MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 18 czerwca 2026 r.

Poz. 620

UCHWAŁA NR 130
RADY MINISTRÓW

z dnia 9 czerwca 2026 r.

w sprawie przyjęcia strategii dotyczącej informatyzacji państwa

Na podstawie art. 12aa ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160) Rada Ministrów uchwala, co następuje:

§ 1. Przyjmuje się strategię dotyczącą informatyzacji państwa, zwaną „Strategią Cyfryzacji Państwa", stanowiącą załącznik do niniejszej uchwały.

§ 2. Uchwała wchodzi w życie z dniem następującym po dniu ogłoszenia.

Prezes Rady Ministrów: *D. Tusk*

Załącznik do uchwały nr 130 Rady Ministrów
z dnia 9 czerwca 2026 r. (M.P. poz. 620)

Strategia Cyfryzacji Państwa

Spis treści

I. Wstęp

Strategia Cyfryzacji Państwa, zwana dalej „Strategią”, stanowi pierwszą w historii Polski kompleksową strategię cyfryzacji kraju. W ostatnich latach cyfryzacja stopniowo przestaje być postrzegana jako odrębny obszar działalności państwa czy wręcz sektor gospodarki podobny do wielu innych. Coraz częściej jest dostrzegany jej horyzontalny charakter, oddziałujący na niemal wszystkie obszary funkcjonowania społeczeństwa, państwa i gospodarki. Sfera technologii cyfrowych jest kluczowym polem nasilającej się rywalizacji geopolitycznej, a inwestycje w tej dziedzinie pośrednio (za sprawą technologii podwójnego zastosowania) lub bezpośrednio przekładają się na poziom bezpieczeństwa państwa.

Przed Polską realizacja kluczowych celów na najbliższą dekadę. Cele te muszą uwzględniać między innymi zmieniający się krajobraz bezpieczeństwa państwa i środowiska międzynarodowego, aktualne trendy i wyzwania w obszarze technologii i jej regulacji, a także specyfikę polskiego społeczeństwa i gospodarki. Polskie ambicje i działania wpisują się w kontekst zauważalnego w ostatnich latach wzrostu znaczenia cyfryzacji na liście priorytetów Unii Europejskiej.

Niniejsza Strategia stanowi ponadsektorowy dokument strategiczny w dziedzinie informatyzacji państwa, określający nadrzędny cel, jakim jest poprawa jakości życia obywateli przez cyfryzację do 2035 r. Jego realizacja jest możliwa tylko dzięki interwencji w szereg obszarów, wykraczających poza tradycyjnie definiowany dział administracji rządowej – informatyzacja[1]. Cele zaplanowane do realizacji obejmują szerokie spektrum zagadnień, począwszy od kwestii horyzontalnych, przez płaszczyznę państwa i jego obywateli, na gospodarce i rozwoju technologii kończąc. Takie podejście pozwoliło na stworzenie nowoczesnej, przekrojowej i odpowiadającej na aktualne wyzwania wizji rozwoju cyfrowego, bazującej na aktualnych trendach europejskich i globalnych, wynikającej z diagnozy aktualnego stanu informatyzacji państwa oraz odpowiadającej na formułowane oczekiwania społeczne.

W początkowych rozdziałach Strategii zawarte zostały: diagnoza stanu informatyzacji opracowana na postawie wyników międzynarodowych wskaźników i badań, wyzwania i trendy, które miały wpływ na określanie kierunków interwencji, analiza silnych i słabych stron, a także szans i zagrożeń dla cyfryzacji Polski oraz ambitna wizja transformacji cyfrowej do 2035 r. wraz prezentacją nadrzędnego celu Strategii i uwarunkowań niezbędnych do jego realizacji.

Dalsza część dokumentu obejmuje obszary horyzontalne, które, ze względu na rangę i znaczenie, istotnie wpływają na efektywność działań w innych obszarach i stanowią punkt wyjścia dla transformacji cyfrowej wielu dziedzin życia społeczno-gospodarczego. Do takich obszarów zaliczono: komunikację elektroniczną, kompetencje przyszłości, cyberbezpieczeństwo oraz koordynację transformacji cyfrowej.

Pozostałe cele Strategii zostały pogrupowane w 23 obszary, podzielone na 3 płaszczyzny: państwo, ludzie oraz gospodarka i technologie. Cele w ramach płaszczyzny „państwo”

[1] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2025 r. poz. 1275, z późn. zm.).

koncentrują się na zwiększeniu i poprawie jakości świadczenia e-usług publicznych, cyfryzacji procesów administracyjnych i postępowań sądowych, optymalizacji funkcjonowania systemów i rejestrów, rozwoju cyfrowej tożsamości, wykorzystaniu chmury obliczeniowej oraz wzmocnieniu otwartości danych i wymiany danych. Cele w ramach płaszczyzny „ludzie" dotyczą nie tylko bezpieczeństwa przestrzeni cyfrowej, ale zgodnie ze zdefiniowanymi wyzwaniami i potrzebami, obejmują również działania w zakresie cyfrowego zdrowia, rozwoju branż kreatywnych, digitalizacji zasobów kultury i nauki oraz rozwoju akademii i nauki w odniesieniu do sektora cyfrowego. Cele w ramach najbardziej przekrojowej płaszczyzny „gospodarka i technologie" koncentrują się na: zagadnieniach cyfrowej transformacji przedsiębiorstw, w tym działaniach wspierających ten proces oraz dotyczących rozwoju e-usług dla przedsiębiorców, priorytetach w zakresie rozwoju sztucznej inteligencji i innych technologii przełomowych, rozwoju technologii kosmicznych, a także finansowaniu i wsparciu innowacji oraz open source. W tej części również zostały określone wyzwania, cele i działania w obszarach cyfrowej i zielonej transformacji oraz przemian cyfrowych w rolnictwie.

Struktura wszystkich obszarów została ujednolicona i zawiera szczegółową diagnozę (jak jest?) pogłębioną w stosunku do szerszego spojrzenia z obszarów wstępnych, cele odpowiadające sformułowanym problemom i deficytom (jak powinno być?) oraz konkretne środki i działania, które pozwolą na osiągnięcie pożądanego stanu (co umożliwi realizację celu?). W Strategii można znaleźć również odnotowane wymierne i realne korzyści, jakie obywatel czy przedsiębiorca uzyska po skutecznym wdrożeniu zaplanowanych działań i realizacji zamierzonych celów. Stanowią one przykłady, w jaki sposób podniesie się jakość życia, tj. nadrzędny cel Strategii.

W ostatnim rozdziale został opisany system wdrażania Strategii, odnoszący się do sposobu i zasad współpracy podmiotów, których dotyczy proces informatyzacji, oraz jej koordynacji, jak również możliwości finansowania działań. Szczególna rola w tym zakresie została przypisana pełnomocnikom do spraw informatyzacji oraz Komitetowi do spraw Cyfryzacji, który zastąpił Komitet Rady Ministrów do Spraw Cyfryzacji. Zaplanowano także opracowanie, cyklicznie aktualizowanego, planu wdrożeniowego. Realizacja ambitnej wizji Strategii wymaga wdrożenia spójnych, zharmonizowanych i konsekwentnych działań, przy ścisłej współpracy interesariuszy. Monitorowanie Strategii będzie obejmowało mierzenie postępów w realizacji określonych celów, w całym cyklu życia Strategii, oraz z wykorzystaniem wskaźników efektywności ujętych w zestawieniu w rozdziale VII Strategii. Zadanie to zostanie powierzone ministrowi właściwemu do spraw informatyzacji, przy zaangażowaniu pozostałych członków Rady Ministrów. Biorąc pod uwagę zasady zarządzania strategicznego oraz tempo rozwoju technologicznego, jest planowana również regularna ewaluacja i aktualizacja Strategii.

Wdrażanie Strategii nie może odbywać się w oderwaniu od otoczenia strategicznego, zarówno krajowego, jak i unijnego. Sformułowane w Strategii cele znajdują odzwierciedlenie w horyzontalnym dokumencie odnoszącym się do polityki rozwoju państwa, zarysowującym wizję rozwoju kraju w długookresowej perspektywie - Koncepcji Rozwoju Kraju 2050. Natomiast cele te zostały uszczegółowione (lub zostaną w nowych wersjach) w szeregu dokumentów z obszaru cyfryzacji, takich jak Strategia Cyberbezpieczeństwa

Rzeczypospolitej Polskiej[2], Narodowy Plan Szerokopasmowy[3] (aktualizacja w 2026 r.), Program Rozwoju Kompetencji Cyfrowych[4] (aktualizacja w 2026 r.) Program Otwierania Danych[5] (obecnie obowiązujący na lata 2021-27), Polityka Rozwoju Sztucznej Inteligencji[6] (obecnie obowiązująca od 2020 r., planowana aktualizacja w 2026 r.).

Na sposób sformułowania Strategii przekładają się też wnioski z realizacji Programu Zintegrowanej Informatyzacji Państwa[7] (PZIP). Realizowany w latach 2014-2024 PZIP był do niedawna głównym dokumentem strategicznym warunkującym cyfrowy rozwój państwa. Przewidziane w PZIP działania przyczyniły się do corocznego postępu w zwiększaniu jakości i zakresu komunikacji między obywatelami a państwem, wzmocnieniu dojrzałości organizacyjnej jednostek administracji publicznej oraz podniesieniu kompetencji cyfrowych obywateli, specjalistów IT i pracowników administracji. Jednak na przestrzeni lat obowiązywania, aktualizacja PZIP nie obejmowała wyznaczenia nowych kierunków transformacji oraz określenia nowych wskaźników (część z nich stała się bowiem nieaktualna w świetle zmian metodologii czy odstąpienia GUS od ich badania). Utrudniona była również aktualizacja planu działań będącego częścią PZIP, ze względu na konieczność przeprowadzenia procesu legislacyjnego. W otoczeniu strategicznym PZIP nastąpiły istotne zmiany determinujące konieczność określenia na nowo kierunków transformacji cyfrowej kraju oraz wyznaczenia ambitnych celów i wskaźników odpowiadających aktualnym wyzwaniom w obszarze cyfryzacji, w szczególności w zakresie efektywnego świadczenia dojrzałych e-usług oraz współpracy i koordynacji działań, a także skutecznego zarządzania procesem cyfryzacji na poziomie całego państwa.

Co więcej, z uwagi na przekrojowy i ponadsektorowy charakter Strategii, zawarte w niej kierunki transformacji cyfrowej należy rozpatrywać w kontekście innych sektorowych dokumentów strategicznych, w tym np. Polityki Cyfrowej Transformacji Edukacji[8], Strategii Produktywności 2030[9], Polityki Energetycznej Polski do 2040 r.[10], Strategii Zrównoważonego Rozwoju Transportu do 2030 roku[11], Strategii migracyjnej na lata 2025-30[12] czy Strategii na

[2] Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. poz. 309).
[3] Uchwała nr 2/2014 Rady Ministrów z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju „Narodowy Plan Szerokopasmowy", zmieniona uchwałą nr 27/2020 Rady Ministrów z dnia 10 marca 2020 r. (niepublikowana).
[4] Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych" (M.P. poz. 318).
[5] Uchwała nr 28 Rady Ministrów z dnia 18 lutego 2021 r. w sprawie Programu otwierania danych na lata 2021–2027 (M.P. poz. 290).
[6] Uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 r. w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020" (M.P. z 2021 r. poz. 23).
[7] Uchwała nr 1/2014 Rady Ministrów z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju „Program Zintegrowanej Informatyzacji Państwa", zmieniona uchwałą nr 117/2016 Rady Ministrów z dnia 27 września 2016 r., uchwałą nr 109/2019 Rady Ministrów z dnia 24 września 2019 r., uchwałą nr 255/2022 Rady Ministrów z dnia 16 grudnia 2022 r. oraz uchwałą nr 232/2023 Rady Ministrów z dnia 23 listopada 2023 r. (niepublikowana).
[8] Uchwała nr 98 Rady Ministrów z dnia 12 września 2024 r. w sprawie przyjęcia polityki publicznej pod nazwą „Polityka Cyfrowej Transformacji Edukacji" (M.P. poz. 812).
[9] Uchwała nr 154 Rady Ministrów z dnia 12 lipca 2022 r. w sprawie przyjęcia „Strategii Produktywności 2030" (M.P. poz. 926).
[10] Uchwała nr 22/2021 Rady Ministrów z dnia 2 lutego 2021 r. w sprawie „Polityki energetycznej Polski do 2040 r." (niepublikowana).
[11] Uchwała nr 105 Rady Ministrów z dnia 24 września 2019 r. w sprawie przyjęcia „Strategii Zrównoważonego Rozwoju Transportu do 2030 roku" (M.P. poz. 1054).
[12] Uchwała nr 120 Rady Ministrów z dnia 15 października 2024 r. w sprawie przyjęcia dokumentu „Odzyskać kontrolę. Zapewnić bezpieczeństwo. Kompleksowa i odpowiedzialna strategia migracyjna Polski na lata 2025–2030 " (niepublikowana).

rzecz Osób z Niepełnosprawnościami 2021-2030[13]. Odnosząc się do europejskich ram strategicznych transformacji cyfrowej, dokument uwzględnia i poszerza cele zarysowane w ramach programu polityki „Droga ku cyfrowej dekadzie do 2030 r."[14]. Strategia obejmuje jednak obszary nieuwzględnione w unijnych celach, ma też bardziej odległy, sięgający 2035 r., horyzont czasowy.

Strategię opracowano w Ministerstwie Cyfryzacji we współpracy z innymi urzędami administracji rządowej oraz z uwzględnieniem postulatów interesariuszy społecznych i środowisk biznesowych. Zastąpi Program Zintegrowanej Informatyzacji Państwa i będzie stanowić podstawę strategiczną dla wydatkowania europejskich funduszy przeznaczonych na cyfryzację, a tym samym będzie wyznaczała kierunek negocjacji obejmujących nadchodzącą perspektywę finansową.

Wyzwania stojące przed Polską w obszarach konkurencyjności gospodarki, demografii, bezpieczeństwa państwa i jego obywateli czy zdrowia sprawiają, że intensywne inwestowanie w cyfryzację w wielu obszarach, a także zwiększenie poziomu suwerenności cyfrowej, przestaje być kwestią wyboru. Staje się koniecznością, bez której pozycja naszego kraju wyraźnie osłabnie. Jeżeli jednak cyfryzacji zostanie nadany odpowiadający jej znaczeniu priorytet, zyskają nie tylko poszczególni obywatele i obywatelki – których jakość życia poprawi się – ale i Polska jako całość.

[13] Uchwała nr 27 Rady Ministrów z dnia 16 lutego 2021 r. w sprawie przyjęcia dokumentu Strategia na rzecz Osób z Niepełnosprawnościami 2021-2030 (M.P. poz. 218).
[14] Uchwała nr 125 Rady Ministrów z dnia 22 października 2024 r. w sprawie Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. (M.P. poz. 989).

II. Wizja

Nieustannie przyspieszający rozwój technologiczny sprawia, że planowanie działań w obszarze cyfryzacji w perspektywie kolejnej dekady jest zadaniem niezwykle trudnym. Tym trudniejszym, że technologie cyfrowe przenikają niemal każdy aspekt ludzkiego życia, a co za tym idzie – wymagają bliskiej współpracy całej administracji. Ta współpraca jest możliwa, gdy kieruje nią wspólna wizja. Niniejszy dokument zarysowuje taką wizję dla całego państwa, a także działania prowadzące do jej realizacji.

Wizja na 2035 r. koncentruje się na człowieku i tym, jak najskuteczniej poprawić jakość życia obywateli. Za dziesięć lat wizyta w urzędzie będzie czymś wyjątkowym – wszystkie kluczowe usługi będą dostępne przez telefon, z każdego miejsca. Państwowe systemy same wykryją, że jakieś działanie powinno być podjęte i zaproponują rozwiązanie. Obywatel czy przedsiębiorca nigdy nie będzie musiał dwa razy podawać tych samych danych – urzędy same się nimi wymienią dzięki pełnej interoperacyjności systemów teleinformatycznych i rejestrów publicznych. Dzięki planowanej poprawie koordynacji między różnymi częściami administracji unikniemy dublowania rozwiązań i niespójności, a tym samym marnowania publicznych pieniędzy.

Intensywny rozwój cyfrowej administracji wymaga inwestycji – w infrastrukturę, w kompetencje urzędników, i w zapewnienie najwyższego poziomu bezpieczeństwa systemów państwowych oraz innych systemów mających dla państwa istotne znaczenie. To szczególnie ważne wobec poważnego pogorszenia międzynarodowej sytuacji bezpieczeństwa i wzrostu cyberprzestępczości. Ale bezpieczeństwo postrzegamy znacznie szerzej – również w kontekście zdrowia psychicznego czy ochrony obywateli przed szkodliwymi treściami. Dlatego wiemy, że polscy obywatele muszą mieć nie tylko wysokie kompetencje w korzystaniu z technologii cyfrowych, ale też świadomość, jak korzystać z nich w zdrowy i racjonalny sposób, a czasem – kiedy warto się po prostu odłączyć. Rozwój sfery cyfrowej musi być zrównoważony – z perspektywy psychologicznej, pracowniczej i klimatycznej. Jednocześnie należy docenić rolę odgrywaną w tym obszarze przez sektor prywatny i podkreślić dążenie do wzmocnienia polskiej gospodarki cyfrowej. Na harmonijny rozwój cyfrowy kraju składają się bowiem zarówno działania państwa, jak i biznesu. Z tak postrzeganym upowszechnianiem technologii wiąże się ogrom szans na poprawę jakości życia, rozwój polskiej gospodarki i pozycji międzynarodowej. Aby to się udało, będziemy stymulować adopcję technologii – przede wszystkim sztucznej inteligencji – w administracji i wśród przedsiębiorstw z różnych branż, a także wzmocnimy konkurencyjność polskich firm technologicznych oraz eksport usług cyfrowych Zapewnimy lepsze ramy do rozwoju technologii na uczelniach i w gospodarce, a także będziemy stymulować procesy wymiany wiedzy i kadr między biznesem a nauką. Poprawimy ponadto jakość pracy w akademii i rozwiniemy infrastrukturę dla polskiej nauki.

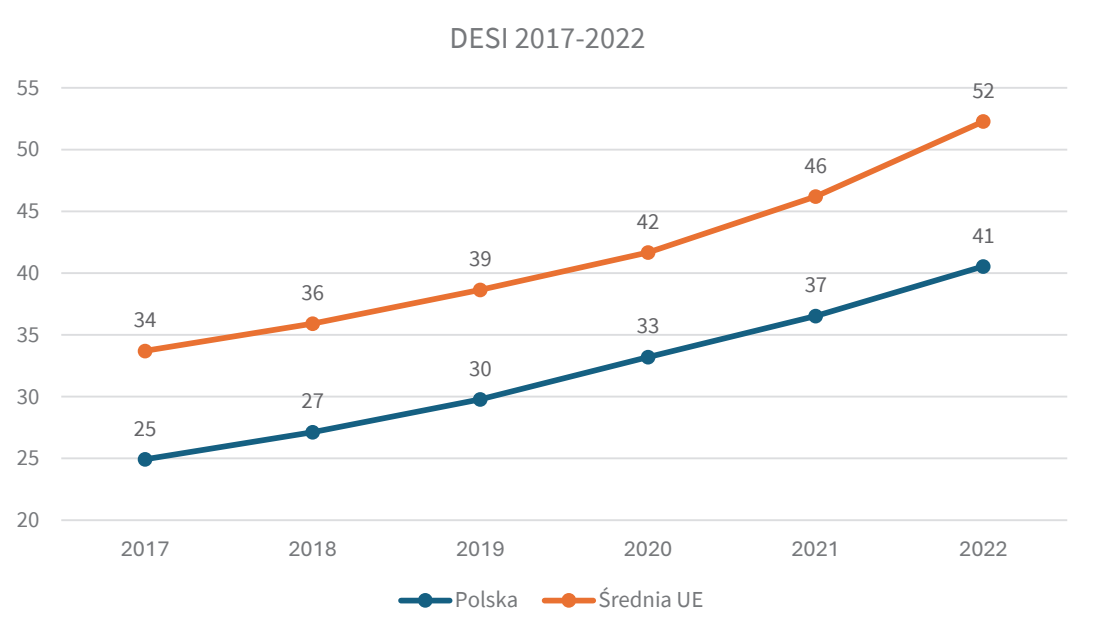
Polska cyfryzacja ma wiele obszarów, z których możemy być dumni, ale nie jesteśmy jeszcze liderem Europy ani tym bardziej świata. Uspójnienie wizji, realizacja przewidzianych w niej działań i znaczne zwiększenie środków przeznaczanych na cyfryzację pozwoli zmienić ten stan rzeczy. Za dziesięć lat Polska będzie prawdziwym cyfrowym liderem.

III. Diagnoza

Cyfrowe państwo

DESI (ang. Digital Economy and Society Index, *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego*)

Wyniki indeksu DESI z lat 2017-2022 wskazują, że każdego roku Polska zajmowała 24. miejsce wśród 27 państw członkowskich UE. Luka cyfrowa jest widoczna we wszystkich badanych obszarach, takich jak kompetencje cyfrowe, telekomunikacja, transformacja cyfrowa przedsiębiorstw i cyfrowe usługi publiczne. Jednak postęp w dziedzinie cyfryzacji staje się coraz bardziej widoczny. **Na przestrzeni 5 lat Polska poprawiła swój wynik z 25 pkt w 2017 r. do 41 pkt w 2022 r., będąc tym samym w czołówce państw najintensywniej nadrabiających dystans do liderów.** Zgodnie z analizą Polskiego Instytutu Ekonomicznego[15] punktacja Polski w indeksie DESI w tym okresie wzrosła z 52,1% do 58,3% punktacji lidera. Jednocześnie niepokoi fakt, że dystans dzielący Polskę od średniej unijnej sukcesywnie rośnie.



Wykres 1. DESI 2017-2022, *źródło: opracowanie własne na podstawie raportów DESI 2017-2022*

[15] https://pie.net.pl/polska-wsrod-unijnych-liderow-postepu-w-rozwoju-cyfryzacji/.

Od 2023 r., zgodnie z założeniami unijnego programu polityki „Droga ku cyfrowej dekadzie" do 2030 r., DESI jest włączany do sprawozdania na temat stanu realizacji programu[16]. Komisja Europejska zrezygnowała z tworzenia rankingu państw członkowskich, udostępniając jednocześnie narzędzie[17] do porównywania wyników państw względem siebie i średniej UE w poszczególnych wskaźnikach. W 2024 r. Polska osiągnęła wyższe wyniki niż średnia UE w 8 na 31 wskaźników: przedsiębiorstwa oferujące szkolenia w zakresie ICT, łączność szerokopasmowa, wykorzystywanie stałych łączy szerokopasmowych o prędkości co najmniej 100Mb/s, zasięg stałych sieci o bardzo dużej przepływności, zasięg technologii „światłowód do lokalu" (FTTP, ang. Fibre to the premises), przedsiębiorstwa korzystające z chmury, przejrzystość przy świadczeniu usług, projektowaniu i danych osobowych oraz dostęp do e-dokumentacji medycznej.

W ostatnim sprawozdaniu z realizacji programu polityki „Droga ku cyfrowej dekadzie" do 2030 r.[18] odnotowano znaczne postępy w obszarze łączności gigabitowej. W przypadku wskaźnika zasięgu sieci o bardzo wysokiej przepustowości **Polska z wynikiem 83,8% objętych gospodarstw domowych przekracza średnią UE (wynoszącą 82,5%)** i jest na dobrej drodze do osiągnięcia 100% zasięgu do 2030 r. Wskaźniki KPI dotyczące cyfryzacji przedsiębiorstw są poniżej średniej unijnej, **wartość wskaźnika wykorzystania sztucznej inteligencji w przedsiębiorstwach wzrosła z 3,7% do 5,9%**, osiągając tempo wzrostu zbliżone do średniej UE. Utrzymywanie się wyzwań w obszarze transformacji cyfrowej przedsiębiorstw jest spowodowane niedoborem specjalistów, wysokimi kosztami, brakiem odpowiedniego finansowania, czy brakiem motywacji wśród przedsiębiorców do wdrażania rozwiązań cyfrowych w połączeniu z niską świadomością potencjalnych korzyści. Ponadto w sprawozdaniu zauważono, że **Polska czyni postępy w takich obszarach jak obliczenia kwantowe – instalacja pierwszego komputera kwantowego – i sztuczna inteligencja, gdzie w 2025 r. został udostępniony pierwszy polski duży model językowy PLLuM, a kraj jest częścią konsorcjum, które zostało gospodarzem fabryki sztucznej inteligencji[19].** Komisja Europejska odnotowała również priorytetowe znaczenie cyberbezpieczeństwa dla polskiej administracji, która wdraża środki mające na celu zwiększenie bezpieczeństwa zarówno w wymiarze technicznym, jak i kompetencyjnym. Polska osiąga wciąż niezadowalające wyniki w zakresie umiejętności cyfrowych i wdrażania zaawansowanych technologii. Rezultat Polski w unijnym sprawozdaniu we wskaźniku *co najmniej podstawowe umiejętności cyfrowe* wynosi 44,3%, co jest poniżej średniej UE, równej 55,6%. Polska osiąga wartość poniżej średniej UE także we wskaźnikach takich jak p*onadpodstawowe umiejętności cyfrowe* (PL 20%, UE 27%) i c*o najmniej podstawowe umiejętności tworzenia treści cyfrowych* (PL 60%, UE 68%).

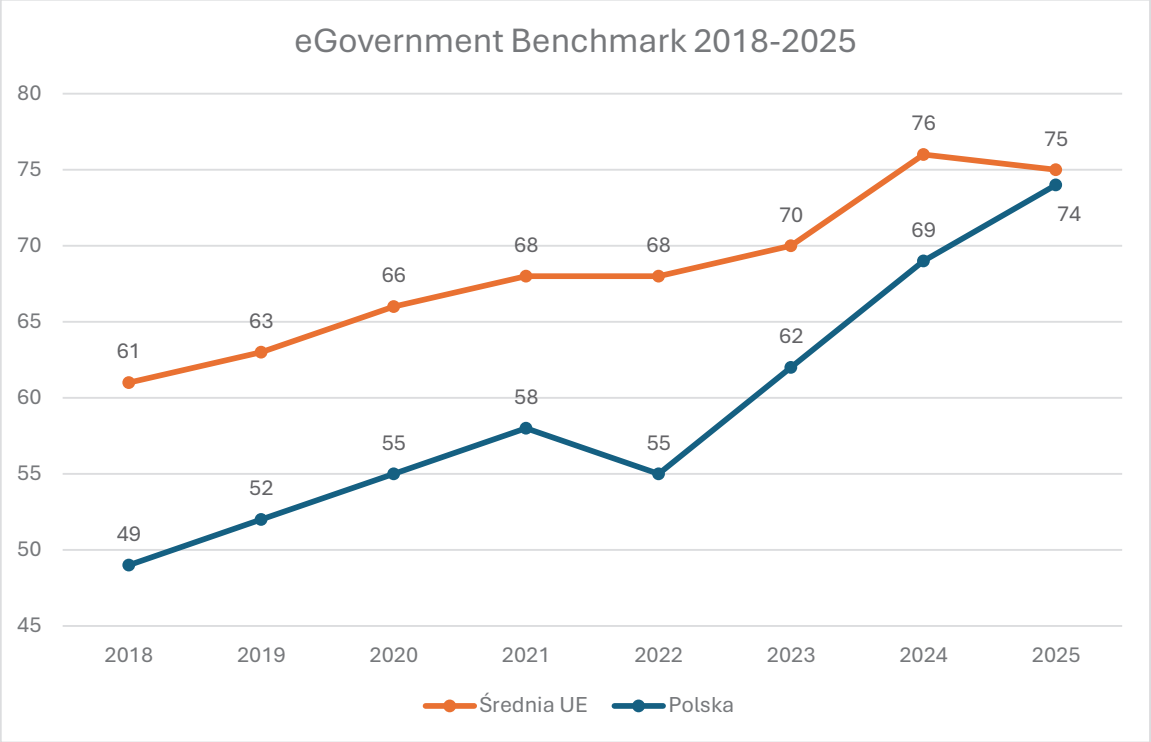
Raport w kontekście europejskim zwraca uwagę na poczynione dotychczas postępy oraz wzrost znaczenia strategicznego myślenia w całej UE. Pilnej uwagi wymagają zagrożenia związane z bezpieczeństwem i suwerennością, niewystarczające umiejętności cyfrowe, czy luki w infrastrukturze. Wyzwania te osłabiają tempo i odporność transformacji cyfrowej.

[16]https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports.
[17] https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dsk_dcc_bab&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK.
[18] https://digital-strategy.ec.europa.eu/en/factpages/poland-2024-digital-decade-country-report.
[19] Dane pochodzą ze sprawozdania opublikowanego w 2025 r. Aktualnie Polska jest gospodarzem dwóch fabryk sztucznej inteligencji.

W 2025 r. Komisja Europejska rozpoczęła prace nad przeglądem programu polityki „Droga ku Cyfrowej Dekadzie” do 2030 r.

eGovernment Benchmark

eGovernment Benchmark[20] jest corocznym badaniem, monitorującym wdrożenie cyfrowych usług publicznych we wszystkich krajach europejskich. W 2025 r. wynik Polski wzrósł do 73,7 pkt; zbliżone wyniki osiągają państwa takie jak Belgia, Słowenia, Czechy, Węgry czy Irlandia. Polska mocno zbliżyła się do średniej UE, dystans obecnie wynosi 0,8 pkt.



Wykres 2. Wyniki eGovernment Benchmark 2018-2025*, źródło: opracowanie własne na podstawie wyników badania 2018-2025*

Wskaźniki e-administracji są zogniskowane wokół trzech wymiarów: dostarczanie usług online, wskaźniki interoperacyjności oraz portale przyjazne dla użytkownika. W raporcie z 2025 r. Polska odnotowuje wyniki na poziomie średniej europejskiej lub powyżej niej w 14 z 27 wskaźników. Najwyższe wyniki prezentują wskaźniki: *dostępność online, przyjazność dla urządzeń mobilnych, transgraniczne ePłatności, transgraniczne dostarczanie rezultatów usług*, w*sparcie użytkownika i przejrzystość projektowania usług*. **Największy wzrost**

[20] https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-egovernment-benchmark-2025.

odnotowano we wskaźnikach: *transgraniczna identyfikacja elektroniczna*, *przejrzystość projektowania usług* oraz *transgraniczne wsparcie użytkownika*. Stosunkowo najwyższe wyniki Polska osiągnęła w kategorii dotyczącej wskaźników interoperacyjności, a także portali przyjaznych dla użytkownika. Pod względem klasyfikacji w odniesieniu do tzw. zdarzeń życiowych, największy wzrost punktowy w 2025 r. odnotowano w zdarzeniu życiowym *transport* (wzrost o 19,1 pkt) i *przeprowadzka (*wzrost o 17 pkt). Mimo rosnących wyników Polski w większości zdarzeń życiowych, nadal pozostaje przestrzeń do poprawy, szczególnie w zdarzeniach życiowych *sprawiedliwość* i *edukacja*, gdzie wyniki są poniżej średniej unijnej.

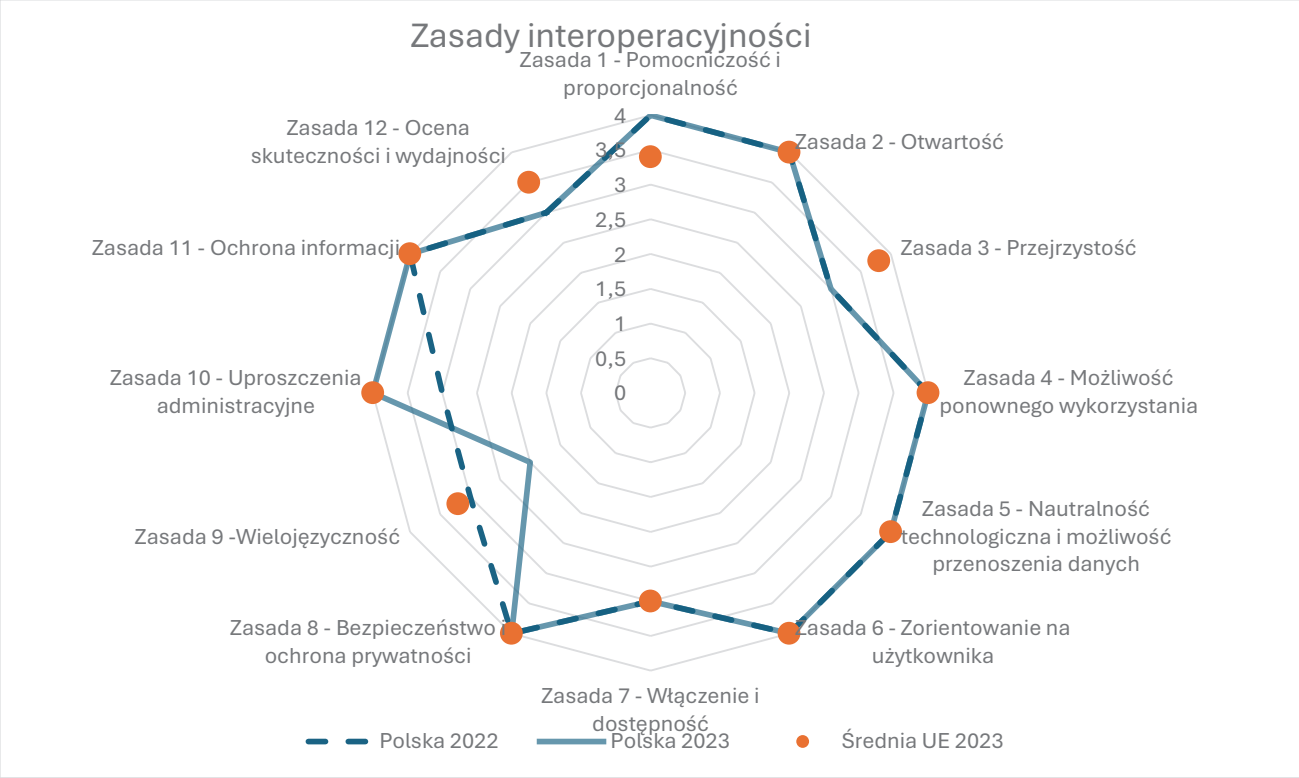
Wnioski z raportu sugerują, że kluczowe w osiągnięciu celów transformacji cyfrowej UE jest **działanie na rzecz wyrównania dysproporcji** między krajami, grupami użytkowników i szczeblami rządowymi **w zakresie integracji i wydajności świadczenia usług cyfrowych**. Ponadto państwa europejskie powinny dążyć do ich **proaktywnego świadczenia**, co oznacza, że obywatel uzyskuje efekt usługi w wyniku automatycznego działania administracji.

DPA (ang. Digital Public Administration Factsheet)

Digital Public Administration Factsheet[21] to unijny raport przedstawiający stan transformacji cyfrowej administracji publicznej ze szczególnym uwzględnieniem aspektów interoperacyjności. Raport jest publikowany corocznie i bazuje na danych przekazywanych przez państwa UE, wskaźnikach Eurostatu, eGoverment Benchmark oraz wynikach uzyskanych w ramach mechanizmu monitorowania Europejskich Ram Interoperacyjności (EIF, ang. European Interoperability Framework).

Na przestrzeni lat 2018-2022 nastąpił stopniowy wzrost we wszystkich wskaźnikach dotyczących cyfrowej administracji publicznej w Polsce. Największy, blisko dwukrotny wzrost (z 21% w 2018 r. do 40% w 2022 r.) dotyczył odsetka osób korzystających z internetu do wysyłania wypełnionych formularzy w kontaktach z administracją publiczną. Zarazem najniższy poziom osiągnął wskaźnik odsetka osób korzystających z internetu w celu pobierania oficjalnych formularzy od administracji publicznej. W 2022 r. zanotowano wzrost jedynie o 7 pkt w stosunku do 2018 r., kiedy odsetek ten wynosił 20%.

[21] https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2024.



Wykres 3. Europejskie Ramy Interoperacyjności, Tablica wyników 1 - Zasady interoperacyjności, *źródło: opracowanie własne na podstawie Digital Public Administration Factsheet 2024*

Według raportu Digital Public Administration Factsheet 2024, Polska poczyniła znaczne postępy w zakresie transformacji cyfrowej administracji publicznej. Wzrost jest widoczny we wszystkich badanych obszarach. W zakresie zasad interoperacyjności Polska osiągnęła wyniki na poziomie średniej unijnej z wyjątkiem zasady 3 *przejrzystość*, zasady 9 *wielojęzyczność*, oraz zasady 12 *ocena skuteczności i wydajności*. Zawarte w raporcie rekomendacje wskazują, że Polska powinna przeznaczać więcej wysiłków na zapewnienie interoperacyjności systemów teleinformatycznych i infrastrukturę techniczną oraz uwzględniać wielojęzyczność przy ustanawianiu europejskich usług użyteczności publicznej. Należy zauważyć, że w 2023 r. zarekomendowano Polsce implementację nowych rozwiązań cyfrowych i optymalizację procesów administracyjnych, a w 2024 r. wynik Polski we wskaźniku *uproszczenia administracyjne* (zasada 10) wzrósł do maksymalnego możliwego poziomu.

Wykres 4. Europejskie Ramy Interoperacyjności, Tablica wyników 4 - Interoperacyjność transgraniczna*, źródło: opracowanie własne na postawie Digital Public Administration Factsheet 2024*

W zakresie interoperacyjności transgranicznej Polska powinna poprawić wyniki we wskaźnikach związanych ze zintegrowanym zarządzaniem usługami publicznymi, a także interoperacyjnością semantyczną, które w obu przypadkach uzyskały wyniki poniżej średniej UE.

DGI (Digital Government Index)

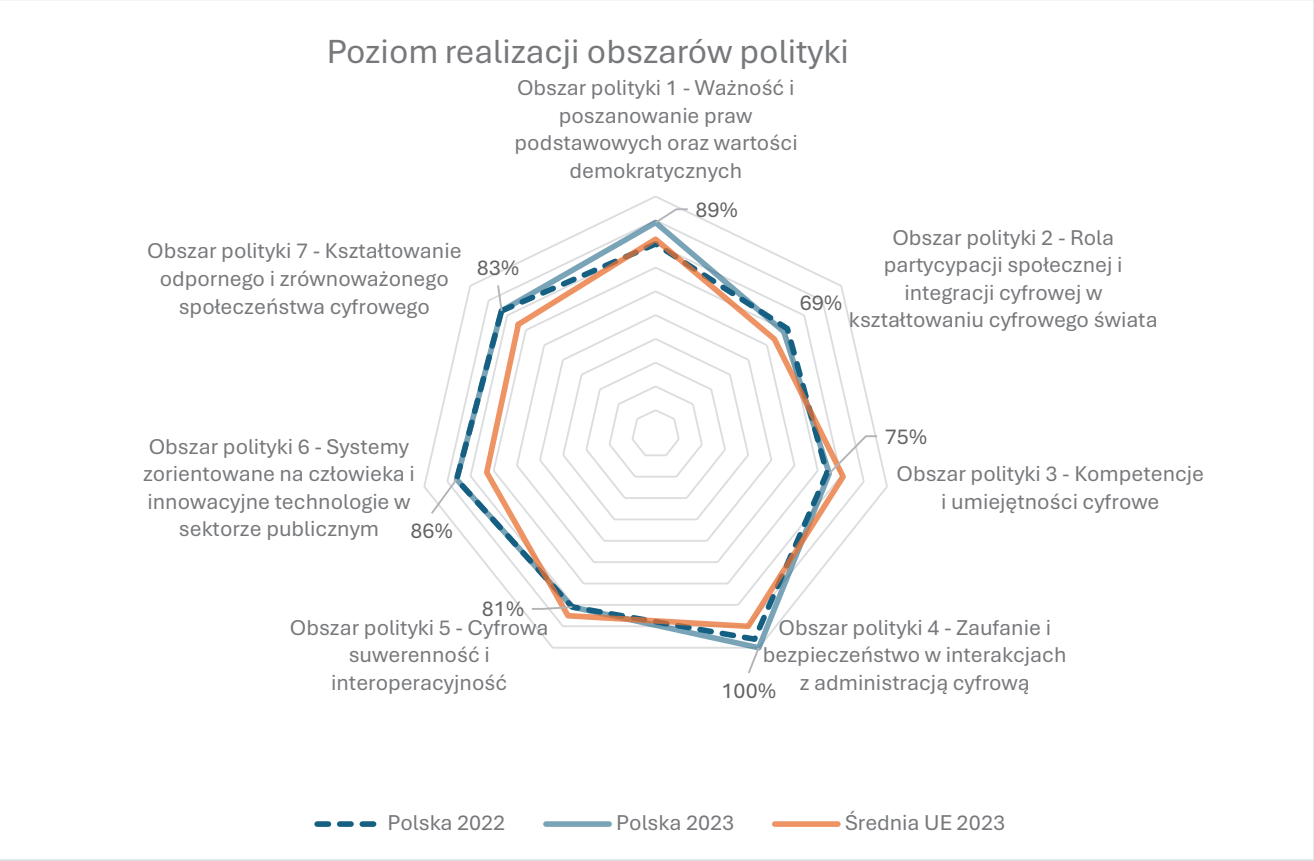
W raporcie OECD (Organizacji Współpracy Gospodarczej i Rozwoju, ang. Organisation for Economic Cooperation and Development) Digital Government Index z 2023 r.[22], oceniającym postępy transformacji cyfrowej sektora publicznego za lata 2020-2022, Polska uplasowała się na 20. miejscu wśród 33 państw członkowskich Organizacji. Wynik wyniósł 57,1%, przy średniej OECD na poziomie 60,5%. Najlepszy wynik, 11 pozycję, Polska osiągnęła w kategorii *rząd jako platforma,* w której mierzone jest funkcjonowanie wspólnych elementów takich jak wytyczne, narzędzia, dane, tożsamość cyfrowa i oprogramowanie, które umożliwią transformację procesów i usług publicznych**.** Obszarem, w którym Polska osiągnęła najsłabszy wynik, 29. miejsce, jest *proaktywność,* definiowana jako *zdolność rządów do przewidywania potrzeb użytkowników i dostawców w celu świadczenia usług publicznych.*

Deklaracja Berlińska

Deklaracja Berlińska w sprawie społeczeństwa cyfrowego i administracji cyfrowej opartej na wartościach określa szereg kluczowych zasad i towarzyszących im obszarów polityki wskazanych, aby zapewnić zgodność transformacji cyfrowej ze wspólnymi europejskimi prawami podstawowymi oraz wartościami. Raport z monitoringu Deklaracji Berlińskiej[23] to narzędzie dokumentujące postępy w realizacji działań w ramach deklaracji dla państw

[22] https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html.
[23] https://joinup.ec.europa.eu/sites/default/files/inline-files/BDM_Report_2023_vFinal_rev.pdf.

sygnatariuszy. Mechanizm monitorowania opiera się na kluczowych wskaźnikach efektywności, do ewaluacji których wykorzystano dane zapewnione przez państwa członkowskie, eGovernment Benchmark, EIF oraz DESI.



Wykres 5. Monitoring Deklaracji Berlińskiej 2023, Poziom realizacji obszarów polityki - Polska w porównaniu ze średnią UE, źródło: opracowanie własne na podstawie Raportu z monitorowania Deklaracji Berlińskiej 2024

W raporcie wydanym w 2024 r. zauważono, że wynik Polski wykazał stabilność. Wystąpiły tylko niewielkie wahania względem podsumowania z poprzedniego roku. **Największy wzrost, o 9 pp., odnotowano w obszarze pierwszym *ważność i poszanowanie praw podstawowych oraz wartości demokratycznych.* Na kolejnym miejscu usytuował się obszar czwarty, *zaufanie i bezpieczeństwo w interakcjach z administracją cyfrową*, w którym wynik wzrósł o 4 pp.** Niewielki spadek, o 2 pp., odnotowano w obszarze drugim *rola partycypacji społecznej i integracji cyfrowej w kształtowaniu cyfrowego świata*. Polska uzyskała wynik wyższy od średniej UE w czterech z siedmiu obszarów. **Największą różnicę, o 13 pp., odnotowano w obszarze szóstym *systemy zorientowane na człowieka i innowacyjne technologie w sektorze publicznym.*** Następnie o 10 i 9 pp. w obszarze czwartym i obszarze siódmym *kształtowanie odpornego i zrównoważonego społeczeństwa cyfrowego*. Obszarami, w których Polska wypada poniżej średniej UE, jest obszar trzeci *kompetencje i umiejętności cyfrowe*, w którym różnica wynosi 6 pp., a także obszar piąty *cyfrowa suwerenność i interoperacyjność* z różnicą wynoszącą 4 pp.

Polska została wyróżniona na tle UE w obszarze siódmym *odporność i zrównoważony rozwój* za inicjatywy na rzecz rozwoju cyfrowych usług zdrowotnych, takich jak Internetowe Konto Pacjenta, aplikacja mojeIKP, e-recepta czy uruchomienie na portalu pacjent.gov.pl

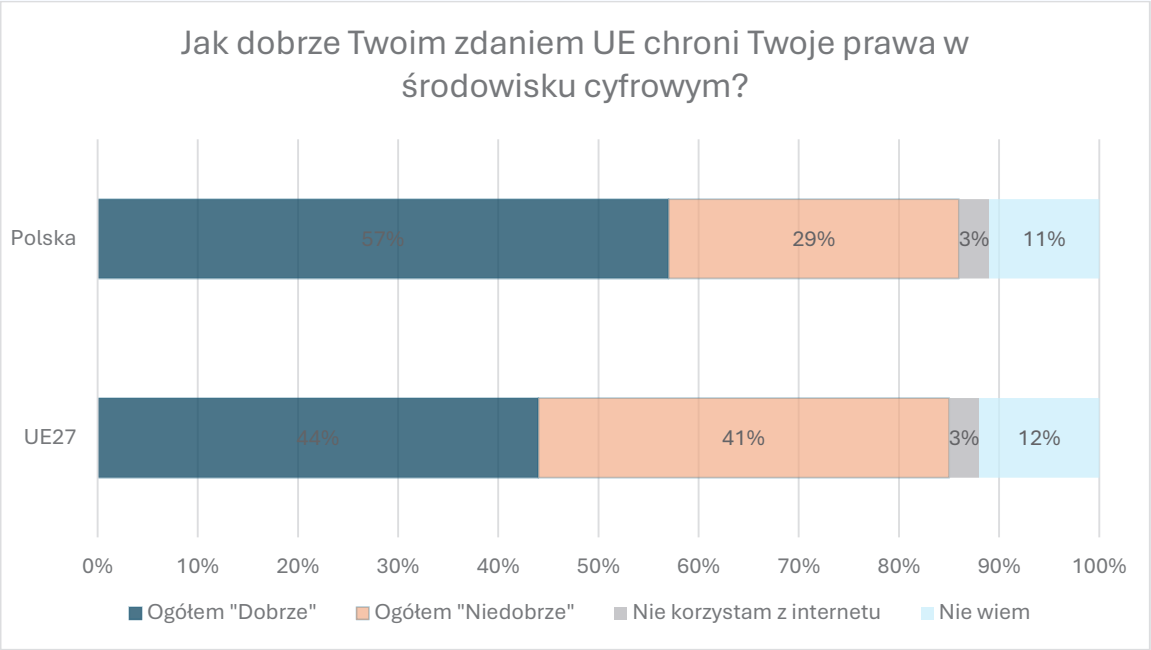
chatbota informującego pacjentów o e-usługach w systemie ochrony zdrowia. **W obszarze czwartym *zaufanie poprzez bezpieczeństwo w sferze cyfrowej* dobrze oceniono rozwój mobilnej aplikacji mObywatel, a w obszarze szóstym *systemy sztucznej inteligencji oparte na wartościach i zorientowane na człowieka* efektywną koordynację działań związanych z rozwojem polskiego ekosystemu AI (m.in. strategiczne działania w Komitecie Rady Ministrów do spraw Cyfryzacji).**

Specjalne badanie Eurobarometru: obywatele europejscy i cyfrowa dekada

Na potrzeby wsparcia monitoringu programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. oraz założeń Europejskiej Deklaracji Praw i Zasad Cyfrowych na zlecenie Komisji Europejskiej przeprowadzono badanie sprawdzające, czy i w jakim stopniu ewoluują postawy obywateli UE wobec technologii cyfrowych. Wnioski z wydanego w 2025 r. raportu[24] wskazują na to, że prawie trzy czwarte Europejczyków (73%) uważa, że cyfryzacja codziennych usług publicznych i prywatnych ułatwia im życie, w tym 17% twierdzi, że „znacznie ułatwia". Nieco mniej niż jedna czwarta (23%) twierdzi, że cyfryzacja codziennych usług publicznych i prywatnych utrudnia im życie.

Przedstawione wyniki wskazują na to, iż **na ogół postawy i postrzeganie technologii cyfrowych przez Polaków jest pozytywne i oceniane na tym samym poziomie lub wyższym niż średnio wśród obywateli Unii**. W zakresie wyobrażeń dotyczących przyszłości technologii cyfrowych aż 78% (o 2 pp. mniej względem 2024 r.) Polaków myśli, że do 2030 r. technologie cyfrowe będą istotne w dostępie do usług opieki zdrowotnej lub korzystania z nich, tego samego zdania jest 80% obywateli UE. W porównaniu do 73% Europejczyków - **78% Polaków uważa, że cyfryzacja codziennych usług publicznych i prywatnych ułatwia im życie**.

[24] https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-special-eurobarometer.



Wykres 6. Specjalne badanie Eurobarometru 551, pytanie QC7, *źródło: opracowanie własne na podstawie Arkusza informacyjnego dla Polski*

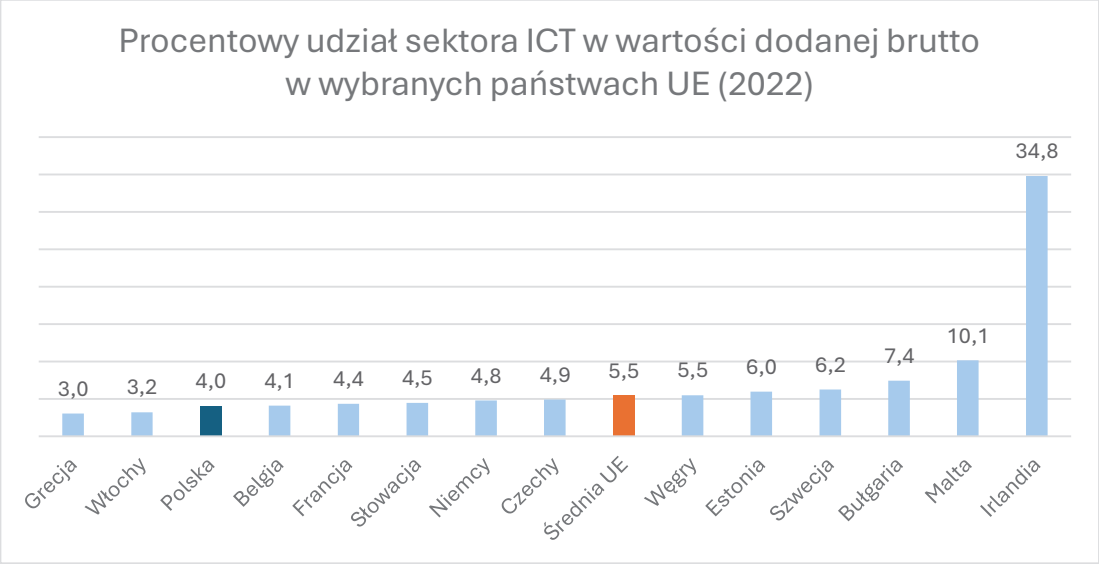
Jedynie 44% obywateli UE sądzi, że Unia dobrze chroni ich prawa w środowisku cyfrowym, podczas gdy tego samego zdania jest 57% obywateli Polski. W zakresie postrzegania stosowania zasad cyfrowych w kraju **najniższy wynik dotyczy zapewnienia bezpiecznego środowiska cyfrowego i treści dla dzieci i młodzieży (56% Polaków sądzi, że są one zapewniane ogólnie dobrze, natomiast 35%, że ogólnie niezbyt dobrze;** średnia UE wynosi 42% - ogółem dobrze, 48% - ogółem niezbyt dobrze) **oraz uzyskania kontroli nad swoim cyfrowym dorobkiem** (np. decydowanie o tym, co się stanie z osobistymi kontami i informacjami po śmierci).

Gospodarka cyfrowa

Jak już podkreślono, kluczowymi komponentami transformacji cyfrowej kraju są działania sektora prywatnego i rozwój cyfrowej gospodarki. Ta gałąź opiera się na technologiach i innowacjach, a jej główne komponenty[25] to wykorzystanie ICT do wymiany danych, automatyzacji procesów kontaktów biznesowych, udostępnianie usług cyfrowych, handel elektroniczny oraz płatności bezgotówkowe, wspierane przez infrastrukturę obliczeniową.

W 2022 r. wartość dodana sektora ICT[26] w UE stanowiła równowartość 5,5% całkowitej wartości dodanej brutto, co odpowiadało 791 mld EUR. W latach 2012–2022 udział usług ICT w wartości dodanej brutto[27] w UE wzrósł o 24,8%, natomiast w Polsce o 28,7%.

[25]https://www.mckinsey.com/pl/~/media/mckinsey/locations/europe%20and%20middle%20east/polska/raporty/digital%20challengers%203/mckinsey_digital%20challengers%20report%202022.pdf.
[26] https://ec.europa.eu/eurostat/databrowser/view/isoc_bde15ag/default/table?lang=en.
[27] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_sector_-_value_added,_employment_and_R%26D&oldid=551753.



Wykres 7. Procentowy udział sektora ICT w wartości dodanej brutto w wybranych państwach Unii Europejskiej w 2022 r., *źródło: opracowanie własne na podstawie danych Eurostatu*

Polska z wynikiem 4,0% znajduje się znacznie poniżej średniej UE wynoszącej 5,5%. Radzi sobie jednak lepiej niż Grecja (3,0%), czy Włochy (3,2%), a jej wynik jest zbliżony do wyniku Belgii (4,1%). W 2022 r. największy w UE udział sektora ICT w wartości dodanej brutto zaprezentowały Irlandia (34,8%) i Malta (10,1%).

W 2023 r. na zlecenie Komisji Europejskiej Bank Światowy przygotował raport[28] odpowiadający na pojawiające się nowe wyzwania w zakresie tworzenia polityk cyfryzacji w Unii Europejskiej. Zwrócono w nim uwagę na fakt, że podstawą europejskiej gospodarki są mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa (MŚP), które stanowią ponad 95% firm w UE. Odpowiadają za więcej niż połowę PKB brutto i za zatrudnienie ponad 100 mln osób. Tempo adaptacji nowych technologii w MŚP warunkuje więc rozwój gospodarki cyfrowej. W 2024 r. wskaźnik intensywności cyfrowej dla przedsiębiorstw zatrudniających od 10 do 249 osób wyniósł dla Polski 68,9% wobec średniej UE 72,9%[29] (Polska znalazła się na 19. miejscu w UE). Państwa, które osiągnęły najwyższy wynik to m.in. Finlandia (92,5%), Dania (90,4%) i Szwecja (86,5%). Z kolei państwa prezentujące najniższe wyniki to Bułgaria (49,9%) i Grecja (53,4%).

Rozwój gospodarki cyfrowej to również działalność badawczo-rozwojowa, a wydatki na B+R zyskują coraz większe znaczenie[30]. W latach 2000–2023 średnie europejskie wydatki na ten obszar wzrosły z 1,8% PKB do 2,2% PKB. Spośród państw członkowskich w latach 2013-2023[31] największy wzrost nakładów na badania i rozwój odnotowano w Belgii (+1 pp.), Polsce (+0,68 pp.), Grecji (+0,67 pp.), czy Chorwacji (+0,60 pp.). W 2023 r. liderem w

[28] Raport The Missing Element of Firm Digitalization – Lessons for the EU Member States: Best practices for enhancing MSMEs Digitalization and Managerial Capacity Building (*Brakujący Element Cyfryzacji Firm – Wnioski dla Państw Członkowskich UE: Najlepsze praktyki wspierające rozwój MMŚP I budowanie potencjału menedżerskiego)*, http://documents.worldbank.org/curated/en/099110723083021800.
[29] https://ec.europa.eu/eurostat/databrowser/view/isoc_e_dii/default/table?lang=en.
[30] https://ec.europa.eu/eurostat/databrowser/view/SDG_09_10/default/table.
[31] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=R%26D_expenditure.

Europie była Szwecja, która przeznacza na B+R 3,6% PKB, następnie Belgia i Austria (po 3,3% PKB). Polska na innowacje wydaje 1,6% PKB, więc dzieli ją duży dystans do liderów.

Chociaż wynik Polski w Europejskim Indeksie Innowacji (EIS, ang. *European Innovation Scoreboard*)[32], czyli prowadzonym od 2017 r. badaniu porównawczym poziomu innowacyjności państw członkowskich UE - systematycznie rośnie, to nadal wyzwaniem pozostaje nadrobienie luki wobec średniej unijnej (110 pkt) oraz liderów rankingu. Wśród wskaźników EIS znajdują się m.in. zasoby ludzkie dla nauki i techniki, edukacja, patenty, czy nakłady na działalności innowacyjną i efekty tej działalności. W 2024 r. wynik Polski wyniósł 72,5 pkt; to ok. połowa wyniku liderów, którymi są Dania (149,3 pkt), Szwecja (146,2 pkt) i Finlandia (140,6 pkt). W porównaniu z rokiem poprzednim wskaźnik dla Polski wzrósł o 3 pkt, co stanowi jeden z najwyższych wzrostów w Europie. Podobny wzrost odnotowano na Litwie (+3,7 pkt) i na Cyprze (+3;3 pkt). W zestawieniu EIS Polska wraz z Chorwacją, Słowacją, Litwą, Bułgarią i Rumunią została zakwalifikowana do najniższej kategorii państw określonych jako „wschodzący innowatorzy".

