DOI: https://doi.org/10.13166/zar/EUOT9930

ADAM ŻYCZKOWSKI
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie

OCHRONA DANYCH OSOBOWYCH W KONTEKŚCIE ZMIAN WYNIKAJĄCYCH Z TRANSFORMACJI CYFROWEJ

PERSONAL DATA PROTECTION IN THE CONTEXT OF CHANGES RESULTING FROM DIGITAL TRANSFORMATION

Abstract

Due to the changing legal environment for data processing organizations, it seems justified to try to answer the question whether this change in the environment requires the reconstruction of IT systems and applications controlling and supporting the actual implementation of the rights of data subjects.

Considering this research question, it is necessary to refer to the legal literature in the field of European and Polish data protection law. It is also necessary to analyze the changing environment, which has a major impact on the pace of evolution within the issues and theses discussed in this article.

The applied methodology takes into account market research methods to the extent necessary to indicate the category of IT solutions that can meet the individual requirements of the GDPR, while the study of the legal literature is necessary, but may not give satisfactory results due to the short period of their use. The research results, as well as the legal analysis, focus on typical legal issues, not on praxeological or economic issues.

It is assumed that based on the analysis of solutions available on the IT market and legal analysis in the context of the basic requirements for personal data administrators, it will be possible to formulate certain directive safeguards that will contribute to the improvement of compliance processes in the field of personal data, taking into account legal and economic approaches appropriate to grades.

Keywords: *Personal data protection, digital transformation, DESI report.*

Wprowadzenie

W celu stworzenia spójnego systemu zapewnienia cyberbezpieczeństwa podmiotów w RP w dniu 5 lipca 2018 r., uchwalono ustawę o Krajowym Systemie Cyberbezpieczeństwa. Ustawa weszła w życie 28 sierpnia 2018 r. W ten sposób opracowano zestaw wytycznych mających na celu podejmowanie skutecznych działań w celu wykrywania, zapobiegania i minimalizowania skutków incydentów cybernetycznych (takich jak cyberataki czy awarie), które naruszają bezpieczeństwo cybernetyczne państwa i bezpieczeństwo jego obywateli. Krajowy System Cyberbezpieczeństwa opiera się na przepisach ustawy z dnia 5 lipca 2018 r., która określa ramy prawne niezbędne do zapewnienia ochrony przed różnymi zagrożeniami występującymi w cyberprzestrzeni. Ustawa i towarzyszące jej regulacje administracyjne w pełni implementują tzw. Dyrektywę NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie wysokiej ogólnej dostępności i bezpieczeństwa sieci na terenie Unii Europejskiej[1]).

Nowy reżim prawny i trwająca przebudowa praw podmiotowych w zakresie RODO ma na celu wzmocnienie ochrony prywatności, a w szczególności skuteczności prawa na potrzebę ochrony człowieka i jego statusu prawnego w społeczeństwie informacyjnym, a z drugiej jest to odpowiedź na wyzwania związane z rozwojem technologii informacyjnej i procesem globalizacji[2]. Powołanie organów nadzorczych w każdym kraju UE oraz rozbudowa ich narzędzi kontrolnych i sankcyjnych doprowadziło do zwiększenia regulacji przetwarzania danych osobowych w systemach informatycznych. Uznanie omawianych regulacji i ich wdrożenie, jest szczególnie ważne dla odbiorców RODO. Stoją oni przed koniecznością reorganizacji i dokonują nowych wyborów ekonomicznych, w obszarze wykorzystywanych przez siebie systemów informatycznych. Spośród podmiotów przetwarzających dane osobowe w systemach informatycznych, wymienimy „aktorów" na rynku IT, czyli producentów i nabywców rozwiązań informatycznych.

Warto w tym miejscu dodać, że pełny koszt przestrzegania przepisów RODO, ponosi administrator danych osobowych. Jego działalność wymaga zatem wsparcia technicznego, które ma na celu wywiązanie się z nałożonych na niego obowiązków – które są jednocześnie istotne ze względu na ryzyko prawne, jakim jest odpowiedzialność za ich niewykonanie. Ze względu na zmienia-

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii; https://eur-lex.europa.eu/legal-content/pl/all/?uri=celex%3a32016l1148, dostęp 02-0502022r.

[2] Safjan M., Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym, Państwo i Prawo, 2002

jące się otoczenie prawne dla organizacji przetwarzających dane, wydaje się zasadnym, aby spróbować odpowiedzieć na pytanie, czy ta zmiana otoczenia wymaga przebudowania systemów i aplikacji informatycznych kontrolujących i wspierających faktyczną realizację praw osób, których dane dotyczą.

Rozważając to pytanie badawcze, konieczne jest odniesienie się do literatury prawnej z zakresu europejskiego i polskiego prawa dot. ochrony danych osobowych. Niezbędną jest również analiza zmieniającego się otoczenia, które ma główny wpływ na tempo ewolucji w obrębie omawianych w tym artykule kwestii i stawianych tez.

Zastosowana metodologia uwzględnia metody badania rynku w zakresie niezbędnym do wskazania kategorii rozwiązań informatycznych, które mogą spełnić indywidualne wymagania RODO, natomiast badanie literatury prawniczej jest niezbędne, ale może nie dać satysfakcjonujących rezultatów ze względu na krótki okres ich użytkowania. Wyniki badań, jak również analiza prawna, skupiają się na typowych zagadnieniach prawnych, a nie na zagadnieniach prakseologicznych czy ekonomicznych.

Zakłada się, że na podstawie analizy rozwiązań dostępnych rynku IT oraz analizy prawnej w kontekście podstawowych wymagań dla administratorów danych osobowych, możliwe będzie sformułowanie pewnych zabezpieczeń dyrektywnych, które przyczynią się do usprawnienia procesów compliance w zakresie danych osobowych, z uwzględnieniem podejść prawnych i ekonomicznych odpowiednich do oceny.

Podstawowe definicje i analiza zmian w otoczeniu na podstawie raportu DESI

Rozważania dotyczące ochrony danych osobowych warto rozpocząć od terminu, które przybliżą nam naturę tego pojęcia. Zgodnie z definicją zaprezentowaną przez Parlament Europejski:

„Dane osobowe oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoba, której dane dotyczą"). Osoba możliwa do zidentyfikowania to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość"[3].

[3] Dane osobowe, definicja: https://www.europarl.europa.eu/privacy-policy/pl/data-protection, Dostęp: 17.02.2022 r.

Transformacja cyfrowa rozumiana jako zjawisko, które polega na wprowadzaniu i właściwym wykorzystaniu rozwiązań opartych na nowoczesnych technologiach cyfrowych[4] – wpływa na wszystkie dziedziny życia, w tym edukację. Im szersze zastosowanie nowoczesnych technologii, tym większe zapotrzebowanie na osoby, które nie tylko umieją i mogą z nich korzystać, ale także projektować, wytwarzać i pracować z ich udziałem. Organizacje międzynarodowe od lat podkreślają wagę rozwijania zdolności cyfrowych, ale przed okresem pandemii COVID-19, aktywności w tym obszarze nie można było opisywać jako nadmiernie rewolucyjnej. Zasadniczo okres pandemii, który dotknął niemal każdy kraj na świecie, wymuszając m.in. zamknięcie szkół i firm, spowodował, że w efekcie edukacja i praca przeniosły się do przestrzeni wirtualnych. Wizje przyszłości, w tym cyfryzacja edukacji, ziściły się niemal z dnia na dzień i nie ma obecnie odwrotu dla tych procesów. Pandemia przyspieszyła cyfrową rewolucję zarówno w edukacji, jak i przyszłym rynku pracy.

Rozwój polskiej gospodarki zależy od wielu aspektów, do których w obecnych czasach z całą pewnością można zaliczać odpowiednio przeprowadzoną transformację cyfrową. W roku 2022, polskie przedsiębiorstwa, polscy pracownicy i polskie instytucje są daleko w tyle pod względem cyfryzacji, co wyraźnie widać, kiedy analizujemy wyniki rankingu DESI[5].

