

Polskie Towarzystwo Informatyczne

ul. Solec 38 lok. 103 00-394 Warszawa

Kontakt: Beata Ostrowska

e-mail: beata.ostrowska@pti.org.pl

Uwagi opracował wspólny Zespół Polskiego Towarzystwa Informatycznego, Sektorowej Rady

ds. Kompetencji – Informatyka, Sektorowej Rady ds. Kompetencji Telekomunikacja i

Cyberbezpieczeństwo w składzie:

Elżbieta Andrukiewicz

Tomasz Cedro

Zbigniew Daleczko

Wacław Iszkowski

Krzysztof Piech

I. KOMENTARZE OGÓLNE DO STRATEGII CYFRYZACJI PAŃSTWA

a. ZMIANY W PRAWODAWSTWIE, NIEZBĘDNE DO SKUTECZNEGO WDROŻENIA STRATEGII CYBERBEZPIECZEŃSTWA

Na granicy Polski trwa wojna. I wojnę światową wygrali chemicy bronią chemiczną, drugą wojnę wygrali fizycy bronią atomową, trzecia wojna światowa to wojna matematyków i informatyków – ona już trwa. Nie mamy żadnych przepisów dotyczących obrony przeciw cyberterroryzmowi jedynie w przepisach o stanie wojennym i wyjątkowym. Polskie prawo jest anachroniczne i wadliwe w zakresie nowych technologii a naszym zdaniem, **nie ma woli rządzących do wprowadzenia zmian dających bezpieczeństwo państwa polskiego**. Podamy kilka przykładów:

1. Ochrona infrastruktury krytycznej w cyberprzestrzeni.

Do ochrony infrastruktury krytycznej zobowiązani są wszyscy szefowie firm, lecz informacja co jest infrastrukturą krytyczną jest informacją niejawną a szefowie firm w znacznej liczbie nie mają dostępu do informacji niejawnych. RCB wydaje czasopismo „Fokus” poświęcone ochronie infrastruktury krytycznej i zarządzaniu kryzysowym. Mamy już w literaturze światowej opisane te przypadki także z Polski, kiedy gimnazjalista z Łodzi za pomocą pilota od telewizora zaatakował infrastrukturę komunikacyjną miasta, przełączając zwrótnice tramwajowe i powodując wypadki. Konieczna jest tutaj nowelizacja obowiązującego prawa.

2. Ochrona patentowa, prawo patentowe, opłaty licencyjne.

Niemcy, Niderlandy i wiele innych państw wprowadziły przepisy ograniczające prawa licencjonodawców, gdyż stale występują nowe zagrożenia w sferze „new tech”, takie jak prawa

patentowe blokujące prawie połowę produkcji firmy Deimler czy Volkswagen. Ustawowe ograniczenie wysokości opłat patentowych i licencyjnych a także standaryzacja zgodna z wytycznymi unijnymi wydaje się być koniecznością. Policzmy, ile kosztują opłaty licencyjne ponoszone przez polską administrację. Koncerny nie są instytucjami dobroczynnymi. Istotne zagrożenia wydają się być w zakresie takich nowych technologii jak sieci 5G.

3. Funkcjonowanie firm wysokiego ryzyka w krajowej cyberprzestrzeni

Pojęcia i zakresy uznawania podmiotów gospodarczych za dostawcę wysokiego ryzyka (DWR) zapoczątkowały w Polsce kolejne akty i decyzje organów UE, a rozwinęła się ona na dobre w chwili pojawienia się projektów nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Tymczasem kontrolę nad bardzo dużą częścią polskiej infrastruktury telekomunikacyjnej – sieciami szerokopasmowymi i lokalnymi – sprawują firmy chińskie, takie jak Huawei. Wiemy też o chipach w samochodach Volvo, które zdalnie sterowane mogą być zatrzymane podczas jazdy autostradą.

4. Prawo telekomunikacyjne

Istnieją poważne zagrożenia związane z impersonizacją abonenta w telefonii VoIP (*caller-ID-spoofing*) gdzie występują zarówno zagrożenia phishingu jak i SPIT (*Spam over Internet Telephony*), zagrożenia podsłuchu bo VoIP nie przewiduje szyfrowania, odmowę realizacji usług, nieuprawniony dostęp do usług, zagrożenia związane z fizycznym dostępem do sieci (<http://www.voipsa.org/Activities/> czy podszywanie się pod tożsamość głosową abonenta <http://www.phonegangster.com/>). Do niedawna funkcjonował portal wykręć numer www.wykretnumer.pl, który umożliwiał podszywanie się pod dowolny numer telefoniczny w tym pod telefony alarmowe, gdyż polskie prawo telekomunikacyjne mówi, iż numer abonenta na całej drodze połączeniowej musi być taki sam, lecz nie musi być on prawdziwy. W sieci GSM plus po połączeniu z numerem *7177 mamy usługę „Żartofon” gdzie mamy opcje zmiany swojego głosu na damski, męski, dziecięcy, starca mamy też do wyboru usługę telefonii GSM „Chcesz kogoś wkręcić” czy „Zapewnij sobie alibi” http://plus.pl/rozrywka_i_informacje/po_godzinach/na_luzie/zartofon/. Techniki zmiany głosu (*morfining*) została także zaimplementowana w niektórych modelach aparatów telefonicznych. Można zaryzykować stwierdzenie, że istnieje możliwość mówienia z numeru Premiera głosem Premiera.

Pojawiające się sieci Botnet: (Hlux, Kelihos...) wysyłające zdalnie spam i atakujące inne komputery w sieci, wykradając poufne informacje lub przeprowadzając ataki typu DDOS (*Distributed Denial of Service*) *scam*, *phishing stale* atakują polskie komputery a szacunki mówią, iż ponad 90% komputerów jest podatnych do zainfekowania i włączenia do sieci botnet.

5. Podpis elektroniczny

Istnieje pilna potrzeba certyfikacji podpisu elektronicznego stworzonego dla potrzeb administracji publicznej: <http://www.pki2.eu/> na podstawie Dyrektywy 1999/93/EC Parlamentu Europejskiego z 13 grudnia 1999:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:24:31999L0093:PL:PDF>

6. Wardriving

W Polsce narasta moda na poszukiwanie sieci bezprzewodowych i przełamywanie ich zabezpieczeń. Działalność ta preferowana jest głównie przez młodych ludzi, pracowników korporacji ale nie tylko. Poszukiwanie sieci bezprzewodowych przez wielu traktowane jest już jako hobby lub nawet sport a wyniki są publikowane. Ograniczenie się do sporządzania wirtualnych map z naniesionymi punktami dostępowymi do sieci jest przejawem zdrowego rozsądku niektórych wardriverów. W Polsce wardriving jest legalny, ale znakowanie tych sieci na murach już nie. Słyszałem przykładowo o sieciach WiFi w kancelariach adwokackich w Jeleniej Górze bez zabezpieczeń

7. Cyberstalking

Mamy także cyberstalking ujęty w art. 190a KK.

Mamy także sieć onion i cennik usług Crime As Service – zablokowanie strony WWW – 9.99\$, fałszywy bankomat 3500\$, karta kredytowa (kopia) ok. 100\$, a części do pistoletu można sobie wydrukować na drukarce 3D.