[32] https://projects.research-and-innovation.ec.europa.eu/en/statistics/performance-indicators/european-innovation-scoreboard/eis-2024#/eis.

IV. Wyzwania i trendy

W ostatnich kilkunastu latach – częściowo w wyniku pandemii – Polska odnotowała istotny postęp w dziedzinie cyfryzacji, zmniejszając szybko dystans dzielący ją od unijnych liderów. Szczególnie wyraźne były postępy w zakresie cyfrowych usług publicznych i otwartych danych. Z drugiej strony, w wielu obszarach różnica względem liderów pozostaje znacząca; zwłaszcza jeśli chodzi o poziom kompetencji cyfrowych obywateli oraz wykorzystanie technologii cyfrowych w sektorze przedsiębiorstw.

Projektując cyfrowy rozwój kraju na kolejne lata nie wystarczy jednak analizować jedynie pozycji Polski w międzynarodowych wskaźnikach. Konieczna jest analiza i przygotowanie odpowiedzi na kluczowe trendy i wyzwania przekładające się na sferę cyfrową. Wśród najważniejszych z nich warto wymienić:

Multipolaryzację świata.

Narastająca rywalizacja między światowymi mocarstwami coraz wyraźniej obejmuje również obszar technologii. Przedmiotem współczesnych napięć geopolitycznych rywalizacji stają się kluczowe technologie, takie jak: półprzewodniki, 5G i 6G, AI, technologie kwantowe czy technologie pozyskiwania energii. Mocarstwa konkurują także o zasoby służące do ich rozwoju – dane i surowce krytyczne. W wyniku pandemii, kurczących się zasobów oraz niestabilności gospodarczej, dotychczasowe globalne łańcuchy dostaw ulegają istotnemu skróceniu. Zjawisko to stanowi zarówno wyzwanie, jak i szansę dla Polski.

Nacisk na suwerenność technologiczną.

Postępująca globalna rywalizacja przekłada się na dążenie do odbudowy unijnej i krajowej produkcji kluczowych komponentów technologicznych oraz upraszczania i dywersyfikacji łańcuchów dostaw. Suwerenność technologiczna zyskuje na znaczeniu jako warunek dalszego rozwoju, w tym utrzymania zdolności produkcyjnych w UE. Równolegle jednak UE towarzyszy pogłębiająca się współpraca z państwami spoza Europy, które podzielają podobne wartości i podejście do rozwoju cyfrowego (tzw. like-minded). Coraz wyraźniej widoczna jest konwergencja technologiczna i regulacyjna między tymi ośrodkami na świecie.

Splinternet.

Jednym z istotnych wyzwań towarzyszących geopolitycznej rywalizacji i zmianom w zakresie suwerenności cyfrowej jest zjawisko splinternetu, tj. fragmentaryzacji otwartego internetu na rozdrobnione sieci pod kontrolą rządów czy korporacji. Taka fragmentaryzacja podważa uniwersalność społeczną i gospodarczą internetu. Dodatkowo ogranicza swobodny dostęp do informacji oraz powoduje ryzyko technologicznej i regulacyjnej separacji, co w dłuższej perspektywie może osłabić globalną współpracę cyfrową.

Wzrost znaczenia cyberbezpieczeństwa.

Nasilająca się rywalizacja międzynarodowa (w tym w obszarze technologii) oraz upowszechnienie technologii przekładają się na konieczność zwiększenia nacisku na kwestie cyberbezpieczeństwa, zwłaszcza w odniesieniu do sektorów o znaczeniu krytycznym. Cyberbezpieczeństwo zyskuje również na znaczeniu z perspektywy obywateli i instytucji, które coraz częściej stają się celem cyberataków i padają ofiarą profesjonalizacji grup cyberprzestępczych. Zagrożenia te z jednej strony przybierają postać prób oszustw w internecie, co przybrało masowy charakter i stanowi bezpośrednie zagrożenia dla obywateli i ich majątku. Z drugiej strony mamy do czynienia z wyrafinowaną wrogą aktywnością grup hakerskich powiązanych z nieprzyjaznymi państwami, która jest wymierzona w instytucje państwa i infrastrukturę krytyczną, co stanowi istotne zagrożenie dla bezpieczeństwa narodowego.

Hiperłączność.

Trend ten odnosi się zarówno do interakcji międzyludzkiej realizowanej za pośrednictwem technologii informacyjno-komunikacyjnych (ICT), jak i interakcji człowiek-maszyna i maszyna-maszyna (internet rzeczy). Rosnąca liczba cyfrowych połączeń i zaangażowania w nie przekłada się bezpośrednio na rosnące znaczenie danych i obciążenie sieci telekomunikacyjnych.

Rosnącą platformizację.

To jeden z istotniejszych trendów współczesnej gospodarki i relacji społecznych. W obszarze gospodarki przekłada się to w wielu przypadkach na zwiększenie efektywności i obniżkę cen, jednak kosztem szeregu efektów zewnętrznych – zaburzeń tradycyjnych sektorów gospodarki czy prekaryzacji siły roboczej. W wymiarze społecznym powszechne wykorzystanie platform społecznościowych, w szczególności mediów społecznościowych, powoduje konieczność reagowania państwa na zagrożenia dla zdrowia psychicznego obywateli oraz dla stabilności ładu informacyjnego.

Zaburzenia konkurencji.

Dominacja dużych platform technologicznych prowadzi do zaburzeń konkurencji oraz ogranicza skuteczność kontroli rządów i stanowi istotne wyzwanie z perspektywy regulacyjnej. Wyzwanie to jest szczególnie istotne, ponieważ, wiele z najistotniejszych platform (społecznościowych czy handlowych) ma pochodzenie pozaunijne. W związku z tym państwo musi angażować się w działania na rzecz zapewniania równego pola gry dla wszystkich uczestników rynku.

Rosnące koszty psychospołeczne związane ze sferą cyfrową.

Modele biznesowe oparte na uzależnianiu użytkowników od treści i na algorytmach śledzących, upowszechnianie nierealistycznych standardów urody, dostęp nieletnich do szkodliwych treści, hejt, szerząca się dezinformacja – wszystkie te czynniki mają negatywny

wpływ na zdrowie psychiczne dzieci i dorosłych, osłabienie więzi społecznych czy polaryzację debaty publicznej i wymagają kompleksowej odpowiedzi.

„Bliźniaczą przemianę".

Oznacza to bezpośrednie powiązanie transformacji cyfrowej z transformacją energetyczną, również w zakresie decyzji inwestycyjnych. Rośnie świadomość konieczności poszukiwania synergii między tymi procesami – wykorzystania zielonej energii do zaspokajania rosnących potrzeb związanych z tworzeniem i wykorzystywaniem ICT, a jednocześnie oparcia ekologicznej energetyki na technologiach cyfrowych.

Rozpowszechnianie się i szybki rozwój sztucznej inteligencji (AI).

AI może stać się fundamentem przemian w sektorze cyfrowym w najbliższych latach. Wdrażanie AI oznacza nowe możliwości m.in. w obszarze badań, tworzenia treści czy usług, ale wiąże się też z zagrożeniami, które wymagają skoordynowanej odpowiedzi instytucji państwa oraz przygotowania obywateli na nowe wyzwania i możliwości.

Oddalenie infrastruktury i usług cyfrowych od użytkownika.

Elastyczność i skalowalność rozwiązań chmurowych sprawiają, że coraz częściej przechowywanie i prowadzenie operacji na danych odbywa się nie przy wykorzystaniu lokalnej infrastruktury, a właśnie w chmurze. Rośnie popularność rozwiązań dostarczanych w modelu subskrypcyjnym – infrastruktury, platform czy usług.

Automatyzację i robotyzację gospodarki.

Jest ona owocem dążenia do zwiększenia efektywności przedsiębiorstw i wynikiem trudności w znalezieniu odpowiednio wykwalifikowanej siły roboczej. Jednocześnie, stanowi zarazem szansę na poprawę wyników gospodarczych, jak i zagrożenie wypchnięciem z rynku pracy niektórych grup pracowników.

Szybkie starzenie się polskiego społeczeństwa.

Jest ono nie tylko obciążeniem dla systemu świadczeń społecznych i wyzwaniem z perspektywy konieczności rozwoju srebrnej gospodarki, lecz także przełoży się na konieczność zwiększenia zastosowania technologii w gospodarce i dostosowania systemu rozwoju kompetencji przyszłości do zmienionej struktury demograficznej.

Niezakończony proces tworzenia jednolitego unijnego rynku cyfrowego.

Ponadto też trudności z dostępem do kapitału (w tym kapitału wysokiego ryzyka), stanowią istotne bariery, które utrudniają skalowanie przedsiębiorstw działających w obszarze ICT.

Większość z wymienionych trendów i wyzwań ma wymiar globalny lub przynajmniej unijny. Tym samym, wymagają one odpowiedzi również na poziomie wspólnotowym – ze względu na konieczność harmonizacji rozwiązań w ramach wspólnego rynku czy większą siłę regulacyjną UE w relacjach z największymi firmami. Jednocześnie, dostrzec należy fakt podjęcia w samej UE refleksji nad zbalansowaniem dotychczasowego modelu rozwoju bloku, w dużej mierze skupionego na regulacjach. Ilustruje to m.in. raport Mario Draghiego „Przyszłość europejskiej konkurencyjności” [33], zwracający uwagę na problemy Europy z utrzymaniem konkurencyjności oraz finansowaniem inwestycji i innowacji. Zdaniem Draghiego, remedium na te problemy ma być m.in. ograniczenie biurokracji, usprawnienie współpracy na unijnym rynku oraz sposobu zarządzania wspólnotą.

Z drugiej strony, na poziomie unijnym (przykładowo, w głośnym raporcie EuroStack[34]) coraz częściej zwraca się także uwagę na kwestie suwerenności cyfrowej, konieczności przenoszenia produkcji kluczowych komponentów stosu technologicznego do Europy i zwiększenia niezależności szeroko pojętej cyfrowej infrastruktury od największych graczy. Jednak efektywne projektowanie cyfrowego rozwoju Polski musi uwzględniać także krajowe oraz regionalne wyzwania i specyfiki. Tempo rozwoju technologicznego wymaga też, aby analiza ta nie odbywała się incydentalnie, przy okazji tworzenia kolejnych strategii, lecz na bieżąco. Tym samym konieczne jest systemowe pogłębienie wiedzy i jej międzyinstytucjonalna wymiana, bez których znacząco utrudniona będzie właściwa alokacja ograniczonych zasobów i osiągnięcie efektu mnożnikowego czy wprowadzanie rozwiązań technicznych i legislacyjnych umożliwiających pogłębianie współpracy w ramach administracji.

Polska administracja musi posiadać też możliwość samodzielnej analizy trendów rynkowych i technologicznych, w celu odróżnienia tych, które mają realny wpływ na gospodarkę i społeczeństwo od tych, które są przede wszystkim tymczasowym medialnym trendem.

Efektywna implementacja wniosków z takich analiz będzie wymagała zaś wzmacniania kompetencji cyfrowych urzędników i szkolenia kadr w zakresie polityk publicznych

[33] https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059.
[34] https://www.euro-stack.info/.

odnoszących się do cyfryzacji. Nie uda się też bez uspójnienia procesów polskiego rozwoju cyfrowego. Ze względu na horyzontalność cyfryzacji, trapiąca wciąż administrację silosowość jest bowiem w tym obszarze szczególnie szkodliwa. Należy budować świadomość konieczności bliskiej współpracy między instytucjami odpowiedzialnymi za budowę cyfrowego państwa, również z sektorów dzielących „wspólną granicę" z cyfryzacją w sensie ścisłym.

V. Analiza SWOT

W celu wyznaczenia priorytetów w obszarze cyfryzacji państwa na kolejną dekadę, było konieczne przeprowadzenie pogłębionej analizy sytuacji w zakresach właściwości poszczególnych ministerstw, a także państwa jako całości. Wspartą materiałami diagnostycznymi innych resortów analizę silnych i słabych stron polskiej cyfryzacji, a także szans i zagrożeń dla niej, wykonał na zlecenie Ministerstwa Cyfryzacji (MC) Polski Instytut Ekonomiczny (PIE). Analiza została przeprowadzona dla pięciu strategicznych obszarów ściśle powiązanych z działalnością MC.

infrastruktury telekomunikacyjnej;

kompetencji przyszłości[35];

cyberbezpieczeństwa;

cyfrowego państwa;

gospodarki cyfrowej.

Obszary te zostały wybrane ze względu na ich kluczowe znaczenie dla rozwoju kraju i potencjalną możliwość osiągnięcia efektu mnożnikowego przez rozwój w ich ramach. Analiza PIE została uzupełniona i zmodyfikowana w efekcie konsultacji społecznych. Zawarte w niej aspekty są także uszczegółowiane w podrozdziałach tematycznych w dalszej części Strategii i przekładają się na zawarte w nich cele.

[35] Cele i działania opisane w Strategii dotyczą kompetencji przyszłości, w zakresie w jakim warunkują one rozwój cyfrowy.

Infrastruktura telekomunikacyjna

Infrastruktura telekomunikacyjna jest przykładem sukcesu wydatkowania środków unijnych, regulacji i zaangażowania przedsiębiorstw prywatnych. Należy mieć na uwadze, że Polska już teraz ma szeroki dostęp do nowoczesnych sieci oraz niezwykle konkurencyjny rynek, dający bardzo dobre warunki konsumentom. Pojawiają się jednak nowe wyzwania – potencjalne wykorzystanie alternatywnych technologii dostępowych (ze względu na bardzo wysokie koszty pokrycia całego kraju światłowodem); konieczność stymulacji popytu na dostęp do internetu i zapewnianie utrzymania sieci wobec rosnących kosztów; tworzenie nowych „infrastruktur" – centrów przetwarzania danych, komputerów kwantowych czy sieci prywatnych w przedsiębiorstwach.

Istotnym zjawiskiem zmieniającym charakter rynku telekomunikacyjnego w ostatniej dekadzie jest stagnacja jego wartości, przy jednoczesnym wzroście dochodów dostawców treści, platform i usług cyfrowych (serwityzacja). Kondycja rynku powinna być uważnie monitorowana pod kątem ewentualnych interwencji wraz ze spełnianiem wymogów dla sieci mobilnych nałożonych w aukcjach częstotliwości 5G oraz wyłanianiem się potencjalnych, danochłonnych aplikacji. Silną stroną polskiego rynku telekomunikacyjnego jest jego elastyczność, uwidoczniona m.in. przez trend oddzielania infrastruktury od usług (w Polsce widoczny zarówno w sieciach ruchomych jak i stacjonarnych), który umożliwił części operatorów telekomunikacyjnych zwiększenie środków na inwestycje, a tym samym poszerzenie pola działalności. Przedsiębiorcy telekomunikacyjni mają jednak ograniczone umiejętności wchodzenia w nowe obszary biznesowe, a niski poziom cyfryzacji firm nie sprzyja ekspansji w tym kierunku. Z ryzykiem może się wiązać również propozycja konsolidacji operatorów sieci mobilnych w UE – dla polskiego rynku mogłoby to raczej oznaczać wzrost cen, przy wątpliwym pozytywnym wpływie na jakość dostępnej infrastruktury sieci mobilnych.

Silne strony	Słabe strony
a) duża konkurencja i dobra oferta dla konsumentów, b) relatywnie szeroki dostęp do światłowodów oraz dobry zasięg usług mobilnych, c) wysoki poziom inwestycji w sieci telekomunikacyjne, znaczące środki prywatne i publiczne oraz duże doświadczenie w zakresie dysponowania nimi, d) rosnący popyt na usługi przetwarzania danych, e) elastyczność rynku, sygnalizowana m.in. przez trend rozdzielania infrastruktury od usług i rozwinięty model dostępu hurtowego.	a) opóźnione postępowania na częstotliwości dla sieci 5G, b) brak uwzględnienia alternatywnych technologii przy zapewnianiu dostępu, c) brak udziału w międzynarodowych projektach wdrażania 5G, d) marginalny udział polskich przedsiębiorstw i nauki w międzynarodowych inicjatywach rozwijających 6G, e) niewielki sektor nowoczesnych centrów przetwarzania danych, f) występowanie barier (prawnych, administracyjnych, finansowych i technicznych) utrudniających i wydłużających realizację inwestycji.
Szanse	**Zagrożenia**
a) zwiększona dostępność do usług satelitarnych o coraz lepszych parametrach jakościowych, b) rozwijanie przez telekomy nowych modeli biznesowych, c) planowane działania stymulujące popyt na łącza o wysokich przepływnościach, d) oparcie nowej infrastruktury centrów przetwarzania danych o obiekty budowane od podstaw z myślą o najnowszych technologiach, e) upraszczanie ram regulacyjnych i usuwanie barier inwestycyjnych, f) zwiększenie efektywności i przewidywalności gospodarki widmem radiowym i współdziałania państw członkowskich w celu eliminowania zakłóceń.	a) nierównomierny dostęp do infrastruktury powodujący występowanie obszarów wykluczonych, b) niewielki popyt na łącza o najwyższych przepływnościach, c) znaczna emisyjność gospodarki i związane z nią koszty energii i koszty regulacyjne, mogące zmniejszać atrakcyjność inwestycji w infrastrukturę centrów przetwarzania danych, d) propozycja paneuropejskiej konsolidacji operatorów sieci mobilnych, e) spadająca (w ujęciu realnym) wartość rynku sektora telekomunikacyjnego, przekładająca się na ograniczenie zdolności inwestycyjnych, f) dezinformacja i manipulacje w przestrzeni informacyjnej skutkujące wywołaniem lub wzmocnieniem sprzeciwu społecznego dla rozwoju infrastruktury telekomunikacyjnej, w szczególności mobilnej oraz centrów danych, g) rozwój cyberprzestępczości zagrażający bezpieczeństwu, integralności i

	nienaruszalności transmisji danych w sieciach szerokopasmowych, h) silna koncentracja rynku usług satelitarnych może tworzyć zależności od kilku dostawców.

Kompetencje przyszłości

W dzisiejszych czasach posiadanie kompetencji cyfrowych jest potrzebne zarówno do rozwoju osobistego, aktywności społecznej i obywatelskiej, jak i funkcjonowania na rynku pracy. Choć ich rozwój był w ostatnich latach przedmiotem wsparcia w ramach wielu inicjatyw, dystans do poziomu średniej unijnej pozostaje znaczący – zaledwie 50% polskich obywateli posiada przynajmniej podstawowe umiejętności cyfrowe przy średniej UE wynoszącej 60%[36]. Silne strony są ograniczone, a część ekspertów wskazuje na utrzymywanie się tych samych barier i wyzwań w dziedzinie kompetencji cyfrowych od wielu lat. Odpowiedź na problemy zdiagnozowane w tym zakresie miał stanowić Program Rozwoju Kompetencji Cyfrowych, którego opracowanie i uchwalenie zajęło ponad 4 lata, w związku z czym na jego efekty trzeba będzie jeszcze poczekać.

W perspektywie kolejnych lat rysują się bardzo istotne wyzwania z obszaru demografii, a także niepokojący trend spadającego odsetka absolwentów kierunków STEM (ang. science, technology, engineering, mathematics, czyli nauka, technologia, inżynieria, matematyka). Z drugiej strony, absolwentów kierunków ICT jest coraz więcej. Niekorzystny wpływ mają również inne czynniki, np. niski poziom cyfryzacji firm i wypływanie za granicę talentów wykształconych w polskich podmiotach systemu nauki i szkolnictwa wyższego. Z drugiej strony, jako niewątpliwą szansę należy traktować łatwą dostępność przykładów dobrych praktyk stosowanych przez inne kraje oraz wysoki poziom wiedzy eksperckiej zgromadzony m.in. w organizacjach społecznych zaangażowanych w rozwijanie kompetencji cyfrowych w Polsce. Upowszechnianie się automatyzacji procesów i zastosowania sztucznej inteligencji ma dwa oblicza – z jednej strony stanowi szansę na ograniczenie deficytów kadrowych, z drugiej – zagrożenie koniecznością pilnego dostosowania kompetencji pracowników do nowych technologii.

[36]https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/default/bar?lang=en&category=isoc.isoc_sk.isoc_sku.

Silne strony	Słabe strony
a) wysoki poziom kształcenia technicznego na uczelniach, b) relatywnie wysoki (na tle Europy Środkowo-Wschodniej) poziom cyfryzacji w szkołach, w tym wyposażenie ich w szerokopasmowy dostęp do internetu, c) wysoki poziom wiedzy eksperckiej zgromadzony m.in. w instytucjach zaangażowanych w rozwijanie kompetencji cyfrowych w Polsce.	a) niski poziom umiejętności cyfrowych obywateli we wszystkich kategoriach wiekowych, nawet wśród tzw. cyfrowych tubylców - osób młodych w wieku 16-19 lat, b) stosunkowo mały zasób specjalistów ICT i udział kobiet w zawodach ICT, c) niewystarczająca jakość edukacji cyfrowej, d) odsetek absolwentów kierunków STEM poniżej średniej unijnej, e) niska w porównaniu z innymi krajami UE aktywność edukacyjna osób dorosłych w Polsce, f) zbyt mały nacisk na rozwój miękkich kompetencji przyszłości.
Szanse	**Zagrożenia**
a) wzrost świadomości wśród decydentów oraz w społeczeństwie znaczenia kompetencji cyfrowych dla jakości życia obywateli i kondycji gospodarki, b) dostępność przykładów dobrych praktyk stosowanych przez inne kraje, c) wzrost efektywności i ograniczenie deficytów kadrowych przez automatyzację procesów, współpracę ludzi z maszynami i sztuczną inteligencję.	a) szybko zmieniający się zakres kompetencji cyfrowych wymagających uzupełniania przez całe życie, b) starzenie się społeczeństwa i wykluczenie cyfrowe seniorów, c) drenaż talentów, d) brak stabilności wsparcia rozwoju kompetencji cyfrowych, e) kryzys zdrowia psychicznego i inne ryzyka związane z ekspozycją na media elektroniczne, f) konieczność dostosowania kompetencji pracowników do skutków automatyzacji i wykorzystania sztucznej inteligencji.

Cyberbezpieczeństwo

Obszar cyberbezpieczeństwa jest powiązany ze wszystkimi innymi obszarami, a silne i słabe strony, szanse i zagrożenia współgrają z tymi wskazanymi w innych częściach. Polska dysponuje istotnym zasobem kapitału ludzkiego – ekspertów w instytucjach zapewniających cyberbezpieczeństwo na poziomie krajowym, czy startupów zajmujących się cyberbezpieczeństwem. Jednocześnie jednak, niski poziom kompetencji cyfrowych (w tym w przedsiębiorstwach) oraz relatywnie niewielkie znaczenie przywiązywane wciąż do cyberbezpieczeństwa mogą przekładać się na narastające ryzyka i dużą liczbę „słabych ogniw". W wielu aspektach kluczowy dla cyberbezpieczeństwa jest wymiar międzynarodowy. Bliskość pełnoskalowej wojny w Ukrainie oraz agresywna postawa Federacji Rosyjskiej i innych aktorów międzynarodowych zwiększa liczbę cyberataków, ale zarazem pozwala rozwijać kompetencje w konfrontacji z realnym zagrożeniem. Korzystnym czynnikiem dla zwiększenia poziomu cyberbezpieczeństwa jest także rozwijający się rynek – zarówno rodzimych firm, jak i obecność światowych potentatów, która pozwala na korzystanie z ich wiedzy, doświadczeń i infrastruktury. Koordynację działań w obszarze cyberbezpieczeństwa może utrudniać rozproszenie odpowiedzialnych za niego instytucji oraz brak „jednego okienka" dla podmiotów krajowego systemu cyberbezpieczeństwa (KSC) i obywateli. Kwestie prawne natomiast są zarówno problemem, jak i szansą – z jednej strony niekorzystne są bowiem opóźnienia w tworzeniu niektórych aktów prawnych oraz ich coraz większa liczba komplikująca system prawny, z drugiej jednak wciąż istnieje możliwość przyjęcia dobrych przepisów oraz poszerzenie debaty na poziomie europejskim.

Silne strony	Słabe strony
a) zespoły CSIRT (ang. Computer Security Incident Response Team - Zespoły Reagowania na Incydenty Bezpieczeństwa) poziomu krajowego i inne instytucje odpowiedzialne za zapewnianie cyberbezpieczeństwa na poziomie krajowym, b) duży zasób specjalistów w sektorze publicznym i prywatnym, c) inicjatywy zwiększające cyberbezpieczeństwa na poziomie krajowym (w tym AntyDDoS, ARAKIS-GOV, ARTEMIS, SKR-Z, S46, CTI), d) duża liczba kierunków studiów związanych z cyberbezpieczeństwem, e) członkostwo w NATO (współpraca sojusznicza i kolektywna obrona) oraz członkostwo w UE (mechanizmy współpracy i regulacje).	a) niskie wykorzystanie chmury obliczeniowej, b) niski poziom umiejętności cyfrowych, braki kompetencyjne w administracji publicznej, c) niska świadomość dotycząca zagrożeń w społeczeństwie i administracji, d) rozproszenie instytucji odpowiedzialnych za cyberbezpieczeństwo, e) bliskość pełnoskalowej wojny w Ukrainie, narażenie na cyberataki ze strony Federacji Rosyjskiej, f) trudności w utrzymaniu specjalistów w sektorze publicznym; braki kadrowe w IT wśród MŚP, g) niski priorytet cyberbezpieczeństwa w polskich firmach oraz w administracji.
Szanse	**Zagrożenia**
a) rosnąca świadomość dotycząca ochrony danych i prywatności, b) wzrost znaczenia bezpieczeństwa w dyskusjach o kierunku rozwoju, przekładająca się na szanse wzrostu finansowania.	a) popularyzacja smart-urządzeń IoT (ang. Internet of Things - internet rzeczy) i rozwój przemysłu 4.0, b) popularyzacja pracy zdalnej, c) wykorzystanie generatywnej AI przy szkodliwej działalności w cyberprzestrzeni, d) rozwój technologii kwantowych jako zagrożenie dla bezpieczeństwa informacji, e) nasilająca się rywalizacja geopolityczna, f) wzrost liczby cyberataków, g) stosowanie rozwiązań technologicznych od niezaufanych dostawców.

Cyfrowe państwo

Rozwój cyfrowych usług publicznych (i prywatnych) to jeden z obszarów w którym Polska radzi sobie relatywnie dobrze. Mimo odległego miejsca w zestawieniach rankingowych DESI, dystans do liderów jest mniejszy niż w innych obszarach, a niektóre krajowe rozwiązania (np. mObywatel) są dobrym przykładem dla innych państw. Ponieważ dla rozwoju usług cyfrowych kluczowe jest zaufanie społeczne do zastosowanych technologii, należy podkreślić, że w ostatnich latach nie było większych incydentów naruszających takie zaufanie. Według badań PIE[37], polscy obywatele mają pozytywne nastawienie do e-usług: 92,5% respondentów deklaruje, że cyfrowe usługi publiczne ułatwiają im załatwianie spraw urzędowych; 66,7% badanych jest zdania, że państwo powinno inwestować więcej w cyfrowe usługi publiczne, jednak tylko 27,2% jest gotowych sfinansować te inwestycje przez podwyżkę podatków. Jednocześnie 60,4% ankietowanych uważa, że państwo powinno wykorzystać sztuczną inteligencję przy tworzeniu cyfrowych usług publicznych.

Istotną trudnością jest znaczne rozproszenie tworzonych usług, w tym dublowanie się zamawianych przed administrację rozwiązań. Sugeruje to słabą koordynację działań w tym zakresie. Jednocześnie wiele usług ma braki na poziomie UX (ang. user experience - doświadczenie użytkownika), podczas gdy w innych ośrodkach na ten aspekt stawia się duży nacisk – brakuje wypracowanych standardów czy przepływu najlepszych praktyk. Ważnym wyzwaniem jest też cyfryzacja prowadzona przez samorządy. Na tym poziomie często bowiem brak kompetencji do wprowadzania cyfrowych usług, pojawiają się trudności z zapewnieniem utrzymania systemów teleinformatycznych (ze względu na jeszcze większy niż na poziomie centralnym niedostatek specjalistów ICT); pojawiają się też obawy przed trwałą utratą pracy wskutek automatyzacji.

[37] https://pie.net.pl/67-proc-polakow-jest-za-szerszym-stosowaniem-ai-w-administracji-publicznej/.

Silne strony	Słabe strony
a) szeroki wachlarz cyfrowych usług publicznych, b) dostęp do funduszy strukturalnych, c) istniejące, dobrze funkcjonujące rozwiązania (mObywatel, Twój e-PIT), d) otwartość na zmiany i aplikowanie nowych rozwiązań, e) rozwinięty rynek komercyjnych rozwiązań w zakresie identyfikacji elektronicznej.	a) dług technologiczny (utrzymujące się stare systemy teleinformatyczne w administracji), b) braki kompetencyjne i obawy w administracji, zwłaszcza po stronie samorządów, c) niski poziom zaufania do państwa, d) niekonkurencyjne wynagrodzenia dla specjalistów ICT w administracji publicznej, e) brak pełnej interoperacyjności systemów teleinformatycznych i rejestrów publicznych wykorzystywanych w administracji publicznej, f) silosowość w administracji publicznej – dublowanie zamówień, brak koordynacji działań i wspólnych standardów.
Szanse	**Zagrożenia**
a) pozytywne nastawienie społeczne do cyfrowych usług publicznych oraz stosowania AI w administracji, b) partnerstwo z biznesem i korzystanie z najlepszych rozwiązań rynkowych, c) rozwój lokalnego rynku ICT.	a) uzależnienie od rozwiązań dostarczanych przez zewnętrznych dostawców, b) nakładanie się różnych mechanizmów i perspektyw czasowych w dokumentach strategicznych, w tym unijnych, c) rywalizacja geopolityczna i zagrożenie uderzeniem w czułe punkty cyfrowej infrastruktury kraju, d) szybko zmieniające się otoczenie technologiczne; oddalanie się sektora prywatnego od publicznego w zakresie stosowanych technologii, e) wysokie koszty budowy i utrzymania rozwiązań ICT, f) niespójność ram regulacyjnych.

Gospodarka cyfrowa

Polska gospodarka cyfrowa znajduje się w fazie intensywnego rozwoju, ale nadal istnieje duża przestrzeń do poprawy cyfryzacji firm, automatyzacji i robotyzacji produkcji. Robotyzacja jest na niskim poziomie w stosunku do krajów regionu, a tym bardziej w odniesieniu do europejskich liderów[38]. Wydaje się jednak, że trendy demograficzne, regulacyjne (m.in. wzrost płacy minimalnej) i rynkowe mogą przyspieszyć zmiany w tym obszarze w Polsce. Silną stroną są relatywnie wysokie wydatki sektora prywatnego na badania i rozwój (w porównaniu do wydatków budżetowych[39]) czy obecność regionów chmurowych największych globalnych dostawców chmury – a zatem ich bezpośrednie zaangażowanie w rozwijanie cyfrowej gospodarki. Trudnością są z kolei bariery mentalne (tj. brak motywacji przedsiębiorców do wdrażania nowych rozwiązań – zdecydowanie trudniejsze do przezwyciężenia niż np. bariery finansowe), „pułapka kraju średniej wielkości" (rynek krajowy wystarczająco duży do utrzymania firmy, brak zewnętrznych bodźców do rozwoju) czy wreszcie niewystarczająca dostępność krajowego kapitału (bariera wykraczająca poza sferę cyfrową). Innym ryzykiem, również wykraczającym poza tylko sferę cyfrową, jest struktura gospodarki, z dużą nadwyżką firm mikro- i małych (najprawdopodobniej niezależnie od dużego odsetka pozornie samozatrudnionych).

W rezultacie może powstać dualna gospodarka, w której firmy z kapitałem zagranicznym, włączone w globalne łańcuchy dostaw czy eksportujące stosują nowoczesne rozwiązania technologiczne i cyfrowe, a druga część pozostaje w tyle. Takie zagrożenie sugerują wskaźniki rozwoju sektora ICT, w tym w odniesieniu do flagowego polskiego obszaru eksportowego – branży gamedev (tworzenie gier komputerowych, ang. game development). Ukazują one bardzo niską liczbę specjalistów ICT w całej gospodarce, wskazującą na niski priorytet cyfryzacji w większości firm.

Istotnym kontekstem dla przyszłości polskiej gospodarki cyfrowej są też trendy demograficzne. Już w 2023 r. 25% osób pracujących (w wieku 18-64 lat) stanowiły osoby w wieku 50 lat lub wyższym[40]. Jak wynika z analizy PIE, do 2035 r. polski rynek pracy skurczy się o 2,1 mln pracowników, czyli 12,6% obecnego zatrudnienia. Najpoważniejsze skutki zmian demograficznych dotkną sektor edukacji (zmniejszenie bazy pracowników o nawet 29%) oraz opieki zdrowotnej (spadek o nawet 23%). Sektory przemysłowe (sekcje B-E Polskiej Klasyfikacji Działalności) mogą do 2035 r. stracić nawet 400 tys. pracowników (spadek o 11%).

Jednym z potencjalnych rozwiązań niwelujących negatywne skutki spadku podaży pracy jest wykorzystanie nowoczesnych technologii. Automatyzacja, wykorzystanie robotów przemysłowych, systemów RPA (Robotic Process Automation) oraz sztucznej inteligencji mogą wspomagać ludzką pracę, zwiększać jej efektywność lub nawet całkowicie ją zastępować[41]. Dzięki takim rozwiązaniom można zautomatyzować część etatów lub

[38] https://ec.europa.eu/eurostat/databrowser/view/isoc_eb_p3d/default/table?lang=en.
[39] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=R%26D_expenditure#R.26D_expenditure_by_source_of_funds.
[40] https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf.
[41] https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf.

zmniejszyć zapotrzebowanie na pracę w sektorach zmagających się z niedoborami siły roboczej – tych, w których nie przyniesie to nadmiernych negatywnych kosztów społecznych.

Pomimo obecnie obserwowanego w Polsce niskiego poziomu adaptacji nowych technologii, można zakładać, że spadająca podaż pracowników, a co za tym idzie wzrost kosztów pracy, przełożą się na potrzebę innowacyjnych inwestycji na rzecz automatyzacji w polskich przedsiębiorstwach[42]. W polskim przemyśle istnieje nadal duży potencjał automatyzacji, ponieważ obecna gęstość robotyzacji należy do najniższych w UE[43]. Również sztuczna inteligencja jako technologia, która jest jednocześnie komplementarna oraz substytucyjna wobec pracowników wysoko wykwalifikowanych, daje duży potencjał na przejmowanie niektórych zadań od ludzi, a jednocześnie zwiększenie efektywności wykonywania pozostałych zadań, co może pomóc zniwelować negatywne skutki zmian demograficznych[44]. Jednocześnie jest niezbędne zapewnienie, aby zastosowanie sztucznej inteligencji w wykonywaniu zadań nie prowadziło do nadużyć względem pracowników.

[42] https://pie.net.pl/wp-content/uploads/2024/10/Podaz-pracy.pdf.
[43] https://pie.net.pl/wp-content/uploads/2024/07/Robotyzacja-w-Polsce-w-2023.pdf.
[44] https://www.whitehouse.gov/wp-content/uploads/2024/03/ERP-2024.pdf.

Silne strony	Słabe strony
a) dostępność technologii największych globalnych graczy, b) wysoki eksport ICT (szczególnie usług), c) relatywnie wysokie nakłady polskich dużych firm na B+R (badania i rozwój, ang. Research and Development), d) rozwinięty rynek polskich komercyjnych rozwiązań w zakresie identyfikacji elektronicznej oraz usług zaufanych ukierunkowanych na wzrost cyberbezpieczeństwa.	a) relatywnie niski poziom robotyzacji, b) brak strategii przemysłowej, c) niski poziom kompetencji cyfrowych, d) niska motywacja pracodawców do wdrażania innowacyjnych/cyfrowych rozwiązań, e) niski odsetek specjalistów ICT zatrudnionych w gospodarce, f) niska dostępność krajowego kapitału, g) niska innowacyjność gospodarki, h) uzależnienie od rozwiązań dostarczanych przez zewnętrznych dostawców, w tym szczególnie kontrolowanych kapitałowo przez podmioty spoza UE.
Szanse	**Zagrożenia**
a) zmniejszanie się zasobu siły roboczej jako potencjalny impuls do automatyzacji/cyfryzacji, b) szybkie tempo rozwoju gospodarki, c) duże doświadczenie krajowe we wdrażaniu e-usług prywatnych, d) wzrost cyberodporności polskiej gospodarki oraz minimalizacja strat wynikających z cyberataków w konsekwencji wzmocnienia bezpieczeństwa procesów identyfikacji elektronicznej.	a) brak silnego ekosystemu inwestycji w startupy, b) mały w stosunku do potrzeb dopływ specjalistów ICT, zagrożenia wynikające z kryzysu demograficznego, c) wysokie koszty zatrudnienia specjalistów ICT, d) "luka cyfrowa" wśród przedsiębiorców – firmy o wysokim poziomie automatyzacji są przeważnie duże, eksportujące, będące w posiadaniu zagranicznego kapitału, e) zwiększająca się niestabilność geopolityczna, przekładająca się na ryzyko prowadzenia działalności gospodarczej.

VI. Cele i czynniki umożliwiające ich realizację

Powyżej zarysowane uwarunkowania – obok doświadczeń z dotychczasowego funkcjonowania MC, rekomendacji z licznych raportów z administracji i rynku oraz ciał doradczych, a także ewaluacji realizacji dotychczas obowiązujących dokumentów strategicznych – były drogowskazem w opracowaniu założeń niniejszej Strategii.

Za jej główne dążenie - biorąc pod uwagę horyzontalność procesów cyfryzacji i jej silny wpływ na wiele aspektów ludzkiego życia – uznajemy podnoszenie jakości życia dzięki cyfryzacji.

Do realizacji tego dążenia przyczynią się cele i działania zarysowane w poszczególnych obszarach tematycznych. Kluczowe znaczenie będzie miała zaś realizacja celów podstawowych, warunkujących powodzenie pozostałych. Są to:

1) zagwarantowanie odpowiedniej jakości sieci telekomunikacyjnej na obszarze kraju poprzez jej rozwój i utrzymanie;
2) wsparcie rozwoju kompetencji koniecznych do poruszania się w świecie cyfrowym;
3) dostarczenie przez państwo szerokiego pakietu e-usług o wysokim poziomie dojrzałości;
4) zapewnienie szeroko pojętego bezpieczeństwa sfery cyfrowej;
5) wsparcie rozwoju innowacyjnej cyfrowej gospodarki.

Aby powyższe cele mogły być skutecznie realizowane, jest konieczne:

a) **zwiększenie koordynacji prac między podmiotami administracji publicznej** – zarówno centralnej, jak i samorządowej – a także wsparcia innych instytucji publicznych. Brak jednego ośrodka odpowiedzialnego za cyfryzację kraju we wszystkich obszarach wymaga poprawy mechanizmów koordynacji między różnymi podmiotami działającymi w tym zakresie. Poruszanie się w szybko zmieniającej się sferze technologii wymaga też zwiększenia elastyczności funkcjonowania państwa w tym obszarze,

b) **przeznaczenie wystarczających zasobów finansowych, kadrowych i organizacyjnych** na rozwój cyfrowego państwa, społeczeństwa i gospodarki opartej na danych. Inwestycje w obszar cyfrowy – zapewnianie cyberbezpieczeństwa, unowocześnianie procesów w administracji, usprawnianie e-usług, podniesienie liczby wdrożeń opartych o sztuczną inteligencję czy wsparcie tworzenia innowacji – są

kluczowe, ale kosztują i wymagają zaangażowania odpowiednio wynagradzanych i kompetentnych kadr,

c) **długofalowe projektowanie cyfrowego rozwoju kraju.** Choć precyzyjne przewidzenie kierunków rozwoju technologii jest często niemożliwe, za istotne należy uznać zwiększenie kompetencji analitycznych ośrodków odpowiedzialnych za tworzenie polityki cyfrowej w Polsce – pozwoli to bowiem na wczesnym etapie identyfikować trendy, których uwzględnienie może być korzystne dla kraju. Należy mieć także na względzie zapewnianie neutralności technologicznej rozwiązań stosowanych przez państwo, co umożliwi uniknięcie długofalowego uzależnienia od jednego dostawcy,

d) **wsparcie sprawiedliwej transformacji cyfrowej**, w ramach której zagwarantowany zostanie zrównoważony rozwój oraz zwiększenie konkurencyjności gospodarki (w tym w powiązaniu z transformacją energetyczną oraz prawami pracowniczymi), włączenie społeczne, dostępność cyfrowa (w szczególności dla osób z niepełnosprawnościami) oraz realizacja praw i zasad cyfrowych, zawartych m.in. w Europejskiej Deklaracji Praw i Zasad Cyfrowych w Cyfrowej Dekadzie. Odpowiednio zaprojektowana transformacja cyfrowa musi uwzględniać m.in. powiązania z transformacją energetyczną, zagwarantowanie praw pracowniczych i wsparcie przekwalifikowania osób, których miejsca pracy są zagrożone przez zmiany technologiczne oraz uwarunkowania demograficzne,

e) **projektowanie cyfrowych przemian w duchu technorealizmu** – uznanie, że rozwój technologii nie jest odpowiedzią na wszystkie problemy. Jakkolwiek ma on potencjał do realnej poprawy jakości życia, wiąże się też z zagrożeniami, w tym z przypadkami naruszenia prawa, na które państwo musi reagować i im zapobiegać. Niezbędne jest pragmatyczne podejście, opierające się na świadomości, że technologia nie jest celem samym w sobie, i wykorzystaniu jej w tych obszarach, gdzie faktycznie przyniesie korzyści,

f) przyjęcie założenia, że wprowadzanie **przez państwo** nowych rozwiązań cyfrowych **powinno być poddawane dogłębnej weryfikacji na etapie projektowania i mitygacji zagrożeń, w celu zapewnienia bezpieczeństwa,** w tym gwarancji ochrony danych osobowych – rozumianego zarówno w odniesieniu do obszaru cyberbezpieczeństwa, jak i praw podstawowych obywateli, ich dobrostanu psychicznego i spójności społecznej,

g) **zapewnienie partnerskiej współpracy międzynarodowej, a także między państwem a biznesem, w tym sektorem MŚP**. Gospodarka cyfrowa jest globalna, a istotna część polskiego prawa cyfrowego bierze swój początek w UE. Tym samym bez dobrej współpracy międzynarodowej rozwój cyfrowego państwa i gospodarki będzie napotykał na istotne przeszkody. Konieczne jest też zapewnienie uczciwych i partnerskich relacji z firmami z sektora ICT. Na szczególną uwagę zasługują relację z największymi globalnymi firmami technologicznymi. Choć funkcjonowanie bez ich produktów często jest niemożliwe, to zarazem muszą one uczciwie kontrybuować do rozwoju państwa, również w obszarze podatkowym. W budowaniu tych relacji jest konieczne utrzymanie suwerenności w kluczowych aspektach dotyczących cyfryzacji. Niezwykle ważną kwestią będzie również współpraca z sektorem pozarządowym oraz w ramach partnerstw publiczno-społecznych.

Na potrzeby usystematyzowania kierunków interwencji określone zostały 4 obszary horyzontalne, które w największym stopniu realizują podstawowe cele Strategii, a ze względu na rangę i znaczenie, istotnie wpływają na efektywność działań w innych obszarach i stanowią punkt wyjścia dla transformacji cyfrowej wielu dziedzin życia społeczno-

gospodarczego. Są to: komunikacja elektroniczna, kompetencje przyszłości, cyberbezpieczeństwo oraz koordynacja transformacji cyfrowej.

1. Obszary horyzontalne

1.1 Komunikacja elektroniczna

Diagnoza – jak jest?

W Polsce odsetek gospodarstw domowych w zasięgu dostępu do internetu o przepustowości dosyłowej łącza wynoszącej co najmniej 100 Mb/s, z możliwością jej zwiększenia do przepustowości mierzonej w gigabitach, wyniósł na dzień 31 grudnia 2024 r. 83,6%[45]. Wskazuje to na znaczący postęp dokonany w ostatnich latach, który został osiągnięty za sprawą znaczących inwestycji finansowanych ze środków publicznych i prywatnych. Jednocześnie jest niezbędne kontynuowanie inwestycji zmierzających - zgodnie z celami Cyfrowej Dekady UE - do zapewnienia powszechnego dostępu do sieci gigabitowych. Wraz z poprawą sytuacji w zakresie zwiększenia obszaru objętego zasięgiem internetu szerokopasmowego coraz bardziej istotną kwestią staje się pobudzenie popytu na usługi dostępu do internetu (z usług stacjonarnego dostępu do internetu w 2024 r. korzystało 67,5% gospodarstw domowych[46]). Za sprawą inwestycji operatorów mobilnych, którzy na skutek przeprowadzonych w 2023 r. i 2025 r. aukcji uzyskali możliwość korzystania z pasm pionierskich dla technologii 5G (3,6 GH i 700 MHz), nastąpiła znacząca poprawa zasięgu usług w tej technologii. W 2025 r. według danych UKE, ponad 90% gospodarstw domowych w Polsce znajduje się w zasięgu sieci 5G[47].

Zapewnienie powszechnego dostępu do bardzo szybkiego internetu wszystkim obywatelom jest jednym z determinantów rewolucji cyfrowej,

bowiem umożliwia budowę kapitału cyfrowego społeczeństwa, upowszechnienie kwalifikacji cyfrowych, wspieranie kompetencji cyfrowych wśród dzieci i młodzieży w procesie edukacji, czy też upowszechnienie cyfrowych usług publicznych. Proces ten nie może odbyć się bez współpracy państwa z przedsiębiorstwami telekomunikacyjnymi w zakresie zapewnienia bezpiecznej, wydajnej i zrównoważonej infrastruktury cyfrowej. Na tej płaszczyźnie coraz większym wyzwaniem staje się sukcesywna eliminacja tzw. białych plam NGA (ang. Next-generation access) ze względu na konieczność dotarcia z inwestycjami do najtrudniejszych – z punktu widzenia dostępności i ukształtowania terenu oraz gęstości zaludnienia – punktów adresowych, które generują konieczność znacznych nakładów finansowych. Ze względu na potencjalnie niską opłacalność dla przedsiębiorców telekomunikacyjnych inwestycje w tych obszarach muszą być finansowane przede wszystkim ze środków pochodzących ze źródeł publicznych. Konieczne jest również sformułowanie odpowiedzi na problem spadającej

[45] Sprawozdanie z działalności Prezesa UKE za 2024 rok, https://bip.uke.gov.pl/sprawozdania/sprawozdania-prezesa-uke/sprawozdanie-prezesa-uke-z-dzialalnosci-prowadzonej-w-2024-r-,8.html.
[46] Raport o stanie rynku telekomunikacyjnego w 2024 roku, https://www.uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2024-roku,590.html.
[47] Raport o stanie rynku telekomunikacyjnego w 2024 roku, https://www.uke.gov.pl/akt/raport-o-stanie-rynku-telekomunikacyjnego-w-2024-roku,590.html.

(w ujęciu realnym) wartości rynku, przekładający się na ograniczenie zdolności inwestycyjnych przedsiębiorstw telekomunikacyjnych. Aby temu zapobiec, w nowelizowanych przepisach Megaustawy[48] zaproponowano działania mające na celu przyspieszenie, uproszczenie i obniżenie kosztów wdrażania stacjonarnych i bezprzedwodowych sieci o bardzo dużej przepustowości.

Za uzupełnienie infrastruktury naziemnej służyć mogą technologie satelitarne, użyteczne szczególnie na obszarach o niskim zaludnieniu.

Należy mieć również na uwadze widoczny trend w zakresie konwergencji sieci naziemnych z nienaziemnymi, w szczególności satelitarnymi. Zakłada się, że sieci komórkowe kolejnej generacji (6G) będą domyślnie zintegrowane z sieciami satelitarnymi. Trend ten jest już widoczny w obecnej generacji (5G). Obecnie coraz częściej dochodzi do współpracy operatorów komórkowych z operatorami satelitarnymi odnośnie do testowania możliwości odbioru sygnałów satelitarnych przez urządzenia mobilne. Po 2030 r. można spodziewać się w pełni zintegrowanych usług w urządzeniach końcowych. Oznacza to, że użytkownicy będą mieli możliwość dostępu do usług telekomunikacyjnych niezależnie od miejsca przebywania. Konwergencja sieci umożliwi również dalszy rozwój usług typu IoT oraz usług autonomicznych, w szczególności związanych z transportem. Należy przy tym zwrócić uwagę na zagrożenia związane z silną koncentracją na rynku usług satelitarnych.

Łączność satelitarną należy też uznać za zasób podwójnego zastosowania (cywilny i wojskowy), który w przypadku potencjalnego zagrożenia umożliwia reakcję na trudne do przewidzenia sytuacje oraz dostarczenie informacji na czas. Zapewnienie prawidłowej komunikacji między podmiotami publicznymi oraz wykorzystywanymi przez nie systemami teleinformatycznymi i rejestrami publicznymi jest kluczowe w sytuacjach kryzysowych.

Jednocześnie należy zauważyć, że obecnie najbardziej zaawansowane systemy satelitarne, takie jak konstelacje LEO oferujące globalną łączność o niskim opóźnieniu, powstają poza UE. Dlatego też, w perspektywie długofalowej, należy rozważyć budowanie i rozwijanie krajowych zdolności w obszarze łączności satelitarnej oraz – w miarę możliwości – szeroko uczestniczyć szczególnie w inicjatywach UE w zakresie budowy systemów łączności satelitarnej. Da to dalsze możliwości rozwoju bezpiecznej łączności państwowej, na potrzeby cywilne i militarne.

[48] Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2026 r. poz. 562).

Cel 1.1.1: Wszyscy użytkownicy na terenie kraju mają dostęp do ultraszybkich usług telekomunikacyjnych – mobilnych i stacjonarnych

Co umożliwi realizację celu:

a) kontynuacja wsparcia finansowego dla przedsiębiorców telekomunikacyjnych w zakresie rozwoju infrastruktury, szczególnie na obszarach tzw. białych plam – terenach problematycznych z punktu widzenia dostępności, ukształtowania terenu i gęstości zaludnienia,

b) wykorzystanie alternatywnych technologii do zapewnienia łączności w najtrudniejszych inwestycyjnie obszarach, gdzie nie ma możliwości uzyskania przepustowości gigabitowych za pomocą technologii przewodowych,

c) likwidowanie barier prawnych i systemowych dla rozwoju sieci telekomunikacyjnych przez nowelizację tzw. Megaustawy, która będzie obejmować zidentyfikowane zarówno przez resort cyfryzacji, jak i zgłaszane przez branżę telekomunikacyjną bariery inwestycyjne. Ponadto wdrożenie do polskiego porządku prawnego postanowień rozporządzenia unijnego Gigabit Infrastructure Act (GIA)[49] w celu wsparcia rozwoju publicznych sieci telekomunikacyjnych przewidującego uruchomienie m.in. otwartego pojedynczego punktu informacyjnego („jedno okienko”), w którym każdy operator ma prawo składać, również w formacie elektronicznym, wnioski o udzielenie wszelkich niezbędnych zezwoleń inwestycyjnych, o odnowienie zezwoleń lub udzielenie prawa drogi, a następnie uzyskuje informacje o statusie swojego wniosku,

d) zapewnienie jednostkom samorządu terytorialnego wsparcia merytorycznego w prowadzeniu procesów inwestycyjnych w obszarze telekomunikacji i wyznaczenie koordynatorów szerokopasmowych we wszystkich gminach i powiatach,

e) kontynuowanie projektów edukacyjno-informacyjnych dotyczących roli infrastruktury telekomunikacyjnej (stacjonarnej i mobilnej – w tym 5G i 6G) dla rozwoju społeczno-gospodarczego kraju wzmacniające odporność społeczną na dezinformację i manipulacje w przestrzeni informacyjnej obejmującej te zagadnienie,

f) utrzymanie i rozwój portalu internet.gov.pl (SIDUSIS) dostarczającego każdemu w łatwej i dostępnej formie informacji o ofercie usług dostępu do internetu w danym punkcie adresowym,

[49] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1309 z dnia 29 kwietnia 2024 r. w sprawie środków mających na celu zmniejszenie kosztów wdrażania gigabitowych sieci łączności elektronicznej, zmieniające rozporządzenie (UE) 2015/2120 i uchylające dyrektywę 2014/61/UE (akt w sprawie infrastruktury gigabitowej) (Dz. Urz. UE L 2024/1309 z 08.05.2024 oraz Dz. Urz. UE L 2024/90315 z 24.05.2024), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1309.

g) utrzymanie i rozwój portalu SI2PEM, w tym także przez wprowadzanie funkcjonalności usprawniających proces inwestycyjny oraz wdrożenie na szeroką skalę monitoringu poziomów PEM w kraju, w celu zapewnienia dostępności wiedzy o poziomach PEM (pola elektromagnetycznego) oraz popularyzacji tej wiedzy w celu rozwoju sieci ruchomej oraz niwelowania obaw o wpływ infrastruktury sieci ruchomej na zdrowie i środowisko,

h) wspieranie rozwoju samorządowych i prywatnych sieci 5G – prowadzenie działań o charakterze informacyjnym oraz organizacja szkoleń dotyczących wdrażania technologii 5G oraz promowanie innowacji – startupów i firm pracujących nad rozwiązaniami wdrażającymi 5G,

i) zagwarantowanie odpowiedniej jakości sieci telekomunikacyjnych – wdrożenie narzędzi systemowych i technicznych w celu pomiaru parametrów usług telekomunikacyjnych, a także wdrożenie skutecznych mechanizmów interwencyjnych w celu poprawy jakości usług telekomunikacyjnych,

j) uruchomienie mechanizmów wsparcia finansowego inwestycji w poprawę odporności fizycznej sieci telekomunikacyjnych w zakresie przekraczającym możliwości komercyjne.

[box] Co z tego wynika: Gdziekolwiek mieszkasz, będziesz mieć dostęp do szybkiego i taniego internetu i sieci komórkowej.

Cel 1.1.2: Bezpieczna łączność elektroniczna jest bezpłatna dla szczególnych grup użytkowników końcowych

Co umożliwi realizację celu:

a) zapewnienie wydajnych, bezpiecznych i wysoce dostępnych usług łączności i infrastruktury dla administracji publicznej, w szczególności dla systemów teleinformatycznych i telekomunikacyjnych zapewniających interoperacyjność między systemami łączności i komunikacji na potrzeby cywilne i militarne,

b) zmodernizowanie Ogólnopolskiej Sieci Edukacyjnej (OSE) – zapewnienie szkołom dostępu do sieci umożliwiającej obsługę ruchu o przepustowościach gigabitowych,

c) wdrożenie bezpłatnej dla użytkowników końcowych usługi Advanced Mobile Location (AML) umożliwiającej precyzyjne lokalizowanie osób dzwoniących na numery alarmowe w oparciu o dane pochodzące z telekomunikacyjnego urządzenia końcowego w sieci ruchomej i przekazywane do regionalnych centrów powiadamiania ratunkowego z wykorzystaniem publicznej sieci ruchomej.

[box] Co z tego wynika: Dostęp do szybkiego internetu ułatwi działanie administracji publicznej oraz szkołom.

Cel 1.1.3: Usługi telekomunikacyjne są powszechnie wykorzystywane przez społeczeństwo, administrację i biznes

Co umożliwi realizację celu:

a) wsparcie finansowe i organizacyjne podmiotów zaangażowanych we wdrażanie sieci nowej generacji. Zapewnienie środków na działania badawczo-rozwojowe dotyczące sieci komunikacyjnych, które będą prowadzone we współpracy instytucji publicznych z instytucjami naukowo-badawczymi i przemysłem w celu rozwoju zastosowań dla sieci telekomunikacyjnych (w szczególności mobilnych),

b) wspieranie ścisłej współpracy z dostawcami usług sieciowych umożliwiającej synchronizację działań, m.in. przez standaryzację, wspólne projekty rozwojowe, tworzenie jednolitego przekazu.

Cel 1.1.4: Cele transformacji cyfrowej państwa są wspierane przez bezpieczny system łączności satelitarnej

Co umożliwi realizację celu:

a) opracowanie, budowa i wyniesienie satelity telekomunikacyjnego na orbitę geostacjonarną wraz z budową całego ekosystemu składającego się z segmentu naziemnego, użytkowników oraz ustanowienia Polskiego Operatora systemów łączności satelitarnej. Zdolności satelitarne powinny być w pełni programowalne, wyposażone w możliwości sterowania transmisją radiową w zakresie przepustowości i pokrycia oraz posiadać łączność laserową między sobą na różnych orbitach,

b) nowe inwestycje i innowacje dla rozwoju i rozbudowy krajowego potencjału w zakresie szybkiej telekomunikacji, opartej na satelitach i naziemnej infrastrukturze, w szczególności sieciach komórkowych nowych generacji (5G/6G) dla świadczenia przez operatorów efektywnych kosztowo wysokiej jakości telekomunikacyjnych usług szerokopasmowych,

c) opracowanie i budowa demonstratora technologii, w zakresie wykorzystania innowacyjnych możliwości technologicznych dla bezpiecznej transmisji i przechowywania danych w przestrzeni kosmicznej, w szczególności przy wykorzystaniu technologii kwantowych oraz świadczenia usług łączności satelitarnej dla administracji publicznej, służb odpowiedzialnych za zarządzanie kryzysowe i bezpieczeństwo,

d) zaangażowanie Polski w projekt IRiS2 – wieloorbitalnej konstelacji satelitów, która zapewni bezpieczne usługi łączności dla organów rządowych państw członkowskich UE oraz szybkie łącza szerokopasmowe dla przedsiębiorstw prywatnych i obywateli.

1.2 Kompetencje przyszłości

Diagnoza – jak jest?