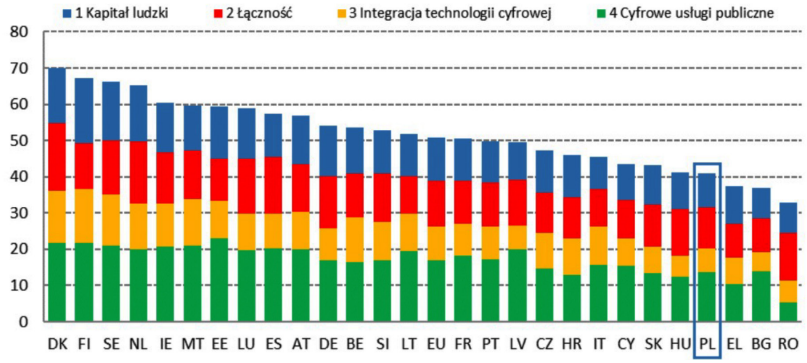
W opublikowanym przez Komisję Europejską rankingu Digital Economy and Society Index (DESI) z 2021 r., Polska zajmuje dopiero 24 miejsce wśród 27 państw członkowskich UE. Jest to spadek o jedną pozycję w stosunku do poprzedniego roku. Za Polską pozostają tylko Grecja, Bułgaria i Rumunia. Autorzy zestawienia wyjaśniają, że Polska poprawiła wiele wskaźników składających się na główny wskaźnik, ale ogólna pozycja kraju nie uległa poprawie ze względu na podobne zmiany w innych krajach w związku z pandemią COVID-19. Warto w tym miejscu dodać, że liderami rankingu są: Dania, Finlandia i Szwecja. Należy również zauważyć, że obecnie ranking ten obejmuje 4 kategorie (kapitał ludzki, łączność,

[4] Transformacja cyfrowa, definicja: https://www.sap.com/poland/insights/what-is-digital-transformation.html, Dostęp: 17.02.2022 r.

[5] Digital Economy and Society Index (DESI) 2021: https://digital-strategy.ec.europa.eu/en/policies/desi, dostęp: 18.02.2022 r.

integracja technologii cyfrowych i cyfrowe usługi publiczne), zamiast wcześniej ocenianych 5-ciu. Modyfikacja wynikała z faktu dostosowania obszarów objętych transformacji zgodne z głównymi kierunkami wskazanymi przez Komisję Europejską w „Kompasie”[6], a mianowicie umiejętnościami dotyczącymi bezpiecznej i zrównoważonej infrastruktury, transformacją korporacyjną oraz cyfryzacją usług publicznych.

Rysunek 1. Ranking Indeksu gospodarki cyfrowej i społeczeństwa cyfrowego, 2021



Źródło: Digital Economy and Society Index (DESI) 2021

Transformacja cyfrowa to ogromny wysiłek jaki powinny podjąć wszystkie państwa rozwijające się. Wiąże się to głównie ze zmianami organizacyjnymi, które powinny być dokonane przede wszystkim na poziomie przedsiębiorstw. Polskie firmy nie wykorzystują szans, jakie daje rewolucja cyfrowa. W tym kontekście instytucje krajowe powinny określić kierunek rozwoju, aby stworzyć jak najkorzystniejsze warunki do wdrażania technologii cyfrowych, wyposażając obywateli i przedsiębiorstwa w odpowiednie narzędzia potrzebne w procesie transformacji cyfrowej. Kraje powinny budować odpowiednią infrastrukturę fizyczną (światłowód, 5G) i prawną (zagwarantować cyberbezpieczeństwo, ochronę prywatności czy bezpieczeństwo danych). Co jednak nie mniej ważne, cyfrowa transformacja, która dotyczy zarządzania

[6] Komunikat komisji do parlamentu europejskiego, rady, europejskiego komitetu konomiczno-społecznego i komitetu regionów, cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a52021dc0118, dostęp: 18.02.2022 r.

zasobami ludzkimi i gospodarkami, wymaga jednocześnie przekształcenia organizacji (w tym również instytucji publicznych) w takie, które są bardziej niż kiedykolwiek skoncentrowane na obywatelach i biznesie, szczególnie w obszarze ochrony osobowych.

Zgodnie z wynikami analizy danych przedstawionych w DESI[7], jednym z celów Cyfrowego Kompasu[8] jest to, aby do 2030 r. co najmniej 80% obywateli UE posiadało przynajmniej podstawowe umiejętności cyfrowe. W 2019 roku było to tylko 56%, a 84% regularnie korzystało z Internetu. Dane z raportu pokazują, że Finlandia przodowała pod względem kapitału ludzkiego, a tuż za nią były Szwecja, Holandia i Dania. Najgorzej wypadły pod tym względem Włochy, Rumunia i Bułgaria. W porównaniu z ubiegłym rokiem największy wzrost kapitału ludzkiego odnotowano w Finlandii (+2,6 punktu procentowego), Estonii (+1,7 punktu procentowego) i Grecji (+1,6 punktu procentowego). W rok 2020, 91% gospodarstw miało dostęp do Internetu w domu. 86% to stali użytkownicy Internetu (korzystało z niego przynajmniej raz w tygodniu), a prawie 80% korzystało z niego codziennie lub prawie codziennie.

W kategorii kapitał ludzki Polska zajmuje 24 miejsce wśród 27 krajów UE i tym samym plasuje się poniżej średniej UE. Poziom umiejętności cyfrowych pozostaje niski w porównaniu ze średnią UE – tylko 44 % osób w wieku 16-74 lata posiada przynajmniej podstawowe umiejętności cyfrowe (UE 56 %), a tylko jedna na pięć osób (21 %) posiada drugorzędne umiejętności cyfrowe. Pod względem przynajmniej podstawowych umiejętności informatycznych Polska uzyskała wynik zaledwie 46%, znacznie poniżej średniej UE wynoszącej 58%.

[7] Digital Economy and Society Index (DESI) 2021: https://digital-strategy.ec.europa.eu/en/policies/desi, dostęp: 18.02.2022 r.

[8] ibidem

Rysunek 2. Wskaźniki kapitału ludzkiego w DESI

	Polska			UE
	DESI 2019	DESI 2020	DESI 2021	DESI 2021
1a1 Co najmniej podstawowe umiejętności cyfrowe % osób	46% 2017	44% 2019	44% 2019	56% 2019
1a2 Ponadpodstawowe umiejętności cyfrowe % osób	21% 2017	21% 2019	21% 2019	31% 2019
1a3 Co najmniej podstawowe umiejętności informatyczne % osób	49% 2017	46% 2019	46% 2019	58% 2019
1b1 Specjaliści w dziedzinie ICT % osób pracujących w wieku 15–74 lat	3,0% 2018	3,1% 2019	3,4% 2020	4,3% 2020
1b2 Kobiety-specjaliści w dziedzinie ICT % specjalistów w dziedzinie ICT	14% 2018	14% 2019	15% 2020	19% 2020
1b3 Przedsiębiorstwa zapewniające szkolenia z zakresu ICT % przedsiębiorstw	13% 2018	13% 2019	18% 2020	20% 2020
1b4 Absolwenci kierunków w dziedzinie ICT % absolwentów	3,5% 2017	3,8% 2018	3,8% 2019	3,9% 2019

Źródło: Digital Economy and Society Index (DESI) 2021

Autorzy raportu zauważyli, że Polska zajmuje 21 miejsce w kategorii „Łączność". W 2020 roku Polska odnotowała wzrost odsetka gospodarstw domowych objętych sieciami stacjonarnymi o bardzo dużych prędkościach – 64,6% w porównaniu do 60,3% w 2019 roku. Wartość ta plasuje Polskę powyżej średniej unijnej dla tego wskaźnika (59,3%). Odnotowano również wzrost zasięgu łączy FTTP (Fiber-to-the-Premises) w Polsce – 44,6% w 2020 r., wobec 38,3% w 2019 r. Łącza FTTP na obszarach wiejskich pozostają na niższym poziomie – tylko 24,1% wiejskie gospodarstwa domowe były objęte tą technologią w 2020 r. (nieco poniżej średniej unijnej wynoszącej 24,9%). W porównaniu z 2019 r., kiedy 17,9% wiejskich gospodarstw domowych miało dostęp do tej technologii, widoczna jest tendencja wzrostowa.