8. Wolne media, sieci społecznościowe, manipulacje

Widzimy, jak ograniczenia w zakresie mediów działają w takich państwach jak Rosja, Białoruś czy nawet niestety Polska. Zdajemy sobie sprawę z globalnej dominacji sieci medialnych społecznościowych. W Chinach mamy totalną inwigilację. W Rosji, mimo istnienia mediów społecznościowych, propaganda manipuluje umysłami obywateli. U nas niestety może być podobnie, co powoduje, że ludzie zamykają się w bańkach informacyjnych i uzależniają się od nich. Osoba uzależniona nie ma krytycznego myślenia, nie odróżnia przekazu fałszywego od prawdziwego i nie widzi, dokąd prowadzi propaganda. Stare media działają w podobny sposób. Ludzie czytają gazety, które najlepiej pasują do tego, co im odpowiada. Ludzie oglądają kanały telewizyjne, które najlepiej odpowiadały ich poglądom. Ktoś ogląda TVN24, a ktoś - TVP. Ktoś czyta "NIE", ktoś – "Najwyższy Czas" a ktoś inny „wSieci”. Sieci społecznościowe odtworzyły ten sam model. Lubimy naszą bańkę informacyjną, w której się zamykamy. Sami ją tworzymy i mamy zniekształcenia percepcyjne, ponieważ zawsze lubimy rzeczy, które potwierdzają nasz punkt widzenia. Doświadczamy cyfrowej dyktatury - jesteśmy manipulowani, a sieci społecznościowe nauczyły się kontrolować umysły miliardów ludzi. Obecnie algorytmy już częściowo panują nad emocjami i pragnieniami milionów ludzi na świecie, a całe kraje

zamienia się w informacyjne kolonie. Taka jest przyszłość Internetu i mediów społecznościowych. Korporacje sektora IT już teraz mogą swobodnie wpływać na obywateli całych państw i wykorzystywać ich dane osobowe. Zdajemy sobie sprawę z globalnej dominacji sieci społecznościowych i tego, jak giganci technologiczni wpływają na umysły milionów ludzi, w ramach szeroko zakrojonego projektu „Algorytm. Kto cię kontroluje?”, bo taka jest nasza natura. Sieci społecznościowe są odzwierciedleniem realnego świata, które mogą być używane zarówno dla dobra, jak i dla zła a efekty, które się tam pojawiły się (smartfonowa igła dopaminowa, stany lękowe, uzależnienie od Internetu) nie zawsze są korzystne. Możemy mieć w sobie jakiś pogląd na stan rzeczy na świecie, a gdy tylko czytamy to samo w sieci społecznościowej, myślimy: „Tak właśnie myślałem, wiedziałem, wierzyłem”. Tak działają media społecznościowe. Algorytm coraz bardziej dostosowuje się do naszych preferencji, a my znajdujemy się w tej pięknej, przytulnej bańce informacyjnej. Obecnie wszystkie informacje są online, co oznacza, że szanse na stwierdzenie, że się mylimy są małe. Media społecznościowe są w stanie poszerzyć horyzonty we wczesnych etapach rozwoju osobowości, ale potem ludzie zaczynają dążyć do zamkniętego, małego świata. **Konieczne jest zatem rozwijanie umiejętności korzystania z mediów i tu jest istotna rola szkół i uczelni. Badania amerykańskie pokazały, jakie wydarzenia w życiu mogą wpłynąć na nasz światopogląd i są to przede wszystkim wpływy uczelni, to tam młody człowiek pierwszy raz spotyka ludzi z radykalnie odmiennych kręgów.** Politycy zorientowali się, jaka jest przyszłość algorytmów sieci społecznościowych i zaczęli je wykorzystywać do własnych celów, co widzimy nie tylko w Chinach, ale także w Rosji, czy USA, gdzie Obama skutecznie wykorzystał portale społecznościowe na potrzeby kampanii wyborczej. Zrobiono to już wcześniej w Azji, przykładowo w wyborach na burmistrza Tokio w 2000 roku. Każda próba sprzedaży reklam politycznych w sieciach społecznościowych jest próbą sprzedaży pewnego eliksiru. **Ludzie wierzą w to, w co chcą wierzyć.** Żadna ilość superinteligentnej propagandy nie przekona Cię do głosowania na kogoś innego. Warto też wiedzieć, że każda reklama polityczna w trakcie kampanii wyborczej działa tylko na dziesięć procent niezdecydowanych. Większość wyborców już wie, czego chce. W mediach dostrzegamy tylko to, co potwierdza naszą opinię. Inną opcją to reklama przez influencerów. Ważną rzeczą jest usuwanie szkodliwych wiadomości przez sieci, czego doświadczył Donald Trump czy Janusz Korwin Mikke. Unia Europejska niedawno zatwierdziła nowe prawo antyterrorystyczne: teraz zabronione treści muszą zostać usunięte w ciągu godziny. Nie sądzimy, by można było sobie poradzić z niechcianymi treściami szczególnie, że rozwija się sieć TOR. Ogromny Facebook z wielomiliardową publicznością ma kilkadziesiąt tysięcy moderatorów, którzy już nie są w stanie działać skutecznie. W YouTube filtry treści chronionych prawami autorskimi działają losowo a ponadto istnieje duża liczba jawnych oszustów, którzy zgłaszają skargi dotyczące treści, przypisując sobie prawa autorskie. W sieci Twittera Jack Dorsey bada możliwość otwarcia sieci społecznościowych w celu interakcji z zewnętrznym oprogramowaniem co oznacza to, że proponuje się przejście od obecnego scentralizowanego modelu do zdecentralizowanego modelu dystrybucji treści. Oznacza to, że firma nie poradzi sobie z niechcianymi treściami i nigdy tego nie zrobi, zamiast tego zostawi wszystko na łasce twórców i odbiorców. Internet traktowany jest jako przestrzeń publiczna, a nie prywatna, ale to Amerykanie uzależnili cały świat od swoich aplikacji. Pytanie filozoficzne – kto i pod kogo powinien się dostosować: sieci społecznościowe powinny

przestrzegać ogólnych reguł państw lub np. powinny przestrzegać pewnych ogólnych zasad np. deklaracji praw człowieka.

Przewidzieli to historycy mediów, tacy jak Marshall McLuhan znany socjolog, który przyczynił się do powstania teorii społeczeństwa informacyjnego. McLuhan przewidział nadejście Internetu i wyjaśnił, że pod wpływem nowych środków komunikacji świat skurczyłby się do rozmiarów wsi, aby opisać to zjawisko McLuhan wprowadził termin „global village”. Już dawno przewidywał, że nie będziemy musieli wychodzić z domu, aby dokonać zakupu - wystarczy skomunikować się, opowiedzieć o swoich potrzebach, a algorytm wybierze informacje i towary, które dana osoba potrzebuje, które zostaną szybko spakowane i wysłane na właściwy adres. McLuhan przewidział zagrożenia, jakie niesie nowa rzeczywistość. Za problem uważał na przykład to, że w środowisku informacyjnym człowiek będzie pozbawiony indywidualności. Twórcy sieci społecznościowych nie widzieli zagrożeń i byli jak dzieci, które dostały w ręce zapalki. Założyciel Facebooka, Mark Zuckerberg, powiedział, że chce zjednoczyć świat, pomyślał, że to świetny pomysł i nie zastanawiał się nad konsekwencjami. Problem z twórcami sieci społecznościowych polega na tym, że myśleli o ludzkości lepiej niż jest w rzeczywistości.

