne i gospodarcze
Inwestycje C1. 2.1. Wzmocnienie potencjału komercyjnych inwestycji w nowoczesne sieci łączności elektronicznej
C2: Rozwój e-usług i ich konsolidacja, tworzenie warunków dla zastosowań przełomowych technologii cyfrowych w sektorze publicznym, gospodarce i społeczeństwie oraz usprawnienie komunikacji między instytucjami publicznymi, obywatelami i biznesem
Reformy: C2. 2. Reforma podstaw cyfryzacji systemu oświaty i wychowania
Inwestycje: C2. 2.1. Rozwój cyfrowego otoczenia procesu wychowania przedszkolnego i kształcenia ogólnego
Wpływa na realizację następujących celów zrównoważonego rozwoju:

Szacowany koszt: 2100 mln euro

Rysunek 18. Cele, które mają być osiągnięte w związku z finansowaniem transformacji cyfrowej w formie pożyczek przyznawanych na podstawie KPO

Źródło: (*Krajowy Plan…*, 2021).

4.5.3. Programy Komisji Europejskiej[29]

Dotychczas omówione tradycyjne i nowe źródła finansowania transformacji cyfrowej gmin należy uzupełnić o kilka innych instrumentów – programów Komisji Europejskiej. Do programów zarządzanych centralnie przez tę komisję należą m.in.: Łącząc Europę (CEF – *Connecting Europe Facility*), Horyzont

[29] Punkt opracowano na podstawie (Tarczyńska, 2021).

Europa, Cyfrowa Europa, InvestEU, WiFi4EU. Środki z tych programów są dodatkowym źródłem finansowania zadań przyczyniających się do osiągnięcia celów UE, w tym z zakresu transformacji cyfrowej państw członkowskich UE. Część środków ujętych w wymienionych programach podzielono pomiędzy poszczególne państwa, ale o większość trzeba się ubiegać, przystępując do konkursów ogłaszanych przez agencje KE (*Programy Komisji…*, b.d.)

Zapewnienie dobrze funkcjonującej, w pełni wykorzystującej możliwości swobodnego przepływu oraz jednolitego rynku UE przez podmioty na nim działające wymaga wysokiego poziomu infrastruktury transportowej w obszarze energii oraz technologii cyfrowych. Do osiągnięcia tych założeń mają się przyczynić środki instrumentu Łącząc Europę (*CEF – Connecting Europe Facility*). Instrument ten, ustanowiony w 2013 r. przez Parlament Europejski oraz Radę UE, zastąpił istniejący wcześniej program Sieci Transeuropejskie (TEN). Jest to instrument finansujący inwestycje strategiczne z zakresu infrastruktury transportowej, energetycznej oraz cyfrowej. Jego celem jest zrównoważony wzrost, który ma sprzyjać włączeniu społecznemu oraz zwiększeniu konkurencyjności i spójności społecznej oraz gospodarczej i terytorialnej.

Instrument Łącząc Europę wspiera projekty z zakresu infrastruktury mające ułatwić integrację (łączenie się) UE i jej regionów w zakresie transportu, energii, klimatu i technologii cyfrowych, co pozwoli na zintensyfikowanie cyfryzacji gospodarki UE oraz jej dekarbonizację (redukcję emisji dwutlenku węgla). W latach 2021–2027 instrument Łącząc Europę opiewa na kwotę 42,3 mld euro, z czego 3 mln przeznaczono na sektor technologii cyfrowych. W tym miejscu zostaną zasygnalizowane tylko działania z zakresu technologii cyfrowych. Ważnym zadaniem jest tu budowanie sieci szerokopasmowych charakteryzujących się jak najwyższą przepustowością oraz infrastruktury niezbędnej do świadczenia usług cyfrowych. Ma to się przyczynić do ogólnie rozumianej transformacji cyfrowej całego społeczeństwa i gospodarki. W tym priorytecie są też finansowane projekty, których realizacja jest efektem strategii na rzecz społeczeństwa gigabitowego z 2016 r. Działanie to kładzie również nacisk na projekty umożliwiające efektywne działanie jednolitego rynku cyfrowego, podmiotów rynku służących społeczeństwu oraz je wspierających, np. szpitale oraz szkoły, korzystających z połączenia gigabitowego oraz jednostek korzystających z sieci 5G. Ostatnim celem instrumentu Łącząc Europę w zakresie cyfrowym jest osiągnięcie bardzo wysokiego poziomu łączności bezprzewodowej na szczeblu lokalnym, a także działania sprzyjające przyłączeniu społeczeństwa oraz gospodarstw domowych państw członkowskich UE do sieci zapewniającej bardzo dużą przepustowość (KE, 2021a).

Horyzont Europa to program ustanowiony na lata 2021–2027, który zastąpił program Horyzont 2020 realizowany na rzecz badań i rozwoju. Z programu wydatkowanych będzie około 95,5 mld euro. Do jego głównych celów należy od-

działywanie na rozwój polityk UE poprzez wspieranie badań i innowacji, wsparcie implementacji innowacyjnych rozwiązań przez przemysł oraz stawianie czoła globalnym wyzwaniom. Program Horyzont Europa ma służyć wspieraniu badań naukowych i innowacji z uwzględnieniem ich zmieniającego się ciągle charakteru, by zapewnić osiąganie jak największej spójności oraz coraz lepsze wyniki (Krajowy Punkt…, 2021).

Horyzont Europa składa się z trzech filarów, które są ze sobą wzajemnie połączone, wspomagając nawzajem swoje działania: 1. Otwarta nauka, 2. Globalne wyzwania i konkurencyjność przemysłowa, 3. Otwarte innowacje. Filar drugi dotyczy działań podejmowanych w celu sprostania wyzwaniom społecznym oraz związanym z technologią przemysłową. Wyzwania te zostały podzielone na pięć grup: zdrowie, integracyjne i bezpieczne społeczeństwo, technologie cyfrowe i przemysł, klimat, energetyka i mobilność, żywność i zasoby naturalne. Na szczególną uwagę zasługują grupy dotyczące bezpieczeństwa cywilnego na rzecz społeczeństwa oraz technologie cyfrowe, przemysł i przestrzeń kosmiczna, ponieważ obszary interwencji w ich ramach koncentrują się na kwestiach związanych bezpośrednio z procesem transformacji cyfrowej, tj.: cyberbezpieczeństwie, internecie nowej generacji, technologiach cyfrowych, sztucznej inteligencji i robotyce czy dużych zbiorach danych (Rozporządzenie, 2018).

Program Horyzont Europa wspiera także unijną politykę spójności, która jest jedną z głównych polityk inwestycyjnych UE, a jej celem jest niwelowanie różnic rozwojowych regionów UE oraz dążenie do zapewnienia równych szans dla jej obywateli oraz przyczynianie się do wzrostu gospodarczego – harmonijnego, zrównoważonego i trwałego (Murzyn, 2018).

Program Cyfrowa Europa jest nowym instrumentem finansowania cyfryzacji w ramie finansowej na lata 2021–2027. Uzupełnia on programy Horyzont Europa i Łącząc Europę służące wspieraniu transformacji cyfrowej. Celem tego programu jest finansowanie inwestycji „w odpowiednie zdolności cyfrowe, których pojedyncze państwo członkowskie nie jest w stanie samodzielnie wcielić w życie" (KE, 2021b). Wyróżnia się pięć priorytetów tego programu: obliczenia superkomputerowe, sztuczną inteligencję, cyberbezpieczeństwo, zaawansowane umiejętności cyfrowe oraz zapewnienie szerokiego zastosowanie technologii cyfrowych w gospodarce i społeczeństwie. Beneficjenci wywodzą się z różnych sektorów i branż. Dofinansowywane są projekty m.in. z zakresu opieki zdrowotnej, bezpieczeństwa samochodów, energii odnawialnej. Wsparcie otrzymają też publiczne i prywatne podmioty zamierzające wykorzystywać sztuczną inteligencję. Wsparcie finansowe zostanie także przeznaczone na szkolenia z zakresu umiejętności cyfrowych pracowników, w tym z sektora małych i średnich przedsiębiorstw oraz administracji publicznej, których efektem stanie się zwiększenie dostępu do wiedzy technicznej.

Pandemia COVID-19 była przyczyną wygospodarowania przez Komisję Europejską dodatkowych środków na wsparcie ożywienia gospodarczego oraz cyfrowej i zielonej transformacji, wsparcie zatrudnienia oraz przeciwdziałanie wykluczeniu społecznemu. Przybrały one postać nowego programu inwestycyjnego UE w perspektywie 2021–2027 – programu InvestEU. Głównym komponentem programu ma być fundusz Invest EU, który docelowo mają utworzyć wszystkie instrumenty finansowe UE. Ma to być główne źródło (poza funduszami UE) finansowania inwestycji w formie pożyczek, gwarancji, regwarancji, instrumentów rynku kapitałowego (*InvestEU*, 2022). Na rysunku 19 przedstawiono cztery obszary (kierunki) wsparcia z tego programu.

Rysunek 19. Obszary wsparcia programu InvestEU

Źródło: https://instrumentyfinansoweue.gov.pl/invest-eu/, 6.02.2022 r.

Projekty, które będą dofinansowane z programu InvestEU w latach 2021–2027, muszą dotyczyć jednego z czterech następujących obszarów programu InvestEU: zrównoważona infrastruktura; badania, innowacje i digitalizacja; małe i średnie przedsiębiorstwa lub inwestycje społeczne i umiejętności. Dla gmin szczególnie atrakcyjne są dwa pierwsze obszary. Środki (w kwocie 9,9 mld euro) na zrównoważoną infrastrukturę są przeznaczone na finansowanie projektów m.in. z zakresu odnawialnych źródeł energii, łączności cyfrowej, transportu, gospodarki obiegu zamkniętego, infrastruktury wodnej i środowiskowej. Środki (w kwocie 6,6 mld euro) na badania, innowacje i digitalizację są przeznaczone na finansowanie projektów m.in. z zakresu badań i innowacji, transferu wyników badań na rynek, digitalizacji przemysłu, sztucznej inteligencji.

Powstało również kilka inicjatyw, z których środki mają się przyczynić do pogłębiania transformacji cyfrowej w gminach. Należy tu wymienić „WiFi4EU", która powstała w latach 2018–2020, ale funkcjonuje nadal. Jej celem jest zapewnienie darmowego dostępu do internetu w takich miejscach publicznych, jak parki, budynki publiczne, biblioteki, szkoły, ośrodki zdrowia czy muzea. O dofinansowania w postaci jednorazowego bonu o wartości 15 tys. euro mogą się ubiegać gminy i ich stowarzyszenia oraz podmioty instalujące Wi-Fi. Lista potencjalnych beneficjentów została uzgodniona pomiędzy Komisją Europejską i państwem członkowskim. Było to niezbędne, dlatego że o dofinansowanie mogą się ubiegać tylko ci beneficjenci, na których terenie nie ma publicznych punktów dostępu do internetu. Każda gmina, która otrzymała dofinansowanie,

może je przeznaczyć na zakup oraz instalację hotspotów Wi-Fi w miejscach publicznych. Dotychczas dofinansowanie otrzymało 181 gmin z Polski (KE, b.d., *Portal*).

Omówione programy Komisji Europejskiej nie wyczerpują potencjalnych źródeł finansowania transformacji cyfrowej gmin. Niektóre programy są bowiem adresowane nie do samych urzędów administracji publicznej, ale do jednostek świadczących usługi na rzecz obywateli. Na przykład o dofinansowanie ze środków programu EU4HEALTH mogą się ubiegać podmioty lecznicze, w tym prowadzone przez jst. Jednym z celów, który ma zostać osiągnięty poprzez dofinansowywanie działań, jest przyspieszenie transformacji cyfrowej usług zdrowotnych i zwiększenie interoperacyjność (synchronizacji) takich usług. Na poziomie UE za program ten odpowiada Europejska Agencja Wykonawcza ds. Zdrowia i Cyfryzacji (*European Health and Digital Executive Agency,* HaDEA) w Brukseli, a w Polsce – Ministerstwo Zdrowia (*Programy Unii…*, b.d.).

4.6. Specjalne programy grantowe w latach 2000–2022[30]

W mediach oraz na oficjalnych stronach różnych podmiotów są ogłaszane informacje o konkursach, w których można wygrać środki finansowe na finansowanie lub dofinansowanie działań składających się na transformację cyfrową. Konkursy takie organizują ministerstwa, agencje wykonawcze, państwowe osoby prawne, a nawet spółki Skarbu Państwa. Niemożliwe jest scharakteryzowanie wszystkich konkursów, w których gminy mogłyby uczestniczyć, poszukując środków na transformację cyfrową, dlatego że nie ma katalogu takich konkursów. Różne podmioty ogłaszają je w różnych terminach. Niekiedy wnioski o dofinansowanie projektów można składać w kilku turach.

Przykładem konkursu organizowanego przez państwowe osoby prawne jest nabór gmin do współpracy przy pilotażu usługi „Zaawansowane loty bezzałogowych statków powietrznych na szeroką skalę", który został ogłoszony przez Polską Agencję Żeglugi Powietrznej (we współpracy z Urzędem Lotnictwa Cywilnego oraz Ministerstwem Infrastruktury) we wrześniu 2021 r. Pilotaż jest

[30] Ogłoszenia o możliwości ubiegania się o dofinansowanie zadań składających się na transformację cyfrową gmin były też publikowane wcześniej. Jednym z takich konkursów był konkurs Human Smart Cities. Inteligentne miasta współtworzone przez mieszkańców, ogłoszony przez Ministerstwo Funduszy i Rozwoju Regionalnego w 2017 r., a finansowany ze środków programu operacyjnego Pomoc Techniczna 2014–2020. Mogły do niego przystąpić gminy miejskie i miejsko-wiejskie. (*Konkurs*, b.d.). Do konkursu zgłosiło się 115 miast, a dofinansowanie otrzymało 25. Wśród nich są m.in.: Kielce, Lublin, Pleszew, Siemianowice Śląskie, Zduńska Wola. Projekty były realizowane do końca 2022 r. (Klyta, 2019).

finansowany w ramach programu operacyjnego Polska Cyfrowa. Agencja poszukiwała gmin zaineresowanych rozwojem „ruchu dronowego". Do konkursu przystąpiło 18 gmin. Ostatecznie stworzono trzy konsorcja składające się z miast Gliwice i Lubin oraz gmin Sośnicowice, Lesznowola, Pilchowice, Nadarzyn, Jastków i Górnośląsko-Zagłębiowskiej Metropolii. Udział w tym przedsięwzięciu umożliwia gminom wykorzystanie dronów, np. do lokalizacji obiektów emitujących zbyt dużo szkodliwych substancji. Dodatkową korzyścią jest wzrost prestiżu gminy, która jawi się jako innowacyjna i nowoczesna (Polska Agencja…, b.d.).

Koniec perspektywy finansowej 2014–2020 (nie licząc okresu na zakończenie projektów, na które przyznano dofinansowanie) zbiegł się z wybuchem pandemii COVID-19. Komisja Europejska podjęła decyzję o wydzieleniu nowego instrumentu będącego „reakcją UE na pandemię COVID-19" pod nazwą REACT-EU. Środki z tego instrumentu (uzupełnione o środki z EFRR) były rozdzielane tylko pomiędzy gminy w formule konkursu (tzw. grantowego) pod nazwą „Cyfrowa gmina", którego celem było wsparcie rozwoju cyfrowego urzędów gmin i gminnych jednostek usługowych oraz zwiększenie cyberbezpieczeństwa. Na ten cel przeznaczono 1 mld zł. Minimalna wysokość dotacji dla gminy wynosiła 100 tys. zł, a maksymalnie można było otrzymać 2 mln zł. Gminy mogły się ubiegać o środki na cyfryzację urzędów, zakup sprzętu komputerowego dla jednostek podległych, przygotowanie urzędników do pracy z nowoczesnymi technologiami, wsparcie z zakresu cyberbezpieczeństwa oraz szkolenia. Środki można było przeznaczyć m.in. na audyt (diagnozę) cyberbezpieczeństwa oraz zakup oprogramowania i urządzeń zwiększających bezpieczeństwo informacji przetwarzanych na systemach informatycznych m.in. poprzez modernizację i doposażenie serwerowni, zakup zestawów komputerowych, licencji i oprogramowania (*Regulamin…*, b.d.). Warunkiem udziału w programie było poddanie się audytowi z zakresu cyberbezpieczeństwa w terminie do 6 miesięcy od dnia zawarcia umowy o przekazanie środków (*Regulamin…*, b.d.). Zorganizowano trzy konkursy (ostatni w terminie 11.01–10.02.2022 r.). Z tego źródła można finansować wydatki poniesione w okresie od lutego 2020 r. do końca września 2023 r.

Część środków Europejskiego Funduszu Rozwoju Regionalnego wydzielono na finansowanie zadań mających na celu ograniczenie negatywnych skutków pandemii COVID-19. Środki te były udostępniane w formie „programów grantowych", co w praktyce oznacza, że potencjalni beneficjenci ubiegali się o dotację, przystępując do konkursu. Jednym z ich był program „Cyfrowa gmina – Wsparcie dzieci z rodzin popegeerowskich w rozwoju cyfrowym – granty PPGR". Celem tego projektu było zapewnienie dostępu do sprzętu komputerowego oraz do internetu rodzinom z dziećmi mieszkającym na tzw. terenach popegeerowskich. Miał on też na celu wyeliminowanie ograniczeń związanych z nauką zdalną, a także zmniejszenie różnic między gminami popegeerowskimi i pozostałymi

gminami. Do konkursu (zorganizowanego w okresie 4.10–5.11.2021 r.) mogły przystąpić gminy, które uzyskały pozytywną opinię Krajowego Ośrodka Wsparcia Rolnictwa dotyczącą „funkcjonowania na terenie gminy zlikwidowanego PPGR" oraz „występowania na terenie gminy mienia/nieruchomości PPGR, w tym nieruchomości zamieszkiwanych przez byłych pracowników PPGR" (Centrum, b.d.). Na ten cel przeznaczono 586,4 mln zł. Można było otrzymać dotację nawet w wysokości 100% kosztów kwalifikowalnych. Trudno jest się oprzeć wrażeniu, że kryteria przyznawania dotacji były bardzo liberalne. Dofinansowanie otrzymały 1604 gminy, co stanowi 64,8% wszystkich gmin w kraju, w tym m.in. Poznań, Kraków, Gdynia (*Cyfrowa*…, b.d.), które nie są kojarzone z terenami popegeerowskimi.

Oba projekty były finansowane ze środków EFRR oraz instrumentu REACT-EU na podstawie programu operacyjnego Polska Cyfrowa na lata 2014–2020, oś priorytetowa V Rozwój cyfrowy jst oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, działanie 5.1. Rozwój cyfrowy jst oraz wzmocnienie cyfrowej odporności na zagrożenia.

CYBERBEZPIECZEŃSTWO JAKO ELEMENT KONTROLI ZARZĄDCZEJ W SAMORZĄDZIE GMINNYM

5.1. Cyberbezpieczeństwo w działalności jednostki samorządowej

W związku z zachodzącymi procesami transformacji cyfrowej, które obejmują również działalność jednostek samorządu terytorialnego, coraz częściej w literaturze przedmiotu zwraca się uwagę, obok korzyści płynących z zastosowania technologii informacyjnych, na zagrożenia i wyzwania z nimi związane. Jednym z największych wyzwań stojących przed organizacjami, również przed jednostkami samorządu terytorialnego, jest konieczność zapewnienia cyberbezpieczeństwa (Macmanus i in., 2013; Ruohonen, 2020; Salminen i Hossain, 2018).

Stosowanie technologii informacyjno-komunikacyjnych (ICT) w działalności jednostek samorządowych wiąże się z koniecznością zapewnienia przez te podmioty bezpieczeństwa sieci i systemów informatycznych wykorzystywanych podczas wykonywania różnego rodzaju zadań. Przemawia za tym również fakt, że z roku na rok liczba zgłoszonych incydentów cyberbezpieczeństwa przez urzędy administracji publicznej jest coraz większa (CSIRT GOV, 2021), a w doniesieniach prasowych coraz częściej pojawiają się informacje o cyberatakach na urzędy jednostek samorządowych (Kubicka-Żach, 2019; Kwiecień, 2020; *Małopolski Urząd…*, 2021; Mastalerz, 2021; Stech, 2021).

Zdaniem autorek wdrożenie rozwiązań, które mają przyczynić się do zapewnienia cyberbezpieczeństwa w funkcjonowaniu jednostek samorządowych, należy do obowiązków kierownika jednostki, który odpowiada za całokształt systemu kontroli zarządczej w danym podmiocie. Mechanizmy kontroli systemów informacyjnych są jednym z rodzajów kontroli wymienionych w standardach kontroli zarządczej, które stanowią wskazówki dotyczące takiego kształtowania kontroli zarządczej, aby realizowała ona cele zdefiniowane prawnie (Ustawa, 2009; Komunikat, 2009).

Skuteczne wdrażanie kontroli zarządczej wymaga z kolei kompleksowego podejścia do rozwiązań wdrażanych w podmiocie. Tylko spójny, integrujący obowiązujące procedury, obejmujący wszystkie obszary i procesy działania jed-

nostki system będzie się przyczyniał do usprawniania jej działalności oraz będzie realizował cele postawione przed kontrolą zarządczą.

Celem rozważań w tym rozdziale jest zaprezentowanie koncepcji, według której rozwiązań w obszarze zapewniania cyberbezpieczeństwa nie można traktować jako odrębnych działań podejmowanych przez kierownika jednostki lub wyznaczonych przez niego pracowników. Zdaniem autorek trzeba je rozpatrywać w szerszym kontekście systemu kontroli zarządczej, a co się z tym wiąże, powinny one uwzględniać standardy kontroli zarządczej.

5.2. Cyberbezpieczeństwo w samorządzie terytorialnym

W literaturze przedmiotu zwraca się uwagę, że nie ma standardowej, powszechnie stosowanej definicji cyberbezpieczeństwa. W niniejszym rozdziale „cyberbezpieczeństwo" będzie rozumiane jako „działania niezbędne do ochrony sieci i systemów informacyjnych, ich użytkowników oraz innych osób narażonych na cyberincydenty" (van der Meulen i in., 2015). Działania te obejmują zapobieganie cyberincydentom, ich wykrywanie, reagowanie na nie oraz przywracanie działalności po takich incydentach. Warto zauważyć, że incydenty mogą zostać wywołane umyślnie lub nieumyślnie i nie zawsze są równoznaczne z cyberatakami. Obejmują one różnorodne zdarzenia, począwszy od niezamierzonego ujawnienia informacji, po ataki na sieci i systemy informacyjne, kradzież danych osobowych, a nawet przypadki zakłócenia przebiegu procesów demokratycznych, w tym wyborów, oraz ogólne kampanie dezinformacyjne mające wpłynąć na debatę publiczną.

Cyberbezpieczeństwo jest współcześnie uznawane za jedno z największych wyzwań społeczno-technicznych, z którymi muszą się mierzyć instytucje publiczne (de Bruijn i Janssen, 2017). Konieczność zapewnienia cyberbezpieczeństwa w działalności samorządu terytorialnego jest coraz mocniej artykułowana w literaturze, w dokumentach rządowych i raportach przygotowywanych przez niezależne instytucje (Ruohonen, 2020; Salminen i Hossain, 2018).

W zależności od tego, w jaki sposób cyberincydent wpływa na dane przetwarzane w systemach informatycznych, można wyodrębnić różne kategorie zagrożeń dla cyberbezpieczeństwa, na jakie narażone są organizacje, w tym jednostki samorządu terytorialnego. Oddziaływanie cyberincydentu na dane może przybrać formę ujawnienia danych, ich modyfikacji, zniszczenia lub uniemożliwienia do nich dostępu. Przy wystąpieniu cyberincydentu dochodzi do naruszenia jednej lub kilku podstawowych zasad bezpieczeństwa informacji: dostępności, poufności i integralności (rysunek 20).

Kłódka oznacza brak oddziaływania na bezpieczeństwo; wykrzyknik oznacza zagrożenie dla bezpieczeństwa.

Rysunek 20. Rodzaje cyberincydentów i zasady bezpieczeństwa informacji, które mogą zostać naruszone w wyniku ich wystąpienia

Źródło: (Komitet, 2020).

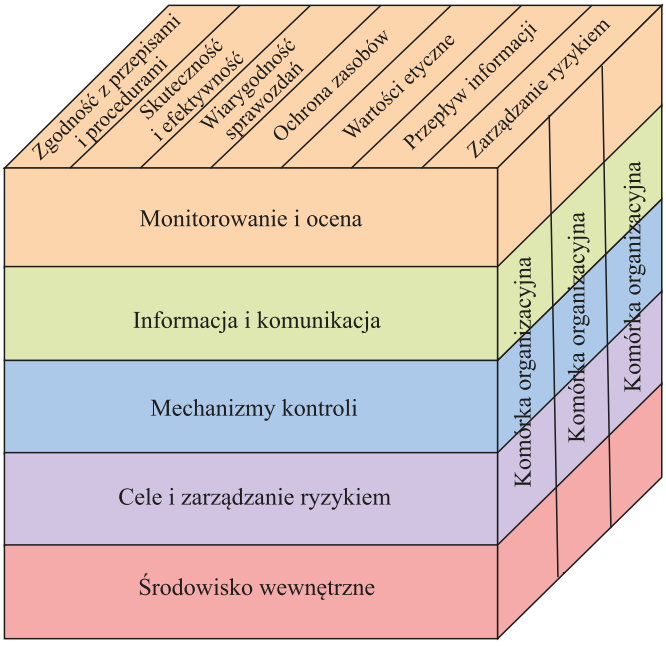
Gdy cyberincydent jest działaniem umyślnym, przybiera formę cyberataku. Skutki cyberataków mogą mieć różną formę i skalę. Do głównych skutków cyberataków zalicza się utratę wrażliwych danych, straty finansowe w wyniku kradzieży, duże koszty związane z odzyskaniem skradzionych danych, utratę reputacji, przechwytywanie newralgicznych informacji, ujawnienie poufnych informacji (w tym danych osobowych), zniszczenie (usunięcie) danych o podstawowym znaczeniu, paraliż funkcjonowania jednostek samorządowych. Konsekwencje cyberataków, mimo że nie zawsze wiążą się ze stratami finansowymi, mogą być bardzo dotkliwe dla jednostki samorządowej (Górka, 2017; Grzelak i Liedel, 2012).

5.3. System kontroli zarządczej w sektorze samorządowym

Kontrola zarządcza we wszystkich jednostkach sektora finansów publicznych, w tym również w jednostkach samorządowych, została wprowadzona do polskiego porządku prawnego ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych. Według ustawodawcy system kontroli zarządczej tworzą wszelkie

działania podejmowane po to, aby zapewnić realizację celów i zadań jednostki w sposób zgodny z prawem, efektywny, oszczędny i terminowy (Ustawa, 2009, art. 68). W definicji tej, oprócz kryterium legalności, przyjęto, że cele jednostki mają być realizowane efektywnie, co oznacza zapewnienie najlepszej możliwej relacji pomiędzy ponoszonymi nakładami i osiąganymi efektami; oszczędnie, a więc przy zapewnieniu najniższego możliwego kosztu realizacji danego celu czy zadania, przy założeniu odpowiedniej jakości wykonania, oraz terminowo, co oznacza wykonanie celów i zadań w założonym czasie, bez wzrostu nakładów lub utraty jakości (MF, 2012).

Koncepcja kontroli zarządczej została oparta na najbardziej spopularyzowanym modelu kontroli wewnętrznej – modelu COSO (COSO I, 2008). Na rysunku 21 przedstawiono tzw. kostkę COSO obrazującą podejście do kontroli w tym modelu.



Rysunek 21. Koncepcja kontroli zarządczej opartej na modelu COSO

Źródło: opracowanie własne na podstawie (COSO I, 2008; Komunikat, 2009).

W modelu COSO kontrola wewnętrzna została opisana jako proces zależny od kierownictwa i pracowników jednostki, zaprojektowany w celu racjonalnego zapewnienia, że zostaną osiągnięte cele dotyczące: (1) efektywności i wydajności operacji – w tym skuteczności, zyskowności oraz ochrony zasobów;

(2) prawdziwości sprawozdań finansowych – w szczególności prawidłowego przygotowania oraz publikacji oświadczeń finansowych, w tym sprawozdań okresowych oraz innych wybranych danych dotyczących finansów jednostki oraz (3) zgodności z obowiązującym prawem i regulacjami, którym podlega jednostka (COSO I, 2008).

Interpretując rysunek 21, należy zaznaczyć, że skuteczne wdrażanie kontroli zarządczej wymaga od kierownictwa jednostki kompleksowego podejścia do rozwiązań wdrażanych w danym podmiocie. Tylko spójny, integrujący obowiązujące procedury, obejmujący wszystkie obszary i procesy działania jednostki system będzie się przyczyniał do usprawniania jej działalności oraz będzie realizował cele postawione przed kontrolą zarządczą. Ustawodawca, bazując na modelu COSO, wymienił siedem celów kontroli zarządczej (Ustawa, 2009):

– zgodność działania jednostki z przepisami prawa oraz procedurami wewnętrznymi,
– skuteczność i efektywność działań jednostki,
– funkcjonowanie w jednostce systemu zarządzania ryzykiem,
– przestrzeganie i promowanie zasad etycznego zachowania,
– wiarygodność sprawozdań sporządzanych przez jednostkę,
– ochrona zasobów jednostki,
– funkcjonowanie efektywnego i skutecznego przepływu informacji.

Cele te są równorzędne i nie należy, co do zasady, dokonywać ich hierarchizacji, jednak z punktu widzenia podjętej w rozdziale tematyki szczególne znaczenie ma ochrona zasobów, a także zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi. Aby kontrola zarządcza dobrze funkcjonowała, należy przyjąć, że działania składające się na zapewnienie cyberbezpieczeństwa w jednostce samorządu terytorialnego są niezbędnym elementem kontroli zarządczej. Cyberbezpieczeństwo nie może być traktowane jako odrębny proces, który będzie funkcjonował niejako „obok" innych rozwiązań przewidzianych w ramach kontroli zarządczej.

System kontroli zarządczej w jednostkach samorządu terytorialnego jest kształtowany zgodnie ze standardami, które stanowią zbiór wskazówek dotyczących pięciu obszarów (Komunikat, 2009):

– środowisko wewnętrzne,
– cele i zarządzanie ryzykiem,
– mechanizmy kontroli,
– informacja i komunikacja,
– monitorowanie i ocena.

Środowisko kontroli jest podstawą funkcjonowania kontroli zarządczej. Składa się na nie zbiór wszystkich sformalizowanych lub nieformalnych rozwiązań,

regulacji wewnętrznych, powiązań i zachowań, które kształtują strukturę, styl działania, charakter i mentalność organizacji. Środowisko wewnętrzne tworzą również wartości etyczne i inne zwyczaje widoczne w działalności organizacji i poszczególnych pracowników. Jest to również sposób zorganizowania działalności jednostki z uwzględnieniem zadań, jakie jednostkach ma wykonywać.

Niezbędnym elementem każdego systemu kontroli zarządczej jest system zarządzania ryzykiem, ściśle powiązany z definiowaniem celów i zadań jednostki. Wyznaczenie misji organizacji, określenie jej celów i zadań, a następnie monitorowanie stopnia ich realizacji stanowi punkt wyjścia do przeprowadzenia procesu zarządzania ryzykiem. Identyfikowanie i analiza ryzyka, a następnie wdrażanie określonych reakcji na ryzyko oraz ciągłe monitorowanie ryzyka dają kadrze kierowniczej informację w zakresie kierunków udoskonalania kontroli zarządczej.

Do mechanizmów kontroli zaliczamy różnego rodzaju działania, przepisy proceduralne zawarte w aktach prawnych, rozwiązania zawarte w wewnętrznych procedurach porządkowych i organizacyjnych, które umożliwiają wykonanie zaplanowanych celów i zadań oraz stanowią odpowiedź na ryzyko. Czynnościom kontrolnym podlegają wszystkie procesy w jednostce, jednak w standardach szczególną uwagę poświęcono ochronie zasobów, zwłaszcza finansowych i informatycznych. Standardy nie tworzą zamkniętego katalogu tych mechanizmów, ponieważ możliwych do zastosowania mechanizmów jest bardzo wiele, a decyzję o tym, które z nich wprowadzić w jednostce, podejmuje jej kierownik.

Kolejny obszar kontroli zarządczej odnosi się do informacji i komunikacji. Funkcjonowanie efektywnego systemu przepływu informacji uznano za jeden z warunków prawidłowego i efektywnego prowadzenia działalności przez jednostkę. Kierownictwo oraz pracownicy powinni w odpowiedniej formie i czasie otrzymywać właściwe i rzetelne informacje potrzebne im do wypełniania obowiązków. Bardzo ważne jest więc przygotowanie odpowiednich kanałów komunikacji, i to nie tylko w ramach organizacji, ale również z podmiotami zewnętrznymi.

Ostatnia grupa standardów kontroli zarządczej odnosi się do oceny skuteczności jej działania. Ocena ta może być prowadzona różnymi sposobami i w różnych formach, np. poprzez bieżące monitorowanie oraz odrębne oceny, dokonywane w szczególności przez kierownika jednostki oraz innych pracowników na stanowiskach kierowniczych, albo poprzez działalność wyspecjalizowanych osób lub komórek zajmujących się weryfikacją działalności i oceną, przykładowo audytorów wewnętrznych. Dokonując oceny kontroli zarządczej, można wykorzystać proste arkusze samooceny lub wyspecjalizowane narzędzia oceny (Przybylska i Zasadzka, 2019). Należy jednak zwrócić uwagę na fakt, że forma czy sposób dokonywania oceny ma znaczenie drugorzędne, ważne jest dokonywanie oceny przynajmniej raz w roku oraz odpowiednie rozumienie podejścia do procesu

oceny – działanie to nie jest ukierunkowane na ocenę działań poszczególnych osób, lecz na ocenę rozwiązań systemowych. Ocenę kontroli zarządczej należy traktować jako narzędzie, które – mimo że może wykazać pewne niesprawności czy mankamenty przyjętych rozwiązań – w dłuższej perspektywie przyczynia się do ulepszania systemu kontroli zarządczej i powoduje, że staje się on jak najlepiej dopasowany do danego podmiotu.