Rysunek 3. Wskaźniki w kategorii Łączność w DESI

	Polska			UE
	DESI 2019	DESI 2020	DESI 2021	DESI 2021
2a1 Ogólne wykorzystanie stałych łączy szerokopasmowych % gospodarstw domowych	**60%** 2018	**62%** 2019	**68%** 2020	**77%** 2020
2a2 Wykorzystanie stałych łączy szerokopasmowych o prędkości co najmniej 100 Mb/s % gospodarstw domowych	**23%** 2018	**28%** 2019	**37%** 2020	**34%** 2020
2a3 Wykorzystanie łączy o prędkości co najmniej 1 Gb/s % gospodarstw domowych	**brak danych**	**0,47%** 2019	**1,10%** 2020	**1,3%** 2020
2b1 Zasięg szybkich łączy szerokopasmowych (dostęp nowej generacji) % gospodarstw domowych	**67%** 2018	**76%** 2019	**76%** 2020	**87%** 2020
2b2 Zasięg stałych sieci o bardzo dużej przepływności % gospodarstw domowych	**29%** 2018	**60%** 2019	**65%** 2020	**59%** 2020
2c1 Zasięg sieci 4G % obszarów zaludnionych	**>99,9%** 2018	**99,9%** 2019	**>99,9%** 2020	**99,7%** 2020
2c2 Gotowość na 5G Przyznane pasmo jako % całkowitego zharmonizowanego widma 5G	**0%** 2019	**0%** 2020	**0%** 2021	**51%** 2021
2c3 Zasięg sieci 5G % obszarów zaludnionych	**brak danych**	**brak danych**	**10%** 2020	**14%** 2020
2c4 Wykorzystanie mobilnych usług szerokopasmowych % osób	**47%** 2018	**58%** 2019	**58%** 2019	**71%** 2019
2d1 Wskaźnik cen łączy szerokopasmowych Wynik (0–100)	**brak danych**	**81** 2019	**88** 2020	**69** 2020

Źródło: Digital Economy and Society Index (DESI) 2021

Jeśli chodzi o korzystanie ze stacjonarnych łączy szerokopasmowych, 68% gospodarstw domowych miało dostęp do różnego rodzaju sieci szerokopasmowej w 2020 r., co stanowiło niewielki wzrost w porównaniu do 62% gospodarstw domowych w 2019 r. Polska osiągnęła dobre wyniki w zakresie dostępu do stacjonarnych łączy szerokopasmowych o przepływności co najmniej 100 Mb/s – 37% polskich gospodarstw domowych korzystało z takich łączy w 2020 r., co dla tego samego wskaźnika jest powyżej średniej unijnej wynoszącej 34%. Jeśli chodzi o zasięg 5G, 10,3% gospodarstw domowych było objętych tą technologią w 2020 r., nieco poniżej średniej UE wynoszącej 13,8% dla tego samego wskaźnika. Chociaż zasięg 4G wynosił 99,9%, wykorzystanie mobilnych usług szerokopasmowych (58%) jest znacznie poniżej średniej UE (71%).

Jeśli chodzi o publiczne finansowanie wdrażania infrastruktury (zarówno stacjonarnej, jak i bezprzewodowej), polskie władze – zgodnie z konkluzjami autorów raportu – planowały kontynuację realizacji Programu Operacyjnego Polska Cyfrowa[9] w latach 2021-2027. Warto przypomnieć, że program ten jest finansowany z funduszy spójności UE i w swych założeniach ma wspierać

[9] https://www.polskacyfrowa.gov.pl/strony/o-programie/, dostep 21.02.2022 r.

projekty w obszarach, w których sieci dostępowe nowej generacji nie istnieją i prawdopodobnie nie zostaną rozwinięte na zasadach komercyjnych w ciągu najbliższych 3 lat.

Innym źródłem środków publicznych służących wspieraniu inwestycji we wdrażanie sieci dostępowych nowej generacji w Polsce jest Fundusz Szerokopasmowy[10], który rozpoczął działalność pod koniec 2020 roku. Fundusz jest finansowany z opłat wnoszonych przez przedsiębiorców telekomunikacyjnych za prawo do korzystania z numeracji zasobów, prawa do użytkowania widma radiowego itp.

W swoim planie działania na rzecz wdrożenia wspólnego unijnego zestawu narzędzi komunikacyjnych[11], Polska wskazała szereg reform jako zmian pożądanych. Wymieniła wśród nich, takie przekształcenia jak: cyfryzacja procedur wydawania pozwoleń, wydanie wytycznych dotyczących dostępu do infrastruktury fizycznej oraz dalsze wzmocnienie roli jednolitej informacji. Należy w tym miejscu zauważyć, że Polski rząd odwołał aukcję 5G dla częstotliwości radiowych w paśmie 3,6 GHz w maju 2020 r. z powodu pandemia COVID-19. Decyzja ta została podjęta około 6 tygodni po rozpoczęciu działalności przez regulatora, który zaoferował cztery koncesje w paśmie 3,6 GHz, ważne do 30 czerwca 2035 r. Nowa procedura aukcyjna miała zostać wkrótce przedstawiona do konsultacji społecznych. Przeprowadzone w okresie od lipca do września 2020 r. konsultacje wykazały, że polscy operatorzy nie potrzebują częstotliwości w paśmie 26 GHz przed 2022-2023.

Pod względem integracji technologii cyfrowej w działalności przedsiębiorstw Polska zajmuje 24 miejsce wśród krajów UE. 52% polskich MSP osiągnęło co najmniej podstawowy poziom wykorzystania technologii cyfrowych, który jest poniżej średniej unijnej wynoszącej 60%. Jeśli chodzi o wskaźnik

[10] https://www.gov.pl/web/cyfryzacja/fundusz-szerokopasmowy—pierwszy-nabor-wnioskow, dostep 21.02.2022 r.

[11] Zalecenie Komisji (UE) 2020/1307 z dnia 18 września 2020 r. w sprawie wspólnego unijnego zestawu narzędzi służących zmniejszeniu kosztów wprowadzania sieci o bardzo dużej przepustowości oraz zapewnieniu terminowego i sprzyjającego inwestycjom dostępu do widma radiowego 5G, aby wspierać łączność z myślą o odbudowie gospodarki po kryzysie związanym z COVID-19 w Unii

ICT[12] dla zrównoważenia środowiskowego, w Polsce odsetek przedsiębiorstw prowadzących działalność środowiskową z wykorzystaniem ICT, które osiągnęły średni/wysoki poziom wykorzystania technologii cyfrowych wynosi 60%, czyli jest niższy niż średnia UE wynosząca 66%. Polskie przedsiębiorstwa powoli w dalszym ciągu korzystały z możliwości, jakie dają technologie cyfrowe, angażując się w e-commerce – 13% MSP prowadziło sprzedaż internetową, a 5% transgraniczną do innych krajów UE. Zaawansowane technologie powoli zyskują popularność wśród polskich przedsiębiorstw. 15% przedsiębiorstw korzysta z rozwiązań chmurowych, a 18% wykorzystuje w swoich działaniach technologię sztucznej inteligencji (AI[13]). Niemniej jednak tylko 14% polskich przedsiębiorstw aktywnie korzysta z mediów społecznościowych, a 29% angażuje się w elektroniczną wymianę informacji.

Rysunek 4. Wskaźniki dot. Integracji technologii cyfrowej

	Polska			UE
	DESI 2019	DESI 2020	DESI 2021	DESI 2021
3a1 MŚP o co najmniej podstawowym poziomie wykorzystania technologii cyfrowych % MŚP	brak danych	brak danych	52% 2020	60% 2020
3b1 Elektroniczna wymiana informacji % przedsiębiorstw	26% 2017	29% 2019	29% 2019	36% 2019
3b2 Media społecznościowe % przedsiębiorstw	10% 2017	14% 2019	14% 2019	23% 2019
3b3 Duże zbiory danych % przedsiębiorstw	8% 2018	8% 2018	8% 2020	14% 2020
3b4 Chmura % przedsiębiorstw	7% 2018	7% 2018	15% 2020	26% 2020
3b5 Sztuczna inteligencja % przedsiębiorstw	brak danych	brak danych	18% 2020	25% 2020
3b6 ICT na rzecz zrównoważenia środowiskowego % przedsiębiorstw prowadzących działania proekologiczne z wykorzystaniem ICT, które osiągnęły średni/wysoki poziom wskaźnika wykorzystania technologii cyfrowych	brak danych	brak danych	60% 2021	66% 2021
3b7 E-faktury % przedsiębiorstw	16% 2018	16% 2018	13% 2020	32% 2020
3c1 MŚP prowadzące sprzedaż internetową % MŚP	12% 2018	13% 2019	13% 2020	17% 2020
3c2 Obroty z tytułu handlu elektronicznego % obrotów MŚP	brak danych 2018	brak danych 2019	brak danych 2020	12% 2020
3c3 Transgraniczna sprzedaż internetowa % MŚP	4% 2017	5% 2019	5% 2019	8% 2019

Źródło: Digital Economy and Society Index (DESI) 2021

[12] Technologia informacyjna i komunikacyjna, w skrócie (ICT), obejmuje wszystkie środki techniczne wykorzystywane do obsługi informacji i komunikacji pomocowej. Obejmuje to zarówno sprzęt komputerowy, jak i sieciowy, a także ich oprogramowanie.