1. Duża część funkcjonalności cyfrowych jest potrzebna chociażby w sytuacji, gdy słabo wykształcony mieszkaniec prowincjonalnych Indii, który nie potrafi pisać, ma możliwość nagrywania wiadomości głosowych w WhatsApp. Ale w tym samym WhatsApp, otrzymuje wiadomości, że w sąsiedniej wiosce mieszka wiedźma, którą trzeba spalić, a ludzie współpracują, by ją zabić (szeroko rozpowszechniły się lincze i masowe bicie lokalnych mieszkańców z powodu fałszywego WhatsAppa 'a w Indiach w latach 2017-2018).

Warto jeszcze dodać, iż do listy zawodów **parlament dopisał zawody jasnowidza i ródźkarza** zapominając o informatykach a działalność informatyków jest sprzeczna z artykułem 269B K.K. *„Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt. 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.”*

b. ELEMENTY STRATEGICZNE I UWAGI WDROŻENIOWE ODNOSZĄCE SIĘ DO CELU STRATEGII NR 5 „Cel 5: Technologie blockchain są wykorzystywane i rozwijane, również w wymiarze europejskim”

Aby Polska mogła stać się liderem innowacji cyfrowych w Europie oraz w pełni wykorzystać potencjał technologii blockchain i aktywów cyfrowych, niezbędne jest dostosowanie Strategii Cyfryzacji Polski do dynamicznie zmieniających się warunków rynkowych. Kluczowe zmiany pozwolą zarówno na rozwój sektora startupów, jak i umożliwią polskim bankom oraz

instytucjom finansowym skuteczną ekspansję międzynarodową poprzez integrację nowoczesnych rozwiązań technologicznych.

Mierzalne cele zmian:

- a) PKO BP stanie się jednym z trzech największych banków w Europie pod względem kapitalizacji rynkowej i wartości aktywów w ciągu 15 lat.
- b) Co najmniej pięć polskich startupów z branży aktywów cyfrowych osiągnie status „jednorożca” do 2035 roku.
- c) Polskie systemy płatnicze będą w pierwszej piątce najbardziej innowacyjnych i efektywnych systemów na świecie w rankingach branżowych do 2030 roku (np. World Payments Report).
- d) Stworzenie w Polsce największego w Europie centrum badań i rozwoju technologii blockchain do 2028 roku.
- e) Wprowadzenie polskiej cyfrowej waluty (CBDC) opartej na blockchain do użytku publicznego do 2030 roku.
- f) Zwiększenie udziału polskich firm technologicznych w rynku usług finansowych na świecie o co najmniej 15% do 2035 roku.

Oczekiwanie skutki wprowadzenia proponowanych zmian:

- a) **Zwiększenie atrakcyjności inwestycyjnej Polski:**
 - Elastyczne regulacje oraz programy wsparcia dla startupów blockchainowych sprawiają, że Polska stanie się jednym z głównych hubów technologicznych w Europie, przyciągając międzynarodowych inwestorów.
 - Przełoży się to na zwiększenie napływu kapitału, tworzenie nowych miejsc pracy oraz wzrost innowacji w sektorze finansowym i technologicznym, co przyczyni się do wzrostu PKB m.in. przez podniesienie stopy inwestycji.
- b) **Wzmocnienie pozycji Ministerstwa Cyfryzacji:**
 - Dzięki wprowadzeniu przodujących regulacji w zakresie blockchain, Ministerstwo Cyfryzacji zyska reputację lidera w tworzeniu innowacyjnych przepisów w Europie. Wzmocni to jego rolę w kształtowaniu europejskiej agendy cyfrowej, co przyniesie uznanie zarówno na poziomie krajowym, jak i międzynarodowym.
- c) **Lepsza pozycja Polski w Unii Europejskiej:**
 - Jako przyszły kraj przewodzący UE, Polska zyska możliwość wpływu na kształtowanie unijnych regulacji dotyczących blockchain i kryptoaktywów.
 - Aktywna rola w harmonizacji MiCA może nie tylko umocnić pozycję Polski jako lidera innowacji cyfrowych, ale także dać nam przewagę w europejskiej i globalnej rywalizacji o miano najważniejszego rynku technologicznego.
- d) **Zabezpieczenie przed marginalizacją lokalnych startupów:**
 - Obecnie przygotowywane wdrożenie regulacji rynku aktywów cyfrowych (MiCA) faworyzuje międzynarodowe podmioty, co może prowadzić do dalszej marginalizacji polskich startupów.

- Wprowadzenie przyjaznych regulacji dla małych i średnich przedsiębiorstw zapewni, że nasze, innowacyjne podmioty będą mogły konkurować z gigantami technologicznymi, a Polska utrzyma kluczową pozycję na rynku cyfrowym.

e) Rozwój kapitału ludzkiego:

- Inwestycje w edukację i szkolenia w zakresie technologii blockchain umożliwią rozwój wykwalifikowanej kadry, co wzmocni pozycję Polski jako innowatora w sektorze cyfrowym.
- Programy edukacyjne na poziomie szkół i uczelni wyższych będą budować fundamenty dla nowej generacji liderów technologicznych, co przyczyni się do długoterminowego wzrostu gospodarki opartej na wiedzy.

f) Przykład dla innych krajów UE:

- Wzorem Malty, Estonii i Litwy, Polska mogłaby przyciągnąć znaczące inwestycje i innowacje poprzez wprowadzenie przyjaznych regulacji blockchainowych.
- Polska stanie się liderem w tej dziedzinie pozwoli na szybszy rozwój rynku aktywów cyfrowych oraz umocni swoją pozycję, jako kluczowego gracza w regionie Europy Środkowo-Wschodniej, zdolnego do konkurowania z Niemcami.

Kluczowe propozycje:

1. Utworzenie właściwych ram regulacyjnych dla technologii blockchain i kryptoaktywów

- Stworzyć dedykowany zespół roboczy w Ministerstwie Cyfryzacji (przenosząc prace nad tym tematem z Ministerstwa Finansów i KNF, jak to jest obecnie), który będzie odpowiedzialny za ponowne opracowanie ram regulacyjnych dla blockchain i kryptoaktywów, niezależnych od KNF. Zespół ten powinien skupić się na dostosowaniu przepisów do dynamicznie zmieniającego się rynku, jednocześnie rozumiejąc technologie, które chce się regulować (czego brakuje w Min.Fin. i KNF).
- Nowe regulacje powinny być elastyczne i uwzględniać różnice w wymogach: inne dla banków, a inne dla startupów czy małych podmiotów finansowych.
- Powrót do grupy doradczej ds. „Blockchain i walut cyfrowych” (2016-18), która była do dziś największą, tego typu grupą doradczą w ww. zakresie któremukolwiek z rządów na świecie. Organizacja „okrągłego stołu” pod kierunkiem Ministerstwa z udziałem przedstawicieli branży, ekspertów, prawników, informatyków, prokuratury, urzędów skarbowych, banków i in. w celu wspólnego opracowania nowych ram regulacyjnych oraz innych zmian w przepisach. Stworzenie wspólnej z sektorem prywatnym „Strategii rozwoju rynku aktywów cyfrowych na kolejne lata w Polsce”, by stać się dominującym takim rynkiem w Europie i jednym z wiodących – na świecie.
- Stworzenie przy Ministerstwie dedykowanych ram regulacyjnych typu sandbox, gdzie startupy mogą testować swoje rozwiązania oparte na blockchainie bez pełnego stosowania regulacji MiCA przez określony czas. Taka „strefa innowacji cyfrowych” mogłaby przyciągnąć inwestycje i wspierać rozwój innowacyjnych technologii, a jednocześnie Ministerstwo mogłoby się uczyć, jak właściwie tworzyć regulacje, chroniąc klientów jednocześnie bez nadmiernego ograniczania rozwoju rynku – co od 2017 r. nie miało miejsca w Polsce.