Szeroko pojęte kompetencje przyszłości[50] mają fundamentalne znaczenie dla rozwoju sfery cyfrowej w państwie. Obywatele muszą nie tylko umieć korzystać z technologii cyfrowych, ale także robić to w zdrowy sposób, znać zasady higieny cyfrowej czy umieć rozpoznać dezinformację. Same zaś kompetencje cyfrowe są kluczowe dla efektywności, innowacyjności i konkurencyjności polskiej gospodarki. Dane Głównego Urzędu Statystycznego[51], wskazują na to, że w 2025 r. odsetek Polaków posiadających co najmniej podstawowe umiejętności cyfrowe wzrósł do 50,4%, a w przypadku umiejętności ponadpodstawowych odsetek ten wzrósł do 23,5%. Szczegółowego porównania z innymi krajami dostarczają dane Eurostatu[52], w 2025 r. w przypadku co najmniej podstawowych umiejętności cyfrowych średnia UE wyniosła 60,4%, a ponadpodstawowych umiejętności cyfrowych[53] – 31,4%.

Deficyt kompetencji cyfrowych jest przede wszystkim widoczny wśród osób starszych (w wieku 65-74 lat), gdzie 87,7% nie posiadało nawet podstawowych umiejętności cyfrowych (średnia UE – 67,0%) i w grupie wiekowej 55–64 lat, w której takie osoby stanowiły 67,7% (średnia UE - 49,5%), podobnie jak wśród rolników (63,8%) i osób z niepełnosprawnościami - 71,5%[54]. Odnotowano także spore dysproporcje wśród osób zamieszkujących miasta i wsie: odsetek mieszkańców terenów wiejskich z co najmniej podstawowymi kompetencjami cyfrowymi wyniósł 40,9% (średnia UE - 52,8%), o 20 punktów procentowych mniej niż w przypadku osób zamieszkujących miasta. Kompetencje cyfrowe powinny umożliwić obywatelom zrozumienie i odnalezienie się w środowisku wykorzystującym technologie w niemal każdym aspekcie życia. Osoby o niskich umiejętnościach cyfrowych znacznie bardziej narażone są na dezinformację i nieumiejętne weryfikowanie informacji otrzymanych drogą cyfrową.

W 2024 r. udział specjalistów ICT w ogólnej liczbie pracujących w Polsce wyniósł 4,5% (średnia UE – 5,0%)[55]. Wobec przewidywanego wzrostu popytu na tę kategorię pracowników oraz wyznaczonego celu dla UE w ramach Cyfrowej Dekady na 2030 r. – 10%, należy uznać, że stan ten jest niesatysfakcjonujący.

[50] OECD definiuje kompetencje przyszłości jako zdolności kognitywne, społeczne i emocjonalne niezbędne do funkcjonowania w złożonym, szybko zmieniającym się świecie, zarówno zawodowo, jak i prywatnie. Należą do nich: kreatywność i krytyczne myślenie, odpowiedzialność i inicjatywa, umiejętność współpracy, umiejętności cyfrowe i medialne. Źródło: OECD Learning Compass 2030.
[51] Wskaźnik poziomu umiejętności cyfrowych na poziomie krajowym mierzony jest przez Główny Urząd Statystyczny co roku. Wyniki na poziomie europejskim także mierzone przez GUS, są prezentowane w bazach Eurostatu z częstotliwością dwuletnią; raport GUS: https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2025-r-,1,19.html.
[52] Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/default/table?lang=en&category=isoc.isoc_sk.isoc_sku.
[53] Wprowadzone w dokumencie rozróżnienie poziomu umiejętności cyfrowych wynika z Europejskich Ram Kompetencji Cyfrowych DIGICOMP. Pełna definicja została przytoczona w słowniku.
[54] https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-przedsiebiorstwach-i-gospodarstwach-domowych-w-2025-r-,3,25.html.
[55] Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf.

Kobiety w Polsce, podobnie jak w UE, stanowiły 19% w grupie specjalistów ICT[56]. Ten brak równowagi działa na niekorzyść samych kobiet, jak też sektora ICT i gospodarki. Jak wynika z danych, polski system edukacji nie gwarantuje uzyskania przez absolwentów szkół średnich podstawowego poziomu kompetencji cyfrowych - w 2023 r. co najmniej podstawowe umiejętności cyfrowe posiadało tylko 57,8% osób w wieku 16-19 lat (średnia UE 66,4%), a w 2025 r. co najmniej podstawowe umiejętności cyfrowe posiadało 72,3% osób w wieku 16-19 lat (średnia UE 73,0%)[57]. Kształcenie na poziomie wyższym nie zapewnia stosownego do potrzeb dopływu specjalistów ICT - w 2022 r. tylko 4,3% wszystkich absolwentów kończyło naukę w dziedzinie ICT (średnia UE - 4,5%[58]. Udział kobiet wśród absolwentów ICT wyniósł 22% (średnia UE – 21%)[59]. W kontekście wsparcia innowacji cyfrowych przez absolwentów szkół wyższych należy również wziąć pod uwagę kształcenie w obszarach STEM, technologii przełomowych i na kierunkach wspierających ich rozwój.

Skuteczna cyfryzacja państwa, obejmująca rozwój usług cyfrowych oraz transformację procesów administracyjnych, wymaga równoległego i systemowego rozwoju kompetencji cyfrowych pracowników administracji publicznej na wszystkich szczeblach. Kompetencje te stanowią warunek nie tylko wdrożenia, ale także utrzymania, rozwoju i bezpiecznego funkcjonowania rozwiązań cyfrowych. Brakuje systemowego rozwiązania dotyczącego podnoszenia kompetencji cyfrowych pracowników administracji publicznej, w tym pracowników jednostek samorządu terytorialnego oraz członków korpusu służby cywilnej, dzięki któremu podniósłby się poziom świadczenia usług e-administracji i poziom satysfakcji obywateli. Istotne jest również podnoszenie świadomości gestorów danych na temat potrzeby dbania o wysoką jakość (w tym cyfryzację) źródeł administracyjnych, w tym prowadzonych przez nich rejestrów i systemów, gdyż na nich opiera się rzetelne informowanie społeczeństwa o rozwoju. W działaniach wspierających należy zwrócić szczególną uwagę na samorządy, ze względu na ich zróżnicowany potencjał do świadczenia e-usług oraz specyficzne wyzwania, jakie przed nimi stoją. W jednostkach samorządu terytorialnego wciąż brakuje dziedzinowych kompetencji cyfrowych, w tym specjalistycznej wiedzy oraz zasobów kadrowych. Wynika to m.in. z niesatysfakcjonujących wynagrodzeń dla pracowników, braku planów ciągłego podnoszenia kompetencji, a także z obawy przed korzystaniem z rozwiązań cyfrowych oraz o miejsca pracy zagrożone automatyzacją.

[56] Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itsps/default/table?lang=en&category=isoc.isoc_sk.isoc_sks.isoc_skslf.
[57] Eurostat: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21__custom_19825455/default/table https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad02__custom_12849024/default/table?lang=en.
[58] Eurostat: https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad03__custom_12512661/default/table?lang=en
[59] Eurostat: https://ec.europa.eu/eurostat/databrowser/view/educ_uoe_grad03__custom_12512714/default/table?lang=en.

Cel 1.2.1: Co najmniej 85% polskiego społeczeństwa posiada przynajmniej podstawowe umiejętności cyfrowe, a 50% umiejętności ponadpodstawowe

Co umożliwi realizację celu:

a) zapewnienie osobom dorosłym, zgodnie z ich potrzebami, możliwości rozwoju umiejętności cyfrowych w tworzonych w zainteresowanych gminach – również przy wykorzystaniu infrastruktury istniejących już instytucji – Klubach Rozwoju Cyfrowego (KRC). Każdy dorosły będzie mógł skorzystać z zajęć organizowanych w KRC oraz z porad edukatorów zatrudnionych w klubach,

b) inicjowanie działań wspierających osoby z niepełnosprawnościami i szczególnymi potrzebami, obejmujących: wsparcie finansowe w zakupie sprzętu niezbędnego do nabycia kompetencji cyfrowych, organizowanie przeznaczonych dla nich szkoleń, wsparcie organizacji non-profit w realizacji działań na rzecz podnoszenia kompetencji cyfrowych wśród osób z niepełnosprawnościami i szczególnymi potrzebami,

c) organizacja lokalnych i ogólnokrajowych kampanii motywujących społeczeństwo do rozwoju kompetencji cyfrowych przez całe życie, przez wskazywanie korzyści i możliwości, jakie daje ich posiadanie,

d) zapewnienie dostępu do szkoleń, także zakończonych ewaluacją zdobytych kompetencji np. w modelu mikropoświadczeń oraz materiałów edukacyjnych na portalu www.kompetencjecyfrowe.gov.pl, na którym zmapowane zostaną miejsca w sieci, wydarzenia oraz materiały do rozwijania kompetencji cyfrowych,

e) budowanie świadomości w zakresie bezpiecznego poruszania się w świecie cyfrowym. Będzie się ono opierać na profilaktyce cyberprzemocy i uzależnień, szerzeniu świadomości zagrożeń i umiejętności reagowania na nie, promowaniu świadomego korzystania z technologii cyfrowych (w tym AI), akcentowaniu konieczności krytycznego myślenia i stosowania zasad higieny cyfrowej, rozwiązywaniu kwestii etycznych pojawiających się wraz z rozwojem AI oraz wyposażaniu społeczeństwa w kompetencje odpowiednie do bezpiecznego i satysfakcjonującego funkcjonowania w świecie cyfrowym,

f) systemowe przeciwdziałanie dezinformacji połączone ze zwiększaniem świadomości obywateli o działaniu mechanizmów dezinformacji, rozwijanie kompetencji krytycznego myślenia, umiejętności weryfikacji informacji i korzystania z mediów na wszystkich poziomach kształcenia,

g) współpraca, mobilizowanie i aktywizowanie podmiotów tworzących ekosystem rozwoju kompetencji cyfrowych w Polsce, tj. organizacji non-profit, przedsiębiorstw, placówek edukacyjnych, kulturalnych, partnerów społecznych, administracji publicznej, w tym samorządów, itp. Promowanie i rozszerzenie

inicjatyw współpracy takich jak Porozumienie na rzecz rozwoju kompetencji cyfrowych PW eSkills,

h) zapewnienie uczniom takiego rozwoju kompetencji cyfrowych, aby każdy uczeń posiadał przynajmniej podstawowe, a najlepiej ponadpodstawowe umiejętności cyfrowe, zgodnie z Polityką Cyfrowej Transformacji Edukacji. System edukacji cyfrowej ma być wspierany dzięki odpowiednio przygotowanej kadrze pedagogicznej, przy uwzględnieniu tempa rozwoju cyfrowego i zmian w technologii, w szczególności dotyczących sztucznej inteligencji, informatyki z urządzeniami fizycznymi oraz interdyscyplinarnego zastosowania robotyki.

[box] Co z tego wynika: W Twojej gminie będzie mógł powstać Klub Rozwoju Cyfrowego, a Twoi bliscy czy znajomi będą mogli w nim lepiej poznać cyfrowy świat.

Cel 1.2.2: Liczba specjalistek i specjalistów w sektorze ICT odpowiada zapotrzebowaniu polskiej gospodarki

Co umożliwi realizację celu:

a) wspieranie uczniów, w szczególności dziewcząt, w rozwoju zainteresowań przedmiotami ścisłymi, w tym informatyką, inicjowanie programów wspierających rozwój kompetencji w nowych obszarach technologii przełomowych, pod kątem przygotowania zawodowego, m.in. AI i technologii kwantowych oraz rozszerzenie Programu Rozwoju Talentów Informatycznych na szkoły podstawowe i uzupełnienie go o komponent technologii przełomowych. Dodatkowym elementem będą działania promocyjne skierowane do rodziców, uczniów i nauczycieli,

b) niwelowanie barier ograniczających obecność kobiet w ICT, promowanie kierunków kształcenia i zawodów ICT, a także zwalczanie stereotypów hamujących dopływ kobiet do zawodów cyfrowych; prowadzenie kampanii informacyjnych przedstawiających możliwe ścieżki kariery w obszarze ICT,

c) stworzenie mechanizmu nowoczesnych szkoleń i szybkich ścieżek umożliwiających chętnym przebranżowienie do zawodu specjalisty ICT, dostępnego dla szerokiego grona zainteresowanych,

d) inicjowanie projektów wspierających rozwój zaawansowanych kompetencji w zakresie nowych technologii cyfrowych dla pracowników, w szczególności sektora MŚP, przemysłu i usług,

e) działania wspierające zwiększenie liczby absolwentów kierunków koniecznych dla rozwoju technologii przełomowych, w tym kierunków STEM, oraz liczby przeprowadzonych doktoratów w środowisku akademickim,

f) stworzenie systemu zachęt mających na celu zwiększenie liczby interdyscyplinarnych specjalistów oraz ekspertów w dziedzinach ICT/STEM, łączących te obszary z innymi kierunkami niezbędnymi dla rozwoju technologii przełomowych,

g) monitorowanie udziału kobiet w ICT, a także zmian świadomości i postaw związanych z wizerunkiem przedmiotów ścisłych, zawodów ICT i rolami płciowymi oraz rolą kobiet w ICT.

Cel 1.2.3: Na wszystkich poziomach kształcenia dostępna jest efektywna i wysokiej jakości edukacja cyfrowa, uwzględniająca potrzeby osób z grup szczególnie wrażliwych

Co umożliwi realizację celu:

a) podniesienie jakości kształtowania kompetencji cyfrowych młodego pokolenia przez rozwój dydaktyki cyfrowej, dostosowanie podstawy programowej do postępu technologicznego oraz metodycznego i występujących cyberzagrożeń. Przygotowanie nauczycieli do realizacji zajęć zgodnie z obowiązującą podstawą programową oraz metodyką wykorzystywania nowych technologii w nauczaniu i zapewnienie niezbędnego wyposażenia szkół,

b) podniesienie kwalifikacji cyfrowych oraz kompetencji w zakresie sztucznej inteligencji (AI) wśród wszystkich nauczycieli, wykładowców, pracowników akademickich i naukowych,

c) zamawianie studiów (także podyplomowych i dokształcających) w zakresie nauczania informatyki, kompetencji cyfrowych nauczycieli oraz wykorzystania nowoczesnych metod nauczania z zastosowaniem technologii cyfrowych,

d) wspieranie rozbudowy programów nauczania na uczelniach o moduły dotyczące nowoczesnych technologii oraz zwiększanie liczby miejsc na studiach o kierunkach informatycznych oraz pokrewnych,

e) wykorzystanie technologii cyfrowych w szkołach do podnoszenia jakości kształcenia, zerwania z podającą formą przekazywania wiedzy, do wspomagania pracy zespołowej, realizacji zespołowych projektów, grywalizacji oraz zapewnienia kontaktu z najnowocześniejszymi technologiami cyfrowymi jak np. AI, roboty, mikro-kontrolery, drukarki 3D, XR (wirtualnej/rozszerzonej rzeczywistości) itp.,

f) wprowadzenie do podstawy nauczania na wszystkich poziomach kształcenia oraz programów kształcenia i doszkalania kadry dydaktycznej:

- rozwijania kompetencji miękkich związanych ze sferą cyfrową, takich jak myślenie krytyczne (rozpoznawanie dezinformacji, umiejętność korzystania z mediów i weryfikacji informacji), oraz z funkcjonowaniem w nowoczesnym społeczeństwie – kreatywność, umiejętność logicznego i krytycznego myślenia, komunikacja interpersonalna, zdolność uczenia się przez całe życie,

- kształtowania umiejętności bezpiecznego korzystania z e-usług publicznych i prywatnych (z obszaru zdrowia, nauki, administracji, komunikacji, finansów, rolnictwa, zasobów kultury itp.) oraz tematów związanych ze sztuczną inteligencją – tłumaczenie jej funkcjonowania, programowanie, sposoby bezpiecznego, etycznego i odpowiedzialnego korzystania z tej technologii,

g) działanie na rzecz wprowadzenia do podstawy programowej na wszystkich poziomach kształcenia zagadnień związanych z dostępnością cyfrową,

h) aktywizowanie uczniów do samodzielnego poszerzenia wiedzy w zakresie nowych technologii przez wsparcie organizacji konkursów, hackatonów i innych form rywalizacji indywidualnej i zespołowej opartej na wiedzy i umiejętnościach,

i) utworzenie bezpłatnego systemu dla wszystkich placówek oświatowych, który umożliwi rodzicom obserwowanie postępów edukacji uczniów i kontakt z pracownikami szkoły.

[box] Co z tego wynika: Polska szkoła przygotuje uczniów do samodzielnego i bezpiecznego korzystania z technologii cyfrowych oraz będzie wspierała wykrywanie i rozwój talentów informatycznych.

Cel 1.2.4: Pracownicy administracji publicznej, w tym samorządowi, posiadają kompetencje cyfrowe niezbędne do efektywnego działania administracji

Co umożliwi realizację celu:

a) zapewnienie pracownikom administracji publicznej, w tym samorządowym, dostępu do wysokiej jakości szkoleń, warsztatów praktycznych oraz pakietów kursów e-learningowych zakończonych ewaluacją zdobytych kompetencji np. w modelu mikropoświadczeń, m.in. w obszarach świadczenia cyfrowych usług publicznych, identyfikacji elektronicznej, zarządzania cyfryzacją, elektronicznego zarządzania dokumentacją, cyfryzacji procesów, cyberbezpieczeństwa, sztucznej inteligencji, systemów chmurowych, zarządzania i analizy danych oraz otwierania danych, inteligentnych miast i wsi (smart city i smart village), open-source (otwarte oprogramowanie) w administracji, zarządzania dostępnością cyfrową i jej wdrażaniem itp.,

b) zwiększenie wynagrodzeń dla specjalistów i specjalistek ICT w administracji oraz wprowadzenie systemowego wsparcia dla jej pracowników chcących się przekwalifikować do zawodu specjalisty ICT,

c) wprowadzenie w administracji publicznej prymatu kształcenia własnych kadr w obszarach zdiagnozowanych potrzeb ICT (np. cyberbezpieczeństwo, sztuczna inteligencja).

[box] Co z tego wynika: Dzięki zwiększeniu własnych kompetencji, urzędnicy skuteczniej pomogą rozwiązać Twoją sprawę.

Cel 1.2.5: Kompleksowe wzmocnienie kompetencji cyfrowych pracowników jednostek samorządu terytorialnego odbywa się z uwzględnieniem specyficznych potrzeb regionalnych i lokalnych

Co umożliwi realizację celu:

a) opracowanie i wdrożenie systemu podnoszenia poziomu kompetencji cyfrowych pracowników samorządowych, w tym skoordynowanie działań zapewniających kompleksowe wsparcie edukacyjne, eksperckie oraz finansowe,

b) wsparcie samorządów w tworzeniu lokalnych, regionalnych lub ponadregionalnych hubów usług i kompetencji cyfrowych zapewniających dostęp do specjalistycznej wiedzy i szkoleń, które będą lepiej dopasowane do potrzeb poszczególnych podmiotów samorządowych,

c) wdrożenie rozwiązań wspierających adekwatne do warunków rynkowych wynagradzanie pracowników zaangażowanych w transformację cyfrową, zatrudnianie ekspertów ICT oraz umożliwienie oddelegowywania pracowników pomiędzy jednostkami różnych szczebli administracji w celu realizacji zadań publicznych związanych z przedsięwzięciami informatycznymi o publicznym zastosowaniu,

d) rozwijanie międzynarodowej współpracy przez tworzenie wspólnych projektów edukacyjnych z unijnymi organizacjami w zakresie kompetencji cyfrowych administracji samorządowej oraz adaptację najlepszych praktyk z innych krajów UE w sposób zharmonizowany z polskimi potrzebami,

e) programy stażowe dla studentów połączone z późniejszym zatrudnieniem w jednostkach samorządu terytorialnego, podczas których mogliby uczestniczyć w procesie transformacji cyfrowej sektora publicznego oraz zdobywać doświadczenie w tym zakresie.

Cel 1.2.6: Wiedza, umiejętności i świadomość polskiego społeczeństwa odpowiadają wyzwaniom i trendom towarzyszącym transformacji cyfrowej i zrównoważonemu rozwojowi

Co umożliwi realizację celu:

a) uwzględnianie w programach kształcenia kwestii wpływu korzystania z usług ICT na środowisko oraz edukowanie na temat tego, jak korzystać z technologii w sposób bardziej zrównoważony. Prowadzenie kampanii społeczno-edukacyjnych podnoszących świadomość w tym zakresie,

b) zwiększanie poziomu edukacji społeczeństwa z zakresu technologii przełomowych, przez organizację szkoleń, warsztatów i edukację pozaformalną, w tym rozwijanie świadomości danych, obejmującej umiejętność pozyskiwania, interpretacji, krytycznej oceny oraz odpowiedzialnego wykorzystywania danych,

c) stworzenie planu komunikacji społecznej w mediach publicznych (w ramach misji publicznej) w celu rozwoju świadomości i wiedzy obywateli na temat zagadnień cyfrowych.

Cel 1.2.7: Polskie przedsiębiorstwa posiadają kompetencje cyfrowe kluczowe do efektywnego prowadzenia biznesu, utrzymania pozycji konkurencyjnej na rynku i strategicznego rozwoju firmy przy wykorzystaniu rozwiązań cyfrowych

Co umożliwi realizację celu:

a) wzmacnianie świadomości właścicieli i pracowników nowopowstających przedsiębiorstw na temat korzyści z wdrożeń technologii dostosowanych do specyfiki działalności, przez sprofilowane doradztwo eksperckie, dostęp do materiałów informacyjnych i edukacyjnych z zakresu transformacji cyfrowej oraz korzystanie z pakietu „Cyfrowego Startu dla Biznesu”,

b) podnoszenie kompetencji właścicieli i pracowników działających przedsiębiorstw w zakresie wykorzystania nowoczesnych technologii, umożliwienie automatycznej samooceny poziomu dojrzałości cyfrowej przedsiębiorstwa oraz zapewnienie dostępu do indywidualnie dopasowanego doradztwa ICT ukierunkowanego na wdrażanie rozwiązań technologicznych i wzmocnienie cyberbezpieczeństwa,

c) budowanie zaufania do technologii cyfrowych przez wzmacnianie wiedzy o bilansie kosztów, korzyści i ryzyk z wdrożenia rozwiązań cyfrowych, o cyberbezpieczeństwie oraz rozwój umiejętności krytycznej oceny jakości i wiarygodności źródeł informacji i identyfikacji dezinformacji,

d) niwelowanie obaw związanych z przestojami procesów w firmie i ryzykiem nietrafionych inwestycji w rozwiązania cyfrowe przez systemowe wsparcie obejmujące rzetelną diagnostykę, ocenę spodziewanych efektów i dobór najlepszych narzędzi do rozwoju cyfrowego firmy,

e) wspieranie programów podnoszenia kwalifikacji dla pracowników w celu zdobycia stosowanych umiejętności w zakresie wykorzystania nowoczesnych technologii w ich obszarach zawodowych.

1.3 Cyberbezpieczeństwo

Diagnoza – jak jest?

Rosnący poziom zagrożeń w cyberprzestrzeni, nowe rodzaje zagrożeń i wzrost aktywności grup cyberprzestępczych, haktywistycznych i powiązanych z innymi państwami mają wpływ na codzienne funkcjonowanie obywateli, przedsiębiorstw i instytucji publicznych. Polska należy do krajów najczęściej atakowanych w cyberprzestrzeni, corocznie rośnie liczba cyberincydentów. Jest to związane m.in. rozprzestrzenianiem technologii (np. AI) umożliwiających dokonywanie cyberataków oraz coraz większe ucyfrowienie naszego codziennego życia oraz digitalizacja gospodarki i państw. Polska i inne państwa Zachodu są także celem ataków hybrydowych Rosji, Białorusi i innych państw, których duża część ma miejsce w cyberprzestrzeni. W wymiarze wojskowym cyberprzestrzeń stała się domeną operacyjną na równi z lądem, morzem, powietrzem i kosmosem. Cyberbezpieczeństwo naszego kraju ma też fundamentalne znacznie z uwagi na centralną rolę na wschodniej flance NATO.

Wojna Rosji z Ukrainą, w której Polska stanowi hub logistyczny wsparcia dla broniącej się Ukrainy, wiązała się z licznymi cyberatakami m.in. na infrastrukturę transportową, co jest ważną lekcją w kontekście mobilności wojskowej i zdolności do kolektywnej obrony. Polska nie pozostaje bierna wobec zagrożeń, ale aktywnie im przeciwdziała. Obejmuje to nie tylko zmiany systemowe, które wprowadza poprzez nowe akty prawne, ale także rozwija zdolności instytucji odpowiedzialnych za cyberbezpieczeństwo na poziomie krajowym, wyposaża je w odpowiednie narzędzia techniczne, jak również dba o odpowiedni zasób specjalistów do spraw cyberbezpieczeństwa (świadczenie teleinformatyczne w ramach Funduszu Cyberbezpieczeństwa oraz powszechne szkolenia z higieny cyfrowej na wszelkich szczeblach).

Polska będzie nieustannie podejmować działania mające na celu systemowe zwiększanie poziomu cyberbezpieczeństwa krajowego i międzynarodowego, zwiększanie poziomu ochrony informacji, a także ograniczanie ryzyk związanych z cyberprzestrzenią.

Będziemy więc kompleksowo rozwijać krajowy system cyberbezpieczeństwa – przez zmiany legislacyjne, podnoszenie odporności i zdolności podmiotów tego systemu oraz wprowadzanie nowych mechanizmów koordynacji działań. W szczególności nowelizacja

ustawy o krajowym systemie cyberbezpieczeństwa[60] (wdrażająca dyrektywę NIS2[61]) oraz ustawy o zarządzaniu kryzysowym[62] (wdrażająca dyrektywę CER[63]) wzmocni odporność cyfrową podmiotów działających w cyberprzestrzeni – zarówno publicznych, jak i prywatnych. Fundamentalną kwestią jest potrzeba powołania centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym. Kluczowe będą także upowszechnianie rozwiązań technicznych podnoszących cyberbezpieczeństwo, rozwój krajowego potencjału technologicznego i przemysłowego w obszarze cyberbezpieczeństwa oraz zwiększanie kompetencji specjalistów oraz społeczeństwa jako całości. Szczegółowe kierunki działań, wraz z rozwiązaniami instytucjonalnymi i technologicznymi, wyznacza Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej[2].

Działania na rzecz zwiększania poziomu cyberbezpieczeństwa muszą być podejmowane w ścisłej współpracy z odpowiednimi resortami i instytucjami państwa. Podobnie jest w przypadku zwalczania cyberprzestępczości, bez którego cyfryzacja się nie powiedzie. Warunkami skutecznego reagowania na współczesne zagrożenia w cyberprzestrzeni są także: wprowadzenie kompleksowych rozwiązań prawnych, zapewnienie i rozwój narzędzi technologicznych oraz systematyczne podnoszenie kompetencji instytucji odpowiedzialnych za walkę z cyberprzestępczością.

Za bardzo istotne należy uznać także działania mające na celu zapewnienie synergii między wojskowym a cywilnym wymiarem cyberbezpieczeństwa, a także między cyberbezpieczeństwem a zarządzaniem kryzysowym. Wyrazem takiego podejścia jest bieżąca, operacyjna i techniczna współpraca w ramach działającego pod egidą Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) pomiędzy Ministerstwem Cyfryzacji a innymi instytucjami odpowiedzialnymi za cyberbezpieczeństwo na poziomie krajowym, w tym zespołami CSIRT, policji, służb specjalnych oraz Ministerstwa Obrony Narodowej i jednostek podległych.

[60] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252).
[61] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80 oraz Dz. Urz. UE L 2025/90884 z 06.11.2025).
[62] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2026 r. poz. 574).
[63] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164).

Cel 1.3.1: Funkcjonujący krajowy system cyberbezpieczeństwa jest dojrzały i efektywny

Co umożliwi realizację celu:

a) powołanie centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym i koordynującej działania innych podmiotów zapewniających cyberbezpieczeństwo na poziomie krajowym, dysponującej odpowiednią pozycją ustrojową, kompetencjami, zasobami osobowymi, budżetem i infrastrukturą,

b) wzmacnianie roli Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Pozwoli to zwiększyć efektywność systemu i zapewni sprawniejsze reagowanie na zagrożenia w cyberprzestrzeni,

c) rozwijanie Systemu S46 jako podstawy wymiany informacji między podmiotami kluczowymi, ważnymi oraz instytucjami państwowymi,

d) wzmacnianie potencjału instytucji odpowiedzialnych za zapewnianie cyberbezpieczeństwa na poziomie krajowym, ze szczególnym uwzględnieniem zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego,

e) tworzenie i rozwój CSIRT-ów sektorowych i współpraca z sektorowymi centrami wymiany i analizy informacji,

f) udzielanie podmiotom krajowego systemu cyberbezpieczeństwa wsparcia w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym jednostkom samorządu terytorialnego w budowie samorządowych struktur odpowiedzialnych za cyberbezpieczeństwo.

Cel 1.3.2: Cyberprzestępczość jest skutecznie zwalczana

Co umożliwi realizację celu:

a) wprowadzenie regulacji pozwalających skuteczniej zwalczać cyberprzestępczość, w tym przepisów karnych, przepisów z zakresu zabezpieczenia elektronicznego materiału dowodowego oraz przeciwdziałania kradzieży tożsamości, przepisów dotyczących banków i instytucji finansowych, z uwzględnieniem regulacji międzynarodowych. Przegląd przepisów o zwalczaniu nadużyć w komunikacji elektronicznej,

b) wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości w zakresie rozwoju zasobu kadrowego i narzędzi służących do zbierania i analizowania dowodów,

c) podnoszenie potencjału organów ścigania i wymiaru sprawiedliwości, w tym przy wykorzystaniu nowych technologii i we współpracy z polskim sektorem naukowym i branżą cyfrową,

d) krajowa i międzynarodowa wymiana wiedzy i doświadczeń z zakresu cyberbezpieczeństwa i cyberprzestępczości.

[box] Co z tego wynika: Organy ścigania i wymiaru sprawiedliwości otrzymają skuteczne środki zwalczania cyberprzestępstw oraz pociągania cyberprzestępców do odpowiedzialności.

Cel 1.3.3: Systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności

Co umożliwi realizację celu:

a) centralne pozyskiwanie i rozwój rozwiązań cyberbezpieczeństwa przez MC na potrzeby własne oraz administracji publicznej i Sił Zbrojnych RP, w szczególności kontynuacja już realizowanych inicjatyw w obszarze rozpoznawania zagrożeń w cyberprzestrzeni (CTI), ochrony przed atakami DDoS oraz bezpiecznej łączności,

b) wprowadzenie mechanizmu uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów i usług ICT oraz specyfikacji tych wymogów, jak również promowanie dobrych praktyk poświęconych zamówieniom publicznym w obszarze cyberbezpieczeństwa,

c) wprowadzenie rozwiązania umożliwiającego szybkie pozyskiwanie usług i produktów związanych z cyberbezpieczeństwem w pilnych przypadkach dotyczących bezpieczeństwa państwa, przy jednoczesnym zachowaniu transparentności procesu zakupowego oraz określeniu szczególnego trybu zastosowania tego rodzaju procedury, co pozwoli uniknąć długotrwałych postępowań przetargowych negatywnie oddziałujących na cyberbezpieczeństwo państwa,

d) monitorowanie bezpieczeństwa systemów i rejestrów państwowych w trybie 24/7 przez zespoły cyberbezpieczeństwa w podmiotach je utrzymujących, stałe podnoszenie zdolności do reagowania na incydenty oraz przez wdrażanie nowych rozwiązań technicznych, proceduralnych i systemowych, jak również przeprowadzanie cyklicznych testów ciągłości działania oraz włączenie aspektów cyberbezpieczeństwa na jak najwcześniejszym etapie rozwoju i utrzymania,

e) opracowanie Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę,

f) wprowadzenie skoordynowanych rozwiązań dotyczących zarządzania podatnościami, w tym ich ujawniania, identyfikowania, katalogowania i eliminacji. Wykorzystanie europejskich rozwiązań związanych z zarządzaniem podatnościami w europejskich programach certyfikacji cyberbezpieczeństwa,

g) rozwijanie krajowych rozwiązań i standardów kryptologicznych (w tym w zakresie kryptografii kwantowej i postkwantowej oraz komunikacji kwantowej i kwantowej dystrybucji klucza), a także budowanie krajowych kompetencji, w szczególności przez inicjowanie programów i projektów badawczo-rozwojowych, wdrożeniowych i innowacyjnych w tym zakresie, aby Polska dysponowała suwerennym potencjałem kryptologicznym oraz dokonała bezpiecznej migracji do kryptografii postkwantowej oraz mogła wykorzystać technologie kwantowe na rzecz bezpieczeństwa państwa,

h) umożliwienie przetwarzania informacji niejawnych w rządowych narzędziach chmurowych oraz zdefiniowanie w przepisach prawa zasad i wymagań dotyczących przetwarzania informacji niejawnych w chmurze obliczeniowej, w tym zasad przyznawania, odbierania i monitorowania dostępu,

i) rozwijanie zdolności w zakresie rozpoznawania zagrożeń w cyberprzestrzeni (ang. Cyber Threat Intelligence) oraz analityki i przewidywania rozwoju sytuacji w cyberprzestrzeni (ang. Cyber Foresight), tak aby móc odpowiadać na aktualne wyzwania. Działania te będą mogły być wykorzystane na potrzeby zarządzania ryzykiem i wprowadzania mechanizmów korygujących cele operacyjne,

j) wspieranie procesów przygotowania i wdrażania planów awaryjnych przez przedsiębiorców telekomunikacyjnych, umożliwiających nieprzerwane świadczenie usług w sytuacjach szczególnych zagrożeń oraz realizację zobowiązań związanych z obronnością, bezpieczeństwem i porządkiem publicznym,

k) rozwijanie zabezpieczeń w zakresie ochrony danych w bazach i rejestrach urzędowych oraz systemach informacji statystycznej.

[box] Co z tego wynika: Opracujemy plan migracji do kryptografii postkwantowej, co zabezpieczy komunikację obywateli z instytucjami i firmami (np. bankami) przed nastaniem „Dnia Q” – technologie kwantowe uzyskają dojrzałość pozwalającą na łamanie dotychczasowych metod szyfrowania.

Cel 1.3.4: Krajowa baza technologiczno-przemysłowa w obszarze cyberbezpieczeństwa posiada rozwinięty potencjał i cechuje się wysokim stopniem suwerenności technologicznej

Co umożliwi realizację celu:

a) zwiększenie bezpieczeństwa łańcuchów dostaw w wymiarze krajowym i międzynarodowym (zarówno w wymiarze sprzętowym jak i oprogramowania), kierując się interesami bezpieczeństwa narodowego oraz polskiej gospodarki,

b) wprowadzenie mechanizmu umożliwiającego wykluczenie produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawców wysokiego ryzyka,

c) rozwijanie krajowego systemu certyfikacji cyberbezpieczeństwa przez wdrażanie europejskich i tworzenie krajowych programów certyfikacji cyberbezpieczeństwa dla produktów, usług, procesów (ICT) oraz kompetencji personelu,

d) realizacja działań prowadzących do stworzenia polskich rozwiązań cyberbezpieczeństwa, w tym programów i projektów badawczo-rozwojowych i innowacyjnych, zarówno sprzętowych, jak i programowych, co pozwoli na budowę krajowych kompetencji technologicznych i przemysłowych oraz zwiększenie suwerenności technologicznej Polski,

e) realizacja inicjatyw wykorzystujących technologie przełomowe (w tym sztuczną inteligencję) na potrzeby cyberbezpieczeństwa.

[box] Co z tego wynika: Umożliwimy wykluczanie dostawców wysokiego ryzyka w przypadku zidentyfikowania zagrożeń dla bezpieczeństwa państwa. Tym samym zapewnimy obywatelom dostęp do bezpiecznych i pewnych produktów, usług i procesów ICT.

Cel 1.3.5: Kadry podmiotów krajowego systemu cyberbezpieczeństwa oraz społeczeństwo posiadają świadomość cyberzagrożeń oraz wiedzę i kompetencje w zakresie cyberbezpieczeństwa

Co umożliwi realizację celu:

a) zwiększanie świadomości i wiedzy społeczeństwa z zakresu cyberbezpieczeństwa przez realizację kompleksowych działań w zakresie szkolenia i kształcenia na wszystkich poziomach edukacji w dziedzinie cyberbezpieczeństwa, podnoszenia umiejętności i świadomości, włączając w to dobre praktyki oraz higienę cyfrową,

b) wzmacnianie kompetencji kadr podmiotów krajowego systemu cyberbezpieczeństwa na wszystkich szczeblach, w tym przez specjalistyczne szkolenia dla kadry kierowniczej,

c) zapewnienie funkcjonowania Funduszu Cyberbezpieczeństwa i świadczeń teleinformatycznych oraz podjęcie prac nad rozwojem oraz modyfikacją formuły tego Funduszu.

[box] Co z tego wynika: Uruchomimy kolejne szkolenia z zakresu cyberbezpieczeństwa. Nauczysz się jak w bezpieczny sposób korzystać z internetu oraz jak chronić swoją prywatność i pieniądze w sieci.

Cel 1.3.6: Polska posiada silną pozycję międzynarodową w obszarze cyberbezpieczeństwa

Co umożliwi realizację celu:

a) aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym np. udział w pracach (również w wymiarze legislacyjnym) nad podnoszeniem poziomu cyberbezpieczeństwa w wymiarze międzynarodowym, pełnienie przez Polskę kluczowych ról w organizacjach międzynarodowych czy udział w inwestycjach międzynarodowych zwiększających cyberodporność,

b) aktywna współpraca międzynarodowa na poziomie operacyjnym oraz technicznym np. wielostronna wymiana informacji i doświadczeń oraz aktywny udział w ćwiczeniach,

c) prowadzenie przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, we współpracy z innymi organami administracji rządowej, w szczególności z ministrem właściwym do spraw informatyzacji, ministrem właściwym do spraw zagranicznych oraz Ministrem Obrony Narodowej, działań koordynacyjnych na arenie międzynarodowej w zakresie współpracy cywilno-wojskowej w obszarze cyberbezpieczeństwa.

1.4 Koordynacja cyfrowej transformacji kraju

Diagnoza – jak jest?

Horyzontalny charakter procesów cyfryzacji sprawia, że nieodzowna jest efektywna międzyresortowa i ponadsektorowa współpraca oraz systematyzacja wiedzy na temat podejmowanych działań w różnych obszarach działalności państwa. Tak szerokie ujęcie modelu współpracy zmaksymalizuje korzyści dla funkcjonowania administracji, gospodarki i społeczeństwa. Chociaż dotychczasowe inicjatywy w tym zakresie przyniosły pewną poprawę, to efektywne zarządzanie cyfryzacją wymaga większej koordynacji. Wciąż brakuje kompleksowej, spójnej i uporządkowanej informacji na temat stanu informatyzacji podmiotów publicznych i ich efektów. Ma to kluczowe znaczenie, ponieważ monitorowanie i kontrolowanie wdrażania projektów e-administracji w całym kraju poprawia skuteczność prowadzenia projektów, natomiast koordynacja wydatków na ICT pozwala na optymalizację kosztów i strategiczną priorytetyzację inwestycji w oparciu o potrzeby kraju. Pozwala jednocześnie na zwiększenie transparentności i odpowiedzialności w zakresie wydatków publicznych, a pośrednio przekłada się także na zwiększenie konkurencyjności kraju na arenie międzynarodowej.

Dla sprawnej koordynacji cyfrowej transformacji Polski istotny jest nie tylko wymiar wewnętrzny.

Konieczna jest także poprawa koordynacji w obszarze dyplomacji cyfrowej – nowego obszaru polityki zagranicznej państwa, związanego z szybkim rozwojem technologii cyfrowych i ich upowszechnieniem się w stosunkach międzynarodowych. Obszar ten obejmuje m.in. międzynarodowe zarządzanie sztuczną inteligencją i innymi technologiami cyfrowymi, przyciąganie inwestycji zagranicznych czy relacje państw z globalnymi korporacjami technologicznymi. W Polsce dyplomacja cyfrowa jest słabo rozwinięta – brakuje odpowiednich podstaw koncepcyjnych, koordynacji organizacyjnej czy spójnej krajowej strategii w tym obszarze. Skuteczna dyplomacja cyfrowa wymaga wspólnego działania resortów spraw zagranicznych, rozwoju i cyfryzacji.

Uznajemy, że jednym z filarów cyfrowej transformacji jest Architektura Informacyjna Państwa (AIP) - metoda zarządzania informatyzacją państwa, oparta na modelach architektonicznych i obejmująca zasady podstawowe (pryncypia), standardy, wytyczne i rekomendacje architektoniczne, w tym dotyczące interoperacyjności, dostępności, zorientowania na użytkownika, reużywalności danych i komponentów technicznych, dokumentacji, doświadczeń. Kluczowe są zmiany w prawodawstwie, które mogą pomóc skutecznie wdrażać AIP, a także propagowanie jej znaczenia i celów oraz korzyści z jej stosowania, ponieważ deficyt wiedzy o AIP negatywnie wpływa na transformację cyfrową państwa.

Wdrożenie AIP i wypracowanie jednolitych standardów mają kluczowe znaczenie również dla samorządów, w których dotychczas udzielane silosowe wsparcie spowodowało duże zróżnicowanie w realizowanych procesach i wykorzystywanych rozwiązaniach technicznych. Brak uporządkowanej koordynacji spowodował dezorientację i dublowanie się zamawianych rozwiązań na poziomie lokalnym, co z kolei utrudnia współpracę i efektywne zarządzanie cyfryzacją administracji publicznej.

Cel 1.4.1: Wymiana informacji na temat stanu cyfryzacji jednostek administracji publicznej, w tym samorządowej, oraz realizowanych przez nie przedsięwzięć informatycznych jest sprawna i efektywna

Co umożliwi realizację celu:

a) działalność Komitetu do spraw Cyfryzacji, mającego szersze kompetencje niż dotychczas funkcjonujący Komitet Rady Ministrów do spraw Cyfryzacji. Komitet do spraw Cyfryzacji ma zapewniać koordynację działań państwa związanych z informatyzacją oraz wsparcie cyfrowego rozwoju państwa. Jego zadania obejmują rozpatrywanie projektów dokumentów rządowych związanych z informatyzacją, monitorowanie, opiniowanie i publikowanie informacji o przedsięwzięciach informatycznych o publicznym zastosowaniu, monitorowanie realizacji Strategii i innych dokumentów o charakterze strategicznym związanych z informatyzacją,

b) działalność pełnomocników do spraw informatyzacji powoływanych w szczególności w ministerstwach oraz w Kancelarii Prezesa Rady Ministrów oraz fakultatywnie w jednostkach samorządu terytorialnego. Do ich podstawowych zadań należy koordynowanie realizacji i wdrażania Strategii w zakresie spraw należących do właściwości działu administracji rządowej, kierowanego przez właściwego ministra,

c) funkcjonowanie forum współpracy i wymiany informacji w zakresie działań podejmowanych na rzecz transformacji cyfrowej administracji publicznej na poziomie centralnym, regionalnym i lokalnym.

[box] Co z tego wynika: Poprawimy koordynację rozwoju cyfrowego kraju.

Cel 1.4.2: Przedsięwzięcia informatyczne są realizowane i zarządzane w sposób skoordynowany, przejrzysty i efektywny

Co umożliwi realizację celu:

a) wdrożenie i upowszechnienie wspólnej, powiązanej z AIP, metodyki zarządzania przedsięwzięciami informatycznymi realizowanymi we wszystkich jednostkach administracji publicznej pozwalającej na efektywne monitorowanie ich postępów oraz efektów w systemie teleinformatycznym,

b) opracowanie standardów i rekomendacji prowadzenia przedsięwzięć,

c) pełne raportowanie dotyczące podmiotów i osób prowadzących przedsięwzięcia informatyczne dla państwa, które umożliwi zwiększenie przejrzystości i optymalizacji wydatkowania środków,

d) przeprowadzenie kompleksowej diagnozy efektywności udzielania i realizowania zamówień publicznych (perspektywa zamawiającego i wykonawcy) dotyczących przedsięwzięć informatycznych. Sprawdzi ona możliwość wprowadzenia szczególnych zasad dla tych przedsięwzięć w ramach Prawa zamówień publicznych, przez bardziej elastyczne rozwiązania prawne uwzględniające konieczność modyfikacji i zmian technologicznych,

e) opracowanie dobrych praktyk, standaryzujących wymagania funkcjonalne i niefunkcjonalne dotyczące rozwiązań ICT w administracji publicznej pozyskiwanych w ramach postępowań zakupowych, w szczególności w zakresie wzorów umów oraz oceny jakości,

f) przygotowanie rozwiązań wspierających uwzględnianie, w ramach postępowań zakupowych na rozwiązania ICT w administracji publicznej, wymogów suwerenności i bezpieczeństwa, w tym rozwiązań promujących polskich dostawców oraz dostawców pochodzących z państw UE realizujących zamówienia w sposób spełniający te wymogi. Zostaną one przygotowane z uwzględnieniem obiektywnych, merytorycznych i niedyskryminacyjnych kryteriów, zgodnie z obowiązującymi przepisami krajowymi i unijnymi. Wykorzystywanie w sektorach krytycznych rozwiązań opierających się o produkty pochodzące z UE.

[box] Co z tego wynika: Poprawimy zarządzanie projektami informatycznymi i będziemy walczyć z nadużyciami w tym obszarze.

Cel 1.4.3: Architektura Informacyjna Państwa stanowi powszechną i ugruntowaną metodę strategicznego zarządzania informatyzacją państwa

Co umożliwi realizację celu:

a) implementacja pryncypiów oraz opracowanie i wdrożenie standardów, wytycznych i rekomendacji architektonicznych w administracji publicznej, w tym samorządach, a także zobowiązanie podmiotów publicznych wdrażających e-usługi publiczne do ich stosowania,

b) wdrożenie przyjętej metody opisu AIP, w tym słownika pojęć, doprecyzowanie zakresu dla którego metoda będzie stosowana oraz przygotowanie wizji AIP odwzorowującej pożądany stan cyfryzacji kraju w zakresie realizacji e-usług publicznych. Celem wizji AIP jest zaprezentowanie uniwersalnego podejścia do planowania i efektywnego świadczenia e-usług publicznych z dużym naciskiem na niezbędną w tym zakresie interoperacyjność systemów teleinformatycznych,

c) aktualizacja metamodelu AIP (metodyki modelowania) oraz modeli AIP w warstwach legislacyjnej, organizacyjnej, semantycznej i technicznej, umożliwiająca spójne i zintegrowane podejście do tworzenia i modyfikowania procesów oraz systemów teleinformatycznych realizujących cele Strategii,

d) utrzymywanie w aktualności i rozbudowywanie repozytorium AIP, czyli systemu teleinformatycznego, w którym gromadzone są w szczególności modele architektoniczne oraz pryncypia, standardy, wytyczne i rekomendacje architektoniczne,

e) poszerzenie dostępu do informacji zgromadzonych w repozytorium AIP w zakresie dozwolonym ochroną danych (informacje udostępniane kontekstowo w odniesieniu do potrzeb poszczególnych interesariuszy) oraz kooperacja i wymiana bieżących informacji istotnych dla rozwoju i utrzymania AIP, w tym dotyczących identyfikowania reużywalnych komponentów z każdej warstw AIP,

f) analizowanie różnic między stanem obecnym cyfryzacji kraju a docelową wizją określoną w AIP, w celu definiowania przedsięwzięć informatycznych, których realizacja zwiększy efektywność cyfrową państwa,

g) wdrożenie mechanizmów nadzoru i monitoringu wdrażania AIP, w tym:

- powołanie we wszystkich resortach Głównych Architektów Korporacyjnych (których rolę będą mogli pełnić pełnomocnicy do spraw informatyzacji) wspierających upowszechnianie, wdrażanie i rozwój AIP oraz biorących udział w pracach zespołu zadaniowego przy Komitecie do spraw Cyfryzacji wspierającego realizację zadań Komitetu w tym zakresie,

- uzależnienie realizacji i finansowania przedsięwzięć informatycznych o publicznym zastosowaniu od pozytywnej oceny Komitetu do spraw Cyfryzacji

m.in. w zakresie zgodności z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa,

- objęcie obowiązkiem inwentaryzacji wszystkich systemów teleinformatycznych i rejestrów publicznych administracji publicznej, w tym systemów dziedzinowych np. księgowych, kadrowych, przy wykorzystaniu systemów inwentaryzacji systemów teleinformatycznych (SIST, SIST JST),

- weryfikowanie w ramach prac Komitetu do spraw Cyfryzacji zgodności projektów aktów prawnych z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi Architektury Informacyjnej Państwa.

[box] Co z tego wynika: W cyfryzacji administracji będzie przyświecała nam jedna, spójna wizja.

Cel 1.4.4: Transformacja cyfrowa jednostek samorządu terytorialnego jest stale wspierana, a koordynacja między administracją poziomu centralnego oraz regionalnego i lokalnego zapobiega dublowaniu rozwiązań

Co umożliwi realizację celu:

a) opracowanie, rozwój i utrzymanie Architektury Informacyjnej Samorządów (jako komponentu AIP), w tym w zakresie inwentaryzacji, optymalizacji i integracji rozproszonych procesów, oraz wsparcie JST w jej wdrażaniu, w szczególności w zakresie jednolitych standardów świadczenia cyfrowych usług publicznych o wysokiej jakości,

b) wsparcie przez administrację centralną, we współpracy z administracją samorządową, rozwoju rozwiązań usprawniających realizację procesów w JST wynikających z Architektury Informacyjnej Samorządów, m.in.:

- dotyczących wdrożenia metodyki zarządzania przedsięwzięciami informatycznymi (na wzór administracji rządowej),
- integrujących regionalne i lokalne systemy teleinformatyczne z centralnymi,
- oraz usprawniających integrację systemów teleinformatycznych i wymianę danych w ramach danej jednostki (współdzielenie danych).

Projekty realizowane na poziomie centralnym na rzecz JST będą tworzone z uwzględnieniem stanowisk dostawców IT,

c) wdrożenie rozwiązań wspierających współpracę pomiędzy JST m.in. umożliwienie objęcia wsparciem małych JST przez duże JST oraz tworzenie kompleksowych rozwiązań cyfrowych na potrzeby kilku gmin i wspólnych rozwiązań instytucjonalnych dla ich rozwoju i utrzymania,

d) ukierunkowanie i usprawnienie przepływu informacji przez m.in. budowę jednego punktu kontaktu w ramach serwisu samorząd.gov.pl, ułatwiającego komunikację administracji regionalnej i lokalnej z centralną, w tym udostępniającego standardy, wytyczne, rekomendacje i dobre praktyki w zakresie realizacji przedsięwzięć informatycznych,

e) stworzenie krajowego systemu wsparcia dla JST w podejmowaniu decyzji o planowanych wdrożeniach rozwiązań, w tym w obszarze Smart City i Smart Village, zapewniających mieszkańcom realizację ich potrzeb, adresujących globalne wyzwania, stosujących nowoczesne technologie oraz wykorzystujących dane znajdujące się w posiadaniu JST,

f) dążenie do zapewnienia w ramach przyszłej perspektywy finansowej UE wysokiego poziomu finansowania transformacji cyfrowej JST.

Cel 1.4.5: Dyplomacja cyfrowa jest skuteczna i efektywnie koordynowana

Co umożliwi realizację celu:

a) opracowanie wspólnego dla administracji publicznej dokumentu strategicznego wyznaczającego cele i kierunki działania w obszarze dyplomacji cyfrowej. Selekcja priorytetowych państw i organizacji międzynarodowych, jak również opracowanie „geograficznych" polityk cyfrowych zarysowujących plany działania. Obok priorytetowych działań w Europie – zwłaszcza w Europie Środkowo-Wschodniej – konieczne jest zarysowanie planów działania również w obu Amerykach oraz Afryce i Azji,

b) rozwinięcie w urzędzie obsługującym ministra właściwego do spraw informatyzacji kompetencji w zakresie pozyskiwania inwestycji zagranicznych w nowoczesne technologie w Polsce i promowania polskich technologii cyfrowych na świecie oraz przeznaczenie odpowiednich zasobów na ten cel. Pozwoli to m.in. na rozwijanie zdolności w zakresie zapewnienia suwerenności technologicznej w kooperacji z partnerami międzynarodowymi,

c) uwzględnienie jako stałe lub priorytetowe zadania w polskich placówkach dyplomatycznych i urzędach konsularnych w głównych ośrodkach cyfrowych na świecie zadań z zakresu realizacji polityki cyfrowej państwa,

d) regularne tworzenie, we współpracy z odpowiednimi resortami i instytucjami nadzorowanymi, materiałów z zakresu cyfrowych technologii i cyfrowej gospodarki przeznaczonych dla polskich placówek dyplomatycznych. Mają one służyć podwyższaniu kompetencji personelu dyplomatycznego, promowaniu polskich rozwiązań technologicznych, wspieraniu współpracy międzynarodowej z polskimi instytucjami i biznesem oraz ułatwianiu pozyskiwania inwestycji zagranicznych,

e) zapewnienie, by technologie cyfrowe w percepcji i działaniach placówek dyplomatycznych stanowiły odrębny zakres aktywności, niebędący podkategorią współpracy naukowej lub gospodarczej, przy jednoczesnej ścisłej korelacji z tymi obszarami współpracy,

f) zwiększanie zaangażowania Polski w prace organizacji i instytucji międzynarodowych, co umożliwi aktywny wpływ na kształtowanie standardów i regulacji determinujących rozwój kluczowych technologii,

g) wspieranie polskich firm przez ich promocję zarówno na gruncie krajowym jak i międzynarodowym, w tym ułatwienie polskim przedsiębiorcom wchodzenia na zagraniczne rynki i skalowania działalności przez wykorzystanie instrumentów dyplomacji cyfrowej.

[box] Co z tego wynika: Polska dyplomacja będzie mieć narzędzia i kompetencje do skutecznego przyciągania cyfrowych inwestycji i promowania polskich innowacji.

2. Państwo

2.1 E-usługi publiczne

Diagnoza – jak jest?

Kluczowym elementem rozwoju e-administracji są elektroniczne usługi publiczne (e-usługi publiczne), które służą realizacji zadań publicznych za pomocą środków komunikacji elektronicznej. System e-usług publicznych w Polsce w ostatnich latach przeszedł zauważalny rozwój. Serwisy rządowe udostępniają obywatelom ponad 1700 e-usług, które osiągnęły minimum 3 poziom dojrzałości[64]. Dotychczasowe działania koncentrowały się przede wszystkim na udostępnianiu jak największej liczby e-usług publicznych dla obywateli, przedsiębiorców i administracji publicznej mających przynieść wartość dodaną dla użytkownika. Obecne działania skupiają się na tworzeniu i udostępnianiu nowoczesnych e-usług na wyższym poziomie dojrzałości, opartych na istniejących mechanizmach, których realizację wspierają systemy teleinformatyczne oraz rejestry publiczne e-administracji. Kierunki rozwoju e-usług wyznaczają również unijne regulacje prawne, m.in. rozporządzenie eIDAS 2.0[65], które ma na celu ułatwienie przeprowadzania transakcji elektronicznych na poziomie międzynarodowym oraz zwiększenie bezpieczeństwa operacji w świecie cyfrowym. Wdrożenie jednolitych standardów przyczyni się do zwiększenia dostępności e-usług publicznych, zarówno na poziomie krajowym, jak i europejskim. Będzie to miało też istotne znaczenie dla dostawców wszelkiego typu e-usług prywatnych.

Dzięki wzrastającej interoperacyjności podmiotom publicznym jest łatwiej uzyskiwać dostęp do danych gromadzonych od lat przez inne podmioty publiczne. W związku z tym uprawnienia i obowiązki wynikające z przepisów prawa mogą być realizowane bez konieczności tworzenia nowych usług publicznych między podmiotami publicznymi a usługobiorcami. Jest to możliwe, ponieważ informacje niezbędne do ich realizacji znajdują się już w publicznych systemach teleinformatycznych i rejestrach publicznych.

Domyślnie stosowanym podejściem powinien być brak angażowania w realizację zadania publicznego użytkownika (w tym obywatela lub przedsiębiorcy), na którym ciąży obowiązek lub któremu przysługuje uprawnienie wynikające

[64] Stosowana skala dojrzałości e-usług obejmuje następujące stopnie: (i) informacja, (ii) interakcja jednokierunkowa, (iii) interakcja dwukierunkowa, (iv) transakcja oraz (v) personalizacja. Skala została zdefiniowana w publikacji „Smarter, Faster, Better eGovernment. 8th Benchmark Measurement" (https://afyonluoglu.org/PublicWebFiles/eGovBenchmark/EU/2009%20EU%20Benchmark.pdf).
[65] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. Urz. UE L 2024/1183 z 30.04.2024, Dz. Urz. UE L 2025/90317 z 09.04.2025 oraz Dz. Urz. UE L 2025/90945 z 24.11.2025).

z przepisów prawa. Dążyć należy także do maksymalnego ułatwienia urzędnikowi realizacji jego zadań.

Skutkuje to oszczędnością czasu i większym poziomem satysfakcji wśród obywateli, przedsiębiorców oraz urzędników. Oczywiście od takiego podejścia mogą istnieć uzasadnione wyjątki.

Aby realizacja usług publicznych drogą elektroniczną nie sprawiała trudności użytkownikom, e-usługi publiczne powinny być zorientowane na użytkownika - proste i zrozumiałe dla każdego obywatela, przedsiębiorcy oraz urzędnika. Prowadzenie spraw utrudnia także żargon urzędniczy i techniczna terminologia, dlatego niezbędne jest powszechne stosowanie prostego i inkluzywnego języka.
Jednocześnie państwo powinno zapewnić dobrowolność korzystania z rozwiązań cyfrowych, związanych z komunikacją z administracją publiczną oraz realizacją usług. Oznacza to, że użytkownik nadal powinien mieć możliwość załatwienia spraw w urzędzie tradycyjnie, a nie tylko cyfrowo.