[13] „Mówiąc najprościej, sztuczna inteligencja (artificial intelligence, AI) to systemy lub maszyny, które naśladują ludzką inteligencję w celu wykonywania zadań i mogą sukcesywnie usprawniać swoje działanie w oparciu o zbierane informacje.": https://www.oracle.com/pl/artificial-intelligence/what-is-ai/, dostep 21.02.2022 r.

Polska, jak i wiele państw w okresie pandemii, rozwinęła dynamicznie wiele aplikacji, które wspierały możliwości cyfrowe społeczeństwa. Zamrożenie gospodarcze po kryzysie COVID-19 pozytywnie wpłynęło na powszechne korzystanie z usług e-administracji. Popularność aplikacji: Profil zaufany (PZ)[14] jako podstawowej usługi uwierzytelniania znacznie wzrosła. W 2020 roku utworzono ponad 4 miliony profili[15], a liczba aktywnych profili podwoiła się w porównaniu do 2019 roku. Wprowadzono również weryfikację wideo, ponieważ jedną z metod potwierdzania tożsamości jest możliwość tworzenia tymczasowych profili zaufanych. Użytkownicy usług PZ, mogą używać aplikacji do wykonywania czynności administracyjnych przez Internet. Są wśród nich takie jak rejestracja, administrowanie danymi, składanie wniosków, itp. Dlatego można uznać, że popularność tego profilu jest ważnym wskaźnikiem popularności wszystkich usług e-administracji.

Realizowana przez polski rząd polityka otwartych danych przynosi efekty: wzrosła ilość dostępnych danych nadających się do ponownego wykorzystania, a coraz więcej firm zdaje sobie sprawę ze swojego potencjału. Open Data (Otwarte dane)[16] – ogólnokrajowy kompleksowy portal dla otwartych danych – zyskał znaczną popularność i międzynarodowe uznanie[17]. W 2020 roku Polska, wg. rankingu: „Stopień zaawansowania wdrożenia polityki otwartych danych w 2020 r.[18]", awansowała z grupy trzeciej (kraje szybko wprowadzające innowacje) do najwyżej notowanej czwartej grupy krajów (kraje wiodące w trendzie), w której kraje są uszeregowane według ich stopnia zaawansowania we wdrożeniu nowoczesnych rozwiązań.

[14] Profil zaufany, Panel do logowania: https://pz.gov.pl/dt/index, dostęp: 21.02.2022 r.

[15] https://www.gov.pl/web/cyfryzacja/cztery-miliony-profili-zaufanych-od-poczatku-tego-roku, dostęp: 21.02.2022 r.

[16] https://dane.gov.pl/pl, dostęp: 21.02.2022 r.

[17] https://data.europa.eu/sites/default/files/country-factsheet_poland_2020.pdf, dostęp: 21.02.2022 r.

[18] Open Data Maturity Report 2021: https://data.europa.eu/sites/default/files/landscaping_insight_report_n7_2021.pdf, dostęp: 22.02.2022 r.

W 2020 r., po wcześniej dokonanej ocenie i konsultacjach społecznych[19], zaktualizowano specyfikację krajowych standardów otwartych danych, a agencje zaczęły stosować te standardy w swojej codziennej działalności. W obszarze zdrowia publicznego działania podejmowane bezpośrednio w odpowiedzi na pandemię obejmują rozbudowę projektu e-zdrowie, finansowanego z polityk strukturalnych UE oraz wprowadzenie podstawowych usług e-rejestracji i telemedycyny w celu zapewnienia konsultacji i zdalnego dostępu do podstawowych usług dot. opieki zdrowotnej. Ponadto rządowy portal pacjenta[20] z powodzeniem wdrożył system elektronicznego wystawiania recept w ramach internetowego konta pacjenta na poziomie aplikacji mObywatel[21].

W ramach wdrożonych rozwiązań, które dla sprawnego działania wykorzystują dane osobowe, można wymienić jeszcze wiele. Dla przykładu, można jeszcze przywołać: e-dowód, systemy CRM, czy narzędzia do remarketingu . Jednak na potrzeby poniższego artykułu, uznaje się, że opisane rozwiązania informatyczne, wyczerpują w pełni zakres, wymagany do przeprowadzonych badań.

Analiza otoczenia prawnego

W ciągu zaledwie jednego roku pandemia COVID-19 zasadniczo zmieniła i przyspieszyła rolę i postrzeganie transformacji cyfrowej w naszym społeczeństwie i gospodarce. Technologia cyfrowa jest obecnie niezbędna do pracy, nauki, zabawy, spotkań towarzyskich, robienia zakupów i uzyskiwania dostępu do różnych usług, od opieki zdrowotnej po dostęp do kultury. Pandemia pokazała nam, że decydujące mogą być radykalne innowacje[22]. Pandemia ujawniła również kruchość przestrzeni

[19] https://dane.gov.pl/pl/article/standardy-otwartosci-danych-raport-z-konsultacji-publicznych, dostęp: 22.02.2022 r.

[20] Portal: IKP (Internetowe Konto Pacjenta): https://pacjent.gov.pl/, dostep 22.02.2022 r,

[21] Portal: mObywatel: https://www.gov.pl/web/mobywatel, dostęp: 22.02.2022 r.

[22] Droga do innowacji a COVID-19, Wyzwania dla CEO: https://www.ayming.pl/wp-content/uploads/sites/16/2020/06/Droga-do-innowacji.-Wyzwania-CEO_raport.pdf, dostep: 21.02.2022 r.

cyfrowej, zależność od technologii pozakrajowych i pozaeuropejskich oraz wpływ dezinformacji na demokratyczne społeczeństwa[23].

We wrześniu 2020 r. prezydent Ursula von der Leyen ogłosiła w swoim orędziu o stanie Unii[24], że mając jasno określone cele i zasady, Europa powinna osiągnąć suwerenność cyfrową do 2030 r. – wspólną wizją UE. Przewodnicząca położyła szczególny nacisk na europejską chmurę obliczeniową, wiodącą rolę w budowie etycznej sztucznej inteligencji, bezpieczną tożsamość cyfrową dla wszystkich oraz znaczną poprawę infrastruktury danych i superkomputerów oraz łączności. W odpowiedzi Rada Europejska wezwała Komisję Europejską do zaproponowania do marca 2021 r. kompleksowych wytycznych cyfrowych, wyznaczających ambitne cele transformacji cyfrowej do 2030 r., ustanawiając systemy monitorowania oraz nakreślając kluczowe kroki i środki służące ich osiągnięciu.

Pandemia COVID-19 podkreśliła i utorowała drogę do powszechnego stosowania innowacyjnych rozwiązań w zakresie telemedycyny i tele-opieki oraz robotyki, w celu ochrony pracowników służby zdrowia i zapewnienia zdalnej pomocy pacjentom w domu. Technologie cyfrowe umożliwiają obywatelom między innymi: monitorowanie własnego zdrowia, zapewniają możliwości samodzielnego życia, pomagają zapobiegać chorobom niezakaźnym oraz zwiększają produktywność świadczeniodawców i systemów opieki zdrowotnej. Obywatele mogą obecnie w większym zakresie dysponować odpowiednimi narzędziami, które pomagają im dbać o zdrowie mimo wieku, a pracownicy służby zdrowia i opiekunowie mogą wykorzystywać rozwiązania cyfrowe do monitorowania i leczenia pacjentów.