- Wykorzystanie polskiej prezydencji do tego, by ograniczyć antyinnovacyjne działania (w ramach MiCA i nie tylko) na rzecz takich, które dawałyby Europie szanse na konkurowanie z USA w zakresie nie tylko blockchain, ale i AI. Wprowadzić zakaz regulowania tzw. „infant industries” na rzecz wprowadzania regulacji, o które rynek wystąpi.

2. Wsparcie dla startupów

- Utworzenie funduszy inwestycyjnych, które będą wspierać startupy rozwijające technologie blockchain i kryptoaktywów. Fundusze te mogłyby być finansowane zarówno z budżetu państwa, jak i z funduszy unijnych, w tym z udziałem środków prywatnych. Powinny być to fundusze dedykowane, z udziałem bardzo kompetentnych osób z rynku, w tym ekspertów – również z zagranicy. Powinny działać z pominięciem dotychczasowych patologii związanych z NCBR / PARP, gdzie nad sensownością projektów dominuje poprawność napisania wniosków o dofinansowanie, a nawet bardzo obiecujące projekty zamyka się przy niewspółmiernie niewielkich uchybieniach (nakazując zwrot dotacji z odsetkami).
- Wprowadzenie programów akceleratornych dla startupów technologicznych, które koncentrują się na zastosowaniu technologii blockchain w różnych sektorach, takich jak finanse, zdrowie, bezpieczeństwo, logistyka i inne. Polska do 2018 r. była trzecim krajem na świecie, który miał taki akcelerator (m.in. po Dubaju, choć tam przeznaczono na to kilkadziesiąt razy większe środki). Po interwencji prezesa NBP, akcelerator zamknięto. Można tu podjąć współpracę np. z najlepszym akceleratorem w Europie – StartupBootCamp, a także z wiodącymi firmami.
- Ufundowanie programów badawczych np. w zakresie cyfrowego złotego, który mógłby m.in. wesprzeć transparentność wydatkowania środków na odbudowę Ukrainy.

3. Możliwości ekspansji rodzimych instytucji finansowych

- Polskie banki i instytucje finansowe powinny uzyskać prawo do korzystania z publicznych sieci blockchain do realizacji transakcji oraz oferowania nowych usług finansowych. To wymaga stworzenia odpowiednich przepisów prawnych, które umożliwią takie działania. Od wielu lat takie były one blokowane w naszym kraju, zaś przygotowywana implementacja MiCA niewiele w tym zakresie poprawi, ponieważ przyjęto w jej przygotowaniu prymat restrykcyjności, nad elastycznością i tworzeniem środowiska regulacyjnego wspierającego innowacje.
- Należy nawiązać współpracę z innymi krajami, które już wdrożyły regulacje sprzyjające rozwojowi kryptoaktywów (np. Estonia), aby wymieniać doświadczenia i najlepsze praktyki.

4. Edukacja i promocja

- Wprowadzenie programów edukacyjnych skierowanych do przedsiębiorców oraz instytucji finansowych na temat wykorzystania technologii blockchain i kryptoaktywów w biznesie.

- Wprowadzenie podstaw kryptoaktywów do zajęć w liceach (przedmiot: Biznes i zarządzanie). Uczenie bezpiecznego inwestowania, by nie stać się ofiarą oszustów i zachęcać, by uczniowie edukowali w tym zakresie swoich rodziców i dziadków.
- Organizowanie misji gospodarczych oraz wydarzeń promujących polskie startupy zajmujące się technologiami blockchain na rynkach zagranicznych.

5. Ministerstwo jako regulator i motor rozwoju cyfrowego

- Ministerstwo Cyfryzacji powinno stać się – ponownie – głównym organem odpowiedzialnym za rozwój „cyfrowego kapitalizmu” w Polsce, działając jako przeciwwaga dla KNF, który od lat ogranicza rozwój rynku kapitałowego. Należy ustanowić jasno określone kompetencje oraz odpowiedzialności obu instytucji w zakresie regulacji i nadzoru rynku kryptoaktywów.
- Rozwijanie projektów w zakresie przechodzenia polskich instytucji finansowych na dużo tańsze i bezpieczniejsze od tradycyjnych – technologii blockchain, by zapewnić ich możliwość międzynarodowej ekspansji tak, by za kilkanaście lat mogły dominować w Europie i mieć znaczącą pozycję na świecie.
- Monitorowanie przypadków uniemożliwiania prowadzenia działalności gospodarczej (czego swoboda zapisana jest w Konstytucji RP) przez banki, które – pod groźbami KNF w zakresie odebrania licencji – uniemożliwiają otwierania i prowadzenie kont bankowych podmiotom, które są ich konkurencją (tj. opierają się na zastosowaniach technologii blockchain).

Przykłady innych krajów

Aby lepiej zrozumieć wpływ regulacji na rozwój rynku aktywów cyfrowych i blockchain, warto zlecić badania i analizy przypadków krajów, które wdrożyły korzystne rozwiązania prawne. Na podstawie tych doświadczeń Polska mogłaby stworzyć własne, unikalne podejście, wykorzystując najlepsze praktyki i unikając błędów innych państw.

- Malta, niegdyś znana jako „wyspa blockchain”, wprowadziła w 2018 roku kompleksowe regulacje dotyczące technologii blockchain i kryptowalut, przyciągając liczne firmy z branży. Jednak w kolejnych latach kraj ten zaostrzył przepisy, co wpłynęło na działalność wielu podmiotów. Zmiany te miały na celu zwiększenie nadzoru i zgodności z międzynarodowymi standardami przeciwdziałania praniu pieniędzy. Warto poznać szczegóły tych doświadczeń.
- Choć Estonia wdrożyła innowacyjny system e-rezydencji, który umożliwił przedsiębiorcom z całego świata zakładanie firm online i korzystanie z usług cyfrowych. Program ten przyciągnął wielu przedsiębiorców, jednak w ostatnich latach Estonia zaostrzyła regulacje dotyczące dostawców usług związanych z aktywami wirtualnymi (VASPs). W marcu 2022 roku wprowadzono nowelizację ustawy AML, co doprowadziło do znacznego spadku liczby licencjonowanych firm kryptowalutowych (z blisko 500 do ok. 100 obecnie). Jest to dobry przypadek do przebadania pod kątem lekcji dla Polski w zakresie równoważenia innowacji z odpowiedzialnym nadzorem regulacyjnym.