5.4. Wymogi prawne w zakresie cyberbezpieczeństwa w jednostkach samorządu terytorialnego

W warunkach gospodarki 4.0 szczególnego znaczenia nabiera zapewnienie bezpieczeństwa informacji przekazywanych pomiędzy poszczególnymi uczestnikami życia społeczno-gospodarczego. Istotność tego zagadnienia wzrasta, gdy przekazywane informacje dotyczą tzw. danych wrażliwych lub mają poufny charakter. Współczesne państwa stoją zatem przed zadaniem stworzenia ram funkcjonowania podmiotów, w tym jednostek samorządu terytorialnego, w sposób zapewniający bezpieczeństwo informacji (Kańduła i Przybylska, 2020). W Polsce do najważniejszych regulacji prawnych, w których są uwzględnione zapisy dotyczące bezpieczeństwa informacji w warunkach gospodarki cyfrowej, należą: (Ustawa, 2018; Rozporządzenie RM, 2012; Rozporządzenie PEiR, 2016).

W ustawie o krajowym systemie cyberbezpieczeństwa na jednostki samorządu terytorialnego nałożono określone obowiązki związane z ich rolą w tym systemie. Do zadań jednostek samorządowych należy wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Powinna to być osoba odpowiedzialna w urzędzie za bezpieczeństwo systemów teleinformatycznych oraz bezpieczeństwo informacji. Taka osoba może utrzymywać kontakt z innymi podmiotami krajowego systemu cyberbezpieczeństwa jedynie w zakresie systemów informatycznych, którymi te jednostki posługują się przy realizacji zadań publicznych (Ustawa, 2018).

Jednostki samorządu terytorialnego są również zobligowane do przygotowania struktur i procedur, które umożliwią odpowiednią reakcję na pojawienie się tzw. incydentu, czyli zdarzenia, które ma lub może mieć negatywny wpływ na cyberbezpieczeństwo. W ramach przyjętych rozwiązań konieczne jest między innymi zapewnienie zarządzania incydentami, a więc zapewnienie obsługi incydentów (w tym incydentów krytycznych), poszukiwanie powiązań między nimi, usuwanie przyczyn ich wystąpienia oraz wypracowanie wniosków z obsługi incydentów. W przypadku wystąpienia incydentu jednostka samorządowa powinna

zgłosić ten fakt właściwemu podmiotowi w ciągu 24 godzin od jego wykrycia (Ustawa, 2018).

Jednostki samorządu terytorialnego mają również obowiązek zapewnić podmiotom, na których rzecz wykonują zadania publiczne, dostęp do wiedzy umożliwiającej zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów ochrony przed tymi zagrożeniami. Warto zaznaczyć, że ustawa o krajowym systemie cyberbezpieczeństwa obejmuje również podmioty nadzorowane przez jednostki samorządowe oraz podmioty, w których mają one udziały. Dotyczy to w szczególności przedsiębiorców, których można zaliczyć do kategorii operatorów usług kluczowych. Będą to przedsiębiorcy z sektorów: energetyki, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną oraz infrastruktury cyfrowej. Wśród jednostek samorządu terytorialnego mogą to być szpitale, przedsiębiorstwa wodociągowo-kanalizacyjne, operatorzy lotnisk. Na tych przedsiębiorcach spoczywa najwięcej obowiązków związanych z budowaniem cyberbezpieczeństwa (Ustawa, 2018).

Jednostki samorządu terytorialnego, jako podmioty realizujące zadania publiczne, są również zobowiązane do opracowania i ustanowienia, a następnie wdrożenia, eksploatacji i monitorowania systemu zarządzania bezpieczeństwem informacji, który ma zapewniać poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Działania, które muszą być podjęte w ramach zapewnienia systemu bezpieczeństwa informacji, zostały zdefiniowane w regulacjach prawnych i nazwane Krajowymi Ramami Interoperacyjności (KRI).

KRI stanowią określenie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych, w których informacje są gromadzone. Za cel KRI przyjęto między innymi zdefiniowanie sposobów wymiany danych pomiędzy systemami informatycznymi stosowanymi do realizacji zadań publicznych, dostosowanie tych systemów do potrzeb osób niepełnosprawnych oraz zapewnienie bezpieczeństwa tych systemów. W rozdziale pominięto dwa pierwsze z wymienionych aspektów, a opisano wymogi w zakresie bezpieczeństwa informacji z racji tego, że zapewnienie ochrony zasobów organizacji (w tym informacji) stanowi jeden z celów kontroli zarządczej.

Zgodnie z wytycznymi KRI każdy podmiot realizujący zadania publiczne, a więc również każda jednostka samorządu terytorialnego, jest zobligowany do wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI). W przepisach prawnych szczegółowo sprecyzowano wymogi, które powinien spełniać SZBI. Podmiot realizujący zadania publiczne musi opracować i wdrożyć system zarządzania bezpieczeństwem informacji, który będzie zapewniać poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak au-

tentyczność, rozliczalność, niezaprzeczalność i niezawodność. System ten musi być również monitorowany i doskonalony.

Kierownik jednostki musi zapewnić warunki umożliwiające realizację i egzekwowanie w ramach KRI wielu działań, które mają zapewnić bezpieczeństwo informacji. Pierwszym z nich, o bardzo ogólnym, ale zarazem nadrzędnym charakterze, jest dbanie o aktualność regulacji wewnętrznych obowiązujących w jednostce. Kolejną kwestią jest utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji. W jednostce powinna być również przeprowadzana okresowa analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowane działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy. Powinny być również podejmowane działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do wykonywanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Osoby zaangażowane w proces przetwarzania informacji powinny mieć zapewnione szkolenia obejmujące takie zagadnienia, jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, oraz stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

W podmiocie realizującym zadania publiczne powinna być również zapewniona ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Uznaje się, że ochrona ta polega na: monitorowaniu dostępu do informacji, czynnościach zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, a także zapewnieniu środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji. W jednostce powinny być także ustanowione podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, a także zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. W umowach serwisowych podpisanych ze stronami trzecimi powinny być zawarte zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji.

Odpowiedni poziom bezpieczeństwa powinien być też zapewniony w systemach teleinformatycznych. W szczególności należy zadbać o aktualizację oprogramowania, minimalizować ryzyko utraty informacji w wyniku awarii, chronić przed błędami, utratą, nieuprawnioną modyfikacją, stosować mechanizmy kryptograficzne w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, zapewnić bezpieczeństwo plików systemowych. Po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeń-

stwa należy niezwłocznie podejmować działania zmierzające do likwidacji tych podatności. W przypadku stwierdzenia incydentów naruszenia bezpieczeństwa informacji jednostka jest zobowiązana do bezzwłocznego zgłaszania tych incydentów, co ma umożliwić szybkie podjęcie działań korygujących.

Zgodnie z wytycznymi KRI podmiot realizujący zadania publiczne ma także obowiązek zapewnienia przynajmniej raz na rok audytu wewnętrznego w zakresie bezpieczeństwa informacji. Warto tutaj doprecyzować, że minister właściwy ds. administracji i cyfryzacji uściślił, iż przez audyt wewnętrzny rozumie się audyt realizowany przez jednostkę na wewnętrzne potrzeby, niekoniecznie przez osoby z wewnątrz organizacji (komórkę audytu wewnętrznego). Podkreśla się jednocześnie potrzebę niezależności komórki audytującej. Można więc taki audyt zlecić firmom lub osobom z zewnątrz. Preferowani do wykonywania zadań audytowych są specjaliści legitymujący się certyfikatami audytora wiodącego ISO 27001, co jest związane z faktem, że uznaje się, iż system bezpieczeństwa informacji spełnia minimalne wymagania, jeśli został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001. Ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie innych norm, w szczególności: PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, oraz PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania (Rozporządzenie z dnia 12 kwietnia 2012; Kańduła i Przybylska, 2020).

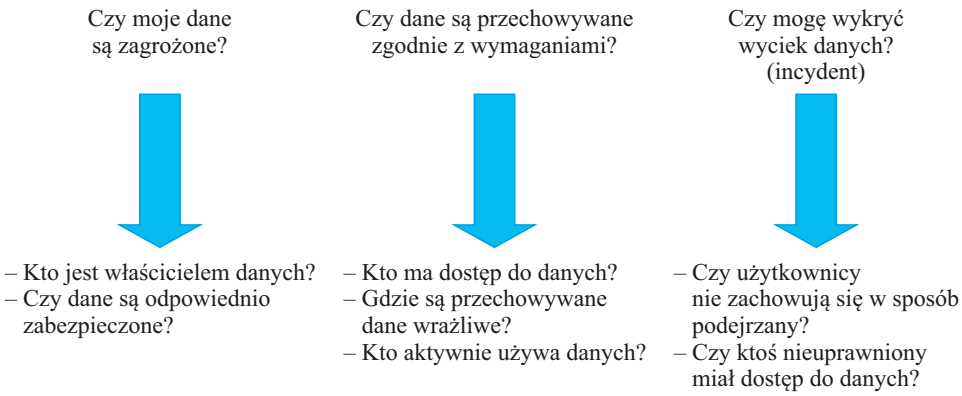
Szczególnej ochronie podlegają dane osobowe. W przepisach prawnych nie określono szczegółowo kształtu systemu, który powinien być wdrożony w każdej jednostce. Obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych adekwatną do aktualnych zagrożeń oraz kategorii danych objętych ochroną ustawodawca nałożył na administratora danych osobowych, którym – w przypadku braku wyznaczenia innej osoby – jest kierownik jednostki. Środki te powinny być dobrane w taki sposób, aby zapewniały stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych. Do środków tych zaliczyć można: kontrolę dostępu do sprzętu, kontrolę nośników danych, kontrolę przechowywania, kontrolę użytkowników, kontrolę dostępu do danych, kontrolę wprowadzania danych, kontrolę przesyłu danych, odzyskiwanie danych. Funkcje tych kontroli zostały omówione w kolejnym punkcie niniejszego rozdziału.

System zapewniający ochronę danych osobowych powinien między innymi uwzględniać:

– pseudonimizację i szyfrowanie danych osobowych;
– zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

– zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
– regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Jednostki samorządu terytorialnego stoją również przed wyzwaniem koordynacji obowiązków wynikających z przepisów ustawy o cyberbezpieczeństwie z obowiązkami wynikającymi z rozporządzenia w sprawie Krajowych Ram Interoperacyjności oraz przepisów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO). Wszystkie te przepisy przeplatają się i przenikają. Ważne jest, aby nie traktować ich oddzielnie. Bezpieczeństwo systemów teleinformatycznych, zarządzanie informacjami i ich ochrona oraz ochrona danych osobowych muszą tworzyć spójny system. Aby sprawdzić, czy jednostka samorządu terytorialnego spełnia jednocześnie wymagania ujęte w przywołanych aktach prawnych, proponuje się zweryfikowanie kwestii ujętych na rysunku 22.



Rysunek 22. Jak spełnić jednocześnie wymagania KSC, KRI oraz RODO

Źródło: opracowanie własne na podstawie (Ustawa, 2018; Rozporządzenie RM, 2012; Rozporządzenie PEiR, 2016).

Udzielenie odpowiedzi na pytania zamieszczone na rysunku 22 stanowi wstęp do dokonania oceny, czy jst spełnia wymagania w zakresie zapewnienia bezpieczeństwa danych. W przypadku gdy zaistnieją trudności w udzieleniu odpowiedzi na te pytania lub udzielona odpowiedź będzie budziła wątpliwości, czy dane są prawidłowo chronione, kierownik jednostki powinien podjąć działania zmierzające do dokładnego zdiagnozowania problemu i wprowadzić nowe lub zmodyfikować istniejące rozwiązania zwiększające bezpieczeństwo przetwarzanych informacji.

Dokonując oceny, czy jst w odpowiedni sposób zarządza kontrolą dostępu zarówno do infrastruktury fizycznej służącej do przetwarzania informacji chro-

nionych (np. pomieszczenia biurowe, serwerownie, archiwum), jak i do danych w systemie informatycznym, należałoby zweryfikować, czy w jednostce istnieje procedura kontroli dostępu logicznego i fizycznego oraz zarządzania prawami dostępu do systemów informatycznych oraz w jaki sposób są przyznawane te prawa. Należy również ustalić, jakie są zasady udzielania dostępu dla administratorów systemu informatycznego oraz jakie metody uwierzytelniania dla tych administratorów są stosowane w jednostce. Ważna jest również weryfikacja, w jaki sposób są przydzielane użytkownikom hasła systemu informatycznego oraz czy w jednostce samorządowej przeprowadzane są przeglądy praw dostępu użytkowników. Należy także sprawdzić stosowane zasady kontroli dostępu fizycznego do obszarów bezpiecznych oraz wdrożenie zasad ochrony fizycznej obszarów, w których przetwarzane są dane osobowe (Cieślik, 2020).

5.5. Zapewnienie cyberbezpieczeństwa w sektorze samorządowym w świetle standardów kontroli zarządczej

5.5.1. Środowisko wewnętrzne

W przepisach prawnych określono siedem celów, które ma realizować dobrze działająca kontrola zarządcza. Jak wspomniano wcześniej, cele te są równorzędne, jednak z punktu widzenia podjętej w tym rozdziale tematyki szczególne znaczenie mają trzy z nich: skuteczność i efektywność działań jednostki, ochrona zasobów jednostki, a także zgodność działalności z przepisami prawa oraz procedurami wewnętrznymi. Aby kontrola zarządcza dobrze funkcjonowała, podstawowym założeniem jest potraktowanie wszystkich przyjętych rozwiązań jako jednego, spójnego systemu, a mechanizmów wdrażanych w celu zapewnienia cyberbezpieczeństwa jako niezbędnego elementu kontroli zarządczej.

Pierwsza grupa standardów kontroli zarządczej – środowisko wewnętrzne – obejmuje cztery standardy: przestrzeganie wartości etycznych, kompetencje zawodowe, strukturę organizacyjną oraz delegowanie uprawnień. Omawiając tę grupę standardów, warto na wstępie przytoczyć wyniki badania ankietowego w zakresie cyberbezpieczeństwa przeprowadzonego przez autorki wśród jednostek samorządowych szczebla gminnego w 2020 r. W opinii 42,0% badanych urzędów gmin cyberprzestępczość stanowi duże lub bardzo duże zagrożenie. 34,9% ankietowanych było zdania, że zagrożenie to jest średnie, natomiast 18,0% stwierdziło, że zagrożenie to jest minimalne lub nie występuje. Uwagę zwraca wysoki odsetek ankietowanych w ostatniej wymienionej grupie. Niemal co piąty respondent nie dostrzegał zagrożenia ze strony cyberprzestępców dla funkcjono-

wania jednostki. Świadczy to o niskiej świadomości cyberzagrożeń, a to z kolei wpływa niekorzystnie na środowisko wewnętrzne organizacji. Takie podejście i postrzeganie cyberprzestępczości może się przekładać na nieodpowiednie podejście zarówno kierownictwa, jak i pracowników. Jeśli cyberprzestępczość nie jest traktowana jako poważne zagrożenie, w jednostce nie zostaną wdrożone odpowiednie mechanizmy kontrolne lub będą miały one charakter fasadowy.

W tabeli 23 zamieszczono standardy kontroli zarządczej z grupy środowisko wewnętrzne z przykładami rozwiązań w zakresie cyberbezpieczeństwa.

Tabela 23. Środowisko wewnętrzne – przykłady rozwiązań z obszaru cyberbezpieczeństwa

Nazwa standardu kontroli zarządczej	Przykłady rozwiązań w ramach kontroli zarządczej
Przestrzeganie wartości etycznych	– kształtowanie przez kierownictwo jednostki tzw. kultury cyberbezpieczeństwa w jst, np. poprzez zachęcanie do podnoszenia kompetencji cyfrowych, podnoszenie świadomości o cyberzagrożeniach – opracowanie polityki cyberbezpieczeństwa
Kompetencje zawodowe	– zatrudnianie na stanowiskach IT osób z odpowiednimi kompetencjami cyfrowymi – cykliczne szkolenia z zakresu cyberbezpieczeństwa wśród wszystkich pracowników
Struktura organizacyjna	– wyodrębnienie w strukturze organizacyjnej komórki lub osoby odpowiedzialnej za cyberbezpieczeństwo – wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa
Delegowanie uprawnień	odpowiednie delegowanie uprawnień z zakresu obsługi IT w celu zapewnienia ciągłości działania jst

Źródło: opracowanie własne.

Decydującą rolę w budowaniu środowiska wewnętrznego, kultury organizacji odgrywa kierownictwo jednostki. Zadaniem kierownika jednostki jest między innymi propagowanie postaw etycznych, ale także podnoszenie świadomości pracowników i zachęcanie do podnoszenia kompetencji, w tym kompetencji cyfrowych. Biorąc pod uwagę zmiany w obszarze społeczno-gospodarczym w ostatnich latach, polegające na intensywnym zwiększaniu się wykorzystania technologii ITC w wykonywaniu zadań przez jednostki samorządu terytorialnego, niezbędne wydaje się podnoszenie wiedzy w zakresie cyberbezpieczeństwa – zarówno zasad bezpiecznego korzystania z systemów informacyjnych, jak i skutecznej ochrony przez atakami cyberprzestępców. Problematyka ta została szerzej omówiona w kolejnym rozdziale monografii.

Kształtowanie świadomości pracowników oraz podnoszenie ich kompetencji w zakresie identyfikowania cyberataków i odpowiedniego reagowania na nie są bardzo istotnym elementem budowania odpowiedniego środowiska organizacji. Szczególnie ważne w tym kontekście są programy z zakresu cyberbezpieczeństwa (polityki cyberbezpieczeństwa). Opracowanie dokumentu (programu) polityki cyberbezpieczeństwa jest jednym z zadań jednostek samorządu terytorialnego w Polsce, ponieważ należą one do grupy podmiotów publicznych, na które nałożono określone obowiązki związane z ich rolą w krajowym systemie cyberbezpieczeństwa.

W ramach kształtowania odpowiedniego środowiska wewnętrznego do wdrażania rozwiązań w zakresie cyberbezpieczeństwa konieczne jest wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Jednostki samorządu terytorialnego muszą również przygotować struktury i procedury, które umożliwią odpowiednią reakcję na pojawienie się tzw. incydentu, czyli zdarzenia, które ma lub może mieć negatywny wpływ na cyberbezpieczeństwo. W ramach przyjętych rozwiązań konieczne jest: (1) zapewnienie zarządzania incydentami, tj. zapewnienie obsługi incydentów, poszukiwanie powiązań między nimi, usuwanie przyczyn ich wystąpienia oraz wypracowanie wniosków z obsługi incydentów; (2) zgłoszenie incydentu właściwemu podmiotowi w ciągu 24 godzin od jego wykrycia; (3) zapewnienie obsługi incydentu i incydentu krytycznego we współpracy z odpowiednim podmiotem poprzez podanie niezbędnych danych, w tym danych osobowych (Ustawa, 2018).

5.5.2. Cele i zarządzanie ryzykiem

Niezbędnym elementem każdego systemu kontroli zarządczej jest system zarządzania ryzykiem. Identyfikowanie i analiza ryzyka, a następnie wdrażanie określonych reakcji na ryzyko oraz ciągłe monitorowanie ryzyka dają informację kadrze kierowniczej dotyczącą kierunków udoskonalania kontroli zarządczej. Wytyczne odnoszące się do tego zagadnienia zostały ujęte w drugiej grupie standardów kontroli zarządczej – cele i zarządzanie ryzykiem, a przykłady rozwiązań zamieszczono w tabeli 24.

Przyjmując założenie, że rozwiązania w zakresie cyberbezpieczeństwa staną się integralną częścią kontroli zarządczej, podczas analizy ryzyka szczególną uwagę należy zwrócić na podatności organizacji sprzyjające występowaniu cyberataków. Wbrew pozorom, wśród czynników zwiększających ryzyko wystąpienia cyberataku należy wymienić przykładowo brak przypadków cyberataków w przeszłości, lekceważenie sygnałów ostrzegawczych, przyjęcie założenia, że jeśli dojdzie do naruszenia bezpieczeństwa systemów informacyjnych zostanie ono wykryte, czy założenie, że najważniejsze dla jednostki obszary są

Tabela 24. Cele i zarządzanie ryzykiem – przykłady rozwiązań z obszaru cyberbezpieczeństwa

Nazwa standardu kontroli zarządczej	Przykłady rozwiązań w ramach kontroli zarządczej
Misja	podczas procesu definiowania lub modyfikowania misji jst zwrócenie uwagi na cyberzagrożenia, które mogą utrudnić jej realizację
Określanie celów i zadań, monitorowanie i ocena ich realizacji	– ustalanie celów i zadań w obszarze budowania cyberbezpieczeństwa jst (np. w zakresie zakupu infrastruktury IT) wraz z miernikami umożliwiającymi ich monitorowanie i ocenę realizacji – strategia rozwoju cyberbezpieczeństwa
Identyfikacja ryzyka	– okresowa (przynajmniej raz na rok) identyfikacja i analiza ryzyka w zakresie utraty integralności, poufności i dostępności informacji – w stosunku do kluczowych rodzajów ryzyka opracowanie planów postępowania z ryzykiem
Analiza ryzyka	
Reakcja na ryzyko	

Źródło: opracowanie własne.

doskonale kontrolowane. Warto w tym miejscu dodać, że według przeprowadzonych w 2020 r. badań sektora samorządowego szczebla gminnego w latach 2017–2019 w 86,7% gmin nie wystąpiły incydenty związane z naruszeniem bezpieczeństwa informacji, a w pozostałych urzędach zaobserwowano do pięciu takich incydentów (10,6%).

Obowiązek przeprowadzania okresowej analizy ryzyka w obszarze cyberbezpieczeństwa, w szczególności w zakresie utraty integralności, poufności i dostępności informacji, wynika nie tylko ze standardów kontroli zarządczej, ale również z uregulowań prawnych. Konieczność dokonywania analizy ryzyka przynajmniej raz w roku jest wskazana zarówno w ustawie o krajowym systemie cyberbezpieczeństwa, rozporządzeniu dotyczącym KRI, jak i rozporządzeniu RODO (Ustawa, 2018; Rozporządzenie RM, 2012; Rozporządzenie PEiR 2016). Jednostki samorządu terytorialnego zostały zatem zobowiązane do dokonywania analizy ryzyka w odniesieniu do cyberbezpieczeństwa. Systematyczne jej przeprowadzanie ma charakter prewencyjny i z założenia ma zmniejszać prawdopodobieństwo wystąpienia cyberzagrożeń. Z przeprowadzonych w 2020 r. badań ankietowych wynika, że mimo obowiązku prawnego w 2019 r. jedynie 78,5% urzędów gmin przeprowadziło okresową analizę ryzyka utraty integralności, poufności i dostępności informacji. Te jst, które jej nie dokonywały, tłumaczyły się głównie brakiem środków finansowych (35,6%) lub brakiem takiej potrzeby (24,7%), co biorąc pod uwagę zapisy regulacji prawnych, jest zastanawiające i stanowi jednocześnie naruszenie legalności działania tych jednostek samorządowych.

Warto dodać, że wyniki rzetelnie przeprowadzonej analizy ryzyka są podstawą udoskonalania i uszczelniania systemu kontroli zarządczej, w tym rozwiązań, które mają zapewnić odpowiedni poziom cyberbezpieczeństwa w jednostce. Identyfikacja ryzyka oraz ocena jego istotności z zestawieniem obowiązujących mechanizmów kontrolnych wskazują na potencjalne podatności organizacji na zagrożenia oraz pozwalają na ocenę, czy wszystkie rodzaje ryzyka są odpowiednio zabezpieczone mechanizmami kontrolnymi.

5.5.3. Mechanizmy kontroli

Reakcją na zidentyfikowane rodzaje ryzyka powinny być odpowiednio dostosowane mechanizmy kontroli. Każdy mechanizm kontrolny ma zbliżać jednostkę do osiągnięcia zaplanowanych celów. Warto w tym miejscu przypomnieć, że zgodnie ze standardami kontroli zarządczej mechanizmy kontrolne mają zapewnić ochronę zasobów organizacji obejmującą: ochronę fizyczną jednostki i jej pracowników, ochronę zasobów materialnych, ochronę środków finansowych oraz ochronę informacji. Rozwiązania w zakresie cyberbezpieczeństwa będą się odnosić przede wszystkim do ochrony informacji oraz zasobów finansowych organizacji, ale również ochrony jej zasobów materialnych. Przykłady zamieszczono w tabeli 25.

W standardach kontroli zarządczej zwrócono szczególną uwagę na aspekt zabezpieczenia informacji i dokumentów ujętych w systemach informatycznych. W przeciwieństwie do tradycyjnej formy utrwalania informacji informacja elektroniczna ma znacznie większe możliwości powielania i rozpowszechniania się, dlatego coraz bardziej istotna staje się potrzeba doskonalenia mechanizmów służących zapewnieniu bezpieczeństwa danych i systemów informatycznych. Należy opracować i wdrożyć odpowiednie procedury zabezpieczające (MF, 2012).

Podstawowy dokument w tym zakresie jest elementem polityki bezpieczeństwa informacji, której przygotowanie wynika z przepisów prawa. Jest to podstawowy dokument, który powinien być opracowany i przyjęty w każdej jednostce samorządu terytorialnego, dotyczący obszaru cyberbezpieczeństwa. Stanowi on trzon systemu zarządzania bezpieczeństwem informacji (SZBI). W przepisach prawnych sprecyzowano szczegółowo wymogi, które powinien spełniać SZBI. Podmiot realizujący zadania publiczne musi opracować i wdrożyć system zarządzania bezpieczeństwem informacji, który będzie zapewniać poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Jednak z przeprowadzonych w 2020 r. badań ankietowych wynika, że dokument ten posiadało jedynie 76,9% badanych gmin. Brak polityki bezpieczeństwa informacji jest również często wskazywany jako nieprawidłowość podczas

Tabela 25. Mechanizmy kontroli – przykłady rozwiązań z obszaru cyberbezpieczeństwa

Nazwa standardu kontroli zarządczej	Przykłady rozwiązań w ramach kontroli zarządczej
Dokumentowanie systemu kontroli zarządczej	– polityka bezpieczeństwa informacji – polityka ochrony danych osobowych
Nadzór	praca pracowników komórki IT wykonywana pod stałym nadzorem
Ciągłość działalności	– zapewnienie ciągłości obsługi IT – plany ciągłości działania dotyczące systemów informatycznych – polityka kopii zapasowych – testowanie odtwarzania kopii zapasowych
Ochrona zasobów	– kontrola dostępu do pomieszczeń, w których znajdują się urządzenia IT – odpowiednie wyposażenie serwerowni – monitoring – kontrola dostępu do danych (finansowych i pozafinansowych) przetwarzanych w systemach IT – kontrola nośników informacji – obowiązek regularnej aktualizacji oprogramowania – wykonywanie regularnych przeglądów infrastruktury IT
Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych	
Mechanizmy kontroli dotyczące systemów informatycznych	

Źródło: opracowanie własne.

kontroli działalności jednostek samorządu terytorialnego dokonywanych przez Najwyższą Izbę Kontroli (NIK, 2014, 2016, 2018).

Znacznie bardziej rozpowszechnionym dokumentem, w którym znajdują się zapisy dotyczące cyberbezpieczeństwa, jest dokument dotyczący polityki ochrony danych osobowych. Jest to również dokument wymagany prawem, jednak należy zwrócić uwagę, że mimo iż dotyczy on po części obszaru cyberbezpieczeństwa, ma ograniczony zakres przedmiotowy – nie dotyczy wszystkich danych, lecz szczególnego ich rodzaju – danych osobowych.

Katalog mechanizmów kontrolnych, które mogą być wdrożone w danej organizacji w odpowiedzi na zidentyfikowane ryzyko związane z funkcjonowaniem systemów informacyjnych, jest bardzo szeroki. Decyzje odnośnie do konkretnych rozwiązań, które będą przyjęte w ramach kontroli zarządczej, podejmuje kierownik jednostki. Budując system kontroli zarządczej w obszarze cyberbezpieczeństwa, należy wziąć pod uwagę różne aspekty działania systemów informacyjnych i zagrożeń z tym związanych. Pierwszym rodzajem kontroli jest kontrola dostępu do sprzętu, która ma za zadanie uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania danych. Kontrola nośników danych jest wdrażana w celu zapobiegania nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych. Podobną

funkcję spełnia kontrola przechowywania wprowadzana po to, aby uniknąć nieuprawnionego wprowadzania danych osobowych oraz nieuprawnionego oglądania, zmieniania lub usuwania przechowywanych danych osobowych. Kontrola użytkowników to mechanizmy zapobiegające korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione. Z kolei kontrola dostępu do danych ma zapewnić osobom, uprawnionym do korzystania z systemu zautomatyzowanego przetwarzania, dostępu wyłącznie do danych osobowych objętych posiadanym przez nie uprawnieniem. Kontrola wprowadzania danych ma umożliwić weryfikację i ustalenie, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo, a kontrola przesyłu danych – weryfikację i ustalenie podmiotów, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przesyłu. Odzyskiwanie z kolei ma zapewnić przywrócenie zainstalowanych systemów w razie awarii.

5.5.4. Informacja i komunikacja

System kontroli zarządczej powinien również uwzględniać funkcjonowanie efektywnego systemu informacyjnego. Jest to jeden z warunków prawidłowego i efektywnego prowadzenia działalności przez jednostkę. Kierownictwo oraz pracownicy powinni otrzymywać w odpowiedniej formie i czasie właściwe i rzetelne informacje potrzebne do wypełniania obowiązków. System informacyjny jednostki, jak każdy element kontroli zarządczej, musi być monitorowany i modyfikowany, aby przekazywane i otrzymywane informacje były istotne, rzetelne, aktualne i kompletne oraz aby środki komunikacji były efektywne. Przykłady rozwiązań z tej grupy standardów zawarto w tabeli 26.

Aspekt cyberbezpieczeństwa nabiera w tym przypadku szczególnego znaczenia, gdy informacje przekazywane są w formie elektronicznej. W ostatnich latach wykorzystanie środków komunikacji elektronicznej staje się coraz bardziej powszechne. Powstaje więc problem weryfikacji, czy informacje przekazywane

Tabela 26. Informacja i komunikacja – przykłady rozwiązań z obszaru cyberbezpieczeństwa

Nazwa standardu kontroli zarządczej	Przykłady rozwiązań w ramach kontroli zarządczej
Bieżąca informacja	wykorzystanie wewnętrznych kanałów komunikacji (intranetu) do przekazywania informacji o bieżących cyberzagrożeniach
Komunikacja wewnętrzna	
Komunikacja zewnętrzna	procedura komunikowania z podmiotami zewnętrznymi w sytuacjach kryzysowych (cyberataku)

Źródło: opracowanie własne.

za pośrednictwem systemów informatycznych pochodzą z wiarygodnego źródła, nie zostały poddane ingerencji, czy są prawidłowo zabezpieczone i przechowywane. Wszystkie te aspekty powinny znaleźć odzwierciedlenie w odpowiednio dobranych mechanizmach kontrolnych w ramach cyberbezpieczeństwa, które omówiono wcześniej.

Z kolei w przypadku wystąpienia nieprawidłowości pracownicy muszą mieć świadomość, że należy raportować każdy przypadek nieoczekiwanego lub nietypowego zdarzenia, który wpływa na ich pracę oraz realizację celów jednostki. Kierownictwo jednostki powinno nie tylko zapewnić kanały komunikacji do przekazywania informacji o potencjalnych nieprawidłowościach, ale również zachęcać do korzystania z tych możliwości i promować w jednostce kulturę otwartości komunikowania.

5.5.5. Monitorowanie i ocena

Ostatnia grupa standardów kontroli zarządczej – monitorowanie i ocena – zawiera trzy standardy. Nazwy tych standardów wraz z przykładami działań, które jst mogą podejmować w tym zakresie, aby podnosić poziom cyberbezpieczeństwa, zestawiono w tabeli 27.

Tabela 27. Monitorowanie i ocena – przykłady rozwiązań z obszaru cyberbezpieczeństwa

Nazwa standardu kontroli zarządczej	Przykłady rozwiązań w ramach kontroli zarządczej
Monitorowanie systemu kontroli zarządczej	– coroczny przegląd polityki bezpieczeństwa informacji – cykliczne przeglądy techniczne kontroli dostępu – testowanie podatności systemów informatycznych
Samoocena	przeprowadzanie raz na rok anonimowej samooceny mechanizmów kontroli zarządczej wdrożonych w celu zapewnienia cyberbezpieczeństwa
Audyt wewnętrzny	przeprowadzanie audytu wewnętrznego według zasad określonych w KRI

Źródło: opracowanie własne.

Zgodnie ze standardami kontroli zarządczej skuteczność tego systemu powinna być monitorowana i poddawana regularnej ocenie. Przegląd procedur powinien dotyczyć również rozwiązań przewidzianych w ramach zapewnienia cyberbezpieczeństwa. Zalecenia w tym zakresie są również zawarte w obowiązujących aktach prawnych. Tylko takie podejście pozwala na bieżące zidentyfikowanie istniejących problemów i wdrażanie usprawnień.

Monitorowanie systemu kontroli zarządczej powinno być przede wszystkim domeną ścisłego kierownictwa, które może jednak przekazać te obowiązki innym pracownikom organizacji. Obiektywną i niezależną ocenę kontroli zarządczej prowadzą również audytorzy wewnętrzni. Warto dodać, że zgodnie z wytycznymi zawartymi w Krajowych Ramach Interoperacyjności podmiot realizujący zadania publiczne ma obowiązek zapewnienia przynajmniej raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. Minister właściwy ds. administracji i cyfryzacji uściślił, że przez audyt wewnętrzny rozumie się audyt realizowany przez jednostkę na wewnętrzne potrzeby, niekoniecznie przez osoby z wewnątrz organizacji (komórkę audytu wewnętrznego). Podkreśla się jednocześnie potrzebę niezależności komórki audytującej. Można więc taki audyt zlecić firmom lub osobom z zewnątrz. Preferowani do wykonywania zadań audytowych są specjaliści legitymujący się certyfikatami audytora wiodącego ISO 27001, co jest związane z faktem, że uznaje się, iż system bezpieczeństwa informacji spełnia minimalne wymagania, jeśli został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (Rozporządzenie RM, 2012).

Mimo prawnego wymogu corocznego audytu bezpieczeństwa informacji, według wyników badań z 2020 r., przeprowadzonych w sektorze samorządowym, 21,5% gmin nie przeprowadziło takiego audytu, a co czwarta z tych gmin zadeklarowała, że nie widzi takiej potrzeby. Wyniki badań nie napawają optymizmem. Świadczą nie tylko o braku znajomości przepisów prawnych, ale również o bagatelizowaniu przez część jednostek zagrożeń związanych z cyberprzestępczością.