Aby obywatele mogli w pełni korzystać ze swoich praw, powinni mieć nie tylko dostęp do niedrogiej, bezpiecznej łączności o wysokiej jakości, być w stanie zdobyć podstawowe umiejętności cyfrowe – co powinno być prawem powszechnym – ale także mieć łatwy dostęp do cyfrowych usług

[23] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego komitetu ekonomiczno-społecznego i Komitetu regionów, cyfrowy kompas na 2030 r.: Europejska droga w cyfrowej dekadze

[24] https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2020_pl, dostęp: 2022.02.2022 r.

publicznych opartych na tożsamości cyfrowej, która jest chroniona przez prawo. Ludzie powinni zatem móc wymagać egzekwowania przepisów, takich jak bezpieczne i zaufane przestrzenie cyfrowe, równowaga między życiem zawodowym a prywatnym w środowisku pracy zdalnej, ochrona mniejszości i podejmowanie decyzji w oparciu o algorytmy etyczne.

Ponadto skoncentrowane na ludziach, bezpieczne i otwarte środowisko cyfrowe musi działać zgodnie z przepisami, a jednocześnie umożliwiać ludziom korzystanie z ich praw, w śród których należy wymienić prawa do prywatności i ochrony danych, wolność wypowiedzi i prawa konsumentów.

Zasady cyfryzacji opierają się na prawie pierwotnym UE[25], w szczególności na Traktacie o Unii Europejskiej (TUE)[26], Traktacie o funkcjonowaniu Unii Europejskiej (TFUE)[27], Karcie praw podstawowych oraz orzecznictwie Europejskiego Trybunału Sprawiedliwości Sprawiedliwość UE[28], a także prawa wtórne.

Ustawa o ochronie danych osobowych[29] istnieje w polskim prawie od dawna – została uchwalona 29 sierpnia 1997 roku. Ze względu na wprowadzenie przepisów RODO[30], została ona znacząco zaktualizowana w maju 2018 r. Zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO[31]) dane osobowe to wszelkie informacje, które pozwalają zidentyfikować osobę fizyczną, zatem dane osobowe takie jak imię i nazwisko czy numer PESEL. Ale nie tylko. Są to również czynniki, które określają cechy fizjologiczne, fizyczne, psychologiczne, ekonomiczne, kulturowe lub społeczne, a nawet adresy IP.

[25] Źródła i zakres prawa Unii Europejskiej: https://www.europarl.europa.eu/factsheets/pl/sheet/6/zrodla-i-zakres-prawa-unii-europejskiej, dostęp: 10 kwietnia 2022 r.

[26] Traktat o Unii Europejskiej (wersja skonsolidowana): https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012m%2ftxt, dostęp 10 kwietnia 2022 r.

[27] Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A12012E%2FTXT, dostep 10 kwietnia 2022 r.

[28] Karta praw podstawowych Unii Europejskie: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012p%2ftxt, dostep 2022 r.

[29] Ustawa z dnia 29 sierpnia 1997 r. – o ochronie danych osobowych. (t.j. Dz.U. 1997 nr 133 poz. 883)

[30] Ustawa z dnia 10 maja 2018 r. – o ochronie danych osobowych (t.j. Dz.U. 2018 poz. 1000)

[31] ibidem

Co do zasady wszystkie wcześniej wskazane informacje mogą być danymi osobowymi. Jest jednak kilka ważnych rzeczy, o których musimy pamiętać przy podejmowaniu decyzji, czy faktycznie mamy z nimi do czynienia, ponieważ niektóre informacje mogą w niektórych przypadkach zostać uznane za dane osobowe, a w innych nie. W pierwszej kolejności należy zauważyć, że zgodnie z definicją zawartą w art. 4.1 RODO[32], aby jakiekolwiek informacje zostały uznane za dane osobowe, muszą dotyczyć (odnosić się) zidentyfikowanej osoby fizycznej lub możliwej do zidentyfikowania osoby fizycznej. Innymi słowy, aby informacje można było uznać za dane osobowe, muszą umożliwiać bezpośrednią lub pośrednią identyfikację konkretnej osoby fizycznej. Dlatego w zdecydowanej większości przypadków informacje takie jak imię, nazwisko, stanowisko, wykształcenie czy numer rachunku bankowego nie będą traktowane jako dane osobowe, ponieważ nie dotyczą konkretnej osoby fizycznej. Na ich podstawie nikt też nie może zostać zidentyfikowany.

Trudności w zaklasyfikowaniu niektórych danych jako danych „normalnych" lub „specjalnej kategorii" wynikają z faktu, że nie wszystkie informacje, które są obecnie odczytywane (informacje behawioralne), mogą być jednoznacznie danymi dotyczącymi określonej kategorii wymienionych w art. 9 sek. 1 RODO. Na przykład PIN do karty kredytowej czy ulubiony kolor nie należą do tego zamkniętego katalogu, a takie dane można bez większych trudności zdobyć i wykorzystać w neuromarketingu lub do celów przestępczych. Ponieważ prawodawca unijny przewidział wyczerpujący wykaz danych z określonej kategorii, należy uznać, że żadne inne dane nie mogą korzystać z przywilejów określonej kategorii danych, zwłaszcza jeśli ich kategoria została wyraźnie wskazana w art. 4 pkt 1 RODO.

W tym miejscu należy zauważyć, że aby zgoda (art. 6 ust. 1 lit. a i art. 9)[33], była ważna, muszą być spełnione łącznie cztery warunki, w tym musi być ona wyrażona świadomie. Zdaniem Naczelnego Sądu Administracyjnego zgoda „nie może mieć (...) abstrakcyjnego charakteru, ale powinna

[32] ibidem

[33] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. (tj. Dz. U. 2018 poz. 1000)

odnosić się do określonego stanu faktycznego, obejmującego tylko określone dane oraz dokładny (specyficzny) sposób i cel ich przetwarzania"[34].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725[35] z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych, które zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej z dnia 21 listopada 2018 r. i zaczęło obowiązywać z dniem 11 grudnia 2018 r, gwarantuje, że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE)[36] stanowi, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Prawo to gwarantuje również art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[37].

Decyzja Prezydium Parlamentu Europejskiego z dnia 17 czerwca 2019 r. ustanawiająca przepisy wykonawcze dotyczące rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE)

[34] Wyrok Naczelnego Sądu Administracyjnego – Ośrodek zamiejscowy w Warszawie z dnia 11 kwietnia 2003 r. (II SA 3942/02).

[35] Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE

[36] Traktat o funkcjonowaniu Unii Europejskiej: Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012e%2ftxt, dostęp: 09 kwietnia 2022 r.

[37] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, (tj. Dz.U. 1993 nr 61 poz. 284)

nr 45/2001 i decyzji nr 1247/2002/WE[38], jest kolejnym, ważnym źródłem prawa, które ustanawia przepisy mające zastosowanie do przetwarzania danych osobowych przez wszystkie instytucje i organy Unii oraz przewiduje powołanie przez każdą instytucję inspektora ochrony danych.

Administracje rządowe i organy regulacyjne odgrywają ważną rolę w zachęcaniu do inwestowania w innowacje cyfrowe i rozwój nowoczesnych technologii z korzyścią dla społeczeństwa. Ich rolą jest ochrona interesów konsumentów i państwa oraz ograniczanie wszelkich, potencjalnie negatywnych konsekwencji w szybko zmieniającym się cyfrowym świecie. Jest to nie tylko ciągły proces podążania za rosnącym tempem rozwoju technologicznego i transformacji cyfrowej, ale z pewnością wyzwaniem jest odzwierciedlenie zmieniających się wartości i preferencji społecznych.

Poczucie bezpieczeństwa jest niezbędne dla konsumentów chcących korzystać z nowych technologii. Na przykład przepisy prawne dotyczące samochodów autonomicznych nie zostały jeszcze opracowane, nie ustalono zatem na kogo w razie wypadku spadnie odpowiedzialność: czy na producenta, właściciela samochodu lub firmę ubezpieczeniową? Prawo nie nadąża za podejściem „startup-owym", które wykorzystuje pewnego rodzaju „luki prawne", które omijają istniejące przepisy prawne, w tym w usługach Uber i Airbnb, platformach handlowych, w przypadku podatku od platform cyfrowych, oraz wiele innych rozwiązań oferowanych przez dostawców na całym świecie za pośrednictwem Internetu.

[38] Decyzja Prezydium Parlamentu Europejskiego z dnia 17 czerwca 2019 r. ustanawiająca przepisy wykonawcze dotyczące rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE

Cyfrowe obywatelstwo – analiza w oparciu o prawa i zasady Europejczyków wyszczególnione w deklaracji dotyczącej zmian wynikających z cyfrowej transformacji

W dniu 26 stycznia 2022 r. Komisja Europejska zaproponowała międzyinstytucjonalną deklarację w sprawie praw cyfrowych i zasad cyfrowej dekady.