- Litwa, dzięki proinnowacyjnemu podejściu i nowoczesnym regulacjom, stała się jednym z najbardziej atrakcyjnych miejsc dla fintechów w Unii Europejskiej. Revolut przeniósł swoją siedzibę do tego kraju, a litewski bank centralny zyskał reputację instytucji rozumiejącej rynek i wspierającej rozwój nowych technologii. Litwa zapewnia szybkie procesy licencyjne i jasne regulacje. Polska mogłaby czerpać inspirację z tych rozwiązań, szczególnie w zakresie tworzenia przyjaznych i przejrzystych ram prawnych.
- Szwajcaria, a szczególnie kanton Zug, znany jako „Crypto Valley”, stała się centrum rozwoju technologii blockchain w Europie. Szwajcarskie podejście łączy innowacyjność z silnym nadzorem, co sprawia, że kraj ten przyciąga największe globalne projekty blockchainowe. Polska mogłaby skorzystać z doświadczeń Szwajcarii, tworząc „Polską dolinę cyfrową”, która zapewniałaby elastyczne, ale i bezpieczne regulacje dla firm blockchainowych.
- Poza Europą warto zwrócić uwagę na Singapur, który stał się jednym z głównych centrów finansowych w regionie Azji dzięki proaktywnemu podejściu do regulacji fintechów i kryptoaktywów. Monetary Authority of Singapore (MAS) wprowadził w 2016 roku FinTech Regulatory Sandbox, umożliwiając firmom testowanie innowacyjnych produktów finansowych w kontrolowanym środowisku. W 2019 roku MAS uruchomił Sandbox Express, przyspieszając proces testowania dla prostszych produktów o niskim ryzyku. W ostatnich latach Singapur zaostrzył regulacje dotyczące kryptowalut i aktywów cyfrowych. W styczniu 2022 roku MAS wydał wytyczne ograniczające reklamowanie takich usług, a w 2023 roku zaostrzono wymogi licencyjne dla dostawców usług płatniczych związanych z kryptowalutami. Singapur jednak nadal promuje innowacje w sektorze fintech (np. Singapore FinTech Festival w listopadzie 2023 nt. AI w finansach). MAS kontynuuje prace np. nad Project Guardian, badającymi zastosowanie tokenizacji aktywów i zdecentralizowanych finansów (DeFi) w bezpiecznym środowisku. To wykracza o kilka lat poza regulacje MiCA i będzie niezbędne do wprowadzenia również w Polsce – kwestia, czy będziemy kopiować propozycje UE, czy je współtworzyć, czy może wręcz narzucać UE własne rozwiązania, będąc ich pionierami.
- W kampanii prezydenckiej Donald Trump zapowiedział, że jeśli wygra wybory, utworzy prezydencką radę ds. blockchain i kryptowalut oraz wyeliminuje ograniczenia w zakresie zakładania kont bankowych dla firm z branży. To pokazuje, że tematy związane z kryptoaktywami stają się przedmiotem dyskusji w najważniejszych kampaniach politycznych na świecie. Polska mogłaby aktywnie obserwować rozwój sytuacji w USA i adaptować korzystne regulacje, zanim rynek globalny wyprzedzi Europę w rozwoju innowacji, bo wtedy nie będzie już szans na to, by polskie firmy zaistniały na szerszych rynkach międzynarodowych.

Projekty celowe Ministerstwa

Tak jak Minister Streżyńska przeszła do historii polskiej cyfryzacji m.in. aplikacją mObywatel, tak proponujemy rozważenie wdrożenia któregoś z następujących pomysłów.

A. Program „Cyfrowy Złoty” dla każdego obywatela

- Polska mogłaby jako pierwszy kraj w Europie (i jeden z kilku pierwszych na świecie) wprowadzić cyfrową wersję złotego (CBDC – Central Bank Digital Currency) dla obywateli, opartą na technologii blockchain, który będzie używany do płatności krajowych i międzynarodowych. Dzięki temu Polska mogłaby wzmocnić swoją cyfrową suwerenność, eliminując zależność od innych walut cyfrowych.
- Projekt wzmocniłby pozycję Polski w innowacjach finansowych, a Polacy mogliby korzystać z szybszych, bezpieczniejszych i tańszych transakcji. Ponadto mogłoby to stworzyć podstawy do transparentniejszego wydatkowania środków publicznych, np. w ramach projektów unijnych czy odbudowy Ukrainy.
- Projektując nowy system, powinny zostać zachowane standardy prywatności tak, by dla codziennych zastosowań cyfrowy złoty był odpowiednikiem gotówki.

B. Narodowy Fundusz Blockchain dla Startupów Obywatelskich

- Stworzenie pierwszego w Europie państwowego funduszu opartego na technologii blockchain (taki, „cyfrowy PFR”), który byłby finansowany zarówno z budżetu państwa, firmy prywatne, a także poprzez crowdfunding obywatelski. Każdy obywatel mógłby inwestować w obiecujące polskie startupy blockchainowe, korzystając z tego funduszu, a jego działania byłyby całkowicie transparentne dzięki zastosowaniu technologii blockchain (i cyfrowego złotego).
- Fundusz mógłby wspierać rozwój innowacyjnych projektów blockchain, tworząc nowe miejsca pracy i zwiększając konkurencyjność polskich startupów na rynku międzynarodowym. Obywatele mieliby możliwość uczestnictwa w rozwoju gospodarki cyfrowej, stając się częścią ekosystemu inwestycyjnego.

C. Blockchainowa platforma głosowania obywatelskiego

- Polska mogłaby stać się pierwszym krajem w UE (oprócz – w pewnym zakresie Estonii i Szwajcarii), który wdroży ogólnokrajowy system głosowania oparty na blockchainie, umożliwiający obywatelom udział w referendach i konsultacjach społecznych w sposób całkowicie bezpieczny, transparentny i niemożliwy do manipulacji.
- Taka platforma zwiększyłaby zaufanie obywateli do systemu demokratycznego, a także wzmocniłaby pozycję Polski jako lidera cyfrowej transformacji w sektorze publicznym. Rynek blockchain zyskałby na znaczeniu, a technologie mogłyby być dalej rozwijane do zastosowań w innych sektorach, takich jak zdrowie czy logistyka.

Podsumowanie

Wdrożenie powyższych zmian w Strategii Cyfryzacji Polski ma potencjał, aby znacząco przyczynić się do dynamicznego rozwoju sektora technologii cyfrowych w kraju, tworząc sprzyjające środowisko dla innowacyjnych startupów oraz umożliwiając polskim instytucjom finansowym skuteczną ekspansję na rynki międzynarodowe. Polska może stać się centrum cyfrowych innowacji w Europie – swoistą „doliną cyfrową” – gdzie nowe technologie rozwijają się przy pełnej współpracy sektora publicznego i prywatnego, co jednocześnie pozwala minimalizować ryzyka już na wczesnym etapie.

Dotychczasowe podejście KNF oraz obecne regulacje, w tym przygotowywana implementacja MiCA, nie wspierają dostatecznie rozwoju polskich firm, faworyzując międzynarodowe podmioty, szczególnie banki. Aby zapobiec dalszej marginalizacji polskich innowatorów, konieczne jest opracowanie spójnej, długofalowej polityki państwa, która będzie uwzględniała specyfikę lokalnego rynku i wspierała rozwój technologii cyfrowych oraz kryptoaktywów. Taka strategia, prowadzona odgórnie i konsekwentnie, może uczynić Polskę liderem cyfrowej transformacji na skalę europejską.

II. UWAGI OGÓLNE DO DOKUMENTU „STRATEGIA CYFRYZACJI POLSKI”

UWAGA 1. Dot. Diagnoz

Dotyczy opisanych diagnoz na podstawie DESI, eGovernment Benchmark, DPA, DGI, Deklaracji Berlińskiej oraz badania Eurobarometru.

Na podstawie własnych doświadczeń, stwierdzamy, że do tych diagnoz opracowywanych przez różne instytucje należy podchodzić z dużym krytycyzmem, gdyż nie zawsze prezentują aktualne dla Polski (zresztą zapewne dla innych krajów również) oceny. Powodem jest brak jednolitych merytorycznie aktualnych danych, na podstawie których wyznaczana jest ocena dla danego kraju, a tym samym miejsce w danym rankingu. Czasem, niestety, również oceniający nie są w pełni rzetelni i dokonują ekstrapolacji części danych na podstawie danych historycznych lub porównawczych.