CYBERATAKI W DZIAŁALNOŚCI JEDNOSTEK SAMORZĄDU GMINNEGO

6.1. Istota analizy cyberataków w samorządzie terytorialnym

Transformacja cyfrowa i coraz bardziej powszechne wykorzystywanie technologii informacyjnych we wszystkich aspektach życia społeczno-gospodarczego wiąże się niewątpliwie z nowymi możliwościami ich zastosowania. Jednocześnie jednak wzrasta ryzyko, że osoby fizyczne, przedsiębiorstwa i instytucje publiczne padną ofiarą cyberprzestępczości lub cyberataku. Społeczne i gospodarcze oddziaływanie tego ryzyka jest coraz większe, a wśród podmiotów narażonych na cyberataki należy wymienić jednostki samorządu terytorialnego, które w swojej działalności coraz częściej stosują rozwiązania wykorzystujące technologię informacyjno-komunikacyjną (ICT).

Stosowanie ICT w działalności jst wiąże się z koniecznością zapewnienia przez te podmioty bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do realizacji różnego rodzaju zadań. Przemawia za tym również fakt, że z roku na rok wzrasta liczba zgłoszonych incydentów cyberbezpieczeństwa na urzędy administracji publicznej (CSIRT GOV, 2021).

W literaturze przedmiotu zwraca się jednocześnie uwagę na istotną różnicą między poziomem wiedzy niezbędnym do zapobiegania cyberatakom oraz potrzebnym do przeprowadzenia samego cyberataku. Niewystarczające umiejętności w zakresie cyberbezpieczeństwa są problemem, który dotyczy pracowników różnego typu organizacji na całym świecie i jest szczególnie widoczny w zazwyczaj niedoinwestowanym sektorze publicznym, w tym samorządowym. Braki kompetencyjne wynikają nie tylko ze zbyt niskich nakładów finansowych przeznaczanych na ten cel, ale również z braku świadomości, że zapewnienie cyberbezpieczeństwa wymaga zaangażowania wszystkich pracowników organizacji. Badania przeprowadzone w jst potwierdzają, że doświadczają one licznych cyberataków, a jednocześnie znaczna część urzędników samorządowych nie jest świadoma tych ataków i naruszeń systemów informatycznych (Caruson i in., 2012; Koszewski i in., 2020; Macmanus i in., 2013).

Zwraca się więc uwagę na potrzebę podejmowania działań przyczyniających się do zwiększenia świadomości cyberbezpieczeństwa w samorządzie terytorialnym oraz budowania tzw. kultury cyberbezpieczeństwa. Niewystarczający poziom umiejętności pracowników może bowiem prowadzić w przyszłości do utraty zdolności obrony przed cyberprzestępcami. Ważne jest więc wdrażanie odpowiednich działań o charakterze prewencyjnym, których pierwszym etapem jest zawsze identyfikacja potencjalnych zagrożeń cyberbezpieczeństwa. Aby tego dokonać, konieczna jest znajomość technik i rozwiązań stosowanych przez cyberprzestępców.

Celem tego rozdziału jest przedstawienie rodzajów cyberataków, których prawdopodobieństwo wystąpienia w jednostkach samorządu terytorialnego jest najwyższe. Podjęto próbę scharakteryzowania schematów działań cyberprzestępców oraz wskazano propozycje działań prewencyjnych zmniejszających ryzyko wystąpienia danego cyberataku, które mogą być wdrożone w sektorze samorządowym. W drugiej części rozdziału zaprezentowano wyniki badania ankietowego przeprowadzonego wśród jednostek samorządu gminnego w Polsce w 2020 r. Badanie dostarczyło informacji między innymi o świadomości istniejących zagrożeń pracowników jednostek samorządu terytorialnego, istniejącej polityce zarządzania bezpieczeństwem informacji oraz rodzajach cyberataków, które wystąpiły w ankietowanych jednostkach.

6.2. Rodzaje cyberataków

Cyberprzestępcy stosują coraz bardziej wyszukane sposoby, aby osiągnąć swój cel – pozyskać pożądane przez nich dane, informacje czy środki finansowe. Wbrew niektórym opiniom, podczas cyberataków nie korzysta się powszechnie z zaawansowanych środków technicznych. Zdecydowanie częściej wykorzystuje się proste i dużo tańsze metody wykorzystujące często moment nieuwagi lub nieświadomość użytkownika systemu informacyjnego.

Do najpopularniejszych cyberataków należą: phishing, spam, wyciek informacji, w tym kradzież danych powiązana niekiedy z ujawnieniem poufnych informacji, botnet, złośliwe oprogramowanie, w szczególności *rogueware, ransomware* czy *scareware*, wstrzyknięcie kodu, *exploit drive-by-download* na zainfekowanej stronie (CSIRT GOV, 2021; Gąska, 2015; Grzelak i Liedel, 2012).

Phishing

Wiele cyberataków odbywa się przez phishing. Pierwszy raz słowo phishing pojawiło się w 1996 r. w kontekście wyłudzenia informacji od użytkowni-

ków dużego amerykańskiego serwisu AOL (America Online). Wysłano wówczas spreparowane wiadomości z prośbą o udostępnienie danych dostępowych do kont użytkowników. Jak się okazało, wielu użytkowników nieświadomie podało komplet informacji (Stępniewski, 2020a). Phishing jest metodą oszustwa, w której cyberprzestępca podszywa się pod inną osobę lub instytucję. Cel phishingu może być różny: (1) wyłudzenie pożądanych informacji (np. dane logowania, szczegóły karty kredytowej, hasła, kody PIN); (2) zainfekowanie komputera złośliwym oprogramowaniem lub (3) nakłonienie ofiary do określonych działań.

Ten rodzaj cyberataku polega na wysyłaniu wiadomości, które na pierwszy rzut oka wyglądają autentycznie. Wiadomość phishingowa najczęściej nakłania atakowaną osobę do konkretnego działania (kliknięcia w link, sprawdzenia szczegółów, zweryfikowania danych, ustawień lub wręcz prośby o zalogowanie się np. w systemie bankowym). Głównym czynnikiem wpływającym na skuteczność tych działań jest łudząco podobny format wiadomości – te same czcionki, stopka w e-mailu, logo firmy czy też styl komunikacji firmy, pod którą podszywają się hakerzy. Chodzi o to, by użytkownik lub klient był przekonany, że otrzymał wiadomość od rzeczywistej firmy. Wyłudzanie informacji metodą phishingu bazuje na nieostrożności osoby atakowanej, która podejmuje działania, do jakich namawia ją treść wiadomości. Technika ta opiera się często na chciwości, strachu lub zaufaniu do autorytetu (CSIRT GOV, 2021; Stępniewski, 2020a).

Szczególnym rodzajem phishingu jest tzw. spear phishing, czyli atak ukierunkowany na konkretnego adresata. Takim atakiem są szczególnie zagrożone osoby publiczne. Przestępcy mogą podszywać się pod znajomych z pracy, dziennikarzy, współpracowników, a wiadomość może być spersonalizowana, tzn. odwoływać się bezpośrednio do relacji atakowanej osoby. Podobnie jak w przypadku standardowego phishingu atakowana osoba otrzymuje wiadomość e-mail, która wydaje się pochodzić od zaufanej osoby lub organizacji. W spear phishingu jednak przestępcy nie rozsyłają zainfekowanych e-maili do milionów przypadkowych użytkowników, lecz dobierają indywidualnie swoje ofiary. Atak spear phishingowy jest poprzedzony pogłębionym wywiadem środowiskowym atakowanej osoby, a jego celem jest wyłudzenie poufnych informacji – haseł dostępu lub tajemnic handlowych (Burns i in., 2019; Kulik, 2013; Parmar, 2012).

W 2020 r. nastąpił wzrost liczby kampanii phishingowych względem 2019 r. Celem tych szeroko zakrojonych kampanii stała się również administracja publiczna, w tym samorządowa. W atakach wykorzystywano wizerunek m.in. firm kurierskich oraz operatorów telekomunikacyjnych. Celem tych ataków była najczęściej próba infekcji złośliwym oprogramowaniem lub pozyskanie danych autoryzacyjnych. Wiadomości zawierały informacje dotyczące rzekomych przesyłek pocztowych oraz link, pod którym można było uiścić dopłatę do przesyłki. W innych przypadkach treść korespondencji nawiązywała do ko-

nieczności opłacenia faktury za usługi telekomunikacyjne. W tej formie wiadomość zawierała zwykle załącznik imitujący plik PDF z fakturą, która okazywała się najczęściej formatem XLS oraz XLSM zawierającym złośliwe oprogramowanie (CSIRT GOV, 2021).

Najskuteczniejszą metodą zabezpieczenia przed atakami phishingowymi jest nieustanne zachowywanie czujności i zdrowego rozsądku. Cyklicznie należy podejmować działania szkoleniowe wśród pracowników, podczas których prezentowane są przykłady wiadomości phishingowych. W wiadomościach tego typu bardzo często występują błędy językowe, zarówno literówki, jak i błędna składnia językowa. Podejrzane powinny się wydać wiadomości z banków z linkiem, wiadomości od podmiotów, z którymi nigdy nie współpracowaliśmy czy wiadomości urzędowe nakłaniające do natychmiastowej wpłaty jakiejś grzywny, kary czy innego zobowiązania. Jeśli do wiadomości, które wzbudzają nasze podejrzenie, są dołączone jakieś pliki, nie należy ich otwierać ani zapisywać na dysku lokalnym. Wszystkie wiadomości o cechach właściwych phishingowi powinny być zgłaszane do komórki (osoby) IT w jednostce.

Spam

Powszechnie spotykanym rodzajem cyberataku jest spam. Spam jest niepożądaną przez odbiorców wiadomością tekstową, która jest wysyłana masowo, do wielu odbiorców, w formie reklamy. Spam to głównie oferty reklamowe i promocyjne różnych produktów i usług. Nadawcą tych wiadomości są firmy (z reguły zagraniczne, które trudno zidentyfikować) lub hakerzy (tzw. spamerzy), którzy mają na celu wyłudzenie danych osobowych lub uzyskanie dostępu do komputera. Do głównych cech spamu zaliczamy: (1) brak zgody odbiorcy na otrzymywanie tego rodzaju wiadomości; (2) pojawia się zawsze, niezależnie od interesującej odbiorcę tematyki, przyjmując najczęściej postać reklam firm farmaceutycznych, organizacji charytatywnych i społecznych; (3) przesłana wiadomość służy osiągnięciu korzyści materialnych przez nadawcę (*Co to jest spam…*, 2022; *Spam…*, 2022; Jindal i Liu, 2007).

Spamerzy chcą nie tylko zachęcić atakowaną osobę do zakupu – ich celem może być zainfekowanie komputera lub poznanie wrażliwych danych. Do wiadomości typu spam mogą być dołączane zainfekowane pliki, które po ściągnięciu samoczynnie instalują na komputerze wirusy lub programy szpiegujące. Najczęściej stosowaną przez spamerów praktyką jest wiadomość tekstowa z prośbą o podanie adresu lub odesłanie e-maila w celu rezygnacji z otrzymywania kolejnych maili. Użytkownicy, wykonując polecenie, weryfikują w ten sposób swoje dane, a to z kolei pozwala na bardziej agresywne ataki spamerskie.

W tym rodzaju cyberataku wykorzystuje się przede wszystkim nieuwagę i niefrasobliwość użytkowników. Bardzo często nie traktują oni adresu mailo-

wego jako wrażliwych danych i dość beztrosko podają go na różnych serwisach, a następnie są wprost zasypywani spamem. Użytkownicy nieświadomie godzą się na otrzymywanie tych wszystkich wiadomości.

Główną formą zabezpieczenia przed spamem jest zachowanie zdrowego rozsądku, ignorowanie – a najlepiej natychmiastowe usuwanie – wiadomości nieznanego pochodzenia i kategoryczny zakaz otwierania nowych e-maili, nawet jeśli ominęły filtry antyspamowe. Wszelkie aktywności związane ze spamem warto od razu zgłaszać administratorowi serwera. Nie należy przy tym zapominać o ochronie komputera programami antywirusowymi i antyspamowymi, których używanie przy regularnych aktualizacjach powinno zminimalizować ryzyko wystąpienia spamu. Administratorzy sieci powinni dodatkowo pamiętać o konfiguracji odpowiednich filtrów antyspamowych oraz wprowadzeniu metody zwanej *greylisting,* polegającą na automatycznym usuwaniu wiadomości od niezidentyfikowanych nadawców, których dodaje się do specjalnej bazy, by uniknąć kolejnych prób przesłania spamu z tego adresu (Hayati i in., 2010; Jindal i Liu, 2007).

Wyciek informacji

Wyciek informacji (danych) jest niepożądanym zdarzeniem skutkującym upowszechnieniem danych, którego przyczyną jest utrata lub nieautoryzowane ich użycie. Do sytuacji takiej dochodzi, gdy nie zostają zachowane atrybuty bezpieczeństwa informacji: dostępność, poufność i integralność (Madej, 2011). Wyciek informacji może nastąpić na skutek błędu ludzkiego, nieświadomego działania pracownika. Natomiast w sytuacji, w której wyciek jest konsekwencją umyślnego działania, przybiera on formę cyberataku.

Wyciek informacji może być spowodowany zagrożeniami wewnętrznymi i zewnętrznymi. Do zagrożeń wewnętrznych zaliczamy błędy użytkowników związane z brakiem odpowiednich szkoleń lub niedbałością w wykonywaniu swoich obowiązków, celowe działania niezadowolonych lub skorumpowanych pracowników skutkujące kradzieżą, fałszerstwem lub zniszczeniem informacji oraz niesprawność systemów informatycznych i sprzętowych spowodowana zużyciem lub nieprawidłowym użytkowaniem. Zagrożeniem zewnętrznym natomiast może być umyślny atak na system informacyjny skutkujący utratą danych, awarią sprzętu wynikającą z braku prądu, kataklizmy naturalne, takie jak powódź, pożar, trzęsienie ziemi czy katastrofy budowlane, komunikacyjne (Czekaj, 2012; *Największe wycieki…*, 2021). Szczególnym typem wycieku danych jest zatem kradzież danych prowadząca niekiedy, choć nie zawsze, do ujawnienia danych wrażliwych. Wyciek danych ma wówczas charakter przestępstwa i powstaje na skutek celowego działania cyberprzestępcy, którego celem jest osiągnięcie korzyści osobistych lub majątkowych.

Konsekwencjami wycieków informacji są nie tylko utrata reputacji i potencjalne straty finansowe, ale przede wszystkim narażenie użytkowników na

działania cyberprzestępców, którzy na skutek tego cyberataku uzyskują dane logowania, numery telefonów, dane osobowe, informacje dotyczące kart kredytowych czy inne dane wrażliwe (Góra, 2013; Machura, 2013).

Zapewnienie bezpieczeństwa i przeciwdziałanie wyciekom informacji wymaga ciągłego doskonalenia systemów informacyjnych. Bezpieczeństwo nie jest bowiem działaniem jednorazowym, które polega na wdrożeniu zabezpieczeń, lecz dynamicznym i złożonym procesem, który wymaga stałego nadzoru i przystosowania do zmiennych warunków otoczenia (Czekaj, 2012). Przykłady rozwiązań budujących bezpieczeństwo informacji, wdrożonych w jednostce samorządu terytorialnego przedstawił Wiśniewski (2014). Ryzyko wycieku informacji mogą zmniejszyć również systematyczne szkolenia pracowników z jednej strony podnoszące świadomość zagrożeń ze strony cyberprzestępców, z drugiej zwiększające poziom tzw. kultury cyberbezpieczeństwa.

Działalność botnetów

Duże znaczenie dla cyberbezpieczeństwa ma dynamicznie rozwijająca się działalność tzw. botnetów. Bot stanowi pojedynczy element (komputer) tzw. botnetu – grupy komputerów zainfekowanych złośliwym oprogramowaniem pozwalającym na zdalną kontrolę nad wszystkimi komputerami należącymi do botnetu. Komputery należące do botnetu mogą być wykorzystywane do ataków bez wiedzy ich właścicieli. Komputer jest narażony na dołączenie do sieci botnet, jeżeli nie są na nim systematycznie wykonywane aktualizacje oprogramowania systemu operacyjnego oraz wszystkich zainstalowanych na nim aplikacji. Czynnikiem zwiększającym ryzyko dołączenia komputera do sieci botnet jest również brak zainstalowanego programu antywirusowego, który jest automatycznie i regularnie aktualizowany. Niezabezpieczony komputer może stać się częścią botnetu przykładowo poprzez kliknięcie w link z wiadomości e-mail, odwiedzenie zainfekowanej strony www czy zainstalowanie oprogramowania pobranego z nieznanego źródła, które ma służyć do innych celów, ale jest jednocześnie zainfekowane.

Sieć botnet jest najczęściej wykorzystywana do rozsyłania spamu lub do rozproszonych ataków typu „odmowa usługi" (DDoS). Ataki te uniemożliwiają dostęp do usług i zasobów, zalewając systemy ogromną liczbą zapytań, których nie sposób obsłużyć, oraz połączeń z daną stroną www. Jeżeli właściciel nie zabezpieczył się na taką okoliczność, może to spowodować czasową niedostępność.

Podstawową formą zabezpieczenia komputerów przed włączeniem ich do sieci botnet jest zachowanie podstawowej zasady aktualizacji oprogramowania. Wszystkie komputery powinny być również zabezpieczone programem antywirusowym, który podlega systematycznej aktualizacji. Cyklicznie należy rów-

nież wykonywać skanowanie komputerów programem antywirusowym w celu wykrycia ewentualnego złośliwego oprogramowania (Abu Rajab i in., 2006; Stępniewski, 2020b; Zhu i in., 2008).

Złośliwe oprogramowanie

Złośliwe oprogramowanie jest terminem określającym różnego rodzaju oprogramowanie, które zostało zaprojektowane w celu uszkadzania lub wykorzystania urządzenia lub sieci. Cyberprzestępcy wykorzystują je zwykle do pobierania danych, aby wywrzeć nacisk na ofiarę w celu uzyskania korzyści, np. finansowej. Cele działania cyberprzestępców mogą być różne, przykładowo oszukanie atakowanej osoby, mające na celu podanie przez nią danych osobowych w celu kradzieży tożsamości, kradzież danych karty kredytowej lub innych danych finansowych, przejmowanie kontroli nad wieloma komputerami w celu przeprowadzenia ataków typu „odmowa usługi" (DDoS) na inne sieci czy infekowanie komputerów i używanie ich do wydobywania kryptowalut (*Co to jest złośliwe…*, 2021; Pathak, 2016).

Cyberprzestępcy wykorzystują różne metody ataku, aby zainfekować urządzenie lub sieć złośliwym oprogramowaniem (*malware*). Do metod tych zaliczamy przykładowo załączniki wiadomości e-mail, złośliwe reklamy w popularnych witrynach, fałszywe instalacje oprogramowania, zainfekowane dyski USB czy zainfekowane aplikacje. Złośliwe oprogramowanie (*malware*) obejmuje różnego rodzaju programy, które charakteryzują się zróżnicowanym schematem działania. Obejmuje ono między innymi wirusy komputerowe, robaki, oprogramowanie typu *ransomware, scareware, rogueware* i *adware*, konie trojańskie i oprogramowanie szpiegujące (Pathak, 2016).

Wirusy komputerowe są aplikacjami, które mogą się same kopiować, dołączając swój kod do innych plików w systemie. Celem działania wirusów jest rozprzestrzenianie się z pliku na plik i z komputera na komputer, zagrażające integralności zainfekowanego komputera. W większości przypadków wirus modyfikuje pliki systemowe, co uniemożliwia uruchomienie systemu operacyjnego. Wirus zwykle przychodzi jako załącznik w wiadomości e-mail, który przechowuje ładunek wirusa, lub jako część złośliwego oprogramowania , które wykonuje szkodliwe działania. Gdy ofiara otwiera plik, urządzenie zostaje zainfekowane. Natomiast robak rozprzestrzenia się bez plików – do działania wystarczą mu luki w systemie operacyjnym. W przeciwieństwie do wirusów, robaki nie wymagają interakcji użytkownika do działania.

Wirusy i robaki są coraz rzadziej stosowane przez cyberprzestępców, którym zależy, aby ich działania pozostawały jak najdłużej niezauważone. Z racji tego, że wirusy i robaki komputerowe atakują pliki i systemy operacyjne, ich działanie jest zbyt widoczne dla użytkowników zaatakowanych komputerów.

Jednym z najbardziej dochodowych, a zatem najpopularniejszych rodzajów złośliwego oprogramowania wśród cyberprzestępców jest oprogramowanie *ransomware*. Działanie oprogramowania typu *ransomware* polega na szyfrowaniu danych, tak aby uniemożliwić użytkownikom dostęp do plików do momentu, aż zostanie opłacony okup (ang. *ransom*) albo użytkownicy wykonają określone działanie (Gazet, 2010; Mohurle i Patil, 2017).

W przypadku gdy cyberprzestępcy, chcąc przekonać do zakupu fałszywej aplikacji, straszą nas i sprawiają, że myślimy, że nasze komputery lub smartfony zostały zainfekowane, mamy do czynienia z cyberatakiem typu *scareware*. Podczas typowego oszustwa *scareware* w trakcie przeglądania internetu może się pojawić alarmujący komunikat „Ostrzeżenie: Twój komputer jest zainfekowany!" lub „Masz wirusa!" Cyberprzestępcy wykorzystują te programy i nieetyczne praktyki reklamowe, aby zastraszyć użytkowników i w ten sposób skłonić do zakupu nieuczciwych aplikacji (Giles, 2010).

Cyberatakiem o wysokiej skuteczności jest metoda oparta na oprogramowaniu typu *rogueware*. *Rogueware* jest fałszywym oprogramowaniem antywirusowym, którego ściągnięcie na komputer lub inne urządzenie jest równoznaczne z jego zainfekowaniem („Rogueware…", 2009). Z kolei cyberatak typu *adware* następuje przy użyciu oprogramowania z reklamami, które pokazuje użytkownikom niechciane reklamy. Oprogramowanie *adware* jest często instalowane w zamian za inną usługę, na przykład prawo do bezpłatnego korzystania z programu. Podczas ataku typu *adware* często pozyskiwane są dane osobowe lub gromadzone informacje marketingowe (Chien, 2005).

Kolejnym typem złośliwego oprogramowania jest koń trojański (trojan). Może on stanowić element samodzielnego oprogramowania lub być narzędziem do przeprowadzenia innych zadań, np. zainfekowania innymi szkodliwymi programami, komunikacji z cyberprzestępcą lub otworzenia systemu na ataki. Trojan nie jest fragmentem kodu, jak wirus, ale samodzielnie działającym programem. Koń trojański wykorzystuje socjotechnikę, czyli różnego typu środki psychologiczne i metody manipulacji, aby nakłonić użytkownika do zainstalowania programu na swoje urządzenie. Konie trojańskie podszywają się pod nieszkodliwe aplikacje, nakłaniając użytkowników do ich pobrania i korzystania z nich. Po uruchomieniu powodują różnego rodzaju szkody. Głównym wyznacznikiem tego, czy dany program jest trojanem, jest mechanizm jego działania – podszywanie się pod przydatne lub ciekawe aplikacje i równoczesne wprowadzanie niepożądanych i ukrytych funkcji (*Rodzaje…*, 2021; Zhenfang, 2015).

Działania trojanów mogą przybierać różną formę. Do najczęściej występujących można zaliczyć: tworzenie luki w zabezpieczeniach systemu, która ma pozwolić na udostępnienie kontroli nad systemem, np. w celu wysyłania spamu; szpiegowanie użytkownika i wykradanie jego poufnych danych, np. danych osobowych, loginów i haseł do bankowości, numerów kart płatniczych; utrud-

nianie lub zaburzanie pracy programów antywirusowych; zmiana strony startowej przeglądarki; kasowanie plików; blokowanie dostępu do systemu komputerowego. Niektóre trojany mogą mieć również dodatkowe funkcje – mniej szkodliwe, jednak wciąż denerwujące, jak np. wyłączanie monitora, wysuwanie napędu DVD czy samoistne otwieranie stron internetowych (*Rodzaje*…, 2021; Zhenfang, 2015).

Do częstych objawów zainfekowania komputera trojanem można zaliczyć przykładowo: samoczynne otwieranie i zamykanie programów, komputer samodzielnie wyświetla pliki, urządzenie nie reaguje na polecenia użytkownika, dostęp do niektórych plików jest zablokowany, pliki i foldery znikają lub zmieniają zawartość, nastąpiło zmniejszenie dostępnej przestrzeni na dysku bez znanego powodu, na skrzynce mailowej pojawia się duża liczba wiadomości o charakterze spamu. Te i inne nietypowe zmiany w funkcjonowaniu urządzenia powinny wzbudzać czujność użytkownika, ponieważ mogą wskazywać na zainfekowanie trojanami (*Rodzaje*..., 2021; Zhenfang, 2015).

Podobnie jak w przypadku innych rodzajów złośliwego oprogramowania najskuteczniejsze w walce z trojanami są działania o charakterze prewencyjnym. W polityce bezpieczeństwa informacji warto wprowadzić kilka podstawowych zasad, których przestrzeganie zmniejszy prawdopodobieństwo zainfekowania urządzenia trojanem. Należą do nich: systematyczna aktualizacja aplikacji i programów, w tym programów antywirusowych (warto skonfigurować system tak, aby aktualizacje instalowały się automatycznie), rezygnacja z instalacji darmowych programów pochodzących z nieznanego źródła, unikanie niebezpiecznych i podejrzanych stron internetowych oraz korzystania z urządzeń zewnętrznych (np. pendrive) nieznanego pochodzenia, używanie złożonych haseł (Kara i Aydos, 2019; *Rodzaje*..., 2021).

Wstrzyknięcie kodu

Wstrzyknięcie kodu jest rodzajem cyberataku na oryginalne kodowanie programu lub słabo zabezpieczonej strony internetowej. Wstrzyknięty złośliwy kod zmienia całą stronę internetową bądź program lub go niszczy. Do cyberataku polegającego na wstrzyknięciu kodu dochodzi najczęściej wówczas, gdy administrator nie dodaje reguł ograniczających użycie niektórych znaków znalezionych w atakach wstrzykiwanych. Wstrzyknięcie kodu może spowodować np. wprowadzenie złośliwego oprogramowania, umożliwienie hakerowi dostępu do prywatnych informacji, umożliwienie hakerowi kradzieży plików cookie i danych sesji lub po prostu zniszczenie oryginalnego kodowania i unieważnienie strony internetowej lub programu (Ray i Ligatti, 2012).

Szczególnym rodzajem wstrzyknięcia kodu jest cyberatak typu *exploit drive-by-download*. Polega on na tym, że do kodu strony znajdującej się na serwerze

wstrzykiwany jest złośliwy skrypt zawierający odnośnik do witryny serwującej szkodliwe oprogramowanie. Po wejściu na zmodyfikowaną stronę następuje niewidoczne dla użytkownika przekierowanie do szkodliwego adresu, uruchomienie exploita, a następnie pobranie i instalacja szkodliwego oprogramowania na komputerze użytkownika. Ten rodzaj cyberataku charakteryzuje prostota działania, szybkość rozprzestrzeniania się zagrożenia oraz wysoka skuteczność, co sprawia, że jest to metoda bardzo popularna wśród cyberprzestępców. W tym ataku jako medium wykorzystuje się internet, co pozwala na dotarcie do szerokiego grona odbiorców. Cyberprzestępcy wykorzystują istniejące witryny internetowe i wypracowane wcześniej zaufanie do nich, korzystają ze znanych porali internetowych oraz stron o statusie uznanym za bezpieczny. Wykorzystanie zaufania jest najważniejszym czynnikiem wpływającym na wysoką skuteczność cyberataku. Charakterystyczna w tym przypadku jest również nieprzewidywalność – nie sposób przewidzieć, która strona może zostać zainfekowana i kiedy. Warto dodać, że proces ten zachodzi bez udziału użytkownika: nie ma konieczności kliknięcia odnośnika, wyrażenia zgody na instalację czy potwierdzenia komunikatu. Szkodliwa strona otwiera się w niewidocznej ramce, nie ma więc nawet żadnych symptomów wskazujących na to, że dzieje się coś, co powinno wzbudzać niepokój użytkownika (Le i in., 2013; Sood i Zeadally, 2016).

Znalezienie skutecznego rozwiązania, które ograniczy liczbę cyberataków typu *exploit drive-by-download*, nie jest łatwe. Ten rodzaj ataku jest kierowany na pojedyncze komputery w sieci. Należy więc zadbać o dobre zabezpieczenie każdej stacji roboczej. Podstawą wydaje się edukacja użytkowników w zakresie zasad bezpiecznego korzystania z internetu. Przede wszystkim należy stosować podstawowe zasady bezpieczeństwa, do których zaliczamy aktualne wersje oprogramowania, aktualny system operacyjny, dobrze skonfigurowana zapora sieciowa oraz skuteczna ochrona antywirusowa.

6.3. Cyberataki w jednostkach samorządu gminnego w świetle badania

Autorki przeprowadziły badanie w zakresie cyberbezpieczeństwa w sektorze samorządowym szczebla gminnego. W badaniu przyjęto założenie, że sektor samorządowy w Polsce charakteryzuje się niską świadomością w zakresie cyberbezpieczeństwa, przez co jest podatny na cyberataki. Badanie dotyczyło między innymi identyfikacji skali i rodzaju cyberataków, które wystąpiły w gminach.

Badanie zostało przeprowadzone w drugim kwartale 2020 r. Do zebrania danych wykorzystano kwestionariusz ankiety w wersji elektronicznej, wypełniany

przez respondentów samodzielnie po przesłaniu do nich prośby zawierającej adres dostępu do badania (*Computer Assisted Web Interview* – CAWI). Zastosowano metodę pełną badania i ankieta została rozesłana do urzędów wszystkich gmin w Polsce. Badaniem objęto w sumie 2477 gmin – 1513 gmin wiejskich, 662 gmin miejsko-wiejskich, 302 gminy miejskie oraz 66 miast na prawach powiatu.

Ostatecznie otrzymano odpowiedzi od *N* – 1787 gmin (zwrotność ankiet wyniosła 72,1%), głównie z gmin wiejskich (60,0%), następnie miejsko-wiejskich (24,0%), mniejszą część stanowiły odpowiedzi z gmin miejskich (13,0%) i miast na prawach powiatu (3,0%). Najwięcej gmin pochodziło z województwa mazowieckiego (13,5%), małopolskiego (9,0%), lubuskiego (8,05%) i śląskiego (8,4%). Pod względem liczby mieszkańców przeważały odpowiedzi osób z gmin do 10 tys. mieszkańców (64,4%), drugą co do znaczenia grupą były osoby z gmin o liczbie mieszkańców 10–20 tys. (20,9%). W badanej grupie przeważały gminy z dochodami bieżącymi poniżej 3 tys. zł na mieszkańca (36,5%), a następnie gminy z dochodami 4–4,5 tys. zł na mieszkańca (18,1%) (tabela 28).

Tabela 28. Badane gminy według województwa, liczby mieszkańców i wysokości dochodów bieżących na mieszkańca

Wyszczególnienie	Liczba	Odsetek w próbie	Wyszczególnienie	Liczba	Odsetek w próbie
Województwo			**Liczba mieszkańców**		
Warmińsko-mazurskie	86	4,8	do 10 000	1150	64,4
Wielkopolskie	6	0,3	10 000–20 000	373	20,9
Dolnośląskie	121	6,8	20 000–30 000	109	6,1
Kujawsko-pomorskie	125	7,0	30 000–40 000	47	2,6
Lubelskie	152	8,5	40 000–50 000	34	1,9
Lubuskie	64	3,6	50 000–100 000	38	2,1
Łódzkie	143	8,0	powyżej 100 000	36	2,0
Małopolskie	161	9,0	**Wysokość bieżących dochodów budżetowych na mieszkańca (w zł)**		
Mazowieckie	241	13,5	poniżej 3000	652	36,5
Opolskie	56	3,1	3000–3500	182	10,2
Podkarpackie	114	6,4	3500–4000	231	12,9
Podlaskie	99	5,5	4000–4500	324	18,1
Pomorskie	95	5,3	4500–5000	213	11,9
Śląskie	151	8,4	powyżej 5000	185	10,4
Świętokrzyskie	76	4,3			
Zachodniopomorskie	97	5,4			

Źródło: opracowanie własne na podstawie badań.

Pytania w pierwszej części badania dotyczyły systemów zarządzania bezpieczeństwem informacji w badanych gminach (tabela 29).

Tabela 29. Charakterystyka zakresu wdrażania systemu zarządzania bezpieczeństwem informacji w gminach

Wyszczególnienie	Liczba	Odsetek	Wyszczególnienie	Liczba	Odsetek
Czy gmina została uznana za operatora usługi kluczowej?			**Przyczyny braku wdrożenia w gminie systemu zarządzania bezpieczeństwem informacji**		
tak	64	3,6	brak wystarczających środków finansowych	155	37,5
nie	1723	96,4	brak elektronicznego obiegu dokumentów	103	24,9
Podmiot wyznaczony do utrzymywania kontaktów z podmiotami krajowego systemu bezpieczeństwa			brak obowiązku prawnego w tym zakresie	83	20,1
wójt (burmistrz, prezydent) lub zastępca	26	40,6	brak specjalisty z zakresu informatyki	15	3,6
sekretarz gminy	6	9,4	nie widzimy potrzeby	26	6,3
pracownik zatrudniony na stanowisku do spraw informatyki	26	40,6	inny powód	31	7,5
inna osoba zatrudniona w urzędzie	6	9,4	**Gmina wdroży system zarządzania bezpieczeństwem informacji, jeżeli:**		
Czy w urzędzie wdrożono system zarządzania bezpieczeństwem informacji?			organy administracji rządowej przekażą na ten cel dodatkowe środki w formie dotacji	216	52,3
tak	1374	76,9	wprowadzony zostanie w urzędzie elektroniczny obieg dokumentów	81	19,6
nie	413	23,1	otrzymamy dofinansowanie ze środków unijnych	54	13,1
Czy wdrożony system zarządzania bezpieczeństwem informacji posiada akredytacje zgodności z normą PN-ISO/IEC 27001:2017-06?			podpiszemy porozumienie z sąsiednimi gminami w sprawie wspólnego wdrożenia takiego systemu	11	2,7
tak	244	17,8	w innych przypadkach	51	12,3
nie	1130	82,2			

Źródło: opracowanie własne na podstawie badań.