Pomimo udostępnienia już wielu e-usług publicznych, wciąż istnieją bariery, które utrudniają ich dostępność, szersze rozpowszechnienie i efektywne wykorzystanie.

Wśród nich można wymienić, m.in.:

a) brak jednego umocowanego prawnie punktu umożliwiającego dostęp do e-usług publicznych dla obywatela, przedsiębiorców i administracji zapewniającego jednolity interfejs, oraz funkcjonalności podpisu elektronicznego i pieczęci elektronicznej,

b) wdrożenie różnorodnych narzędzi (platform) świadczenia i realizacji e-usług publicznych, które nie są zbudowane w oparciu o jednolite standardy umożliwiające uwzględnienie specyficznych potrzeb użytkowników e-usług, m.in.:

   – narzędzi projektowania e-usług publicznych, w tym projektowania formularzy elektronicznych,
   – mechanizmów pozwalających na optymalizację świadczenia e-usługi publicznej, w tym standardów udostępniania usług API,
   – mechanizmów automatyzacji realizacji procesów biznesowych, będących podstawą efektywnej i optymalnej realizacji e-usług publicznych,
   – mechanizmów wykorzystujących rozwiązania horyzontalne wspierające świadczenie i realizację e-usług publicznych, m.in. usługi rejestrowanego doręczenia elektronicznego, systemy realizacji e-płatności, platformy udostępniania rejestrów referencyjnych oraz repozytorium spraw;

c) brak katalogów administracji publicznej, które wspierają interoperacyjność prawną, organizacyjną, semantyczną i techniczną administracji publicznej,

d) brak spójnych mechanizmów zarządzania i monitorowania realizacji e-usług publicznych w celu opracowywania kierunków zwiększania ich efektywności,

e) ograniczone możliwości organizacyjne i finansowe w zakresie wdrażania e-usług, w tym przeprowadzania integracji z dostawcami oprogramowania wspierającego świadczenie i realizację e-usług, również w zakresie w e-płatności,

f) ograniczony katalog e-usług publicznych umożliwiających załatwiane sprawy w pełni on-line oraz brak powszechności stosowania EZD (elektronicznego zarządzania dokumentacją) pozwalającego elektronicznie realizować daną e-usługę także po stronie administracji,

g) niezintegrowane rejestry publiczne oraz systemy teleinformatyczne administracji publicznej, a także brak katalogu metadanych rejestrów publicznych oraz katalogu API (interfejsów programistycznych aplikacji) publicznych systemów teleinformatycznych, co wymusza m.in. wielokrotne wprowadzanie przez użytkownika danych będących w zasobach administracji publicznej,

h) niewystarczający poziom otwartości danych oraz stosowania otwartych formatów wymiany danych, a także wykorzystania platform ich udostępniania w celu wsparcia realizacji e-usług publicznych,

i) brak e-usług publicznych akceptujących transgraniczne metody uwierzytelnienia,

j) niewykorzystany potencjał nowych technologii w procesach tworzenia e-usług publicznych, w tym chmury obliczeniowej,

k) wykluczenie cyfrowe części społeczeństwa utrudniające elektroniczną komunikację z administracją publiczną, np. przez nierówny dostęp do internetu, niedostateczne umiejętności cyfrowe,

l) niedostosowanie e-usług do osób ze szczególnymi potrzebami czy osób starszych.

Działania dotyczące administracji publicznej w tym obszarze mają odpowiednie zastosowanie do sądów powszechnych i wojskowych oraz Prokuratury, uwzględniając jej pozycję prawno-ustrojową i realizowane zadania.

Cel 2.1.1: E-usługi publiczne są dostępne w jednym miejscu i uwzględniają potrzeby wszystkich użytkowników

Co umożliwi realizację celu:

a) wdrożenie jednego punktu dostępu do e-usług publicznych dla każdej z grup odbiorców (obywateli, przedsiębiorców i urzędników), w tym systemu webowego mObywatel i aplikacji mobilnej mObywatel. Zapewniać on będzie jednolity interfejs uspójniający dostępne kanały komunikacji realizacji e-usług - intuicyjny i dostosowany do zróżnicowanych i szczególnych potrzeb użytkowników (m.in. dzięki wykorzystaniu sztucznej inteligencji),

b) dostosowanie wymaganych oraz wybranych istotnych e-usług publicznych do wymogów europejskiego portfela tożsamości cyfrowej, będącego certyfikowanym, uznawanym środkiem identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa, oraz jednolitego portalu cyfrowego[66],

c) organizacja systemowego wsparcia podmiotów świadczących e-usługi publiczne w uspójnieniu działań w zakresie zapewnienia jednolitego dostępu do e-usług oraz środków identyfikacji elektronicznej,

d) opracowanie listy kluczowych e-usług publicznych, pozwalającej na wyznaczenie priorytetów w zakresie modernizacji i wdrażania systemów teleinformatycznych wspomagających ich realizację,

e) prowadzenie i udostępnianie badań potrzeb obywateli, przedsiębiorców lub administracji publicznej w zakresie nowych i modyfikacji istniejących e-usług publicznych. Pozwoli to na wskazywanie, zgodnych z AIP, głównych kierunków tworzenia, rozwijania i optymalizowania procesów oraz rozwiązań cyfrowych wspierających realizację e-usług, a także tworzenia e-usług w językach innych niż polski,

f) opracowanie systemu monitorowania satysfakcji użytkowników, obejmującego regularne zbieranie i analizę danych dotyczących korzystania z e-usług publicznych,

g) opracowanie i wdrożenie spójnego mechanizmu zarządzania i monitorowania realizacji e-usług publicznych w celu określania kierunków ich rozwoju i zwiększania efektywności,

h) opracowanie standardów UX/UI dla wszystkich e-usług oraz bieżące testowanie ich z różnorodnymi grupami użytkowników, na wszystkich etapach procesu wytwórczego oraz umożliwienie wymiany dobrych praktyk dotyczących projektowania doświadczeń użytkowników wśród jednostek administracji publicznej,

[66] Jednolity portal cyfrowy ustanowiony na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1724 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także zmieniającego rozporządzenie (UE) nr 1024/2012 (Dz. Urz. UE L 295 z 21.11.2018, str. 1, z późn. zm.).

i) osiągnięcie pełnej zgodności e-usług z krajowymi i europejskimi wymaganiami dostępności cyfrowej[67], w tym dostosowanie istniejących rozwiązań i obowiązkowe wdrażanie standardów dostępności cyfrowej w nowych projektach[68] oraz prowadzenie bieżących audytów obecnie działających usług pod kątem dostępności,

j) wsparcie użytkownika e-usług publicznych w realizacji jego spraw przy wykorzystaniu chatbota wytrenowanego na danych, niestanowiących danych osobowych, pochodzących z obszarów administracji publicznej.

[box] Co z tego wynika: Udostępnimy w jednym miejscu e-usługi, które będą spójne i zrozumiałe. W korzystaniu z nich pomoże Ci chatbot.

[67] Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440) wdrażająca dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz. Urz. UE L 327 z 02.12.2016, str. 1) oraz ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. poz. 1411).

[68] Określonych w polskiej normie wprowadzającej normę europejską EN 301 549.

Cel 2.1.2: Wdrożone jednolite narzędzia służące realizacji e-usług publicznych ułatwiają interakcję podmiotów świadczących e-usługi z ich użytkownikami

Co umożliwi realizację celu:

a) budowa, udostępnienie i rozwój platform realizacji e-usług publicznych świadczonych na poziomie krajowym, w tym obszarowym, oraz regionalnym i lokalnym, zapewniających standaryzację realizacji e-usług, ich bezpieczeństwo, zgodnie z zasadą „security by design” oraz wysoki poziom dojrzałości,

b) zwiększenie zakresu e-usług publicznych świadczonych przy wykorzystaniu jednolitych platform realizacji e-usług,

c) wyposażenie platform w mechanizmy automatyzacji przy realizacji procesów biznesowych, będących podstawą efektywnej i optymalnej realizacji e-usług publicznych,

d) wyposażenie podmiotów świadczących e-usługi publiczne w generator formularzy - intuicyjne narzędzie do wsparcia samodzielnego wdrażania e-usług publicznych w jednym wspólnym standardzie, dzięki czemu będą one użyteczniejsze i bardziej przyjazne dla użytkownika,

e) wdrożenie funkcjonalności wspierających użytkownika (w tym osób z niepełnosprawnościami) w szybkim załatwieniu spraw online bez jego nadmiernego angażowania,

f) wdrożenie mechanizmów bezpiecznego przesyłania dokumentów elektronicznych, w tym z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej albo kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, umożliwiający jednoznaczną identyfikację nadawcy lub adresata oraz danych przesyłanych w ramach tych usług,

g) wdrożenie systemu obsługi e-płatności wspierającego realizację e-usług publicznych, w tym funkcjonalności obsługi rozrachunków i rozliczeń z obywatelem lub przedsiębiorcą, zarówno polskim, jak i transgranicznym, ze szczególnym uwzględnieniem administracji samorządowej,

h) wdrożenie funkcjonalności automatycznej obsługi spraw załatwianych w ramach realizacji e-usług publicznych, w tym w systemach elektronicznego zarządzania dokumentacją z wykorzystaniem algorytmów sztucznej inteligencji do analizy i przetwarzania danych, zapewniających ochronę danych osobowych,

i) rozbudowa i przekształcenie centralnego rejestru wzorów dokumentów elektronicznych w Katalog wzorów dokumentów, umożliwiający obywatelom posługiwanie się elektronicznymi wersjami dokumentów o charakterze krajowym, regionalnym, lokalnym i zawodowym,

j) zapewnienie dla platform e-usług publicznych odpowiedniej infrastruktury, która pozwoli zagwarantować wysoką jakość e-usług, wydajność i możliwości integracji systemów teleinformatycznych wspomagających ich realizację,
k) ustalenie jednolitych ram integracji i monitorowania usług zewnętrznych (realizowanych zarówno przez podmioty publiczne jak i prywatne) z usługami publicznymi.

[box] Co z tego wynika: E-usługę zrealizujesz szybko i bezpiecznie – pobierzesz dokument z portfela wzorów dokumentów, bezpiecznie prześlesz dane, a Twoja sprawa zostanie możliwie automatycznie obsłużona przez urząd.

Cel 2.1.3: Rozwiązania horyzontalne zapewniają optymalizację świadczonych e-usług publicznych

Co umożliwi realizację celu:

a) wdrożenie rozwiązań horyzontalnych wspierających świadczenie i realizację e-usług publicznych, zapewniających w praktyce bezpieczeństwo oraz wysoki poziom dojrzałości świadczonych e-usług oraz zwiększoną interoperacyjność publicznych systemów teleinformatycznych i rejestrów publicznych wspomagających ich realizację, w tym:

- katalogów pełnomocnictw i upoważnień,

- referencyjnych rejestrów publicznych Katalogów Administracji Publicznej, tj. Katalogu Procesów Administracyjnych, Katalogu Spraw, Katalogu Usług Publicznych, Katalogu Wzorów Dokumentów oraz Katalogu Rejestrów Publicznych i Katalogu Podmiotów Publicznych, uspójniających i zwiększających efektywność działań podejmowanych przez administrację publiczną, w tym wobec obywateli i przedsiębiorców w ramach świadczenia lub realizacji e-usług publicznych,

- krajowej platformy udostępniania danych, katalogu metadanych rejestrów publicznych i API publicznych systemów teleinformatycznych usprawniających wykorzystanie udostępnionych danych, w szczególności danych referencyjnych,

- repozytorium spraw gromadzących informacje o załatwianych przez obywatela i przedsiębiorcę sprawach urzędowych, w tym o statusie tych spraw.

[box] Co z tego wynika: Nie będziesz musieć wielokrotnie podawać tych samych danych – urzędnik sam je pobierze z systemu.

2.2 Cyfryzacja procesów administracyjnych i postępowań sądowych

Diagnoza – jak jest?

Cyfryzacja działania podmiotów publicznych jest procesem ciągłym i ewoluującym. Zależy od wielu czynników, takich jak możliwości technologiczne, potrzeby społeczeństwa, kompetencje cyfrowe obywateli i pracowników instytucji, uwarunkowania prawne. Dlatego też jest konieczne stałe monitorowanie poziomu cyfryzacji instytucji publicznych, analizowanie zjawisk warunkujących ten poziom i odpowiednie reagowanie na bariery we wdrażaniu rozwiązań cyfrowych.

Obecnie w sektorze publicznym funkcjonuje wiele systemów teleinformatycznych i miejsc, w których są gromadzone dane i załatwiane sprawy obywateli.

Warto wspomnieć o całkowitej cyfryzacji procesu wnioskowania o dokumenty paszportowe, stworzeniu systemu rejestrów państwowych czy rozwoju systemów klasy EZD wykorzystywanych w organach administracji publicznej jako narzędzia elektronicznego obiegu dokumentacji.

Niemniej ich potencjał nadal nie jest w pełni wykorzystany. Cyfrowa administracja w Polsce rozwijała się do tej pory w sposób niewystarczająco skoordynowany. Poszczególne podmioty samodzielnie tworzyły różne systemy teleinformatyczne, np. w celu zapewnienia e-usług publicznych, elektronicznego obiegu dokumentów, czy realizacji specyficznych dla danego podmiotu spraw. Ponadto platforma ePUAP zapewniała możliwość udostępnienia stosunkowo prostych usług online, co nie odpowiadało w pełni potrzebom części podmiotów publicznych i prowadziło do tworzenia przez nie własnych rozwiązań pozwalających na świadczenie bardziej złożonych usług. Efektem takiego stanu rzeczy jest to, że obywatel lub przedsiębiorca chcąc załatwić sprawę w sposób elektroniczny, musi używać kilku systemów teleinformatycznych niezależnie, a nawet posługiwać się dokumentami w postaci papierowej. Co więcej, obywatele i przedsiębiorcy często nie wiedzą, w którym miejscu, za pośrednictwem którego systemu e-usług publicznych mają załatwić swoją sprawę.

Brak systematycznego rozwoju odpowiednich rozwiązań informatycznych ogranicza także zakres informacji na temat procesu tworzenia prawa, które są udostępniane obywatelom i przedsiębiorcom (w tym na temat treści projektowanych przepisów i stanu prowadzonych prac). Wpływa to na zmniejszenie ich udziału w tym procesie oraz na dostęp do informacji o prawie, a także na efektywność samego procesu legislacyjnego.

Dodatkowo, pomimo iż wskutek dotychczasowej cyfryzacji instytucji publicznych powstało wiele dużych, skomplikowanych systemów teleinformatycznych i rejestrów publicznych, to nadal występują obszary niezinformatyzowane, gdzie jest wymagana budowa i dostarczenie rozwiązań teleinformatycznych z poziomu centralnego.

Aż 63% instytucji publicznych[69] wciąż funkcjonuje w oparciu o papierowy obieg dokumentów, a w obszarze cyfrowej transformacji instytucji publicznych widać wiele wyzwań.

Niektóre z nich mają charakter systemowy, co uniemożliwia ich rozwiązanie na poziomie poszczególnych instytucji. Dotyczy to m.in. niedostatecznej integracji między publicznymi systemami teleinformatycznymi, braku zunifikowanych, ustandaryzowanych narzędzi elektronicznych do realizacji zadań publicznych czy utrzymania części rejestrów publicznych w postaci papierowej. Brakuje także standaryzacji stosu technologicznego oraz komponentów architektury zorientowanej na usługi w administracji publicznej. Dostępność dostosowanej do potrzeb administracji, skalowalnej infrastruktury jest nadal niska. Zróżnicowany poziom kompetencji urzędników oraz różnice w możliwościach finansowych instytucji publicznych przekładają się na nierównomierny poziom ich cyfryzacji. Wobec nieustającego postępu w sektorze informatycznym, jest konieczne ciągłe dostosowywanie publicznych systemów teleinformatycznych do nowoczesnych rozwiązań.

Działania te obniżą koszty realizacji procesów i ich obsługi w instytucjach publicznych np. przez wprowadzenie centralnych zamówień na usługi w zakresie chmury publicznej, dzięki którym jednostki będą mogły szybko nabywać usługi chmurowe przy znacznie mniejszym zaangażowaniu urzędników.

Działania dotyczące administracji publicznej i wymiaru sprawiedliwości w tym obszarze mają odpowiednie zastosowanie do Prokuratury, uwzględniając jej pozycję prawno-ustrojową i realizowane zadania.

[69] Informacja na podstawie badań własnych NASK: „Systemy klasy EZD w administracji publicznej - badanie samorządów", marzec 2022; „Badanie potrzeb jednostek administracji rządowej w zakresie wdrożeń EZD", październik 2023.

Cel 2.2.1: Procesy back-office w administracji publicznej są prowadzone cyfrowo

Co umożliwi realizację celu:

a) wdrożenie ujednoliconego sposobu opisu i ustandaryzowanych procesów oraz procedur dotyczących funkcjonowania administracyjnego zaplecza jednostek administracji publicznej, które wspomagają realizację głównych zadań dotyczących załatwiania spraw po stronie obywatela, przedsiębiorcy i administracji,

b) automatyzacja i optymalizacja wykonywania procesów administracyjnych, z wykorzystaniem referencyjnych procesów z Katalogu Procesów Administracyjnych, danych pozyskiwanych przez API publicznych systemów teleinformatycznych oraz rozwiązań sztucznej inteligencji - przy zachowaniu nadzoru i możliwości interwencji przez człowieka,

c) wprowadzenie obowiązku stosowania elektronicznego zarządzania dokumentacją jako podstawowego modelu zarządzania dokumentacją w podmiotach publicznych przy użyciu systemów teleinformatycznych klasy EZD. Jednym z elementów tego działania będzie wskazanie minimalnego poziomu funkcjonalności dla systemów klasy EZD, w tym w zakresie integracji z innymi systemami,

d) nowelizacja przepisów kancelaryjno-archiwalnych oraz monitorowanie poziomu wykorzystania systemów klasy EZD w podmiotach realizujących zadania publiczne pod kątem redukcji spraw dokumentowanych papierowo,

e) rozwój i upowszechnianie aplikacji EZD RP oraz udostępnienie usługi chmurowej EZD RP, bezpłatnie świadczonych na rzecz administracji publicznej. Zapewnienie podmiotom publicznym nieodpłatnego wsparcia we wdrażaniu i utrzymaniu EZD RP oraz wsparcie procesu migracji do EZD RP,

f) ustawowe umocowanie systemu EZD RP, dostarczającego podmiotom publicznym narzędzi do realizacji zadań kancelaryjno-archiwalnych oraz umożliwienie integracji z innymi systemami back office dla administracji publicznej. Wskazanie podmiotu odpowiedzialnego za rozwój systemu EZD RP oraz bezpłatne wsparcie wdrożeniowe i utrzymaniowe EZD RP świadczone na rzecz podmiotów publicznych,

g) przyjęcie „Polityki wdrażania elektronicznego zarządzania dokumentacją do 2035 r.” wyznaczającej planowany zakres działań w obszarze cyfryzacji back-office administracji publicznej do 2035 r.,

h) budowa i wdrożenie jednolitego i dostępnego nieodpłatnie systemu dla jednostek sektora finansów publicznych do obsługi finansowo-księgowej i kadrowej. Zapewnienie podmiotom wsparcia we wdrażaniu, procesie migracji oraz utrzymaniu systemu.

[box] Co z tego wynika: Komunikacja wewnątrz urzędów i między nimi będzie uproszczona i bardziej efektywna, a praca urzędników łatwiejsza i szybsza.

Cel 2.2.2: Otoczenie prawne sprzyja informatyzacji podmiotów publicznych

Co umożliwi realizację celu:

a) dostosowanie przepisów prawa do realizacji zadań publicznych za pomocą środków komunikacji elektronicznej, w tym wprowadzenie domyślności cyfrowej w KPA (kodeksie postępowania administracyjnego)[70], KPK (kodeksie postępowania karnego)[71] i KPC (kodeksie postępowania cywilnego)[72], uproszczenie procedur administracyjnych oraz wprowadzanie elektronicznej postaci dokumentów. Ułatwi to znacznie użytkownikom komunikację z organami administracji publicznej i innymi podmiotami zewnętrznymi,

b) pełne wdrożenie i upowszechnienie elektronicznych doręczeń (e-Doręczeń) zarówno w relacjach między podmiotami publicznymi, jak i z podmiotami niepublicznymi, które zastąpi doręczanie korespondencji przez elektroniczną skrzynkę podawczą ePUAP,

c) wprowadzenie obowiązku integracji e-usług z e-Doręczeniami, co zapewni obywatelom i przedsiębiorcom jedno miejsce, w którym będą mieli zgromadzoną całą korespondencję z urzędami, bez względu na to, z którego serwisu udostępniającego e-usługi korzystali.

[box] Co z tego wynika: Załatwisz online jeszcze więcej spraw, a cała korespondencja ze wszystkimi urzędami będzie w jednym miejscu – w skrzynce e-Doręczeń.

[70] Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).
[71] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2026 r. poz. 490, 421 i 638).
[72] Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2026 r. poz. 468 i 473).

Cel 2.2.3: Monitorowanie informatyzacji podmiotów publicznych pozwala efektywniej kierować procesem wdrażania zmian w tym zakresie

Co umożliwi realizację celu:

a) monitorowanie wdrażania w budowanych lub rozwijanych systemach teleinformatycznych, w tym wspierających realizację e-usług publicznych, rozwiązań horyzontalnych (na przykład takich jak wykorzystanie środków identyfikacji elektronicznej, platform udostępniania danych, systemów realizacji e-płatności oraz repozytorium spraw),

b) monitorowanie postępów i efektów realizowanych przedsięwzięć informatycznych o publicznym zastosowaniu w ramach prac Komitetu do spraw Cyfryzacji,

c) formułowanie wniosków z przeprowadzonego monitoringu działań podejmowanych w ramach informatyzacji podmiotów publicznych i weryfikacja przyjętych kierunków działań na tej podstawie.

[box] Co z tego wynika: Będziemy monitorować poziom informatyzacji podmiotów publicznych i na tej podstawie wyznaczymy kierunki działań.

Cel 2.2.4: Wykorzystanie e-usług i nowoczesnych technologii wspiera funkcjonowanie wymiaru sprawiedliwości

Co umożliwi realizację celu:

a) udostępnienie zaawansowanych e-usług z zakresu wymiaru sprawiedliwości wspieranych nowoczesnymi technologiami, które m.in. umożliwią dwukierunkową komunikację, dostęp do informacji oraz realizację spraw przez obywateli i przedsiębiorców w sposób elektroniczny, przy jednoczesnym zwiększeniu transparentności procesów,

b) optymalizacja ekonomiki procesowej przy uwzględnieniu stosowania elektronicznych dokumentów, elektronicznych czynności procesowych czy przeprowadzania posiedzeń i rozpraw w formie wideokonferencji,

c) podniesienie komfortu oraz jakości pracy pracowników wymiaru sprawiedliwości przez wdrażanie rozwiązań automatyzujących pracę, w tym opartych na sztucznej inteligencji. Rozwiązania te będą stosowane po przeprowadzeniu analizy ryzyk oraz z zachowaniem poszanowania praw i wolności obywatelskich,

d) uzyskanie wysokiego poziomu interoperacyjności systemów wymiaru sprawiedliwości z systemami krajowym i międzynarodowymi z ich otoczenia pozwalający na wzmocnienie cyfrowej współpracy oraz dostępu do danych.

Cel 2.2.5: Wykorzystanie nowoczesnych technologii wspiera tworzenie prawa oraz powszechny dostęp do informacji o prawie

Co umożliwi realizację celu:

a) wprowadzenie jednolitego sposobu identyfikacji prac legislacyjnych,

b) wdrożenie systemu zapewniającego powszechny, przejrzysty dostęp do informacji na temat prac legislacyjnych i do dokumentów związanych z procesem legislacyjnym oraz narzędzia upraszczające, w tym zwiększające automatyzację czynności wykonywanych podczas prac nad projektami aktów normatywnych,

c) budowa systemu zapewniającego powszechny dostęp do skonsolidowanych tekstów obowiązujących aktów prawnych, który umożliwia zamieszczanie dodatkowych informacji dotyczących przepisów prawnych,

d) opracowanie narzędzi AI wspierających tworzenie jasnych i zrozumiałych przepisów prawa i ocen skutków regulacji, monitoring zmian w przepisach prawa i obsługę procesu legislacyjnego oraz powszechny dostęp do informacji o prawie,

e) opracowanie standardów do przygotowania oraz publikacji aktów prawnych w strukturze gotowej do odczytu maszynowego i wykonywania maszynowego (ang. law as code),

f) budowa i rozwój rejestrów publicznych zapewniających powszechny dostęp do danych przestrzennych. Opracowanie standardów, w szczególności aktów prawnych tworzonych w postaci ustandaryzowanych i jednolitych schematów danych przestrzennych,

g) rozwój narzędzi cyfrowych zwiększających dostępność informacji i zasobów związanych z konsultacjami publicznymi.

[box] Co z tego wynika: Łatwiej odnajdziesz informacje na temat praw i obowiązków wynikających z prawa.

2.3 Publiczne systemy teleinformatyczne i rejestry publiczne

Diagnoza – jak jest?

Systemy teleinformatyczne i rejestry publiczne wykorzystywane przez administrację publiczną nie są w pełni interoperacyjne. Wielokrotne, niepotrzebne gromadzenie danych powoduje, że podmioty publiczne napotykają liczne bariery utrudniające wdrożenie optymalnych rozwiązań dla realizacji zadań publicznych. Liczne niezgodności danych w różnych rejestrach publicznych utrudniają identyfikację zasobów dostępnych w systemach administracji, z których podmioty publiczne mogłyby korzystać. Instytucje publiczne mają wciąż niewystarczającą wiedzę o dostępnych danych i rozwiązaniach gotowych do ponownego wykorzystania oraz możliwości ich wykorzystania na etapie wdrażania nowych lub rozwijanych istniejących rozwiązań IT dla administracji. Powoduje to niewystarczająco sprawną współpracę instytucji publicznych. W efekcie podmioty publiczne angażują pracowników do czasochłonnego poszukiwania i weryfikacji danych w wielu źródłach, bez gwarancji jakości tych danych.

Dane do rejestrów publicznych są w dużej mierze dostarczane i aktualizowane wskutek obowiązków, jakimi są objęte podmioty publiczne. Biorąc pod uwagę liczbę systemów teleinformatycznych i rejestrów publicznych, w których podmioty muszą uzupełniać dane oraz brak komunikacji i wymiany danych między systemami i rejestrami w zakresie tych samych danych, a także rozwiązań automatyzujących te procesy, utrzymanie wysokiej jakości danych jest obarczone ryzykiem.

Widoczny jest także niedostatek danych i narzędzi do analizy zachowań użytkowników systemów teleinformatycznych i rejestrów publicznych wykorzystywanych przez administrację publiczną. Jest to istotne, aby zidentyfikować potrzeby użytkowników i newralgiczne zmiany konieczne do wprowadzenia w dostarczanych systemach i rejestrach. Podmioty publiczne są zobowiązane do udostępniania danych z rejestrów publicznych innym podmiotom na warunkach, w sposób, w zakresie i terminie określonym w przepisach, na których podstawie jest prowadzony rejestr. Istotnym wyzwaniem pozostaje brak jednolitych standardów dotyczących procedur uzyskiwania dostępu do rejestrów publicznych. Brak jest powszechnie obowiązującego i publicznie dostępnego standardu API dla systemów teleinformatycznych służących do realizacji zadań publicznych, który ułatwiałby i przyspieszał integrację rozwiązań cyfrowych, przyczyniając się do zwiększenia interoperacyjności, w tym dostępności i jakości zasobów informacyjnych państwa.

Działania dotyczące administracji publicznej w tym obszarze mają odpowiednie zastosowanie do sądów powszechnych i wojskowych oraz Prokuratury, uwzględniając jej pozycję prawno-ustrojową i realizowane zadania.

Cel 2.3.1: Publiczne systemy teleinformatyczne i rejestry publiczne są interoperacyjne

Co umożliwi realizację celu:

a) upowszechnienie i wdrożenie pryncypiów architektonicznych oraz standardów, wytycznych i rekomendacji architektonicznych, w tym dotyczących interoperacyjności systemów teleinformatycznych i rejestrów publicznych oraz ponowne wykorzystanie danych i komponentów technicznych, jako podstawowych zasad tworzenia i rozwoju systemów informacyjnych państwa,

b) opracowanie i wejście w życie aktu wykonawczego regulującego Krajowe Ramy Interoperacyjności, minimalne wymagania dla rejestrów publicznych i minimalne wymagania dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi[73], na gruncie którego ustandaryzowany zostanie możliwie jak najszerszy i najwygodniejszy dostęp do zasobów informacyjnych państwa za pomocą API, w trybie do odczytu maszynowego,

c) powierzenie Komitetowi do spraw Cyfryzacji zadań związanych z weryfikowaniem projektów aktów prawnych oraz przedsięwzięć informatycznych o publicznym zastosowaniu mających na celu tworzenie publicznych systemów teleinformatycznych i rejestrów publicznych m.in. pod kątem zgodności ze Strategią Cyfryzacji Państwa i Strategią Cyberbezpieczeństwa RP, przepisami dotyczącymi interoperacyjności europejskiej oraz krajowej, a także zgodności z minimalnymi wymaganiami dla publicznych systemów teleinformatycznych, rejestrów publicznych i wymiany danych z podmiotami publicznymi oraz uzależnienie realizacji i finansowania przedsięwzięć informatycznych o publicznym zastosowaniu od pozytywnej oceny Komitetu,

d) wdrożenie mechanizmów wspierających budowanie nowych i modyfikowanie istniejących publicznych systemów teleinformatycznych i rejestrów publicznych w sposób spełniający wymagania interoperacyjności prawnej, organizacyjnej, semantycznej i technologicznej, w tym unikających nadmiernego angażowania ich użytkowników,

e) przeprowadzanie okresowych przeglądów użyteczności systemów teleinformatycznych w oparciu o mierzalne wskaźniki, których celem jest identyfikacja obszarów do poprawy i podjęcie interwencji poprawiających jakość systemu,

f) zapewnienie unikalnych identyfikatorów dla zasobów informacyjnych państwa w ramach warstw interoperacyjności prawnej, organizacyjnej, semantycznej i technologicznej (dotyczących m.in. aktów prawa powszechnego, dokumentów

[73] Projekt rozporządzenia Rady Ministrów w sprawie szczegółowych sposobów realizacji obowiązków w zakresie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych, minimalnych wymagań dla systemów teleinformatycznych używanych do realizacji zadań publicznych i wymiany danych z podmiotami publicznymi.

strategicznych, rejestrów publicznych, publicznych systemów teleinformatycznych), w celu zapewnienia jednoznacznego przywoływania takich zasobów w dokumentacji i jednoznacznej identyfikacji powiązań między takimi zasobami (w tym na potrzeby wyników ocen interoperacyjności krajowej i transgranicznej),

g) dokonywanie cyklicznie przeglądu standardów oraz specyfikacji dotyczących publicznych systemów teleinformatycznych i rejestrów publicznych, w celu ich oceny pod kątem zdolności do zapewniania interoperacyjności,

h) przeprowadzanie ocen interoperacyjności krajowej i ocen interoperacyjności transgranicznej, obejmujących analizę wpływu zmian wprowadzanych w publicznych systemach teleinformatycznych i rejestrach publicznych na krajowe i europejskie podmioty publiczne,

i) zwiększanie interoperacyjności transgranicznej zgodnie z zasadami Europejskich Ram Interoperacyjności:

- domyślności cyfrowej (tj. domyślne dostarczanie e-usług publicznych i danych za pośrednictwem kanałów cyfrowych),

- domyślnej transgraniczności (tj. e-usługi publiczne są dostępne dla wszystkich obywateli UE),

- domyślnej otwartości (tj. e-usługi publiczne umożliwiające ponowne wykorzystanie, uczestnictwo/dostęp i przejrzystość).

Cel 2.3.2: Udostępnianie wysokiej jakości danych z rejestrów publicznych i publicznych systemów teleinformatycznych odbywa się w sposób bezpieczny i zautomatyzowany

Co umożliwi realizację celu:

a) zapewnienie kompletności, dostępności, przejrzystości, spójności i jednolitości danych zbieranych i aktualizowanych na potrzeby rejestrów publicznych i publicznych systemów teleinformatycznych,

b) umocowanie w przepisach koncepcji referencyjnych rejestrów publicznych, czyli rejestrów publicznych formalnie wskazanych jako autentyczne źródła danych dla innych rejestrów publicznych i systemów teleinformatycznych w określonym zakresie danych,

c) przygotowanie, udostępnienie i aktualizacja referencyjnych rejestrów publicznych „Katalogów Administracji Publicznej", tj. Katalogu Procesów Administracyjnych, Katalogu Spraw, Katalogu Usług Publicznych, Katalogu Wzorów Dokumentów (uwzględniając funkcjonujące Centralne Repozytorium Wzorów Dokumentów Elektronicznych) oraz Katalogu Rejestrów Publicznych (uwzględniając przygotowane repozytorium interoperacyjności),

d) umocowanie prawne katalogów administracji publicznej w celu automatycznego zasilania i wymiany danych oraz zmniejszenia obciążeń administracyjnych obywateli, przedsiębiorców i administracji publicznej związanych z dostarczaniem i aktualizowaniem tych danych, w tym Katalogu Podmiotów Publicznych (KPP) w zakresie obligatoryjnej integracji KPP z systemami administracji publicznej, które wymagają danych dotyczących podmiotów publicznych i niepublicznych, którym powierzono lub zlecono realizację zadań publicznych,

e) przegląd obowiązujących przepisów prawa ustanawiających rejestry publiczne i pełne zobligowanie prawne do prowadzenia rejestrów publicznych jedynie przy pomocy systemów teleinformatycznych oraz stosowania jednolitych mechanizmów ułatwiających walidację i monitorowanie jakości gromadzonych w nich danych, z uwzględnieniem działań administracji rządowej wspierających jednostki samorządu terytorialnego,

f) przyjęcie powszechnie obowiązującego i jawnego standardu API dla systemów teleinformatycznych służących do realizacji zadań publicznych, wykorzystującego doświadczenia rynku dostawców produktów i usług IT,

g) nałożenie wymogu udostępniania danych z publicznych systemów teleinformatycznych i rejestrów publicznych przez API, przy jednoczesnym uwzględnieniu architektury poszczególnych rejestrów oraz wymogów bezpieczeństwa,

h) udostępnianie publicznie katalogu API publicznych systemów teleinformatycznych, a także informacji o strukturze i znaczeniu danych przechowywanych we wszystkich

rejestrach publicznych; poszerzone o informacje o słownikach, schematach klasyfikacyjnych, taksonomiach oraz listach kodowych w rejestrach publicznych,

i) wprowadzenie wymogu publikacji informacji o interfejsach programistycznych aplikacji systemów teleinformatycznych używanych do realizacji zadań publicznych oraz ustandaryzowanego zbioru metadanych każdego rejestru publicznego w repozytorium interoperacyjności, a także zapewnienia poprawności, aktualności i kompletności takich metadanych,

j) stworzenie krajowej platformy udostępniania danych, jako rozwiązania organizacyjno-technicznego zapewniającego ustandaryzowane mechanizmy dostępu do danych referencyjnych przetwarzanych w rejestrach publicznych, umożliwiającego m.in. mechanizm subskrypcji powiadomień o zmianach kluczowych danych w rejestrach za zgodą osób, których dane dotyczą,

k) wykorzystywanie Zintegrowanej Platformy Analitycznej umożliwiającej analizę zbiorów danych poddanych pseudonimizacji i zintegrowanych danych pochodzących z różnych źródeł administracji publicznej do efektywnego projektowania polityk publicznych,

l) sukcesywne wdrażanie mechanizmów typu piaskownice API udostępniających aktualizowane prototypy API kolejnych systemów administracji publicznej, umożliwiających podmiotom zainteresowanym łatwiejsze opracowywanie innowacyjnych projektów nowych e-usług w oparciu o te dane,

m) dalsze upraszczanie i cyfryzacja procesów wnioskowania o dostęp do rejestrów publicznych, obejmujące klarowny opis procesu uzyskania dostępu i właściwie adresujący dedykowane wnioski wraz z instrukcjami, niezbędne do uzyskania dostępu do rejestrów, w zależności od trybu dostępu i rodzaju aplikującego o dostęp podmiotu,

n) poszerzenie mechanizmów dostępu do danych z rejestrów publicznych z poziomu systemów komercyjnych, przez wprowadzenie automatycznych powiadomień o zmianach danych, w sposób zapewniający ochronę danych osobowych,

o) rozszerzanie wykorzystywania źródeł administracyjnych i danych od gestorów prywatnych, w tym w celu ograniczenia redundancji danych, na rzecz rozszerzenia zasobu informacyjnego statystyki publicznej, dostosowanego do potrzeb różnych grup użytkowników.

[box] Co z tego wynika: Załatwianie spraw w urzędach będzie znacznie szybsze i łatwiejsze – przy jednoczesnym zachowaniu nadzoru człowieka nad procesami decyzyjnymi.

2.4 Cyfrowa tożsamość

Diagnoza – jak jest?

W Polsce od wielu lat z powodzeniem funkcjonuje federacyjny model tożsamości cyfrowej, w którym użytkownik samodzielnie decyduje, z jakiego środka identyfikacji elektronicznej chce skorzystać w e-usłudze publicznej. Obecnie użytkownicy w ramach publicznego systemu identyfikacji elektronicznej mają do dyspozycji profil zaufany, profil osobisty (w warstwie elektronicznej tzw. e-dowodu) oraz profil mObywatel. Profil osobisty i profil mObywatel mogą być wykorzystywane również do uwierzytelniania użytkowników w e-usługach niepublicznych, tym samym rozwój środków identyfikacji elektronicznej przyczynia się do rozwoju ekosystemu usług prywatnych. Dodatkowo polscy obywatele i rezydenci mogą także korzystać z tzw. środków bankowych dostępnych w ramach systemu mojeID. Rozwiązanie to nie tylko sprawia, że użytkownicy e-usług przyłączonych do węzła krajowego identyfikacji elektronicznej mają możliwość swobodnego wyboru środka identyfikacji elektronicznej, lecz także pozwala podmiotom świadczącym usługi online integrować je z całym pakietem dostępnych środków identyfikacji elektronicznej.

Oprócz identyfikacji elektronicznej zapewniającej potwierdzenie tożsamości osób w e-usługach, niezbędnym elementem uzupełniającym możliwość korzystania z takich usług są podpisy elektroniczne. Obecnie na rynku dostępne są publiczne, nieodpłatne rozwiązania: podpis zaufany oraz podpis osobisty, a także komercyjne, odpłatne, oferowane przez kwalifikowanych dostawców usług zaufania kwalifikowane podpisy elektroniczne.

Powyższe modele obarczone są jednak ograniczeniami, które wpływają negatywnie na powszechność zastosowania środków identyfikacji elektronicznej, podpisów elektronicznych i szerzej e-usług.

Ze środków identyfikacji elektronicznej korzystać mogą teraz wyłącznie osoby fizyczne, bez rozróżnienia na role czy konteksty, w których uwierzytelniają się online. Nie zostały dotychczas wdrożone rozwiązania, które pozwalałyby na bezpośrednie uwierzytelnianie się spółek, instytucji czy innych podmiotów zbiorowych (osób prawnych), a także osób fizycznych działających jako pełnomocnicy czy przedstawiciele osób prawnych (w tym urzędników). Obecnie, aby doszło do uwierzytelnienia tych podmiotów, konieczne jest dodatkowe potwierdzenie uprawnień do reprezentacji oraz ich weryfikacja, co prowadzi do utrudnień w obsłudze spraw i wydłuża czas oczekiwania na załatwienie sprawy.

Aktualnie osoba fizyczna, która działa w imieniu i na rzecz osoby prawnej w e-usłudze publicznej, musi po uwierzytelnieniu przedstawić dodatkowo informację, a często także stosowny dokument potwierdzający jej uprawnienia do reprezentacji, a po stronie urzędu musi nastąpić manualna weryfikacja tego faktu. W sytuacji, w której dana e-usługa publiczna skierowana jest bezpośrednio do osób prawnych (np. spółek handlowych), dostawca często

musi albo stosować niekonwencjonalne metody potwierdzania tożsamości osób prawnych lub przeznaczyć dodatkowe zasoby kadrowe na weryfikację praw do reprezentacji.

Brak dostosowania e-usług publicznych do obsługi osób prawnych jest zauważalny także w aspekcie obsługi podpisów elektronicznych w sytuacjach, w których wieloosobowa reprezentacja podmiotu wymaga złożenia więcej niż jednego podpisu elektronicznego. Brakuje gotowego, nieodpłatnego, prostego do integracji narzędzia, które umożliwiałoby proste składanie wielu podpisów z poziomu e-usługi publicznej, bez względu na to, jakim podpisem dysponuje osoba podpisująca (kwalifikowanym, osobistym czy zaufanym).

Podmioty publiczne mierzą się również z problemem niewystarczająco wygodnej obsługi podpisów elektronicznych. Ułatwione powinno zostać w szczególności składanie kwalifikowanych podpisów elektronicznych, zwłaszcza tak zwanych podpisów zdalnych – składanych za pomocą urządzeń do składania podpisu elektronicznego na odległość. Ułatwienie składania zdalnych kwalifikowanych podpisów elektronicznych we wszystkich krajowych usługach publicznych jest ważne także z tego powodu, że kwalifikowane podpisy elektroniczne, w odróżnieniu od podpisu zaufanego i podpisu osobistego – nie mają ograniczeń formalnoprawnych w ich zastosowaniu i są ważne zarówno w usługach publicznych jak prywatnych w całej Unii Europejskiej. Ponadto w dyrektywie NIS 2 znajduje się wytyczna, aby zachęcać podmioty kluczowe i ważne (czyli również podmioty publiczne) do korzystania z kwalifikowanych usług zaufania.

Konieczne jest również umożliwienie weryfikowania dokumentów opatrzonych nie tylko podpisem zaufanym, ale także podpisem osobistym i kwalifikowanym podpisem elektronicznym oraz eliminacja błędów, które pojawiły się na przestrzeni lat w rozwoju rynku podpisów elektronicznych.

Ponadto zauważalne są ograniczenia w transgranicznym korzystaniu z e-usług publicznych i to pomimo obowiązującej unijnej zasady wzajemnego uznawania przez państwa członkowskie notyfikowanych środków identyfikacji elektronicznej oraz kwalifikowanych podpisów elektronicznych.

Polska posiada dwa notyfikowane środki identyfikacji elektronicznej: profil zaufany i profil osobisty, jednak ich praktyczne użycie w usługach online innych państw członkowskich jest nieznaczne.

Problemy w tym obszarze wynikają głównie z tego, że zestaw danych składający się imienia, nazwiska i daty urodzenia nie identyfikuje osób fizycznych jednoznacznie, a niepowtarzalne identyfikatory nadawane przez państwa członkowskie stanowiące uzupełnienie tego zestawu nie są rozpoznawane w innych krajach niż kraj, w którym je nadano. Na przykład w Polsce w zdecydowanej większości usług online wymagany jest numer PESEL, co powoduje, że w praktyce akceptowalność notyfikowanych środków z innych państw członkowskich jest na bardzo niskim poziomie. Podobnie jest w przypadku używania polskich notyfikowanych środków identyfikacji elektronicznej w innych krajach Unii, w których oczekuje się identyfikatora innego niż PESEL. Komisja Europejska, dostrzegając te systemowe i praktyczne problemy we wzajemnym uznawaniu środków identyfikacji elektronicznej, zaproponowała szereg rozwiązań nakierowanych na wzmocnienie bezpieczeństwa i swobody przeprowadzania transakcji elektronicznych w ramach jednolitego rynku

cyfrowego, dla których podstawą prawną jest rozporządzenie eIDAS 2.0. Przewiduje ono wprowadzenie do końca 2026 r. europejskich portfeli tożsamości cyfrowej, zapewniających identyfikację elektroniczną na wysokim poziomie bezpieczeństwa, dzięki którym obywatele będą mogli swobodnie korzystać z publicznych i komercyjnych usług online oraz w sposób selektywny i bezpieczny dzielić się informacjami o sobie. Transgraniczną skuteczność europejskich portfeli tożsamości cyfrowej, jak również już notyfikowanych środków identyfikacji elektronicznej państwa członkowskie mają zapewnić świadcząc specjalne usługi dopasowywania tożsamości umożliwiające swobodne korzystanie co najmniej z usług publicznych. Rozporządzenie zwraca szczególną uwagę na ochronę danych osobowych i prywatności użytkowników europejskiego portfela tożsamości cyfrowej oraz podkreśla, że korzystanie z niego jest dobrowolne, a w konsekwencji zapewniona musi być możliwość korzystania z usług również w inny sposób. Ponadto portfele mają zapewnić możliwość składania kwalifikowanego podpisu elektronicznego dostępnego za darmo, co najmniej do użytku nieprofesjonalnego.

W celu promowania i przyspieszania rozwoju systemów identyfikacji elektronicznej, a także jednoczesnego dbania o bezpieczeństwo ich licznych użytkowników, jest konieczne ciągłe podnoszenie poziomu cyberbezpieczeństwa środków identyfikacji elektronicznej wydawanych w ramach tych systemów. Niezbędna jest również dalsza edukacja publiczna w zakresie możliwości realizacji spraw urzędowych online oraz właściwego sposobu korzystania ze środków identyfikacji elektronicznej, tak aby zapobiegać kradzieżom tożsamości, naruszeniom ochrony danych osobowych, cyberatakom i innym niebezpiecznym sytuacjom w Internecie.

Działania dotyczące administracji publicznej w tym obszarze mają odpowiednie zastosowanie do sądów powszechnych i wojskowych oraz Prokuratury, uwzględniając jej pozycję prawno-ustrojową i realizowane zadania.

Cel 2.4.1: Osoby prawne mogą w prosty sposób i w krótkim terminie załatwiać sprawy urzędowe online

Co umożliwi realizację celu:

a) utworzenie w ramach publicznego systemu identyfikacji elektronicznej środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej reprezentującej osobę prawną,

b) skuteczne umocowanie prawne środka identyfikacji elektronicznej dla osoby prawnej oraz środka identyfikacji elektronicznej dla osoby fizycznej repezentującej osobę prawną, aby mógł on służyć do automatycznego uwierzytelniania w usługach publicznych online, bez konieczności każdorazowej manualnej weryfikacji przez urzędnika prawidłowości i aktualności przedstawianych pełnomocnictw lub upoważnień do reprezentacji,

c) stworzenie nowych lub zmodyfikowanie istniejących usług publicznych tak, aby akceptowały wydane środki identyfikacji elektronicznej dla osób prawnych i środki identyfikacji elektronicznej dla osób fizycznych reprezentujących osoby prawne,

d) udostępnienie narzędzia zapewniającego możliwość łatwego i wygodnego składania w usługach publicznych podpisów elektronicznych niezależnie od ich rodzaju i formatu dokumentu w przypadku wieloosobowej reprezentacji osoby prawnej (“wielopodpis”),

e) udostępnienie europejskiego portfela tożsamości cyfrowej do użytku osób prawnych.

[box] Co z tego wynika: Osoby prawne i ich reprezentanci sprawnie załatwią sprawy urzędowe i biznesowe oraz potwierdzą swoje usprawnienia i złożą podpisy na dokumentach.

Cel 2.4.2: Podpisy elektroniczne są dostępne i powszechnie używane, a ich weryfikacja jest prosta i niezawodna bez względu na format dokumentu i rodzaj podpisu

Co umożliwi realizację celu:

a) rozwój narzędzi do podpisywania i weryfikowania dokumentów podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym. Opracowanie, we współpracy z rynkiem, krajowej polityki tworzenia, akceptacji i weryfikacji podpisów elektronicznych, poprzedzonej kompleksową inwentaryzacją istniejących mechanizmów,

b) rozpowszechnienie informacji o korzyściach wynikających z korzystania z możliwości składania i weryfikowania podpisów elektronicznych w ich systemach w ujednolicony sposób wspierających realizację e-usług publicznych,

c) zapewnienie w ramach europejskiego portfela tożsamości cyfrowej możliwości składania kwalifikowanego podpisu elektronicznego (w tym nieodpłatnie co najmniej do celów innych niż profesjonalne).

[box] Co z tego wynika: Obywatel będzie mógł używać wszystkich trzech rodzajów podpisów elektronicznych w usługach publicznych (kwalifikowany podpis elektroniczny, podpis osobisty, podpis zaufany) i w wygodny sposób zweryfikować ich ważność.

Cel 2.4.3: Środki identyfikacji elektronicznej są bezpieczne i wygodne w użyciu

Co umożliwi realizację celu:

a) budowa oraz wdrożenie modelu szerokiego wykorzystywania warstwy elektronicznej dowodu osobistego,

b) dołączenie do węzła krajowego identyfikacji elektronicznej środka identyfikacji elektronicznej zapewniającego wysoki poziom bezpieczeństwa, jakim będzie europejski portfel tożsamości cyfrowej (niezależnie od możliwości bezpośredniej komunikacji strony ufającej z portfelem),

c) dodanie do węzła krajowego identyfikacji elektronicznej możliwości zbierania na żądanie użytkownika historii użycia jego środków identyfikacji elektronicznej,

d) dodanie weryfikacji, czy urządzenie, z którego następuje logowanie do systemów teleinformatycznych przyłączonych do węzła krajowego identyfikacji elektronicznej, jest na liście urządzeń zaufanych użytkownika,

e) realizacja działań edukacyjnych, które wspomogą użytkowników w bezpiecznym korzystaniu ze środków identyfikacji elektronicznej.

[box] Co z tego wynika: Skorzystasz z bezpiecznych środków identyfikacji elektronicznej – zabezpieczonych przed kradzieżą tożsamości, naruszeniem ochrony danych osobowych, cyberatakami i innymi niebezpiecznymi sytuacjami w internecie, a także umożliwimy sprawdzenie historii ich użycia.

Cel 2.4.4: Obywatele i przedsiębiorcy swobodnie i bezpiecznie korzystają z transgranicznych publicznych i prywatnych usług

Co umożliwi realizację celu:

a) utworzenie rejestru podmiotów, które będą chciały świadczyć swoje usługi w oparciu o europejski portfel tożsamości cyfrowej, zapewniającego tym podmiotom wygodną rejestrację i możliwość modyfikacji danych bez zbędnych barier biurokratycznych, ale z jednoczesnym zapewnieniem jednoznacznego rozpoznawania tych podmiotów,

b) stworzenie i udostępnienie mechanizmu weryfikacji niektórych danych użytkowników w rejestrach publicznych, aby można było wydawać elektroniczne poświadczenia atrybutów równoważne prawnie z zaświadczeniami tradycyjnymi i uznawane również za granicą,

c) wprowadzenie procedur jednoznacznego transgranicznego dopasowywania tożsamości, w którym dane identyfikujące osobę ze środka identyfikacji elektronicznej wydanego za granicą umożliwiają uwierzytelnienie w krajowych usługach publicznych,

d) modyfikacja krajowych systemów teleinformatycznych, w tym wspierających realizację e-usług publicznych, aby uznawały środki identyfikacji elektronicznej, w tym europejskie portfele tożsamości cyfrowej wydawane przez inne państwa członkowskie, oraz ułatwiały korzystanie z publicznych e-usług użytkownikom z innych państw członkowskich, w szczególności osobom nieposiadającym nadanego numeru PESEL.

[box] Co z tego wynika: Będziesz bezpiecznie i wygodnie potwierdzać swoje dane oraz swobodnie korzystać z wielu usług w krajach Unii Europejskiej.

2.5 Chmura obliczeniowa

Diagnoza – jak jest?

Koszt realizacji procesów i ich obsługi w instytucjach publicznych jest wysoki, a wdrażanie nowych e-usług publicznych i systemów teleinformatycznych zbyt powolne. W konsekwencji rozwój e-usług o wyższym poziomie dojrzałości i złożoności jest hamowany. Jednocześnie jest konieczne zwrócenie uwagi na ryzyko przerwania ciągłości działania e-usług publicznych i systemów teleinformatycznych oraz utraty danych kluczowych systemów administracji publicznej.

Uznajemy, że efektywne i bezpieczne gromadzenie oraz przetwarzanie danych dotyczących obywateli, przedsiębiorców i działania państwa, ze względu przede wszystkim na skalę (wolumen tych danych), jest na dłuższą metę niemożliwe bez wykorzystania chmury obliczeniowej.

Biorąc pod uwagę uwarunkowania rynku chmurowego oraz kwestie bezpieczeństwa, szczególnie istotne są już realizowane inicjatywy, takie jak centra superkomputerowe HPC czy sieć PIONIER.

Działania dotyczące administracji publicznej w tym obszarze mają odpowiednie zastosowanie do sądów powszechnych i wojskowych oraz Prokuratury, uwzględniając jej pozycję prawno-ustrojową i realizowane zadania.

Cel 2.5.1: Infrastruktura chmurowa administracji publicznej i usługi oparte na danych są rozwinięte

Co umożliwi realizację celu:

a) wytworzenie w ramach Rządowej Chmury Obliczeniowej innowacyjnych usług chmurowych przeznaczonych dla administracji publicznej. Będą to usługi dostarczane w modelach infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) czy oprogramowanie jako usługa (SaaS), w zależności od charakterystyki wspierające działanie systemów informatycznych, możliwe do wykorzystania jako bloki budowlane do tworzenia nowoczesnych systemów informatycznych, wspomagających projektowanie i wdrażanie oprogramowania w oparciu o usługi chmury obliczeniowej lub niezależnie do realizacji usług publicznych i procesów obsługiwanych w jednostkach,

b) stworzenie warunków dla powstania, rozwoju i utrzymania Chmury Samorządowej, oferującej możliwości podobne do tych w ramach Rządowej Chmury Obliczeniowej. Chmura Samorządowa umożliwi korzystanie jednostkom samorządu terytorialnego z nowoczesnych usług chmurowych w sposób dostosowany do ich potrzeb i umożliwi osiągnięcie efektu synergii. Wprowadzane będą rozwiązania legislacyjne wspierające samorządy,

c) zapewnienie, że wdrażane usługi będą bazować na najlepszych, sprzyjających bezpieczeństwu i suwerenności, krajowych, unijnych i międzynarodowych standardach, zgodne z polskimi i unijnymi regulacjami prawnymi oraz zgodnie z pryncypiami Architektury Informacyjnej Państwa,

d) zwiększenie dostępności skalowalnych usług infrastrukturalnych dostarczanych w modelu chmury obliczeniowej, dostosowanych do zmieniających się potrzeb administracji,

e) uproszczenie stosu technologicznego, komponentów architektury zorientowanych na usługi oraz udostępnienie standardów architektonicznych i predefiniowanych modułów oprogramowania, pozwalające na uproszczenie i przyspieszenie procesu wdrożenia nowych e-usług publicznych i systemów IT,

f) stworzenie ambasad danych – zlokalizowanych poza granicami kraju jednostek umożliwiających składowanie kluczowych danych i informacji z rejestrów publicznych i teleinformatycznych systemów państwowych oraz zapewnienie ciągłości działania tych rejestrów i systemów w przypadku wystąpienia sytuacji kryzysowych na terytorium RP (przy zapewnieniu ochrony krajowymi rozwiązaniami kryptograficznymi oraz zachowaniu pełnej jurysdykcji i kontroli RP),

g) podejmowanie działań na rzecz zwiększenia bezpieczeństwa danych przez wykorzystanie informacji przetwarzanych w ramach wspólnych przestrzeni danych oraz na rzecz wykorzystania potencjału współpracy w ramach inicjatyw europejskich typu Gaia-X,

h) przyjęcie rozwiązań legislacyjnych kształtujących warunki korzystnego rozwoju chmury obliczeniowej w Polsce oraz wzmacniających bezpieczeństwo i pewność prawną w związku z jej wykorzystywaniem.

[box] Co z tego wynika: Zabezpieczymy działanie kluczowych systemów teleinformatycznych i rejestrów publicznych przed zakłóceniami, a dane w nich gromadzone przed utratą.

Cel 2.5.2: Infrastruktura przetwarzania danych jest nowoczesna i rozbudowana

Co umożliwi realizację celu:

a) budowa i rozwój Krajowego Centrum Przetwarzania Danych, obejmującego budowę trzech nowoczesnych, skalowalnych i wysoce wydajnych centrów przetwarzania, które zapewnią ciągłość działania systemów i bezpieczeństwo zasobów administracji publicznej. Połączone światłowodami centra będą wykorzystywały zieloną energię,

b) zapewnienie ciągłości świadczenia e-usług publicznych i funkcjonowania systemów teleinformatycznych przez zabezpieczenie danych systemów administracji publicznej przetwarzających dane o charakterze referencyjnym przed utratą, określenie gwarantowanego czasu odtworzenia danych w przypadku poważnej awarii oraz udostępnienie ustandaryzowanych usług wspomagających plany zachowania ciągłości działania, tworzenia archiwów i kopii bezpieczeństwa, w tym do długotrwałego składowania danych, odtworzenia danych oraz wspierających przywrócenie działania standardowych komponentów systemów teleinformatycznych,

c) rozbudowa państwowej infrastruktury na rzecz świadczenia e-usług publicznych umożliwiającej efektywne przetwarzanie danych, w tym optymalizację sieci ośrodków obliczeniowych zabezpieczających ciągłość świadczenia e-usług oraz przepływu danych na potrzeby systemów teleinformatycznych wspierających ich realizację m.in. dla sektora ochrony zdrowia, finansów, sądownictwa oraz statystyki publicznej,

d) rozwijanie współpracy sektora publicznego z dostawcami usług centrów przetwarzania danych zlokalizowanych na terenie kraju.