Dlatego też proponujemy dopisanie działania Ministerstwa Cyfryzacji na rzecz zapewnienia rzetelności tych indeksów w kolejnych latach. Aby to było możliwe, MC powinno zadbać o gromadzenie aktualnych danych dotyczących cyfryzacji w Polsce i udostępnianie ich instytucjom opracowującym te diagnozy. Warto też dokonywać weryfikacji wyznaczanych indeksów, ewentualnie żądając ich poprawienia.

UWAGA 2. Dot. Terminologii

Dobrze by było uporządkować stosowaną w „Strategii” terminologię, gdyż znajdujemy tam:

ICT 92 razy, Informatyzacja tylko raz jako dział administracji, rdzeń informaty... 134 razy, informatyka tylko raz, a informatyków 2 razy. Z kolei rdzeń telekomunikac... 32 razy, a teleinformatyczn.. 55 razy. Za to mamy cyfryzacja 15, a rdzeń cyfrow... 402 razy.

Po pierwsze, zrezygnowałbym ze skrótu ICT, który dla większości populacji w Polsce jest obcy i niezrozumiały. Został on zapożyczony z języka angielskiego (z Wlk. Brytanii, bo w USA nie jest używany) do dokumentów unijnych, po czym przeniesiony w tłumaczeniach do polskich wersji tych dokumentów. Jego tłumaczenie na język polski jako TIK się nie przyjęło (w Strategii nie występuje). Poprawnym jego odpowiednikiem w języku polskim jest **teleinformatyka** i takiego też terminu należy używać. Wtedy też naturalnym będzie używanie terminu telekomunikacja oraz informatyka.

W rozwoju zastosowań techniki cyfrowej mieliśmy już komputeryzację, potem informatyzację, a obecnie cyfryzację – głównie poprzez tworzenie nowych nazw ministerstwa. Niestety nie

widać następnego podobnego terminu na nową nazwę przyszłego ministerstwa – chyba że będzie to Ministerstwo Sztucznej Inteligencji.

W Strategii Cyfryzacji Państwa dominuje rdzeń „cyfrow” przywoływany w różnych kontekstach. Trudno z tym polemizować, ale może warto pamiętać, że gdy z 40 lat temu dominowała technika analogowa w: radiach, telewizorach, telefonach, to nikt nie epatował pojęciem rozwoju analogowego. Teraz zaś, nadajemy specjalne znaczenie rozwojowi techniki cyfrowej, jako czegoś niezwykle nowoczesnego. Warto zauważyć, że dla młodego pokolenia ta technika nie jest niczym nowym, gdyż oni tej analogowej już nie widzieli i nie używali. Propozycją jest, aby w treści Strategii nieco zmniejszyć znaczenie tej techniki cyfrowej na rzecz rozwoju teleinformatyki jako pojęcia ogólniejszego i bardziej adekwatnego do tego, co się w tej dziedzinie dzieje.

Tak, przy okazji – bibliotekarze na cyfryzację dokumentów mówią digitalizacja dokumentów, chociaż jest to to samo. Ot, po prostu komuś nie chciało się (albo nie potrafił) przetłumaczyć digitalization na cyfryzację.

Jest jeszcze kłopot z nadużywaniem pojęcia technologia jako bezrozumnego tłumaczenia angielskiego technology. W polskiej terminologii mamy bowiem:

- pojęcie technika: 1. «wiedza na temat praktycznego wykorzystania osiągnięć nauki w przemyśle, transporcie, medycynie itp.; też: praktyczne wykorzystanie tej wiedzy», 2. «metoda», 3. «wyuczona i wyćwiczona umiejętność wykonywania jakichś czynności»,
- a pojęcie technologia jest ograniczone do: 1. «metoda przeprowadzania procesu produkcyjnego lub przetwórczego» oraz 2. «dziedzina techniki zajmująca się opracowywaniem nowych metod produkcji wyrobów lub przetwarzania surowców» [wg. SJP PWN].

Niestety, pojęcie technologia tak już się rozprzestrzeniło w polskim słownictwie, że zmiana tego jest mało możliwa. Ale Ministerstwo jako organ państwowy, powinno również dbać o jakość języka polskiego i dopuścić nieco techniki w opisie Strategii Cyfryzacji.

UWAGA 3. Dot. Kompetencji (str. 47)

W diagnozie dla kompetencji przyszłości są prezentowane zbiorczo wszystkie kategorie kompetencji, które powinny być wyraźniej rozdzielone, gdyż tylko wtedy można dokładniej określić możliwości i potrzeby, jakie powinny być uwzględnione w Strategii Cyfryzacji. Możemy wyróżnić następujące kategorie kompetencji:

Kompetencje rozwoju teleinformatyki. W tej kategorii mamy osoby, które zostały wykształcone na studiach I oraz II stopnia w dyscyplinie informatyka (dziedzinie nauk matematycznych) lub w dyscyplinie informatyka techniczna i telekomunikacja (dziedzinie nauk technicznych) na kierunkach informatycznych, teleinformatycznych, telekomunikacyjnych oraz pokrewnych. Absolwenci studiów uniwersyteckich nabywają umiejętności w zakresie architektury i rozumienia funkcjonalności urządzeń cyfrowych (komputerów, itp.) oraz logicznego myślenia i teorii obliczeń w projektowaniu złożonych algorytmów wraz z ich implementacją w postaci oprogramowania, oraz systemów informatycznych i aplikacji.

Absolwenci studiów technicznych nabywają umiejętności projektowania i wykonywania sprzętu cyfrowego (komputerów, sterowników, modemów, smartfonów, itp.) oraz projektowania i implementacji algorytmów oprogramowania systemowego, systemów teleinformatycznych oraz aplikacji użytkowych. Uzyskując dyplom informatyka lub inżyniera informatyka, teleinformatyka, telekomunikacji są przygotowani do eksploatacji istniejącego sprzętu cyfrowego i oprogramowania oraz do jego rozwoju. Wg GUS¹ w roku akademickim 2023/2024 mieliśmy 14 tys. absolwentów technologii teleinformacyjnych (chyba bez informatyków z uniwersytetów). Znacznie więcej było tych absolwentów w poprzednich latach. Przy tym trzeba uwzględnić, że około 10% rozpoczynających studia, rezygnuje z nich w trakcie, często skuszonych dobrymi finansowo ofertami pracy. Przy poszukiwaniu możliwości zwiększenia naboru kandydatów musimy brać pod uwagę kilka czynników. Pierwszy z nich wynika z natury genetyki, gdy talenty formułowania bardziej złożonych algorytmów ma jedynie niewielki procent młodzieży w danej populacji – grupie kandydatów na studia. Wraz z drugim czynnikiem – niżem demograficznym - będziemy w najbliższym czasie dysponować znacznie mniejszą grupą dobrych kandydatów i kandydatek na studia informatyczne. Trzecim czynnikiem są znaczne braki w dobrej kadrze nauczającej, gdyż poziom wynagrodzeń uczelnianych jest znacznie niższy od średnich wynagrodzeń w przemyśle teleinformatycznym – co nawet przy zmniejszonej liczbie kandydatów ma istotne znaczenie na przyszłość – brak kandydatów na asystentów oznacza bowiem potem ograniczenia w badaniach rozwojowych oraz wyższej kadry naukowej. Z braku istnienia wpisu zawodów informatyk oraz inżynier informatyk w Klasyfikacji Zawodów i Specjalności, oraz braku możliwości oszacowania liczby zatrudnionych informatyków wg klasyfikacji PKD (informatycy są zatrudniani we wszystkich działach PKD) nie dysponujemy dobrymi szacunkami, ilu mamy aktywnych zawodowych informatyków w kraju. Coraz większa ich część jest wykorzystywana przez ośrodki zwalczania cyberzagrożeń oraz przez służby i wojsko. Wielu z nich, często najzdolniejszych, wyjeżdża za granicę, głównie do USA, do pracy dającej nie tyle większe wynagrodzenie, ile większe możliwości rozwoju zawodowego. Większość z nich tracimy bezpowrotnie. W jakimś stopniu możemy ich zastąpić obecnie informatykami (zawodowymi programistami) z Białorusi i Ukrainy, ale nie jest zbyt dobre rozwiązanie. Pozostaje jeszcze oszacowanie, rzeczywiście ilu informatyków będziemy potrzebować w najbliższych latach, gdy obecnie notujemy objawy recesji przemysłu teleinformatycznym.