Za operatora usługi kluczowej uznanych zostało jedynie 3,6% badanych gmin. Do utrzymywania kontaktów z podmiotami krajowego systemu bezpieczeństwa w gminie zostali wyznaczeni głównie pracownicy zatrudnieni na stanowisku do spraw informatyki (40,6%) lub kierownicy jednostek (odpowiednio wójt, burmistrz lub prezydent miasta) (40,6%). System zarządzania bezpieczeństwem informacji został wdrożony w 76,9% badanych gmin, z czego w przypadku 82,2% gmin system ten posiadał akredytację zgodności z normą PN-ISO/IEC 27001:2017-06. W gminach, w których nie wdrożono systemu bezpieczeństwa informacji, jako główne przyczyny wskazywano brak wystarczających środków finansowych (37,5%) i brak elektronicznego obiegu dokumentów (24,9%). Badane gminy deklarowały, że do wdrożenia systemu zarządzania bezpieczeństwem informacji przekonałoby je przekazanie na ten cel dodatkowych środków przez organy administracji rządowej (52,3%) lub wprowadzenie elektronicznego obiegu dokumentów (19,6%).

Następnie ankietowani zostali zapytani o postrzeganie cyberprzestępczości jako zagrożenia dla działalności urzędu. W opinii badanych osób cyberprzestępczość stanowi średnie (34,9%) lub duże (31,4%) zagrożenie dla urzędu. Jedynie 3,5% osób było zdania, że cyberprzestępczość nie stanowi zagrożenia dla urzędu. W przypadku 78,5% urzędów była przeprowadzana okresowa analiza ryzyka utraty integralności, poufności i dostępności informacji. Wśród przyczyn nieprzeprowadzania takiej analizy były głównie braki w środkach finansowych (35,6%). Prawie co czwarty ankietowany (24,7%) uważał, że nie ma takiej potrzeby. Aktualna i kompletna elektroniczna ewidencja sprzętu informatycznego była prowadzona w przypadku 81,0% urzędów. Coroczny audyt wewnętrzny bezpieczeństwa informacji był przeprowadzany najczęściej przez usługodawcę zewnętrznego (44,9% urzędów), w 30,1% przez audytora wewnętrznego. W co czwartym urzędzie nie było takiego audytu. Powodem nieprzeprowadzenia wewnętrznego audytu bezpieczeństwa informacji w większości przypadków był również brak środków finansowych (59,3%). Incydenty związane z naruszeniem bezpieczeństwa informacji w latach 2017–2019 nie wystąpiły w 86,7% urzędów. W pozostałych przypadkach zaobserwowano do pięciu takich incydentów (10,6%). W przypadku wystąpienia takich incydentów aż 44,4% urzędów nigdzie ich nie zgłosiło.

W badaniu zapytano również o elementy urzędu najbardziej podatne – zdaniem ankietowanych – na cyberprzestępczość. Najczęściej wymienianymi byli pracownicy (57,5%), dane osobowe (54,1%) i sprzęt pracowniczy (44,0%), a za najmniej podatną na cyberprzestępczość badani uważali infrastrukturę w chmurze (8,1%). Natomiast w części badania poświęconej rodzajom działalności cyberprzestępczej, która najczęściej występowała w ankietowanych gminach, uzyskano informację, że był to spam (79,1%), następnie phishing (26,5%) i złośliwe oprogramowanie (26,5%). W urzędach z działań zabezpieczających używane

były głównie programy antywirusowe (96,3%), *firewalle* (89,0%) oraz blokady i filtry spamu (69,2%). Bardzo sporadycznie były w gminach stosowane SIEM (2,7%), szyfrowanie VOIP (5,4%) oraz systemy wczesnego ostrzegania (7,8%) (tabela 30).

Tabela 30. Elementy urzędu podatne na cyberprzestępczość, rodzaje działalności cyberprzestępczej oraz zastosowane w urzędzie rozwiązania zabezpieczające

Wyszczególnienie	Liczba	Odsetek	Wyszczególnienie	Liczba	Odsetek	Wyszczególnienie	Liczba	Odsetek
Elementy urzędu szczególnie podatne na cyberprzestępczość			**Przykłady działalności cyberprzestępczej, które wystąpiły w urzędzie**			**Rozwiązania zabezpieczające przed cyberatakami stosowane w urzędzie**		
infrastruktura krytyczna	301	16,8	phishing	474	26,5	*firewalle*	1591	89,0
infrastruktura w chmurze	145	8,1	spam	1413	79,1	antywirusy	1720	96,3
dane osobowe	967	54,1	wyciek informacji	54	3,0	skanery podatności	294	16,5
usługi online/ aplikacje webowe/strony internetowe	593	33,2	botnet	28	1,6	blokady i filtry spamu	1237	69,2
systemy płatności	347	19,4	złośliwe oprogramowanie	474	26,5	szyfrowanie danych	992	55,5
pracownicy	1028	57,5	wstrzyknięcie kodu	26	1,5	systemy wczesnego ostrzegania	139	7,8
stacje robocze (sprzęt pracowników)	787	44,0	kradzież danych (ujawnienie poufnych informacji)	19	1,1	szyfrowanie VOIP	97	5,4
inne	45	2,5	*rogueware/ ransomware/ scareware*	143	8,0	dedykowane zasoby VPN	627	35,1
			exploit drive-by--download	62	3,5	SIEM	49	2,7
			inne	211	11,8	systemy IDS/IPS	644	36,0
						systemy DLP	184	10,3
						inne	78	4,4

Źródło: opracowanie własne na podstawie badań.

W tabeli 31 przedstawiono rozkład rodzajów cyberataków, które wystąpiły w badanych urzędach gmin, według typu gminy, wielkości gminy i bieżących dochodów budżetowych na mieszkańca.

Tabela 31. Rozkład rodzajów działalności cyberprzestępczej występującej w urzędzie według typu gminy, wielkości gminy i bieżących dochodów budżetowych na mieszkańca (w %)

Przykłady działalności cyberprzestępczej, które wystąpiły w urzędzie	Typ gminy				Wielkość gminy			Dochody		
	gmina wiejska	gmina miejska	gmina miejsko-wiejska	miasto na prawach powiatu	do 10 tys.	10–30 tys.	powyżej 30 tys.	poniżej 3 tys. zł	3–4,5 tys. zł	powyżej 4,5 tys. zł
Phishing	24,2	24,9	30,6	47,4	22,7	32,4	36,8	23,0	26,6	32,2
Spam	78,8	79,3	78,9	84,2	77,0	82,0	85,2	76,5	78,8	83,7
Wyciek informacji	1,9	5,9	2,6	15,8	1,9	4,4	7,1	2,6	2,7	4,3
Botnet	1,4	1,3	1,2	8,8	1,2	1,7	3,9	1,4	0,8	3,3
Złośliwe oprogramowanie	24,5	32,5	26,8	38,6	24,2	30,1	32,9	26,1	26,3	27,6
Wstrzyknięcie kodu	0,8	2,1	1,7	8,8	1,1	0,8	5,8	0,9	1,6	2,0
Kradzież danych (ujawnienie poufnych informacji)	0,8	2,5	0,5	3,5	1,0	1,0	1,9	0,9	1,2	1,0
Rogueware/ ransomware/ scareware	7,0	9,7	8,4	17,5	7,1	8,5	12,9	6,6	6,8	12,6
Exploit drive-by-download	2,9	5,9	3,1	7,0	2,9	4,4	5,2	3,1	3,9	3,3
Inne	12,0	13,1	11,7	3,5	13,7	8,7	7,1	13,5	11,8	9,0

Źródło: opracowanie własne na podstawie badań.

Wyniki badań wykazały, że w gminach o liczbie mieszkańców powyżej 30 tys., szczególnie w miastach na prawach powiatu, częściej występowały przykłady większości rodzajów cyberataków. Gminy różniły się głównie pod

względem występowania wycieku danych i phishingu. W gminach z wyższymi bieżącymi dochodami budżetowymi na mieszkańca częściej mieliśmy do czynienia z cyberatakami typu phishing, spam, *rogueware/ransomware/scareware* oraz z użyciem botnetu.

Z odpowiedzi respondentów uzyskanych w toku badania wynika, że w ponad 3/4 urzędów opracowano i wdrożono politykę bezpieczeństwa informacji oraz co roku był przeprowadzany audyt wewnętrzny bezpieczeństwa informacji. Informacje te mogą świadczyć o odpowiedniej organizacji bezpieczeństwa informacji. Jednak część badanych gmin nie podjęła wystarczających działań, aby zapobiec incydentom związanym z bezpieczeństwem informacji. Tylko w połowie gmin uczestniczących w badaniu są przeprowadzane szkolenia urzędników w zakresie cyberbezpieczeństwa, w 9% badanych jst przeszkolono tylko kadrę kierowniczą. Niespełna 12% badanych ubezpieczyło się od ryzyka cyberataku. Wyniki te wydają się zaskakujące, biorąc pod uwagę fakt, że jednocześnie dla około 66% gmin uczestniczących w badaniu cyberprzestępczość stanowi średnie lub duże zagrożenie. Co prawda w latach 2017–2019 w większości badanych gmin (86,7%) nie wystąpiły incydenty związane z naruszeniem bezpieczeństwa informacji, ale ich ryzyko jest coraz większe. Te jst, w których takie incydenty zaistniały, nie zawsze zgłaszały je odpowiednim organom.

Uzyskane odpowiedzi wskazują, że jedną z przyczyn zaniedbań w obszarze cyberbezpieczeństwa może być brak świadomości zagrożeń związanych z coraz powszechniejszym funkcjonowaniem w cyberprzestrzeni. Niewywiązywanie się z wykonywania zadań z zakresu cyberbezpieczeństwa tłumaczy się brakiem zagrożeń, brakiem odpowiedniej kadry lub wystarczających zasobów finansowych. Zagrożenia takie jednak istnieją. Konieczne jest więc postulowanie upowszechnienia wiedzy w tej dziedzinie.

7

GOTOWOŚĆ SAMORZĄDU GMINNEGO DO FUNKCJONOWANIA W GOSPODARCE 4.0 W ŚWIETLE BADAŃ WŁASNYCH

7.1. Metodyka badań i charakterystyka gmin uczestniczących w badaniu

Na podstawie analizy literatury przedmiotu w przeprowadzonym badaniu sformułowano dwa pytania badawcze – czy typ gminy wpływa na jej przygotowanie do funkcjonowania w gospodarce cyfrowej, a także czy stopień przygotowania gmin do funkcjonowania w gospodarce cyfrowej jest zróżnicowany w poszczególnych województwach.

Badanie zostało przeprowadzone w pierwszym kwartale 2022 r. Do zebrania danych wykorzystano kwestionariusz ankiety w wersji elektronicznej, wypełniany przez respondentów samodzielnie po przesłaniu do nich prośby zawierającej adres dostępu do badania (Computer Assisted Web Interview – CAWI). Zastosowano metodę pełną badania i ankieta została rozesłana do urzędów wszystkich gmin w Polsce. Badaniem objęto 2477 gmin – 1513 gmin wiejskich, 662 gmin miejsko-wiejskich, 302 gminy miejskie oraz 66 miast na prawach powiatu. Ostatecznie otrzymano odpowiedzi od 1730 gmin (zwrotność ankiet wyniosła 70,0%).

W badaniu ankietowym odpowiedziało $N = 1730$ osób z gmin, głównie wiejskich (60,1%), a następnie miejsko-wiejskich (26,4%). Najmniejszą część stanowiły gminy miejskie (1,0%) i miasta na prawach powiatu (2,5%). Najwięcej gmin pochodziło z województwa mazowieckiego (12,9%), następnie wielkopolskiego (8,8%), lubelskiego (8,6%) i małopolskiego (7,9%). Pod względem liczby mieszkańców przeważały odpowiedzi z gmin do 10 tys. mieszkańców (65,0%). Drugą co do wielkości grupą były gminy z liczbą mieszkańców 10–20 tys. (22,2%). W badanej grupie przeważały gminy, w których bieżące dochody na mieszkańca wyniosły w 2021 r. ponad 5 tys. zł (41,8%), kolejną grupą były gminy z dochodami na osobę poniżej 3 tys. zł (32,0%) (tabela 32).

Tabela 32. Charakterystyka badanych gmin pod względem województwa, liczby mieszkańców i bieżących dochodów na mieszkańca

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi[a]	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Województwo			**Typ gminy**		
Dolnośląskie	113	6,5	gmina wiejska	1039	60,1
Kujawsko-pomorskie	102	5,8	gmina miejsko-wiejska	456	26,4
Lubelskie	150	8,6	gmina miejska	190	11,0
Lubuskie	57	3,3	miasto na prawach powiatu	45	2,5
Łódzkie	117	6,8	**Liczba mieszkańców**		
Małopolskie	136	7,9	do 10 000	1125	65,0
Mazowieckie	223	12,9	10 000–20 000	382	22,2
Opolskie	56	3,2	20 000–30 000	95	5,5
Podkarpackie	103	6,0	30 000–40 000	44	2,5
Podlaskie	90	5,2	40–000–50 000	26	1,5
Pomorskie	79	4,6	50 000–100 000	35	2,0
Śląskie	124	7,2	powyżej 100 000	23	1,3
Świętokrzyskie	80	4,6	**Wysokość bieżących dochodów budżetowych na mieszkańca (w zł)**		
Warmińsko-mazurskie	76	4,4	poniżej 3000	553	32,0
Wielkopolskie	152	8,8	3000–3500	119	6,9
Zachodniopomorskie	72	4,2	3500–4000	74	4,3
			4000–4500	92	5,3
			4500–5000	167	9,7
			powyżej 5000	725	41,8

[a] Informacja na temat struktury odnosi się do liczby gmin, które wypełniły ankietę.

Źródło: opracowanie własne na podstawie badań.

7.2. Wyniki ankiety i przeprowadzonych na jej podstawie analiz

Celem badania była ocena przygotowania gmin do funkcjonowania w gospodarce 4.0. W badaniu pytano respondentów zarówno o stosowanie w gminie różnego rodzaju rozwiązań, które są niezbędne do budowania gospodarki 4.0, jak i o zakres wykorzystywania przez urzędy gmin technologii informacyjno-komunikacyjnych (tabela 33). Zdecydowana większość badanych gmin (86,7%) nie

Tabela 33. Charakterystyka gmin pod względem odsetka lokali mieszkalnych z dostępem do internetu, posiadania nadajników 5G, rodzajów dostępu urzędu gminy do internetu oraz kanałów wykorzystywanych do komunikacji zewnętrznej

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Lokale mieszkalne na terenie gminy z dostępem do internetu			**Rodzaj dostępu urzędu gminy do internetu**		
poniżej 10%	21	1,2	stałe łącze w technologii DSL	1026	59,3
10–19,99%	15	0,9	inne szerokopasmowe łącze stałe	1103	63,8
20–29,99%	15	0,9	szerokopasmowe łącze mobilne (co najmniej 3G)	295	17,1
30–39,99%	22	1,3	wąskopasmowe łącza mobilne	45	2,6
40–49,99%	18	1,0	**Środki komunikacji wykorzystywane przez urząd gminy do komunikacji zewnętrznej**		
50–59,99%	18	1,0	Instagram	114	6,6
60–69,99%	27	1,6	Facebook	1244	71,9
70–79,99%	36	2,1	Youtube	485	28,0
80–89,99%	35	2,0	Twitter	49	2,8
90–99,99%	23	1,3	portal lokalnej gazety	313	18,1
100%	0	0,0	strona internetowa urzędu gminy w ramach biuletynu informacji publicznej	1658	95,8
urząd gminy nie ma takiej informacji	1500	86,7	aplikacja mobilna urzędu	407	23,5
Usytuowanie na terenie gminy nadajników telefonii 5G			chatbot	8	0,5
tak	163	9,5	wirtualny asystent	4	0,2
nie	395	22,8	e-mail	1618	93,5
urząd gminy nie ma takiej informacji	1172	67,7	kontakt korespondencyjny (przesłanie listu)	1506	87,1

Źródło: opracowanie własne na podstawie badań.

dysponowała wiedzą w zakresie odsetka lokali mieszkalnych na terenie gminy z dostępem do internetu. Pozostałe gminy szacowały, że około 70–90% lokali mieszkalnych ma dostęp do internetu. Wyniki te są zbieżne z ustaleniami poczynionymi przez GUS (2019, 2021), według którego w 2019 r. dostęp do internetu w domu miało 86,7% gospodarstw domowych, a w 2021 r. – 92,4%. W przy-

szłych analizach zebranego przez nas materiału warto zwrócić uwagę na to, czy odsetek ten jest zróżnicowany w zależności od typu gospodarstwa, stopnia urbanizacji, miejsca zamieszkania oraz województwa, co wynika z badania GUS.

Nadajniki 5G znajdowały się na terenie niemal co dziesiątej badanej gminy (9,5%). Blisko 68% gmin przyznało, że nie posiada informacji na temat występowania na terenie gminy takich nadajników. Jest to bardzo zaskakujące, ponieważ organ wykonawczy ustala lokalizację celu publicznego, jakim jest budowa stacji telefonii komórkowej. Inwestycja celu publicznego, a takim jest budowa masztu telefonii komórkowej (Frey, 2011), jest lokalizowana na podstawie planu miejscowego, a w przypadku jego braku – w drodze decyzji o ustaleniu lokalizacji inwestycji celu publicznego, którą na szczeblu gminy wydaje wójt (burmistrz, prezydent) (Ustawa, 2003).

„Zakres i sposób wykorzystania internetu w administracji publicznej oraz udostępnianie e-usług są uwarunkowane szybkością posiadanego łącza internetowego" (Ziemba i in., 2015, s. 174). Urzędy gmin miały zapewniony dostęp do internetu zazwyczaj przez stałe łącze w technologii DSL (59,3%) i szerokopasmowe stałe łącze (63,8%). Rzadziej internet dostarczany był przez szerokopasmowe łącze mobilne (17,1%) i wąskopasmowe łącza mobilne (2,6%). Zatem większość gmin nie powinna mieć problemów z poprawnym dostarczaniem e-usług, nawet takich, których świadczenie odbywa się za pomocą interakcji online. Wyniki te nie są zbieżne z ustaleniami poczynionymi przez GUS (2021), według którego w 2020 r. 99,8% gmin wykorzystywało technologię szerokopasmowego dostępu do internetu. Różnicę tę można tłumaczyć brakiem pełnej wiedzy na temat dostępu do internetu wśród niektórych osób odpowiadających na pytania w obu ankietach oraz różnym stopniem zwrotności ankiet. Ponadto GUS zgromadził dane za 2020 r., a nasze badanie odwołuje się do roku późniejszego, co może mieć znaczenie w odniesieniu do innych pytań, np. dotyczących przeprowadzonych szkoleń czy zakupu sprzętu. Należy przypuszczać, że w 2020 r. w budżetach zaplanowano wyższe wydatki na ten cel niż rok później ze względu na niepewną sytuację wywołaną pandemią COVID-19 oraz obostrzenia dotyczące gromadzenia się ludzi w zamkniętych pomieszczeniach.

Badane przez nas gminy wykorzystywały do komunikowania się z mieszkańcami i podmiotami gospodarczymi zarówno kanały komunikacji tradycyjnej, jak i kanały komunikacji elektronicznej. Niemal wszystkie gminy wykorzystywały w tym celu stronę internetową (95,8%) oraz pocztą elektroniczną (93,5%). Dane te potwierdzają obserwację Dylewskiego i Kępy (2009), że biuletyn informacji publicznej umieszczany na stronie internetowej urzędu w dalszym ciągu jest bardzo popularnym narzędziem komunikacji. Co ciekawe, te dwa kanały komunikacji były częściej stosowane niż tradycyjny kontakt korespondencyjny (87,1%). Dodatkowo z badań GUS (2021) wynika, że w 2020 r. 25,5% badanych

jednostek administracji publicznej deklarowało możliwość udziału obywateli w głosowaniach i konsultacjach społecznych online.

W badaniach przeprowadzonych przez zespół Ziemby (2015) w okresie grudzień 2013 – kwiecień 2014 r. około 34% jednostek administracji publicznej uznało, że wydatki na media społecznościowe (Facebook, Twitter, czaty, blogi) są zdecydowanie nieuzasadnione. Tymczasem z naszego badania wynika, że gminy wykorzystują wymienione kanały komunikacji (tabela 33): Facebook (71,9%), Youtube (28,0%), aplikację mobilną urzędu[31] (23,5%) oraz portal lokalnej gazety (18,1%). Obecność jst w mediach społecznościowych nie jest uregulowana w przepisach prawnych, dlatego fanpejdż gminy lub wójta (burmistrza, prezydenta) może być wykorzystywany w różnych celach. Media społecznościowe pełnią przede wszystkim funkcję informacyjną (Gawłowski i Miliszewski, 2019), która zwiększyła się w czasie pandemii COVID-19 (Kańduła i Przybylska, 2022b), i promocyjną. Może być też miejscem dyskusji i interakcji z mieszkańcami[32]. Gminny profil w tych mediach ułatwia codzienny kontakt z mieszkańcami, może być też wykorzystywany do zamieszczania ogłoszeń i edukowania mieszkańców (*Jak urzędy…*, 2022). Chatbot i wirtualny asystent był wykorzystywany sporadycznie przez niewielką część badanych gmin (odpowiednio 0,5% i 0,2%). Z chatbotem spotkali się już np. mieszkańcy Wrocławia. Działał on m.in. w serwisie poświęconym COVID-19 na www.wroclaw.pl oraz na Facebook Messengerze Urzędu Miejskiego (Dubec, 2020). Z pomocy wirtualnego asystenta do szybkiego zgłaszania usterek w infrastrukturze miejskiej korzysta np. Gdynia. Ten moduł w miejskiej aplikacji został nagrodzony w międzynarodowym konkursie GO SART Award (Mejna, 2020). Dane te świadczą o tym, że nowoczesne formy komunikacji są nadal stosunkowo rzadko wykorzystywane przez administrację gminną, co może dziwić, ponieważ ankietę rozesłano do gmin po trzeciej fali pandemii COVID-19. Niemniej pandemia była katalizatorem zmian w sposobie prowadzenia polityki komunikacyjnej w gminach.

Zwęglińska-Gałecka (2020) dowodzi, że różnorodne informacje dotyczące pandemii, w tym apele o przestrzeganie obostrzeń, były publikowane przez gminy głównie na stronie internetowej urzędu, co potwierdza stosunkowo niewielkie zainteresowanie gmin wykorzystywaniem innych kanałów komunikacji. Jednak z badań Kańduły i Przybylskiej (2022b) wynika, że w czasie pandemii upowszechniło się korzystanie przez włodarzy gmin z mediów społecznościowych – głównie w miastach na prawach powiatu.

---

[31] Aplikacja mobilna to publicznie dostępne oprogramowanie z interfejsem dotykowym zaprojektowane do wykorzystania w przenośnych urządzeniach elektronicznych, z wyłączeniem aplikacji przeznaczonych do użytku w przenośnych komputerach osobistych (Ustawa, 2019).

[32] Taką funkcję pełni np. Facebook Tadeusza Czajki, wójta gminy Tarnowa Podgórnego z województwa wielkopolskiego, który odbywa regularne wirtualne spotkania z mieszkańcami gminy pod hasłem #Porozmawiajmy o samorządzie (*Tadeusz Czajka…*, b.d.).

Wewnętrzna sieć internetowa (intranet) jest jednym z podstawowych sposobów udostępniania zasobów urzędu pracownikom oraz narzędziem służącym do komunikacji w obrębie jednostki. Według naszego badania ten sposób wykorzystywała niemal połowa gmin (47,9%). Dane zgromadzone przez GUS (GUS, 2021) pokazują, że w 2020 r. intranet miało 54,1% urzędów gmin. Intranet jest wykorzystywany do wymiany danych pomiędzy komórkami jednostki, pełni też funkcję systemu pracy grupowej, umożliwia korzystanie z biuletynu informacyjnego. W mniejszym stopniu ma zastosowanie w procesie obsługi klienta (GUS, 2021). Obsługę informatyczną urzędu zapewniała zazwyczaj komórka organizacyjna urzędu lub wydzieleni pracownicy (58,8%), rzadziej podmiot zewnętrzny (16,4%). W co czwartym urzędzie gminy obsługa informatyczna była częściowo zapewniana przez podmiot zewnętrzny, a częściowo przez pracownika urzędu. Wyniki te nie są zbieżne z ustaleniami poczynionymi przez GUS (2021). Prawdopodobne przyczyny tego stanu wskazano wcześniej.

W 2021 r. niemal 2/3 badanych gmin nie przeprowadziło żadnych szkoleń z zakresu technologii informacyjno-komunikacyjnych. Koresponduje to z wynikami badań zespołu pod kierunkiem Ziemby (2015), który ustalił, że wydatki na podniesienie kompetencji pracowników z zakresu ICT znajdują się dopiero na trzecim miejscu w rankingu potrzeb inwestycyjnych ICT jednostek administracji publicznej. Pozostałe urzędy gmin takie szkolenia organizowały zazwyczaj dla specjalistów ICT (29,3%), rzadziej dla wszystkich pracowników urzędu (16,9%). Z danych zgromadzonych przez GUS (GUS, 2021) wyłania się nieco bardziej optymistyczny obraz. W 2020 r. połowa zbadanych gmin (50,2%) organizowała szkolenia dla pracowników z zakresu ICT.

W 2021 r. 95,0% gmin poniosło wydatki na zakup sprzętu informacyjno-komunikacyjnego oraz oprogramowania na potrzeby urzędu gminy oraz jednostek organizacyjnych podległych urzędowi lub nadzorowanym przez urząd. Wyniki badań autorek niniejszej publikacji potwierdzają ustalenia powołanego wcześniej zespołu badaczy (Ziemba i in., 2015), którzy pokazali, że wydatki na sprzęt informatyczny są priorytetowym kierunkiem wydatków na projekty ICT w analizowanych jednostkach. Ponad połowa gmin ponosiła wydatki na zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych (57,3%). Ponadto gminy przeznaczały środki budżetowe na zakup sprzętu ICT dla szkół (40,1%) i zakup usług ICT dla urzędu (31,7%). Wydatki gmin w tym zakresie mieściły się zazwyczaj w przedziale 30–100 tys. zł (30,7%). W co czwartej gminie wydatki te wynosiły 10–30 tys. zł (26,5%), a 23,3% ankietowanych gmin wydawało na funkcjonowanie w gospodarce 4.0 100–500 tys. zł. Stosunkowo niewielkie kwoty przeznaczane na wymienione wydatki korespondują z wcześniejszymi ustaleniami dotyczącymi preferowanych kierunków wydatków (zakup sprzętu).

Z dotychczasowych badań wynika, że większość jednostek administracji publicznej nie ma wystarczających środków finansowych za zakup i wdrożenie nowych technologii (Ziemba i in., 2015), także związanych z zapewnieniem cyberbezpieczeństwa (Chodakowska i in., 2022a; Norris i in., 2021). Zaskakujące są więc odpowiedzi na pytanie dotyczące źródeł finansowania wydatków na ICT (tabela 34) – zwykle wskazywano dochody własne gminy (95,3%), rzadziej dotacje z budżetu państwa (31,7%) oraz dotacje z budżetu Unii Europejskiej (20,6%). Na małą i zdecydowanie małą rolę w finansowaniu transformacji cyfrowej jednostek administracji publicznej zwracali jednak uwagę także respondenci uczestniczący w badaniu pod kierunkiem Ziemby (2015). Praktyka zdecydowanie odbiega tu od deklaracji przedstawicieli rządu dotyczących dostępności środków na transformację cyfrową. Należy jednak podkreślić, że ten kierunek wydatkowania środków z funduszy UE nabrał znaczenia dopiero w 2020 r. i najprawdopodobniej nie ma jeszcze odzwierciedlenia w uzyskanych odpowiedziach.

Tabela 34. Wykorzystanie intranetu i obsługa informatyczna w urzędach gmin, szkolenia w zakresie ICT oraz wydatki gmin na funkcjonowanie w gospodarce 4.0

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Wykorzystanie intranetu w pracy urzędu gminy			**Wysokość wydatków na funkcjonowanie w gospodarce 4.0 (2021)**		
nie	902	52,1	0 zł	52	3,0
tak	828	47,9	0,01–10 000 zł	199	11,5
Obsługa informatyczna urzędu gminy			10 001–30 000 zł	458	26,5
komórka organizacyjna urzędu lub wydzieleni pracownicy	1018	58,8	30 001–100 000 zł	531	30,7
podmiot zewnętrzny	283	16,4	100 001–500 000 zł	403	23,3
część zadań wykonują pracownicy lub komórka organizacyjna a część podmiot zewnętrzny	429	24,8	500 001–1 000 000 zł	45	2,6
Szkolenia w zakresie ICT dla pracowników urzędu gminy (2021)			powyżej 500 000 zł	42	2,4
nie	1021	59,0	**Źródła finansowania wydatków na funkcjonowanie w gospodarce cyfrowej (2021)**		
tak, dla specjalistów ICT	507	29,3	dochody własne	1648	95,3
tak, dla wszystkich pracowników	292	16,9	dotacje z budżetu państwa	549	31,7

cd. tabeli 34

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
tak, dla kadry kierowniczej	78	4,5	dotacje z funduszy europejskich	356	20,6
Rodzaje wydatków gmin na funkcjonowanie w gospodarce cyfrowej (2021)			środki zwrotne (krajowe i zagraniczne)	19	1,1
zakup sprzętu informacyjno-komunikacyjnego oraz oprogramowania na potrzeby urzędu gminy/jednostek podległych urzędowi lub nadzorowanym przez urząd	1643	95,0	środki od sponsorów i darczyńców	26	1,5
zakup usług ICT dla urzędu	549	31,7			
zakup sprzętu ICT dla szkół	694	40,1			
szkolenia dla pracowników z zakresu usług cyfrowych	463	26,8			
szkolenia dla pracowników z zakresu cyberbezpieczeństwa	490	28,3			
zapewnienie cyberbezpieczeństwa samorządowych systemów informatycznych	992	57,3			

Źródło: opracowanie własne na podstawie badań.

Jak podkreśla Cellary (PAP, 2014), papier jest symbolem nieefektywności, tymczasem system elektronicznego zarządzania dokumentami był wykorzystywany jako podstawowy sposób obiegu dokumentów jedynie w 8,1% urzędów gmin, które odpowiedziały na ankietę, natomiast 2/3 gmin zadeklarowało, że tego systemu używa jako systemu pomocniczego. W ponad 32% badanych urzędów nie wdrożono elektronicznego systemu do zarządzania dokumentami (EZD). Wśród przyczyn braku tego systemu ankietowani najczęściej deklarowali, że ich urząd jest zbyt małą jednostką. W prawie 23% urzędów gmin nie dostrzegano potrzeby wdrożenia tego systemu, a co czwarta gmina zadeklarowała brak środków finansowych na ten cel. Warto dodać, że 38,4% urzędów gmin planowało wprowadzić EZD do końca 2022 r.

Politykę udostępniania otwartych danych publicznych (tzw. *open data*) opracowało jedynie 6% ankietowanych gmin. Ponad 40% ankietowanych gmin uznało, że urząd gminy jest zbyt mały, aby podjąć takie działania. Niemal co trzecia gmina nie widziała potrzeby opracowania takiej strategii. Podobny odsetek respondentów nie opracował tego dokumentu z uwagi na niewystarczające środki finansowe. Dane z rejestrów publicznych lub innych zasobów danych gromadzonych w urzędzie do ponownego wykorzystania udostępniało 41,6%. Gminy, które nie udostępniały tych danych, wskazywały jako przyczyny takiego stanu rzeczy brak zapotrzebowania interesantów, zbyt małą wielkość urzędu gminy, brak potrzeb w tym zakresie oraz niewystarczające środki finansowe (tabela 35). Takie tłumaczenie nie napawa optymizmem, ponieważ świadczy o tym, że różna jest jakość usług publicznych w zależności od liczby mieszkańców gminy. Może to być też argument za zmniejszeniem fragmentaryzacji gmin, czyli ograniczeniem ich liczby w przyszłości lub narzuceniem obowiązkowej współpracy w niektórych dziedzinach w celu zmniejszenia nakładów publicznych i wzrostu ich efektywności.

Tabela 35. Wykorzystanie w urzędach gmin systemu elektronicznego zarządzania dokumentami, otwartych danych oraz udostępnianie danych online

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Wykorzystanie systemu elektronicznego zarządzania dokumentami w urzędzie gminy			**Przyczyny braku strategii udostępniania otwartych danych publicznych**		
nie	555	32,1	nie ma takiej potrzeby	458	28,1
tak, jest to podstawowy sposób obiegu dokumentów	140	8,1	jesteśmy zbyt małym urzędem gminy	681	41,9
tak, jest to pomocniczy sposób obiegu dokumentów	1035	59,8	brak środków finansowych	456	28,0
Przyczyny braku elektronicznego zarządzania dokumentami w urzędzie			brak osób z odpowiednimi kwalifikacjami	237	14,6
nie ma takiej potrzeby	127	22,9	nasi interesariusze nie zgłaszają takiego zapotrzebowania	627	38,5
jesteśmy zbyt małym urzędem gminy	216	38,9	planujemy opracować do końca 2022 r.	227	14,0
brak środków finansowych	139	25,0	**Udostępnianie online danych z rejestrów publicznych do ponownego wykorzystania**		
brak osób z odpowiednimi kwalifikacjami	49	8,8	nie	1011	58,4

cd. tabeli 35

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
obawy o cyberbezpieczeństwo	24	4,3	tak	719	41,6
planujemy wdrożyć do końca 2022 r.	213	38,4	**Przyczyny braku udostępniania online danych z rejestrów publicznych**		
inne	59	10,6	nie ma takiej potrzeby	372	36,8
Czy urząd gminy opracował strategię udostępniania otwartych danych publicznych?			jesteśmy zbyt małym urzędem gminy	345	34,1
nie	1627	94.0	brak środków finansowych	215	21,3
tak	103	6,0	brak osób z odpowiednimi kwalifikacjami	106	10,5
			nasi interesariusze nie zgłaszają takiego zapotrzebowania	427	42,2
			planujemy udostępniać do końca 2022 r.	131	13,0
			inne	19	1,9

Źródło: opracowanie własne na podstawie badań.