Cel 2.5.3: Podmioty publiczne mają zapewnione wsparcie w nabywaniu, wdrażaniu i wykorzystywaniu systemów i rozwiązań informatycznych w oparciu o usługi chmurowe

Co umożliwi realizację celu:

a) prowadzenie regularnych badań popytu na usługi rządowej i publicznej chmury obliczeniowej w administracji publicznej,

b) koordynacja i realizacja przez wyznaczony podmiot centralnych zamówień na usługi w zakresie chmury publicznej w przypadku usług najczęściej wykorzystywanych przez administrację publiczną, w tym zawieranie umów ramowych poszerzających katalog usług chmurowych dostępnych dla administracji publicznej po przeprowadzaniu uproszczonych postępowań wykonawczych,

c) wspieranie bezpiecznego pozyskiwania usług chmurowych w ramach postępowań zakupowych dzięki rozwijanemu i rozbudowywanemu systemowi Zapewniania Usług Chmurowych (ZUCH). System zapewni obsługę pełnego procesu zakupowego PZP, w tym postępowań wykonawczych oraz umożliwi podpisywanie umów i porozumień bezpośrednio w systemie ZUCH,

d) wspieranie konkurencyjności w pozyskiwaniu i wyszukiwaniu usług chmurowych przez bezpośrednią integrację systemu ZUCH z portalami zarządzania usługami chmurowymi dla chmur publicznych i prywatnych wspierających procesy porównywania, powoływania, raportowania i rozliczania usług, co pozwoli na zapewnienie niezależności od konkretnych dostawców usług,

e) udostępnienie w systemie ZUCH funkcjonalności Biznesowej Platformy Zarządzania Usługami Chmurowymi od wielu dostawców usług chmurowych do prostego zarządzania usługami od różnych dostawców usług chmurowych,

f) udostępnienie w systemie ZUCH, dla nowotworzonych innowacyjnych usług chmurowych na rządowej chmurze obliczeniowej, funkcjonalności do konfiguracji, zarządzania i rozliczania wykorzystania tych usług chmurowych,

g) utworzenie Akademii Chmury, gdzie jednostki administracji będą mogły pozyskać wiedzę o bezpiecznych rozwiązaniach i dobrych praktykach w tworzeniu i utrzymaniu rozwiązań na infrastrukturze chmury obliczeniowej,

h) wspieranie jednostek administracji publicznej w unikaniu uzależnienia od rozwiązań dostarczanych przez dostawców zewnętrznych (tzw. vendor locking) przez przygotowanie wytycznych dotyczących odpowiedniego przygotowania postępowania o zamówienia publiczne pod tym kątem.

[box] Co z tego wynika: Wszystkie usługi chmurowe dla administracji publicznej będą zamawiane centralnie, co zwiększy bezpieczeństwo i przejrzystość tego procesu, a także zmniejszy koszty dla administracji.

2.6 Otwarte dane i wymiana danych

Diagnoza – jak jest?

Dane mają wysokie znaczenie w gospodarce i społeczeństwie. Generowane przez komputery, smartfony i urządzenia codziennego użytku opatrzone licznymi czujnikami napędzają rozwój gospodarczy, konkurencyjność, innowacyjność i postęp społeczny. Według Komisji Europejskiej bezpośrednia wartość ekonomiczna informacji sektora publicznego została obliczona w ocenie skutków na 52 mld EUR w 2018 r., a szacuje się, że do 2030 r. wzrośnie do 149 mld EUR[74]. Wnioski z systemu monitorowania Programu otwierania danych na lata 2021-2027[5] wskazują m.in. na konieczność zwiększenia ilości danych w portalu dane.gov.pl oraz obiektów w kronika.gov.pl, dbanie o jakość danych oraz zwiększenie zakresu danych, podjęcie cyklicznego i długotrwałego działania na rzecz podniesienia poziomu wiedzy i umiejętności kadry administracyjnej w zakresie otwierania danych i zarządzania nimi, wdrożenie działań z zakresu promowania polityki otwartego dostępu do danych oraz działań informujących o możliwości udostępniania danych w portalu dane.gov.pl i płynących z tego korzyściach.

Ponadto, mając na względzie dynamiczny rozwój sztucznej inteligencji, która bazuje na dobrych jakościowo danych, są niezbędne działania ulepszające jakość zasobów publikowanych w portalu dane.gov.pl również na potrzeby uczenia maszynowego[75].

Ewaluacja ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[76] wskazała obszary wymagające podjęcia zintensyfikowanych działań pozalegislacyjnych. Należą do nich: potrzeba wzmocnienia sieci pełnomocników do spraw otwartości danych, dalszy rozwój portalu dane.gov.pl, podjęcia działań informacyjnych, edukacyjnych oraz promocyjnych nakierowanych na poszerzanie wiedzy na temat procesu otwierania i ponownego wykorzystywania danych publicznych.

[74] Open data maturity report 2023, https://data.europa.eu/en/publications/open-data-maturity/2023, za https://digital-strategy.ec.europa.eu/en/library/impact-assessment-review-directive-200398ec-reuse-public-sector-information.
[75] Pojęcie wyjaśnione w motywie 12 preambuły rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. Urz. UE L 2024/1689 z 12.07.2024).
[76] Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

Na poziomie UE, Komisja Europejska podejmuje działania w celu zwiększania wymiany i dzielenia się danymi pomiędzy różnymi aktorami, tj. konsumentami, przedsiębiorstwami i podmiotami sektora publicznego, w tym na rzecz rozwijania zasobu informacyjnego statystyki publicznej. Następstwem przyjmowania unijnych aktów prawnych jest konieczność zapewniania przez Polskę, jako państwo członkowskie, odpowiedniego stosowania lub wdrażania przyjmowanych przez UE instrumentów prawnych dotyczących danych. Stały monitoring przepisów krajowych i unijnych jest kluczowy dla dostosowania się do zmieniających się potrzeb użytkowników danych.

Identyfikujemy potrzebę stymulowania powstającego w Polsce rynku danych, który ma podlegać nowoprzyjętym europejskim ramom regulacyjnym (dotyczy to w szczególności sektora pośredników danych i organizacji altruizmu danych). Podejmowane przez nas działania będą miały na celu wsparcie wymiany danych między uczestnikami niewykształconego jeszcze w pełni rynku, który musi się szybko dostosować do nakładanych na niego regulacji. Ważne jest w szczególności włączenie polskich podmiotów z sektora publicznego oraz spoza niego w powstające jednolite europejskie przestrzenie danych. Równolegle należy tworzyć warunki wspierające podmioty działające na rynku danych w tworzeniu przestrzeni danych w oparciu o możliwości jakie niosą wdrażane przez nas nowe regulacje unijne.

Cel 2.6.1: Administracja publiczna świadomie działa na rzecz otwartości danych

Co umożliwi realizację celu:

a) uzależnienie realizacji i finansowania przedsięwzięć informatycznych od pozytywnej oceny Komitetu do spraw Cyfryzacji m.in. w zakresie zgodności z zasadami tworzenia danych,

b) upowszechnianie zasad tworzenia danych w fazie projektowania i otwartości domyślnej w procesach i projektach, w tym informatycznych realizowanych przez administrację publiczną, oraz uwzględnienie w nich udostępniania danych poprzez API,

c) poszerzenie sieci pełnomocników do spraw otwartości danych na wielu poziomach instytucjonalnych,

d) realizacja systematycznych szkoleń dla administracji w zakresie zarządzania danymi, analityki danych, wizualizacji oraz wykorzystywania danych w procesach kształtowania polityk publicznych.

[box] Co z tego wynika: Otwieranie danych w administracji będzie powszechniejsze i brane pod uwagę przy finansowaniu projektów.

Cel 2.6.2: Otoczenie prawne w obszarze zarządzania danymi sprzyja rozwojowi ekosystemu wymiany danych

Co umożliwi realizację celu:

a) ustanowienie przyjaznego środowiska legislacyjnego dla dzielenia się danymi z pobudek altruistycznych oraz wymiany danych w relacjach B2B[77] oraz B2G[78] (w tym przyjęcie przepisów krajowych służących stosowaniu Aktu w sprawie zarządzania danymi[79] i Aktu w sprawie danych[80]),

b) uczestnictwo w tworzeniu kolejnych aktów prawnych urzeczywistniających jednolity rynek danych w UE oraz w rewizji unijnych aktów prawnych zgodnie z potrzebami i kierunkami rozwoju krajowego rynku danych,

c) optymalizacja przepisów ustawy o otwartych danych w kierunku ułatwienia i poszerzenia zakresu ponownego wykorzystania danych publicznych,

d) zapewnienie ram prawnych i technicznych dla tworzenia wspólnych przestrzeni danych w obszarze usług publicznych, w tym w szczególności w polityce społecznej, ochronie zdrowia, edukacji i rynku pracy, umożliwiających bezpieczną, zgodną z przepisami ochrony danych osobowych wymianę informacji pomiędzy systemami resortowymi na potrzeby kompleksowej obsługi obywateli.

[box] Co z tego wynika: Wymiana danych między zainteresowanymi podmiotami i sektorami, zarówno prywatnymi jak i publicznym, będzie łatwiejsza i pewniejsza.

[77] Business-to-Business (ang.) – transakcje między co najmniej dwoma podmiotami gospodarczymi.
[78] Business-to-Government (ang.) – transakcje między podmiotami gospodarczymi a instytucjami rządowymi.
[79] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz. Urz. UE L 152 z 03.06.2022, str. 1, Dz. Urz. UE L 132 z 17.05.2023, str. 89 oraz Dz. Urz. UE L 2023/90204 z 21.12.2023).
[80] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz. Urz. UE L 2023/2854 z 22.12.2023 oraz Dz. Urz. UE L 2024/90790 z 09.12.2024).

Cel 2.6.3: Dostęp do danych o wysokiej jakości do ponownego wykorzystywania i uczenia maszynowego jest powszechny

Co umożliwi realizację celu:

a) badania w zakresie określenia poziomu podaży i popytu w odniesieniu do danych,

b) współpraca z posiadaczami danych w zakresie zwiększenia wolumenu danych[81], w tym danych połączonych oraz dynamicznych, w portalu dane.gov.pl, w szczególności dostępnych za pośrednictwem API przykładowo w obszarach dotyczących mieszkalnictwa, zanieczyszczenia środowiska, sektora energetycznego,

c) stały rozwój zaufanego portalu dane.gov.pl mający na celu zwiększenie jego użyteczności m.in. przez stworzenie mechanizmów wpływających na poprawę jakości danych i zwiększenie możliwości ich efektywnego wykorzystania oraz ulepszenie zarządzania danymi,

d) identyfikacja danych o wysokiej wartości i budowanie, w partnerstwach publicznych, API, które będą je udostępniać.

[box] Co z tego wynika? Udostępnimy w portalu dane.gov.pl ponad 100 tys. danych dostępnych dla każdego, bezpłatnie do dowolnego użytku.

[81] Dane w kontekście portalu dane.gov.pl rozumiane są jako każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu zobowiązanego zgodnie z ustawą o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego lub będąca w posiadaniu innego podmiotu niż podmiot zobowiązany i przez niego wytworzoną. Zbiór danych rozumiany jest jako zestaw, gromadzący dane z konkretnej tematyki.

Cel 2.6.4: Polski rynek wymiany danych jest dojrzały

Co umożliwi realizację celu:

a) podnoszenie świadomości społecznej w zakresie udostępniania danych przez działania informacyjne i edukacyjne dotyczące procesu otwierania danych i możliwości ich ponownego wykorzystywania,

b) rekomendowanie systemowego finansowania projektów wspierających rozwój usług pośrednictwa danych i altruizmu danych w ramach nowej perspektywy finansowej UE,

c) stymulowanie wymiany danych z interesariuszami spoza administracji oraz pomiędzy nimi,

d) aktywny udział w tworzeniu warunków dla rozwoju europejskich wspólnych przestrzeni danych,

e) wspieranie instytucji publicznych we wdrażaniu nowych modeli dzielenia się danymi m.in. przez utworzenie krajowego punktu wsparcia rozwoju przestrzeni danych.

3. Ludzie

3.1 Bezpieczna przestrzeń cyfrowa

Diagnoza – jak jest?

Wśród głównych czynników mających wpływ na podejście społeczeństwa do e-państwa można wyróżnić: użyteczność narzędzi, aspekty społeczne (zachowania innych), potencjalne ryzyka oraz dostępny już obywatelowi sprzęt i umiejętności. Szczególnie jednak istotnym czynnikiem, wpływającym m.in. na wykorzystanie e-usług publicznych, jest zaufanie.

Z tego względu, państwo ma obowiązek dążenia do budowy bezpieczeństwa szeroko pojętej sfery cyfrowej – dbałości o bezpieczeństwo użytkowników[82], respektowania zasad demokratycznego państwa prawa i praw obywatelskich, a także ochrony przestrzeni informacyjnej w sieci.

Kluczową kwestią jest ochrona bezpieczeństwa obywateli i ich danych oraz konkurencji rynkowej, a także budowanie suwerenności technologicznej. Konieczne jest więc podążanie za regulacjami oraz standardami cyfrowymi chroniącymi prawa obywatelskie, powstającymi w UE. Szczególnie ważna jest implementacja na poziomie krajowym unijnej deklaracji praw i zasad cyfrowych z cyfrowej dekady z 2022 r.[83] Celem deklaracji jest wspieranie transformacji cyfrowej w UE, ze szczególnym ukierunkowaniem na człowieka, solidarność i włączenie społeczne, swobodę wyboru oraz bezpieczeństwo i ochronę. Przyjęcie założenia, że ochrona obywateli stanowi priorytet, musi przekładać się m.in. na zapewnianie odpowiednich zasobów instytucjonalnych dla wdrażania i stosowania krajowych i unijnych aktów legislacyjnych w tym obszarze.

Prawa cyfrowe realizują się zarówno w relacjach jednostki z instytucjami władzy, jak i użytkowników z dostawcami usług cyfrowych. W kontekście tych ostatnich zagrożeniem są kwestie nieuzasadnionej moderacji treści przez platformy, niejasności w regulaminach i standardach cyfrowych społeczności, tzw. zwodniczych interfejsów, braku transparentności algorytmów i rozliczalności za działania platform oraz nieprzestrzeganie praw konsumentów. Problemy te wiążą się z modelem biznesowym opartym na walce o zaangażowanie użytkowników, stwarzającym ryzyka dla prywatności i wykorzystania danych osobowych.

[82] Na bezpieczeństwo użytkowników istotny wpływ ma także skuteczne zwalczanie cyberprzestępczości, które zostało szczegółowe omówione w części 1.3 niniejszej Strategii.
[83] Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie (2023/C 23/01) (Dz. Urz. UE C 23 z 23.01.2023, str. 1).

Brak reakcji na te zjawiska skutkuje długotrwałą i rosnącą społeczną polaryzacją, co podważa zarówno ład demokratyczny, jak i ład informacyjny państwa.

Na prawa podstawowe w sferze cyfrowej należy patrzeć również z perspektywy jej wpływu na pracowników.

Istnieje konieczność uwzględniania możliwości i ryzyk związanych z wykorzystaniem narzędzi cyfrowych, dążeniem do zwiększenia wydajności pracy przy jednoczesnej optymalizacji kosztów oraz pracy zdalnej. Należy zauważyć, że wykorzystanie technologii cyfrowych ma również negatywny wpływ na pracowników - przejawiający się naruszaniem równowagi między życiem prywatnym a zawodowym, co prowadzi do spadku produktywności oraz wypalenia zawodowego.

Nowe trendy związane z automatyzacją i digitalizacją procesów w firmach dotyczą zarówno pracowników fizycznych, jak i umysłowych. Narzędzia cyfrowe pozwalają na szeroko zakrojoną kontrolę pracowników, co może wiązać się z naruszaniem ich prywatności i dobrostanu. Wzrost popularności pracy zdalnej umożliwił elastyczną organizację czasu i przyniósł korzyści wielu pracownikom i pracodawcom. Równocześnie jednak generuje ryzyko związane z oczekiwaniem ciągłej dostępności od pracownika oraz utrudnia rozgraniczanie życia zawodowego i osobistego. Obserwujemy także dalszy intensywny rozwój niekonwencjonalnych modeli biznesowych, na czele których znalazła się gospodarka współdzielenia. Z jednej strony otworzyła ona przed konsumentami, przedsiębiorcami i pracownikami nowe możliwości, z drugiej jednak doprowadziła do destabilizacji warunków pracy i pozbawienia osób pracujących za pośrednictwem aplikacji ich podstawowych praw. Przerzucenie odpowiedzialności i kosztów działalności na pracowników platform - których liczba w UE ma sięgnąć 43 mln[84] - prowadzi do wzrostu niepewności zatrudnienia i upowszechniania się zjawiska prekariatu.

Wreszcie, zapewnienie kompleksowego bezpieczeństwa sfery cyfrowej wymaga skutecznej walki z dezinformacją oraz obcą ingerencją i manipulacją w środowisku informacyjnym. Dezinformacja oznacza informacje weryfikowalnie nieprawdziwe, wprowadzające w błąd lub celowo dobrane i zestawione w sposób manipulacyjny, tworzone, przedstawiane lub rozpowszechniane - niezależnie od użytego kanału lub nośnika - w celu osiągnięcia korzyści gospodarczych, politycznych, militarnych lub społecznych, realizacji celów obcego państwa lub podmiotu pozapaństwowego, bądź w celu wywołania błędu w postrzeganiu rzeczywistości przez odbiorcę, które mogą wyrządzić szkodę interesom publicznym, bezpieczeństwu państwa, infrastrukturze krytycznej, integralności procesów demokratycznych lub prawom i wolnościom jednostki. Przez obcą ingerencję i manipulację w środowisku informacyjnym rozumie się wzorzec zachowania, który przeważnie nie jest nielegalny, ale zagraża lub może potencjalnie negatywnie wpłynąć na wartości, procedury i procesy polityczne. Takie działania mają charakter manipulacyjny, są prowadzone w sposób celowy i skoordynowany przez podmioty państwowe lub niepaństwowe, w tym przez ich pełnomocników, na ich własnym terytorium i poza nim.

Warto zauważyć, że do prowadzonych działań dezinformacyjnych są wykorzystywane różnego rodzaju tematy zmierzające do polaryzacji społecznej, osłabienia procesów demokratycznych czy wywołania niepokojów społecznych. W tym kontekście należy

[84] https://www.consilium.europa.eu/pl/policies/platform-work-eu/.

podkreślić dezinformację dotyczącą m.in. procesów wyborczych, klimatu i środowiska, praw mniejszości, migracji, wojen i konfliktów, technologii czy zdrowia.

Dezinformacja prowadzona przez podmioty krajowe służy przede wszystkim budowaniu kapitału politycznego lub finansowego, a jej oddziaływanie może być instrumentalizowane przez podmioty zewnętrzne. Dezinformacja prowadzona przez podmioty zagraniczne - obce państwa lub podmioty pozapaństwowe działające na ich zlecenie - zmierza do destabilizacji sytuacji społeczno-politycznej oraz pogłębienia polaryzacji społecznej.

Najaktywniejszymi adwersarzami państwa polskiego w przestrzeni informacyjnej są państwa prowadzące przeciwko Polsce działania hybrydowe, w tym Rosja i Białoruś. Te działania obejmują m.in. działania dezinformacyjne, operacje wpływu, cyberataki oraz działania wywiadowcze, dywersyjne i sabotażowe. Propagowane przez nie przekazy dezinformacyjne realizują zarówno cele wewnętrzne tych państw - w tym umacnianie legitymizacji władzy - jak i zewnętrzne, takie jak stymulowanie nastrojów antynatowskich, antyunijnych, antyamerykańskich i antyukraińskich.

Istotnymi dla skutecznej walki ze zjawiskiem dezinformacji są działania podejmowane w celu budowania rzetelnych i wiarygodnych mediów, w tym wspieranie niezależności redakcyjnej oraz przejrzystości finansowania podmiotów medialnych. Równie ważnym elementem jest zwiększanie roli edukacji medialnej i informacyjnej - rozumianej jako kształtowanie kompetencji krytycznego odbioru treści, weryfikacji źródeł oraz rozpoznawania technik manipulacji - prowadzonej na wszystkich poziomach systemu edukacji oraz w ramach programów skierowanych do osób dorosłych. Działania te, realizowane we współpracy organów administracji publicznej, instytucji edukacyjnych, organizacji społeczeństwa obywatelskiego i podmiotów medialnych, stanowią fundament odporności społecznej na dezinformację.

W Polsce zadania związane z tym obszarem prowadzone są przez szereg instytucji, w tym NASK-PIB, Ministerstwo Spraw Zagranicznych, Krajową Radę Radiofonii i Telewizji (edukacja medialna), Rządowe Centrum Bezpieczeństwa (analiza zagrożeń, w tym związanych z dezinformacją), odpowiednie służby (w tym SKW – Służba Kontrwywiadu Wojskowego i ABW – Agencja Bezpieczeństwa Wewnętrznego). Zgodnie z unijnym aktem o usługach cyfrowych[85] w działania – jako koordynator do spraw usług cyfrowych – będzie włączony też Prezes Urzędu Komunikacji Elektronicznej. Wielość instytucji działających w obszarze dezinformacji przekłada się na jedno z głównych wyzwań w tym obszarze – brak odpowiedniej koordynacji i komunikacji, a także niespójność w metodach działania i kryteriach oceny zagrożeń. Wśród innych wyzwań wskazać należy:

- rozwój nowych technologii (w tym AI) umożliwiających szybsze i tańsze tworzenie i rozpowszechnianie treści dezinformacyjnych, przy tym trudniejsze do wykrycia,

- nieefektywną współpracę z platformami społecznościowymi w procesie zarówno identyfikacji, weryfikacji i zdejmowania treści dezinformacyjnych oraz kont je rozpowszechniających (w tym botów),

- konieczność pogłębienia działań (krajowych i unijnych) zmierzających do analizowania kampanii dezinformacyjnych w sposób kompleksowy,

- niską świadomość społeczną oraz potrzebę rozwoju kompetencji w zakresie edukacji medialnej, myślenia krytycznego oraz bezpieczeństwa informacyjnego na wszystkich poziomach edukacji,

[85] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 27.10.2022, str. 1 oraz Dz. Urz. UE L 163 z 29.06.2023, str. 107).

- publikację w celach dezinformacyjnych fałszywych materiałów wytworzonych przy pomocy technologii deepfake pozwalającej na zmanipulowanie obrazu lub dźwięku,

- promowanie przez algorytmy rekomendacyjne treści silnie emocjonalnych, w tym dezinformacyjnych oraz ich wzmacnianie poprzez mechanizmy podpowiadania podobnego typu treści, co skutkuje zamknięciem użytkownika w tzw. bańce informacyjnej,

- rozproszenie i niewystarczające finansowanie organizacji pozarządowych zajmujących się przeciwdziałaniem dezinformacji,

- brak ustalonych na poziomie centralnym oraz samorządowym strategii reagowania na dezinformację lub komunikacji kryzysowej.

Cel 3.1.1: Otoczenie instytucjonalne i regulacyjne w sferze cyfrowej wspiera ochronę praw podstawowych

Co umożliwi realizację celu:

a) wspieranie silnego otoczenia instytucjonalnego wokół regulacji mających za zadanie zapewnić poszanowanie uznanych wartości i praw jednostek w sieci przez wyposażenie podmiotów odpowiedzialnych za egzekwowanie ich przepisów w środki techniczne, osobowe i finansowe,

b) promowanie tego, by projektowanie, opracowywanie, wdrażanie i wykorzystywanie rozwiązań technologicznych odbywało się z poszanowaniem praw podstawowych przez stosowanie zasady „etyki już na etapie projektowania" („ethics by design") oraz z zachowaniem otwartości na audyt społeczny,

c) przeprowadzanie oceny wpływu na prawa podstawowe obywateli (FRIA) w przypadku wykorzystywania systemów automatycznego podejmowania decyzji oraz systemów AI w administracji państwowej,

d) stworzenie formularza do oceny wymiaru etycznej AI stosowanej przez państwo,

e) wypracowanie krajowych rozwiązań w zakresie domniemania istnienia stosunku pracy w obszarze gospodarki współdzielenia oraz niezwłoczne wdrożenie do polskiego prawa dyrektywy o pracownikach platformowych[86],

f) bieżące badanie wpływu technologii cyfrowych, zwłaszcza AI, na rynek pracy, w tym dobrostan pracowników (fizyczny, psychiczny i społeczny),

g) zapewnianie skutecznego przestrzegania reguł prawa pracy i aktualności polityk publicznych w odniesieniu do dynamicznie zmieniającego się pod wpływem digitalizacji i wywołanej nią trendów rynku pracy. Mowa tutaj o ochronie pracowników przed ryzykiem bycia ciągle dostępnym (przyjęcie prawa do odłączenia się), nieprzejrzystym „scoringiem" i zbudowanymi na uprzedzeniach ocenami pracowników (wdrożenie regulacji związanych z wykorzystywaniem AI w obszarze pracy) i cyfrową inwigilacją (egzekwowanie przepisów dotyczących prywatności),

h) aktywność na forum krajowym i unijnym na rzecz wdrażania rozwiązań, w szczególności legislacyjnych, dla ochrony prawa do prywatności, ochrony danych osobowych i prawa do odłączenia się,

i) cyfryzacja obywatelskiej inicjatywy ustawodawczej i wsparcie rozwoju cyfrowych narzędzi partycypacji obywatelskiej. Wsparcie będzie realizowane przez wdrażanie partycypacyjnych platform i narzędzi cyfrowych w oparciu o najlepsze międzynarodowe standardy i zasady deliberacji online, finansowanie badań i edukacji w tym zakresie, udostępnianie praktycznych przewodników, wdrażanie e-konsultacji, narzędzi CivicTech, instytucjonalizację demokratycznych innowacji oraz prowadzenie spójnej polityki partycypacji i transparentności.

[86] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2831 z dnia 23 października 2024 r. w sprawie poprawy warunków pracy za pośrednictwem platform (Dz. Urz. UE L 2024/2831 z 11.11.2024).

Cel 3.1.2: Publiczna przestrzeń cyfrowa jest przyjazna użytkownikom i budzi zaufanie obywateli

Co umożliwi realizację celu:

a) praktyczna realizacja założeń Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie we wszelkich interakcjach państwa z obywatelami w sferze cyfrowej,

b) rozwój e-usług społecznych, które przez wykorzystanie centralnych rejestrów i algorytmów sztucznej inteligencji, będą świadczyć usługi proaktywne, przeciwdziałając tym samym wykluczeniu społecznemu,

c) budowa zaufania do e-państwa przez większe włączenie obywateli w proces tworzenia cyfrowego prawa (w tym z wykorzystaniem narzędzi cyfrowych) i cyfrowych usług publicznych, zwiększenie dostępu do wiarygodnej informacji publicznej, wykorzystywanie przez instytucje publiczne agregatorów treści, a także zlikwidowanie luki w cyfryzacji dokumentów istotnych dla opinii publicznej (publikowanie w sposób dostępny cyfrowo, w formacie umożliwiającym odczyt maszynowy takich dokumentów jak np. oświadczenia majątkowe parlamentarzystów) i dążenie do większej przejrzystości procesu przetwarzania spraw i danych obywatela,

d) zaprojektowanie rozwiązań mających umożliwić obywatelom dostęp do informacji o tym, jaki organ i w jakiej sprawie miał dostęp do ich danych – wykorzystywanie mechanizmów „privacy by design” (prywatności w fazie projektowania) i „security by design” (bezpieczeństwo w fazie projektowania) z uwzględnieniem reguł RODO[87] oraz „innovation by design” (projektowanie skoncentrowane na użytkowniku), wprowadzenia zasady automatycznego wykrywania operacji na danych umożliwiającej obywatelom kontrolę ich danych i zgłaszanie naruszeń oraz wykorzystywania analizy historii zapytań o dane w celu wychwytywania zagrożeń. Zapewnienie stosowania takich rozwiązań powinno być uwzględnione na etapie procesu legislacyjnego,

e) stworzenie kodeksu dobrych praktyk w zakresie wykorzystania danych osobowych w systemach teleinformatycznych,

f) zwiększenie świadomości użytkowników o przysługujących im środkach ochrony danych osobowych (zarówno technicznych, organizacyjnych i prawnych).

[box] Co z tego wynika: Bez problemu sprawdzisz, jaki organ i w jakiej sprawie miał dostęp do Twoich danych.

[87] 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35).

Cel 3.1.3: Działania jednostek przeciwdziałających dezinformacji są skoordynowane

Co umożliwi realizację celu:

a) ustalenie organu odpowiedzialnego za nadzorowanie oraz koordynację działań różnych podmiotów zajmujących się przeciwdziałaniem dezinformacji,

b) zapewnienie klarownej struktury komunikacyjnej i przepływu informacji między wszystkimi zaangażowanymi jednostkami przez regularne spotkania i platformy wymiany danych,

c) opracowanie jednolitych lub zbliżonych procedur i standardów operacyjnych stosowanych przez wszystkie jednostki zajmujące się przeciwdziałaniem dezinformacji,

d) zapewnienie zaawansowanych narzędzi technologicznych do zwalczania dezinformacji oraz szkoleń dla pracowników jednostek,

e) aktywna współpraca i wymiana informacji na poziomie międzynarodowym (zwłaszcza europejskim) na rzecz wspólnego zwalczania dezinformacji.

Cel 3.1.4: Poziom świadomości społecznej na temat dezinformacji jest stale pogłębiany

Co umożliwi realizację celu:

a) realizacja kampanii informacyjnych i społecznych na temat dezinformacji i odpowiedzialnego korzystania z mediów tradycyjnych i społecznościowych,

b) prowadzenie działań edukacyjnych do wybranych grup społecznych dotyczących dezinformacji i narzędzi wykorzystywanych do jej tworzenia (m.in. generatywna AI, deepfake, algorytmy podpowiadające treści silnie emocjonalne, bańki informacyjne),

c) prowadzenie specjalistycznych kampanii informacyjnych w związku z kluczowymi wydarzeniami, jak np. w okresie wyborczym,

d) stworzenie interaktywnych platform e-learningowych i multimedialnych materiałów dydaktycznych,

e) organizowanie dyskusji, debat i warsztatów na temat etycznych aspektów działalności medialnej, takich jak: prywatność, ochrona danych, prawa autorskie i odpowiedzialność za publikowane treści,

f) włączanie lokalnych społeczności i organizacji społecznych w proces budowania świadomości medialnej oraz planowania działań komunikacyjnych,

g) zapewnienie środków finansowych dla podmiotów społeczeństwa obywatelskiego prowadzących działania w zakresie zwalczania dezinformacji; poszerzenie narzędzi wspierających tworzenie rzetelnych treści medialnych.

Cel 3.1.5: Platformy społecznościowe sprawnie usuwają treści nielegalne

Co umożliwi realizację celu:

a) stały monitoring treści znajdujących się na platformach społecznościowych, uwzględniający proaktywne badanie czy i w jaki sposób platformy wypełniają obowiązki wynikające z aktu o usługach cyfrowych,

b) działalność zaufanych podmiotów sygnalizujących (ang. trusted flaggers) odpowiedzialnych za wykrywanie potencjalnie nielegalnych treści i ostrzeganie platform internetowych, a także ustanowienie odpowiednich ścieżek wymiany informacji dla zaufanych podmiotów sygnalizujących (zgodnie z aktem o usługach cyfrowych),

c) ustanowienie jasnych i transparentnych kryteriów prowadzących do uzyskania statusu zaufanego podmiotu sygnalizującego. Zaufane podmioty sygnalizujące powinny posiadać szczególną wiedzę fachową i kompetencje w zakresie wykrywania, identyfikowania i zgłaszania nielegalnych treści oraz być niezależne od platform internetowych,

d) wdrożenie efektywnych mechanizmów penalizujących platformy mediów społecznościowych oraz usługodawców IT za brak działań ukierunkowanych na zwalczanie dezinformacji oraz innych treści szkodliwych i nielegalnych; oraz aktywne działania na szczeblu europejskim na rzecz tworzenia otoczenia regulacyjnego w tym zakresie,

e) utworzenie ram współpracy z sektorem prywatnym, szczególnie z platformami mediów społecznościowych.

3.2 Cyfrowe zdrowie

Diagnoza – jak jest?

Kompleksowa diagnoza relacji między sferą technologii a sferą zdrowia wymaga dostrzeżenia dwóch, często sprzecznych wymiarów tej relacji.

Pierwszy aspekt relacji między technologiami a zdrowiem ma pozytywny wydźwięk i wiąże się z

ogromnymi możliwościami, jakie cyfryzacja zdrowia daje w odniesieniu do zwiększania skuteczności diagnostyki, leczenia i profilaktyki.

Diagnoza sytuacji wokół cyfryzacji sektora zdrowia w Polsce wskazuje na zaawansowaną, ale wciąż rozwijającą się infrastrukturę e-zdrowia. Wg unijnego raportu o stanie cyfrowego zdrowia ostatniej dekady, Polska zajmuje, odpowiednio, 6. oraz 5. miejsce pod względem dostępu do Elektronicznej Dokumentacji Medycznej (EDM) oraz dostępu do technologii wśród 27 krajów UE[88], zajmując miejsce poniżej średniej dla UE jedynie w zakresie kategorii dostępnych dla pacjenta danych.

Kluczowymi elementami polskiego cyfrowego zdrowia jest Platforma e-Zdrowie (P1) oraz różnorodne rejestry publiczne, systemy dziedzinowe i platformy regionalne. Platforma P1 stanowi centralny punkt cyfrowych usług zdrowotnych, oferując m.in. e-recepty, elektroniczne skierowania, a także dostęp do EDM. Rozwój tej platformy wpłynął na zwiększenie wykorzystania Internetowego Konta Pacjenta (IKP), z którego korzysta obecnie ponad 19 mln Polaków. Wskazać należy też na sukces wdrożenia systemu e-recept, który pozwolił na wystawienie 2,5 mld e-recept do kwietnia 2025 r.[89]. Wprowadzone w pierwszej kolejności e-usługi zdrowotne stanowią jednak przede wszystkim cyfrowe odzwierciedlenie tradycyjnych procesów i nie wykorzystują pełni potencjału digitalizacji.

Na poziomie lokalnym, wg badania stopnia informatyzacji Podmiotów Wykonujących Działalność Leczniczą (PWDL) prowadzonego przez Centrum e-Zdrowia, na koniec 2024 r. ponad 98% szpitali posiadało rozwiązania IT niezbędne do prowadzenia dokumentacji medycznej w wersji elektronicznej w podstawowym zakresie, 84% wdrożyło indeksowanie EDM w P1, a prawie połowa prowadzi wymianę EDM z innymi podmiotami[90]. Odsetek ten jest znacznie niższy dla podmiotów niebędących szpitalami.

[88] https://op.europa.eu/en/publication-detail/-/publication/78938111-461e-11ee-92e3-01aa75ed71a1/language-en.
[89] https://pacjent.gov.pl/aktualnosc/48-proc-polakow-uzywa-ikp.
[90] Dane Centrum e-Zdrowia.

Warunkiem rozwoju usług cyfrowych w sferze zdrowia jest zapewnienie bezpieczeństwa danych.

Pomimo działań podejmowanych przez Centrum e-Zdrowia oraz Ministerstwo Zdrowia, poziom cyberbezpieczeństwa na poziomie lokalnym nadal nie jest zadowalający. Wg danych ankietowych Centrum e-Zdrowia na kwiecień 2022 r., 81% podmiotów leczniczych nie ma planu zarządzania podatnościami, w 68% brak odmiejscowionych kopii bezpieczeństwa, a 86% kierowników jednostek nie odbyło szkoleń z zakresu cyberbezpieczeństwa[91].

Istotnym problemem dla rozwoju e-zdrowia jest również silosowość danych, która nie pozwala uzyskać pełnego obrazu zdrowia pacjenta, i brak demokratycznych zasad dostępu do danych na cele badawczo-rozwojowe (B+R). Niejasne zasady dostępu do zgromadzonych już danych, w tym wątpliwości dotyczące podstawy prawnej przetwarzania danych o stanie zdrowia w celach B+R – oraz niepewność co do adekwatności zebranych w centralnych rejestrach danych[92] wpływają na spowolnienie rozwoju medycyny. Odnotować należy również zagrożenia wynikające ze stosowania danych syntetycznych, które – w nadmiernym stopniu – może przekładać się na ryzyko błędnej ich interpretacji, istotne zwłaszcza w obszarze zdrowia.

Odsetek podmiotów leczniczych korzystających z nowych technologii, takich jak sztuczna inteligencja, jest rosnący i wynosi obecnie13% dla szpitali[93]. Rośnie również zainteresowanie i świadomość korzyści wynikających ze stosowania AI w medycynie.

Drugim z wymiarów jest

negatywny wpływ niektórych aspektów wykorzystania technologii cyfrowych na kondycję psychiczną obywateli.

Wiąże się on m.in. z przeciążeniem informacyjnym odbiorców, a także z uzależniającym mechanizmem działania platform społecznościowych i szkodliwym – sensacyjnym, rysującym nierealne standardy urody czy gloryfikującym przemoc – charakterem niektórych pojawiających się tam treści. Szczególnie wyraźnie rysującym się problemem, również wobec niedostatecznej skuteczności mechanizmów weryfikacji wieku, jest powszechny dostęp dzieci do treści szkodliwych, godzących w ich rozwój i propagujących niewłaściwe wzorce. Istotnym problemem jest też wykorzystywanie małoletnich w sieci. Państwo jest zobowiązane do tego, by na te wyzwania reagować – również w ramach współpracy międzynarodowej, której charakter wyzwań niejednokrotnie wymaga.

[91] Dane Centrum e-Zdrowia.
[92] https://www.mdpi.com/1660-4601/19/19/11964.
[93] Dane Centrum e-Zdrowia.

Cel 3.2.1: Państwo działa na rzecz minimalizacji negatywnego wpływu technologii cyfrowych na dobrostan psychiczny i fizyczny

Co umożliwi realizację celu:

a) uruchomienie programu finansowania badań:

- wpływu technologii cyfrowych na zdrowie psychiczne i rozwój psychospołeczny obywateli, zarówno dzieci i młodzieży, jak i dorosłych,

- rozwoju technologii cyfrowych wspierających odporność społeczną,

b) realizacja kampanii społecznych i informacyjnych na temat higieny cyfrowej i praw obywateli (zarówno dzieci, jak i dorosłych) w przestrzeni cyfrowej, w tym dotyczących zapewniania obszarów screen-free, oraz udostępnienie mechanizmów i narzędzi do filtrowania informacji oraz ich priorytetyzacji, profilaktyka uzależnień od treści oraz przeciwdziałanie zagrożeniom wynikającym np. cyberprzestępczości, cyberprzemocy lub negatywnych wzorców w mediach społecznościowych,

c) wdrażanie środków zapobiegających wykorzystywaniu seksualnemu małoletnich w internecie,

d) wprowadzenie standardów ochrony małoletnich w produktach i usługach cyfrowych, z uwzględnieniem standardów europejskich. Powinny one w szczególności:

- wspierać modyfikowanie systemów rekomendacyjnych platform w celu zmniejszenia ryzyka napotkania szkodliwych i uzależniających treści oraz umożliwienie dzieciom większej kontroli nad publikowanymi przez nich treściami,

- zakładać wykorzystanie narzędzi skutecznej weryfikacji wieku użytkownika, przy zachowaniu anonimowości i ochrony jego danych osobowych,

- określić bezpieczny wiek korzystania z produktów cyfrowych, zwłaszcza z platform społecznościowych, na podstawie aktualnego stanu wiedzy o wpływie technologii na dobrostan małoletnich,

- wykluczać rozwiązania prowadzące do utraty kontroli nad czasem ekranowym,

- wprowadzać rozwiązania chroniące wizerunek dzieci i młodzieży w internecie.

Cel 3.2.2: Elektroniczna Dokumentacja Medyczna jest powszechna, kompletna i prowadzona w sposób umożliwiający wymianę dokumentacji między podmiotami leczniczymi

Co umożliwi realizację celu:

a) dalszy rozwój systemów e-usług zdrowotnych w systemie P1,

b) upowszechnienie prowadzenia EDM wraz z indeksowaniem w systemie P1 oraz możliwością wymiany dokumentacji z innym podmiotem,

c) umożliwienie dostępu do poprzednio wytworzonej dokumentacji elektronicznej pacjentów dla osób wykonujących zawód medyczny, w procesie podejmowania decyzji klinicznych,

d) umożliwienie wzbogacania danych gromadzonych w systemie P1 o dane gromadzone przez urządzenia do noszenia i urządzenia wszczepialne,

e) uspójnienie sposobu prowadzenia dokumentacji medycznej szczególnie w zakresach, w których dane nie są zesłownikowane,

f) promowanie interoperacyjności pomiędzy systemami informatycznymi w ochronie zdrowia i jakości gromadzonych danych, w tym uspójnienie procesu migracji między systemami.

[box] Co z tego wynika: Idąc do lekarza nie musisz mieć przy sobie swojej papierowej historii leczenia – lekarz pobierze Twoją dokumentację medyczną z systemu centralnego.

Cel 3.2.3: Dysponujemy dużymi zasobami wiarygodnych danych o stanie zdrowia, a zasady dostępu do nich dla celów B+R są transparentne, demokratyczne i efektywne

Co umożliwi realizację celu:

a) wdrożenie działań operacyjnych w związku z wejściem w życie European Health Data Space (Europejskiej Przestrzeni Danych dotyczących Zdrowia)[94] oraz Data Governance Act (Aktu w sprawie zarządzania danymi),

b) promowanie idei dawstwa (altruizmu) danych medycznych wśród pacjentów,

c) uregulowanie zasad dostępu do danych jednostkowych i statystycznych na cele B+R, w tym wystandaryzowanie zasad dostępu do danych gromadzonych w rejestrach publicznych oraz dokumentacji medycznej przechowywanej przez PWDL,

d) ustalenie standardu anonimizacji i pseudonimizacji danych medycznych, spójnego ze standardami europejskimi.

[box] Co z tego wynika: Będziesz mieć szerszy dostęp do nowych terapii, wytycznych, rozwiązań cyfrowych, które są dostosowane do diagnozowania i leczenia takich pacjentów jak Ty. Będziesz decydować o tym, co się dzieje z Twoimi danymi medycznymi.

[94] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (Dz. Urz. UE L 2025/327 z 05.03.2025).

Cel 3.2.4: Sztuczna inteligencja oraz inne nowe technologie cyfrowe są wykorzystywane w sposób bezpieczny i skuteczny dla poprawy jakości opieki nad pacjentem

Co umożliwi realizację celu:

a) finansowanie stosowania nowych technologii cyfrowych w zdrowiu, w tym AI, rozwiązań telemedycznych, urządzeń medycznych do noszenia i aplikacji zdrowotnych, ze środków publicznych w ramach świadczeń gwarantowanych, przez m.in.:

   - uwzględnienie tych rozwiązań w opisie standardu istniejących świadczeń gwarantowanych,

   - wprowadzenie mechanizmu refundacji dla tych rozwiązań,

   - alokowanie niezbędnych środków na pokrycie kosztów finansowania tych rozwiązań,

b) wprowadzenie niezbędnych zmian w administracji publicznej, w tym wprowadzenie nowych przepisów, procedur i wzmocnienie kompetencji w zakresie finansowania i monitorowania rozwiązań cyfrowych, m.in. przez stworzenie standardu oceny koszto-efektywności technologii opartych o AI, jak również skuteczne mechanizmy kontroli nowych technologii medycznych na poziomie krajowym,

c) wprowadzenie przez Centrum e-Zdrowia nowych narzędzi, umożliwiających analizę danych medycznych gromadzonych w rejestrach centralnych w celu profilowania zdrowotnego, profilaktyki i monitorowania efektywności programów profilaktycznych, analityki predykcyjnej i podejmowania interwencji w oparciu o uzyskane wyniki (np. kontakt z pacjentem czy porada edukacyjna), przy uwzględnieniu najwyższych standardów prywatności i umożliwieniu pacjentowi zadecydowania, czy chce być objęty takim programem,

d) rozszerzenie modułu e-recept o dwustronną komunikację umożliwiającą wyświetlanie alertów umożliwiających optymalizację farmakoterapii,

e) prowadzenie uczciwej komunikacji i edukacji w zakresie możliwości i ograniczeń związanych ze stosowaniem AI w zdrowiu skierowanej zarówno do pacjentów, jak również do pracowników medycznych,

f) dostosowanie wytycznych ministerialnych dla kierunków medycznych do edukacji studentów w zakresie nowych technologii cyfrowych, w tym AI,

g) ułatwienie dostępu dla pacjenta do informacji dotyczącej organizacji opieki zdrowotnej i wiedzy medycznej przez wykorzystanie najskuteczniejszych i najbardziej adekwatnych narzędzi cyfrowych, w tym – tam, gdzie jest to uzasadnione - rozwiązań opartych na sztucznej inteligencji,

h) wykorzystywanie telemedycyny zgodnie ze standardami jakości jako systemowego uzupełnienia procesu opieki nad pacjentem, w tym w szczególności opieki nad osobami o utrudnionym dostępie do świadczeń,

i) promowanie wykorzystania nowych technologii cyfrowych do celów organizacyjno-administracyjnych, w tym lepszej koordynacji procesu opieki nad pacjentem w ochronie zdrowia oraz pod kątem cyberbezpieczeństwa podmiotów medycznych. Podnoszenie kompetencji cyfrowych personelu medycznego,

j) współpraca ze środowiskiem akademickim w zakresie badań nad zastosowaniem AI w ochronie zdrowia.

[box] Co z tego wynika: Otrzymasz leczenie z wykorzystaniem najnowocześniejszej, sprawdzonej technologii. Będziesz otrzymywać informacje o ryzyku zachorowania zanim nastąpi incydent zdrowotny, co umożliwi Ci podjęcie działań profilaktycznych.

Cel 3.2.5: W sposób kompleksowy i transparentny monitorujemy jakość interwencji zdrowotnych, w oparciu o dane ze świata rzeczywistego

Co umożliwi realizację celu:

a) umożliwienie bieżącego monitorowania ścieżek diagnostyczno-leczniczych pacjentów o określonym profilu, bazującego na realnych danych ze świata rzeczywistego,

b) wprowadzenie publicznie dostępnego systemu monitorowania jakości udzielanych świadczeń w PWDL,

c) zapewnienie dostępu do danych ze świata rzeczywistego dla celów wdrażania instrumentów dzielenia ryzyka dla technologii lekowych i wybranych technologii nielekowych, opartych o mierzalny efekt zdrowotny dla pacjentów, przy czym dane te w formie statystycznej dostępne byłyby publicznie.

[box] Co z tego wynika: Otrzymasz świadczenia medyczne o najwyższej jakości, która będzie potwierdzona na podstawie realnych danych.

Cel 3.2.6: Poziom cyberbezpieczeństwa w PWDL i centralnych repozytoriach danych jest wysoki

Co umożliwi realizację celu:

a) kontynuowanie programów dofinansowań dla szpitali w celu poprawy infrastruktury IT oraz wzmocnienia cyberbezpieczeństwa, w tym korzystania z usług wyspecjalizowanych podmiotów trzecich,

b) przekształcenie Sektorowego Zespołu Cyberbezpieczeństwa w Centrum e-Zdrowia w sektorowy CSIRT oraz wzmocnienie go w zakresie proaktywnego wspierania PWDL w utrzymaniu odpowiedniego poziomu cyberbezpieczeństwa,

c) regularne szkolenia dla kadry zarządzającej jednostkami leczniczymi oraz personelu medycznego w zakresie podstawowej wiedzy z cyberbezpieczeństwa,

d) intensyfikacja działań w zakresie cyberbezpieczeństwa systemów centralnych,

e) dostosowanie wytycznych ministerialnych dla kierunków medycznych do edukacji studentów w zakresie podstawowych zasad cyberbezpieczeństwa.

[box] Co z tego wynika: Wrażliwe dane o Twojej chorobie będą odpowiednio zabezpieczone i nie dostaną się w niepowołane ręce.

3.3 Branże kreatywne

Diagnoza – jak jest?

Przemysły kreatywne są stosunkowo nowym sektorem światowej gospodarki, opierającym się na kreatywnych, innowacyjnych i wynikających z talentu działaniach twórców szeroko pojętej sztuki, mediów i projektowania. Specyfiką sektora jest wysoki poziom wartości dodanej charakteryzujący wytwarzane w nim dobra, który bazuje na zaawansowanej i multidyscyplinarnej wiedzy twórców. Znaczenie gospodarcze sektora rośnie zarówno w odniesieniu do generowanej wartości, jak i rynku. W 2021 r. sektory kultury i kreatywne w Polsce wygenerowały bezpośrednio 31,2 mld zł wartości dodanej. Uwzględniając wpływ pośredni było to nawet ponad 82 mld zł (3,58 % PKB)[95]. Pod względem udziału wartości dodanej tworzonej w tych sektorach w PKB Polska znajduje się poniżej średniej UE, jednak gdy weźmie się pod uwagę również wpływ pośredni Polska zajmuje trzecie miejsce w Europie, ustępując tylko Cyprowi i Szwecji (spośród 15 badanych państw).

Wpływ przemysłów kreatywnych na rozwój państwa nie może być mierzony jedynie wskaźnikami gospodarczymi.

Lokuje się on bowiem na przecięciu obszarów gospodarki, kultury, technologii i biznesu – ma duże znaczenie kulturotwórcze i edukacyjne, sprzyjając jednocześnie innowacyjności. Jego rozwój jest zaś relatywnie mało zależny od wykorzystania surowców naturalnych czy infrastruktury przemysłowej. Zmiany społeczne, ważne dla budowania popytu na produkty i usługi, rysują dobre perspektywy dla rozwoju branż kreatywnych. Nie sposób jednak pominąć kilku istotnych zagrożeń. Można wśród nich wymienić m.in.: niewystarczające finansowanie, niesprzyjające, skomplikowane i zmienne regulacje prawne, wzrost konkurencji międzynarodowej, deficyt wykwalifikowanych pracowników, negatywny sentyment wśród inwestorów czy konieczność konkurowania z silniejszymi producentami z zagranicy.

Z perspektywy Strategii cyfryzacji, spośród różnorodnych przemysłów kreatywnych – na które składają się m.in.: przemysły filmowy, muzyczny oraz rozrywkowy, media i rynek wydawniczy - szczególne znaczenie ma sektor gier wideo i powiązanego z nim e-sportu. W 2022 r., spośród 5300 studiów deweloperskich w UE, 494 znajdowało się w Polsce[96], co zaraz po Szwecji, Niemczech i Francji stanowiło czwarty najwyższy wynik. W tym czasie 15 tys. z liczącej 90 tys. pracowników branży pracowało w Polsce. Mimo dużego rozmiaru branży, jej obroty w 2022 r. stanowiły jedynie 1,35 mld euro[97], co stanowi połowę obrotów branży niemieckiej (3,8 mld euro), która może pochwalić się statusem lidera w tej kategorii. Polską specjalizacją są gry klasy premium na duże platformy sprzętowe – komputery i konsole. Pod względem liczby zatrudnionych osób w branży, Polskę w Europie wyprzedza jedynie Wielka Brytania oraz Francja. Eksportowy charakter sektora (krajowa sprzedaż nie przekracza kilku procent) oznacza konieczność konfrontacji z nasiloną konkurencją, w tym

[95] https://pie.net.pl/wp-content/uploads/2023/12/PIE-Raport_Przemysly-kreatywne_2023.pdf.
[96] https://www.egdf.eu/2022-european-video-games-industry-insight-report/.
[97] Tamże.

ze strony największych światowych graczy. Tymczasem zarówno polski, jak i światowy gamedev mierzy się z kryzysem, wynikającym m.in. z odwrócenia nieorganicznych trendów wzrostowych z czasów pandemii.

W kontekście rozwoju branży należy uwzględnić jej kulturowy i kulturotwórczy aspekt.

Gry wideo coraz częściej bywają wykorzystywane w procesie nauczania. Sięgają po nie już nie tylko dzieci, młodzież i ludzie w średnim wieku, lecz także osoby starsze. W związku ze starzeniem się polskiego społeczeństwa, zjawisko tzw. *silver gamingu* będzie coraz powszechniejsze. Trend ten jest istotny z punktu widzenia dostępności gier dla szerokiego grona odbiorców, w tym osób z niepełnosprawnościami. Uznajemy, że gry powinny być traktowane jako tekst kultury podobnie jak filmy czy literatura, co oznacza m.in. wsparcie dla ich polonizacji i archiwizacji. Jednocześnie jest konieczne stałe zwracanie uwagi na kwestie higieny cyfrowej i przeciwdziałania uzależnieniom.

Działania państwa powinny objąć także obszar e-sportu, czyli profesjonalnych rozgrywek w branży gier komputerowych. Globalny rynek e-sportu w 2023 r. osiągnął wartość 3,8 mld dolarów, a prognozowane tempo rocznego wzrostu do 2028 r. wynosi 14,8%[98]. Polska zajmuje obecnie 19. miejsce na arenie międzynarodowej z sektorem o wartości 12,6 mln dolarów[99]. Polscy gracze mogą jednak pochwalić się zauważalnymi osiągnięciami, w naszym kraju odbywa się jedna z największych imprez branżowych na świecie. Rynek e-sportu wciąż dynamicznie się rozwija, głównie za sprawą przenikania kultury gamingowej do kultury popularnej. Zwiększająca się obecność gamingu i e-sportu w przestrzeni medialnej przyciąga zarówno widzów, jak i sponsorów. Można więc spodziewać się dalszej popularyzacji tego obszaru, także wśród dzieci i młodzieży w Polsce. Środowisko nie jest jednak wolne od (propagowanych na popularnych kanałach) negatywnych wzorców – toksycznych zachowań graczy względem siebie, niekorzystnego wpływu długotrwałej gry na zdrowie fizyczne i psychiczne, dyskryminacji ze względu na płeć i innych form wykluczenia etc. Dlatego z jednej strony należy wspierać rozwój tej branży i doceniać sukcesy polskich graczy, z drugiej - aktywnie przeciwdziałać pojawiającym się w tym sektorze negatywnym zjawiskom.

[98] https://markethub.pl/rynek-e-sportu/.
[99] https://en.parp.gov.pl/storage/publications/pdf/The_Game_Industry_Poland_2023_12_07.pdf4.

Cel 3.3.1: Rozwój branży gamingowej jest szybki

Co umożliwi realizację celu:

a) opracowanie strategii sektorowej skoncentrowanej na wsparciu producentów, promocji polskiego sektora gier wideo oraz zapewnieniu odpowiednich kwalifikacji przyszłym pracownikom branży,

b) rozwinięcie istniejącego wsparcia dla producentów gier przez dostosowanie istniejących programów do aktualnych potrzeb rynkowych, powiększenie kwot, o które mogą się oni ubiegać, i rozciągnięcie programów wsparcia na kilka lat oraz wypracowanie nowych form wsparcia,

c) wsparcie w promocji i marketingu gier jako polskiej marki na rynkach docelowych, szczególnie tych trudnych ze względu na geograficzną odległość i koszty, jak USA czy rynki azjatyckie, oraz budowanie pozytywnej atmosfery przez wykorzystanie narzędzi z zakresu dyplomacji kulturalnej i ekonomicznej w miejscach istotnych dla branży,

d) wsparcie w wykorzystaniu szans jakie niesie rewolucja AI dla rozwoju branży gier, uwzględniając jednocześnie potencjalne zagrożenia dla interesów twórców i dla rynku pracy w branży,

e) utworzenie lub dostosowanie zadań jednej z instytucji rządowych posiadającej kompetencje oraz narzędzia umożliwiające świadczenie realnego i wymiernego wsparcia, tylko dla branży gier wideo,

f) systemowe wsparcie dla programów stażowych i stypendialnych ułatwiających wejście w branżę młodym, zdolnym ludziom,

g) ułatwienia dla studiów zatrudniających wysokiej klasy ekspertów oraz managerów spoza Polski w obszarach, gdzie brak wykwalifikowanych polskich pracowników,

h) wsparcie dla procesów lokowania oddziałów zagranicznych firm w Polsce oraz oddziałów polskich firm poza granicami kraju, obejmujące m.in. doradztwo prawne i podatkowe, analizę lokalnych rynków, pomoc w doborze lokalizacji i rekrutacji personelu, a także koordynację formalności związanych z rejestracją działalności oraz integracją z lokalnym otoczeniem biznesowym,

i) wsparcie, we współpracy z sektorem akademickim, instytutami badawczymi, instytutami naukowymi i ekspertami branżowymi, procesu edukacji w zakresie kompetencji niezbędnych w studiach tworzących gry,

j) wsparcie przez instytucje publiczne lokalnych wydarzeń branżowych o zasięgu międzynarodowym,

k) wsparcie działań mających na celu uczynienie pracy w branży game dev[100] bardziej przyjazną i otwartą dla każdej grupy społecznej,

[100] Skrót od ang. game development – tworzenie gier.

l) promowanie gier wideo jako dzieła kultury – ze szczególnym uwzględnieniem polskich wersji językowych (zarówno gier polskich producentów, jak i zagranicznych),

m) opracowanie mechanizmu archiwizacji polskich gier wideo,

n) promowanie implementacji technologii dostępnościowych w grach wideo.

Cel 3.3.2: Bariery prawne utrudniające rozwój branż e-sportu i kreatywnej w Polsce są likwidowane, a e-sport popularyzowany

Co umożliwi realizację celu:

a) stosowanie prawnych aspektów e-sportu, w skład których wchodzi m.in. prawnoautorski status gier wideo, odzwierciedleń wizerunków i transmisji wydarzeń e-sportowych,

b) ewaluacja regulacji związanych z przekazywaniem majątkowych praw autorskich oraz licencjonowaniem i dostosowanie ich z uwzględnieniem realiów branż kreatywnych,

c) popularyzacja zawodów e-sportowych przez wsparcie w organizacji amatorskich zawodów na poziomie szkolnym,

d) promowanie profilaktyki zdrowia fizycznego i psychicznego u graczy, a także pozytywnych i inkluzywnych zachowań społecznych,

e) działanie na rzecz wprowadzenia specjalistycznych programów edukacyjnych w szkołach i na uczelniach wyższych, które będą kształcić przyszłych profesjonalistów w dziedzinie e-sportu, zarówno jako zawodników, jak i menedżerów czy analityków,

f) stworzenie przepisów prawnych, które będą regulować kwestie związane z e-sportem, takie jak kontrakty zawodników, prawa do transmisji czy ochrona młodzieży,

g) reprezentowanie polskiego e-sportu na międzynarodowych konferencjach i targach branżowych,

h) finansowanie i pomoc organizacyjna zapewniona przez jednostki administracji publicznej, we współpracy z organizacjami pozarządowymi i partnerami prywatnymi, dla lokalnych klubów e-sportowych, które promują zdrową rywalizację i rozwój talentów.