Komisja zaproponowała zmiany w sześciu zakresach, którym jej zdaniem powinny stanowić swoistą busolę na drodze do cyfryzacji społeczeństwa europejskiego:

1. Najważniejsi są ludzie.
   Technologie cyfrowe powinny chronić prawa człowieka, wspierać demokrację i zapewniać odpowiedzialne i bezpieczne działanie wszystkich podmiotów cyfrowych. UE promuje te wartości globalnie.
2. Solidarność i integracja społeczna.
   Technologia powinna łączyć ludzi, a nie ich dzielić. Każdy powinien mieć dostęp do Internetu, umiejętności cyfrowych, cyfrowych usług publicznych i uczciwych warunków pracy.
3. Wolność (swoboda) wyboru.
   Obywatele UE powinni mieć możliwość korzystania z uczciwego środowiska internetowego, wolnego od nielegalnych i szkodliwych treści, oraz mieć dobrą pozycję do korzystania z pojawiających się technologii, takich jak sztuczna inteligencja.
4. Uczestnictwo.
   Obywatele powinni mieć możliwość uczestniczenia w procesach demokratycznych na wszystkich poziomach i sprawowania kontroli nad własnymi danymi.
5. Bezpieczeństwo i ochrona.
   Środowisko cyfrowe powinno być bezpieczne i chronione. Od dzieci po osoby starsze, wszyscy użytkownicy muszą być wzmocnieni i chronieni.
6. Zrównoważony rozwój.
   Urządzenia cyfrowe powinny wspierać zrównoważony rozwój

i transformację ekologiczną. Ludzie muszą wiedzieć, jaki wpływ na środowisko mają ich urządzenia i ile zużywają energii.[39]

Cyfrowe prawa i zasady określone w deklaracji uzupełnią istniejące prawa, takie jak prawa wynikające z Karty praw podstawowych UE oraz przepisy dotyczące ochrony danych i prywatności. Zapewnią one obywatelom ramy odniesienia na temat ich praw cyfrowych oraz poprowadzą państwa członkowskie UE i przedsiębiorstwa w zakresie korzystania z nowych technologii. Mają one na celu pomóc wszystkim obywatelom UE w jak najlepszym wykorzystaniu transformacji cyfrowej.

Proponowane prawa i zasady[40]:

1. Prawa człowieka to najważniejszy element cyfrowej transformacji. Technologia powinna służyć i przynosić korzyści wszystkim Europejczykom oraz umożliwiać im realizację ich aspiracji. Nie powinna zagrażać ich bezpieczeństwu ani prawom podstawowym. Sygnatariusze deklaracji zobowiązali się:
   - Wzmocnić demokratyczne ramy transformacji cyfrowej z korzyścią dla wszystkich, co ma wpłynąć na poprawę jakość życia wszystkich Europejczyków;
   - Podejmować niezbędne kroki w celu zapewnienia poszanowania wartości Sojuszu oraz praw osób w Internecie i poza nim;
   - Wspierać odpowiedzialne i rzetelne działania wszystkich podmiotów cyfrowych, publicznych i prywatnych, w celu zbudowania bezpiecznego środowiska cyfrowego;
   - Aktywnie realizować wizję cyfrowej transformacji.

[39] Cyfrowa dekada Europy: cele cyfrowe na 2030 r.: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl, dostęp 11 kwietnia 2022 r.

[40] Decision of the European Parliament and of the Council Establishing the 2030 policy programme "path to the digital decade": https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52021pc0574, dostęp 11 kwietnia 2022 r.

2. Wsparcie solidarności i integracji społecznej.
   Każdy mieszkaniec Europy powinien mieć dostęp do technologii, która powinna sprzyjać rozwojowi społecznemu i promować prawa Europejczyków.
   Sygnatariusze zobowiązują się:
   - Zapewnić, że rozwiązania technologiczne będą tworzone z poszanowaniem prawa ludzi;
   - Zadbać by cyfrowa transformacja nikogo nie pozostawiała w tyle. W szczególności powinna obejmować osoby starsze, osoby niepełnosprawne lub zmarginalizowane, słabsze lub pozbawione praw obywatelskich oraz osoby działające w ich imieniu;
   - Należy opracować odpowiednie ramy umożliwiające wszystkim uczestnikom rynku korzystającym z transformacji cyfrowej, wypełnienie ich obowiązków społecznych oraz wniesienie sprawiedliwego i proporcjonalnego wkładu w rozwój dóbr publicznych, usług i infrastruktury z korzyścią dla wszystkich Europejczyków.

   Dokument programowy obejmuje wiele obszarów, co ma pomóc w tym by nikt nie pozostawał w tyle w cyfrowej transformacji. Obszary te obejmują:

Komunikację:
- Zapewnienie doskonałej łączności wszystkim, niezależnie od miejsca zamieszkania i dochodów;
- Neutralny i otwarty internet, który chroni treści, usługi i aplikacje przed nieuzasadnionym blokowaniem lub obniżeniem poziomu.

Edukację cyfrowa i umiejętności cyfrowe:
- Ułatwienie i wsparcie działań mających na celu wyposażenie wszystkich instytucji edukacyjnych i szkoleniowych w łączność cyfrową, infrastrukturę i narzędzia,
- Wsparcie wysiłków na rzecz umożliwienia uczącym się i nauczycielom nabywania i dzielenia się wszystkimi niezbędnymi umiejętnościami i kompetencjami cyfrowymi, aby aktywnie

uczestniczyć w procesach gospodarczych, społecznych i demokratycznych.
- Umożliwienie każdemu możliwość dostosowania się do zmian, jakie niesie cyfryzacja pracy poprzez szkolenia i możliwość przekwalifikowania się.

Środowisko pracy:
- Zapewnienie wszystkim możliwości korzystania z gwarancji równowagi między życiem zawodowym, a prywatnym w środowisku cyfrowym.

Cyfrowe usługi publiczne:
- Zapewnienie wszystkim Europejczykom przystępności do bezpiecznej i uwiarygodnionej tożsamości cyfrowej, zapewniającej dostęp do szerokiej gamy usług online;
- Zapewnienie powszechnej dostępności do informacji rządowych;
- Ułatwianie bezproblemowego, bezpiecznego dostępu do cyfrowych usług zdrowotnych i opiekuńczych, w tym dokumentacji medycznej, w całej UE, zaprojektowanych w celu zaspokojenia potrzeb ludzi.

3. Zapewnienie wolności wyboru w Internecie.
   Ludzie powinni mieć możliwość dokonywania własnych świadomych wyborów w Internecie. Oświadczenie składane przez sygnatariuszy, ma na celu przyrzeczenie:
   - Zapewnienie przejrzystości w korzystaniu z algorytmów i sztucznej inteligencji oraz zapewnienie ludziom udzielania zgód i informacje zwrotne podczas interakcji w trakcie procesu ich udzielania;
   - Zadbanie o to, że systemy algorytmiczne są oparte na odpowiednich zbiorach danych, aby uniknąć bezprawnej dyskryminacji i zgody na to, aby ludzki nadzór miał wpływ na wyniki działań algorytmów;
   - Zapewnienie, że technologie takie jak algorytmy i sztuczna inteligencja nie będą wykorzystywane do predefiniowania wyborów ludzi, takich jak zdrowie, edukacja, zatrudnienie i życie prywatne;

- Upewnienie się, że sztuczna inteligencja i systemy cyfrowe są bezpieczne i używane z pełnym poszanowaniem podstawowych praw człowieka.

Wolność wyboru obejmuje również swobodę doboru usług internetowych, z których korzystamy w oparciu o obiektywne, przejrzyste i rzetelne informacje. To z kolei oznacza zapewnienie każdemu prawa do konkurowania i wprowadzania innowacji w cyfrowym świecie.

W związku z tym sygnatariusze zobowiązują się do:

- Zapewnienia bezpiecznego i uczciwego środowisko internetowego, w którym chronione są prawa podstawowe, a obowiązki platform, zwłaszcza tzw. dużych graczy i nadzorców, są jasno określone.