Kompetencje zastosowań teleinformatyki. W tej kategorii mamy osoby, które mają się zajmować specjalistycznym zastosowaniem produktów i usług teleinformatycznych w określonych tematach. Specjalistami tymi mogą być zawodowi informatycy, absolwenci studiów Informatyki Stosowanej oraz osoby o innych zawodach technicznych, matematycy, fizycy, chemicy oraz ekonomiści i z wielu kierunków humanistycznych (prawnicy, socjologowie, psychologowie), a także nawet medycy i muzycy (STEM). Konieczne jest przy tym douczenie ich na szkoleniach lub studiach podyplomowych podstaw teleinformatyki przez informatyków, a informatyków podstaw z dziedzin, dla których ma być zastosowane rozwiązania teleinformatyczne. Z racji powszechnego zastosowania rozwiązań teleinformatycznych

¹ <https://stat.gov.pl/obszary-tematyczne/edukacja/edukacja/szkolnictwo-wyzsze-w-roku-akademickim-20232024,8,10.html>

praktycznie w całej gospodarce, sektorze finansowym oraz w administracji i edukacji, a także w medycynie, sądownictwie, bezpieczeństwie państwa liczba specjalistów teleinformatyki, według szacunków UE, w Polsce powinna być rzędu miliona. W tym przypadku możliwe i pożądane jest znaczące zwiększenie liczby specjalistek teleinformatyki, korzystając z ich zawodowego wykształcenia. Jednocześnie konieczne jest stałe analizowanie, jak bardzo obecne i przyszłe zastosowania systemów SI mogą ograniczyć lub zwiększyć liczby aktywnych specjalistów i specjalistek teleinformatyki. Należy też uwzględnić potrzeby zapewnienia podstawowego bezpieczeństwa systemów teleinformatycznych oraz służb i wojska w przypadku prowadzenia działań obronnych lub walki z klęskami żywiołowymi.

Kompetencje użytkowania teleinformatyki. [częściowo z wykorzystaniem tekstu ze Strategii] W tej kategorii mamy wszystkich polskich obywateli w wieku od 7 do 90+ lat. Pomijamy najmłodsze pokolenie, które ma już do czynienia z użytkowaniem smartfonów i tabletów od 2-3 lat, oczywiście pod kontrolą (nie zawsze) rodziców. Pokolenie młodzieży szkolnej od 7 do 18 lat użytkuje sprzęt cyfrowy i wiele aplikacji bez problemu, jednakże brakuje im krytycyzmu co do oceny rzetelności i jakości kontentu oraz etycznych zasad użytkowania. Są też narażeni na zagrożenia na cyberataki i oszustwa internetowe. Brakuje im też umiejętności korzystania z zasobów informacyjnych w samodzielnym uczeniu się. Tutaj znaczącą rolę powinna mieć edukacja szkolna, nie tylko na przedmiocie informatyka, ale praktycznie na każdym z przedmiotów.

W grupie dorosłych według danych Eurostatu, w 2023 r. tylko 44% polskich obywateli posiadało co najmniej podstawowe (średnia UE - 56%), a 20% – ponadpodstawowe umiejętności cyfrowe (średnia UE - 27%). Deficyt kompetencji cyfrowych jest przede wszystkim widoczny wśród osób starszych (w wieku 65-74 lata), gdzie 87% nie posiadało nawet podstawowych umiejętności cyfrowych (średnia UE - 72%) i w grupie wiekowej 55–64 lat, w której takie osoby stanowiły 76% (średnia UE - 56%), podobnie jak wśród rolników i osób z niepełnosprawnościami - 77%. Odnotowano także spore dysproporcje wśród osób zamieszkujących miasta i wsie: odsetek mieszkańców terenów wiejskich z co najmniej podstawowymi kompetencjami cyfrowymi wyniósł 33% (średnia UE - 47%), o 22 punkty procentowe 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 – są narażeni na cyberoszustwa oraz cyberataki. Osoby dorosłe w wieku produkcyjnym powinny być obowiązkowo doszkalanie w umiejętnościach teleinformatycznych pożądanych w wykonywaniu zadań ich pracy zawodowej. Należy też stworzyć możliwość szkolenia całej populacji dorosłych (w tym seniorów) w umiejętnościach korzystania z teleinformatyki w życiu prywatnym oraz w kontaktach z administracją państwową. Szczególną uwagę należy zwrócić na umiejętność racjonalnego i rozumnego korzystania z systemów AI, upraszczających korzystanie z rozwiązań i zasobów teleinformatycznych.

UWAGA 4. Wymagania dla zwiększania kompetencji cyfrowych

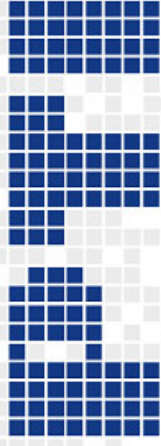
Komentarz ogólny. Polskie Towarzystwo Informatyczne zwraca uwagę na kwestie kadry kształcącej nie tylko studentki i studentów, ale także na poziomie szkół średnich. Poważnym

problemem jest brak skoordynowanych działań dotyczących edukacji informatycznej na poziomie szkół średnich. Chodzi o metodykę nauczania nauk ścisłych, w szczególności informatyki. W kraju mamy zaledwie dwa kierunki poświęcone dydaktyce informatyki (UAM w Poznaniu i bodaj UMC w Lublinie), cała reszta to studia podyplomowe. Osoby zajmujące się metodyką nauczania nauk ścisłych (dotyczy to w równej mierze chemii, fizyki, matematyki) mają bardzo ograniczone możliwości awansu naukowego, a potrzeby rynku są ogromne, 30 miejsc na <https://wmi.amu.edu.pl/dla-kandydata/studia-i-stopnia/nauczanie-matematyki-i-informatyki> nie zaspokaja nawet potrzeb Wielkopolski. A wiemy dobrze, jak bardzo źle jest nauczana informatyka w szkołach średnich. Z powyższego względu optujemy za uwzględnieniem tego aspektu w strategii.