Cel 3.3.3: Branże kreatywne są wspierane w procesie rozwoju

Co umożliwi realizację celu:

a) dotacje i granty na rozwój projektów kreatywnych, umożliwiające artystom i firmom rozwijanie nowych projektów i technologii,

b) wsparcie rozwoju programów edukacyjnych i szkoleń, które kształcą w zakresie kreatywności, nowych technologii i zarządzania projektami kreatywnymi, a także współpraca z uniwersytetami i szkołami wyższymi w celu rozwijania programów nauczania dostosowanych do potrzeb branż kreatywnych,

c) uwzględnienie w stypendiach i programach mentorskich dla młodych, talentów w obszarze kultury branż kreatywnych i ich specyfiki,

d) tworzenie klastrów, inkubatorów i akceleratorów, które zapewniają przestrzeń do pracy, wsparcie techniczne i możliwość współpracy z innymi podmiotami z branży,

e) działania ułatwiające twórcom dostęp do nowoczesnych technologii i narzędzi, które wspierają twórczość i innowacje,

f) organizowanie kampanii promujących polskie branże kreatywne na arenie międzynarodowej, w tym uczestnictwo w targach i wystawach,

g) wzmocnienie przepisów dotyczących ochrony własności intelektualnej, co zapewni twórcom lepszą ochronę ich prac i zachęci do innowacji,

h) wspieranie organizacji konferencji, hackathonów, warsztatów i spotkań branżowych, które umożliwią wymianę doświadczeń i nawiązywanie kontaktów,

i) tworzenie partnerstw z sektorem prywatnym w celu realizacji wspólnych projektów i inicjatyw wspierających rozwój branż kreatywnych,

j) wprowadzenie programów wsparcia dla startupów, które oferują mentoring, dostęp do finansowania i sieci kontaktów branżowych,

k) wspieranie współpracy międzybranżowej i międzysektorowej.

3.4 Cyfrowy dostęp do wiedzy i kultury

Diagnoza – jak jest

Sektor instytucji odpowiedzialnych za ochronę dziedzictwa kulturowego w Polsce charakteryzuje się dużym zróżnicowaniem zarówno pod względem liczby podmiotów, jak i ich form organizacyjnych oraz zakresu misji. Zasoby dziedzictwa są przechowywane nie tylko w muzeach, bibliotekach i archiwach, lecz także w teatrach, operach, uczelniach, szkołach (zwłaszcza artystycznych), organizacjach pozarządowych, kościołach, związkach wyznaniowych, jednostkach samorządu terytorialnego oraz w rękach prywatnych. Samych państwowych instytucji kultury nadzorowanych przez Ministra Kultury i Dziedzictwa Narodowego jest ponad 140. Wszystkie te podmioty gromadzą obszerne zasoby o kluczowym znaczeniu dla tożsamości kulturowej i narodowej. Według danych GUS na koniec 2024 r. w rejestrze zabytków znajdowało się 79 935 obiektów nieruchomych. Poza tym istnieją także ogromne zbiory bibliotek, archiwów, muzeów i instytucji audiowizualnych.

Choć w ostatnich latach obserwuje się postęp w zakresie digitalizacji, jej tempo jest nadal nierównomierne. W 2024 r. zdigitalizowano 1,1 mln obiektów w instytucjach kultury (6% wszystkich dotychczas zdigitalizowanych zasobów)[101]. Choć w 2024 r. w Archiwach Państwowych wykonano blisko 8 mln skanów, dotychczas cyfryzacji poddano jedynie 2,99% zbiorów archiwalnych[102]. Dane te wskazują na pilną potrzebę kontynuacji i koordynacji działań digitalizacyjnych, by utrwalić dokumentację i zapewnić dostępność zbiorów dla przyszłych pokoleń. Wśród głównych wyzwań związanych z digitalizacją i monitorowaniem jej postępów zidentyfikowano m.in.: niewystarczające finansowanie, brak koordynacji działań, niespójność standardów opisu i odwzorowań cyfrowych, rozproszenie wykorzystywanych narzędzi i systemów informatycznych, niską interoperacyjność oraz ograniczoną skalę długoterminowej archiwizacji danych cyfrowych.

Szczególnym wyzwaniem pozostaje zabezpieczenie trwałości zasobów natywnie cyfrowych[103] (tzw. *born digital*) oraz treści publikowanych w internecie. Obecnie są one archiwizowane w bardzo ograniczonym zakresie, co niesie ryzyko ich bezpowrotnej utraty. Konieczne jest również ujednolicenie krajowych wytycznych dotyczących archiwizacji wieczystej oraz przegląd obowiązujących regulacji prawnych.

Zwiększenie spójności i integracja działań prowadzonych w sektorach kultury i nauki są kluczowe dla efektywnego wykorzystania zasobów, infrastruktury oraz dla rozwoju wspólnych standardów, narzędzi i usług cyfrowych odpowiadających potrzebom zróżnicowanych grup odbiorców.

Postępująca cyfryzacja i dynamiczny rozwój technologii wymagają stałego podnoszenia kwalifikacji pracowników sektora kultury nie tylko w celu zapewnienia odpowiedniego

[101] Kultura i dziedzictwo narodowe w 2024 r.: https://stat.gov.pl/obszary-tematyczne/kultura-turystyka-sport/kultura/kultura-i-dziedzictwo-narodowe-w-2024-r-,2,22.html.
[102] Sprawozdanie z działalności Archiwów Państwowych w 2024 roku: https://www.gov.pl/web/archiwa/rok-20251.
[103] Zasoby, które zostały wytworzone cyfrowo, nie posiadają analogowej, pierwotnej formy.

zabezpieczenia zasobów, lecz także dla tworzenia atrakcyjnych i użytecznych usług cyfrowych.

Niska świadomość społeczna dotycząca istniejących zbiorów oraz możliwości ich ponownego wykorzystania (*re-use*), w połączeniu z ograniczoną liczbą badań użytkowników i słabo rozwiniętymi usługami cyfrowymi, znacząco ograniczają społeczny i gospodarczy potencjał tych zasobów. Różnorodność cyfrowych zasobów kultury i nauki sprzyja popularyzacji idei cyfryzacji, ukazując dane nie tylko jako narzędzie administracyjne, lecz także jako nośnik wartości artystycznych, edukacyjnych i estetycznych. Mogą one wspierać edukację, w tym budowanie kompetencji cyfrowych oraz przyczyniać się do rozwoju sektora kreatywnego i nowoczesnego społeczeństwa informacyjnego.

Poza samą digitalizacją kluczowym zadaniem w zakresie cyfryzacji jest zapewnienie dostępu do informacji o zbiorach (nie tylko zdigitalizowanych) muzeów, archiwów i bibliotek w ogólnodostępnych, centralnych systemach katalogowych. Obecnie nadal wiele z tych instytucji nie posiada w pełni skatalogowanych zbiorów lub dane te nie zostały jeszcze poddane cyfryzacji. Pozwoli to nie tylko na zwiększenie wiedzy na temat tych zasobów, ujednolicenie danych, określenie potrzeb digitalizacyjnych, ale znacznie wpłynie na ich ochronę i bezpieczeństwo. Zadania te są realizowane obecnie m.in. przez Archiwa Państwowe, które bezpłatnie udostępniają zainteresowanym podmiotom Zintegrowany System Informacji Archiwalnej (ZoSIA) oraz umożliwiają publikowanie skanów dokumentów online w serwisie „Szukaj w Archiwach” (SwA) - w którym zgromadzono ponad 16 mln rekordów pochodzących ze 118 instytucji) oraz Bibliotekę Narodową, wdrażającą Zintegrowany System Zarządzania Zasobami Bibliotek, tworzony w ramach budowy ogólnokrajowej sieci bibliotecznej, w którym współkatalogują 153 biblioteki (stan na wrzesień 2025 r.). Powyższe działania powinny być nadal rozwijane oraz wdrażane w innych podmiotach takich jak np. muzea.

Cel 3.4.1: Kompleksowo wdrażany jest system wsparcia digitalizacji, udostępniania i długoterminowego przechowywania zasobów kultury i nauki

Co umożliwi realizację celu:

a) przyjęcie dokumentów kierunkowych dla digitalizacji zasobów dziedzictwa, definiujących cele, standardy i priorytety w zakresie zasobów kultury, dziedzictwa narodowego i nauki,

b) rozwój instrumentów finansowych, w tym zapewniających ciągłość finansowania projektów, wspierających digitalizację, udostępnianie i trwałe przechowywanie zasobów cyfrowych, modernizację repozytoriów cyfrowych i portali oraz tworzenie infrastruktury typu *data center* do archiwizacji wieczystej,

c) budowanie współpracy między instytucjami publikującymi dane z obszaru nauki, kultury i dziedzictwa narodowego oraz dane statystyczne w celu wspólnego rozwijania standardów, usług, narzędzi do digitalizacji, udostępniania i archiwizacji zasobów (także *born digital*), z uwzględnieniem najwyższych standardów bezpieczeństwa i integralności danych,

d) wprowadzenie systemowych rozwiązań dla archiwizacji zasobów natywnie cyfrowych, w tym przegląd i aktualizacja ram prawnych, wsparcie legislacyjne oraz rozwój inicjatyw archiwizacji stron internetowych podmiotów publicznych, ze szczególnym uwzględnieniem zasobów domeny gov.pl oraz portali instytucji publicznych,

e) wzmocnienie roli działających w sektorze kultury Centrów Kompetencji do spraw digitalizacji jako liderów w tym obszarze, a także wzmocnienie roli krajowych agregatorów danych w zakresie integracji i transgranicznego udostępniania zasobów, m.in. za pośrednictwem platformy Europeana oraz powstałej w oparciu o jej zasoby wspólnej europejskiej przestrzeni danych na potrzeby dziedzictwa kulturowego,

f) rozszerzenie zakresu gromadzonych danych statystycznych dotyczących procesów digitalizacji w instytucjach sektorów kultury i nauki oraz realizacja badań dotyczących potrzeb i zachowań cyfrowej publiczności, w celu lepszego projektowania usług cyfrowych,

g) rozwój kompetencji kadr sektora kultury i twórców przez systemową realizację szkoleń i otwarte udostępnianie materiałów edukacyjnych w zakresie digitalizacji (w tym technik specjalistycznych dokumentacji 3D), prawa autorskiego, re-use, cyberbezpieczeństwa, systemów back-office, etc.,

h) wypracowanie i wdrożenie zasad regulujących wykorzystanie cyfrowych zasobów kultury w procesach rozwoju i trenowania systemów sztucznej inteligencji.

Cel 3.4.2: Zasoby kultury i nauki są udostępniane obywatelom dzięki wdrożeniu nowoczesnych narzędzi technologicznych

Co umożliwi realizację celu:

a) modernizacja systemów cyfrowych wykorzystywanych przez instytucje kultury i nauki, w tym systemów centralnych takich jak Kronik@, oraz innych agregatorów danych, z uwzględnieniem standardów technicznych, interoperacyjności i otwartości danych. Działania obejmą także rozwój zaawansowanych funkcjonalności, takich jak: inteligentne wyszukiwanie, personalizacja treści i analiza preferencji użytkowników, co umożliwi bardziej intuicyjny i efektywny dostęp do zasobów oraz realizację kwerend,

b) budowa i wdrażanie otwartych interfejsów API oraz wsparcie i wykorzystanie istniejących metodyk i standardów pozwalających na integrację systemów instytucji kultury i nauki z portalami udostępniającymi zasoby cyfrowe, w celu konsolidacji rozproszonych zbiorów publikowanych w tzw. „portalach wyspowych", wspierania rozwoju nowych aplikacji i funkcjonalności opartych na cyfrowych danych,

c) zwiększanie dostępności cyfrowej zasobów dla osób z niepełnosprawnościami przez m.in.: zapewnianie zgodności efektów projektów digitalizacyjnych ze standardami dostępności, wykorzystanie nowoczesnych technologii (w tym sztucznej inteligencji) wspierających ten proces, organizację szkoleń w zakresie stosowania tych technologii w kontekście poprawy dostępności cyfrowej,

d) upowszechnianie wiedzy o zasobach cyfrowych przez prowadzenie działań edukacyjnych i informacyjno-promocyjnych skierowanych do obywateli, rozwój kampanii tematycznych, serwisów edukacyjnych i działań w mediach społecznościowych wspierających świadomość oraz zachęcających do korzystania z cyfrowego dziedzictwa,

e) wzmacnianie udziału Polski w międzynarodowych inicjatywach cyfrowego dziedzictwa, w tym zaangażowanie instytucji centralnych i jednostek odpowiedzialnych za zasoby cyfrowe w rozwój wspólnej europejskiej przestrzeni danych na potrzeby dziedzictwa kulturowego oraz aktywne uczestnictwo w projektach takich jak Europejska Chmura Dziedzictwa Kulturowego.

3.5 Cyfrowa akademia

Diagnoza – jak jest?

Rozwój cyfrowego państwa i gospodarki wymaga współpracy z akademią i sektorem naukowym, ale także dostrzeżenia konieczności długofalowego wsparcia dla rozwoju tego obszaru.

Bez oparcia się o silną krajową bazę naukową, polska sfera cyfrowa nie będzie rozwijała się harmonijnie.

Tymczasem polska nauka zmaga się ze strukturalnymi problemami, wynikającymi m.in. z niskiej atrakcyjności kariery, w szczególności wśród początkujących naukowców. Odpływ kadr oraz relatywnie niski odsetek absolwentów STEM stanowią poważne przeszkody dla rozwoju zrównoważonego systemu szkolnictwa wyższego i nauki, a niewielki przepływ doświadczonych naukowców między nauką a przemysłem ogranicza innowacyjność gospodarki. Te strukturalne problemy ulegają wzmocnieniu w przypadku kierunków ICT, które od lat dominują ranking wynagrodzeń w systemie monitorowania Ekonomicznych Losów Absolwentów[104]. Ze względu na silną presję ze strony przemysłu część studentów nie kończy studiów, koncentrując się na rozwoju kariery zawodowej. Bardzo niewiele osób decyduje się na karierę akademicką, co prowadzi do coraz silniej obserwowanej luki pokoleniowej w wielu ośrodkach akademickich[105]. Na braki specjalistów IT wskazuje także raport Polskiego Instytutu Ekonomicznego przygotowany we współpracy z Software Development Association Poland (SoDA)[106]. Z kolei przygotowany przez Uniwersytet Stanforda raport „2024 AI Index Report" sugeruje, że te luki doprowadziły już do spadku liczby kształconych w Polsce specjalistów ICT[107].

Negatywne trendy w rozwoju talentów IT są poważnym problemem, zwłaszcza za względu na szybki rozwój AI. Coraz większe strategiczne znaczenie tej technologii sprawia, że konieczny jest jej rozwój na poziomie krajowym. Polski system akademicki musi ulec wzmocnieniu w zakresie kształcenia specjalistów AI oraz możliwości horyzontalnego wykorzystania AI w interdyscyplinarnych badaniach naukowych. Należy podkreślić, że ze względu na dwa unikatowe wypracowane przez lata uwarunkowania, polska nauka jest w dobrej pozycji startowej w wyścigu o prymat w nadchodzących zmianach. Po pierwsze, mimo braku długofalowego wzrostu liczby studentów, mamy bardzo wysoki poziom kształcenia informatycznego, a polskiej szkole algorytmiki i programowania zawdzięczamy istotne sukcesy polskich informatyków w licznych konkursach, zawodach i olimpiadach. Po drugie, Polska jest jednym z liderów informatyzacji szkolnictwa wyższego i nauki w Europie, przede wszystkim dzięki sieci Zintegrowanego Systemu Informacji o Szkolnictwie Wyższymi i Nauce POL-on, a także budowanych na jej podstawie e-usług publicznych.

[104] https://ela.nauka.gov.pl/.
[105] https://www.zycieuczelni.p.lodz.pl/luka-pokoleniowa-problem-dla-uczelni-i-biznesu/.
[106] https://pie.net.pl/wp-content/uploads/2022/11/PIE_Raport_Ilu-specjalistow-IT-brakuje-w-Polsce.pdf.
[107] https://aiindex.stanford.edu/report/.

Cel 3.5.1. Pracownicy akademiccy kluczowi dla rozwoju kadr na potrzeby cyfrowego państwa są efektywnie wspierani w pracy naukowej i dydaktycznej

Co umożliwi realizację celu:

a) zadbanie o stabilność i bezpieczeństwo zatrudnienia w instytucjach naukowo-badawczych oraz uczelniach. Stworzenie mechanizmów uznawania znaczenia naukowej mobilności międzysektorowej (w tym wzajemnego uznawania doświadczenia między sektorami) oraz zmiany systemu oceny publikacji na skoncentrowaną na jakości i znaczeniu wyników prowadzonych badań.
W technologiach cyfrowych bardzo wielu badaczy często przepływa między nauką a przemysłem, dlatego jest ważne promowanie znaczenia takiego przemysłowego doświadczenia w uczelni oraz akademickiego w przemyśle. Dzięki tak ułatwionemu przepływowi ludzi zwiększy się i zacieśni współpraca nauki z biznesem,

b) dążenie do zwiększenia wsparcia finansowego dla osób uczących się i młodych naukowców w dziedzinach kluczowych dla cyfrowego państwa. Poszukiwanie innych modeli stabilnego wsparcia finansowego oraz nagród i premii za badania i publikacje IT, AI i STEM we wszystkich dyscyplinach,

c) promocja kariery naukowej w zakresie STEM w obszarze nowych technologii, jako dającej duże możliwości rozwoju – od pracy w jednostkach i centrach badawczych, na uczelniach po zakładanie startupów. Wsparcie współpracy między różnymi typami jednostek badawczych,

d) ustrukturyzowanie w zakresie nietradycyjnych ścieżek kariery, w tym stworzenie stanowisk inżynierów badawczych na uczelniach, oraz inne mechanizmy zapewniające lepszą mobilność między sektorem publicznym i prywatnym. Zwiększenie znaczenia doświadczenia zdobytego w przemyśle w karierze akademickiej.

Cel 3.5.2: Polska nauka jest wspierana przez zaawansowaną infrastrukturę informatyczną

Co umożliwi realizację celu:

a) inwestycje w moce obliczeniowe na potrzeby prowadzenia badań naukowych, w szczególności potrzebne do wykorzystania AI w interdyscyplinarnych dziedzinach nauki. Zwiększenie mocy obliczeniowych musi następować razem ze stworzeniem w ramach HPC (wysokowydajne przetwarzanie, ang. high-performance computing)/PLGrid systemów raportowania obciążenia, liczby projektów/grantów oraz wspartych startupów,

b) dalszy rozwój systemów POL-on (Zintegrowany System Informacji o Szkolnictwie Wyższym i Nauce), ELA (Ekonomiczne Losy Absolwentów) i OSF (Obsługa Strumieni Finansowania), aby stały się referencyjnymi źródłami danych dla e-usług publicznych pozwalającymi skuteczniej mierzyć i analizować efektywność realizowanych projektów naukowych i komercjalizować wyniki badań,

c) rozwój e-usług cyfrowych skierowanych do kandydatów na studia, studentów, doktorantów i absolwentów uczelni, takich jak: system wspierający kandydatów na studia w wyborze uczelni i kierunku studiów, eDyplomy, udostępnienie zestawu narzędzi wspierających właściwy wybór kierunków studiów, mLegitymacje,

d) stworzenie portalu gromadzącego informacje o potencjale badawczym, komercjalizacyjno-wdrożeniowym i aparaturowym zainteresowanych jednostek naukowych, który ułatwi nawiązywanie współpracy między nimi oraz między nauką i biznesem w celu realizacji wspólnych projektów w konsorcjach naukowych i naukowo-przemysłowych,

e) wspieranie działań sektora naukowo-badawczego w Polsce w obszarze cyberbezpieczeństwa, aby zapewnić kompleksową ochronę danych, technologii oraz infrastruktury badawczej w polskich uczelniach i instytutach badawczych.

Cel 3.5.3: Polska nauka w dziedzinie ICT jest widoczna na arenie międzynarodowej

Co umożliwi realizację celu:

a) promocja oraz umiędzynarodowienie polskiej nauki, m.in. przez współpracę z najlepszymi uczelniami w Europie i na świecie oraz propagowanie sukcesów polskich informatyków,

b) rozwój dyplomacji naukowej w zakresie podwyższenia poziomu pozyskiwania zagranicznych środków publicznych (w tym europejskich) na badania naukowe oraz zwiększenie promocji i szkoleń z pozyskiwania funduszy europejskich na badania i rozwój,

c) dostosowanie i poprawa systemu oceny parametrycznej jednostek naukowo-badawczych tak by bardziej wspierała komercjalizację wyników badań naukowych oraz wypracowanie nowych ścieżek komercjalizacji badań uwzględniających nowoczesne, międzynarodowe modele prowadzenia badań,

d) wsparcie udziału polskich instytucji oraz naukowców w międzynarodowych sieciach oraz organizacjach technologicznych, które mają na celu wspieranie rozwoju w sektorze ICT,

e) wzmocnienie wiodących uczelni informatycznych i centrów badawczych oraz stworzenie w Polsce instytucji badawczych, które mają szansę zyskać renomę międzynarodową. Uznajemy, że istnienie w kraju instytucji badawczych o renomie międzynarodowej jest jednym z najbardziej skutecznych działań przeciwdziałających drenażowi mózgów. Wykorzystanie Instytutu IDEAS, który przez prowadzenie interdyscyplinarnych badań będzie promował wykorzystanie AI w zróżnicowanych dziedzinach, a także Ośrodka Badań nad Bezpieczeństwem Sztucznej Inteligencji NASK - PIB, który będzie podejmował podobne działania w obszarze bezpieczeństwa tej technologii.

4. Gospodarka i technologie

4.1 Cyfrowa transformacja przedsiębiorstw

Diagnoza – jak jest?

W 2024 r. ponad dwie trzecie polskich przedsiębiorstw zostało zakwalifikowanych do grupy o bardzo niskiej lub niskiej intensywności cyfrowej, a 33% przedsiębiorstw charakteryzowało się wysokim lub bardzo wysokim poziomem intensywności cyfrowej. Sektor MŚP w Polsce tworzący 99,8% ogółu przedsiębiorstw generuje 46,6% PKB (dane za 2022 r.)[108]. Małe i średnie przedsiębiorstwa pełnią kluczową rolę w rozwoju polskiej gospodarki, a ich transformacja cyfrowa jest warunkiem utrzymania i poprawy pozycji konkurencyjnej Polski na rynku międzynarodowym.

W 2024 r. odsetek przedsiębiorstw mających szerokopasmowy dostęp do internetu wyniósł prawie 99%. W 2025 r. 93,1% przedsiębiorstw stosowało przynajmniej jeden z badanych środków bezpieczeństwa ICT, przy czym najczęściej była to identyfikacja i uwierzytelnianie silnym hasłem (81,0%). Technologie oparte na sztucznej inteligencji najczęściej wykorzystywano w procesach związanych z marketingiem i sprzedażą (5,0%), najrzadziej – w dziedzinie logistyki (0,8%). Z technologii sztucznej inteligencji korzystało 42% podmiotów dużych. Wśród podmiotów dużych największym zainteresowaniem cieszyło się zastosowanie AI w procesach związanych z bezpieczeństwem ICT (22,5%)[109]. W 2025 r. z technologii chmurowych korzystało 55,3% firm, z analityki danych – 25,9%, 40,5% przedsiębiorstw wykorzystywało oprogramowanie ERP[110], a CRM[111] - 25,1%[112]. W 2025 r. AI wykorzystywało 8,7% firm[113], a sprzedaż przez internet prowadziło 18,3% przedsiębiorstw[114]. W 2024 r. 20% MŚP nie wykorzystywało żadnych narzędzi cyfrowych, natomiast te, które ich używały, najczęściej wskazywały podstawowe narzędzia cyfrowe, jak wykorzystanie mediów społecznościowych do promocji firmy czy usług przetwarzania danych w chmurze[115].

Poziom cyfryzacji przedsiębiorstw skorelowany jest z ich wielkością: im większe, tym przeciętnie więcej wydatków przeznacza na prace badawczo-rozwojowe i wdrażanie nowych technologii.

[108] Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce, 2025, PARP.
[109] Społeczeństwo informacyjne w Polsce w 2025 r., GUS.
[110] Enterprise Resource Planning (ang.) – oprogramowanie do zarządzania przedsiębiorstwem.
[111] Customer Relationship Management (ang.) – oprogramowanie do zarządzania relacji z klientami
[112] Dane za: Eurostat 2025, https://ec.europa.eu/eurostat/databrowser/view/isoc_cicce_use/default/table?lang=en.
[113] Dane za: Eurostat 2025.
[114] Społeczeństwo informacyjne w Polsce w 2025 r., GUS.
[115] Raport BGK „Cyfryzacja w sektorze MŚP – szanse i ograniczenia”.

Podobna zależność występuje w przypadku innowacyjności przedsiębiorstw: największy odsetek podmiotów aktywnych innowacyjnie występuje wśród dużych firm. Częściej są wprowadzane innowacje w procesach biznesowych niż innowacje produktowe.

Innym aspektem cyfrowej transformacji jest wdrażanie zaawansowanych technologii Przemysłu 4.0. Diagnoza wdrażania Przemysłu 4.0 w Polsce na lata 2022-2024 wskazuje na stopniowe, choć nierównomierne postępy w adaptacji nowoczesnych technologii w różnych sektorach gospodarki. Tempo wdrażania jest ściśle powiązane z wielkością przedsiębiorstwa (najczęściej technologie Przemysłu 4.0. wdrażają duże firmy o przychodach przekraczających 500 mln zł). Polska jest w początkowej fazie wdrażania Przemysłu 4.0, jednak posiada znaczny potencjał wzrostu, szczególnie wśród dużych przedsiębiorstw. Niemniej niskie tempo adopcji technologii przełomowych oraz brak długoterminowych planów w zakresie ich wdrażania stawiają polski przemysł w niekorzystnej pozycji w porównaniu z innymi państwami członkowskimi Unii Europejskiej, gdzie poziom inwestycji w cyfryzację jest na wyższym poziomie.

Poziom zaawansowania technologicznego polskich firm, w tym zwłaszcza małych i średnich przedsiębiorstw, wymaga podniesienia, aby możliwy był wzrost ich produktywności.

To z kolei jest warunkiem dalszego, dynamicznego rozwoju polskiej gospodarki. Z badań dotyczących produktywności polskich przedsiębiorstw wynika, że istnieje duży potencjał do zwiększenia jej poziomu dzięki zastosowaniu usprawnień w postaci nowoczesnych narzędzi cyfrowych.

W Polsce dominuje produkcja niskoseryjna o dużej różnorodności, dlatego tradycyjne podejście do cyfryzacji, automatyzacji i robotyzacji nie może przynieść oczekiwanych efektów ekonomicznych. Różnego typu zaawansowane urządzenia, maszyny, obrabiarki i roboty wymagają wykwalifikowanej obsługi ludzkiej. Niż demograficzny może jeszcze bardziej pogorszyć obecną sytuację. Koszty przygotowania produkcji oraz pozyskania nowych zleceń stanowią większy udział w ogólnych kosztach produkcji. Ten obszar w ogóle nie jest objęty automatyzacją.

Poza zaprojektowaniem odpowiednich instrumentów wsparcia finansowego dla firm konieczne są również działania związane ze zwiększaniem świadomości firm z korzyści, jakie niesie za sobą zastosowanie nowych technologii, rozwój kompetencji i umiejętności pracowników oraz osób zarządzających przedsiębiorstwami w zakresie stosowania nowoczesnych rozwiązań cyfrowych, a także rozwój systemu otoczenia biznesu sprzyjającego innowacjom.

Do głównych barier w obszarze transformacji cyfrowej należą[116]:

- brak przekonania o korzyściach – typu zysk z inwestycji w cyfryzację,

- niedobór specjalistów na rynku oraz brak kompetencji, w szczególności w zakresie umiejętności tworzenia oprogramowania, złożonej analizy danych i matematycznych,

[116] eSkills for Jobs Index, Dojrzałość technologiczna polskich firm oraz raport BGK z 2024 r. Cyfryzacja w sektorze MŚP – szanse i ograniczenia.

umiejętności zarządzania projektem z wykorzystaniem narzędzi IT czy opracowania strategii cyfrowej i zdolności przywódczych,

- wysokie koszty wdrożenia narzędzi cyfrowych i brak odpowiednich możliwości finansowania,

- brak czasu na wdrażanie rozwiązań cyfrowych,

- problemy z bezpieczeństwem informatycznym,

- wciąż występujący brak dostępu do szybkiego Internetu na niektórych obszarach kraju.

Wśród polskich firm od lat widoczny jest także brak chęci rozwoju sprzedaży w Internecie. W związku z tym, konieczna jest nie tylko kontynuacja wsparcia w ogólnie pojętej transformacji cyfrowej, ale także celowane działania, które pozwolą na budowę silnej marki Polski w handlu międzynarodowym i wpłyną pozytywnie na konkurencyjność firm i gospodarki.

Cel 4.1.1: Funkcjonuje sprawny system zarządzania działaniami w obszarze wspierania transformacji cyfrowej przedsiębiorstw[117]

Co umożliwi realizację celu:

a) powołanie podmiotu koordynującego transformację cyfrową przedsiębiorstw, w tym zwłaszcza sektora MŚP, który definiowałby cele i działania, monitorował postępy, oceniał stopień realizacji zakładanych celów, identyfikował potrzeby technologiczne oraz oczekiwania i możliwości MŚP,

b) opracowanie wspólnej i spójnej na poziomie krajowym wizji cyfryzacji przedsiębiorstw, w tym przede wszystkim sektora MŚP, uwzględniającej wpływ dużych przedsiębiorstw na cyfryzację MŚP w ich łańcuchu dostaw, a także określającej strategie i standardy, które będą wspierać integrację MŚP z cyfrowymi rozwiązaniami wdrażanymi przez duże firmy,

c) opracowanie jasnych zasad podatkowych w zakresie korzystania przez MŚP z nieodpłatnych programów wspierających transformację cyfrową,

d) zapewnienie zrozumiałości i dostępności informacyjnej programów wspierających cyfryzację przedsiębiorstw,

e) udostępnienie w jednym miejscu kompleksowej informacji o dostępnych programach wsparcia oraz przeznaczonych dla przedsiębiorców materiałach i szkoleniach.

[box] Co z tego wynika: Każda firma, która będzie chciała wdrożyć rozwiązania cyfrowe, będzie wiedziała, gdzie i do kogo się zwrócić po informację.

[117] Automatyzacja i robotyzacja są narzędziami transformacji cyfrowej przedsiębiorstw.

Cel 4.1.2: Przedsiębiorcy postrzegają transformację cyfrową jako proces ułatwiający działalność firmy i zwiększający jej efektywność

Co umożliwi realizację celu:

a) prowadzenie działań edukacyjnych budujących świadomość korzyści płynących z procesu cyfryzacji oraz rozwoju kompetencji cyfrowych pracowników i kadry menedżerskiej,

b) ocena istniejących rozwiązań wspierających cyfryzację przedsiębiorstw oraz zaprojektowanie, na podstawie przeprowadzonej diagnozy, i zaimplementowanie nowych instrumentów wspierających transformację cyfrową przedsiębiorstw, które będą dopasowane do potrzeb poszczególnych kategorii przedsiębiorców,

c) określenie branży kluczowych, które gwarantują transfer technologii i tworzenie wewnętrznego łańcucha dostaw opartego na rodzimych firmach, w których Polska posiada potencjał do przewagi konkurencyjnej i skierowanie w te obszary celowanych działań. Kluczowe będą te branże, które mają istotny wpływ na polskie PKB, duży udział w eksporcie oraz znaczący potencjał wzrostu produktywności w wyniku transformacji cyfrowej i wdrażania technologii Przemysłu 4.0,

d) wprowadzenie instrumentu „Cyfrowy start dla biznesu", który wspierałby nowopowstałe firmy w rozwoju cyfrowym. Pakiet ten zawierałby propozycje rozwiązań cyfryzujących procesy biznesowe już na początku działania firmy i ułatwiających jej prowadzenie – np. oprogramowanie biurowe, księgowe i finansowe, zarządzania relacjami z klientami oraz dokumentami, programy do komunikacji i współpracy, oprogramowanie cyberbezpieczeństwa, ewentualnie systemy planowania zasobów przedsiębiorstwa,

e) skuteczne wsparcie przedsiębiorców w zmianie cyfrowej, obejmujące w szczególności automatyczną samoocenę dojrzałości cyfrowej przedsiębiorstwa oraz spersonalizowane dopasowanie rozwiązań cyfrowych dla danej firmy. Wsparcie to będzie realizowane przez system skoordynowanego doradztwa świadczonego przez Doradców ICT w zakresie wdrożenia technologii i cyberbezpieczeństwa, szkolenia, możliwości przetestowania i eksperymentowania rozwiązań w ramach pilotaży oraz pomoc w znalezieniu źródeł finansowania transformacji cyfrowej. System wsparcia będzie uwzględniał m.in. sieć EDIH - European Digital Innovation Hubs, czyli europejskie centra innowacji cyfrowych,

f) wsparcie cyfryzacji podmiotów spółdzielczych m.in. w zakresie zwiększania cyberbezpieczeństwa, usprawniania procesów zarządzania oraz ułatwienia efektywnego zarządzania komunikacją i relacjami organów podmiotów spółdzielczych z jej członkami.

[box] Co z tego wynika: Ułatwimy przedsiębiorstwom zrozumienie korzyści z cyfryzacji i wesprzemy w transformacji cyfrowej, proponując najlepsze dla firmy narzędzia.

Cel 4.1.3: Cyfrowe usługi publiczne dla przedsiębiorców są proaktywne i dojrzałe, a interoperacyjność systemów umożliwia zredukowanie obciążeń administracyjnych

Co umożliwi realizację celu:

a) rozwijanie usług publicznych do coraz wyższego stopnia dojrzałości, opartych o potrzeby użytkowników, które proponują użytkownikom wykonanie czynności lub akceptację działań wykonanych przez system,

b) pełna cyfryzacja relacji między przedsiębiorcami a państwem (w tym przez cyfryzację procedur administracyjnych np. w ramach procesów budowlanych),

c) wprowadzenie zasady „tylko raz”, co oznacza, że obywatele i przedsiębiorstwa dostarczają swoje dane administracji publicznej tylko raz, a administracja publiczna następnie wewnętrznie udostępnia te dane pomiędzy instytucjami, unikając obciążania obywateli i przedsiębiorców.

[box] Co z tego wynika: Kontakt firmy z administracją publiczną będzie ograniczony do niezbędnego minimum, a urzędy między sobą wymienią się danymi. Firma nie będzie zmuszona to kilkukrotnego podawania tych samych danych różnym urzędom.

Cel 4.1.4: Przedsiębiorcy są świadomi cyberzagrożeń i sięgają po instrumenty zapobiegawcze

Co umożliwi realizację celu:

a) rozpowszechnianie podstawowych informacji z zakresu cyberbezpieczeństwa,

b) udostępnianie (również w ramach „Firmy Bezpiecznej Cyfrowo”) szkoleń i kursów obejmujących zakresem tematykę m.in. cyberzagrożeń (również bezpłatnych ankiet samooceny poziomu cyberbezpieczeństwa firmy wraz z rekomendacjami wdrożenia zmian) i dezinformacji oraz działania wspierające odnoszące się do miejsca przedsiębiorstwa w łańcuchu dostaw i zakresu odpowiedzialności (np. mikro i małe firmy, producenci produktów i usług IT, przedsiębiorstwa objęte dyrektywą NIS 2),

c) wprowadzenie systemu dobrowolnej certyfikacji cyberbezpieczeństwa w przedsiębiorstwach,

d) powiązanie systemu certyfikacji cyberbezpieczeństwa z ubezpieczeniami od ryzyk cyberbezpieczeństwa i uzależnienie wysokości składki z posiadanym ubezpieczeniem.

[box] Co z tego wynika: Pomożemy firmom w zapewnieniu im najwyższego bezpieczeństwa w cyfrowym świecie.

Cel 4.1.5: Przedsiębiorcy z sektora przemysłu są świadomi korzyści wykorzystywania technologii Przemysłu 4.0 i wdrażają je w swoich firmach

Co umożliwi realizację celu:

a) wspieranie adopcji zaawansowanych technologii Przemysłu 4.0 przez stymulację współpracy międzyinstytucjonalnej, w tym współpraca z technicznymi ośrodkami akademickimi w celu opracowania programów podnoszących kwalifikacje pracowników przemysłowych, współpraca między sektorem publicznym a prywatnym w celu budowy nowoczesnych centrów danych i platform cyfrowych,

b) tworzenie platform wymiany wiedzy online, które umożliwiają przedsiębiorstwom dzielenie się doświadczeniami i przykładami najlepszych praktyk w zakresie Przemysłu 4.0, a także kierunków rozwoju w stronę Przemysłu 5.0,

c) ułatwianie przedsiębiorcom dotarcia do źródeł finansowania technologii Przemysłu 4.0, w tym ulg podatkowych i grantów na innowacje, kredytów technologicznych i programów pilotażowych wdrożeń.

[box] Co z tego wynika: Ułatwimy firmom sprawne wdrożenie zaawansowanych technologii Przemysłu 4.0., pomagając im w uzyskaniu źródeł finansowania oraz stwarzając warunki do podnoszenia kwalifikacji pracowników i wymiany doświadczeń.

4.2 Sztuczna inteligencja

Diagnoza – jak jest?

Implementacja najnowszych technologii oraz korzystanie z systemów opartych na zorientowanej na człowieka, zrównoważonej, godnej zaufania bezpiecznej i sprzyjającej włączeniu społecznemu sztucznej inteligencji (AI) są kluczowe dla rozwoju Polski.

Technologia ta może znacząco poprawić moce produkcyjne w przemyśle, efektywność i jakość świadczonych usług, a także wspierać procesy decyzyjne i zarządzanie zasobami.

AI jako technologia automatyzująca procesy jest również kluczowym narzędziem pozwalającym ograniczyć negatywne skutki trendów demograficznych. Wreszcie, technologia ta ma potencjał transformacyjny we współpracy z innymi przełomowymi technologiami, takimi jak chmura obliczeniowa czy internet rzeczy. Ten konglomerat, którego centralnym elementem jest AI, określany bywa jako AI+. Rośnie liczba i skala inwestycji w produkty i usługi AI[118]. W tym wyścigu stawką jest udział w szybko rosnącym rynku AI i powiązanych z nim korzyści – eksportu ICT, wzrostu produktywności i innowacji. Dzisiejsze szacunki wskazują, że do końca dekady korzyści te sięgną 10% globalnego produktu brutto, zaś wartość samego rynku AI przekroczy 1,3 bln dolarów. Kraje uczestniczą w tym wyścigu tworząc atrakcyjne warunki dla inwestorów i innowatorów. Polska jest w nim poza światową czołówką, wyprzedzają nas – prócz globalnych gigantów – kraje europejskie takie jak Wielka Brytania, Niemcy, Szwecja, Hiszpania[119]. Wyścig ten jest jednak na wczesnym etapie i zmiana tego stanu rzeczy jest konieczna i możliwa.

Dlatego administracja publiczna, ośrodki akademickie oraz instytucje naukowo-badawcze, przy wsparciu infrastrukturalnym centrów HPC, muszą systematycznie monitorować trendy, w tym te, których kierunku dziś nie jesteśmy w stanie w pełni przewidzieć – jak rozwój agentowych systemów AI, sztucznej inteligencji wspieranej obliczeniami kwantowymi czy interfejsów mózg–komputer. Tylko takie podejście zapewni Polsce długofalową gotowość do reagowania na przełomy technologiczne, które dopiero nadchodzą.

W kontekście rozwoju AI przed Polską stoi dodatkowo szereg wyzwań strukturalnych i infrastrukturalnych. Budowa i rozwój przyjaznego ekosystemu AI w Polsce wymaga równoczesnej stymulacji tempa wzrostu inwestycji publicznych, jak i prywatnych w badania, infrastrukturę i innowacje, przy czym te ostatnie są szczególnym wyzwaniem w odniesieniu do małych i średnich firm. Aby znaleźć się w gronie liderów konieczne jest również

[118] https://www.goldmansachs.com/insights/articles/ai-investment-forecast-to-approach-200-billion-globally-by-2025.html.
[119] https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392_EN.pdf.

budowanie świadomości przedsiębiorców o korzyściach ze stosowania AI/AI+, zwiększenie dostępu do specjalistycznej wiedzy oraz mocy obliczeniowych.

Kluczowym potencjałem dla rozwoju sektora są specjaliści. Od początku 2020 r. do pierwszej połowy 2023 r. nadano w Polsce około 19 tys. stopni doktora, w tym 622 w dyscyplinach związanych z informatyką i 207 z tematyki sztucznej inteligencji[120]. To wskaźniki, które plasują nas poza pierwszą 15. w Europie w kategorii absolwentów kierunków informatycznych, zarówno ilościowo, jaki i w przeliczeniu na 100 000 mieszkańców[121].

Konieczne jest przyjęcie i egzekwowanie spójnych ram prawnych, stosowania standardów i kodeksów dobrych praktyk, a także podniesienie poziomu dostępu do wysokiej jakości, optymalnej energetycznie infrastruktury (teleinformatycznej, obliczeniowej, energetycznej). Polska ma obowiązek przeprowadzenia procesu legislacyjnego – wdrożenia uzgadniającego krajowy porządek prawny z unijnym AI Act[122] i prawem międzynarodowym, czego efektem będzie obowiązywanie przepisów dotyczących sztucznej inteligencji w Polsce. Przed Polską stoi również wdrożenie zbieżnej z regulacjami unijnymi Konwencji Ramowej o sztucznej inteligencji, prawach człowieka, demokracji i praworządności przyjętej przez Komitet Ministrów Rady Europy.

Ważne jest wdrożenie tych regulacji w sposób sprzyjający innowacjom, równoważący troskę o godną zaufania, bezpieczną AI, z dbaniem o rozwój i wdrażanie innowacji w przedsiębiorstwach.

Ta równowaga powinna przejawić się zarówno w podejściu instytucjonalnym (rola i zakres działania polskich organów nadzoru współpracujących z europejskim Biurem ds. AI), jak i w systemie finansowania inwestycji. Jednocześnie państwo nie może decydować się na wdrażanie konkretnej technologii bez przeprowadzania pogłębionych analiz dotyczących spodziewanych efektów i ryzyk wynikających z implementacji. Państwo powinno stosować AI tam, gdzie maksymalnie ułatwi życie obywatelom i realnie odpowie na potrzeby społeczne, a jednocześnie nie wygeneruje nadmiernych ryzyk, w związku z czym kluczową rolę pełni NASK - PIB, który podejmuje działania w obszarze zapewnienia bezpieczeństwa (algorytmów) AI.

Stąd też silna potrzeba aktualizacji polityki publicznej dotyczącej rozwoju sztucznej inteligencji w Polsce, w tym wskazanie obszarów strategicznych dla rozwoju gospodarki, w których AI powinna być wdrażana priorytetowo. Obecnie trwają prace nad nową Polityką AI

[120] https://ideas-ncbr.pl/wp-content/uploads/2024/04/04.2024_Raport_IDEAS_NCBR_Trendy_w_ksztalceniu_w_obszarze_AI_na_poziomie_doktoranckim.pdf.
[121] Stanford Institute for Human-Centered Artificial Intelligence, 2024 AI Index Report, Chapter Education, 2024.
[122] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. Urz. UE L 2024/1689 z 12.07.2024).

dla Polski – dokumentem kierunkowym, który określi najważniejsze priorytety, działania oraz ramy instytucjonalne w obszarze rozwoju i wdrażania sztucznej inteligencji. Taka polityka musi uwzględniać aktualne trendy i wyzwania oraz zapewniać spójność i koordynację na szczeblu rządowym i umożliwić aktywną współpracę międzynarodową.

AI, jako technologia podwójnego zastosowania (*dual-use*), odgrywa kluczową rolę nie tylko w gospodarce, ale i we współczesnych konfliktach, dlatego tak istotne jest wdrażanie Resortowej strategii sztucznej inteligencji do roku 2039[123], która zapewni skuteczne, bezpieczne i odpowiedzialne zastosowanie tej technologii w środowisku operacyjnym.

Polacy mają wysoką świadomość istnienia sztucznej inteligencji – 98,8% osób deklaruje, że o niej słyszało[124]. Połowa Polaków (51,1%) uważa, że sztuczna inteligencja przyniesie społeczeństwu więcej korzyści niż szkód. Jednocześnie 25% badanych było przekonanych, że szkody wyrządzone przez AI przewyższą korzyści. Polacy darzą AI sporym zaufaniem, 41% badanych jest skłonnych polegać na informacjach dostarczanych przez sztuczną inteligencję. Mimo tego 40% wskazuje na potrzebę zapewnienia nadzoru człowieka nad rozwojem AI.

Polacy w dużej mierze[125] wyrażają poparcie dla wykorzystania AI przez państwo. Według 60,4% sztuczna inteligencja powinna być wykorzystywana przy tworzeniu cyfrowych usług publicznych. Zdaniem 32% badanych sztuczna inteligencja może przyspieszyć i zautomatyzować procesy administracyjne oraz skrócić czas realizacji usług publicznych. Inną często podnoszoną przez badanych nadzieją na wykorzystanie AI w usługach publicznych jest zwiększenie ich dostępności dla osób z niepełnosprawnościami. Polacy są niechętni wobec wykorzystania sztucznej inteligencji do zautomatyzowanego podejmowania decyzji administracyjnych, które mogą mieć wpływ na ich życie. Natomiast wyższym poparciem darzą możliwość automatyzacji prostych czynności administracyjnych, ostrzegania w sytuacjach nadzwyczajnych czy wykorzystania AI jako wsparcia dla obywateli przy wypełnianiu dokumentów. Wdrażane systemy AI muszą być nie tylko sprawiedliwe, ale optymalne w kontekście wykorzystania zasobów, uwzględniając poszanowanie danych osobowych i praw autorskich, a także wykorzystanie mniejszych, bardziej optymalnych modeli w specjalistycznych procesach, minimalizując zużycie energii.

Podsumowując, kluczowe dla rozwoju technologii jest stworzenie szerokiego ekosystemu AI+, który obejmuje współpracę publicznych i prywatnych podmiotów w zakresie edukacji, badań, innowacji, produkcji oraz bezpiecznego wdrażania rozwiązań z wykorzystaniem sztucznej inteligencji.

[123] https://www.gov.pl/web/obrona-narodowa/resortowa-strategia-sztucznej-inteligencji-do-roku-2039.
[124] https://pie.net.pl/wp-content/uploads/2024/09/Sztuczna-inteligencja-w-administracji-publicznej.pdf.
[125] Tamże.

Cel 4.2.1: Rozwój gospodarki, przemysłu cyfrowego i dobrostanu społecznego jest wspierany przez sprawny i skoordynowany ekosystem sztucznej inteligencji

Co umożliwi realizację celu:

a) stworzenie zgodnego z przepisami unijnymi oraz przyjaznego dla przedsiębiorczości systemu nadzoru nad systemami AI, dzięki czemu obywatele, konsumenci i firmy będą miały świadomość oraz pewność, że rozwiązania AI używane na rynku i w administracji publicznej są bezpieczne, zgodne z przepisami i etyką,

b) koordynacja współpracy instytucji badawczych wchodzących w skład ekosystemu AI przez instytucję wiodącą,

c) zagwarantowanie przejrzystego, skoordynowanego i efektywnego finansowania rozwoju polskich firm w obszarze AI i innowacji cyfrowych, a także zwiększanie poziomu wsparcia (prywatnego, publicznego) dla przedsiębiorców rozwijających i wdrażających AI,

d) utworzenie zgodnych z podejściem unijnym piaskownic regulacyjnych (sandboxów) dla innowatorów. Objęcie nimi sektorów kluczowych dla rozwoju i wdrożenia AI,

e) stworzenie jednolitej, dostępnej publicznie listy systemów AI używanych w administracji publicznej wraz z opisem funkcji lub celu oraz podstawowych parametrów technicznych dostępnych dla obywateli w celu zwiększenia transparentności administracji publicznej. Opracowanie i egzekwowanie zasad stosowania AI w administracji publicznej, ze szczególnym uwzględnieniem wymogów cyberbezpieczeństwa,

f) rozwijanie krajowych rozwiązań i standardów w zakresie bezpieczeństwa technologii przełomowych, w szczególności sztucznej inteligencji, w tym również inicjowanie programów i projektów badawczo-rozwojowych w tym zakresie – w celu stymulacji możliwości użycia rozwiązań opartych na AI w sektorze usług publicznych, a także w zastosowaniach dla bezpieczeństwa państwa,

g) zbudowanie wokół Ośrodka Badań nad Bezpieczeństwem Sztucznej Inteligencji organizacji skupiającej przedstawicieli firm i instytucji badawczych mającej na celu promowanie wzajemnej współpracy w zakresie prac badawczo-rozwojowych w obszarze bezpieczeństwa sztucznej inteligencji i ich promocji,

h) wypracowanie z partnerami (polskimi i międzynarodowymi) narzędzi oraz prowadzenie stosowanych regularnych badań w kreowaniu polityk publicznych poświęconych wpływowi technologii AI na rynek pracy, gospodarkę, środowisko

oraz społeczeństwo uwzględniających zarówno potencjały, jak i zagrożenia, z uwzględnieniem sytuacji osób zagrożonych wykluczeniem,

i) utworzenie cyfrowych standardów struktur danych zgodnych ze standardami ISO i IEC dla wszystkich gałęzi gospodarki w celu budowania i uczenia modeli AI,

j) promowanie odpowiedzialnego i etycznego korzystania ze sztucznej inteligencji, także generatywnej, w sektorze publicznym i prywatnym. Opracowanie przypadków zastosowania i najlepszych praktyk w celu wykorzystania sztucznej inteligencji, także generatywnej w kluczowych branżach i usługach publicznych.

[box] Co z tego wynika: Rozwój AI zapewnią badania, zabezpieczenie przed cyberatakami oraz skoordynowany system finansowania. Stosowanie rozwiązań AI będzie bezpieczne oraz zgodne z przepisami i etyką.

Cel 4.2.2: Realizacja i finansowanie B+R oraz wdrożeń sztucznej inteligencji odbywa się w sposób efektywny i transparentny

Co umożliwi realizację celu:

a) stworzenie i zarządzanie mechanizmem koordynacji obecnych funduszy, konkursów i sposobów ich realizacji, aby uniknąć duplikacji działań i nieefektywnego wydatkowania środków inwestycyjnych wraz z koniecznością centralizowania agendy badawczej, rozwojowej oraz wdrożeniowej,

b) priorytetyzacja w finansowaniu komercjalizacji i wykorzystania technologii sztucznej inteligencji przez startupy, administrację publiczną, MŚP, duże przedsiębiorstwa oraz organizacje pozarządowe,

c) utworzenie jednego miejsca dostępu do informacji o wszystkich źródłach finansowania projektów AI, w którym będzie możliwość znalezienia najbardziej odpowiedniego dla projektu funduszu,

d) wsparcie MŚP we wdrożeniu AI przez dostęp do tanich usług doradczych oraz podnoszenie zarówno podstawowych kompetencji w zakresie AI, jak i kompetencji cyfrowych powiązanych z AI w przedsiębiorstwach i sektorze publicznym. Powinno ono obejmować wspieranie programów, które pomagają wdrażać założenia edukacji ustawicznej, w tym szkolenia zawodowe w zakresie AI i programy podnoszenia kwalifikacji dla pracowników w celu zdobycia stosowanych umiejętności w zakresie AI w ich konkretnych sektorach,

e) zapewnienie 50% finansowania krajowego dla projektów związanych ze sztuczną inteligencją współfinansowanych z funduszy unijnych,

f) opracowanie i realizacja projektów AI o największym potencjale dla rozwoju gospodarczego i technologicznego oraz dobrostanu społecznego w Polsce, w oparciu o wyznaczone obszary priorytetowe,

g) wdrożenie i upowszechnienie polskich dużych modeli językowych w modelu open-source, z typem licencji pozwalającej na ich wykorzystanie na rynku oraz dalsze udoskonalanie.

Cel 4.2.3: Zapewnienie odpowiedniej infrastruktury obliczeniowej i zasobów danych ułatwiających rozwój sztucznej inteligencji w integracji z innymi technologiami przełomowymi

Co umożliwi realizację celu:

a) dostarczenie ogólnodostępnej zdecentralizowanej mocy obliczeniowej na potrzeby realizacji projektów sztucznej inteligencji, w tym przez rozszerzanie i promowanie inicjatyw takich jak PLGrid i zintegrowanego ekosystemu infrastruktury,

b) zwiększenie transparentności procesu dostępu do mocy obliczeniowej w ramach ekosystemu infrastruktury dla celów naukowych i komercyjnych,

c) wsparcie centralnych rozwiązań umożliwiających udostępnianie danych językowych dla konkretnych rozwiązań AI, oznakowanych i opisanych pod kątem ich jakości. Wsparcie ekosystemu otwartych danych wielu typów oraz budowanie modeli i zbiorów danych na zasadzie struktury PPP w szybko postępującym ekosystemie AI pozwoli na efektywne zarządzanie innowacją,

d) ułatwienie przedsiębiorstwom i ośrodkom naukowym dostępu do zbiorów danych do testowania i rozwijania algorytmów AI,

e) określenie standardu wytwarzania danych zasilających systemy sztucznej inteligencji zgodnie z interoperacyjnością, zasadami etycznymi oraz prawami człowieka zgodnymi z unijnymi i międzynarodowymi standardami,

f) aktywny udział polskich reprezentantów w pracach nad międzynarodowymi standardami związanymi z AI, ICT, cyberbezpieczeństwem czy też opracowaniem struktur danych.

4.3 Inne technologie przełomowe

Diagnoza – jak jest?

Technologie przełomowe w transformacji cyfrowej (niezależnie od wyodrębnionego osobno obszaru sztucznej inteligencji) to m.in. technologie kwantowe, przetwarzanie brzegowe[126], XR i blockchain, technologie kosmiczne. Wśród obserwowanych trendów znajduje się również rozwijająca się ekonomia światów wirtualnych[127], której znaczenie będzie wymagać monitorowania i potencjalnych działań w przyszłości. Niezbędna lub oczekiwana interwencja państwa warunkuje zarówno w wymiarze polskim, jak i europejskim powodzenie szansy utrzymania strategicznej autonomii gospodarki i ograniczanie ryzyka zależności technologicznej od podmiotów zagranicznych. Zastosowanie różnych mechanizmów wsparcia inwestycji przemysłowych, sektora badań i rozwoju, ułatwienia dla startupów, inwestowanie w osiąganie twardych umiejętności w procesie kształcenia zawodowego, a także wdrażanie zastosowań technologii przełomowych w sektorze publicznym ma sprzyjać lokalizacji przedsięwzięć technologicznych w Polsce. W przypadku najważniejszych trendów technologicznych działania rozwojowe są programowane na poziomie UE. Polska angażuje się aktywnie w te przedsięwzięcia w projektach międzynarodowych, dających możliwość osiągania ekonomii skali niezbędną w konkurencji globalnej, zarówno pod kątem efektywności łańcucha dostaw, jak i wprowadzania na rynek praktycznych zastosowań.

Widać to w obszarze technologii kwantowych, w którym polskie środowisko zbudowało silne kompetencje naukowo-badawcze. Polska jest bowiem sygnatariuszem Europejskiej Deklaracji w sprawie technologii kwantowych i przystąpiła do Grupy Koordynacyjnej ds. Technologii Kwantowych. Niektóre już realizowane projekty, jak sieć komunikacji kwantowej EuroQCI (European Quantum Communication Infrastructure) w światłowodowej części naziemnej i segmencie satelitarnym czy budowa w Polsce komputera kwantowego w ramach europejskiej infrastruktury EuroQCS nie miałyby szansy powodzenia bez współpracy wielu państw. Wyzwania wciąż obejmują zastosowania, metrologię (sensory), kryptografię postkwantową czy produkcję mikroprocesorów ery postkwantowej.

Zwiększenie liczby węzłów w systemach przetwarzania brzegowego stało się jednym z celów polityki UE do 2030 r., dostarczających rynkowi bodźców do optymalizacji sieci przetwarzania danych. Co do zasady infrastruktura sieci przetwarzania danych jest obecnie

[126] Zgodnie z założeniami programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. przetwarzanie brzegowe to wykorzystanie zdolności węzłów brzegowych w zakresie rozproszonego przetwarzania danych. Są podłączone do sieci i zlokalizowane blisko fizycznego punktu końcowego lub w fizycznym punkcie końcowym, gdzie generowane są dane. Ich zdolności umożliwiają obliczenia rozproszone i przechowywanie rozproszone na potrzeby przetwarzania danych charakteryzującego się niskim opóźnieniem.

[127] Światy wirtualne wcześniej określane jako metaverse to trwałe środowiska immersyjne bazujące na technologiach takich jak 3D i rzeczywistość rozbudowana, które umożliwiają łączenie światów fizycznych i cyfrowych w czasie rzeczywistym do wielu różnych celów, m.in. na potrzeby projektowania, przeprowadzania symulacji, prowadzenia współpracy, uczenia się, odbywania spotkań towarzyskich, przeprowadzania transakcji lub zapewniania rozrywki;
komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Inicjatywa UE w sprawie technologii Web 4.0 i światów wirtualnych: dobra pozycja wyjściowa na drodze ku kolejnej transformacji technologicznej
(COM/2023/442 final) (https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52023DC0442).

budowana i utrzymywana głównie przez sektor prywatny, ale aspiracje planów rozwoju systemów AI, IoT, smart cities, sieci 5G nie zawsze idą w parze z planami inwestycji prywatnych. Zapewnienie energooszczędnego rozwoju i cyberbezpieczeństwa ma uzasadnienie w polityce publicznej.