Źródłem dostępu do danych z rejestrów publicznych lub innych zasobów danych gromadzonych w urzędzie gminy była najczęściej strona internetowa urzędu (91,0%), rzadziej specjalny gminny portal z danymi publicznymi (17,1%).

Narzędzia *business intelligence,* umożliwiające integrację danych z różnych systemów, w tym danych gromadzonych przez gminne jednostki organizacyjne, stosowało jedynie 10,8% gmin. Wśród głównych powodów niestosowania tego narzędzia był brak potrzeby w tym zakresie, mała wielkość urzędu gminy, a także brak środków finansowych. Stronę internetową wykonaną zgodnie z kryteriami WCAG 2.0 na poziomie AA (tzn. czy dostępną dla użytkowników niezależnie od ich niepełnosprawności, wieku, używanego sprzętu i oprogramowania) posiadało 86,2% gmin, a pozostałe gminy zazwyczaj pracowały nad dostosowaniem strony do tych wymogów. Stronę internetową przystosowaną do obsługi przez urządzenia mobilne posiadało 88,0% badanych gmin. Większość pozostałych gmin planowała udostępnić taką możliwość do końca 2022 r. Aplikacje do pobrania na urządzenia mobilne udostępniało 30,9% gmin. Urzędnicy pozostałych gmin zazwyczaj nie odczuwali takiej potrzeby lub nie mieli środków finansowych na takie działania (tabela 36). W świetle wyzwań stojących przez gospodarką i społeczeństwem w warunkach gospodarki 4.0 dane te nie

napawają optymizmem Świadczą raczej o tym, że urzędy gmin są co najwyżej w połowie drogi do nowej gospodarki.

Tabela 36. Źródła dostępu do danych z rejestrów publicznych, stosowanie narzędzi *business intelligence* oraz posiadana strona internetowa w urzędach gmin

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Źródło dostępu do danych z rejestrów publicznych			**Strona internetowa przystosowana do obsługi przez urządzenia mobilne**		
strona internetowa urzędu gminy/BIP[a]	654	91,0	nie	208	12,0
gminny portal z danymi publicznymi	123	17,1	tak	1522	88,0
strona dane.gov.pl	53	7,4	**Przyczyny braku dostosowania strony internetowej do obsługi przez urządzenia mobilne**		
inne	57	7,9	nie ma takiej potrzeby	30	14,4
Zastosowanie narzędzi *business intelligence*			brak środków finansowych	61	29,3
nie	1544	89,2	brak osób z odpowiednimi kwalifikacjami	15	7,2
tak	186	10,8	obawy przed cyberprzestępcami	13	6,3
Przyczyny braku zastosowania narzędzi *business intelligence*			nasi interesariusze nie zgłaszają takiego zapotrzebowania	55	26,4
nie ma takiej potrzeby	725	47,0	planujemy poprawić dostępność cyfrową strony internetowej urzędu do końca 2022 r.	106	51,0
jesteśmy małą gminą, wszystko można załatwić w najbliższym sąsiedztwie	617	40,0	inne	8	3,8
brak środków finansowych	478	31,0	**Urząd gminy udostępnia aplikacje urządzenia mobilne**		
brak osób z odpowiednimi kwalifikacjami	177	11,5	nie	1196	69,1
nasi interesariusze nie zgłaszają takiego zapotrzebowania	437	28,3	tak	534	30,9

cd. tabeli 36

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
planujemy zintegrować dane do końca 2022 r.	111	7,2	**Przyczyny braku udostępniania aplikacji na urządzenia mobilne**		
inne	27	1,7	nie ma takiej potrzeby	619	51,8
Strona internetowa wykonana zgodnie z kryteriami WCAG 2.0 na poziomie AA			jesteśmy małą gminą, wszystkie usługi można załatwić w urzędzie	421	35,2
nie	239	13,8	brak środków finansowych	338	28,3
tak	1491	86,2	brak osób z odpowiednimi kwalifikacjami	70	5,9
Przyczyny braku strony internetowej wykonanej zgodnie z kryteriami WCAG 2.0 na poziomie AA			obawy przed cyberprzestępczością	65	5,4
brak środków finansowych	56	23,4	nasi interesariusze nie zgłaszają takiego zapotrzebowania	397	33,2
brak osób z odpowiednimi kwalifikacjami	13	5,4	planujemy udostępnić aplikację do końca 2022 r.	99	8,3
planujemy dostosować stronę do wymogów do końca 2022 r.	190	79,5	inne	116	9,7
nie wiedzieliśmy o takim wymogu	0	0,0			
inne	23	9,6			

[a]BIP – Biuletyn Informacji Publicznej.

Źródło: opracowanie własne na podstawie badań.

Służbowe urządzenia mobilne (laptopy i telefony komórkowe) nie były rozpowszechnionym narzędziem pracy w badanych urzędach gmin. W większości gmin (63,9%) mniej niż 5% pracowników było wyposażonych w takie urządzenia. Należy przypuszczać, że wynika to z ograniczonych zasobów finansowych oraz wątpliwości dotyczących czasu pracy. Czy pracownik wyposażony w takie urządzenie powinien – poza sytuacjami kryzysowymi – być dostępny przez 24 godziny?

Usługi elektroniczne świadczyło 78,0% badanych gmin. Były to zazwyczaj usługi elektroniczne w zakresie spraw obywatelskich (67,2%), zamówień publicznych

(60,4%), podatków i opłat lokalnych (54,0%), rejestracji działalności gospodarczej (49,0%) oraz ochrony środowiska i gospodarki odpadami (47,4%). Przesłankami do świadczenia usług elektronicznych w gminach było zazwyczaj skrócenie czasu świadczenia usługi (59,2%), wzrost satysfakcji interesantów (48,9%) i uproszczenie procesu ich obsługi (47,6%), a także postrzeganie gminy jako nowoczesnej (40,0%). W gminach, które nie świadczą usług elektronicznych, panuje przekonanie, że nie ma potrzeby wdrażania rozwiązań w tym zakresie. Co czwarta gmina zadeklarowała, że interesariusze nie zgłaszają potrzeb w zakresie rozwoju tej formy świadczenia usług. W niemal połowie tej grupy gmin wyrażono pogląd, że ze względu na małą wielkość gminy wszystkie usługi można załatwić w urzędzie stacjonarnie. Nieco ponad 25% ankietowanych gmin jako barierę wdrożenia i świadczenia usług elektronicznych wskazało brak środków finansowych (tabela 37).

Tabela 37. Usługi elektroniczne w badanych urzędach gmin

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Pracownicy urzędu gminy wyposażeni w służbowe urządzenia mobilne z dostępem do internetu			**Urząd gminy świadczy usługi elektronicznie z następujących dziedzin:**		
mniej niż 5%	1105	63,9	sprawy obywatelskie	1162	67,2
5–10%	260	15,0	zamówienia publiczne	1045	60,4
10,1–15%	110	6,4	rejestracja działalności gospodarczej	848	49,0
15,1–20%	74	4,3	ochrona środowiska i gospodarka odpadami	823	47,6
20,1–25%	44	2,5	gospodarka przestrzenna	786	45,4
25,1–30%	39	2,3	gospodarka komunalna	589	34,0
powyżej 30%	98	5,7	edukacja	319	18,4
Czy urząd gminy świadczy usługi elektroniczne?			turystyka	197	11,4
nie	381	22,0	kultura	227	13,1
tak	1349	78,0	transport	207	12,0
Przyczyny braku usług elektronicznych			podatki i opłaty lokalne	935	54,0
nie ma takiej potrzeby	109	28,6	praca	181	10,5
jesteśmy małą gminą, wszystkie usługi można załatwić w urzędzie	171	44,9	zdrowie	127	7,3

cd. tabeli 37

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
brak środków finansowych	97	25,5	inne	27	1,6
brak osób z odpowiednimi kwalifikacjami	26	6,8	**Przesłanki świadczenia usług elektronicznych**		
obawy przed cyberprzestępczością	19	5,0	skrócenie czasu świadczenia usługi	1024	59,2
nasi interesariusze nie zgłaszają takiego zapotrzebowania	89	23,4	wyeliminowanie dublowania danych	222	12,8
planujemy świadczyć usługi elektroniczne do końca 2022 r.	76	19,9	wzrost efektywności czasu pracy	608	35,1
inne	18	4,7	postrzeganie gminy jako nowoczesnej	692	40,0
			uproszczenie procesu obsługi interesantów	823	47,6
			obniżenie kosztów obsługi interesantów	472	27,3
			wzrost satysfakcji interesantów	846	48,9
			informacja zwrotna od interesantów dotycząca ich potrzeb, jakości obsługi, propozycji usprawnień	116	6,7
			inne	43	2,5

Źródło: opracowanie własne na podstawie badań.

Jedną z cech gospodarki 4.0 jest powszechne wykorzystywanie chmury obliczeniowej. Chmura ta jest nowym sposobem przetwarzania danych, charakteryzującym się brakiem wymogu dysponowania niezbędnymi zasobami (sprzętem, oprogramowaniem) do wykonywania zadań informatycznych. Niekiedy określa się ją też jako „usługi obliczeniowe proponowane przez zewnętrzne podmioty i dostępne na życzenie w dowolnym momencie, skalujące się dynamicznie w skutek zmieniającego się zapotrzebowania" (Hauke, 2018, s. 81). Gminy mogłyby utworzyć/zakupić prywatną chmurę obliczeniową, ale bardziej efektywnym rozwiązaniem jest korzystanie z chmury wspólnej (publicznej). Z tej drugiej odmiany korzystają podmioty, które realizują wspólną misję (Hauke, 2018), np. udzielają zamówień publicznych.

Z badania autorek niniejszej monografii wynika, że ten sposób analizowania danych nie jest jeszcze popularny w urzędach gmin, które odpowiedziały na ankietę. W badanej grupie było tylko 10,8% gmin korzystających z chmury obliczeniowej. Pozostałe gminy nie odczuwały potrzeby korzystania z tego rozwiązania lub nie miały środków finansowych na takie inwestycje. Plany wdrożenia chmury obliczeniowej do końca 2022 r. zgłosiło jedynie 3,8% gmin, które nie korzystały dotąd z tego rozwiązania. Przesłankami do posiadania chmury obliczeniowej w gminach było podniesienie bezpieczeństwa danych i procesu świadczenia usług (55,6%), obniżenie kosztów utrzymania systemów informatycznych (41,7%) i brak konieczności utrzymywania gminnej infrastruktury informatycznej (43,3%). Pojazdy autonomiczne stosowano w 0,4% gminach, a drony w 12% gmin. Gminy stosowały drony zazwyczaj w celu kontroli stanu powietrza (47,1%), inwentaryzacji dzikich wysypisk śmieci (14,9%) oraz terenów zielonych (11,5%) (tabela 38).

Tabela 38. Chmura obliczeniowa i pojazdy autonomiczne w badanych urzędach gmin

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Wykorzystanie chmury obliczeniowej w pracy urzędu			**Czy w gminie testowano używanie pojazdów autonomicznych?**		
nie	1543	89,2	nie	1723	99,6
tak	187	10,8	tak	7	0,4
Przyczyny niekorzystania z chmury obliczeniowej			**Zastosowanie dronów**		
nie ma takiej potrzeby	1084	70,3	nie	1522	88,0
nie znamy tego rozwiązania	147	9,5	tak	208	12,0
brak środków finansowych	383	24,8	**Obszary zastosowania dronów**		
brak osób z odpowiednimi kwalifikacjami	108	7,0	inwentaryzacja terenów zielonych	24	11,5
obawy przed cyberprzestępczością	258	16,7	tworzenie bazy modeli 3d budynków na potrzeby gminnego geoportalu	1	0,5
planujemy przenieść nasze dane do chmury obliczeniowej do końca 2022 r.	59	3,8	monitoring nośników reklamy w przestrzeni publicznej	2	1,0
inne	34	2,2	monitoring stanu nawierzchni dróg, oznakowania poziome i pionowe oraz kontroli zajęcia pasa drogowego	15	7,2

cd. tabeli 38

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Przesłanki korzystania z chmury obliczeniowej			kontrola stanu powietrza	98	47,1
podniesienie bezpieczeństwa danych i procesu świadczenia usług	104	55,6	inwentaryzacja dzikich wysypisk śmieci	31	14,9
obniżenie kosztów utrzymania systemów informatycznych	78	41,7	monitoring hałd pokopalnianych lub wysypisk śmieci	10	4,8
zaufanie do rozwiązań chmurowych	37	19,8	ewidencja zbiorników bezodpływowych i przydomowych oczyszczalni ścieków	4	1,9
brak konieczności utrzymywania gminnej infrastruktury informatycznej	81	43,3	wykrywanie nielegalnego zrzutu ścieków	10	4,8
dostęp do najnowszych technologii	70	37,4	monitoring wałów przeciwpowodziowych, sieci drenarskich i terenów zalewowych	12	5,8
inne	21	11,2	inne	95	45,7

Źródło: opracowanie własne na podstawie badań.

Niemal połowa badanych urzędów gmin (48,4%) nie wykorzystywała w swojej działalności żadnych rozwiązań internetu rzeczy (IoT). Tak wysoki odsetek negatywnych odpowiedzi przeczy nieco doniesieniom medialnym, w których jest opisywane zastosowanie zaawansowanych usług IoT m.in. w inżynierii ruchu, gospodarce odpadowej, zarządzaniu sieciami wodociągowymi i monitoringu ulicznym. Tego typu rozwiązania są stosowane m.in. Mysłowicach, Bydgoszczy, Chorzowie (Gadomski, 2018). W urzędach, w których rozwiązania tego typu zostały wdrożone, najczęściej znajdowały one zastosowanie w: monitoringu zanieczyszczenia powietrza poprzez czujniki (28,0%) oraz automatycznych odczytach liczników wody (17,3%). W 15,2% urzędów gmin stosowano bezprzewodowe drukarki, a w 11,8% systemy inteligentnego oświetlenia.

Sztuczna inteligencja była wykorzystywana w działalności urzędów gmin sporadycznie. 94,3% gmin nie stosowało żadnych rozwiązań w tym zakresie. Gminy, które stosowały sztuczną inteligencję, najczęściej używały jej do ostrzegania o klęskach żywiołowych (2,0%) oraz w celu weryfikacji deklaracji na odbiór odpadów (1,3%) i przewidywania awarii sieci wodociągowej

(1,3%) (tabela 39). Ciekawe rozwiązanie zastosowano w Urzędzie Miasta w Gdyni, w którym „zatrudniono" voicebota. Jest to asystent głosowy „oparty na sztucznej inteligencji, algorytmach uczenia głębokiego, uczenia maszynowego i technologii rozpoznawania mowy" (*Sztuczna inteligencja*, b.d.). Urządzenie to „umożliwia rezerwację wizyty w sprawach takich jak: rejestracja pojazdów, prawo jazdy, meldunek, numer PESEL. Mieszkaniec dzwoniący na infolinię zamiast oczekiwać na połączenie z konsultantem, jest natychmiastowo połączony z asystentem głosowym. Po poinformowaniu go, jaką sprawę chce załatwić, system przeanalizuje zapytanie i dopasuje do odpowiedzi, które zawarte są w bazie wiedzy, po czym poinformuje o efekcie interesanta. Zaproponuje konkretną datę i miejsce wizyty, po czym zapyta rozmówcę czy termin ten może być zaakceptowany przez niego. W przypadku odpowiedzi negatywnej, voicebot postara się dopasować inną datę, a na koniec rozmowy potwierdzi rezerwację". Praca tego urządzenia umożliwiła skrócenie średniego czasu rozmowy z 4 minut do 1,5 minuty (*Sztuczna inteligencja*, b.d.).

Tabela 39. Zastosowanie rozwiązań z zakresu internetu i sztucznej inteligencji w urzędach gmin

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
Rodzaje zastosowanych rozwiązań z zakresu internetu rzeczy			**Obszary zastosowania sztucznej inteligencji**		
automatyczny odczyt liczników wody	300	17,3	weryfikacja deklaracji na odbiór odpadów	22	1,3
automatyczny odczytu zużycia ciepła	59	3,4	weryfikacja deklaracji na podatki lokalne	9	0,5
monitoring zanieczyszczenia powietrza	485	28,0	sterowanie ruchem w mieście	16	0,9
monitoring zagrożeń typu pożar, zalanie, powódź, zamieszki publiczne	102	5,9	przewidywanie awarii sieci wodociągowej	22	1,3
pojemniki na odpady sygnalizujące ich zapełnienie	11	0,6	ostrzeganie o klęskach żywiołowych	34	2,0
ewidencja liczby wolnych/zajętych miejsc na parkingu /w strefie płatnego parkowania	19	1,1	kontakt z interesariuszami	5	0,3

cd. tabeli 39

Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi	Wyszczególnienie	Liczba odpowiedzi	Odsetek odpowiedzi
monitoring natężenia ruchu i dostosowywanie sygnalizacji świetlnej	23	1,3	analiza danych pozyskanych przez drony	4	0,2
inteligentne oświetlenie gminy	205	11,8	nie wykorzystujemy rozwiązań sztucznej inteligencji	1632	94,3
automatyczne podlewanie terenów zielonych	48	2,8	inne	10	0,6
inteligentne systemy współdzielenia rowerów, hulajnóg	38	2,2			
bezprzewodowe drukarki w urzędzie	263	15,2			
możliwy zakup biletów komunikacji miejskiej przez aplikację	41	2,4			
usługi teleopiekuńcze	43	2,5			
inteligentne rozwiązania w budynku urzędu	33	1,9			
nie wykorzystujemy żadnych rozwiązań internetu rzeczy	837	48,4			
inne	17	1,0			

Źródło: opracowanie własne na podstawie badań.

Analizując zróżnicowanie przygotowania gmin do funkcjonowania w gospodarce 4.0, w pierwszej kolejności sprawdzono, czy rodzaj gminy jest czynnikiem różnicującym stopień tego przygotowania. Z przeprowadzonych badań wynika, że nadajniki telefonii 5G występowały zdecydowanie częściej w miastach na prawach powiatu i gminach miejskich niż w gminach miejsko-wiejskich i wiejskich. Również gminy miejskie i miasta na prawach powiatu częściej dysponowały intranetem służącym do komunikacji wewnątrz urzędu oraz do przekazywania danych. W gminach tych w 2021 r. częściej przeprowadzano szkolenia w zakresie technologii informacyjno-komunikacyjnych. W gminach wiejskich obsługę informatyczną urzędu gminy zapewniał za-

zwyczaj podmiot zewnętrzny, a w gminach miejskich i miastach na prawach powiatu zapewniali ją pracownicy lub komórka organizacyjna urzędu (rysunek 23).

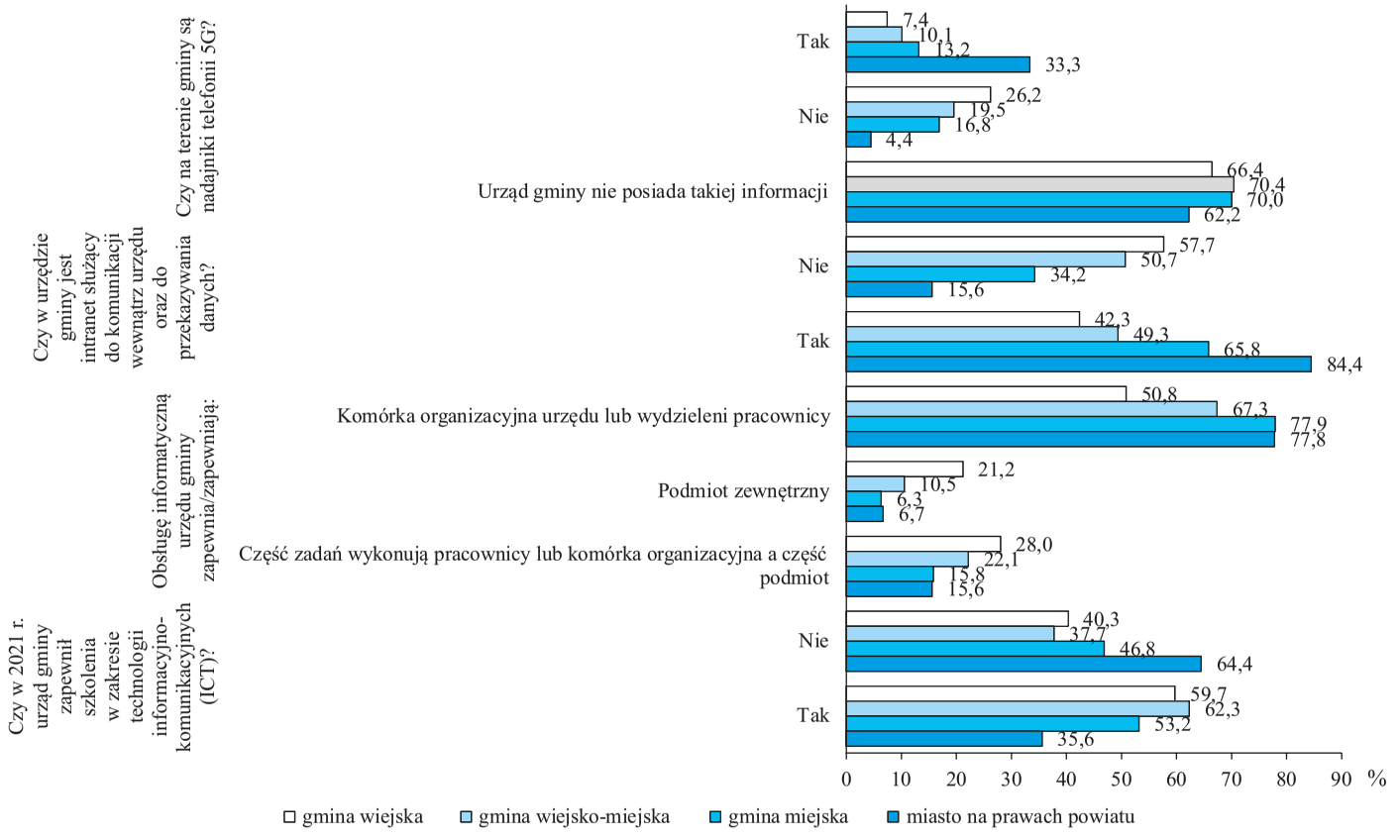
Dalsze badania wykazały, że miasta na prawach powiatu ponosiły największe wydatki na funkcjonowanie w gospodarce 4.0. W gminach miejskich i miastach na prawach powiatu najczęściej wykorzystywano system elektronicznego zarządzania dokumentami jako pomocniczy lub podstawowy sposób obiegu dokumentów. Miasta na prawach powiatu i gminy miejskie najczęściej udostępniały online otwarte dane publicznie oraz dane z rejestrów publicznych lub innych zasobów danych gromadzonych w urzędzie do ponownego wykorzystania (rysunek 24).

Kolejna seria analiz wykazała, że typ gminy wpływał na stopień wykorzystania rozwiązań typu *business intelligence*, posiadania strony internetowej wykonanej zgodnie ze standardem WCAG 2.0 na poziomie AA oraz przystosowania jej do obsługi przez urządzenia mobilne. Narzędzia *business intelligence* stosowały głównie miasta na prawach powiatu. Strony internetowe wykonane zgodnie z WCAG 2.0 na poziomie AA posiadały głównie gminy miejskie i miejsko-wiejskie, a strony dostosowane do urządzeń mobilnych gminy miejskie i miasta na prawach powiatu. Miasta na prawach powiatu oraz gminy miejskie zdecydowanie częściej udostępniały również do pobrania aplikacje na urządzenia mobilne oraz miały większy odsetek pracowników urzędu gminy wyposażonych w służbowe urządzenia mobilne z dostępem do internetu w celu obsługi gminnych aplikacji elektronicznych (rysunek 25).

Badania wykazały również, że gminy miejskie i miasta na prawach powiatu częściej świadczyły usługi elektroniczne i częściej korzystały z chmury obliczeniowej. Miasta na prawach powiatu jako jedne z nielicznych używały pojazdów autonomicznych (z przekazów medialnych wynika, że pilotaż w tym zakresie przeprowadzono tylko w Gdańsku) (*Rewolucja*, 2021) oraz zdecydowanie najczęściej używały dronów (rysunek 26).

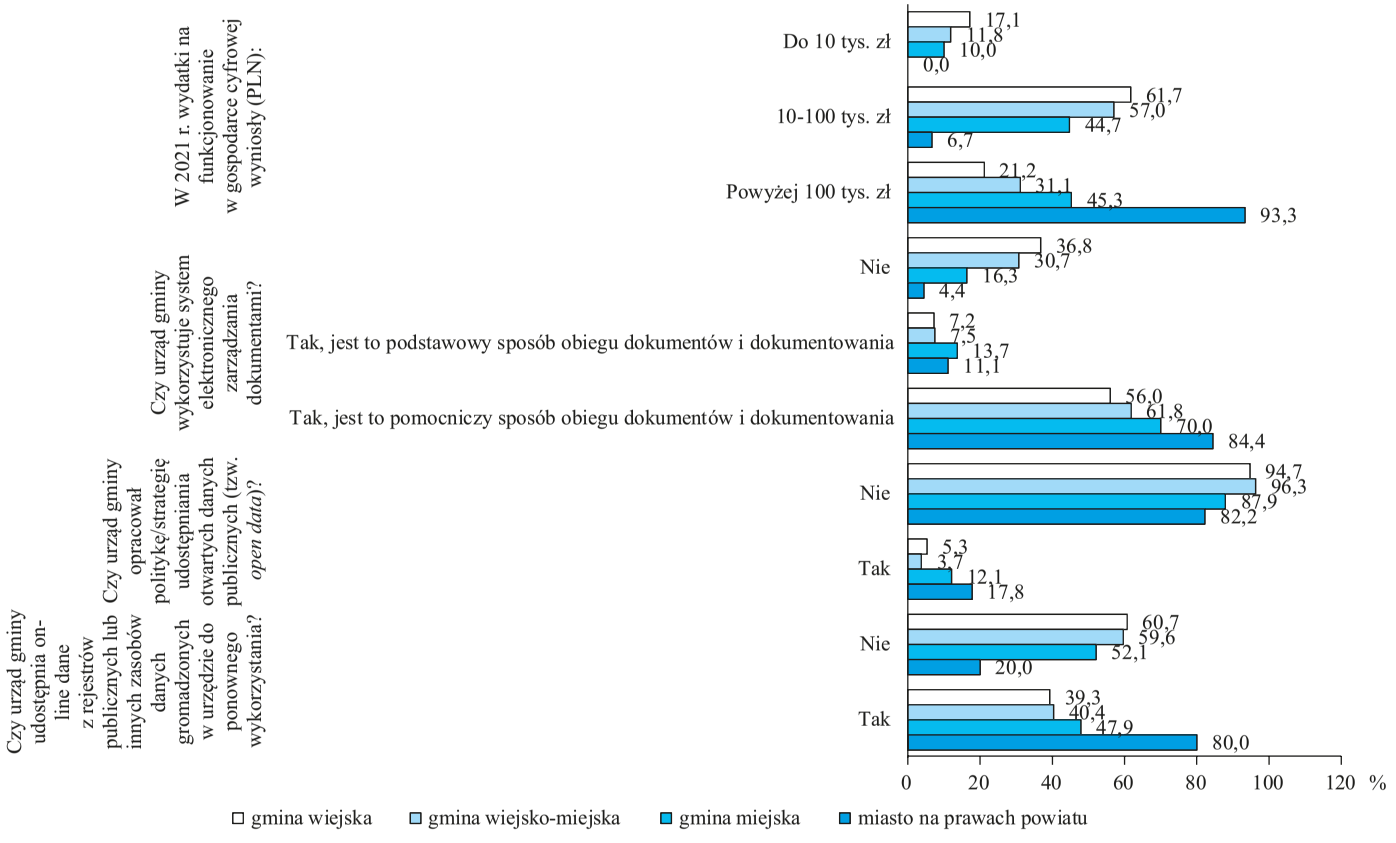
Drugim aspektem branym pod uwagę podczas badań nad przygotowaniem gmin do funkcjonowania w gospodarce 4.0 było zróżnicowanie terytorialne. Sprawdzono, czy występował związek pomiędzy stopniem przygotowania gmin do funkcjonowania w gospodarce 4.0 a województwem. Rozkład wyników przedstawiono w tabelach 40 i 41.

Na podstawie danych w tabelach można zauważyć, że najwięcej gmin dobrze przygotowanych do funkcjonowania w gospodarce 4.0 było w województwie śląskim, dolnośląskim, opolskim i warmińsko-mazurskim. Różnice między województwami nie były jednak tak zauważalne, jak wpływ typu gminy na przygotowanie do funkcjonowania w gospodarce cyfrowej.



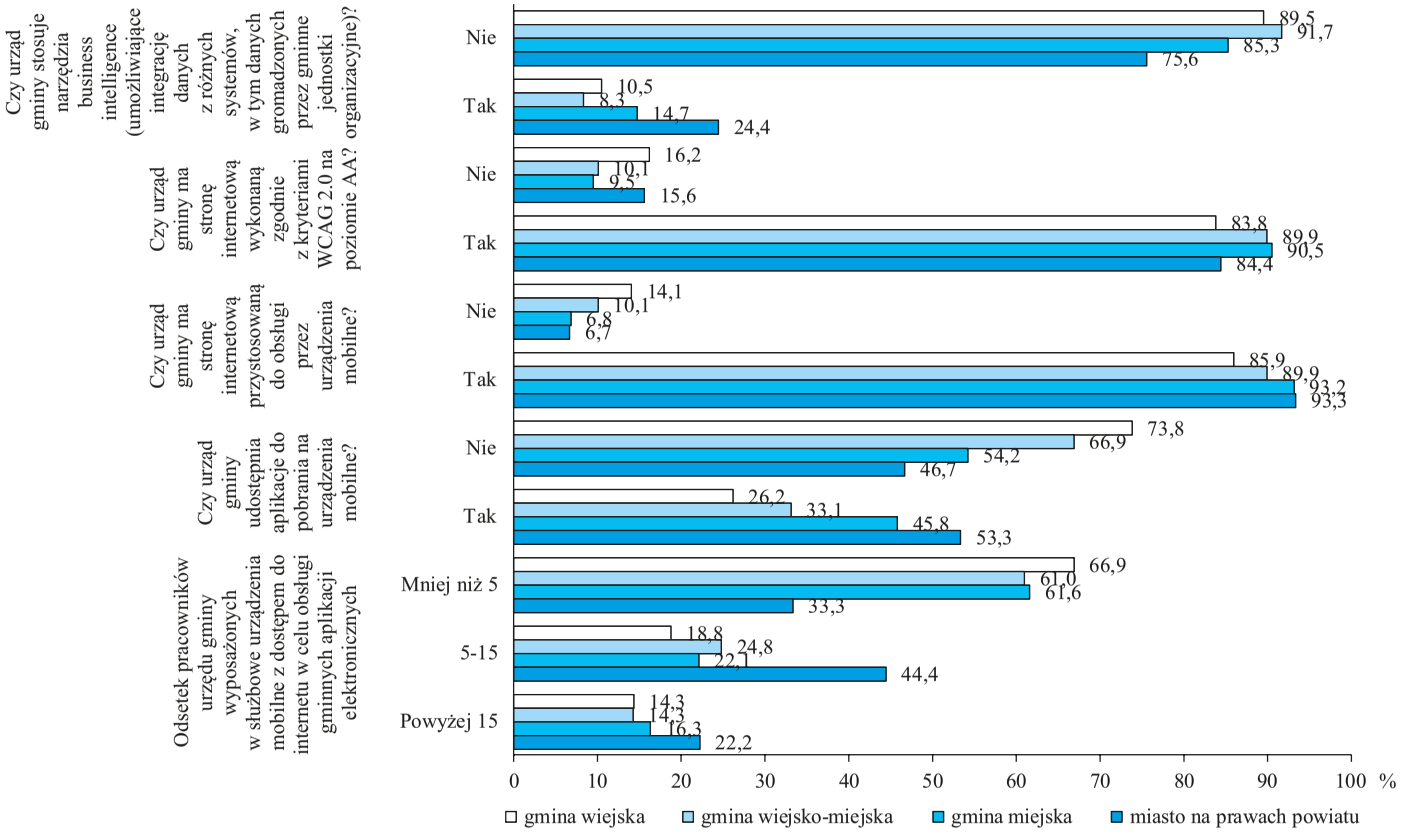
Rysunek 23. Związek typu gminy z posiadaniem nadajników 5G, intranetu, modelem obsługi informatycznej i zapewnianiem szkoleń z zakresu ICT

Źródło: opracowanie własne na podstawie badań.



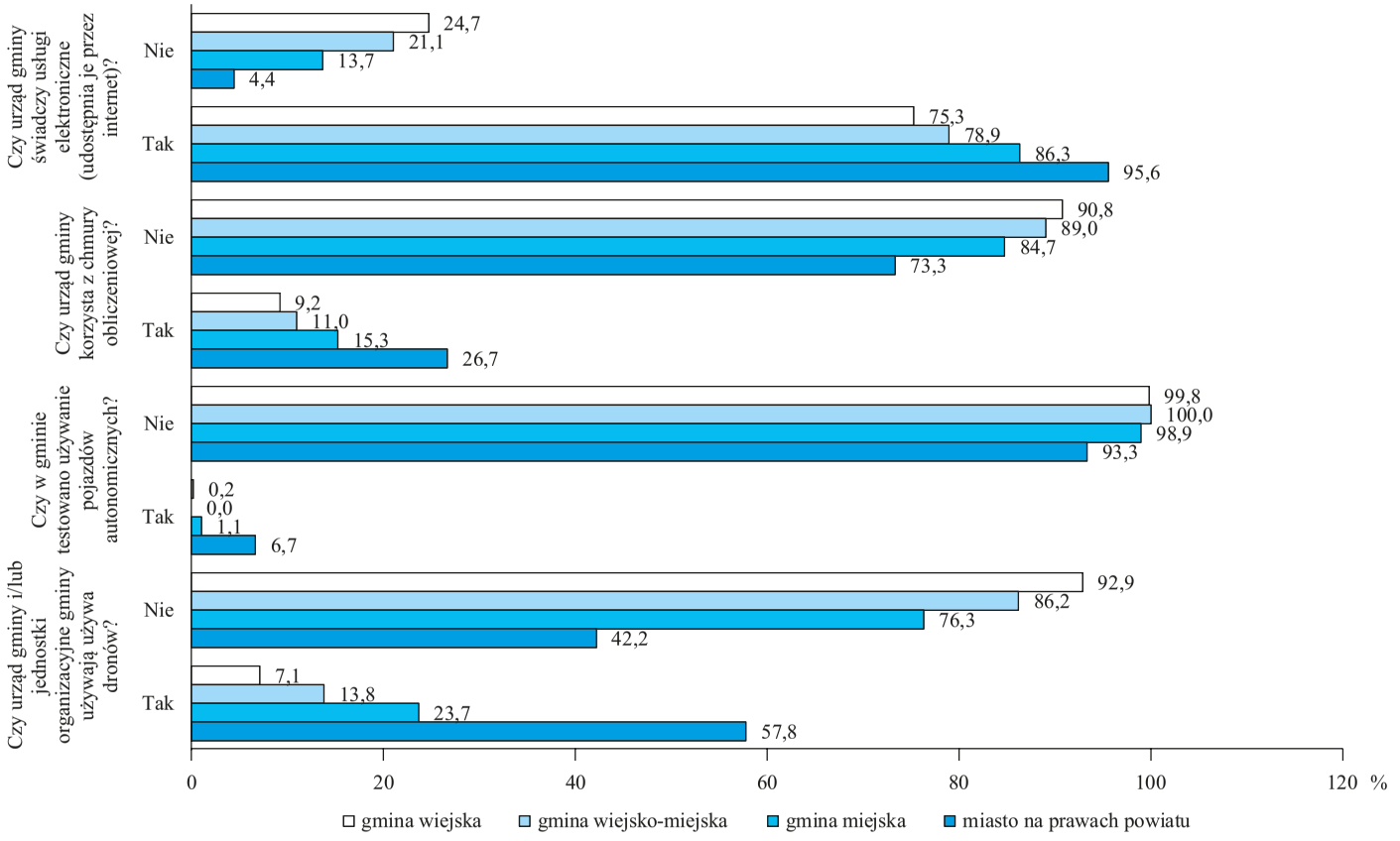
Rysunek 24. Związek typu gminy z wysokością wydatków na funkcjonowanie w gospodarce 4.0, korzystaniem z elektronicznego zarządzania dokumentami oraz udostępnianiem online otwartych danych publicznych i innych zbiorów danych

Źródło: opracowanie własne na podstawie badań.