4. Wspieranie uczestnictwa w cyfrowych przestrzeniach publicznych. Każdy powinien mieć dostęp do informacji, która jest godna zaufania, zróżnicowanego i wielojęzycznego środowiska internetowego oraz powinien wiedzieć, kto jest właścicielem usług, z których korzysta lub je kontroluje. Powinni mieć możliwość wypowiadania się w Internecie bez obaw o cenzurę lub zastraszanie. Promuje to zróżnicowaną debatę publiczną i demokratyczny w niej udział. Digital Principles zobowiązują sygnatariuszy, by wspierali użytkowników Internetu poprzez:
   - Wsparcie rozwoju i optymalne wykorzystanie technologii cyfrowych w celu stymulowania zaangażowania obywatelskiego i uczestnictwa w demokratycznych wyborach;
   - Kontynuację ochrony praw podstawowych w Internecie, zwłaszcza wolności słowa i informacji.
5. Poprawa bezpieczeństwa, ochrony i upodmiotowienia ludzi. Każdy powinien mieć możliwość korzystania z bezpiecznych i przyjaznych technologii promujących prywatność, a także produktów i usług cyfrowych, które ją wspierają. Digital Rules mają na celu ochronę interesów wszystkich Europejczyków przed cyberprzestępczością, w tym cyberatakami i naruszeniami bezpieczeństwa danych, oraz zwalczanie tych, którzy

chcą podważyć bezpieczeństwo środowiska internetowego. Sygnatariusze planują to zrobić poprzez:

- Ochronę interesów osób, firm i instytucji publicznych przed cyberprzestępczością, w tym naruszeniami danych i cyberatakami. Obejmuje to ochronę tożsamości cyfrowej przed kradzieżą lub manipulacją tożsamości.
- Znalezienie i postawienie przed sądem tych, którzy dążą do podważenia bezpieczeństwa internetowego i integralności europejskiego środowiska cybernetycznego lub promowania przemocy i nienawiści za pomocą środków cyfrowych.
- Zapewnienie możliwość łatwego przesyłania danych osobowych między różnymi usługami cyfrowymi.

Przepisy cyfrowe mają również na celu zapewnienie dzieciom i nastolatkom bezpieczeństwa w Internecie. Możliwe to będzie dzięki: Stworzeniu pozytywnego, odpowiedniego do wieku i bezpiecznego środowiska cyfrowego dla dzieci i młodzieży;

Zapewnienie wszystkim dzieciom możliwości zdobycia niezbędnych umiejętności i zdolności do aktywnego i bezpiecznego poruszania się po Internecie oraz dokonywania świadomych wyborów w Internecie;Ochronę wszystkie dzieci przed szkodliwymi i nielegalnymi treściami, bezpiecznego korzystania z Internetu, manipulacją i nadużyciami oraz zapobieganiem wykorzystywania przestrzeni cyfrowych do popełniania lub ułatwiania przestępstwa.

6. Promowanie zrównoważonego rozwoju w cyfrowej przyszłości. Transformacja cyfrowa jest ściśle związana z ekologią. Chociaż technologie cyfrowe wspierają wiele rozwiązań wspierających procesy dotyczące zmian klimatu, należy zadbać o to, by same nie powodowały tych problemów. Produkty i usługi cyfrowe muszą być projektowane, wytwarzane i usuwane w sposób zmniejszający ich wpływ na środowisko i społeczeństwo. Powinno być również więcej informacji na temat wpływu takich usług na środowisko, w tym zużycie energii. Sygnatariusze deklarują obowiązek:
   - Wspierania rozwoju i wykorzystania zrównoważonych technologii cyfrowych o minimalnym wpływie na środowisko i społeczeństwo;

- Opracowywanie i wdrażanie rozwiązań cyfrowych, które pozytywnie wpływają na środowisko i klimat[41].

W okresie tzw. „cyfrowej dekady", pozostaje wiele wyzwań związanych z transformacją cyfrową. UE musi zwiększyć swoją strategiczną autonomię technologiczną oraz opracować nowe zasady i technologie, aby chronić obywateli przed podrabianymi produktami, kradzieżą cybernetyczną i dezinformacją. Przede wszystkim UE musi zająć się przepaścią cyfrową, która dzieli kraje należące do jej struktury.

Komisja ocenia wdrażanie przepisów cyfrowych w swoim rocznym sprawozdaniu o stanie cyfrowej dekady. Przeprowadzi również coroczne badanie Eurobarometru w celu monitorowania działań następczych ze strony państw członkowskich. Raport Eurobarometru dostarczy danych jakościowych opartych na tym, jak obywatele postrzegają korzystanie z praw cyfrowych w praktyce w różnych państwach członkowskich. Parlament Europejski i Rada Unii Europejskiej omówią wniosek przed jego przyjęciem.

Mechanizm współpracy będzie obejmował:

- Ustrukturyzowany, przejrzysty i oparty na współpracy system monitorowania oparty na Indeksie Gospodarki Cyfrowej i Społeczeństwa Cyfrowego (DESI) w celu pomiaru postępów w osiąganiu celów na 2030 r.
- Roczny raport o stanie Cyfrowej Dekady, w którym Komitet będzie oceniał postępy i formułował rekomendacje działań
- Wieloletni strategiczny plan działań na rzecz cyfrowej dekady, w którym państwa członkowskie określają przyjęte lub planowane polityki i środki wspierające osiągnięcie celu na 2030 r.
- Ustrukturyzowane ramy umożliwiające omawianie i rozwiązywanie problemów dotyczących niedostatecznych postępów w Komitecie i państwach członkowskich poprzez wspólne zobowiązania
- Mechanizmy wsparcia realizacji projektów z udziałem krajów.

[41] European Digital Rights and Principles: https://digital-strategy.ec.europa.eu/en/policies/digital-principles, dostęp: 12 kwietnia 2022 r.

Aby osiągnąć cele i zadania cyfryzacji, Komisja Europejska przyspieszy i ułatwi realizację projektów angażujących różne kraje, czyli projektów o dużej skali, których nie może zrealizować samodzielnie żadne państwo członkowskie[42].

Rola projektów:

- W oparciu o wspólne inwestycje z budżetu UE (również z Funduszu Odbudowy i Odbudowy), państw członkowskich i sektora prywatnego
- Eliminowanie luk w kluczowych zdolnościach UE
- Wspierać łączność i bezpieczeństwo jednolitego rynku cyfrowego.
- Komitet przygotował wstępną listę projektów z udziałem różnych krajów. Lista obejmuje następujące obszary inwestycyjne: procesory o niskim poborze mocy, łączność 5G, przetwarzanie na dużą skalę, bezpieczna komunikacja kwantowa, administracja publiczna, technologia blockchain, centra innowacji cyfrowych i umiejętności cyfrowe.

Jaka powinna być przyszłość cyfryzacji w Europie i w Polsce? Jakie powinny być nasze cele transformacji cyfrowej do roku 2030? Jak zapewnić, że osiągniemy nasze cele?

To są główne pytania, na które spróbują odpowiedzieć liderzy Digital Decade w czerwcu 2022 r.

Ostatnie 18 miesięcy zrewolucjonizowało Europę i świat. Z powodu trwającej pandemii, świat cyfryzuje się szybciej niż kiedykolwiek. Cyfryzacja jest tym, co napędza społeczeństwa. Jednocześnie pogłębia się przepaść między tymi, którzy mogą migrować do technologii cyfrowych i czerpać z nich korzyści, a tymi, którzy tego nie robią.

Wszelkie zmiany powinny mieć jednak szczególnie na uwadze prawa człowieka, a w tym zwłaszcza prawo do ochrony danych osobowych i dostępu do wiarygodnych informacji.

[42] Wniosek dotyczący decyzji ustanawiającej program polityczny 2030 „Droga do cyfrowej dekady": https://digital-strategy.ec.europa.eu/en/library/proposal-decision-establishing-2030-policy-programme-path-digital-decade, dostęp: 12 kwietnia 2022 r.

Podsumowanie

Ekspansja technologii cyfrowych i związany z nią proces transformacji gospodarczej i społecznej to jedna z najbardziej dynamicznych zmian dotyczących współczesności. Innowacyjne technologie cyfrowe, rozprzestrzeniają się na całym świecie znacznie szybciej niż wynalazki w epoce przemysłowej. Cyfryzacja jako ciągły proces łączenia świata realnego i wirtualnego, jest czynnikiem zmian, tworzącym nowe możliwości rozwoju społeczno-gospodarczego, poprawiającym konkurencyjność i innowacyjność gospodarczą, a także niosącym niepewność i różne zagrożenia, w tym automatyzację procesów produkcyjnych mających wpływ na wymiar społeczno-gospodarczy.