Polska od 2018 r. uczestniczy w Europejskim Porozumieniu Blockchain. W 2024 r. budowana w ramach tego porozumienia europejska sieć blockchain EBSI została przekazana do EUROPEUM-EDIC, nowego podmiotu utworzonego z udziałem Polski w nowych ramach prawnych dla projektów wielokrajowych. Również w tym obszarze współpraca europejska daje okazję do wdrażania wielkoskalowych projektów zastosowań technologii przełomowych w usługach sektora publicznego, które będą katalizować wdrożenia w innych dziedzinach.

Kluczowy dla rozwoju gospodarki cyfrowej przemysł półprzewodnikowy jest w Polsce rozwinięty w niewielkim stopniu – obecnie w Polsce nie prowadzi się masowej produkcji półprzewodników. Jest ona realizowana w skali pilotażowej, co najwyżej małoseryjnej. Są to głównie półprzewodniki do zastosowań specjalnych produkowane w sieci Łukasiewicz – Instytucie Mikroelektroniki i Fotoniki. Polską specyfiką jest także mała liczebność wykwalifikowanych kadr, co rodzi obawy branży o ich odejście z polskich firm i ośrodków naukowych w sytuacji, gdy w Polsce pojawi się zagraniczny podmiot z dużą inwestycją w tym obszarze. Działalność dydaktyczna skoncentrowana jest w wąskiej grupie ośrodków akademickich takich jak Politechnika Warszawska czy Akademia Górniczo-Hutnicza; widoczne są też obiecujące projekty współprowadzone przez Politechnikę Poznańską. Okazją na nadchodzące lata jest jednak dostrzeżenie wagi tematu na poziomie unijnym, wyrażone przez przyjęcie Aktu w Sprawie Chipów[128] czy dążenie Unii do osiągnięcia poziomu 20% światowej produkcji półprzewodników w 2030 r. Odnotować trzeba również powstanie Krajowych Ram Wspierania Strategicznych Inwestycji Półprzewodnikowych[129] – programu, który ma zapewniać wsparcie lokowania w Polsce kosztownych, zaawansowanych zakładów produkcyjnych.

Krajowy rozwój technologii przełomowych, od AI po technologie kosmiczne oraz oparcie na nich rozwoju polskiej gospodarki, zależeć będzie w znacznym stopniu od bezpiecznego dostępu do wysokiej jakości mocy obliczeniowych. Skala wzrostu rynku AI czy IoT sprawia, że tempo wzrostu podaży usług przetwarzania w centrach danych w Polsce może być niewystarczające wobec nadchodzących potrzeb. Rozwój tak znaczącej dla funkcjonowania gospodarki infrastruktury na własnym terytorium ma więc dla państwa znaczenie strategiczne.

[128] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1781 z dnia 13 września 2023 r. w sprawie ustanowienia ram dotyczących środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników oraz zmiany rozporządzenia (UE) 2021/694 (akt w sprawie czipów) (Dz. Urz. UE L 229 z 18.09.2023, str. 1).
[129] Uchwała nr 239 Rady Ministrów z dnia 8 grudnia 2023 r. w sprawie ustanowienia rządowego programu pod nazwą "Krajowe Ramy Wspierania Strategicznych Inwestycji Półprzewodnikowych" (M.P. poz. 1419).

Cel 4.3.1: Rozbudowa ekosystemu badań i kompetencji wspiera rozwój w obszarze technologii przełomowych

Co umożliwi realizację celu:

a) stworzenie programu wieloletniego wspierania rozwoju technologii przełomowych w celu koordynacji agendy badawczej, konsolidacji wysiłków i zasobów oraz wyznaczenia wysokopoziomowych kierunków działań na najbliższe lata. Program będzie elastyczny i będzie umożliwiał dostosowanie do zmian technologicznych. Program umożliwi stabilizację pracy naukowej i finansowania interdyscyplinarnych zespołów badawczych. Musi zarazem stawiać na wysokojakościową współpracę międzynarodową i dostęp do najlepszego światowego know-how,

b) uspójnienie zarządzania agendą badawczą dookoła technologii przełomowych we współpracy ze środowiskiem naukowym, biznesowym i akademickim,

c) nawiązanie partnerskich relacji z wiodącymi światowymi ośrodkami badań w zakresie technologii przełomowych.

Cel 4.3.2: Technologie kwantowe są wykorzystywane w kluczowych gałęziach gospodarki i obszarach działalności państwa

Co umożliwi realizację celu:

a) identyfikowanie kluczowych obszarów gospodarki, gdzie technologia kwantowa ma potencjał zwiększenia produktywności, bezpieczeństwa i wydajności, a następnie wsparcie zastosowania technologii kwantowych w tych obszarach,

b) przygotowanie i przyjęcie krajowego dokumentu strategicznego dla rozwoju technologii kwantowych,

c) organizacja odpowiedniego systemu edukacji i budowy kompetencji (m.in. z wykorzystaniem laboratoriów i eksperymentów w obszarze technologii kwantowych) oraz wsparcie prac badawczo-rozwojowych w obszarze technologii kwantowych, np. przez zapewnienie dostępu do know-how i infrastruktury kwantowej ośrodkom akademickim i biznesowi,

d) wsparcie przedsiębiorczości opartej na produktach/usługach związanych z technologiami kwantowymi (np. akcelerator startupów, konkursy),

e) opracowanie krajowych rozwiązań i wykorzystanie metrologii kwantowej w gospodarce, np. w przemyśle półprzewodnikowym, sektorze kosmicznym, obronności, przy badaniu i lokalizacji złóż surowców naturalnych oraz standaryzacji czasu, częstotliwości i innych wielkości fizycznych,

f) skoordynowanie działań mających na celu zapewnienie rozwoju technologii kwantowych na poziomie polskim i międzynarodowym, w tym w zakresie mechanizmów finansowania,

g) zapewnienie 50% finansowania krajowego dla projektów związanych z technologiami kwantowymi współfinansowanych z funduszy unijnych.

[box] Co z tego wynika: Wykorzystamy technologie kwantowe w najważniejszych obszarach działania państwa, zwiększając ich bezpieczeństwo, produktywność i wydajność.

Cel 4.3.3: Technologie internetu rzeczy są wykorzystywane w kluczowych sektorach gospodarki i w ośrodkach miejskich i wiejskich

Co umożliwi realizację celu:

a) opomiarowanie głównych szlaków komunikacyjnych w celu monitorowania ruchu w czasie rzeczywistym, a także zapewnienie danych on-line w zakresie dostępności infrastruktury paliw alternatywnych, co przełoży się na optymalizację i zmniejszoną emisyjność transportu,

b) budowa farm demonstracyjnych zawierających najnowsze rozwiązania internetu rzeczy (IoT), na przykład czujniki wilgotności gleby w każdym województwie, w celu edukacji i wdrożenia IoT w sektorze rolniczym,

c) wspieranie rozwoju i wdrażania rozproszonej infrastruktury węzłów przetwarzania brzegowego w celu efektywnego przetwarzania danych pochodzących z urządzeń IoT,

d) zbudowanie albo wdrożenie platformy smart city w modelu open source dostępnej dla mniejszych miasteczek i wsi w celu popularyzacji rozwiązań inteligentnych miast i wsi w mniej skomunikowanych regionach, przy zapewnieniu ochrony prywatności i danych osobowych mieszkańców,

e) zapewnienie interoperacyjności i standardów wymiany danych w systemach IoT, w tym na rzecz wykorzystania tych danych do rozwijania zasobów statystyki publicznej,

f) rozbudowa sieci bieżącego i automatycznego monitoringu środowiskowego, tworzonego w oparciu o technologie IoT wykorzystujące bardzo efektywne energetycznie lub autonomiczne systemy naziemnej transmisji danych dalekiego zasięgu i satelitarnej. Prowadzenie analiz i predykcji bazujących na dostępnych danych.

[box] Co z tego wynika: Wsie i miasta będą miały dostęp do wiedzy i rozwiązań smart city. Wykorzystanie technologii IoT usprawni działanie najważniejszych sektorów gospodarki m.in. umożliwi monitorowanie jakości wód i powietrza oraz monitorowanie ruchu i optymalizację transportu.

Cel 4.3.4: Polska rozwija sektor półprzewodników dzięki zwiększonym inwestycjom

Co umożliwi realizację celu:

a) utworzenie i wdrożenie szczegółowej i spójnej polityki rozwoju sektora półprzewodników w Polsce, uwzględniającej kontekst międzynarodowy (w tym współpracę z partnerami w globalnych łańcuchach wartości i wsparcie unijne), zidentyfikowane bariery rozwoju i istniejące obszary specjalizacji takie jak projektowanie układów, fotonika scalona i nowe materiały,

b) wsparcie rozbudowy polskiego ekosystemu sektora półprzewodników – z uwzględnieniem podmiotów ze wszystkich etapów łańcucha wartości – oraz włączania polskich firm i jednostek badawczych w rozwijający się europejski łańcuch wartości sektora półprzewodników,

c) zapewnienie stałej współpracy między resortami i instytucjami kluczowymi dla rozwoju sektora półprzewodnikowego w celu zapewnienia synergii inwestycji, również w kontekście europejskim) oraz budowy korzystnych warunków dla inwestorów (m.in. uproszczenia procedur) i przyciągania inwestycji zagranicznych,

d) utworzenie polskiego centrum kompetencji do spraw półprzewodników,

e) zwiększenie dostępu polskich firm (zwłaszcza MŚP) do platform projektowych i narzędzi wspierających rozwój oprogramowania do projektowania układów scalonych - także open source - oraz do pilotażowych linii produkcyjnych,

f) długofalowe utrzymanie programu Krajowe Ramy Wspierania Strategicznych Inwestycji Półprzewodnikowych i zwiększenie elastyczności jego zasad,

g) wsparcie rozwoju pilotażowych i małoskalowych linii produkcyjnych w kraju, w tym utworzenie pierwszej krajowej linii pilotażowej,

h) utworzenie parku technologicznego dla sektora półprzewodników, zapewniającego zintegrowaną przestrzeń do wspólnych prac badawczo-rozwojowych, testowania i wdrażania produkcji oraz kształcenia kadr.

Cel 4.3.5: Technologie blockchain są wykorzystywane i rozwijane, również w wymiarze europejskim

Co umożliwi realizację celu:

a) stworzenie ram prawnych wdrażania technologii blockchain, które zapewnią bezpieczeństwo i zgodność z przepisami krajowymi oraz unijnymi,

b) skoncentrowanie na zwiększaniu przejrzystości i rozliczalności wybranych procesów w administracji publicznej i gospodarce za pomocą technologii blockchain. Technologia ta może ograniczać pole do nadużyć i manipulacji, m.in. przez wykorzystanie takich rozwiązań jak weryfikowalne poświadczenia, suwerenna tożsamość (ang. Self Sovereign Identity, SSI), europejski portfel tożsamości cyfrowej, e-weksel, pieczęć elektroniczna, trwały nośnik oraz innych instrumentów,

c) rozwijanie zdolności europejskiej sieci EBSI i zastosowań blockchain w usługach sektora publicznego przez współtworzony przez Polskę wielokrajowy podmiot EUROPEUM EDIC. Wypracowanie dobrych praktyk we wszystkich testowanych i wdrażanych zastosowaniach technologii blockchain w usługach transgranicznych. Standaryzowanie procesów w usługach, interoperacyjności w rozproszonych systemach rejestrów i usługodawców usług, z zachowaniem ich lokalnej suwerenności, sprawiedliwego dostępu i możliwości użycia w ramach ekosystemu europejskiego,

d) integracja zastosowań technologii blockchain w infrastrukturze rynków finansowych i kapitałowych, obejmująca możliwość tokenizacji różnych kategorii papierów wartościowych oraz różnych kategorii praw posiadania, a także systemów płatności, rejestrów akcji,

e) wzmacnianie cyberbezpieczeństwa technologii blockchain, również w odniesieniu do kryptografii postkwantowej, a także wykorzystywanie, technologii blockchain do rozwiązywania niektórych problemów z cyberbezpieczeństwem, np. w systemach AI.

[box] Co z tego wynika: Zwiększymy zastosowanie technologii blockchain, również w wymiarze europejskim, przy jednoczesnym zapewnieniu dobrych praktyk, standardów i wzmocnieniu cyberbezpieczeństwa.

Cel 4.3.6: Sieć centrów przetwarzania danych zaspokaja potrzeby wewnętrzne i umożliwia obsługę rynków zagranicznych.

Co umożliwi realizację celu:

a) wytworzenie spójnego i przejrzystego środowiska prawnego, standaryzacyjnego i certyfikacyjnego mającego zachęcać do inwestycji w centra przetwarzania danych, w tym wprowadzenie uproszczeń i ułatwień procesów związanych z budową i lokalizacją centrów, dotyczących przyłączania do sieci energetycznych czy też dostępu do źródeł energii,

b) koordynacja planowania budowy centrów przetwarzania danych z planowaniem dotyczącym rozwoju sieci telekomunikacyjnych, energetycznych i pozostałej powiązanej infrastruktury, uwzględnienie w planowaniu potrzeb w zakresie projektów wymagających przetwarzania brzegowego,

c) uwzględnienie budowy centrów przetwarzania danych w ramach programów i regulacji dotyczących zielonej energii i optymalizacji energetycznej (np. OZE, energetyka jądrowa, wykorzystania obiegu zamkniętego czy optymalizacji chłodzenia).

4.4 Technologie kosmiczne

Diagnoza – jak jest?

Mimo, iż przemysł kosmiczny wykorzystuje technologie cyfrowe i jest gotowy na wprowadzanie nowych, w dalszym ciągu napotyka problemy we współpracy między uczestnikami zaawansowanych projektów. Domena kosmiczna musi wdrażać cyfryzację w kontekście ograniczonym, wynikającym z procesów, organizacji i doświadczenia technologicznego. Polega to na zapewnieniu realizacji potrzeb interoperacyjności wszystkich narzędzi, między dyscyplinami, w całym cyklu życia i w całym łańcuchu dostaw. W tym kontekście Europejska Agencja Kosmiczna (ESA) w swoim dokumencie „ESA AGENDA 2025: Make space for Europe" dokonała harmonizacji niezbędnych przedsięwzięć wskazując społeczności sektora kosmicznego, a w szczególności Delegacjom Państw Członkowskich ESA, kierunki rozwoju i wdrażania wspólnie z przemysłem, złożonych i ambitnych misji i programów kosmicznych. ESA zapewniła również, że dokona pełnej cyfryzacji zarządzania projektami, umożliwiając rozwój możliwych do powielania kopii cyfrowych (digital twins), zarówno przez wykorzystanie inżynierii systemów opartych na modelach, jak i zamówień publicznych i finansów, osiągając pełną kompatybilność cyfrową z przemysłem.

Polska, podobnie jak inne państwa, traktuje rozwój rodzimego sektora kosmicznego jako zasób strategiczny i biznesowy, który zyskuje coraz większe znaczenie dla gospodarki krajowej i jest motorem coraz szerszej współpracy międzynarodowej.

Wstąpienie Polski do ESA umożliwiło jeszcze większy postęp w rozwoju technologii kosmicznych i technik satelitarnych przez polski przemysł, a zwiększenie poziomu inwestycji z budżetu państwa, zarówno w programy opcjonalne, jak i obowiązkowe, umożliwia zapewnienie administracji państwowej danych satelitarnych, wsparcie polskich podmiotów w zakresie pozyskiwania doświadczenia kosmicznego, inwestycje w specjalistyczną infrastrukturę laboratoryjną i testową, rozwój zdolności w wybranych obszarach technologii kosmicznych, które mają wpływ na zwiększenie szeroko rozumianego bezpieczeństwa naszego kraju.

Ale członkostwo Polski, udział polskich firm kosmicznych w projektach ESA, to także ścisła realizacja wytycznych, wynikających z przepisów, norm i innych dokumentów obejmujących m.in. konieczność cyfryzacji w dziedzinie inżynierii. Dzięki temu polskie podmioty zdobywają nieocenione doświadczenie wymagane w sektorze kosmicznym. Pozwala ono inżynierom systemów i zespołom projektowym opanować złożoność systemu kosmicznego, zrozumiale wyrażać koncepcję operacji, strukturyzować wymagania i śledzić je od projektowania i produkcji aż do testowania. Te praktyczne umiejętności wyraźnie wskazują, że Polska wpisuje się w cele cyfryzacji wskazane przez ESA, jednocześnie sprzyjając postępowi technologicznemu w kraju i przyczyniając się do zaspokajania potrzeb krajowych, jak

również zwiększaniu potencjału konkurencyjności polskiego przemysłu kosmicznego na rynkach globalnych.

Cel 4.4.1: Technologie obserwacji Ziemi są udoskonalane na potrzeby monitorowania środowiska i zarządzania katastrofami

Co umożliwi realizację celu:

a) stworzenie systemu łączności satelitarnej zapewniającej łączność w czasie rzeczywistym poza terytorium Polski,

b) stworzenie scentralizowanej platformy do agregowania danych z różnych misji kosmicznych, satelitów i czujników,

c) wdrażanie zaawansowanych narzędzi analitycznych wykorzystujących AI do przetwarzania i interpretacji danych w celu prognozowania i wspierania decyzji w czasie rzeczywistym np. w zarządzaniu kryzysowym,

d) wykorzystywanie technologii cyfrowych bliźniaków satelitów w celu optymalizacji ich działania, predykcji usterek oraz zarządzania cyklem życia,

e) rozwój krajowych narzędzi i systemów monitorowania i alarmowania o zakłóceniach systemów nawigacji satelitarnej GNSS (GPS, Galileo), w szczególności pod kątem jammingu[130], spoofingu i meaconingu[131]. Zjawiska te stanowią duże zagrożenie dla wielu segmentów gospodarki czy państwa, wymagających niezawodnych i wiarygodnych danych lokalizacyjnych, a w ostatnich kilku latach ich skala nasiliła się w sposób bezprecedensowy, zarówno na obszarze Polski, jak i w krajach sąsiednich.

[box] Co z tego wynika: Obserwacja Ziemi, w tym monitorowanie środowiska i zarządzanie kryzysowe, jest wspierana przez wykorzystywanie technologii cyfrowych, które umożliwiają m.in. agregowanie danych oraz wykorzystywanie AI w narzędziach analitycznych.

[130] Działanie polegające na celowym zakłócaniu sygnałów systemu nawigacji satelitarnej.
[131] Działanie polegające na przechwytywaniu i retransmisji sygnałów nawigacyjnych

Cel 4.4.2: Infrastruktura kosmiczna jest bezpieczna

Co umożliwi realizację celu:

a) wdrożenie kompleksowych środków cyberbezpieczeństwa w celu ochrony systemów kosmicznych i danych przed zagrożeniami, zapewniając ciągłość operacyjną,

b) rozwój i wdrożenie systemów komunikacji kwantowej dla bezpiecznej transmisji danych,

c) opracowywanie i wdrażanie zaawansowanych systemów zarządzania ruchem kosmicznym - technologii śledzenia śmieci kosmicznych i kolizji satelitów oraz zarządzania nimi; udział w programach i projektach UE i ESA w tym obszarze,

d) wsparcie rozwoju AI, automatyki i robotyki na potrzeby autonomicznych operacji satelitarnych, wykrywania anomalii, serwisowania, napraw i montażu na orbicie,

e) opracowywanie, rozwój i wdrażanie narzędzi informatycznych dla sterowania pojazdami kosmicznymi i systemami ich wynoszenia oraz zapewnienia bezpieczeństwa lotu i optymalizacji zużycia paliwa,

f) rozwój oprogramowania do kalkulacji manewrów pojazdów kosmicznych: liczenie trajektorii lotu rakiety, strefy upadku, modelowanie aerodynamiczne i gazodynamiczne, specjalne moduły do podwójnego zastosowania, umożliwiające również wykonywanie zaawansowanych obliczeń, w tym z wykorzystaniem AI do przetwarzania danych bezpośrednio na pokładzie satelitów.

[box] Co z tego wynika: Zapewnimy ciągłość operacyjną systemów kosmicznych i zabezpieczymy je przed cyberzagrożeniami, wykorzystując najnowsze technologie cyfrowe.

4.5 Finansowanie i wsparcie innowacji

Diagnoza – jak jest?

W 2023 r. Polska zajęła dalekie, 17. miejsce w UE oraz 20. w Europie pod względem kapitału zainwestowanego w startupy na rożnych fazach wzrostu. Mimo zwiększenia skali finansowania nieznacznie spadł procentowy udział Polski w całkowitym kapitale zainwestowanym przez fundusze venture capital/private equity (VC/PE) w Europie w ciągu ostatnich trzech lat (2021-2023) w stosunku do trzech poprzednich lat (2018-2020). Największe wzrosty odnotowały Holandia, Norwegia, Estonia, Austria i Niemcy[132]. W 2023 r. Warszawa zajęła wysokie 3. miejsce wśród miast z regionu Europy Środkowo-Wschodniej pod względem nominalnej wartości zainwestowanego kapitału, ale sam region nadal pozostaje na poziomie o 70% niższym np. w stosunku do regionu DACH (Niemcy, Austria, Szwajcaria), pod względem procentowego udziału finansowania startupów w PKB[133]. W ostatnich latach wzrosła w Polsce skala finansowania startupów na etapie pre-seed (przed-zalążkowym) oraz seed (zalążkowym), jednak nadal występuje problem finansowania na kolejnych etapach rozwoju.

Na szczeblu krajowym w ostatnich latach podjęto szereg działań mających zwiększyć finansowanie, do których można przede wszystkim zaliczyć wzrost aktywności Polskiego Funduszu Rozwoju. Odegrał on kluczową rolę w zwiększeniu finansowania, wspierając 80 funduszy w formule funduszy poprzez PFR Ventures[134]. Działalność PFR przyciągnęła do Polski szereg zagranicznych funduszy VC. Zwrócić uwagę należy także na utworzenie funduszu PFR Deep Tech. Jest to pozytywny sygnał zarówno ze względu na samo pojawienie się nowego instrumentu finansowego (mimo jego relatywnie niewielkiej skali w porównaniu do inwestycji zachodnich), jak i ze względu na podkreślenie znaczenia obszaru deep tech, charakteryzującego się dużym komponentem naukowym w tworzonych produktach. To szczególnie istotne ze względu na znaczny potencjał przełomów technologicznych generowanych w tym obszarze (nie zawsze, lecz często związanych z cyfryzacją) i dawaną m.in. przez AI perspektywę skrócenia (znacznie dłuższego niż w „tradycyjnych" startupach[135]) czasu, jaki zajmuje w nim osiągnięcie gotowości rynkowej.

Do zdiagnozowanych problemów z obszaru finansowania zaliczyć można brak wystarczających zachęt i szerokiego spektrum dopuszczalnych mechanizmów do finansowania startupów przez fundusze emerytalne, brak efektywnej współpracy banków komercyjnych z BGK, szereg barier prawnych w sektorze bankowym w zakresie finansowania startupów przez instrumenty dłużne czy niedostatecznie skuteczne działania akceleratorów finansowanych ze środków publicznych. Dane wskazują na stosunkowo

[132] State of European Tech 2023, Atomico, https://www.investeurope.eu/media/7424/atomico-state-of-european-tech-report-2023.pdf.
[133] Central and Eastern European startups 2024, Dealroom, https://dealroom.co/reports/central-and-eastern-european-startups-2024.
[134] https://pfrventures.pl/; dane z 13 maja 2025 r.
[135] Deep Tech Decoded: A strategic investor's guide, Hello Tomorrow and Deepbright Ventures, https://hello-tomorrow.org/deep-tech-decoded/.

wysoką liczbę startupów w Polsce, jednak wynika to z faktu, że polska gospodarka jest jedną z największych w UE.

Pod względem liczby wszystkich startupów, również tych bez zapewnionego finansowania, Polska zajmuje w UE 9. miejsce oraz 11. w Europie. Jednak pod względem liczby startupów jakie uzyskały finansowanie przypadających na mieszkańca, Polska jest dopiero 23. w UE. Podobnie jest w przypadku tzw. jednorożców (innowacyjnych firm o wycenie powyżej 1 mld USD) – nominalnie Polska zajmuje 9. miejsce, ale per capita – już 22[136].

W ostatnich pięciu latach udział regionu EŚW w całkowitej wartości startupów w Europie wzrósł z 4,9% w roku 2019 do 5,7% w roku 2024. Pod względem wzrostu całkowitej wartości startupów za okres ostatnich pięciu lat Polska zajęła 6. miejsce w regionie EŚW (wzrost o 240%, w porównaniu do 740% w Chorwacji). Pod względem udziału Polski w całkowitej wartości TOP100 największych spółek technologicznych regionu EŚW Polska zajmuje 1. miejsce z udziałem 38%[137].

Porównując polski ekosystem startupowy z ekosystemami wiodących krajów w UE można zaobserwować szereg różnic, do których można zaliczyć: brak kompleksowego programu ułatwiającego współpracę spółek skarbu państwa (SSP) ze startupami, niedostatecznie efektywne wsparcie dla rozwoju ekosystemu innowacji i niedostatecznie skuteczną promocję Polski jako centrum innowacji. Reprezentanci polskiego ekosystemu zwracają także uwagę na brak spójnego wsparcia na wszystkich etapach rozwoju startupu, jednego miejsca zbierającego informacje o programach wsparcia dla startupów czy brak ułatwień dla powoływania i prowadzenia celowych wehikułów inwestycyjnych (SPV) umożliwiających inwestorom finansowanie startupów poprzez projekty inwestycyjne.

[136] State of European Tech 2023, Atomico, https://www.investeurope.eu/media/7424/atomico-state-of-european-tech-report-2023.pdf.
[137] Central and Eastern European startups 2024, Dealroom, https://dealroom.co/reports/central-and-eastern-european-startups-2024.

Cel 4.5.1: Istnieje zintegrowany i sprawny system finansowania dla startupów i scale-upów

Co umożliwi realizację celu:

a) zintegrowanie środowiska finansowego (fundusze VC, BGK, GPW, banki prywatne) w celu intensyfikacji współpracy oraz wypracowania rozwiązań na rzecz mobilizacji kapitału dla startupów,

b) wprowadzenie zachęt fiskalnych dla krajowych i zagranicznych inwestorów instytucjonalnych i prywatnych (w tym dużych przedsiębiorstw) z tytułu inwestycji w startupy,

c) usprawnienie ekosystemu akceleratorów finansowanych ze środków publicznych, we współpracy z prywatnymi inwestorami i poszukiwanie możliwości koinwestycji z wiodącymi światowymi akceleratorami,

d) rozwijanie programu finansowania rozwiązań deep tech umożliwiający budowanie sektora w Polsce i finansowanie start-upów i scale-upów,

e) wypracowanie mechanizmów ograniczających straty inwestorów indywidualnych w odniesieniu do inwestycji w startupy,

f) umożliwienie funduszom emerytalnym i planom długoterminowego oszczędzania przeznaczenia części zarządzanych środków na inwestycje w fundusze VC/PE z Europy Środkowo-Wschodniej, poddane uprzednio odpowiedniej certyfikacji wraz z wprowadzeniem mechanizmów częściowego mitygowania ryzyka inwestycji,

g) stworzenie mechanizmów premiujących rozwój i skalowanie startupów z siedzibą w Polsce, w tym zachęt dla założycieli do utrzymywania praw własności intelektualnej oraz centrów decyzyjnych w kraju, w trakcie ekspansji zagranicznej.

[box] Co z tego wynika: Startupy i scale-upy będą miały łatwiejszy dostęp do kapitału na rozwój.

Cel 4.5.2: Startupy i scale-upy rozwijają się bez nadmiernych barier regulacyjnych

Co umożliwi realizację celu:

a) identyfikacja i zniesienie barier prawnych dla wzrostu startupów i ich skalowania,

b) umożliwienie tworzenia celowych wehikułów inwestycyjnych (SPV) do inwestycji w fundusze lub startupy,

c) dostosowanie procedur administracyjnych w celu zwiększenia zainteresowania prowadzeniem innowacyjnych firm i inwestowania w Polsce przez podmioty z zagranicy,

d) wypracowanie rozwiązań prawnych przyciągających talenty z zagranicy,

e) wprowadzenie celowanych piaskownic regulacyjnych.

[box] Co z tego wynika: Ułatwimy działalność startupów i scale-upów zmieniając prawo i dostosowując procedury administracyjne do ich specyfiki.

Cel 4.5.3: Państwo zwiększa pulę talentów i liczebność podmiotów ekosystemu w Polsce

Co umożliwi realizację celu:

a) wprowadzenie, w ścisłej współpracy z reprezentatywnymi organizacjami sektora technologicznego, systemowych rozwiązań na rzecz mapowania i integracji podmiotów ekosystemu startupowego oraz potencjału jego rozwoju i powiązania z ośrodkami naukowymi,

b) uznanie tzw. cyfrowych nomadów ICT pochodzących spoza UE za preferowanych z punktu widzenia polityki migracyjnej; stworzenie programu przedstawiającego im zalety stałego osiedlenia się w Polsce,

c) rozwinięcie wsparcia w administracji publicznej dla pewnej puli zagranicznych talentów ICT przed przybyciem do Polski we współpracy z agencjami pracy i wspierającymi relokacje. Jego zakres obejmować będzie procedury administracyjne i wsparcie logistyczne,

d) wzmocnienie innowacyjności w regionach i między regionami przez ekosystemy innowacji łączące przedstawicieli poczwórnej helisy (tj. biznesu, nauki, administracji publicznej oraz przedstawicieli obywateli).

Cel 4.5.4: Skalowanie startupów jest skuteczniej wspierane przez państwo

Co umożliwi realizację celu:

a) wypracowanie kompleksowego programu współpracy i skalowania wdrożeń polskich startupów w Spółkach Skarbu Państwa (SSP) oraz administracji centralnej, obejmującego mechanizmy wymiany informacji, wsparcia administracyjnego i technicznego reprezentantów innowacyjnych firm,

b) wsparcie promocji polskich innowacji technologicznych przez wytworzenie dla nich jednej wspólnej marki,

c) stworzenie centrum wiedzy na temat wszelkich konkursów, naborów do inkubatorów, akceleratorów, o grantach i projektach z zakresu otwartych innowacji we współpracy z partnerami z regionu Europy Środkowo-Wschodniej,

d) stworzenie serii wydarzeń i konkursów pozwalających skalować polskie startupy i innowacje we współpracy z administracją publiczną i spółkami skarbu państwa,

e) wdrożenie instrumentów dedykowanych transferowi technologii cyfrowych z ośrodków akademickich do sektora przemysłu i usług, w tym wsparcie dla spółek typu spin-off oraz centrów kompetencji cyfrowych działających przy uczelniach.

4.6 Open source

Diagnoza – jak jest?

Polska jest państwem o silnym sektorze IT, który jednak w niewielkim stopniu wykorzystuje potencjał otwartego oprogramowania. Kluczowym wyzwaniem jest brak kompleksowych ram instytucjonalnych i strategicznych, które wspierałyby rozwój polskiego ekosystemu open source. Jako jedno z nielicznych państw UE, Polska nie posiada strategii rozwoju i wspierania otwartego oprogramowania; brak też centralnej jednostki mającej za zadanie wspierać jego adopcję w administracji publicznej[138]. Choć bowiem otwarte oprogramowanie jest komplementarne do rozwoju ekosystemu otwartych danych, które są w Polsce na wysokim poziomie, to administracja wykorzystuje je w ograniczonym stopniu.

Równocześnie, tworzenie i wykorzystywanie otwartego oprogramowania jest ważnym narzędziem pozwalającym zapewnić suwerenność cyfrową. Dzięki większej interoperacyjności pozwala zmniejszać zależność od określonego, komercyjnego oprogramowania; zwiększa przejrzystość i kontrolę nad wykorzystywanymi technologiami, jest też bardziej efektywne kosztowo. Otwarte oprogramowanie pozwala też budować powiązania między sektorem IT oraz różnorodnymi środowiskami rozwijającymi i korzystającymi z technologii. W ostatnich latach przykładem takiego podejścia jest rozwój polskich otwartych modeli językowych, a także zaangażowanie polskich programistów w rozwój otwartych narzędzi czy systemów operacyjnych.

[138] Blind, K.; Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., Schubert, T. (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, Final Study Report. Brussels, s. 226.

Cel 4.6.1: Polska administracja publiczna w większym stopniu wykorzystuje otwarte oprogramowanie oraz otwarte standardy technologiczne

Co umożliwi realizację celu:

a) utworzenie Biura Programów Otwartego Oprogramowania, jako podmiotu odpowiedzialnego za koordynację rozwoju i wdrażania otwartego oprogramowania w polskiej administracji publicznej, a także rozwoju kompetencji w tym zakresie,

b) inwentaryzacja aktualnego oraz planowanego wykorzystania otwartego oprogramowania w administracji publicznej oraz identyfikacja możliwości, braków, potrzeb, a także ryzyk związanych z jego stosowaniem,

c) opracowanie programu wdrażania otwartego oprogramowania i otwartych standardów technologicznych w polskiej administracji, obejmującego standardy wykorzystania oprogramowania oraz projekty pilotażowe,

d) określanie zasad prowadzenia przetargów na wdrożenia IT w administracji publicznej, które będą wykorzystywać, ale też w jasno określony i rozliczalny sposób wspierać wykorzystanie otwartego oprogramowania,

e) utworzenie repozytorium zweryfikowanego pod kątem bezpieczeństwa otwartego oprogramowania dla polskiej administracji,

f) wprowadzenie rekomendacji sprzyjających większej adopcji otwartego oprogramowania w administracji publicznej.

[box] Co z tego wynika: Zwiększymy wykorzystanie otwartego oprogramowania w administracji publicznej. Zapewnimy dostęp do oprogramowania i wsparcie przy wdrożeniu. Zapewnimy wsparcie dla wykorzystywanych projektów otwartego oprogramowania, aby mogły się rozwijać.

Cel 4.6.2: Polski ekosystem otwartego oprogramowania jest silniejszy

Co umożliwi realizację celu:

a) wprowadzenie instrumentu finansowania dla firm, organizacji oraz programistów na tworzenie otwartego oprogramowania, a także rozwiązań typu open hardware,

b) wsparcie rozwoju otwartych systemów sztucznej inteligencji oraz ich wdrażania w administracji publicznej,

c) wsparcie rozwoju otwartych protokołów zwiększających autonomię i bezpieczeństwo użytkowników platform internetowych (np. umożliwiającym im korzystanie z różnych algorytmów rekomendujących treści),

d) wsparcie rozwoju otwartych rozwiązań dla administracji samorządowej - połączone wsparcie dla lokalnych przedsiębiorstw oraz administracji samorządowej wdrażających oprogramowanie, wykorzystujących otwarte narzędzia i realizujących wspólne projekty,

e) promowanie polityk open source na rynku krajowym oraz międzynarodowym m.in. przez organizację konkursów na rozwiązania open source.

[box] Co z tego wynika: Firmy i programiści tworzący otwarte oprogramowanie otrzymają zwiększone finansowanie. Proces wdrażania otwartego oprogramowania i sprzętu będzie rozwijany i wspierany.

4.7 Cyfrowa i zielona transformacja

Diagnoza – jak jest?

Obecnie w Polsce realizowanie inicjatyw na rzecz zielonej i cyfrowej transformacji wynika głównie z unijnych wymogów regulacyjnych i wytycznych w zakresie finansowania projektów z funduszy europejskich, nie zaś z obranej przez państwo ambitnej strategii w zakresie tzw. "bliźniaczej przemiany". Zaproponowane w Krajowym planie do programu polityki „Droga ku cyfrowej dekadzie" działania w tym obszarze skupiają się przede wszystkim na tworzeniu sandboxów dla rozwiązań AI, uczestnictwie w inicjatywie Komisji Europejskiej Earth Destination, inwestycjach i wymogach związanych z wdrażaniem innowacji środowiskowych (przede wszystkim gospodarki obiegu zamkniętego). Dotychczas niewiele uwagi poświęcono także wpływowi państwowych rozwiązań cyfrowych na środowisko i zmiany klimatu. Równocześnie wiadome jest, że ślad węglowy generowany wskutek produkcji i użytkowania rozwiązań cyfrowych stale rośnie w Polsce i na świecie. Szacuje się, że globalne emisje sektora ICT wynoszą od 2,1% do 3,9%[139] i są większe niż te generowane przez przemysł lotniczy. Wyzwaniem pozostaje zwiększenie dostępności czystej i taniej energii dla rosnących potrzeb obywateli i przedsiębiorców korzystających z rozwiązań cyfrowych.

Niezbędne jest więc bardziej kompleksowe niż dotychczas podejście do cyfrowej i zielonej transformacji

oraz współpraca międzyresortowa, która obejmie wątki zarówno energochłonności narzędzi cyfrowych, potencjału technologii w walce ze zmianami klimatu i ograniczeniem emisji, jak również ekologii cyfrowej.

Wśród polskiego biznesu rośnie świadomość wpływu nowych technologii na środowisko i klimat. Zgodnie z ostatnimi danymi[140], ponad 64% firm z sektora ICT zwraca uwagę na kwestie takie jak zużycie energii czy możliwość łatwej wymiany części przy wyborze sprzętu lub dostawcy usług. Równocześnie brakuje systemów monitorowania wpływu technologii cyfrowych wykorzystywanych przez firmy na środowisko. Obowiązek raportowania kwestii związanych z ryzykiem klimatycznym, wynikający z dyrektywy ws. sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (tzw. CSRD – The Corporate Sustainability Reporting Directive[141]) na ten moment dotyczy jedynie największych jednostek zainteresowania publicznego. To natomiast może prowadzić do ograniczonego raportowania

[139] https://www.sciencedirect.com/science/article/pii/S2666389921001884.
[140] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_in_enterprises_and_the_environment.
[141] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2464 z dnia 14 grudnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 537/2014, dyrektywy 2004/109/WE, dyrektywy 2006/43/WE oraz dyrektywy 2013/34/UE w odniesieniu do sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (Dz. Urz. UE L 322 z 16.12.2022, str. 15, Dz. Urz. UE L 2025/794 z 16.04.2025, Dz. Urz. UE L 2025/90790 z 08.10.2025 oraz Dz. Urz. UE L 2026/470 z 26.02.2026).

bądź też greenwashingu (fałszywego przedstawiania produktów lub usług jako ekologicznych) w przypadku podmiotów mniejszych oraz tych nienotowanych na giełdzie. W zakresie certyfikacji, istnieją unijne systemy weryfikacji technologii, jak chociażby ETV[142] (Environmental Technology Verification – Program weryfikacji technologii środowiskowych Unii Europejskiej). Jednak odnoszą się one przede wszystkim do technologii środowiskowych (tj. mających na celu redukcję emisji gazów cieplarnianych, ograniczenie zużycia zasobów takich jak woda czy surowce) nie zaś do produktów sektora ICT, które w coraz większym stopniu odpowiadają za zużycie energii. Ponadto są one dobrowolne, co może stawiać pod znakiem zapytania ich skuteczność.

Pierwsze polskie badania[143] sugerują, że świadomość obywateli na temat ekologii cyfrowej jest niska.

Terminy takie jak “cyfrowy ślad węglowy” i “ekologia cyfrowa” są nadal mało rozpoznawalne wśród osób spoza sektora ICT. Znajomość pojęcia „cyfrowy ślad węglowy” zadeklarowało jedynie 19% osób niezwiązanych z branżą IT, natomiast termin „ekologia cyfrowa” był znany tylko 12% z nich. Choć wskaźniki te były nieco wyższe w grupie specjalistów IT, poziom świadomości wciąż pozostaje niski. Pojęcie „cyfrowy ślad węglowy” znało 25% pracowników branży IT, a termin “ekologia cyfrowa” - 23%.

[142] https://lifeproetv.eu/pl/strona-glowna/.
[143] https://blog.theprotocol.it/artykul/cyfrowa-ekologia-w-pracy-i-zyciu-polakow-raport-theprotocol.

Cel 4.7.1: Systemy energetyczne, w tym ciepłownicze, opierają się na innowacyjnych systemach zarządzania i optymalizacji

Co umożliwi realizację celu:

a) wzmacnianie cyberbezpieczeństwa oraz zapewnienie infrastruktury cyfrowej wspierającej innowacje, takie jak chociażby zaawansowane magazynowanie energii, sztuczna inteligencja w energetyce i urządzenia grid-edge, które pozwolą na integrację energii z OZE oraz z elektrowni jądrowych z obecnie funkcjonującym systemem energetycznym, sieciami dystrybucji i przesyłu energii oraz zapewnią ciągłość dostaw i sprawne działanie systemu energetycznego,

b) współpraca międzyresortowa w zakresie aktualizacji i wdrażania dokumentów strategicznych w zakresie transformacji sektora energetycznego (takich, jak chociażby Krajowy Plan w dziedzinie Energii i Klimatu do 2030 r. z perspektywą do 2040 r. [KPEiK]) w celu wszechstronnego uwzględnienia kwestii digitalizacji systemu energetycznego,

c) dalszy rozwój inteligentnych sieci (smart grids) zgodny z unijnymi zasadami interoperacyjności, wytycznymi Grupy Roboczej “Clean Energy Package”[144] oraz założeniami projektu KPEiK. Dzięki coraz bardziej powszechnemu zastosowaniu inteligentnych liczników, rozbudowa smart grids i digitalizacja systemu energetycznego (zwiększania jego opomiarowania, sprawności, inteligentnego sterowania) jest możliwa. W przyszłości kluczowe będzie także wdrażanie coraz to bardziej zaawansowanych narzędzi AI, które pozwolą na przetwarzanie na bieżąco wiedzy o kształcie lokalnego i krajowego rynku energetycznego - analizowanie coraz większych ilości danych rosnącego grona prosumentów, zjawisk atmosferycznych w celu prognozowania zużycia energii, danych z czujników i urządzeń IoT mówiących o nawykach odbiorców energii,

d) wspieranie, równolegle z cyfryzacją systemu elektroenergetycznego, rozwoju podobnych rozwiązań w ciepłownictwie. Rozwiązania pozwolą na zmapowanie całej sieci ciepłowniczej czy stworzenie pełnego cyfrowego modelu sieci, zintegrowanego z innymi systemami działającymi w przedsiębiorstwie ciepłowniczym,

e) wspieranie innowacji w sektorze energetycznym przez inwestycje w prace badawczo-rozwojowe (B+R) oraz szkolenia specjalistów ICT skupione na tworzeniu rozwiązań cyfrowych dla sektora energetycznego.

[box] Co z tego wynika: Usprawnimy funkcjonowanie sektora energetycznego zwiększając zastosowanie rozwiązań cyfrowych, inwestując w prace badawczo-rozwojowe i zapewniając rozwój specjalistów ICT.

[144] https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart Grids and Meters/Smart Grids/finalreportwg-cep_2019.pdf.

Cel 4.7.2: Wpływ technologii ICT wykorzystywanych przez administrację publiczną na środowisko jest weryfikowany i ograniczany

Co umożliwi realizację celu:

a) mierzenie cyfrowego śladu węglowego administracji publicznej generowanego na skutek korzystania z urządzeń elektronicznych i internetu w sektorze publicznym, a także zużywania energii niezbędnej do utrzymania państwowej infrastruktury (centrów danych, serwerów),

b) mapowanie i monitorowanie łańcucha dostaw systemów i usług ICT wykorzystywanych w administracji publicznej. Opracowanie norm zużycia energii dla systemów i usług ICT, które są brane pod uwagę przy realizacji zamówień publicznych oraz premiowanie dostawców systemów i usług ICT, którzy zobowiązali się do osiągnięcia neutralności klimatycznej do 2050 r. (zgodnie z Porozumieniem paryskim) bądź wcześniej, przedstawiając rzetelny plan działania i wykazując udokumentowane postępy w realizacji celów,

c) zaprojektowanie zasad zrównoważonego rozwoju ICT (w tym źródeł zasilania) i ekologii cyfrowej w organach administracji publicznej oraz uwzględnianie ich przy projektowaniu krajowych polityk publicznych i strategii.

Cel 4.7.3: Przyjazny środowisku sektor ICT

Co umożliwi realizację celu:

a) promowanie rozwoju i wykorzystania energooszczędnych rozwiązań wśród operatorów telekomunikacyjnych. Dążenie do zapewnienia większej efektywności energetycznej w projektowaniu, budowie i eksploatacji sieci, w tym dbanie o wymianę urządzeń sieciowych na bardziej energooszczędne, włączanie funkcji oszczędzania energii w nieużywanych komponentach, optymalizację z wykorzystaniem sztucznej inteligencji,

b) przygotowanie we współpracy z sektorem ICT, przedsiębiorstwami przemysłu technologicznego, instytucjami szkolnictwa wyższego, instytutami badawczymi, wytycznych i najlepszych praktyk dotyczących zrównoważonego rozwoju w projektowaniu produktów i usług cyfrowych, w tym promowanie wykorzystania i rozwoju niskoemisyjnych i zeroemisyjnych źródeł energii,

c) zachęcanie operatorów centrów przetwarzania danych do uwzględnienia dobrych praktyk, o których mowa w europejskim kodeksie postępowania w sprawie efektywności energetycznej centrów danych[145], również w obliczu dynamicznych zmian na rynku energii. Zachęcanie do podnoszenia efektywności energetycznej układów chłodzenia serwerów przez stosowanie systemów odzysku ciepła na potrzeby własne operatorów centrów danych, a także na potrzeby eksportu ciepła do sieci ciepłowniczych,

d) zachęcanie do tworzenia narzędzi cyfrowych generujących rozwiązania przyjazne środowisku, poprzez konkursy tematyczne i „hackathony”.

[145] https://joint-research-centre.ec.europa.eu/scientific-activities-z/energy-efficiency/energy-efficiency-products/code-conduct-ict/european-code-conduct-energy-efficiency-data-centres_en.

Cel 4.7.4: Obywatele są świadomi wpływu technologii ICT na środowisko i dysponują podstawową wiedzą w zakresie ekologii cyfrowej

Co umożliwi realizację celu:

a) uwzględnianie w programach kształcenia kwestii wpływu korzystania z usług ICT na środowisko oraz edukowanie na temat tego, jak korzystać z technologii w sposób bardziej zrównoważony. Prowadzenie kampanii społeczno-edukacyjnych podnoszących świadomość w ww. obszarach,

b) podnoszenie świadomości znaczenia przekazywania zużytego sprzętu elektrycznego i elektronicznego do recyklingu oraz zwiększanie wiedzy na temat dostępnych form i możliwości przekazywania elektroodpadów,

c) propagowanie stosowania norm i oznakowań dotyczących zrównoważonego rozwoju w odniesieniu do produktów i usług cyfrowych.

[box] Co z tego wynika: Umożliwimy Ci zwiększenie wiedzy o wpływie technologii ICT na środowisko oraz pokażemy jak korzystać z niej zgodnie z zasadami ekologii cyfrowej.

4.8 Cyfrowa modernizacja rolnictwa

Diagnoza – jak jest?

Obszary rolnicze zajmują 60% powierzchni kraju, a w Polsce funkcjonuje ok. 1,2 mln gospodarstw rolnych. W 2020 r. ponad 99% z nich stanowiły gospodarstwa indywidualne, posiadające 91,3% użytków rolnych[146]. Swoje produkty sprzedawało 70,8% gospodarstw, a 15,7% produkowało wyłącznie na własny użytek[147]. W III kwartale 2024 r. w rolnictwie pracowało 6% ogółu pracujących[148]. Wartość eksportu polskiej żywności w 2024 r. wyniosła 53,8 mld euro, z tego 73,9% eksportowane było na rynki unijne. Udział polskich produktów w rynku europejskim stale zwiększa się, podobnie jak dodatnie saldo wymiany handlowej. Odsetek eksportu w sektorze rolno-spożywczym w eksporcie ogółem wyniósł w 2024 r. 15,2%[149].

Aby zachować ten korzystny trend, konieczne jest utrzymanie konkurencyjności polskich producentów rolno-spożywczych, szczególnie w kontekście nowych wyzwań przewidzianych w ramach Europejskiego Zielonego Ładu. Dokument zakłada m.in. zmniejszenie stosowania środków ochrony roślin o 50%, nawozów o 20% oraz zwiększenia udziału upraw ekologicznych do 25% powierzchni użytków rolnych. Przewiduje się, że wdrożenie tych celów może doprowadzić do zmniejszenia produkcji i dochodów rolników, wzrostu cen żywności i pogorszenia międzynarodowej konkurencyjności polskiego rolnictwa[150]. Warto także zwrócić uwagę na inny dokument, który może mieć znaczny wpływ na kształt polskiego rolnictwa w przyszłości – końcowe sprawozdanie z zainicjowanego przez przewodniczącą Komisji Europejskiej Ursulę von der Leyen dialogu strategicznego nt. przyszłości rolnictwa w UE pn. *Wspólna perspektywa rolnictwa i żywności w Europie*. Dokument zawiera rekomendacje m.in. dotyczące rozwoju rolnictwa w kierunku zrównoważonym czy konieczności powstania jednolitych zasad oceny odziaływania działalności rolniczej na środowisko (np. w kontekście redukcji emisji gazów cieplarnianych), a także potrzebie wzrostu inwestycji w badania i innowacje oraz promocję możliwości cyfrowych w rolnictwie[151].

Mimo rozwoju nowoczesnych metod produkcji, efektywność pracy w rolnictwie pozostaje niska: w 2023 r. sektor ten wygenerował 3,3% PKB[152]. Polska wytwarza 6,6% produkcji sektora rolnego państw UE, przy udziale powierzchni użytków rolnych 8,3%, co wskazuje na niewykorzystanie potencjału produkcji[153]. Pomóc w tym zakresie może m.in. wdrażanie nowoczesnych technologii. W zależności od funkcji gospodarstwa, kierunku produkcji i jej

[146] Powszechny Spis Rolny 2020 – Charakterystyka gospodarstw rolnych w 2020 r., raport GUS.
[147] Obszary wiejskie w Polsce w 2022 r., analizy statystyczne GUS.
[148] https://rynekpracy.org/statystyki/pracujacy-w-rolnictwie-przemysle-i-uslugach/.
[149] https://www.gov.pl/web/rolnictwo/polski-handel-zagranicznyartykulami-rolno-spozywczymi-2024-r.
[150] Raport Polityka Insight: https://www.politykainsight.pl/bibliotekaraportow/2151464,wplyw-europejskiego-zielonego-ladu-na-polskie-rolnictwo.read.
[151] Main initiatives: Strategic Dialogue on the future of EU agriculture, https://agriculture.ec.europa.eu/common-agricultural-policy/cap-overview/main-initiatives-strategic-dialogue-future-eu-agriculture_en#strategic-dialogue-report.
[152] https://www.ifp.org.pl/20-lat-polskiego-rolnictwa-w-ue-perspektywa-makroekonomiczna-wybrane-fakty/.
[153] "Transformacja Polski dzięki wykorzystaniu inteligentnych rozwiązań cyfrowych. Studium programu." Raport Grupy roboczej ds. Sztucznej Inteligencji przy Ministerstwie Cyfryzacji. Warszawa, październik 2024.

skali, producenci sektora rolno-spożywczego potrzebują albo rozwiązań opierających się o przełomowe technologie, albo rozwiązań prostych, już sprawdzonych, które są możliwe do wdrożenia bez zaawansowanych zmian technologicznych, a które usprawniają procesy produkcyjne[154].

Wdrażanie w rolnictwie nowoczesnych technologii zachodzi jednak w różnym stopniu, w zależności od wielkości ekonomicznej gospodarstwa. Te o dużej wielkości implementują wiele rozwiązań w zakresie cyfryzacji czy rolnictwa precyzyjnego, a gospodarstwa średnie i małe potrzebują takich rozwiązań, które dostosowane będą do ich skali[155].

Do najistotniejszych problemów utrudniających wdrożenie i upowszechnienie nowoczesnych technologii cyfrowych w rolnictwie należą[156]:

- niedobór wyspecjalizowanych ekspertów w ośrodkach doradztwa rolniczego, instytucjach edukacyjnych i administracji publicznej,
- ograniczone możliwości inwestycyjne właścicieli małych i średnich gospodarstw rolnych w Polsce i obawy związane z ryzykiem inwestycji,
- ograniczone zachęty dla całego łańcucha dostaw do szerszego korzystania z narzędzi Rolnictwa 4.0,
- brak otwartego systemu gromadzenia, przetwarzania i udostępniania danych,
- trudności w dopasowaniu odpowiednich rozwiązań do specyfiki i potrzeb gospodarstwa w kontekście ich efektywności ekonomicznej,
- brak dostępu do szybkiego i niezawodnego internetu.

Przezwyciężenie powyższych problemów, przekładające się na szersze i bardziej efektywne wykorzystanie technologii cyfrowych w rolnictwie, przyczyni się do rozwiązania szeregu wyzwań stojących przed tym obszarem.

[154] Uchwała nr 193 Rady Ministrów z dnia 17 października 2023 r. w sprawie przyjęcia aktualizacji „Strategii zrównoważonego rozwoju wsi, rolnictwa i rybactwa 2030” (M.P. poz. 1214).
[155] Uchwała nr 193 Rady Ministrów z dnia 17 października 2023 r. w sprawie przyjęcia aktualizacji „Strategii zrównoważonego rozwoju wsi, rolnictwa i rybactwa 2030”.
[156] Raport przygotowany przez PwC w ramach projektu ,,Cyfrowa transformacja rolnictwa w Polsce”.

Cel 4.8.1: Stworzenie warunków sprzyjających powszechnemu wdrażaniu i wykorzystywaniu nowoczesnych technologii w rolnictwie

Co umożliwi realizację celu?

a) opracowanie sektorowej strategii cyfryzacji rolnictwa, uwzgledniającej potrzeby cyfrowej transformacji rolnictwa i obszarów wiejskich, jak i niezbędne zmiany organizacyjne, procesowe oraz technologiczne w instytucjach publicznych tego sektora, zgodne z Architekturą Informacyjną Państwa, zapewniając spójność działań, ich trwałość oraz skuteczną realizację celów polityki rolnej,

b) rozwój kompetencji instytucjonalnych w zakresie zarządzania danymi i analityki na potrzeby projektowania, monitorowania i oceny polityk publicznych w rolnictwie i na obszarach wiejskich,

c) stworzenie systemu zachęt finansowych i wsparcia z przeznaczeniem na wdrożenie nowoczesnych technologii, dopasowanych do potrzeb różnych typów gospodarstw rolnych,

d) stworzenie przejrzystego portalu informującego o instrumentach wsparcia i możliwościach jego pozyskania oraz rozwój zintegrowanej platformy usług na rzecz sektora rolno-spożywczego,

e) rozwój i promocja mechanizmów podziału kosztów i użytkowania technologii rolniczych na poziomie lokalnych grup producenckich,

f) stworzenie i regularna aktualizacja katalogu rozwiązań Rolnictwa 4.0, ze wskazaniem ich zastosowania w praktyce, gospodarstw demonstracyjnych, w których są stosowane, oraz zmapowania ich pod kątem potrzeb rolników,

g) budowa lub modernizacja infrastruktury technicznej na obszarach wiejskich, prowadzona w sposób zintegrowany z działaniami służącymi zwiększeniu dostępności cyfrowej obszarów wiejskich (m.in. rozwój infrastruktury zapewniającej dostęp do szerokopasmowego Internetu),

h) opracowanie charakterystyki sieci teleinformatycznych oraz standardów wymiany danych na potrzeby m.in. rozwiązań Rolnictwa 4.0 i 5.0 oraz wsparcie ich wdrożenia,

i) wspieranie rozwoju sieci czujników pomiarowych,

j) budowa, wdrażanie i promocja rozwiązań dla wspólnych przestrzeni danych oraz promocja i stosowanie wspólnych standardów w zakresie wymiany i analizy danych,

k) wspieranie rozwoju opartych na danych narzędzi cyfrowych dla rolnictwa, w szczególności systemów wspomagania decyzji (DSS), w tym wykorzystujących algorytmy sztucznej inteligencji i uczenia maszynowego,

l) promocja interoperacyjności, tworzenie otwartych zbiorów danych wysokiej jakości niezbędnych dla rozwoju nowych innowacyjnych usług w rolnictwie oraz wdrożenie mechanizmów walidacji i ewaluacji jakości danych,

m) działania uświadamiające korzyści wynikające z wymiany danych i wspierające zaangażowanie lokalnych społeczności w proces tworzenia przestrzeni wymiany danych,

n) tworzenie infrastruktury testowej umożliwiającej testowanie rozwiązań IoT i AI w rolnictwie na dużą skalę w bezpiecznym środowisku regulacyjnym.

Cel 4.8.2: Zwiększanie bezpieczeństwa i konkurencyjności polskiej żywności poprzez wykorzystanie nowoczesnych technologii z uwzględnieniem dbałości o środowisko naturalne i dobrostan zwierząt

Co umożliwi realizację celu?

a) budowa systemu IT służącego do efektywnego monitorowania i identyfikowania informacji o produktach rolno-spożywczych w łańcuchach dostaw,

b) automatyzacja procesów monitorowania i śledzenia produktów na każdym etapie produkcji umożliwia szybką reakcję na zagrożenia związane z jakością i bezpieczeństwem żywności,

c) wspieranie rozwoju opartych na danych systemów oceny i zapewnienia jakości produktów rolno-spożywczych w gospodarstwach rolnych i w łańcuchach dostaw,

d) wspieranie wykorzystania technologii satelitarnych w rolnictwie dostarczających precyzyjnych informacji o zróżnicowaniu lokalnych warunków upraw,

e) wspieranie korzystania w produkcji rolnej z rozwiązań cyfrowych ograniczających negatywny wpływ na środowisko oraz uwzględniających dbałość o dobrostan zwierząt.