Rysunek 25. Związek typu gminy ze stosowaniem narzędzi *business intelligence*, posiadaniem strony internetowej w odpowiednim formacie oraz udostępnianiem aplikacji mobilnych

Źródło: opracowanie własne na podstawie badań.



Rysunek 26. Związek typu gminy ze świadczeniem usług elektronicznych, korzystaniem z chmury obliczeniowej, z pojazdów autonomicznych i z dronów

Źródło: opracowanie własne na podstawie badań.

Tabela 40. Rozkład odpowiedzi na pytania o przygotowanie gmin do funkcjonowania w gospodarce 4.0 według województw (w %) – część I

Wyszczególnienie		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Nadajniki 5G	tak	7,1	7,8	13,3	17,5	6,8	8,1	11,7	5,4	2,9	6,7	7,6	19,4	8,8	2,6	9,2	9,7
	nie	25,7	21,6	32,0	29,8	22,2	16,9	21,5	21,4	34.0	32,2	24,1	12,9	22,5	19,7	18,4	13,9
	brak informacji	67,3	70,6	54,7	52,6	70,9	75,0	66,8	73,2	63,1	61,1	68,4	67,7	68,8	77,6	72,4	76,4
Intranet	nie	46,9	67,6	48,0	61,4	48,7	45,6	58,7	55,4	57,3	62,2	57,0	39,5	47,5	38,2	54,6	45,8
	tak	53,1	32,4	52,0	38,6	51,3	54,4	41,3	44,6	42,7	37,8	43,0	60,5	52,5	61,8	45,4	54,2
Obsługa informatyczna	zapewniana wewnętrznie	58,4	56,9	57,3	52,6	53,0	72,1	48,4	64,3	62,1	35,6	67,1	65,3	72,5	82,9	52,6	59,7
	podmiot zewnętrzny	26,5	3,9	14,7	31,6	12,8	11,0	22,0	12,5	3,9	24,4	20,3	13,7	6,3	6,6	27,0	18,1
	system mieszany	15,0	39,2	28,0	15,8	34,2	16,9	29,6	23,2	3 4.0	40,0	12,7	21,0	21,3	10,5	20,4	22,2
Szkolenia w zakresie ICT	nie	34,5	43,1	33,3	33,3	38,5	55,1	32,7	53,6	46,6	41,1	48,1	55,6	23,8	46,1	42,8	31,9
	tak	65,5	56,9	66,7	66,7	61,5	44,9	67,3	46,4	53,4	58,9	51,9	44,4	76,3	53,9	57,2	68,1
Wydatki na funkcjonowanie informatyczne	do 10 tys. zł	15,9	12,7	26,0	7,0	12,8	5,9	13,9	7,1	25,2	22,2	12,7	12,1	17,5	26,3	6,6	5,6
	10–100 tys. zł	52,2	60,8	57,3	73,7	58,1	41,9	61,0	60,7	46,6	65,6	54,4	48,4	56,3	50,0	68,4	66,7
	powyżej 100 tys. zł	31,9	26,5	16,7	19,3	29,1	52,2	25,1	32,1	28,2	12,2	32,9	39,5	26,3	23,7	25,0	27,8
System elektronicznego zarządzania dokumentami	nie	21,2	54,9	28,0	56,1	59,0	18,4	20,6	51,8	35,0	27,8	20,3	14,5	16,	26,3	48,7	41,7
	podstawowy sposób obiegu dokumentów	15,0	2,9	9,3	7,0	4,3	8,8	12,6	1,8	5,8	2,2	13,9	9,7	13,8	3,9	5,9	2,8
	pomocniczy sposób obiegu dokumentów	63,7	42,2	62,7	36,8	36,8	72,8	66,8	46,4	59,2	70,0	65,8	75,8	70,0	69,7	45,4	55,6

cd. tabeli 40

Wyszczególnienie		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Stosowanie otwartych danych	nie	91,2	94,1	96,7	96,5	9 4.0	94,1	95,1	91,1	92,2	93,3	94,9	91,9	92,5	88,2	98,0	95,8
	tak	8,8	5,9	3,3	3,5	6,0	5,9	4,9	8,9	7,8	6,7	5,1	8,1	7,5	11,8	2,0	4,2
Udostępnianie danych online	nie	50,4	58,8	64,7	64,9	59,0	56,6	50,7	53,6	65,0	68,9	55,7	50,0	60,0	59,2	64,5	62,5
	tak	49,6	41,2	35,3	35,1	41,0	43,4	49,3	46,4	35,0	31,1	44,3	50,0	40,0	40,8	35,5	37,5

1 – dolnośląskie
2 – kujawsko-pomorskie
3 – lubelskie
4 – lubuskie
5 – łódzkie
6 – małopolskie
7 – mazowieckie
8 – opolskie
9 – podkarpackie
10 – podlaskie
11 – pomorskie
12 – śląskie
13 – świętokrzyskie
14 – warmińsko-mazurskie
15 – wielkopolskie
16 – zachodniopomorskie

Źródło: opracowanie własne na podstawie badań.

Tabela 41. Rozkład odpowiedzi na pytania o przygotowanie gmin do funkcjonowania w gospodarce 4.0 według województw (w %) – część II

Wyszczególnienie		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Business intelligence	nie	89,4	90,2	92,7	86,0	92,3	88,2	89,7	92,9	83,5	91,1	88,6	79,8	95,0	88,2	87,5	97,2
	tak	10,6	9,8	7,3	14,0	7,7	11,8	10,3	7,1	16,5	8,9	11,4	20,2	5,0	11,8	12,5	2,8
Strona internetowa zgodna z WCAG 2.0	nie	8,0	9,8	15,3	17,5	18,8	19,9	13,0	7,1	19,4	14,4	19,0	10,5	13,8	3,9	11,2	18,1
	tak	92,0	90,2	84,7	82,5	81,2	80,1	87,0	92,9	80,6	85,6	81,0	89,5	86,3	96,1	88,8	81,9
Strona internetowa na urządzenia mobilne	nie	8,8	15,7	12,7	8,8	16,2	16,9	14,8	3,6	12,6	13,3	11,4	7,3	10,0	14,5	7,9	9,7
	tak	91,2	84,3	87,3	91,2	83,8	83,1	85,2	96,4	87,4	86,7	88,6	92,7	90,0	85,5	92,1	90,3
Udostępnianie aplikacji	nie	59,3	61,8	79,3	50,9	79,5	63,2	81,2	41,1	68,0	80,0	60,8	63,7	75,0	67,1	61,8	84,7
	tak	40,7	38,2	20,7	49,1	20,5	36,8	18,8	58,9	32,0	20,0	39,2	36,3	25,0	32,9	38,2	15,3
Służbowe urządzenia mobilne u pracowników	mniej niż 5%	58,4	53,9	7 4.0	61,4	66,7	63,2	63,2	67,9	73,8	73,3	58,2	62,1	77,5	57,9	54,6	56,9
	5–15%	25,7	29,4	17,3	21,1	21,4	22,1	21,5	16,1	20,4	13,3	29,1	23,4	16,3	21,1	18,4	26,4
	powyżej 15%	15,9	16,7	8,7	17,5	12,0	14,7	15,2	16,1	5,8	13,3	12,7	14,5	6,3	21,1	27,0	16,7
Usługi elektroniczne	nie	20,4	21,6	30,0	35,1	27,4	16,9	21,5	21,4	15,5	28,9	29,1	9,7	30,0	13,2	17,8	25,0
	tak	79,6	78,4	70,0	64,9	72,6	83,1	78,5	78,6	84,5	71,1	70,9	90,3	70,0	86,8	82,2	75,0
Chmura obliczeniowa	nie	92,0	76,5	89,3	94,7	88,0	90,4	89,2	71,4	90,3	92,2	92,4	89,5	88,8	92,1	93,4	90,3
	tak	8,0	23,5	10,7	5,3	12,0	9,6	10,8	28,6	9,7	7,8	7,6	10,5	11,3	7,9	6,6	9,7

cd. tabeli 41

Wyszczególnienie		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Pojazdy autonomiczne	nie	99,1	100,0	99,3	100,0	100,0	99,3	100,0	100,0	100,0	100,0	98,7	98,4	100,0	98,7	100,0	100,0
	tak	0,9	0,0	0,7	0,0	0,0	0,7	0,0	0,0	0,0	0,0	1,3	1,6	0,0	1,3	0,0	0,0
Drony	nie	81,4	85,3	91,3	91,2	95,7	84,6	87,0	85,7	91,3	93,3	87,3	79,0	93,8	90,8	86,2	90,3
	tak	18,6	14,7	8,7	8,8	4,3	15,4	13,0	14,3	8,7	6,7	12,7	21,0	6,3	9,2	13,8	9,7

1 – dolnośląskie
2 – kujawsko-pomorskie
3 – lubelskie
4 – lubuskie
5 – łódzkie
6 – małopolskie
7 – mazowieckie
8 – opolskie
9 – podkarpackie
10 – podlaskie
11 – pomorskie
12 – śląskie
13 – świętokrzyskie
14 – warmińsko-mazurskie
15 – wielkopolskie
16 – zachodniopomorskie

Źródło: opracowanie własne na podstawie badań.

ZAKOŃCZENIE

Za cel monografii autorki przyjęły diagnozę wykorzystania przez gminy w Polsce nowych technologii informacyjno-komunikacyjnych. Postawiły tezę, że stopień zaawansowania gmin (mierzony liczbą wykorzystywanych nowych rozwiązań technologicznych) jest uzależniony od typu administracyjnego gminy oraz jej położenia. Rozważania w monografii rozpoczęto od zarysu koncepcji gospodarki 4.0, ze szczególnym uwzględnieniem samorządu gminnego. Najważniejszym aspektem funkcjonowania organizacji w gospodarce 4.0 jest cyfryzacja wywołująca dynamiczne zmiany w otoczeniu każdego podmiotu (państwa, województwa, powiatu, gminy, przedsiębiorstwa, obywatela). Jej przyczyną jest rozwój naukowo-techniczny, a przede wszystkim wynalezienie komputera oraz powstanie internetu. Cyfryzacja to także liczne, powiązane ze sobą rozwiązania technologiczne prowadzące do powstawania coraz nowocześniejszych koncepcji technicznych i organizacyjnych. Pojawianie się coraz nowszych ICT wpływa także na rozwój człowieka, ponieważ nieodłącznym elementem cyfryzacji są: wiedza, informacja i dane. Cyfrowa rewolucja jest związana z wiedzą określaną jako najważniejsze dobro, które dzięki cyfryzacji stało się dostępne dla każdego. Procesy tworzenia cyfrowych danych oraz usieciowienia przyczyniły się do przejścia z gospodarki tradycyjnej do gospodarki cyfrowej, której konsekwencje zauważalne są niemal w każdej dziedzinie życia. Skutkami gospodarki cyfrowej są: automatyzacja pracy, a co za tym idzie – wzrost jej efektywności, spadek kosztów produkcji oraz powstawanie coraz nowszych modeli biznesowych. Cyfryzacja pociąga za sobą tworzenie się relacji (m.in. konsument–producent, obywatel–państwo), wzrost liczby oferowanych produktów oraz powstawanie nowych – usług. Ponadto dzięki niej powstała sztuczna inteligencja znajdująca zastosowanie m.in. w bankowości, służbie zdrowia, sądownictwie, administracji lokalnej. Wynika z tego, że cyfryzacja jest adaptacją technologii informacyjno-komunikacyjnych do różnych sfer życia gospodarczego i społecznego, w tym do działalności samorządu gminnego.

Transformacja cyfrowa samorządu gminnego to zmiany zachodzące w gminach dotyczące zasobów, usług, procesów, kultury organizacyjnej oraz kompetencji, dokonywane w celu podnoszenia jakości usług publicznych, usprawnienia pracy urzędu, wsparcia procesów podejmowania decyzji, zwiększenia przejrzystości działania tego samorządu oraz angażowania mieszkańców w życie wspólnoty samorządowej, wykorzystując ICT. Transformacja cyfrowa gmin jest niezbędnym warunkiem ich zrównoważonego rozwoju, ponieważ technologie te

mogą być wykorzystywane do bardziej efektywnego świadczenia usług administracyjnych, społecznych i komunalnych.

Ze zjawiskiem cyfryzacji jest związany problem nierówności cyfrowych, którym poświęcono drugi rozdział monografii. Są one jedną z podstawowych barier transformacji cyfrowej samorządu gminnego. Nierówności te można rozpatrywać na trzech poziomach.

Pierwszy poziom nierówności cyfrowych, którego miarą jest dostępność do internetu, stał się podstawowym narzędziem do pomiaru wykluczenia cyfrowego, dzięki któremu możliwe stało się wyodrębnienie obszarów geograficznych zamieszkiwanych przez osoby wykluczone cyfrowo. Na podstawie przeprowadzonej analizy danych można dostrzec „linie podziału cyfrowego". Gminy Polski południowo-zachodniej mają średnio wyższe wskaźniki dostępu do szerokopasmowego internetu niż gminy w Polsce północno-wschodniej. Mieszkańcy tej drugiej części Polski są zatem w większym stopniu zagrożeni wykluczeniem cyfrowym. Dodatkowo wykazano, że większym wykluczeniem cyfrowym zagrożone są obszary wiejskie. Z kolei drugi poziom nierówności cyfrowych określono mianem nierówności uczestnictwa, ponieważ wskazuje się na różnice między grupami ludzi w zakresie ich umiejętności niezbędnych do efektywnego korzystania z internetu. Na podstawie badań literaturowych zidentyfikowano zmienne, które wpływają na kompetencje cyfrowe i sposób korzystania z internetu. Do czynników tym zaliczono: wiek, poziom dochodu, status zatrudnienia oraz płeć. Trzeci poziom nierówności cyfrowych dotyczy dysproporcji w korzyściach z użytkowania internetu wśród osób o podobnym profilu wykorzystywania sieci i z podobnym poziomem dostępu do infrastruktury internetowej oraz technologii informacyjno-komunikacyjnych. Obserwuje się zarówno pozytywne, jak i negatywne konsekwencje korzystania z internetu.

W związku ze zidentyfikowanym problemem wykluczenia cyfrowego w dalszej części monografii autorki prowadziły rozważania dotyczące warunków zrównoważonego rozwoju gmin. Problematyka rozwoju zrównoważonego jest szeroka i wielowątkowa. Niezadowalające efekty „odgórnej" polityki rozwoju sprawiają, że rośnie znaczenie teorii rozwoju regionalnego i lokalnego „od dołu". Podkreślono, że w zrównoważonym rozwoju społeczeństwa szczególną rolę odgrywa samorząd terytorialny, szczególnie na szczeblu gmin. Bez zrównoważonego rozwoju na poziomie lokalnym nie jest możliwy rozwój zrównoważony w ujęciu krajowym i dalej globalnym. Samorząd gminny, będący najbliżej społeczności lokalnej, jest w stanie najszybciej i najtrafniej zidentyfikować potrzeby mieszkańców (np. w czasie pandemii COVID-19 w zakresie sprzętu do nauki zdalnej) oraz dotrzeć do osób, które są zagrożone wykluczeniem cyfrowym. Działania gmin ograniczają się do zadań zdefiniowanych ustawowo, jednak ich zakres obejmuje dziedziny ważne z punktu widzenia zrównoważo-

nego rozwoju (edukacja, ochrona zdrowia, kultura, pomoc społeczna, ochrona środowiska na szczeblu lokalnym, transport publiczny).

W literaturze przedmiotu najczęściej są wyróżniane trzy filary zrównoważonego rozwoju: gospodarka (ekonomia), społeczeństwo i środowisko. Niektórzy autorzy wyodrębniają też filar czwarty, którym jest np. kultura lub zdrowie. Mając w pamięci pandemię COVID-19 oraz biorąc pod uwagę funkcjonowanie społeczeństwa w warunkach gospodarki 4.0, autorki opowiadają się za traktowaniem zdrowia jako czwartego filaru zrównoważonego rozwoju oraz proponują filar piąty – integrację cyfrową (*digital inclusion*). Piąty filar jest związany z niwelowaniem nierówności w cyfrowym rozwoju społeczeństwa. W warunkach gospodarki 4.0 zmniejszenie tych różnic jest punktem wyjścia do osiągnięcia celów zrównoważonego rozwoju, a nawet koniecznością. Autorki zwracają przy tym uwagę na rolę samorządu terytorialnego (szczególnie gmin) w zrównoważonym rozwoju cyfrowym. Realizacja celów wpisujących się w ten filar – zapewnienie dostępności sieci, sprzętu oraz rozwijanie umiejętności cyfrowych społeczeństwa – w dużej mierze spoczywa na samorządzie gminnym, który będąc najbliżej swoich mieszkańców, jest w stanie najszybciej i najrzetelniej zidentyfikować braki w tym zakresie oraz zainicjować działania zmierzające do ich usunięcia. Dopiero zapewnienie zrównoważonego rozwoju na szczeblu lokalnym pozwala na realizację tej idei na szczeblu regionalnym, narodowym i globalnym.

Szansą na przyspieszenie przemian i wdrażanie pożądanych działań jest wzrost liczby źródeł finansowania rozpatrywanej transformacji ze środków europejskich, dlatego że dotychczas, dążąc do cyfryzacji gmin, napotykano wiele barier, w tym finansowych. Unia Europejska aktywnie wspiera rozwój cyfryzacji, tworząc jednolity rynek cyfrowy, który ma umożliwiać swobodę transakcji dokonywanych za pomocą kanałów elektronicznych oraz wpłynąć na rozwój europejskich gospodarek za pomocą rozwiązań prawnych. Jednym z tych rozwiązań jest dokument Europejska Cyfrowa Dekada zawierający kierunki działań oraz cele, które powinny zostać osiągnięte do 2030 r. Komisja Europejska stworzyła też finansowe instrumenty umożliwiające finansowanie rozwoju cyfryzacji. Do najważniejszych należą programy: Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, Instrument na rzecz Odbudowy i Zwiększania Odporności, Cyfrowa Europa, Horyzont Europa i Łącząc Europę oraz InvestEU.

Nasycenie nowymi technologiami informacyjno-komunikacyjnymi polskiej gospodarki, w tym administracji publicznej, mierzone wskaźnikiem DESI na tle innych państw Unii Europejskiej nie jest zadowalające. Polska znajduje się na 23. miejscu z wynikiem niższym od średniej unijnej. Jednak sytuacja Polski z roku na rok się poprawia, co więcej, znajdujemy się na pierwszym miejscu pod względem wykorzystywania mobilnych usług szerokopasmowych (głównie w bankowości).

W związku z niską pozycją Polski na tle innych państw członkowskich UE oraz zobowiązaniami wobec Komisji Europejskiej Polska wprowadza w życie wiele strategii i programów przyspieszających proces cyfryzacji kraju. Jednym z dokumentów strategicznych jest Plan Zintegrowanej Informatyzacji Państwa mający na celu zapewnienie obywatelom usług publicznych na jak najwyższym poziomie, służąc tym samym osiąganiu celów jednolitego rynku cyfrowego. Rozdział poświęcony Polsce cyfrowej znalazł się też w „Długookresowej strategii rozwoju kraju. Polska 2030. Trzecia fala nowoczesności". Jej aktualną wersją jest Strategia na rzecz odpowiedzialnego rozwoju z perspektywą do 2030 r. Ważne zagadnienia zapisano też w programie społeczno-gospodarczym rządu Polski Ład, w którym zaplanowano działania prowadzące do zmniejszenia skutków pandemii COVID-19. Jednym z ujętych w nim zagadnień jest program Cyber Poland 2025, w którym opisano zmiany prowadzące do cyfryzacji kraju.

Wymienione programy przyczyniły się do tego, że w Polsce funkcjonują już rozwiązania z zakresu elektronicznej administracji publicznej. Elektroniczne usługi publiczne są dostępne m.in. na Elektronicznej Platformie Usług Administracji oraz EZD.gov.pl Korzystanie z tych usług jest możliwe dzięki profilowi zaufanemu, który z roku na rok ma coraz więcej obywateli. Dzięki tym portalom mieszkańcy mogą załatwić sprawy w różnych urzędach, w tym w urzędach gmin i urzędach stanu cywilnego.

W cyfryzacji samorządu gminnego upatruje się wielu korzyści. Przewiduje się, że (docelowo) wyeliminuje się dokumenty w wersji papierowej, a tym samym zmniejszy presję na gospodarcze wykorzystywanie środowiska naturalnego i zmniejszy koszty. Elektroniczne załatwianie wielu spraw uprości pracę urzędników i poprawi jakość obsługi obywateli i innych interesariuszy. Elektroniczne świadczenie usług ułatwi też pozyskiwanie informacji zwrotnej o ich jakości. Wszystko to wpłynie na wzrost efektywności świadczenia lokalnych usług publicznych. Transformacja cyfrowa samorządu gminnego będzie też impulsem do podnoszenia kompetencji cyfrowych, samej organizacji (urzędu gminy), pracowników samorządowych, obywateli i przedsiębiorców.

Proces transformacji cyfrowej, który obejmuje również działalność jednostek samorządu terytorialnego, obok korzyści płynących z zastosowania technologii informacyjnych wiąże się z nowymi zagrożeniami. Jednym z największych wyzwań stojących przed organizacjami, również przed jednostkami samorządu gminnego, jest konieczność zapewnienia cyberbezpieczeństwa – bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do wykonywania różnego rodzaju zadań. W monografii podkreślono, że wprowadzanie w życie rozwiązań, które mają się przyczynić do zapewnienia cyberbezpieczeństwa w jednostkach samorządowych, należy do obowiązków kierownika jednostki, który odpowiada za system kontroli zarządczej w danym podmiocie. Natomiast skuteczne wdrażanie kontroli zarządczej wymaga kompleksowego podejścia do procedur obo-

wiązujących w podmiocie. Rozwiązań składających się na zapewnienie cyberbezpieczeństwa jednostki samorządowej nie można traktować jako odrębnych działań podejmowanych przez kierownika jednostki lub wyznaczonych przez niego pracowników, lecz trzeba je rozpatrywać w szerszym kontekście systemu kontroli zarządczej, a co się z tym wiąże – powinny one uwzględniać standardy tej kontroli.

Rozwiązania przyjmowane przez jednostki samorządu gminnego, które mają kształtować i wzmacniać cyberbezpieczeństwo organizacji, powinny się opierać na działaniach prewencyjnych przyczyniających się do zwiększenia świadomości cyberbezpieczeństwa w jednostkach samorządu terytorialnego oraz budowania tzw. kultury cyberbezpieczeństwa. Niewystarczający poziom umiejętności pracowników administracji gminnej może prowadzić do utraty zdolności obrony przed cyberprzestępcami. Bardzo ważna jest umiejętność identyfikacji potencjalnych zagrożeń cyberbezpieczeństwa. Aby tego dokonać, konieczna jest znajomość technik i rozwiązań stosowanych przez cyberprzestępców. W związku z tym w monografii przedstawiono rodzaje cyberataków, których prawdopodobieństwo wystąpienia w jednostkach samorządu terytorialnego jest najwyższe. Podjęto też próbę scharakteryzowania schematów działań cyberprzestępców oraz wskazano propozycje działań prewencyjnych zmniejszających ryzyko wystąpienia danego cyberataku, które mogą być wdrożone w podsektorze samorządowym. Zaprezentowano również rodzaje cyberataków, jakie wystąpiły w jednostkach samorządu gminnego w Polsce w świetle badania przeprowadzonego w 2020 r.

W ostatnim rozdziale monografii zaprezentowano wyniki badania dotyczącego gotowości gmin do funkcjonowania w gospodarce 4.0. Podczas badań weryfikowano tezę, że stopień zaawansowania urzędów gmin (mierzony liczbą wykorzystywanych nowych rozwiązań technologicznych) jest uzależniony od typu administracyjnego gminy oraz jej położenia (województwa). W pierwszej kolejności sprawdzono, czy rodzaj gminy jest czynnikiem różnicującym stopień przygotowania gminy do funkcjonowania w gospodarce 4.0. Z przeprowadzonych badań wynika, że jednostkami najlepiej przygotowanymi w tym zakresie są miasta na prawach powiatu. To właśnie tam zdecydowanie najczęściej są zlokalizowane nadajniki telefonii 5G, miasta te częściej dysponowały intranetem służącym do komunikacji wewnątrz urzędu oraz do przekazywania danych, najczęściej przeprowadzały szkolenia w zakresie technologii informacyjno-komunikacyjnych, wykorzystywały system elektronicznego zarządzania dokumentami jako pomocniczy lub podstawowy sposób obiegu dokumentów, najczęściej udostępniały online otwarte dane publiczne oraz dane z rejestrów publicznych, wykorzystywały narzędzia *business intelligence*, posiadały strony internetowe dostosowane do urządzeń mobilnych, zdecydowanie częściej udostępniały również aplikacje na urządzenia mobilne oraz miały większy odsetek pracowników urzędu gminy wyposażonych w służbowe urządzenia mobilne z dostępem do in-

ternetu w celu obsługi gminnych aplikacji elektronicznych. Badania wykazały również, że miasta na prawach powiatu częściej świadczyły usługi elektroniczne i częściej korzystały z chmury obliczeniowej, a także jako jedne z nielicznych używały (testowały) pojazdów autonomicznych oraz zdecydowanie najczęściej używały dronów. W związku z najszerszym katalogiem działań przygotowujących gminę do funkcjonowania w gospodarce 4.0 podejmowanych w miastach na prawach powiatu ponoszono tam największe wydatki na finansowanie tych działań, co zostało potwierdzone w badaniach. Drugą grupą jednostek samorządu terytorialnego najlepiej przygotowanych do działania w gospodarce 4.0 były gminy miejskie i kolejno miejsko-wiejskie i wiejskie.

Następnym aspektem branym pod uwagę podczas badań nad przygotowaniem gmin do funkcjonowania w gospodarce 4.0 było zróżnicowanie terytorialne. Sprawdzono, czy występował związek pomiędzy stopniem przygotowania gmin do funkcjonowania w gospodarce 4.0 a województwem. Najwięcej gmin dobrze przygotowanych do funkcjonowania w gospodarce 4.0 było w województwie śląskim, dolnośląskim, opolskim i warmińsko-mazurskim. Różnice między województwami nie były jednak tak zauważalne jak wpływ typu gminy na przygotowanie do funkcjonowania w gospodarce cyfrowej.

Badania zamieszczone w monografii wzbogacają literaturę przedmiotu. Pokazują bowiem, że transformacja cyfrowa samorządu terytorialnego następuje wolno. Zespół badaczy pod kierunkiem Ziemby (2018) już kilka lat temu zdiagnozował czynniki determinujące poziom wykorzystania przez administrację publiczną nowych technologii, które można też uznać za bariery transformacji cyfrowej. Zaliczono do nich czynniki: (1) ekonomiczne, związane z dostępem do źródeł finansowania transformacji cyfrowej; (2) technologiczne (np. integrację oprogramowania ułatwiającą przepływ informacji i bezpieczeństwo informacji); (3) społeczno-kulturowe, np. odpowiednie kompetencje pracowników jednostek administracji publicznej; (4) organizacyjne, w tym komunikację elektroniczną między tymi jednostkami. Powołani autorzy sformułowali też rekomendacje dotyczące zmian, które powinny się przyczynić do wzrostu wykorzystania ICT w działalności gmin i rozwój usług cyfrowych.

Podzielamy opinię zespołu Ziemby (2018), że działania składające się na transformację cyfrową samorządu gminnego wykraczają poza możliwości organizacyjne, kadrowe i finansowe poszczególnych gmin. Nasze badanie pokazuje, że w dalszym ciągu należy podejmować działania zmierzające do likwidacji tych barier.

Ograniczenia finansowe są szczególnie widoczne w małych jednostkach. Powodują trudności nie tylko w zakupie sprzętu, we wdrażaniu nowych technologii oraz podstawowych technicznych środków bezpieczeństwa, ale także w pozyskiwaniu informatyków, programistów i fachowców z zakresu bezpieczeństwa informacji (Chodakowska i in., 2022b; Eisenstein, 2019). W krótkim okresie

remedium na lukę finansową mogą być nieodpłatne szkolenia i konferencje organizowane przez organy administracji rządowej, w tym korzystanie z przygotowanych przez nie oraz placówki naukowe materiałów informacyjnych. W długim okresie należałoby wygospodarować środki na kształcenie przedstawicieli organów lokalnych, kadry kierowniczej i innych pracowników samorządowych. Szkolenia mogłyby być finansowane z różnych źródeł.

Niedostateczna liczba szkoleń może być spowodowana nie tylko brakiem środków finansowych, ale także brakiem świadomości ich znaczenia dla sprawnego funkcjonowania gminy, przeciążeniem pracowników (udział w szkoleniu nie zwalnia z obowiązku wykonywania codziennej pracy), obawą o niezadowolenie mieszkańców, którzy oceniają działalność wójta przez pryzmat widocznych zmian w swoim otoczeniu, oraz innymi czynnikami. Łukaszuk (2022) twierdzi, że brakuje skoordynowanych działań w zakresie nabywania i pogłębiania kompetencji cyfrowych. Jej zdaniem, aby pracownicy administracji samorządowej skutecznie rozwijali swoje kompetencje, niezbędne jest podejście systemowe, współdziałanie na szczeblu rządowym i samorządowym. Niezbędne jest też pozyskanie do współpracy w tych szkoleniach sektora prywatnego i organizacji pozarządowych. Pracownicy samorządowi posiadający odpowiednie kompetencje cyfrowe umożliwiające bezpieczne i efektywne czerpanie korzyści z rozwoju technologii cyfrowych staną się rzeczywistymi wykonawcami założeń transformacji cyfrowej dokonującej się w samorządzie terytorialnym (Łukaszuk, 2022).

Sam udział w rozmaitych szkoleniach nie spowoduje automatycznego wzrostu nasycenia działalności gmin nowymi technologiami informacyjno-komunikacyjnymi i zwiększenia liczby oferowanych usług cyfrowych. W każdej gminie potrzebny jest lider transformacji cyfrowej (Szczepaniak, 2021), osoba, która będzie miała wizję celu, do którego gmina dąży w krótkim i długim okresie. Powinna to być osoba, która będzie potrafiła zachęcać organy władzy lokalnej i pracowników samorządowych do wychodzenia ze strefy komfortu, z dobrze znanej im procedury świadczenia określonych usług i spojrzenia na nie w inny, nowoczesny, cyfrowy sposób.

Konieczne jest też informowanie gmin o potencjalnych (w tym europejskich) źródłach finansowania wydatków na transformację cyfrową i upowszechnienie dobrych praktyk z tym związanych. Ze źródeł tych można bowiem finansować zakup sprzętu informatycznego i oprogramowania, wydatki na tworzenie usług cyfrowych i poprawę cyberbezpieczeństwa, wydatki na rozbudowę sieci internetowej na terenie gminy, szkolenia (dla pracowników samorządowych, przedstawicieli władz, mieszkańców, przedsiębiorców) itd. Mając świadomość wyzwań stojących przed jednostkami samorządu terytorialnego, i to nie tylko związanych z transformacją cyfrową, z niepokojem patrzymy na przedłużającą się procedurę udostępnienia Polsce funduszy z budżetu Unii Europejskiej po 2022 r.

Odpowiedzią na ograniczone możliwości organizacyjne, kadrowe i finansowe poszczególnych gmin może też być udział przedstawicieli gmin w konferencjach branżowych, współpraca i wymiana doświadczeń w dziedzinie cyfryzacji w urzędach i ich jednostkach organizacyjnych. Innym sposobem jest nawiązywanie partnerstw z sąsiednimi jst (gminami, powiatami, samorządem województwa) w celu wymiany wiedzy i wspólnego ponoszenia wydatków. Wymiana doświadczeń, wspólne budowanie systemów, a także wykorzystanie efektu ekonomii skali to najważniejsze aspekty, na które gminy powinny zwrócić uwagę, rozważając podjęcie współpracy (Chodakowska i in., 2022). Współpraca międzygminna także napotyka przeszkody. Bariery we współpracy mogą mieć podłoże mentalne i ideologiczne. Jednostki samorządu terytorialnego mają osobowość prawną i zagwarantowaną prawnie samodzielność działania. W drodze do dojrzałej transformacji cyfrowej powinny jednak współdziałać nie tylko ze sobą, ale również z przedstawicielami administracji państwowej i agencjami rządowymi (Hatcher i in., 2020). Uważamy, że spodziewana skala oszczędności i rosnąca świadomość społeczeństwa zwiększają presję na gminy do poszukiwania efektywnych i skutecznych rozwiązań. Jednym z takich rozwiązań jest wspólna dostawa elektronicznych usług publicznych, co może pomóc w utrzymaniu niskich kosztów ich świadczenia, a co za tym idzie – zwiększyć efektywność wydatków publicznych oraz jakość usług publicznych (Kaczyńska, 2020).