Wykorzystywanie technologii cyfrowych przez osoby fizyczne, przedsiębiorstwa, rządy i instytucje publiczne napędza transformację cyfrową. Dzięki technologiom cyfrowym osoby fizyczne mają dostęp do nowych możliwości: komunikowania się, uczestniczenia w życiu społecznym i kulturalnym, uczenia się i pracy, zarabiania i wydawania pieniędzy. Firmy mogą również korzystać z narzędzi opartych na innowacyjnych rozwiązaniach cyfrowych, wykorzystujące dane. Rządy i sektor publiczny mogą wykorzystać technologie cyfrowe do świadczenia usług publicznych w sposób bardziej efektywny i tworzyć wydajniejsze i zorientowane na użytkownika rozwiązania cyfrowe oraz wspierać tworzenie wartości gospodarczej i społecznej poprzez wykorzystywanie otwartych danych.

Zagadnienia omawiane w niniejszym rozdziale należą do aktualnego i niezwykle ważnego obszaru badań zarówno ekonomicznych, jak i społecznych. Wyniki rozważań teoretycznych i badań empirycznych mogą stanowić ważne argumenty do dyskusji podkreślających pozytywne wartości transformacji cyfrowej oraz negatywne zjawiska mające wpływ procesy obsługi danych. Wyniki przeprowadzonych badań mogą przyczynić się do działań mających na celu zmniejszenie nierównowagi w poziomie cyfryzacji polskich sektorów i branż gospodarki oraz gospodarstw domowych. W związku z tym badania w formie niniejszej monografii mogą okazać się przydatne m.in. dla pracowników i studentów Wyższych Uczelni, kierowników przedsiębiorstw, pracowników instytucji publicznych, przedstawicieli rodzin i innych osób zainteresowanych problemem,

którego dotyczą. Szczególnie należy zatem zwrócić uwagę na fakt, że bardzo dynamiczne zmiany w otoczeniu prawnym oraz ich konieczność wynikająca z dynamiki zmian wywołanych zarówno Pandemią COVIDE-19, jak i potrzebami wskazywanymi przez UE, wymagają pilnego przebudowania systemów i aplikacji informatycznych kontrolujących i wspierających faktyczną realizację praw osób, których przetwarzanie danych dotyczy. Koniecznym jest również zwrócenie uwagi na fakt, iż wg. rankingu Indeksu gospodarki cyfrowej i społeczeństwa cyfrowego, Polska znajduje się na jednym z ostatnich miejsc, zatem dynamika zmian w polskim prawie i systemach wspierających ochronę danych, powinien znacznie przyśpieszyć, aby nie narazić społeczeństwa polskiego na konsekwencje wynikające z ich utraty i niekorzystnego wykorzystywania.

References

Safjan, M. (2002). *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*. Państwo i Prawo.

Źródła prawa i inne dokumenty:

Decyzja Prezydium Parlamentu Europejskiego z dnia 17 czerwca 2019 r. ustanawiająca przepisy wykonawcze dotyczące rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów, Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie.

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, (tj. Dz.U. 1993 nr 61 poz. 284).

Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

Ustawa z dnia 10 maja 2018 r. - o ochronie danych osobowych (t.j. Dz.U. 2018 poz. 1000).

USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych. (tj. Dz. U. 2018 poz. 1000).

Ustawa z dnia 29 sierpnia 1997 r. - o ochronie danych osobowych. (t.j. Dz.U. 1997 nr 133 poz. 883).

Wyrok Naczelnego Sądu Administracyjnego – Ośrodek zamiejscowy w Warszawie z dnia 11 kwietnia 2003 r. (II SA 3942/02).

Zalecenie Komisji (UE) 2020/1307 z dnia 18 września 2020 r. w sprawie wspólnego unijnego zestawu narzędzi służących zmniejszeniu kosztów wprowadzania sieci o bardzo dużej przepustowości oraz zapewnieniu terminowego i sprzyjającego inwestycjom dostępu do widma radiowego 5G, aby wspierać łączność z myślą o odbudowie gospodarki po kryzysie związanym z Covid-19 w Unii.

Źródła internetowe:

Cyfrowa dekada Europy: cele cyfrowe na 2030 r.: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl, dostęp 11 kwietnia 2022 r.

Cztery miliony profili zaufanych od początku tego roku: https://www.gov.pl/web/cyfryzacja/cztery-miliony-profili-zaufanych-od-poczatku-tego-roku, dostęp: 21.02.2022 r.

Dane osobowe, definicja: https://www.europarl.europa.eu/privacy-policy/pl/data-protection, Dostęp: 17.02.2022 r.

Decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade": https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52021pc0574, dostęp 11 kwietnia 2022 r.

Digital Economy and Society Index (DESI) 2021: https://digital-strategy.ec.europa.eu/en/policies/desi, dostęp: 18.02.2022 r.

Digital Economy and Society Index (DESI) 2021: https://digital-strategy.ec.europa.eu/en/policies/desi, dostęp: 18.02.2022 r.

Droga do innowacji a COVID-19, Wyzwania dla CEO: https://www.ayming.pl/wp-content/uploads/sites/16/2020/06/Droga-do-innowacji.-Wyzwania-CEO_raport.pdf, dostep: 21.02.2022 r.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii; https://eur-lex.europa.eu/legal-content/pl/all/?uri=celex%3a32016l1148, dostęp 02-0502022r.

European Digital Rights and Principles: https://digital-strategy.ec.europa.eu/en/policies/digital-principles, dostęp: 12 kwietnia 2022 r.

Fundusz Szerokopasmowy – pierwszy nabór wniosków: https://www.gov.pl/web/cyfryzacja/fundusz-szerokopasmowy--pierwszy-nabor-wnioskow, dostep 21.02.2022 r.

Karta praw podstawowych Unii Europejskie: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012p%2ftxt, dostep 2022 r.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a52021dc0118, dostęp: 18.02.2022 r.

Open Data Maturity Report 2021: https://data.europa.eu/sites/default/files/landscaping_insight_report_n7_2021.pdf, dostęp: 22.02.2022 r.

Open data maturity: https://data.europa.eu/sites/default/files/country-factsheet_poland_2020.pdf, dostęp: 21.02.2022 r.

Orędzie o stanie Unii 2020: https://ec.europa.eu/info/strategy/strategic-planning/state-union-addresses/state-union-2020_pl, dostęp: 2022.02.2022 r.

Portal danych: https://dane.gov.pl/pl, dostęp: 21.02.2022 r.

Portal: IKP (Internetowe Konto Pacjenta): https://pacjent.gov.pl/, dostep 22.02.2022 r,
Portal: mObywatel: https://www.gov.pl/web/mobywatel, dostęp: 22.02.2022 r.
Profil zaufany, Panel do logowania: https://pz.gov.pl/dt/index, dostęp: 21.02.2022 r.
Serwis programu Polska cyfrowa: https://www.polskacyfrowa.gov.pl/strony/o--programie/, dostep 21.02.2022 r.
Standardy otwartości danych - raport z konsultacji publicznych: https://dane.gov.pl/pl/article/standardy-otwartosci-danych-raport-z-konsultacji-publicznych, dostęp: 22.02.2022 r.
Traktat o funkcjonowaniu Unii Europejskiej: Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012e%2ftxt, dostęp: 09 kwietnia 2022 r.
traktat o unii europejskiej (wersja skonsolidowana): https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012m%2ftxt, dostęp 10 kwietnia 2022 r.
Transformacja cyfrowa, definicja: https://www.sap.com/poland/insights/what--is-digital-transformation.html, Dostęp: 17.02.2022 r.
Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej: https://eur-lex.europa.eu/legal-content/pl/txt/?uri=celex%3a12012e%2ftxt, dostep 10 kwietnia 2022 r.
Wniosek dotyczący decyzji ustanawiającej program polityczny 2030 „Droga do cyfrowej dekady": https://digital-strategy.ec.europa.eu/en/library/proposal-decision-establishing-2030-policy-programme-path-digital-decade, dostęp: 12 kwietnia 2022 r.
Źródła i zakres prawa Unii Europejskiej: https://www.europarl.europa.eu/factsheets/pl/sheet/6/zrodla-i-zakres-prawa-unii-europejskiej, dostęp: 10 kwietnia 2022 r.