Cel 4.8.3: Zwiększenie możliwości rozwoju kompetencji cyfrowych dzięki powszechnemu dostępowi do szkoleń, efektywnego doradztwa i transferu wiedzy

Co umożliwi realizację celu?

a) tworzenie i wzmacnianie sieci współpracy między instytucjami publicznymi, światem nauki, rolnikami, producentami, przetwórcami i dystrybutorami w celu wymiany wiedzy, doświadczeń oraz wspólnego wdrażania innowacyjnych rozwiązań,

b) wsparcie sieci doradztwa w zakresie nowoczesnych rozwiązań, w tym Rolnictwa 4.0 i 5.0, w szczególności sztucznej inteligencji, robotów autonomicznych czy systemów wspierania decyzji,

c) działania promujące i uświadamiające korzyści płynące z wprowadzania innowacji i nowoczesnych technologii, w tym efektywności ekonomicznej wprowadzania innowacji,

d) stworzenie systemu efektywnych działań edukacyjnych nakierowanych na rozwój wiedzy i umiejętności rolników i pracowników sektora rolno-spożywczego w zakresie wdrażania nowoczesnych metod produkcji i technologii,

e) wspieranie powstawania i wzmocnienie roli gospodarstw demonstracyjnych i eksperymentalnych, jako miejsc istotnych w procesie demonstrowania praktycznego zastosowania i korzyści płynących z używania nowoczesnych technologii.

VII. System wdrażania

Koordynacja

Za realizację Strategii odpowiadają członkowie Rady Ministrów, a organem odpowiedzialnym za monitorowanie jej realizacji będzie minister właściwy do spraw informatyzacji.

Cyfryzacja jest procesem przekrojowym i wielowymiarowym, co znajduje odzwierciedlenie w bardzo szerokim zakresie przedmiotowym Strategii. Realizacja głównego jej celu, jakim jest podnoszenie jakości życia przez cyfryzację, wymaga zaangażowania i ścisłej, skoordynowanej, współpracy wielu jednostek sektora publicznego. Niemniej interwencja nie ogranicza się jedynie do sfery funkcjonowania państwa, ale zakłada również inspirowanie działań na rzecz transformacji cyfrowej przy zaangażowaniu sektora prywatnego.

Strategiczny horyzont czasowy obejmuje perspektywę dziesięcioletnią do 2035 r., natomiast operacjonalizacja działań wymaga elastycznego modelu w krótszej perspektywie czasowej. W celu zagwarantowania mechanizmu skoordynowanej, skutecznej i terminowej realizacji celów określonych w Strategii, minister właściwy do spraw informatyzacji opracuje plan operacyjny. Plan operacyjny zostanie przyjęty przez Komitet do spraw Cyfryzacji i będzie wspierać proces monitorowania realizacji Strategii. Dokument będzie identyfikować i agregować działania o charakterze priorytetowym wskazując na harmonogram realizacji oraz źródła ich finansowania. Będzie on obejmować trzyletni horyzont czasowy, natomiast jego coroczna aktualizacja umożliwi dostosowywanie do zmieniających się warunków technologicznych, społecznych i prawnych.

Szczególną rolę w procesie wdrażania Strategii odegrają pełnomocnicy do spraw informatyzacji, powoływani obligatoryjnie w urzędach obsługujących ministrów kierujących działami administracji rządowej oraz w Kancelarii Prezesa Rady Ministrów (fakultatywnie natomiast w pozostałych urzędach). Działania pełnomocników będą skoncentrowanie na sprawach należących do właściwości działu administracji rządowej, kierowanego przez właściwego ministra, w tym na sprawach należących do właściwości jednostek organizacyjnych lub organów podległych temu ministrowi i przez niego nadzorowanych. Głównym ich zadaniem będzie wsparcie w koordynowaniu realizacji Strategii, w tym przygotowywanie aktualnych informacji na temat postępów w jej realizacji oraz związanego z tym ryzyka, a także diagnozowanie obszarów koniecznych zmian dla dalszego wdrażania Strategii oraz wprowadzania nowych technologii cyfrowych.

Realizacja Strategii wymaga spójnych, zharmonizowanych i konsekwentnych działań, niejednokrotnie jednak przecinających tradycyjny podział obszarów działalności państwa oraz wertykalnych względem działów administracji rządowej. Służyć ma temu bieżące współdziałanie powołanych pełnomocników do spraw informatyzacji, a w wymiarze instytucjonalnym możliwe to będzie dzięki roli Komitetu do spraw Cyfryzacji.

Zadaniem Komitetu do spraw Cyfryzacji będzie zapewnienie koordynacji działań państwa związanych z informatyzacją oraz wsparcie rozwoju cyfrowego państwa, co ma kluczowe znaczenie dla wdrażania Strategii. Działalność Komitetu do spraw Cyfryzacji polegająca na opiniowaniu i monitorowaniu przedsięwzięć informatycznych o publicznym zastosowaniu, ma na celu zapewnienie ich spójności z działaniami strategicznymi państwa, w tym zgodności ze Strategią oraz z założeniami AIP. Natomiast uzależnienie możliwości finansowania ze

środków publicznych przedsięwzięć informatycznych o publicznym zastosowaniu od pozytywnej oceny Komitetu do spraw Cyfryzacji wpłynie pozytywnie na zwiększenie interoperacyjności i komplementarności rozwiązań informatycznych funkcjonujących w państwie, a także na zwiększenie efektywności gospodarowania środkami publicznymi.

Realizacja głównego celu Strategii wymaga, aby zaangażowanie wielu jednostek sektora publicznego, o którym mowa powyżej, odbywało się wielokierunkowo i na wielu płaszczyznach. Działania służące realizacji celu będą realizowane bowiem w formie programów, projektów, aktów prawnych i przepisów technicznych.

Przegląd

Z uwagi na potrzebę dobrego planowania, spójności i ciągłości procesów cyfryzacji państwa, Strategia obejmuje wieloletnią perspektywę. Jednak tempo rozwoju technologicznego i trudność w przewidzeniu jego długofalowych kierunków sprawia, że niezbędny jest jej regularny przegląd i ewentualna aktualizacja. Minister właściwy do spraw informatyzacji we współpracy z członkami Rady Ministrów, będzie dokonywał przeglądu Strategii co 2 lata. Sprawozdanie z przeprowadzonego przeglądu będzie poddawane konsultacjom społecznym, a następnie przedkładane Radzie Ministrów w terminie 2 miesięcy od zakończenia przeglądu. Do opracowania informacji z realizacji Strategii w celu dokonania przeglądu zobowiązani będą pełnomocnicy do spraw informatyzacji.

Monitorowanie

Minister właściwy do spraw informatyzacji monitoruje realizację Strategii raz w roku. System monitorowania obejmuje badanie postępu zaplanowanych działań w ramach celów horyzontalnych i kierunkowych oraz badanie ilościowe dotyczące stopnia realizacji przyjętych wskaźników efektywności ujętych w zestawieniu poniżej. Wyniki z przeprowadzonego monitoringu realizacji Strategii będą przedstawiane Komitetowi do spraw Cyfryzacji w formie raportu oraz publikowane na stronie internetowej Ministerstwa Cyfryzacji nie później niż do 31 marca. Komitet do spraw Cyfryzacji jest uprawniony do koordynacji działań w zakresie monitorowania realizacji Strategii, w zakresie której przyjmie plan operacyjny stanowiący narzędzie wspierające proces monitorowania oraz jego efektywną koordynację.

Raport z monitorowania będzie sporządzany przez ministra właściwego do spraw informatyzacji w szczególności na podstawie:

a) przekazanych przez pełnomocników do spraw informatyzacji informacji na temat każdego z zaplanowanych w Strategii działań i danych statystycznych w odniesieniu do przyjętych wskaźników, zgodnie z właściwością poszczególnych członków Rady Ministrów,
b) analizy źródeł danych dla kluczowych wskaźników efektywności określonych w zestawieniu.

W raporcie będą zawarte: opisy podjętych działań zaplanowanych w Strategii wraz z oceną stopnia ich zaawansowania, ewentualne zdiagnozowane problemy z ich wdrażaniem oraz rekomendacje dla poszczególnych członków Komitetu do spraw Cyfryzacji na kolejny okres.

Integralnym elementem monitoringu Strategii będzie zestaw wskaźników efektywności, odnoszących się do celów wyznaczonych w poszczególnych obszarach, ze wskazaniem wartości bazowej oraz docelowej. Źródłem danych dla pomiaru wskaźników będzie przede wszystkim krajowa statystyka publiczna, ale również System Inwentaryzacji Systemów Teleinformatycznych (SIST), informacje z działalności Komitetu do spraw Cyfryzacji, dane własne podmiotów odpowiedzialnych za realizację poszczególnych działań oraz dostępne, cykliczne raporty i badania rynku.

Poniższe zestawienie prezentuje kluczowe wskaźniki efektywności określone dla Strategii.

Obszary horyzontalne

1.1 Komunikacja elektroniczna

1. Odsetek gospodarstw domowych objętych zasięgiem stacjonarnych sieci o bardzo dużej przepustowości (VHCN)[157]
   Wartość bazowa: 83,8% (2024)[158]

   Wartość docelowa: 100%

   Rok, do którego wskaźnik ma zostać osiągnięty: 2030

   Źródło danych: raport o stanie cyfrowej dekady

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
90,4%	94%	96,6%	98,3%	99,3%	100%	100%	100%	100%	100%	100%

2. Odsetek gospodarstw domowych objętych zasięgiem przynajmniej 1 sieci 5G[159]
   Wartość bazowa: 89,3% (2024)[160]

   Wartość docelowa: 100%

   Rok, do którego wskaźnik ma zostać osiągnięty: 2030

   Źródło danych: raport o stanie cyfrowej dekady

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
94,9%	98,1%	99,3%	99,7%	99,9%	100%	100%	100%	100%	100%	100%

[157] Wskaźnik zgodny z celami programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.
[158] Dane za 2025 r. nie są jeszcze dostępne.
[159] Wskaźnik zgodny z celami programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.
[160] Dane za 2025 r. nie są jeszcze dostępne.

1.2 Kompetencje przyszłości

3. Odsetek osób, które posiadają podstawowe lub ponadpodstawowe umiejętności cyfrowe[161]
   Wartość bazowa: 50,4% (2025)

   Wartość docelowa: 85% osób w wieku 16-74 lata

   Rok, do którego wskaźnik ma zostać osiągnięty: 2035

   Źródło danych: GUS

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
56,3%	62,2%	68,2%	74,1%	80%	82%	83%	84%	84,5%	85%

4. Odsetek osób, które posiadają ponadpodstawowe umiejętności cyfrowe
   Wartość bazowa: 23,5% (2025)

   Wartość docelowa: 50% osób w wieku 16-74 lata

   Rok, do którego wskaźnik ma zostać osiągnięty: 2035

   Źródło danych: GUS

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
26,8%	30,1%	33,4%	36,7%	40%	42,3%	45,1%	47,1%	48,7%	50%

5. Udział specjalistów ICT wśród pracujących[162]
   Wartość bazowa: 4,5% (2024)[163]

   Wartość docelowa: 10% pracujących

   Rok, do którego wskaźnik ma zostać osiągnięty: 2035

   Źródło danych: Eurostat

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
4,8%	5,0%	5,3%	5,5%	5,8%	6,0%	7,6%	8,6%	9,2%	9,8%	10,0%

[161] Wskaźnik zgodny z celami programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.
[162] Wskaźnik zgodny z celami Programu Rozwoju Kompetencji Cyfrowych oraz programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.
[163] Dane za 2025 r. nie są jeszcze dostępne.

6. Udział kobiet wśród specjalistów ICT[164]
   Wartość bazowa: 17,5% (2024)[165]
   Wartość docelowa: 36%
   Rok, do którego wskaźnik ma zostać osiągnięty: 2035
   Źródło danych: Eurostat

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
21,4%	22,9%	24,5%	26,0%	27,6%	29,0%	30,4%	31,8%	33,2%	34,6%	36%

1.3 Cyberbezpieczeństwo

7. Powołanie centralnej instytucji odpowiedzialnej za cyberbezpieczeństwo na poziomie krajowym
   Wartość bazowa: 0 (2026)

   Wartość docelowa: 1

   Rok, do którego wskaźnik ma zostać osiągnięty: 2029

   Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	0	0	1						

8. Osiągnięcie pełnej zdolności operacyjnej w zakresie przetwarzania informacji niejawnych w rządowych narzędziach chmurowych.
   Wartość bazowa: 0

   Wartość docelowa: 1

   Rok, do którego wskaźnik ma zostać osiągnięty: 2029

   Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	0	0	1						

[164] Wskaźnik zgodny z celami Programu Rozwoju Kompetencji Cyfrowych oraz programu polityki „Droga ku cyfrowej dekadzie" do 2030 r.
[165] Dane za 2025 r. nie są jeszcze dostępne.

9. Odsetek terminowo zgłoszonych incydentów poważnych do zespołów CSIRT przez zobowiązane ustawowo podmioty Krajowego Systemu Cyberbezpieczeństwa
Wartość bazowa: 76% (2024)[166]

Wartość docelowa: 100%

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: zespoły CSIRT

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
77,5%	79,0%	80,5%	82,0%	83,5%	85,0%	88,0%	91,0%	94,0%	97,0%	100%

1.4 Koordynacja cyfrowej transformacji kraju

10. Udział urzędów obsługujących ministrów kierujących działami administracji rządowej, w których powołany został pełnomocnik do spraw informatyzacji w ogólnej liczbie urzędów obsługujących ministrów kierujących działami administracji publicznej i KPRM
Wartość bazowa: 95% (2025)

Wartość docelowa: 100%

Rok, do którego wskaźnik ma zostać osiągnięty: 2026

Źródło danych: dane własne MC/KdsC

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

11. Udział przedsięwzięć informatycznych o publicznym zastosowaniu, których założenia są zgodne z pryncypiami, standardami, wytycznymi i rekomendacjami architektonicznymi AIP w ogólnej liczbie przedsięwzięć informatycznych o publicznym zastosowaniu, których założenia są opiniowane przez Komitet do spraw Cyfryzacji
Wartość bazowa: 33% (2025)

Wartość docelowa: 95%

Rok, do którego wskaźnik ma zostać osiągnięty: 2030

Źródło danych: dane własne MC/KdsC

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
50%	61%	73%	84%	95%	95%	95%	95%	95%	95%

[166] Dane za 2025 r. nie są jeszcze dostępne.

Państwo

2.1 E-usługi publiczne

12. Odsetek usług publicznych dla obywateli, zgodnych z listą kluczowych usług publicznych eGovernment Benchmark, które są w pełni cyfrowe[167]
Wartość bazowa: 70,7% (2024)[168]

Wartość docelowa: 100%

Rok, do którego wskaźnik ma zostać osiągnięty: 2030

Źródło danych: raport o stanie cyfrowej dekady

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
88,5%	93,2%	96,3%	98,2%	99,3%	100%	100%	100%	100%	100%	100%

13. Integracja z usługą ePłatności minimum jednej instytucji/urzędu w ramach JST w Polsce
Wartość bazowa: 5,6% (2025)

Wartość docelowa: 100%

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane własne COI

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
8,1%	12,1%	22,2%	32,3%	40,3%	52,4%	68,6%	80,7%	88,7%	100%

2.2 Cyfryzacja procesów administracyjnych i postępowań sądowych

14. Odsetek jednostek administracji publicznej korzystających z EZD w stosunku do ogólnej liczby jednostek administracji
Wartość bazowa: 84,7% (2024)[169]

Wartość docelowa: 100%

Rok, do którego wskaźnik ma zostać osiągnięty: 2028

Źródło danych: GUS

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
91,9%	93,5%	94,7%	100%	100%	100%	100%	100%	100%	100%	100%

[167] Wskaźnik zgodny z celami programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.
[168] Dane za 2025 r. nie są jeszcze dostępne.
[169] Dane za 2025 r. nie są jeszcze dostępne.

15. Odsetek urzędów administracji publicznej wykorzystujących technologie sztucznej inteligencji

Wartość bazowa: 6,8% (2024)[170]

Wartość docelowa: 80%

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: GUS

Wartość pośrednia (proc.)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
20%	30%	40%	50%	65%	75%	77%	77,5%	79%	79,5%	80%

2.3 Publiczne systemy teleinformatyczne i rejestry publiczne

16. Udział liczby publicznych systemów teleinformatycznych, dla których w repozytorium interoperacyjności udostępniono opisy API, w stosunku do liczby publicznych systemów teleinformatycznych monitorowanych w SIST.

Wartość bazowa: 0 (2025)

Wartość docelowa: 100%

Rok, do którego wskaźnik ma zostać osiągnięty: 2031

Źródło danych: Dane własne MC (SIST)

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0%	0%	20%	60%	90%	100%	100%	100%	100%	100%

17. Umocowanie prawne referencyjnych rejestrów publicznych

Wartość bazowa: 0 (2025)

Wartość docelowa: 1

Rok, do którego wskaźnik ma zostać osiągnięty: 2028

Źródło danych: Dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	0	1							

[170] Dane za 2025 r. nie są jeszcze dostępne.

2.4 Cyfrowa tożsamość

18. Liczba wydanych środków identyfikacji elektronicznej dla osób prawnych
Wartość bazowa: 0 (2025)

Wartość docelowa: 180000

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane własne COI

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	4787	11335	25533	52029	90000	127971	154467	168665	180000

19. Liczba aktywowanych portfeli tożsamości cyfrowej
Wartość bazowa: 0 (2025)*

Wartość docelowa: 20 mln użytkowników

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane własne COI

Wartość pośrednia (mln)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	14,7	15,9	16,7	17,4	17,8	18,2	18,5	18,7	20

*planowane uruchomienie narzędzia w roku 2027

2.5 Chmura obliczeniowa

20. Minimum 70% systemów wykorzystywanych do realizacji cyfrowych usług publicznych korzysta ze współdzielonej infrastruktury obliczeniowej (chmury obliczeniowej)
Wartość bazowa: brak danych* - wartość bazowa do określenia na późniejszym etapie

Wartość docelowa: 70%

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane własne MC (SIST)

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
bd	bd	bd	bd	bd	bd	bd	bd	bd	70%

*wartość bazowa i wartości pośrednie zostaną oszacowane po inwentaryzacji SIST w połowie 2026 r.

2.6 Otwarte dane i wymiana danych

21. Liczba danych udostępnionych przez podmioty publiczne w portalu dane.gov.pl
Wartość bazowa: 43700 (2025)

Wartość docelowa: 93700

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane.gov.pl

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
48700	53700	58700	63700	68700	73700	78700	83700	88700	93700

Ludzie

3.1 Bezpieczna przestrzeń cyfrowa

22. Stworzenie i wprowadzenie systemu oceny wymiaru etycznego narzędzi SI stosowanych przez państwo
Wartość bazowa: 0 (2025)

Wartość docelowa: 1

Rok, do którego wskaźnik ma zostać osiągnięty: 2027

Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	1								

23. Odsetek referencyjnych rejestrów publicznych w zakresie danych osobowych, umożliwiających obywatelom weryfikację, jaka instytucja miała dostęp do ich danych
Wartość bazowa: 0 (2025)

Wartość docelowa: 60%[171]

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane własne MC

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	0	0	0	0%	0%	15%	30%	45%	60%

[171] W kolejnych latach zakłada się dążenie do osiągnięcia 100%.

24. Ustalenie organu odpowiedzialnego za nadzorowanie i integrowanie działań różnych podmiotów zajmujących się przeciwdziałaniem dezinformacji
Wartość bazowa: 0 (2025)

Wartość docelowa: 1

Rok, do którego wskaźnik ma zostać osiągnięty: 2026

Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
1									

3.2 Cyfrowe zdrowie

25. Odsetek PWDL podłączonych do systemu P1 i raportujących Zdarzenia Medyczne
Wartość bazowa: 24% (2025)
Wartość docelowa: 100%
Rok, do którego wskaźnik ma zostać osiągnięty: 2035
Źródło danych: CeZ (Centrum e-Zdrowia)

Wartość pośrednia (proc.)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
33%	42%	52%	62%	72%	80%	88%	95%	98%	100%

26. Wprowadzenie narzędzi predykcyjnych w systemie centralnym

Wartość bazowa: brak danych* - wartość bazowa i wartości pośrednie do określenia na późniejszym etapie

Wartość docelowa: 100 jednostek chorobowych

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: CeZ

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
bd	bd	bd	bd	bd	bd	bd	bd	bd	100

*określenie wartości bazowej oraz wartości pośrednich będzie możliwe po udostępnieniu Platformy Usług Inteligentnych (PUI) MZ; planowany pierwszy odczyt 2026/2027

3.3 Branże kreatywne

27. Przychody polskiego sektora producentów gier wideo

Wartość bazowa: 1293 mln EUR (2024)[172]

Wartość docelowa: 3689 mln EUR

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: PARP/GIC

Wartość pośrednia (mln euro)										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
1422	1565	1721	1893	2082	2291	2520	2772	3049	3354	3689

3.5 Cyfrowa akademia

28. Liczba absolwentów kierunków kształcących w obszarze ICT (dyscypliny wg klasyfikacji ISCED 0610, 0611, 0612, 0613, 0618, 0619, 0688)

Wartość bazowa: 17920 (2025)

Wartość docelowa: 20000

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: system POL_on

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
18128	18336	18544	18572	18960	19168	19376	19584	19792	20000

29. Ilość mocy obliczeniowej dla obliczeń HPC dostępnej w PLGrid

Wartość bazowa: 87 petaflopsów (2025)

Wartość docelowa: 1000 petaflopsów (1 eksaflops)

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: PLGrid

Wartość pośrednia (PFLOPS)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
100	110	160	250	300	400	500	600	800	1000

[172] Dane za 2025 r. nie są jeszcze dostępne.

30. Ilość mocy obliczeniowej dla obliczeń AI dostępnej w PLGrid

Wartość bazowa: 3 eksaflopsy (2025)

Wartość docelowa: 100 eksaflopsów

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: PLGrid

Wartość pośrednia (EFLOPS)									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
20	40	40	44	60	64	68	72	80	100

Gospodarka i technologie

4.1 Cyfrowa transformacja przedsiębiorstw

31. Udział przedsiębiorstw sektora MŚP wykorzystujących na co najmniej podstawowym poziomie technologie cyfrowe[173]

Wartość bazowa: 69% (2024)[174]

Wartość docelowa: 92%

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: Eurostat

Wartość pośrednia										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
71,9%	75,5%	79,1%	82,2%	86,4%	90,0%	90,6%	90,8%	91,4%	91,8%	92%

32. Odsetek przedsiębiorstw korzystających z technologii sztucznej inteligencji[175]

Wartość bazowa: 8,7% (2025)

Wartość docelowa: 50%

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: GUS

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
14,9%	20,3%	25,1%	29,4%	33,3%	36,8%	40%	43%	46,2%	50%

[173] Wskaźnik zgodny z celami programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.
[174] Dane za 2025 r. nie są jeszcze dostępne.
[175] Wskaźnik zgodny z celami programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.

4.2 Sztuczna inteligencja

33. Stworzenie mechanizmu koordynacji wdrożenia i finansowania projektów AI w administracji publicznej

Wartość bazowa: 0 (2025)

Wartość docelowa: 1

Rok, do którego wskaźnik ma zostać osiągnięty: 2026

Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
1									

4.3 Inne technologie przełomowe

34. Stworzenie programu wieloletniego wspierania rozwoju technologii przełomowych

Wartość bazowa: 0 (2025)

Wartość docelowa: 1

Rok, do którego wskaźnik ma zostać osiągnięty: 2030

Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	0	0	0	1					

4.6 Open source

35. Utworzenie Biura Programów Otwartego Oprogramowania

Wartość bazowa: 0 (2025)

Wartość docelowa: 1

Rok, do którego wskaźnik ma zostać osiągnięty: 2027

Źródło danych: dane własne MC

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	1								

4.7 Cyfrowa i zielona transformacja

36. Odsetek gospodarstw domowych wyposażonych w inteligentne liczniki

Wartość bazowa: 33% (2024)[176]

Wartość docelowa: 80%

Rok, do którego wskaźnik ma zostać osiągnięty: 2028

Źródło danych: monitoring realizacji PEP

Wartość pośrednia										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
35%	55%	65%	80%	80%	80%	80%	80%	80%	80%	80%

4.8 Cyfrowa modernizacja rolnictwa

37. Liczba e-usług na wysokim poziomie dojrzałości (transakcja lub personalizacja) świadczonych przez jednostki administracji publicznej sektora rolnictwa na zintegrowanej platformie usług

Wartość bazowa: 4 (2025)

Wartość docelowa: 47

Rok, do którego wskaźnik ma zostać osiągnięty: 2035

Źródło danych: dane własne MRiRW

Wartość pośrednia									
2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
22	25	32	35	37	39	41	43	45	47

[176] Dane za 2025 r. nie są jeszcze dostępne.

Działania zaplanowane w każdym z obszarów będą koordynowane przez wyszczególnione w poniższym zestawieniu resorty wiodące, a wspierane przez inne urzędy, ze szczególnym naciskiem na resorty oznaczone poniżej.

Obszar		Organ wiodący	Organy współpracujące
Obszary horyzontalne	Komunikacja elektroniczna	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw wewnętrznych, Prezes Urzędu Komunikacji Elektronicznej, Minister Obrony Narodowej, Minister właściwy do spraw gospodarki
	Kompetencje przyszłości	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw oświaty i wychowania, Minister właściwy do spraw nauki i szkolnictwa wyższego, Szef Służby Cywilnej, Minister właściwy do spraw gospodarki
	Cyberbezpieczeństwo	Minister właściwy do spraw informatyzacji	Prezes Rady Ministrów, Minister Obrony Narodowej, Minister właściwy do spraw wewnętrznych
	Koordynacja cyfrowej transformacji kraju	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw administracji publicznej, Minister właściwy do spraw zagranicznych
Państwo	E-usługi publiczne	Minister właściwy do spraw informatyzacji	Członkowie Rady Ministrów oraz organy podległe ministrom lub przez nich nadzorowane, a także centralne organy administracji rządowej
	Cyfryzacja procesów administracyjnych i postępowań sądowych	Minister właściwy do spraw informatyzacji	Członkowie Rady Ministrów oraz organy podległe ministrom lub przez nich nadzorowane, a także centralne organy administracji rządowej, Prokurator Generalny
	Publiczne systemy teleinformatyczne i rejestry publiczne	Minister właściwy do spraw informatyzacji	Członkowie Rady Ministrów oraz organy podległe ministrom lub przez nich nadzorowane, a także centralne organy administracji rządowej

	Cyfrowa tożsamość	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw gospodarki
	Chmura obliczeniowa	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw administracji publicznej, Minister właściwy do spraw wewnętrznych, Minister Obrony Narodowej, Minister właściwy do spraw zagranicznych, Minister właściwy do spraw gospodarki
	Otwarte dane i wymiana danych	Minister właściwy do spraw informatyzacji	Członkowie Rady Ministrów oraz organy podległe ministrom lub przez nich nadzorowane, a także centralne organy administracji rządowej
Ludzie	Bezpieczna przestrzeń cyfrowa	Minister właściwy do spraw informatyzacji	Minister Obrony Narodowej, Minister właściwy do spraw wewnętrznych, Minister Sprawiedliwości, Minister właściwy do spraw pracy, Minister właściwy do spraw zagranicznych, Prezes Urzędu Komunikacji Elektronicznej
	Cyfrowe zdrowie	Minister właściwy do spraw zdrowia	Minister właściwy do spraw informatyzacji, Minister właściwy do spraw wewnętrznych
	Branże kreatywne	Minister właściwy do spraw kultury dziedzictwa narodowego	Minister właściwy do spraw informatyzacji, Minister właściwy do spraw gospodarki, Minister właściwy do spraw nauki i szkolnictwa wyższego
	Cyfrowy dostęp do wiedzy i kultury	Minister właściwy do spraw kultury dziedzictwa narodowego	Minister właściwy do spraw informatyzacji, Minister właściwy do spraw nauki i szkolnictwa wyższego
	Cyfrowa akademia	Minister właściwy do spraw nauki i szkolnictwa wyższego	Minister właściwy do spraw informatyzacji, Minister właściwy do spraw gospodarki
Gospodarka i technologie	Cyfrowa transformacja przedsiębiorstw	Minister właściwy do spraw gospodarki	Minister właściwy do spraw informatyzacji

	Sztuczna inteligencja	Minister właściwy do spraw informatyzacji	Minister Obrony Narodowej, Minister właściwy do spraw nauki i szkolnictwa wyższego, Minister właściwy do spraw wewnętrznych
	Inne technologie przełomowe	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw nauki i szkolnictwa wyższego, Minister Obrony Narodowej, Minister właściwy do spraw gospodarki
	Technologie kosmiczne	Minister właściwy do spraw gospodarki	Minister Obrony Narodowej, Minister właściwy do spraw informatyzacji, Minister właściwy do spraw nauki i szkolnictwa wyższego, Minister właściwy do spraw wewnętrznych
	Finansowanie i wsparcie innowacji	Minister właściwy do spraw gospodarki	Minister właściwy do spraw nauki i szkolnictwa wyższego, Minister właściwy do spraw finansów publicznych, Minister właściwy do spraw informatyzacji
	Open source	Minister właściwy do spraw informatyzacji	Minister właściwy do spraw gospodarki, Minister właściwy do spraw nauki i szkolnictwa wyższego
	Cyfrowa i zielona transformacja	Minister właściwy do spraw klimatu, Minister właściwy do spraw środowiska	Minister właściwy do spraw informatyzacji, Minister właściwy do spraw gospodarki, Minister właściwy do spraw gospodarki surowcami energetycznymi, Minister właściwy do spraw energii
	Cyfrowa modernizacja rolnictwa	Minister właściwy do spraw rolnictwa	Minister właściwy do spraw informatyzacji

VIII. Finansowanie

Działania zebrane i zaproponowane w Strategii mają charakter przekrojowy i wpływają na wiele obszarów, takich jak bezpieczeństwo państwa, utrzymanie konkurencyjności gospodarki, edukację czy postęp naukowy i technologiczny. Zaplanowane działania będą realizowane przez różne podmioty, z udziałem nakładów finansowych pochodzących w szczególności z następujących źródeł:

- budżet państwa – cele Strategii będą realizowane przez interwencje publiczne finansowane z części budżetu państwa poszczególnych ministrów. Ponadto z budżetu państwa będą pochodziły środki na współfinansowanie dla projektów realizowanych ze źródeł zagranicznych,

- budżety jednostek samorządu terytorialnego,

- środki innych podmiotów realizujących zadania publiczne,

- fundusze celowe m.in.: Fundusz Szerokopasmowy, Fundusz Cyberbezpieczeństwa, Fundusz - Centralna Ewidencja Pojazdów i Kierowców (CEPIK),

- Instrument na rzecz Odbudowy i Zwiększania Odporności (RRF): Krajowy Plan Odbudowy i Zwiększania Odporności (KPO),

- fundusze europejskie przeznaczone na realizację Polityki spójności (w tym Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Program Fundusze Europejskie dla Rozwoju Społecznego 2021-2027, Fundusze Europejskie dla Nowoczesnej Gospodarki), programy regionalne oraz Wspólnej polityki rolnej w perspektywie 2021–2027, jak również fundusze na perspektywę 2028-2034,

- inne instrumenty i programy europejskie m.in.: Instrument „Łącząc Europę” (Connecting Europe Facility, CEF), Program “Cyfrowa Europa” (Digital Europe Programme, DEP), Program “Horyzont Europa” (Horizon Europe), Program „Obywatele, Równość, Prawa i Wartości” (Citizens, Equality, Rights And Values Programme, CERV),

- inne środki publiczne, w tym środki ze źródeł zagranicznych (np. Norweski Mechanizm Finansowy), inne instrumenty funkcjonujące w oparciu o środki publiczne, jak np. instrumenty BGK w ramach oferty Grupy Polskiego Funduszu Rozwoju,

- instrumenty finansowe międzynarodowych instytucji finansowych (z kredytów, gwarancji, obejmowania udziałów, fundusze Venture Capital),

- środki prywatne – realizacja celów Strategii będzie wymagała również zaangażowania środków prywatnych, w szczególności w zakresie zapewnienia współfinansowania projektom współfinansowanym ze środków UE,

- Narodowy Fundusz Zdrowia (NFZ), a także współpłacenie pacjentów za świadczenia zdrowotne (np. w refundacji aptecznej) oraz współpłacenie przez dostawców technologii (np. instrumenty dzielenia ryzyka, podmioty zainteresowane dostępem do danych).

Strategia nie stanowi podstawy do zwiększenia limitu wydatków w ramach poszczególnych części budżetowych. Realizacja określonych w Strategii kierunków działania będzie odbywać się w ramach dotychczas posiadanych środków budżetowych w odpowiednich częściach budżetowych oraz w ramach reguł określonych w poszczególnych przepisach zarówno w roku wejścia w życie uchwały, jak i w latach następnych i nie może stanowić podstawy do ubiegania się o dodatkowe środki z budżetu państwa na ten cel. Według szacunków Ministerstwa Cyfryzacji wydatki na szeroko pojęty obszar cyfryzacji w 2025 r. wyniosą ponad 32 mld zł, co stanowi ok. 0,8 % PKB. Szacunki te zostały oparte na prognozie przepływów w części budżetowej 27 w ramach środków budżetu państwa oraz funduszy Unii Europejskiej (w tym w szczególności środków na Krajowy Plan Odbudowy i Zwiększania Odporności (KPO) i Fundusze Europejskie na Rozwój Cyfrowy (FERC))[177], analizie planów zamówień publicznych urzędów centralnych oraz wybranych jednostek samorządu terytorialnego. Na tej podstawie dokonano ekstrapolacji na wydatki ogółem.

Intensywny rozwój sfery cyfrowej i nowe wyzwania w tym obszarze przekładają się jednak na konieczność znaczącego zwiększenia poziomu inwestycji w sektorze. Bez zapewnienia odpowiednio wysokiego poziomu finansowania nie uda się bowiem zrealizować celów strategicznych i zagwarantować miejsca Polsce jako europejskiego lidera cyfryzacji. Wydatki na rozwój i utrzymanie systemów informatycznych będą rosły również ze względu na postępującą cyfryzację państwa. Nowe wydatki w tym zakresie będą jednak obniżały koszty w ujęciu globalnym.

Wsparciem dla wydatków krajowych będą środki europejskie z polityki spójności w perspektywie finansowej 2021-2027 oraz pochodzące z KPO (do 2026 r.). W ramach przeglądu śródokresowego polityki spójności, uwzględniając aktualne wyzwania wynikające z sytuacji geopolitycznej, KE akcentuje konieczność wsparcia działań, które zwiększą innowacyjność i konkurencyjność Europy, wzmocnią jej niezależność oraz pobudzą inwestycje w sektory kluczowe. Będzie to miało decydujący wpływ na kierunki finansowania działań w najbliższych latach. Państwa członkowskie będą dostosowywać swoje programy do nowych ram określonych przez Komisję Europejską, zakładających m.in. zwiększenie wsparcia inwestycji w technologie strategiczne (STEP), wzmocnienie zdolności cyfrowych oraz skalowanie innowacyjnych przedsiębiorstw.

Wsparcie będzie kontynuowane również w unijnej perspektywie finansowej na lata 2028-2034. Przewiduje się, że w perspektywie finansowej 2028-2034 znaczenie środków UE będzie nadal istotne, choć stanie się relatywnie mniejsze. W lipcu 2025 r. został opublikowany projekt Wieloletnich Ram Finansowych na lata 2028-2034, w którym zostały określone m.in. limity wydatków budżetu wieloletniego oraz ogólne kierunki przeznaczenia środków, w oparciu o które będą prowadzone negocjacje. W obszarze cyfryzacji priorytetem powinno stać się w szczególności wsparcie innowacji i transformacji technologicznej, rozwoju e-administracji i usług publicznych online, kompetencji cyfrowych oraz infrastruktury cyfrowej i łączności. Pozwoliłby to na wsparcie działań wskazanych w Strategii oraz w Krajowym planie działania do programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.

W systemie środków europejskich znacząco wzrasta wykorzystanie instrumentów zwrotnych. Systematycznie rosnąć będzie pula środków pochodzących ze spłat pożyczek, która – zgodnie z regulacjami europejskimi – może zostać ponownie wykorzystana, pod warunkiem

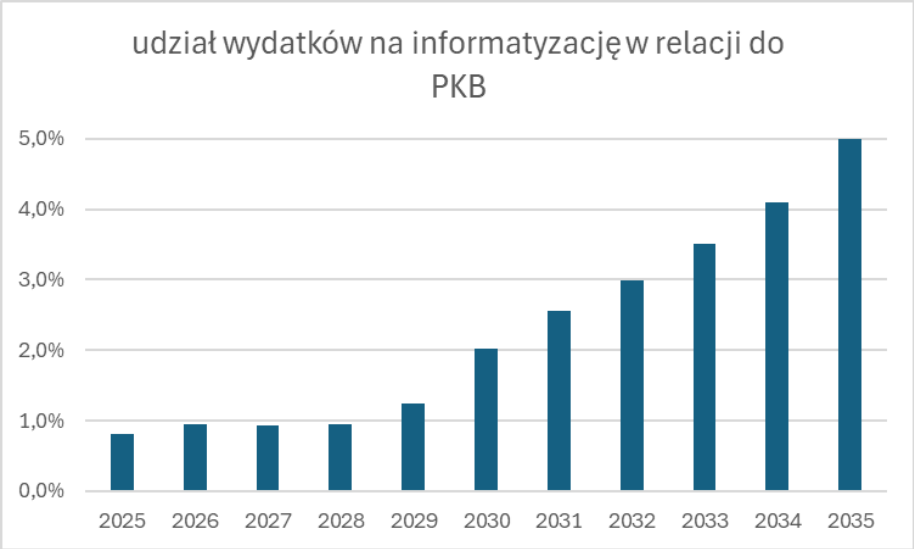
[177] Łącznie dla dysponenta I i III stopnia: 22,09 mld zł.

przeznaczenia tych środków na cele zgodne z celami programów, w ramach których instrumenty finansowe zostały ustanowione.

Interwencje publiczne będą w większym stopniu finansowane w oparciu o krajowe środki publiczne. Istotne będzie skoncentrowanie środków UE na projektach o najwyższej wartości dodanej i pozytywnych efektach zewnętrznych. Jednocześnie, biorąc pod uwagę potrzebę przeznaczenia znacznych środków na cyfryzację, konieczna może być zmiana struktury finansowania rozwoju branży, która w dużej mierze opiera się o kontrybucję sektora telekomunikacyjnego, a pomija innych graczy, korzystających ze wspólnej infrastruktury.

Sektor publiczny wspiera finansowanie transformacji cyfrowej, jednak dźwignią rozwoju muszą być również inwestycje prywatne. W Polsce, w porównaniu do innych państw europejskich, sektor prywatny inwestuje relatywnie niechętnie. W 2023 r. inwestycje sektora publicznego wyniosły 5% PKB (średnia UE 3,56%), natomiast inwestycje sektora prywatnego wyniosły 9,11% (średnia UE 12,97%). Polska zajmuje pod tym względem 4 miejsce od końca wśród państw członkowskich UE[178]. Niekorzystną sytuację pokazują również nieco starsze dane: udział inwestycji w technologie informacyjno-komunikacyjne w stosunku do PKB wyniósł w 2022 r. w Polsce 0,98%. Podczas gdy średnia dla UE to 2,97%[179]. Tym samym, by zrealizować ambitne cele strategiczne, konieczna będzie mobilizacja sektora prywatnego.

W przyjętym modelu założono, że do 2028 r. będą podejmowane działania zmierzające do wykonania programów obecnej perspektywy finansowej i utrzymanie rozwoju obecnych usług, to przełoży się na utrzymanie stabilnego poziomu wydatków na informatyzację w relacji do PKB. Po 2028 r. planuje się rozpoczęcie inwestycji w ramach nowych wieloletnich ram finansowych, a także kumulację wydatków utrzymaniowych w zakresie nowych usług, centrów danych i cyberbezpieczeństwa. Wydatki w 2030 r. mają osiągnąć poziom 2% PKB. Pułap 5% PKB planuje się uzyskać w 2035 r. Wydatki od 2026 r. będą mierzone według stałej metodologii opracowanej przez Ministerstwo Cyfryzacji we współpracy z właściwymi ośrodkami analitycznymi i w konsultacji z Ministerstwem Finansów.



Źródło: opracowanie własne MC

[178] https://ec.europa.eu/eurostat/databrowser/view/sdg_08_11/default/table?lang=en.
[179] https://goingdigital.oecd.org/indicator/30.

IX. Słownik

1) altruizm danych – zgodnie z art. 2 pkt 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniającego rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz. Urz. UE L 152 z 03.06.2022, str. 1, Dz. Urz. UE L 132 z 17.05.2023, str. 89 oraz Dz. Urz. UE L 2023/90204 z 21.12.2023) - dobrowolne dzielenie się danymi na podstawie wyrażonej przez osoby, których dane dotyczą, zgody na przetwarzanie dotyczących ich danych osobowych lub na podstawie udzielonego przez posiadaczy danych pozwolenia na wykorzystywanie ich danych nieosobowych, bez żądania ani otrzymania za to wynagrodzenia wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych do celów leżących w interesie ogólnym określonych – w stosownych przypadkach – w prawie krajowym, takich jak opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie polityki publicznej lub do celów badań naukowych leżących w interesie ogólnym;

2) Architektura Informacyjna Państwa (AIP) – zgodnie z art. 3 pkt 29 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160) - metoda zarządzania informatyzacją państwa, oparta na modelach architektonicznych i obejmująca zasady podstawowe (pryncypia), standardy, wytyczne i rekomendacje architektoniczne;

3) blockchain - złożona kombinacja technologii kryptograficznych i technologii systemów rozproszonych, pozwalająca potwierdzać prawdziwość danych w różnych procesach transakcyjnych. Pozwala stronom, które się nie znają, zaufać procesom, procedurom lub pomiarom, bez potrzeby angażowania pośredników, którzy mieliby takie zaufanie gwarantować. Niekiedy kojarzona również z pojęciem WEB 3.0.;

4) Centra Wymiany i Analizy Informacji (ang. Information Sharing and Analysis Center, ISAC) - centra wymiany wiedzy i doświadczeń dotyczących incydentów cyberbezpieczeństwa w danym sektorze gospodarki;

5) chmura obliczeniowa (ang. cloud computing) - model przetwarzania umożliwiający powszechny i wygodny dostęp za pośrednictwem sieci do wspólnej puli konfigurowalnych zasobów przetwarzania (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które mogą być szybko udostępniane przy minimalnym wysiłku ze strony zespołów zarządzania lub dostawcy usług;

6) CSIRT poziomu krajowego – zespoły reagowania na incydenty bezpieczeństwa komputerowego, o których mowa w art. 2 pkt 1-3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252), realizujące zadania określone w art. 26 tej ustawy;

7) CSRD (ang. Corporate Sustainability Reporting Directive) – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2464 z dnia 14 grudnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 537/2014, dyrektywy 2004/109/WE, dyrektywy 2006/43/WE oraz dyrektywy 2013/34/UE w odniesieniu do sprawozdawczości przedsiębiorstw w zakresie zrównoważonego rozwoju (Dz. Urz. UE L 322 z 16.12.2022, str. 15, Dz. Urz. UE L 2025/794 z 16.04.2025, Dz. Urz. UE L 2025/90790 z 08.10.2025 oraz z Dz. Urz. UE L 2026/470 z 26.02.2026). Dyrektywa nakłada m.in. obowiązek raportowania kwestii związanych z ryzykiem klimatycznym;

8) deep tech - najnowocześniejsze i przełomowe technologie, których fundamentalnym założeniem jest wykorzystanie odkryć naukowych, innowacji inżynieryjnych lub postępów w dziedzinach badań, mających potencjał radykalnej transformacji przemysłu, gospodarki i życia.

9) DESI (ang. Digital Economy and Society Index) – indeks gospodarki cyfrowej i społeczeństwa cyfrowego stworzony na zlecenie Komisji Europejskiej jako narzędzie monitorujące wskaźniki postępu cyfrowego państw członkowskich UE;

10) dostępność cyfrowa - projektowanie i tworzenie m.in. stron internetowych, aplikacji mobilnych oraz usług cyfrowych w sposób umożliwiający samodzielne i wygodne korzystanie z nich wszystkim osobom, niezależnie od wieku, poziomu sprawności czy używanego urządzenia;

11) dyplomacja cyfrowa - strategiczne podejście do globalnych spraw cyfrowych, które ma na celu wzmocnienie roli i pozycji państwa w międzynarodowym ładzie cyfrowym;

12) elektroniczne doręczenia (tzw. e-Doręczenia) – uregulowane ustawą z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3 i 507), obejmujące publiczną usługę rejestrowanego doręczenia elektronicznego, publiczną usługę hybrydową oraz kwalifikowaną usługę rejestrowanego doręczenia elektronicznego. Dzięki tej usłudze podmioty publiczne, obywatele i firmy mogą korzystać z wygodnych i bezpiecznych doręczeń elektronicznych. Są one równoważne prawnie tradycyjnej przesyłce poleconej za potwierdzeniem odbioru;

13) elektroniczna platforma usług administracji publicznej (ePUAP) - system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet (art. 3 pkt 13 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne);

14) Ekosystem AI – ma charakter horyzontalnego środowiska inicjującego i wspierającego działania podejmowane przez szerokie grono interesariuszy na rzecz rozwoju polskiej innowacyjności w obszarze AI i pozycjonowania polskiej własności intelektualnej na możliwie wysokich poziomach globalnego łańcucha wartości. W przypadku Polski kluczowe podmioty funkcjonujące w ramach Ekosystemu to: uczelnie, ośrodki badawcze, centra badawczo-rozwojowe, przedsiębiorstwa, organy administracji publicznej oraz organizacje społeczne;

15) Europejskie Ramy Interoperacyjności (ang. European Interoperability Framework, EIF) – unijne wspólnie uzgodnione podejście do świadczenia europejskich usług użyteczności publicznej w sposób interoperacyjny. Określono w nich podstawowe wytyczne dotyczące interoperacyjności w formie wspólnych zasad, modeli i zaleceń;

16) fundusze Venture Capital (fundusze VC) – model finansowania inwestycji w przedsięwzięcia biznesowe na wczesnym etapie rozwoju, charakteryzujący się wysoką stopą ryzyka. Fundusze VC z reguły inwestują w przedsięwzięcia innowacyjne, tworzone przez niewielkie firmy, licząc na wysoką stopę zwrotu;

17) fundusze Private Equity (fundusze PE) - model finansowania, w ramach którego gromadzone środki inwestowane są w przedsiębiorstwa o dużym potencjale wzrostu wartości. W odróżnieniu od funduszy VC, fundusze PE inwestują także w firmy na późniejszych etapach rozwoju;

18) generatywna sztuczna inteligencja (GenAI) - technologia, która za pomocą poleceń, pozwala użytkownikom tworzyć nowe treści. Algorytmy GenAI działają w oparciu o dane dostarczone zarówno na etapie tworzenia narzędzia, jak i te wprowadzone w trakcie użytkowania;

19) hackaton - wydarzenie, podczas którego programiści, projektanci i inni specjaliści współpracują intensywnie w celu rozwiązania określonego problemu lub stworzenia nowego produktu w krótkim czasie, zazwyczaj od 24 do 72 godzin;

20) ICT (ang. Information and Communication Technologies) - rodzina technologii umożliwiających przetwarzanie, gromadzenie i przesyłanie informacji w formie elektronicznej;

21) inteligentne miasto (ang. smart city) - obszar miejski, w którym technologia i gromadzenie danych pomagają poprawić jakość życia, a także zrównoważony rozwój i wydajność działania miasta. Jedną z technologii wykorzystywanych w ramach inteligentnych miast jest Internet Rzeczy (IoT);

22) inteligentna wieś (ang. smart village) –- obszar wiejski, który wykorzystuje nowoczesne technologie w celu zrównoważonego i innowacyjnego rozwoju oraz w celu poprawy jakości i poziomu życia jej mieszkańców;

23) interfejs programistyczny aplikacji (ang. application programming interface, API) – zbiór technicznych funkcji umożliwiających połączenie i wzajemną wymianę danych lub metadanych między programami komputerowymi lub systemami teleinformatycznymi (art. 2 pkt 9 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524));

24) Internet Rzeczy (ang. Internet of Things, IoT) – systemy, składające się z połączonych urządzeń często nazywanych "inteligentnymi". Urządzenia te zbierają i wymieniają między sobą dane oraz mogą być sterowane i monitorowane przez Internet;

25) MŚP - mikroprzedsiębiorstwo lub małe lub średnie przedsiębiorstwo w rozumieniu zalecenia Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczącego definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. Urz. UE L 124 z 20.05.2003, str. 36 oraz Dz. Urz. UE L 2024/90772 z 05.12.2024);

26) Ogólnopolska Sieć Edukacyjna (OSE) – zgodnie z art. 2 ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (Dz. U. z 2024 r. poz. 1768) publiczna sieć telekomunikacyjna służąca świadczeniu publicznie dostępnych usług telekomunikacyjnych szkole w rozumieniu art. 2 pkt 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2025 r. poz. 1043, z późn. zm.), z wyjątkiem szkół dla dorosłych;

27) otwarte oprogramowanie (ang. open-source) – rodzaj oprogramowania, którego kod źródłowy jest publicznie dostępny i może być swobodnie modyfikowany oraz dystrybuowany przez użytkowników;

28) PLGrid - ogólnopolska infrastruktura obliczeniowa zbudowana w celu wsparcia badań naukowych i prac rozwojowych dla wielu dziedzin nauki i gospodarki. W ramach PLGrid możliwy jest dostęp do superkomputerów, komputerów kwantowych, specjalizowanych akceleratorów dla sztucznej inteligencji, chmury obliczeniowej, pamięci dyskowych, zoptymalizowanego oprogramowania obliczeniowego oraz wsparcia ekspertów z całej Polski;

29) poziomy dojrzałości e-usług**:**
    a) I – poziom informacyjny – możliwość wyszukania na stronie internetowej lub BIP urzędu informacji o urzędzie oraz świadczonych usługach,

b) II – poziom interakcji jednokierunkowej – możliwość wyszukania informacji oraz pobrania oficjalnych formularzy ze strony internetowej lub BIP urzędu,

c) III – poziom interakcji dwukierunkowej – możliwość wyszukania informacji i pobrania oficjalnych formularzy, a także możliwość odesłania wypełnionych formularzy drogą elektroniczną,

d) IV – poziom transakcji – pełna obsługa procesu – możliwość uzyskania informacji, pobrania i odesłania formularzy, a także uiszczenia wymaganych opłat oraz otrzymania oficjalnego pozwolenia, zaświadczenia lub innego dokumentu, o który dana osoba/firma występuje,

e) V – poziom spersonalizowany – pełna obsługa sprawy urzędowej drogą elektroniczną wraz z personalizacją obsługi (automatyczne dostarczenie konkretnych, spersonalizowanych usług, nieinicjowanych przez użytkownika, np. decyzja w sprawie wymiaru podatku od nieruchomości);

30) Przemysł 4.0 – termin odnoszący się do czwartej rewolucji przemysłowej, która oznacza integrację inteligentnych maszyn, systemów oraz wprowadzanie zmian w procesach produkcyjnych mających w celu zwiększania wydajności wytwarzania oraz wprowadzenie możliwości elastycznych zmian asortymentu. Przemysł 4.0 dotyczy nie tylko technologii, ale też nowych sposobów pracy i roli ludzi w przemyśle;

31) rejestr publiczny – zgodnie z art. 3 pkt 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne zbiór danych służący do realizacji zadań publicznych, prowadzony na podstawie przepisów ustawowych, przez podmiot realizujący zadania publiczne;

32) rozporządzenie eIDAS 2.0 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. Urz. UE L 2024/1183 z 30.04.2024, Dz. Urz. UE L 2025/90317 z 09.04.2025 oraz Dz. Urz. UE L 2025/90945 z 24.11.2025);

33) rozporządzenie GIA (ang. Gigabit Infrastructure Act) - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1309 z dnia 29 kwietnia 2024 r. w sprawie środków mających na celu zmniejszenie kosztów wdrażania gigabitowych sieci łączności elektronicznej, zmieniające rozporządzenie (UE) 2015/2120 i uchylające dyrektywę 2014/61/UE (akt w sprawie infrastruktury gigabitowej) (Dz. Urz. UE L 2024/1309 z 08.05.2024 oraz Dz. Urz. UE L 2024/90315 z 24.05.2024);

34) rzeczywistość rozszerzona (ang. Extended Reality, XR) – grupa technologii, które łączą świat wirtualny z rzeczywistym. XR to parasolowe pojęcie, obejmujące: VR (Virtual Reality / rzeczywistość wirtualna), AR (Augmented Reality / rzeczywistość rozszerzona) oraz MR (Mixed Reality / rzeczywistość mieszana);

35) srebrna gospodarka, również gospodarka senioralna - sektor gospodarki ukierunkowany na osoby starsze;

36) startup - dynamiczna, zazwyczaj młoda firma lub projekt, który ma na celu wprowadzenie innowacyjnego produktu, usługi lub rozwiązania na rynek, poszukująca modelu biznesowego, który zapewniłby jej zyskowny rozwój;

37) STEM (ang. science, technology, engineering, mathematics) – skrót oznaczający naukę, technologię, inżynierię, matematykę. Jest to termin używany do określenia tych czterech dziedzin, które są ze sobą powiązane i mają kluczowe znaczenie w kontekście edukacji oraz rozwoju zawodowego;

38) system EZD – system teleinformatyczny do elektronicznego zarządzania dokumentacją umożliwiający wykonywanie w nim czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych (§ 2 pkt 13 rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. poz. 67 i 140));

39) system EZD RP - system klasy EZD, którego możliwości, budowa i oferowane funkcje realizują rzeczywiste potrzeby biznesowe polskiej administracji publicznej. EZD RP powstał w ramach projektu realizowanego przez NASK w partnerstwie z Wojewodą Podlaskim. Jest wdrażany w środowiskach produkcyjnych kolejnych jednostek administracji publicznej i usprawnia ich funkcjonowanie poprzez udostępnienie nowoczesnych i uniwersalnych rozwiązań cyfrowych back-office w obszarze elektronicznego zarządzania dokumentacją;

40) System Inwentaryzacji Systemów Teleinformatycznych (SIST) –-zgodnie z art. 20ga ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, system teleinformatyczny prowadzony przez ministra właściwego do spraw informatyzacji służący do zbierania informacji o planowanych, istniejących i wycofanych systemach teleinformatycznych, współpracy pomiędzy nimi, rejestrach prowadzonych przez administrację publiczną oraz możliwościach wykorzystania zbieranych w nich informacji;

41) system teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252) (art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne);

42) system zarządzania cyberbezpieczeństwem S46 – system teleinformatyczny, który wspiera zgłaszanie i obsługę incydentów, wymianę informacji i współpracę pomiędzy uczestnikami krajowego systemu cyberbezpieczeństwa (KSC). Zapewnia również szacowanie ryzyka na poziomie krajowym i ostrzeganie o zagrożeniach cyberbezpieczeństwa;

43) Sztuczna Inteligencja (ang. Artificial Intelligence, AI/SI) - dziedzina wiedzy obejmująca m.in. sieci neuronowe, robotykę i tworzenie modeli zachowań inteligentnych oraz programów komputerowych symulujących te zachowania, włączając w to również uczenie maszynowe (ang. machine learning), głębokie uczenie (ang. deep learning) oraz uczenie wzmocnione (ang. reinforcement learning);

44) umiejętności cyfrowe[180] - zestaw określonych umiejętności cyfrowych służący do rozróżniania poziomu kompetencji cyfrowych wśród społeczeństwa, używany przez urzędy statystyczne, składa się z pięciu podkategorii, są to umiejętności cyfrowe z konkretnych rodzajów: umiejętności w zakresie korzystania z informacji i danych, komunikacji i współpracy, tworzenia treści cyfrowych, bezpieczeństwa oraz rozwiązywania problemów:

[180] Według Europejskich Ram Kompetencji Cyfrowych – DIGICOMP, https://www.digcomp.pl/download/raport-eccc-digcomp-pl/?wpdmdl=396&masterkey=56f68effb867e.

a) osoby posiadające podstawowe umiejętności cyfrowe – osoby, które korzystały z internetu w ciągu ostatnich 3 miesięcy i posiadały 5 z 5 wyżej wymienionych cyfrowych umiejętności, ale co najmniej jeden rodzaj na poziomie podstawowym,

b) osoby posiadające ponadpodstawowe umiejętności cyfrowe – osoby, które korzystały z internetu w ciągu ostatnich 3 miesięcy i posiadały 5 z 5 wyżej wymienionych cyfrowych umiejętności, a do tego każdy rodzaj był na poziomie ponadpodstawowym;

45) wysokowydajne przetwarzanie komputerowe (ang. High-performance computing, HPC) – zaawansowana infrastruktura obliczeniowa przeznaczona do realizacji najbardziej wymagających zadań naukowych, inżynieryjnych oraz komercyjnych;

46) zasada bezpieczeństwo w fazie projektowania (ang. security by design) - podejście, które zakłada, że bezpieczeństwo systemów informatycznych powinno być integralną częścią procesu projektowania i tworzenia;

47) zasada etyki na etapie projektowania (ang. ethics by design) - podejście, które integruje kwestie etyczne na etapie projektowania technologii, w szczególności w kontekście sztucznej inteligencji (AI) i innych nowoczesnych rozwiązań technologicznych;

48) zasada otwartości w fazie projektowania i otwartości domyślnej – podejście, które promuje dostępność danych i informacji w sposób umożliwiający ich swobodne wykorzystanie i ponowne wykorzystywanie, już na etapie projektowania;

49) zasada prywatności w fazie projektowania (ang. privacy by design) - podejście, które zakłada, że kwestie związane z prywatnością (ochroną danych osobowych) powinny być integralną częścią procesu projektowania systemów, aplikacji i usług.