Ograniczenie samodzielności gmin i nadmierna ingerencja organów państwa w ich działanie nie są wprawdzie pożądane, ale w kontekście transformacji cyfrowej należy też postulować korzystanie z doświadczeń administracji rządowej i z oferty usług chmurowych adresowanych do jst, które są dostępne w systemie Zapewniania Usług Chmurowych ZUCH (*ZUCH…*, 2021) działającym od połowy 2021 r. Jakość i bezpieczeństwo tych usług zostały zweryfikowane przez pracowników ówczesnego Ministerstwa Cyfryzacji.

Problematyka transformacji cyfrowej samorządu terytorialnego, w tym gminnego, jest złożona, ważna i aktualna. Przytoczone w monografii przykłady innowacji i wyniki badań potwierdzają, że samorząd gminny stanowi swego rodzaju laboratorium do testowania nowych rozwiązań w zakresie innowacji społecznych i technologicznych, które, jeśli okażą się sukcesem, stanowią wzorzec do naśladowania bądź są bezpośrednio wdrażane w innych jednostkach samorządu terytorialnego, a nawet na poziomie centralnym, w całym kraju.

Zmiany w stopniu nasycenia działalności urzędów gmin i gminnych placówek usługowych zachodzą niemal każdego dnia, co stanowi przesłankę kontynuacji badań nad tym zagadnieniem. Jednym z możliwych kierunków badań jest określenie dojrzałości cyfrowej gmin. Warto byłoby również przeprowadzić analizy statystyczne, aby ocenić zależności występujące na przykład między typem administracyjnym gminy a wykorzystywanymi technologiami informacyjno-komunikacyjnymi. Można też szukać odpowiedzi na pytania: Czy na moty-

wację gmin do wprowadzania innowacji cyfrowych wpływa dążenie do reelekcji wójta (burmistrza, prezydenta miasta) i składanie przez niego tzw. obietnic wyborczych? Czy istnieje związek między wprowadzaniem nowych technologii a wiekiem wójta (burmistrza, prezydenta miasta)? Czy gminy naśladują swoich sąsiadów w przyjmowaniu nowych rozwiązań? Uzyskane wyniki mogą stanowić też punkt wyjścia do badań jakościowych, które umożliwiłyby wyciągnięcie wniosków na temat przyczyn stosunkowo niewielkiego wykorzystania tych technologii przez niektóre gminy.

BIBLIOGRAFIA

Abu Rajab, M., Zarfoss, J., Monrose, F. i Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on internet measurement*, 41–52. https://dl.acm.org/doi/10.1145/1177080.1177086

Anderson, R. H., Bikson, T. K., Law, S. A. i Mitchell, B. M. (1997). Universal access to e-mail: Feasibility and societal implications. *Educational Media International*, *34*(2), 86–87. https://www.tandfonline.com/doi/abs/10.1080/0952398970340208

Aplikacja Kwarantanna domowa. (b.d.). https://www.gov.pl/web/koronawirus/kwarantanna-domowa

Arendt, Ł. (2013). Mazowieckie wykluczenie cyfrowe. W: M. Pokrzywa i S. Wilk (red.), *Wykluczenie społeczne: Diagnoza, wymiary i kierunki badań* (s. 311–327). Wydawnictwo Uniwersytetu Rzeszowskiego.

Atkinson, A. B. (1970). On the measurement of inequality. *Journal of Economic Theory*, *2*(3), 244–263. https://doi.org/10.1016/0022-0531(70)90039-6

Ayanso, A., Cho, D. I. i Lertwachara, K. (2013). Information and communications technology development and the digital divide: A global and regional assessment. *Information Technology for Development*, *20*(1), 60–77. https://doi.org/10.1080/02681102.2013.797378

Barber, B. R. (2014). *Gdyby burmistrzowie rządzili światem. Dysfunkcyjne kraje, rozkwitające miasta*. Warszawskie Wydawnictwo Literackie Muza.

Bartak, J. (2019). Instytucjonalne uwarunkowania nierówności szans edukacyjnych w Polsce. *Nierówności Społeczne a Wzrost Gospodarczy*, *57*(1), 387–401. https://doi.org/10.15584/nsawg.2019.1.28

Basikowska, J. (2011). *Stan realizacji i perspektywy rozwoju e-adminstracji w Polsce*. Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.

Baszyński, A. (2020). Crowdlearning – od pruskiego modelu edukacji do nauczania zdalnego dzięki społeczności. W: R. Kamiński (red.), *Przedsiębiorstwo, gospodarka i społeczeństwo w kręgu zainteresowania ekonomistów* (s. 81–95). Polskie Towarzystwo Ekonomiczne.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G., Portugali, Y. (2012). Smart cities of the future. *The European Physical Journal Special Topics*, *214*, 481–518. https://doi.org/10.1140/epjst/e2012-01703-3

Bednarek, M. (2020). *Po Katowicach jeździ książkobus. Dostarcza książki osobom starszym i niepełnosprawnym*. https://katowice.wyborcza.pl/katowice/7,35063,26190395,po-katowicach-jezdzi-ksiazkobus-dostarcza-ksiazki-osobom.html

Beinare, D. i McCarthy, M. (2012). Civil society organisations, social innovation and health research in Europe. *The European Journal of Public Health*, *22*(6), 889–893. https://doi.org/10.1093/eurpub/ckr152

Bendkowski, J. (2017). Zmiany w pracy produkcyjnej w perspektywie koncepcji „Przemysł 4.0". *Zeszyty Naukowe Politechniki Śląskiej*, *1990*, 112, 23.

Brandtzaeg, P. B., Heim, J. i Karahasanović, A. (2011). Understanding the new digital divide – A typology of internet users in Europe. *International Journal of Human-Computer Studies*, *69*(3), 123–138. https://doi.org/10.1016/j.ijhcs.2010.11.004

Brennenn, S., Kreiss, D. (2014, sierpień). *Digitalization and digitization*. https://culture-digitally.org/2014/09/digitalization-and-digitization/

Burns, A. J., Johnson, M. E. i Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24–39. https://doi.org/10.1080/10919392.2019.1552745

Bynner, J. i Reder, S. (2010). *The three divides. The digital divide and its relation to basic skills and employment in Portland, USA and London, England*. http://www.lsal.pdx.edu/docs/pdf/the_three_divides_2010.pdf

Calsyn, R. J. (2003). A modified ESID approach to studying mental illness and homelessness. *American Journal of Community Psychology, 32*(3/4), 319–331. https://doi.org/10.1023/b:ajcp.0000004751.98756.ef

Caragliu, A., Del Bo, C. i Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, *18*(2), 65–82. https://doi.org/10.1080/10630732.2011.601117

Caruson, K., MacManus, S. A. i McPhee, B. D. (2012). Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Journal of Homeland Security and Emergency Management*, *9*(2). https://doi.org/10.1515/jhsem-2012-0003

Cellary, W. (2019a). *Gospodarka 4.0*. https://docplayer.pl/146279397-Gospodarka-4-0-wojciech-cellary-katedra-technologii-informacyjnych.html

Cellary, W. (2019b). Przemysł 4.0 i Gospodarka 4.0. *Biuletyn Polskiego Towarzystwa Ekonomicznego*, *3*(86), 48–52.

Cellary, W. (2022a). Dokumenty cyfrowe podstawą funkcjonowania instytucji państwa. *Biuletyn Polskiego Towarzystwa Ekonomicznego*, *1*(96), 40–44.

Cellary, W. (2022b). *Nowe technologie w finansach. Referat wygłoszony podczas konferencji z okazji 30-lecia Katedry Finansów Przedsiębiorstw UEP*.

Centrum Badań i Analiz Rynku. (2015). *Wpływ cyfryzacji na działanie urzędów administracji publicznej w Polsce w 2015 r.*

Centrum Projektów Polska Cyfrowa. (b.d.). *Regulamin konkursu grantowego Cyfrowa gmina – Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym –„Granty PPGR"*. https://www.gov.pl/web/cppc/wsparcie-ppgr

Chaba, D. (2021). Warunki cyfryzacji samorządu terytorialnego w Polsce. *Samorząd Tertorialny*, *5*, 11–20.

Chałubińska-Jentkiewicz, K. (2021). Cybersecurity as a Public Task in Administration. W: K. Chałubińska-Jentkiewicz, M. Karpiuk i J. Kostrubiec (Eds.), *The legal status of public entities in the field of cybersecurity in Poland* (s. 19–38). Institute for Local Self-Government Maribor. https://doi.org/10.4335/2021.5

Chesbrough, H. W. (2003). *Open innovation. The new imperative for creating and profiting from technology*. Harvard Business School Press Boston.

Chien, E. (2005). Techniques of adware and spyware. *Proceedings of the Fifteenth Virus Bulletin Conference*. https://www.virusbulletin.com/conference/vb2005/abstracts/techniques-adware-and-spyware/

Chodakowska, A., Kańduła, S. i Przybylska, J. (2022a). Cybersecurity in the local government sector in Poland: More work needs to be done. *Lex localis – Journal of Local Self-Government*, *20*(1), 161–192. https://doi.org/10.4335/20.1.161-192(2022)

Chodakowska, A., Kańduła, S. i Przybylska, J. (2022b). Jak polskie gminy radzą sobie z cyberbezpieczeństwem. *Kontrola Państwowa*, *1*, 129–148. https://doi.org/10.53122/ISSN.0452-5027/2022.1.08

Chomiak-Orsa, I. (2016). Znaczenie technologii informacyjno-komunikacyjnych w zrównoważonym rozwoju miast. *Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie*, *23*(1), 36–45. https://doi.org/10.17512/znpcz.2016.3.1.04

Cieślik, T. (2020). *KRI i RODO – jak połączyć wymagania przy audycie bezpieczeństwa w podmiotach publicznych?* https://www.politykabezpieczenstwa.com.pl/audyt-kri-i-rodo/

Ciupa, S. (2020). *Podejście systemowe do wdrażania technologii cyfrowych w zarządzaniu miastem*. https://forumrozwojulokalnego.pl/okiem-eksperta/80

Ciupa, S. (2021). Rola danych w zarządzaniu miastem. W: W. Łachowski (red.), *Zarządzanie danymi w miastach. Podręcznik dla samorządów*. Obserwatorium Polityki Miejskiej. Instytut Rozwoju Miast i Regionów. https://obserwatorium.miasta.pl/wp-content/uploads/2021/10/IRMiR_Zarzadzaniedanymi_20210922-4.pdf

Clark, R. i Moloney, G. (2020). Facebook and older adults: Fulfilling psychological needs? *Journal of Aging Studies*, *55*, 1–7. https://doi.org/10.1016/j.jaging.2020.100897

Colla, V., Pietrosanti, C., Malfa, E. i Peters, K. (2020). Environment 4.0: How digitalization and machine learning can improve the environmental footprint of the steel production processes. *Matériaux & Techniques*, *108*(507), 1–11. https://doi.org/10.1051/mattech/2021007

Coskun, V., Ozdenizci, B. i Ok, K. (2013). A survey on Near Field Communication (NFC) technology. *Wireless Personal Communications*, *71*, 2259–2294. https://doi.org/10.1007/s11277-012-0935-5

COSO I – *Kontrola wewnętrzna. Zintegrowana struktura ramowa*. (2008). Polski Instytut Kontroli Wewnętrznej.

Costa, R. N. i Pérez-Duarte, S. (2019). *Not all inequality measures were created equal. The measurement of wealth inequality, its decompositions, and an application to European household wealth*. https://www.ecb.europa.eu/pub/pdf/scpsps/ecb.sps31~269c917f9f.en.pdf

Co to jest spam i jak zablokować niechciane wiadomości? (2022). https://www.orange.pl/poradnik/twoj-internet/co-to-jest-spam-i-jak-zablokowac-niechciane-wiadomosci/

Co to jest złośliwe oprogramowanie? (2021). https://www.mcafee.com/pl-pl/antivirus/malware.html

CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego). (2021). *Raport o stanie bezpieczeństwa cyberprzestrzeni w RP w 2020 roku*. https://www.ksoin.pl/wp-content/uploads/2021/09/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2020-1.pdf

Cyfrowa dekada Europy: cele cyfrowe na 2030 r. (b.d.). https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl%0A

Cyfryzacja KPRM. (2022). *Fundusz Szerokopasmowy – pierwszy nabór wniosków*. https://www.gov.pl/web/cyfryzacja/fundusz-szerokopasmowy--pierwszy-nabor-wnioskow

Czekaj, J. (red.). (2012). *Podstawy zarządzania informacją*. Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.

Ćwiklicki, M., Duplaga, M. i Klich, J. (Eds.). (2021). *The digital transformation of healthcare. health 4.0*. Routledge. https://doi.org/10.4324/9781003144403

de Bruijn, H. i Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

Digital transformation: *A roadmap for billion-dollar organizations.* (2011). MIT Center for Digital Business and Capgemini Consulting. https://www.capgemini.com/wp-content/uploads/2017/07/Digital_Transformation__A_Road-Map_for_Billion-Dollar_Organizations.pdf

DiMaggio, P., Hargittai, E. W., Neuman, R. i Robinson, J. P. (2021). Social implications of the internet. *Annual Review of Sociology*, *27*, 307–336.

Dmowski, J., Jędrzejewski, M., Suffczyńska-Hałabuz, N., Iwasieczko, M., Libucha, J., Owerczuk, M., Pławik, K. i Kowalska, I. (2016). *Przemysł 4.0 PL. Szansa czy zagrożenie dla rozwoju innowacyjnej gospodarki?* The Boston Counsulting Group. https://docplayer.pl/24443942-Przemysl-4-0-pl-szansa-czy-zagrozenie-dla-rozwoju-innowacyjnej-gospodarki.html

Dobre wsparcie. (b.d.). https://dobrewsparcie.org/. Pobrane 12 września 2020.

Dobrowolski, Z. (2005). Koncepcja społeczeństwa informacyjnego Daniela Bella. W: B. Sosińska-Kalata, M. Przastek-Samokowa i A. Akrzypcak (red.), *Od informacji naukowej do technologii społeczeństwa informacyjnego* (s. 87–105). Stowarzyszenie Bibliotekarzy Polskich.

Dubec, M. (2020). *Chatbot – dowiedz się więcej o działaniach miasta związanych z koronawirusem*. https://tinyurl.com/ymsfufds

Dufva, T. i Dufva, M. (2019). Grasping the future of the digital society. *Futures*, *107*, 17–28. https://doi.org/10.1016/j.futures.2018.11.001

Dylewski, M. i Kępa, M. (2009). E-urząd: innowacyjny partner w społeczeństwie informacyjnym. *Problemy Zarządzania, Finansów i Marketingu*, *13*(516), 135–145. http://bazekon.icm.edu.pl/bazekon/element/bwmeta1.element.ekon-element-000171363725

Dziemianowicz, R. I., Kargol-Wasiluk, A. i Bołtromiuk, A. (2018). Samodzielność finansowa gmin w Polsce w kontekście koncepcji good governance. *Optimum. Economic Studies*, *4*(4(94)), 204–219. https://doi.org/10.15290/oes.2018.04.94.16

Eisenstein, L. (2019). *Why municipalities should care about cybersecurity*. https://insights.diligent.com/cybersecurity-local-government/why-municipalities-care-cybersecurity

EKG. (Europejska Komisja Gospodarcza). (2021). Ageing in the digital era. *UNECE Policy Brief on Ageing*, *26*, 1–28. https://unece.org/sites/default/files/2021-07/PB26-ECE-WG.1-38.pdf

Estevez, E., Lopes, N. V. i Janowski, T. (2016). *Smart sustainable cities. Reconnaissance study*.https://mostwiedzy.pl/pl/publication/smart-sustainable-cities-reconnaissance-study,139312-1

Eurostat. (2022). *Households – level of internet access.* https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_in_h/default/table?lang=en

Falconer, G. i Mitchell, S. (2012). *Smart city framework. A* systematic process for enabling smart + connected communities. CISCO. https://www.cisco.com/c/dam/en_us/about/ac79/docs/ps/motm/Smart-City-Framework.pdf

Federacja Konsumentów. (2021). *Wykluczenie cyfrowe podczas pandemii. Dostęp oraz korzystanie z internetu i komputera w wybranych grupach społecznych*. *Raport*. http://www.federacja-konsumentow.org.pl/s,1479,wykluczenie-cyfrowe-podczas-pandemii.html

Felis, P. (2011). Financial independence of local self-government units in acquisition of sources to finance their activity – challenges for self-government theory and practice. *Journal of Management and Financial Sciences*, *4*(6), 41–61. https://bazekon.uek.krakow.pl/rekord/171308669

Ferreira, D., Vale, M., Carmo, R. M., Encalada-Abarca, L. i Marcolin, C. (2021). The three levels of the urban digital divide: Bridging issues of coverage, usage and its outcomes in VGI platforms. *Geoforum*, *124*, 195–206. https://doi.org/10.1016/j.geoforum.2021.05.002

Filipiak, B. Z. i Dylewski, M. (2021). Dylematy wyboru samorządowych instrumentów dłużnych. *Studia BAS*, *68*(4), 107–129. https://doi.org/10.31268/studiabas.2021.38

Frey, D. (2011, 13 maja). Budowa masztów telefonii komórkowej: sam sprzeciw mieszkańców nie zablokuje decyzji lokalizacyjnej. *Rzeczpospolita*. https://www.rp.pl/orzecznictwo/art6354641-budowa-masztow-telefonii-komorkowej-sam-sprzeciw-mieszkancow-nie-zablokuje-decyzji-lokalizacyjnej

Fuchs, C. (2009). The role of income inequality in a multivariate cross-national analysis of the digital divide. *Social Science Computer Review*, *27*(1), 41–58. https://journals.sagepub.com/doi/10.1177/0894439308321628

Fundusze Europejskie na lata 2021–2027. (b.d.). https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/

Fundusze Europejskie na Rozwój Cyfrowy 2021–2027. Projekt programu przyjęty przez Radę Ministrów w dniu 5 stycznia 2022 r. (2022).

Gadomski, M. (2018). *internet rzeczy dociera do miast. Uwaga na zagrożenia*. Portal Samorządowy. https://www.portalsamorzadowy.pl/smart-city/internet-rzeczy-dociera-do-miast-uwaga-na-zagrozenia,114495.html

Galperin, H. i Arcidiacono, M. (2021). Employment and the gender digital divide in Latin America: A decomposition analysis. *Telecommunications Policy*, *45*(7), 1–12. https://doi.org/10.1016/j.telpol.2021.102166

Ganczar, M. i Sytek, A. (2021). *Informatyzacja administracji publicznej. Skuteczność regulacji*. CeDeWu.

Gawłowski, R. i Miliszewski, K. (2019). Social media w administracji samorządowej na przykładzie powiatów województwa. *Samorząd Terytorialny*, *5*, 71–83.

Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in Computer Virology*, *6*(1), 77–90. https://doi.org/10.1007/s11416-008-0092-2

Gąska, D. (2015). *Bezpieczeństwo w cyberprzestrzeni – zarys problemu, wyzwania i zagrożenia*. https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia

Gdańska Platforma Edukacyjna. (b.d.). https://edu.gdansk.pl/

Gevelt, T. Van i Holmes, J. (2015). A vision for smart villages. *Smart Villages New thingking for off-grid communities worldwide*, *5*(5), 1–6. www.e4sv.org

Giełda Miejskich Technologii. (b.d.). https://gieldamiejskichtechnologii.pl/aktualnosci. Pobrane 26 października 2022.

Giles, J. (2010). Scareware: the inside story. *New Scientist*, *205*(2753), 38–41. https://doi.org/10.1016/S0262-4079(10)60731-2

Głąbicka, K. i Grewiński, M. (2005). *Polityka spójności społeczno-gospodarczej Unii Europejskiej*. Dom Wydawniczy ELIPSA.

Gómez Barroso, J. L. i Pérez Martínez, J. (2004). The geography of the digital divide: broadband deployment in the Community of Madrid. *Universal Access in the Information Society*, *3*, 264–271. https://doi.org/10.1007/s10209-004-0103-0

Góra, J. (2013). *Efektywne zarządzanie bezpieczeństwem informacji*. http://www.ipblog.pl/wp-content/uploads/downloads/2013/04/RAPORT-2013.pdf

Górka, M. (2017). Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa. *Cywilizacja i Polityka*, *15*, 295–315. https://tinyurl.com/2p992ys9

Graham, M. (2011). Time machines and virtual portals: The spatialities of the digital divide. *Progress in Development Studies*, *11*(3), 211–227. https://doi.org/10.1177/146499341001100303

Greenstein, S. i Prince, J. (2006). *The diffusion of the internet and the geography of the digital divide in the United States.* NBER Working Paper, 12182. https://www.nber.org/system/files/working_papers/w12182/w12182.pdf

Grodner, M., Kokot, W., Kolenda, P., Krejtz, K., Legoń, A., Rytel, P. i Wierzbiński, R. (2016). *internet rzeczy w Polsce*. https://www.iab.org.pl/wp-content/uploads/2016/05/Raport-internet-Rzeczy-w-Polsce.pdf

Grzelak, M. i Liedel, K. (2012). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski–zarys problemu. *Bezpieczeństwo Narodowe*, *22*(2), 125–139.

GUS. (Główny Urząd Statystyczny). (2019). *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2015–2019*. https://tinyurl.com/yscdbv97

GUS. (Główny Urząd Statystyczny). (2021). *Społeczeństwo informacyjne w Polsce w 2021 r.* https://tinyurl.com/fvtacdsd

Guz, H. (2022). E-administracja – doświadczenia samorządu regionalnego w budowie systemu informatycznego – studium przypadku. *Perspektywy Kultury*, *4*(39), 195–218.

Guzal-Dec, D. (2018). Inteligentny rozwój wsi – koncepcja smart villages: założenia, mozliwości i ograniczenia implementacyjne. *Economics and Regional Studies/Studia Ekonomiczne i Regionalne*, *11*(3), 32–49. https://doi.org/10.2478/ers-2018-0023

Gwizda, M., Kosewska-Kwaśny, M. i Żółciński, S. (2014). *Fundusze UE 2014–2020*. Wydawnictwo C.H. Beck.

Hakovirta, M. i Denuwara, N. (2020). How COVID-19 redefines the concept of sustainability. *Sustainability*, *12*(9), 3727. https://doi.org/10.3390/su12093727

Hargittai, E. (2002). Second-level digital divide: differences in people's online skills. *First Monday*, *7*(4). https://doi.org/10.5210/fm.v7i4.942

Hatcher, W., Meares, W. L. i Heslen, J. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302–325. https://doi.org/10.1080/23738871.2020.1792956

Hauke, K. (2017). Business intelligence in the process management in local government units on the level of the community. *Studia Informatica Pomerania*, *43*(1), 35-48. https://doi.org/10.18276/si.2017.43-04

Hauke, K. (2018). Model przetwarzania danych w chmurze obliczeniowej na przykładzie gminy. *Przedsiębiorstwo we współczesnej gospodarce – teoria i praktyka*, *2*(25), 79–92. https://doi.org/10.19253/reme.2018.0.006

Hawken, P. (1994). *The ecology of commerce*. HarperCollins.

Hawkes, J. (2001). *The fourth pillar of sustainability: culture's essential role in public planning*. Common Ground Publishing. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/referencespapers.aspx?referenceid=2738442

Hayati, P., Potdar, V., Talevski, A., Firoozeh, N., Sarenche, S. i Yeganeh, E. A. (2010). Definition of spam 2.0: New spamming boom. *4th IEEE International Conference on Digital Ecosystems and Technologies*, 580–584. https://doi.org/10.1109/DEST.2010.5610590

Hayward, G. i Garvin, K. (2010). The international regulatory, social, and political framework. W: K. Brown, W. L. Hall, M. H. Snook i K. Garvin (Eds.), *Sustainable land development and restoration: decision consequence analysis* (s. 3–11). Butterworth-Heinemann.

Heales, C. i Green, H. (2017). *Social innovation in health and social care: case study results*. https://www.si-drive.eu/wp-content/uploads/2017/03/SI-DRIVE-Deliverable-D9_3-Health-1.pdf

Hilbert, M. (2011). Digital gender divide or technologically empowered women in developing countries? A typical case of lies, damned lies, and statistics. *Women's Studies International Forum*, *34*(6), 479–489. https://doi.org/10.1016/j.wsif.2011.07.001

IERC. (Illionis Education Research Council). (2015). *IERC – European research cluster on the internet of things*. http://www.internet-of-things-research.eu/about_iot.htm

Ilnicki, D. (2009). *Przestrzenne zróżnicowanie poziomu rozwoju usług w Polsce. Teoretyczne i praktyczne uwarunkowania badań*. Wydawnictwo Uniwersytetu Wrocławskiego.

InvestEU. (2022). https://instrumentyfinansoweue.gov.pl/invest-eu/

Jak urzędy gmin korzystają z mediów społecznościowych? (2022). https://backend.sprawdzamyjakjest.pl/media/annotations/mission/report_file/SJJ_raport_lajki.pdf

Janicki, T. i Goździewska-Nowicka, A. (2018). Digital economy as a strategy of economic development in the 21st century. *Torun Business Review*, *17*(1), 1–6. https://doi.org/10.19197/tbr.v18i1.313

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, *32*(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

Jastrzębska, K. (2018). *Elektronicza administracja jako narzędzie wdrażania zmian organizacyjnych*. CeDeWu.

Jindal, N. i Liu, B. (2007). Review spam detection. *Proceedings of the 16th international conference on World Wide Web*, 1189–1190. https://www.cs.uic.edu/~liub/publications/reviewSpam-2007.pdf

Jurczak, T. (2020). *No title*. Inteligentny monitoring w Gdyni wykryje tłum. https://www.sztucznainteligencja.org.pl/inteligentny-monitoring-w-gdyni-wykryje-tlum/

Kaczyńska, A. (2020). Inter-municipal cooperation in education as a possible remedy for current difficulties of local government in Poland. *Acta Universitatis Lodziensis. Folia Oeconomica*, *5*(350), 101–125. https://doi.org/10.18778/0208-6018.350.06

Kaczyńska, A., Kańduła, S. i Przybylska, J. (2021). Transformacja cyfrowa z punktu widzenia samorządu terytorialnego – wybrane zagadnienia. *Nierówności Społeczne a Wzrost Gospodarczy*, *65*(1), 27–46. https://doi.org/10.15584/nsawg.2021.1.2

Kalinowski, S., Komorowski, Ł. i Rosa, A. (2021). Koncepcja smart villages: Przykłady z Polski. W: *Koncepcja smart villages: Przykłady z Polski*. Wydawnictwo Grupa Cogito. https://doi.org/10.53098/9788389900623

Kańduła, S. (2003). *Samodzielność finansowa samorządu gminnego w Polsce po 1993 roku*. Wydawnictwo Akademii Ekonomicznej w Poznaniu.

Kańduła, S. i Przybylska, J. (2020). Internal audit of the national interoperability framework as a tool for assessing information security in the conditions of economy 4.0. W: O. M. Polinkiewicz i L. W. Szostak (red.). *Materialy Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi: Innovacijnyj rozvytok ta bezpeka pidpryjemstv v umovah neoindustrial'nogo suspil'stva* (s. 518–520). Wschodnioeuropejski Państwowy Uniwersytet im. Lesi Ukrainki w Łucku.

Kańduła, S. i Przybylska, J. (red.). (2022a). *Gospodarka w cieniu pandemii COVID-19*. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. https://doi.org/10.18559/978-83-8211-104-0

Kańduła, S. i Przybylska, J. (2022b). Instrumenty polityki komunikacyjnej w zarządzaniu kryzysowym gmin w Polsce podczas pierwszej fazy pandemii CIVID-19. *Finanse Komunalne, 4*(22), 19–35.

Kańduła, S. i Przybylska, J. (2022c). Zarządzanie kryzysowe w gminach w reakcji na pierwszą falę pandemii COVID-19. W: S. Franek (red.), *Finanse – wielowymiarowość procesów i perspektywy rozwoju* (s. 29–42). Wydawnictwo Naukowe Uniwersytetu Szczecińskiego.

Kara, İ. i Aydos, M. (2019). The ghost in the system: technical analysis of remote access trojan. *International Journal on Information Technologies & Security*, *11*(1), 73–84.

Karahasanović, A., Brandtzæg, P. B. ., Heim, J., Lüders, M., Vermeir, L., Pierson, J., Lievens, B., Vanattenhoven, J. i Greet, J. (2009). Co-creation and user-generated content-elderly people's user requirements. *Computers in Human Behavior*, *25*(3), 655–678. https://doi.org/10.1016/j.chb.2008.08.012

KBN (Komitet Badań Naukowych). (2003). *Strategia informatyzacji rzeczypospolitej polskiej – ePolska*. https://historiainformatyki.pl/dokument.php?nrar=10&nrzesp=2&sygn=X/2/5&handle=1591

KE (Komisja Europejska.) (b.d.). *Instrument na rzecz Odbudowy i Zwiększania Odporności*. https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_pl

KE (Komisja Europejska). (b.d.). *Portal WiFi4EU*. https://wifi4eu.ec.europa.eu/#/home

KE (Komisja Europejska). (b.d.). *Smart cities*. Pobrane w 2022 r. z https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

KE (Komisja Europejska). (2017a). *Europejski Semestr – zestawienie informacji tematycznych: Rozwiązanie problemu nierówności*. https://ec.europa.eu/info/sites/default/

files/file_import/european-semester_thematic-factsheet_addressing-inequalities_pl.pdf
KE (Komisja Europejska). (2017b). *Rozwiązanie Problemu Nierówności*. Europejski semestr – zestawienie informacji tematycznych.
KE (Komisja Europejska). (2021a). *Instrument „Łącząc Europę”*. https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_pl
KE (Komisja Europejska). (2021b). *Program „Cyfrowa Europa”*. https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_pl
Kemp, R. i Pearson, P. (2007). *Final report MEI project about measuring ecoinnovation*. UM-MERIT. https://www.oecd.org/env/consumption-innovation/43960830.pdf
Keynes, J. M. (2011). *Essays in persuasion*. A Project Gutenberg Canada Ebook. https://gutenberg.ca/ebooks/keynes-essaysinpersuasion/keynes-essaysinpersuasion-00-h.html#Economic_Possibilities
Klyta, T. (2019). *Konkurs Human Smart Cities rozstrzygnięty: 25 miast dostanie pieniądze na swoje projekty*. https://tinyurl.com/2zne3z5a
Komitet Kontaktowy najwyższych organów kontroli (NOK) Unii Europejskiej. (2020). Cyberbezpieczeństwo w UE i państwach członkowskich UE. Kontrole dotyczące odporności krytycznych systemów informacyjnych i infrastruktury cyfrowej na cyberataki. https://www.consilium.europa.eu/pl/policies/cybersecurity/
Komunikat (2009). Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz. Urz. MF z 2009 r. No 15, poz. 84).
Konkurs „HUMAN SMART CITIES. Inteligentne miasta współtworzone przez mieszkańców” (b.d.). https://tinyurl.com/2zne3z5a
Korenik, A. (2019). *Smart cities. Inteligentne miasta w Europie i Azji*. CeDeWu.
Kornberger-Sokołowska, E., Zdanukiewicz, J. i Cieślak, R. (2010). *Jednostki samorządu terytorialnego jako beneficjenci środków europejskich*. Wolters Kluwer Polska.
Kostrubiec, J. (2021). The role of public order regulations as acts of local law in the performance of tasks in the field of public security by local self-government in Poland. *Lex Localis – Journal of Local Self-Government*, *19*(1), 111–129.
Koszeluk, J. (2021). *Smart city jako współczesna koncepcja rozwoju miast*. Uniwersytet Ekonomiczny w Poznaniu.
Koszewski, R., Oręziak, B. i Wielec, M. (red.). (2020). *Możliwe przyczyny i rodzaje przestępczości w przyszłości oraz przygotowania prewencyjne*. Wydawnictwo Instytutu Wymiaru Sprawiedliwości.
Kotlińska, J. (2009). Dochody własne jednostek samorządu terytorialnego w Polsce. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, *3*, 143–161.
Kotlińska, J. (2011). Finanse jednostek samorządu terytorialnego. W: T. Juja (red.), *Finanse publiczne* (s. 79–100). Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.
Krajowy Plan Odbudowy i Zwiększania Odporności. (2021). https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/krajowy-plan-odbudowy/o-kpo/

Krajowy Punkt Kontaktowy. (2021). *Horyzont Europa – nowy program ramowy badań i innowacji UE*. https://www.kpk.gov.pl/horyzont-europa-nowy-program-ramowy-badan-i-innowacji

Kroik, J. i Skonieczny, J. (2013). *Innowacja społeczna a społeczna odpowiedzialność przedsiębiorstwa*. https://docplayer.pl/6854234-Innowacja-spoleczna-a-spoleczna-odpowiedzialnosc-przedsiebiorstwa.html

Krynicka, H. (2006). Koncepcja nowego zarządzania w sektorze publicznym. *Studia Lubuskie*, *2*, 193–202.

Kubicka-Żach, K. (2019). *Urząd zaatakowany przez cyberprzestępców, wójtowi grozi kara*. https://www.prawo.pl/samorzad/cyberatak-na-gminna-strone-internetowa-kto-odpowie-za,496647.html

Kulik, W. (2013). *Co to jest spear phishing i czym grozi?* https://www.benchmark.pl/aktualnosci/spear-phishing-co-to-jest-ataki-coraz-popularniesze.html

Kwiecień, B. (2020). *Atak hakerów na Starostwo Powiatowe w Oświęcimiu. Chcieli okupu. System informatyczny urzędu z problemami. Trwa śledztwo policji*. https://oswiecim.naszemiasto.pl/atak-hakerow-na-starostwo-powiatowe-w-oswiecimiu-chcieli/ar/c15-7983251

Le, V. L., Welch, I., Gao, X. i Komisarczuk, P. (2013). Anatomy of drive-by download attack. *Proceedings of the Eleventh Australasian Information Security* Conference (Vol. 138, s. 49–58). https://tinyurl.com/3daefa4j

Linia współpracy 2016 – zaproszenie do współpracy budowy wspólnych rozwiązań IT. (b.d.). https://www.gov.pl/web/cyfryzacja/linia-wspolpracy-2016-zaproszenie-%0A-do-wspolpracy-budowy-wspolnych-rozwiazan-it

Lipowicz, I. (2019). *Samorząd terytorialny XXI wieku*. Wolters Kluwer Polska.

Liu, D., Chen, S. i Chou, T. (2011). Resource fit in digital transformation: Lessons learned from the CBC Bank global e-banking project. *Management Decision*, *49*, 10, 1728–1742. https://doi.org/10.1108/00251741111183852

Loogma, K., Tafel-Viia, K. i Ümarik, M. (2012). Conceptualising educational changes: A social innovation approach. *Journal of Educational Change*, *14*(3), 283–301. https://doi.org/10.1007/s10833-012-9205-2

Łachowski, W. (red.). (2021). *Zarządzanie danymi w miastach. Podręcznik dla samorządów*.

Łachowski, W., Pistelok, P. i Dziadowicz, K. (2022). Zarządzanie miastem z wykorzystaniem danych. W: *Zarządzanie miastem z wykorzystaniem danych*. Badania Obserwatorium Polityki Miejskiej. https://doi.org/10.51733/opm.2022.02

Łuczyn, R. (2020). *Lokalne społeczności a pandemia . Przykłady innowacji społecznych*. https://www.batory.org.pl/wp-content/uploads/2022/02/Lokalne-spolecznosci-a-pandemia.-Przyklady-innowacji-spolecznych.pdf

Łukaszuk, A. (2022). Problematyka kompetencji cyfrowych kadr administracji publicznej jako istotnego czynnika procesu transformacji cyfrowej jednostek samorządu terytorialnego w Polsce. *Studia Prawnoustrojowe*, *58*, 287–313. https://doi.org/10.31648/sp.7985

Machura, E. (2013). Informacja i jej znaczenie we współczesnym świecie w kontekście ochrony informacji niejawnych w Polsce. *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej*, *1*(5), 155–167.

Macmanus, S. A., Caruson, K. i McPhee, B. D. (2013). Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. *Journal of Urban Affairs*, *35*(4), 451–470. https://doi.org/10.1111/j.1467-9906.2012.00640.x

Madej, J. (2011). Wydatki na bezpieczeństwo systemów informatycznych: inwestycja czy koszt funkcjonowania systemu? *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, *865*, 35–45.

Makrakis, V., Gkotzos, D. i Larios, N. (2012). ICT-enabled climate change education and children rights. *Journal of Teacher Education for Sustainability*, *14*(2), 54–72. https://doi.org/10.2478/v10099-012-0011-y

Malucha, M. (2018). internet of things – the technological context and areas of application. *Studia i Prace WNEiZ*, *54*(54), 51–69. https://doi.org/10.18276/sip.2018.54/2-04

Małopolski Urząd Marszałkowski zaatakowany przez hakerów. (2021). https://samorzad.pap.pl/kategoria/aktualnosci/malopolski-urzad-marszalkowski-zaatakowany-przez-hakerow

Marciniak, S. (2010). *Innowacyjność i konkurencyjność gospodarki*. Wydawnictwo C.H. Beck.

Martin, S. P. i Robinson, J. P. (2007). The income digital divide: Trends and predictions for levels of internet use. *Social Problems, 54*(1), 1–22. https://doi.org/10.1525/sp.2007.54.1.1

Maruyama, Y., Nishikido, M. i Iida, T. (2007). The rise of community wind power in Japan: Enhanced acceptance through social innovation. *Energy Policy*, *35*(5), 2761–2769. https://doi.org/10.1016/j.enpol.2006.12.010

Mastalerz, M. (2021). *Urząd miejski w Otwocku padł ofiarą cyberataku*. https://samorzad.pap.pl/kategoria/e-urzad/urzad-miejski-w-otwocku-padl-ofiara-cyberataku

Matheus, R., Janssen, M. i Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

MC (Ministerstwo Cyfryzacji). (2016). *Kierunki działań strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych*. https://www.gov.pl/web/cyfryzacja/kierunki-dzialan-strategicznych-ministra-cyfryzacji-w-obszarze-informatyzacji-uslug-publicznych1

MC (Ministerstwo Cyfryzacji). (2019). *Program zintergowanej informatyzacji państwa na lata 2014-2022, wersja zaktualizowana*.

Mejna, K. (2020). *Cyfrowy Asystent Mieszkańca doceniony w międzynarodowej sieci Smart Cities*. https://www.gdynia.pl/gdynia-innowacyjna,7581/cyfrowy-asystent-mieszkanca-doceniony-w-miedzynarodowej-sieci-smart-cities,548794

Mensah, J. (2019). Sustainable development: Meaning, history, principles, pillars, and implications for human action: Literature review. *Cogent Social Sciences*, *5*(1), 1–21. https://doi.org/10.1080/23311886.2019.1653531

MF (Ministerstwo Finansów). (2012). *Kontrola zarządcza w sektorze finansów publicznych. Istota, unormowania prawne i otoczenie*. https://mf-arch2.mf.gov.pl/c/document_library/get_file?uuid=ec119301-3422-4b56-af7d-318b470fd973&groupId=764034

MFiPR (Ministerstwo Funduszy i Polityki Regionalnej). (2022a). *Fundusze Europejskie dla Rozwoju Społecznego 2021 – 2027*. https://www.power.gov.pl/media/108159/PROGRAM_FERS.pdf

MFiPR (Ministerstwo Funduszy i Polityki Regionalnej). (2022b). *Fundusze Europejskie na Infrastrukturę, Klimat i Środowisko – założenia programu*. https://www.pois.gov.pl/strony/o-programie/fundusze-europejskie-na-infrastrukture-klimat-srodowisko/zalozenia-programu/

MFiPR (Ministerstwo Funduszy i Polityki Regionalnej). (2022c). *Zasady realizacji instrumentów terytorialnych w Polsce w perspektywie finansowej UE na lata 2021–2027*. https://tinyurl.com/2j472xus

Miazga, A., Dziadowicz, K. i Pistelok, P. (2022). *Cyfryzacja urzędów miast*. https://doi.org/10.51733/opm.2022.01

Millward, P. (2003). The „grey digital divide": Perception, exclusion and barriers of access to the internet for older people. *First Monday*, *8*(7). https://doi.org/10.5210/fm.v8i7.1066

Mohurle, S. i Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940. https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Moldan, B., Janousková, S. i Hák, T. (2012). How to understand and measure environmental sustainability: Indicators and targets. *Ecological Indicators*, *17*, 4–13. https://doi.org/10.1016/j.ecolind.2011.04.033

Moon, M. J. (2002). The evolution of e-government among municipalities: Rhetoric or Reality? *Public Administration Review*, *62*(4), 424–433. https://doi.org/10.1111/0033-3352.00196

Mulgan, G. (2006). The process of social innovation. *Innovations: Technology, Governance Globalization*, *1*(2), 145–162. https://doi.org/10.1162/itgg.2006.1.2.145

Mulgan, G., Tucker, S., Ali, R. i Sanders, B. (2007). *Social innovation: what it is, why it matters, how it can be accelerated*. https://www.researchgate.net/publication/277873357_Social_Innovation_What_It_Is_Why_It_Matters_and_How_It_Can_Be_Accelerated

Murzyn, D. (2018). Spójność społeczna i inkluzywność jako priorytety polityki spójności UE. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, *537*, 66–75. https://doi.org/10.15611/pn.2018.537.06

Największe wycieki danych i sposoby ochrony przed tym zagrożeniem. (2021). https://www.nazwa.pl/blog/najwieksze-wycieki-danych-i-sposoby-ochrony

Ndou, V. (2004). E- Government for developing countries: Opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, *18*(1), 1–8. https://doi.org/10.1002/j.1681-4835.2004.tb00117.x

Nielsen, J. (2006). *Digital Divide: The 3 Stages*. https://www.nngroup.com/articles/digital-divide-the-three-stages/

NIK (Najwyższa Izba Kontroli). (2014). *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu. Informacja o wynikach kont*.

NIK (Najwyższa Izba Kontroli). (2016). *System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność. Informacja o wynikach kontroli*.

NIK (Najwyższa Izba Kontroli). (2018). *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli*.

NIK (Najwyższa Izba Kontroli). (2016). *System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność. Informacja o wynikach kontroli.*

NIK (Najwyższa Izba Kontroli). (2018). *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego. Informacja o wynikach kontroli*.

Norris, D. F., Mateczun, L., Joshi, A. i Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, *43*(8), 1173–1195. https://doi.org/10.1080/07352166.2020.1727295

Oates, W. E. (1999). An Essay on Fiscal Federalism. *Journal of Economic Literature*, *37*(3), 1120–1149.

OECD (Organizacja Współpracy Gospodarczej i Rozwoju). (2019). *Enhancing the contribution of digitalization to the smart cities of the future*. https://www.oecd.org/cfe/regionaldevelopment/Smart-Cities-FINAL.pdf

OECD i Eurostat. (2005). *Podręcznik Oslo. Zasady gromadzenia i interpretacji danych dotyczących innowacji*. https://tinyurl.com/2zamy4dn

Ojo, A. (2019). Next Generation Government – Hyperconnected, Smart and Augmented. W: L. M. Camarinha-Matos, H. Afsarmanesh i D. Antonelli (Eds.), *Collaborative networks and digital transformation. PRO-VE 2019. IFIP advances in information and communication technology* (s. 285–294). Springer, Cham. https://doi.org/10.1007/978-3-030-28464-0_25

ONZ (Organizacja Narodów Zjednoczonych). (2016). *New urban agenda*. *Resolution adopted by the General Assembly on 23 December 2016*. https://habitat3.org/wp-content/uploads/New-Urban-Agenda-GA-Adopted-68th-Plenary-N1646655-E.pdf

Ostrom, V., Tiebout, C. M. i Warren, R. (1961). The organizaion of government in metropolitan areas: A theoretical inquiry. *The American Political Science Review*, *55*(4), 831–842.

Otoikamanu, F. K. (2020). *Closing the digital divide; supporting vulnerable countries*. https://www.broadbandcommission.org/insight/closing-the-digital-divide-supporting-vulnerable-countries/

PAP (Polska Agencja Prasowa). (2014). *Ekspert o e-administracji: papier to symbol nieefektywności*. https://www.prawo.pl/samorzad/ekspert-o-e-administracji-papier-to-symbol-nieefektywnosci,94481.html

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

Pathak, P. B. (2016). Malware a growing cybercrime threat: Understanding and combating malvertising attacks. *International Journal of Advanced Research in Computer Science*, *7*(2), 9–11.

Patrzałek, L., Poniatowicz, M., Guziejewska, B. i Kańduła, S. (2022). *Od rozwoju do erozji finansów samorządu terytorialnego w Polsce*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Penc, J. (1999). *Innowacje i zmiany w firmie*. Poltex.

Perdał, R. (2014). *Czynniki rozwoju elektronicznej administracji w samorządzie lokalnym w Polsce*. Bogucki Wydawnictwo Naukowe.

Peters, M. A., Marginson, S. i Murphy, P. (2009). *Creativity and the global knowledge economy*. Peter Lang Publishing.

Peters, M., Schneider, M., Griesshaber, T. i Hoffmann, V. H. (2012). The impact of technology-push and demand-pull policies on technical change – Does the locus of policies matter? *Research Policy*, *41*(8), 1296–1308. https://doi.org/10.1016/j.respol.2012.02.004

Philips, S. D., Laforest, R. i Graham, A. (2010). From shopping to social innovation: getting public financing right in Canada. *Policy and Society*, *29*(3), 189–199. https://doi.org/10.1016/j.polsoc.2010.06.001

Piro, G., Cianci, I., Grieco, L. A., Boggia, G. i Camarda, P. (2013). Information Centric Services in Smart Cities. *Journal of Systems and Software*, *88*, 169–188. https://doi.org/10.1016/j.jss.2013.10.029

Podlaski Urząd Wojewódzki w Białymstoku. (2022). *System EZD PUW już nie tylko w administracji rządowej*. https://ezd.gov.pl/www/samorzady/samorzadyaktualnosci

Po raz trzeci programiści zaprojektowali innowacyjne aplikacje dla Płocka 3. City Coders Hackathon Płock. (2019). http://cifal.pl/2019/11/26/po-raz-trzeci-programisci-%0Azaprojektowali-innowacyjne-aplikacje-dla-plocka-3-city-coders-hackathon-%0A-plock/

Pol, E. i Ville, S. (2009). Social innovation: buzz word or enduring term? *The Journal of Socio-Economics*, *38*(6), 878–885. https://doi.org/10.1016/j.socec.2009.02.011

Polityka cyfrowej transformacji miasta stołecznego Warszawy. (2020). https://bip.warszawa.pl/NR/exeres/AADAC0E2-C65F-4040-8E3F-2BD52F071842,frameless.htm

Polska Agencja Żeglugi Powietrznej. (b.d.). *Usługi cyfrowe dla bezzałogowych statków powietrznych*. https://www.pansa.pl/konkurs3obszary/

Polski Fundusz Rozwoju. (b.d.). *PFR dla miast*. https://pfr.pl/pfr-dla-miast.html

Poniatowicz, M. (2018). *Koncepcja federalizmu fiskalnego w systemie finansów samorządu terytorianego*. CeDeWu.

Programy Komisji Europejskiej. (b.d.). https://programymiedzynarodowe.pomorskie.eu/programy-komisji-europejskiej/?doing_wp_cron=1667907017.5279710292816162109375

Programy Unii w dziedzinie zdrowia. (b.d.). https://www.gov.pl/web/zdrowie/programy-unii-w-dziedzinie-zdrowia

Projekt Umowy partnerstwa dla realizacji polityki spójności 2021–2027 w Polsce. (2021). https://www.gov.pl/web/fundusze-regiony/umowa-partnerstwa

Przekota, G. (2021). Wybrane koncepcje pomiaru nierówności dochodowych. *Nierówności Społeczne a Wzrost Gospodarczy*, *66*(2), 16–32. https://doi.org/10.15584/nsawg.2021.2.2

Przybylska, J. i Zasadzka, J. (2019). Narzędzia oceny kontroli zarządczej w jednostkach sektora finansów publicznych. W: I. Kowalska i A. Wasilewska (red.), *Stan i perspektywy rozwoju sektora finansów publicznych* (s. 181–191). Wydawnictwo SGGW.

Purvis, B., Mao, Y. i Robinson, D. (2019). Three pillars of sustainability: in search of conceptual origins. *Sustainability Science*, *14*, 681–695. https://doi.org/10.1007/s11625-018-0627-5

Rao, B. C. (2013). How disruptive is frugal? *Technology in Society*, *35*(1), 65–73. https://doi.org/10.1016/j.techsoc.2013.03.003

Raufflet, E. (2009). Mobilizing business for post-secondary education: CIDA university, South Africa. *Journal of Business Ethics*, *89*, 191–202. http://www.jstor.org/stable/27749768

Ray, D. i Ligatti, J. (2012). Defining code-injection attacks. *ACM SIGPLAN Notices*, *47*(1), 179–190. https://doi.org/10.1145/2103621.2103678

Regulamin konkursu grantowego Cyfrowa gmina. (b.d.). https://tinyurl.com/5d8yvmvc

Rodzaje trojanów komputerowych. (2021). https://www.omegasoft.pl/blog/rodzaje-trojanow-komputerowych/

Rogueware continues to grow. (2009). *Network Security*. https://doi.org/10.1016/S1353-4858(09)70035-2

Rosen, H. S. i Gayer, T. (2014). *Public Finance* (10 wyd.). McGraw Hill.

Rot, A. (2017). Zastosowania koncepcji internetu rzeczy w kontekście inteligentnego miasta. Wybrane zagadnienia bezpieczeństwa. *Problemy Zarządzania*, *15*(4), 41–53. https://doi.org/10.7172/1644-9584.71.3

Rozporządzenie PEiR. (2016). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). https://uodo.gov.pl/404

Rozporządzenie PEiR. (2018). Rozporządzenie Parlamentu Europejskiego i Rady UE z 7 czerwca 2018 r. ustanawiające program ramowy w zakresie badań naukowych i innowacji „Horyzont Europa" oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie. (b.d.). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018PC0435

Rozporządzenie PEiR. (2020). Rozporządzenie Parlamentu Europejskiego i Rady 2020/2092 z 16 grudnia 2020 roku w sprawie ogólnego systemu warunkowości służącego ochronie budżetu Unii (OJ L 433I , 22.12.2020, p. 1–10).

Rozporządzenie PEiR. (2021). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/241 z dnia 12 lutego 2021 r. ustanawiające Instrument na rzecz Odbudowy i Zwiększania Odporności (Dz.U.UE.L.2021.57.17).

Rozporządzenie RM. (2012). Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz. U. z 2017 r., poz. 2247).

Rozporządzenie RM. (2020). Rozporządzenie Rady Ministrów z dnia 7 października 2020 r. w sprawie zniesienia Ministerstwa Cyfryzacji (Dz. U. z 2020 r., poz. 1730).

Ruohonen, J. (2020). An acid test for Europeanization: Public cyber security procurement in the European Union. *European Journal for Security Research*, *5*, 349–377. https://doi.org/10.1007/s41125-019-00053-w

Rzeszowski projekt innowacyjnej edukacji na konferencji Microsoft EduDay 2020. (b.d.). https://www.erzeszow.pl/

Sabatini, F. (2019). Culture as fourth pillar of sustainable development: Perspectives for integration, paradigms of action. *European Journal of Sustainable Development*, *8*(3), 31–40. https://doi.org/10.14207/ejsd.2019.v8n3p31

Salminen, M. i Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North. *Polar Record*, *54*(2), 108–118. https://doi.org/10.1017/S0032247418000268

Scheerder, A., van Deursen, A. i van Dijk, J. (2017). Determinants of internet skills, uses and outcomes. A systematic review of the second- and third-level digital divide. *Telematics and Informatics*, *34*, 1607–1624. https://doi.org/10.1016/j.tele.2017.07.007

Schoenmaker, D. (2017). *From risk to opportunity: A framework for sustainable finance*. W: *The international encyclopedia of communication theory and philosophy*. John Wiley & Sons, Inc. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066210

Shuldiner, A. (2020). The smart village. *IEEE Pervasive Computing*, *19*(1), 83–86. https://doi.org/10.1109/MPRV.2020.2966338

Sikora-Fernandez, D. (2018). Smarter cities in post-socialist country: Example of Poland. *Cities*, *78*, 52–59. https://doi.org/10.1016/j.cities.2018.03.011

Smart Cities Council. (2012). *Our vision*. https://www.smartcitiescouncil.com/article/our-vision

Sobczak, A. (2012). Architektura korporacyjna państwa jako narzędzie zarządzania cyfrową transformacją organizacji sektora publicznego. *Roczniki Kolegium Analiz Ekonomicznych*, *24*, 263–281.

Sood, A. K. i Zeadally, S. (2016). Drive-by download attacks: A comparative study. *IT Professional*, *18*, 18–25. https://doi.org/10.1109/MITP.2016.85

Sostero, M., Milasi, S., Hurley, J., Fernández-Macías, E. i Bisello, M. (2021). *Telework-ability and the COVID-19 crisis: a new digital divide?* https://econpapers.repec.org/paper/iptlaedte/202005.htm

Spam – definicja, rodzaje, historia powstania oraz sposoby ochrony. (2022). https://poradnikprzedsiebiorcy.pl/-spam-definicja-rodzaje-historia-powstania-oraz-sposoby-ochrony

Stech, B. (2021). *Atak hakerów na strony Urzędu Miasta w Kołobrzegu i serwisy informacyjne. Fake news o morderstwie księdza*. https://koszalin.wyborcza.pl/koszalin/7,179397,27465486,atak-hakerow-na-strone-urzedu-miasta-w-kolobrzegu-zamiescili.html

Stępniewski, R. (2020a). *Co to jest phishing?* https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-phishing

Stępniewski, R. (2020b). *Czym jest botnet?* https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-botnet

Stolterman, E. i Fors, A. (2004). Information technology and the good life. *Proceedings from IFIP 8.2 Manchester Conference*, 687–692. https://doi.org/10.1007/1-4020-8095-6_45

Strategia rozwoju społeczeństwa informacyjnego Województwa Mazowieckiego na lata 2020–2030. (2020). https://geodezja.mazovia.pl/pliki/strategia/strategia-rozwoju-spoleczenstwa-informacyjnego-wm-092020.pdf

Sullivan, C. M. (2003). Using the ESID model to reduce intimate male violence against women. *American Journal of Community Psychology*, *32*, 295–303. https://psycnet.apa.org/record/2003-10373-009

Surowiec, J. (2021). *Kim są zwycięzcy konkursu „Moja SMART wieś. IDEA I FAKT”?* https://ksow.pl/aktualnosc/kim-sa-zwyciezcy-konkursu-moja-smart-wies-idea-i-fakt

Surówka, K. i Owsiak, K. (2018). Administrowanie czy rozwój – 20 lat doświadczeń finansowania polskiego samorządu terytorialnego. *Nierówności społeczne a wzrost gospodarczy*, *56*(4), 23–36. https://doi.org/10.15584/nsawg.2018.4.2

Synowiec, A. (2021). Wieś i obszary wiejskie w kontekście inteligentnego rozwoju – w stronę Smart Village. W: *Miasto, przedsiębiorstwo i społeczeństwo w gospodarce 4.0. Wybrane aspekty* (s. 65–88). CeDeWu.

Szczepaniak, S. (2021). *Prawdziwe oblicze transformacji cyfrowej*. https://wspolnota.org.pl/newsletter/prawdziwe-oblicze-transformacji-cyfrowej

Szczepańska, M. (2017). Innowacje społeczne w polskich miastach. W: A. Kaszkur i A. Laska (red.), *Innowacyjność w warunkach współczesnych miast* (s. 219–228). Wydawnictwo Uniwersytetu Kazimierza Wielkiego.

Szewc, T. (2020). Smart City jako zadanie publiczne. W: I. Jonek-Kowalska i J. Kaźmierczak (red.), *Inteligentny rozwój inteligentnych miast*. CeDeWu.

Sztuczna inteligencja usprawnia obsługę mieszkańców w Gdyni. (b.d.). Pobrane w 2023 r. z https://pfrdlamiast.pl/baza-miejskich-innowacji/gdynia-sztuczna-inteligencja-usprawnia-obsluge-mieszkancow-w-gdyni.html

Szymańska, A. (2019). *Fundusze unijne i europejskie 2007–2013 dla mieszkańców obszarów wiejskich*. Municipium.

Śledziewska, K. i Włoch, R. (2020). *Cyfrowa gospodarka. Jak nowe technologie zmieniają świat*. Wydawnictwo Uniwersytetu Warszawskiego.

Świetlne i gastronomiczne atrakcje Auto Skyway Festival. (b.d.). http://archiwum.tak.torun.pl/a/845

Tadeusz Czajka – wójt gminy Tarnowo Podgórne. (b.d.). https://www.facebook.com/tadeuszczajkatp/

Tarczyńska, J. (2021). *Cyfryzacja administracji publicznej w Polsce*. Uniwersytet Ekonomiczny w Poznaniu.

Teets, J. C. (2012). Reforming service delivery in China: The emergence of a social innovation model. *Journal of Chinese Political Science*, *17*(1), 15–32. https://doi.org/10.1007/s11366-011-9176-9

Telefon Porad Cyfrowych – pomoc dla seniorów. (b.d.). https://rtk.poznan.pl/telefon-porad-cyfrowych-pomoc-dla-seniorow/

Tiebout, C. M. (1956). A pure theory of local expenditures. *Journal of Political Economy*, *64*, 416–424. https://doi.org/10.1086/257839

Tolkiehn, G. U., Lührs, C. i Weigert, P. (2018). *Public transport 4.0 and the alternatives – on a single page*. https://tolkiehn-partner.de/textsrc/Public-transport-4dot0-on-a-single-page-18-08.pdf

Tomaszewicz, A. i Buko, J. (2015). Determinanty rozwou e-administracji publicznej w Polsce. *Zeszyty Naukowe Uniwersytetu Szczecińskiego*, *852*, 643–651.

Townsend. L., Sathiaseelan, A. i Wallace, C. (2013). Enhanced broadband access as a solution to the social and economic problems of the rural digital divide. *Local Economy*, *28*(6), 580–595. https://doi.org/10.1177/0269094213496974

Transformacja cyfrowa – czym jest i po co to robić? (2022). https://global4net.com/ecommerce/transformacja-cyfrowa-czym-jest-i-po-co-to-robic/

Tremblay, D. i Pilati, T. (2013). Social innovation through arts and creativity. W: F. Moulaert, D. MacCallum, A. Mehmood i A. Hamdouc (Eds.), *International handbook*

on social innovation. social innovation, collective action and transdisciplinary research (s. 67–79). Edward Elgar. https://doi.org/10.4337/9781849809993.00015

UN (United Nations). (1987). *Our common future. Report of the World Commission on Environment and Development*. https://www.are.admin.ch/are/en/home/media/publications/sustainable-development/brundtland-report.html

UN (United Nations). (2019). *Value creation and capture: Implications for developing countries*. Digital Economy Report 2019. https://unctad.org/system/files/official-document/der2019_en.pdf

UN (United Nations). (2020). About the Sustainable Development Goals-United Nations Sustainable Development. United Nations. www.un.org/sustainabledevelopment/sustainable-development-goals/

UN (United Nations). (2021). *Cross-border data flows and development: For whom the data flow*. Digital Economy Report 2021. https://unctad.org/system/files/official-document/der2021_en.pdf

UNESCO (Organizacja Narodów Zjednoczonych do spraw Oświaty, Nauki i Kultury). (2009). *Guide to measuring information and communication technologies (ICT) in education*. https://unesdoc.unesco.org/ark:/48223/pf0000186547

Ustawa. (2003). Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (tekst jedn. Dz. U. z 2022 r., poz. 503).

Ustawa. (2009). Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jedn. Dz. U. z 2009 r., poz. 1240).

Ustawa. (2005). Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz. U. z 2021 r., poz. 2070 ze zm.).

Ustawa. (2009). Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jedn. Dz. U. z 2022 r., poz. 1634 ze zm.).

Ustawa. (2010a). Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (tekst jedn. Dz. U. z 2022 r., poz. 884 ze zm.).

Ustawa. (2010b). Ustawa z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym (tekst jedn. Dz. U. z 2022, poz. 1343).

Ustawa. (2014). Ustawa z dnia 21 lutego 2014 r. o funduszu sołeckim (Dz. U. z 2014 r., poz. 301).

Ustawa. (2018). Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2022 r., poz. 1863).

Ustawa. (2019). Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r., poz. 848).

Ustawa. (2020). Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (tekst jednolity Dz. U. z 2022 r., poz. 569 ze zm.).

Ustawa. (2021). Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2021 r., poz. 1641).

van der Meulen, N., Jo, E. i Soesanto, S. (2015). *Cybersecurity in the European Union and beyond: Exploring the threats and policy responses*. https://doi.org/10.7249/rr1354

van Deursen, A. J. A. M. i Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? *Communication and Information Technologies Annual: Studies in Media and Communications*, *10*, 29–52. https://doi.org/10.1108/S2050-206020150000010002

van Dijk, J. A. G. M. (2006). Digital divide research, achievements and shortcomings. *Poetics*, *34*(4–5), 221–235. https://doi.org/10.1016/j.poetic.2006.05.004

van Dijk, J. (2013). Ewolucja wykluczenia cyfrowego. Od dostępu po kompetencje i użytkowanie. W: M. Pokrzywa i S. Wilk (red.), *Wykluczenie społeczne: Diagnoza, wymiary i kierunki badań* (s. 207–232). Wydawnictwo Uniwersytetu Rzeszowskiego.

van Dijk, J. (2020). *The digital divide*. Polity Press.

Warschauer, M. (2004). *Technology and social inclusion*. The MIT Press. https://doi.org/10.7551/mitpress/6699.001.0001

Wasserman, I. M. i Richmond-Abbott, M. (2005). Gender and the internet: Causes of variation in access, level, and scope of use. *Social Science Quarterly*, *86*(1), 252–270. https://www.jstor.org/stable/42956060#metadata_info_tab_contents

Węgrzyn, G. i Miłaszewicz, D. (2017). Sektor usług w gospodarce opartej na wiedzy – analiza porównawcza. *Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania*, *47*(3), 433–444. https://doi.org/10.18276/SIP.2017.47/3-34

Wiatrak, A. P. (2004). Inicjatywy wspólnotowe w Unii Europejskiej jako narzędzia wyrównywania różnic w rozwoju regionalnym. *Nierówności Społeczne a Wzrost Gospodarczy*, *5*, 33–43.

Wilk, S. (2014). *E-administracja w społeczeństwie informacyjnym. Model a rzeczywistość na przykładzie województwa podkarpackiego*. Wydawnictwo Uniwersytetu Rzeszowskiego.

Wiśniewski, D. (2014). Bezpieczeństwo informacji oraz ochrona przed ich wyciekiem na przykładzie wybranego urzędu miejskiego. *Przedsiębiorczość i Zarządzanie*, *15*(9), 129–146. http://piz.san.edu.pl/docs/e-XV-9-1.pdf

Wojtasiewicz, L. (2004). O potrzebie zmian w modelu działalności samorządu terytorialnego w Polsce. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, *LXVI*(2), 115–128.

Yuan, Z. i Jia, G. (2021). Profiling the digital divide of the elderly based on internet big data: evidence from China. *Data Science and Management*, *3*, 33–43. https://doi.org/10.1016/j.dsm.2021.10.001

Zespół Szkół Technicznych Tarnowo Podgórne. (2021). https://zst-tp.pl/

Zhang, X. (2013). Income disparity and digital divide: The internet Consumption Model and cross-country empirical research. *Telecommunications Policy*, *37*(6–7), 515–529. https://doi.org/10.1016/j.telpol.2012.12.011

Zhenfang, Z. (2015). Study on computer Trojan horse virus and its prevention. *International Journal of Engineering and Applied Sciences*, *2*(8), 95–96.

Zhu, Z., Lu, G., Chen, Y., Fu, Z. J., Roberts, P. i Han, K. (2008). Botnet research survey. *2008 32nd Annual IEEE International Computer Software and Applications Conference*, 967–972. https://doi.org/10.1109/COMPSAC.2008.205

Ziemba, E. (red.). (2018). *Czynniki sukcesu i poziom wykorzystania technologii informacyjno-komunikacyjnych w Polsce* (2 wyd.). CeDeWu.

Ziemba, E., Papaj, T. i Descours, D. (2015). Krytyczne czynniki sukcesu i poziom wykorzystania ICT w administracji publicznej. W: *Czynniki sukcesu i poziom wykorzystania technologii informacyjno-komunikacyjnych w Polsce* (s. 147–226). CeDeWu.

Zillien, N. i Hargittai, E. (2009). Digital distinction: Status-specific types of internet usage. *Social Science Quarterly*, *90*(2), 274–291. http://www.jstor.org/stable/42940587

ZUCH. System Zapewniania Usług Chmurowych. (2021). https://chmura.gov.pl/zuch
Zwęglińska-Gałecka, D. (2020). Koronakryzys. Lokalne zróżnicowanie globalnej pandemii. *Wieś i Rolnictwo*, *3*(188), 67–90. https://doi.org/10.53098/wir032020/04

SPIS TABEL

SPIS RYSUNKÓW

DIGITAL TRANSFORMATION OF LOCAL GOVERNMENT IN POLAND

(Summary)

The monograph focuses on the conditions, barriers, sources of financing and aspects of the digital transformation of municipalities. Its purpose is to diagnose the use of new information and communication technologies by municipalities and thus prepare them to function in the economy 4.0.

Economy 4.0 is an economy of huge amounts of data. These data are collected, transmitted, processed and analysed with the help of newer information and communication technologies. The rapid development of these technologies has forced various entities to adapt to functioning in the new reality. Not only enterprises, financial institutions, households, but also authorities and public administration units are entering the path of digital transformation. The digital metamorphosis of municipalities is also of great importance. This transformation should be understood as changes taking place in local government using information and communication technologies. Digital transformation concerns resources, services, processes, organizational culture and competences. It is carried out in order to enhance the quality of public services, improve the work of the office, support decision-making processes, increase the transparency of the activities of municipalities, involve residents in the life of the local community, local government and strive for a sustainable development.

The degree of the digital transformation of municipalities so far varies. The conducted research shows that among urban, rural, urban-rural municipalities and municipalities with county rights, the latter are best prepared to function in economy 4.0. However, in each category of municipalities there are those that actively look for the possibility of using information and communication technologies to provide services. At the same time they encounter financial, socio-cultural, technological and organizational barriers. Nevertheless, to a certain extent municipalities change almost overnight in order to more effectively meet the needs of their residents. The research results confirm that the local government can be perceived as a laboratory for testing technological and social innovations, which, if successful, constitute a model to follow or are directly adapted by other local government units and even the central government administration.

Keywords: economy 4.0, digital transformation, municipalities.

Tematem monografii są warunki, bariery, źródła finansowania oraz przejawy transformacji cyfrowej gmin. Jej celem jest diagnoza wykorzystywania przez gminy nowych technologii informacyjno-komunikacyjnych, a tym samym ich przygotowania do funkcjonowania w gospodarce 4.0.

Gospodarka 4.0 to gospodarka ogromnych ilości danych, które są gromadzone, przetwarzane, analizowane i archiwizowane za pomocą coraz nowszych technologii informacyjno-komunikacyjnych. Szybki rozwój tych technologii wymusił konieczność przystosowania się różnych podmiotów do funkcjonowania w nowych realiach. Na ścieżkę transformacji cyfrowej wstępują nie tylko przedsiębiorstwa, instytucje finansowe, gospodarstwa domowe, ale też organy władzy i administracji publicznej (na przykład gminy). Dotyczy ona zasobów, usług, procesów, kultury organizacyjnej oraz kompetencji, a służy podnoszeniu jakości usług publicznych, usprawnieniu pracy urzędu, wsparciu procesów podejmowania decyzji, zwiększeniu przejrzystości działania gmin, angażowaniu mieszkańców w życie wspólnoty lokalnej, samorządowej oraz dążeniu do zrównoważonego rozwoju.

Różny jest stopień dotychczasowej transformacji cyfrowej gmin. Z przeprowadzonych badań wynika, że jednostkami najlepiej przygotowanymi do funkcjonowania w gospodarce 4.0 są miasta na prawach powiatu. Jednak w każdej kategorii gmin znajdują się takie, które aktywnie poszukują możliwości zastosowania technologii informacyjno-komunikacyjnych do świadczenia usług, choć napotykają bariery finansowe, społeczno-kulturowe, technologiczne i organizacyjne.

ISBN 978-83-8211-165-1