W odniesieniu do wyniku pracy edukacyjnej, wskazujemy następujące zagadnienia:

1. Utrzymanie wyodrębnionego przedmiotu informatyka w programie szkoły podstawowej oraz średniej wraz z ujęciem technik (nie technologii!) cyfrowych jako elementu profilu absolwenta(tki) szkół na wskazanych poziomach. W programie nauczania tych przedmiotów powinna być zwrócona uwaga na nabywanie umiejętności poprawnego korzystania ze sprzętu cyfrowego oraz aplikacji użytkowych wraz z dbałością o bezpieczeństwo ich użytkowania.
2. Wprowadzenie na każdym z przedmiotów szkolnych odpowiednich aplikacji wspomagających tematycznie program nauczania wraz z umiejętności wykorzystania systemów SI.
3. Utrzymanie przedmiotu informatyka rozszerzona w programie szkoły średniej z wprowadzeniem prawa do zdawania informatyki na egzaminie maturalnym.
4. Wspomaganie organizacji konkursów oraz olimpiad matematyczno-informatycznych, szczególnie w szkołach średnich dla wyodrębnienia uczniów i uczennic mających zdolności matematyczno-informatyczne.
5. Zwiększenie liczby miejsc na studiach o kierunkach informatycznych oraz pokrewnych (bezpieczeństwo systemów teleinformatycznych, modelowanie systemów SI, itp.) poprzez dofinansowywanie kosztów prowadzenia tych zajęć – kontrowersyjne, gdyż brak jest możliwości różnicowania wynagrodzeń pracowników dydaktycznych.
6. Zwiększenie liczby miejsc na studiach na kierunkach zastosowania teleinformatyki oraz włączenie przedmiotu zastosowania teleinformatyki na każdym prowadzonym kierunku studiów.
7. Utworzenie, z zapewnieniem finansowania, centrów naukowo-badawczych w dziedzinie teleinformatyki – np. rozwój metod bezpieczeństwa systemów teleinformatycznych, rozwój modelowania oraz generowania specjalistycznych systemów SI, rozwój metod identyfikacji i weryfikacji osób (w tym ich akceptacji dokumentów), rozwój nowych form przetwarzania informacji (w tym urządzenia mechaniki kwantowej), itp. Tego typu centra mają dostarczyć gospodarce nowe rozwiązania teleinformatyczne, ale też mają zatrzymać najlepsze kadry specjalistów teleinformatyki.
8. Obserwowanie działalności oraz czasowe zapraszanie na uczelnie lub do centrów badawczych naszych profesjonalnych naukowców z informatyki.

9. Zweryfikowanie jakości nauczania (treści oraz umiejętności prowadzących) wszystkich szkoleń i studiów podyplomowych w przyuczaniu osób z innymi niż teleinformatyczne zawodami do pracy jako specjaliści teleinformatyki. [lepiej, aby nie było casusu Collegium Humanum].
10. Stałe weryfikowanie jakości i dostępności oraz użyteczności wszystkich aplikacji teleinformatycznych udostępnianych przez administrację publiczną i samorządową do wykorzystania przez obywateli (z uwzględnieniem osób młodych, pracujących zawodowo, starszych oraz z niepełnosprawnościami, itp.). Utrzymywanie klasycznych procedur administracyjnych dla osób nie „akceptujących” rozwiązań teleinformatycznych.
11. Wprowadzenie wymogu na opracowanie rozwiązań teleinformatycznych umożliwiających ograniczone (ale skuteczne) użytkowanie aplikacji w warunkach niezwykłych (braku prądu, klęsk żywiołowych, katastrof, stanu zagrożenia lub wojny). Konieczne jest odpowiednie rozpropagowanie tych rozwiązań zastępczych.



POLSKIE TOWARZYSTWO INFORMATYCZNE

Zarząd Główny, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: + 48 22 838 47 05, tel./fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl, www.pti.org.pl

III. UWAGI SZCZEGÓŁOWE DO DOKUMENTU „STRATEGIA INFORMATYZACJI POLSKI”

Lp.	Strona	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
1.	59-62		Nieprawdziwe, propagandowe uwagi na temat cyberbezpieczeństwa zarówno dotyczące sprzętu jak i oprogramowania.	Stworzenie krajowych, bezpiecznych repozytoriów oprogramowania typu <i>open source</i> zgodnie z zaleceniami Komisji Europejskiej przeznaczonych dla administracji rządowej samorządowej i szeroko rozumianego szkolnictwa.	Nie ma bezpieczeństwa administracji, skoro nie istnieje system weryfikacji zarówno oprogramowania i zweryfikowanych urządzeń służących do komunikacji produkowanych niekiedy przez dostawców wysokiego ryzyka (np. wielcy dostawcy pochodzący z Chin). Da to ogromną oszczędność z Chin). Da to ogromną oszczędność liczoną w miliardach złotych rocznie.
2.	65-67		Zobowiązanie urzędów do stosowania tam, gdzie tylko jest to możliwe dokumentów o formacie zgodnym z oprogramowaniem opartym na otwartym kodzie źródłowym.	Ustawowe usankcjonowanie zakazu wymagania od obywateli w komunikacji elektronicznej korzystania z formatów dokumentów komercyjnych producentów oprogramowania.	Architektura Informacyjna Państwa (AIP) nie może bazować na produkcie firmy Microsoft i przymuszać obywateli do zakupu oprogramowania typu MS Office (Word, Excel,...). Urzędy, szkoły i obywatel musi płacić rocznie miliardy, aby móc korzystać z technik teleinformatycznych.
3.	168	Polska jest państwem o silnym sektorze IT, który jednak w niewielkim	Polska administracja nie wykorzystuje ani nie wspiera potencjału <i>open source</i> . <i>open-source</i> to nie tylko oprogramowanie, ale również sprzęt - dla przykładu, otwarta	Polska jest państwem o silnym sektorze IT, w którym administracja w niewielkim stopniu wykorzystuje czy nawet promuje potencjał rozwiązań typu <i>open source</i> w obszarze oprogramowania czy sprzętu.	Nasi informatycy i elektronicy są dosyć dobrze znani w świecie <i>open source</i> . Jest wielu specjalistów tworzących otwarte narzędzia i systemy, ale bardzo często dla zagranicznych klientów lub w wolnym czasie, za darmo. <i>Open</i>

		stopniu wykorzystuje potencjał otwartego oprogramowania.	architektura mikroprocesorów RISC-V, która obecnie buduje potęgę Chin, pomimo różnych blokujących regulacji (cła, embarga), czy też różnego rodzaju projekty DIY/FAB		source to nie tylko oprogramowanie, ale też sprzęt.
4.		Jako jedno z nielicznych państw UE, nie posiada strategii rozwoju i wspierania otwartego oprogramowania.	To nie jest tylko kwestia strategii, ale aktywnych narzędzi promujących i wspierających rozwój <i>open source</i> .	Jako jedno z nielicznych państw UE, Polska nie posiada strategii rozwoju ani narzędzi promocji czy wspierania otwartego oprogramowania.	Polacy, którzy tworzą <i>open source</i> powinni mieć aktywne wsparcie państwa w formie grantów, dofinansowań, czy ulg za stosowanie, a tym bardziej tworzenie rozwiązań Open-Source. To są bardzo często drogie do wytworzenia rozwiązania, które później dostępne są dla wszystkich za darmo, nie gwarantując nawet podstawowych środków na przeżycie. Stąd potencjał marnuje się, ponieważ inżynierowie wybierają komercyjne kontrakty skutkujące zamkniętymi produktami firm zagranicznych.
5.		Równocześnie, tworzenie i wykorzystywanie otwartego oprogramowania są ważnym narzędziem pozwalającym zapewnić suwerenność cyfrową. ..	Nie tylko oprogramowania, ale również sprzęt. Wszystkie rozwiązania software determinuje hardware, na którym działa, włącznie z całym ekosystemem narzędziowym, kompilatorami, bibliotekami, systemami, sterownikami, itp. Komputery PC zdominowała architektura Intel x86, obecnie	Równocześnie, tworzenie i wykorzystywanie otwartego oprogramowania oraz sprzętu jest ważnym narzędziem pozwalającym zapewnić suwerenność cyfrową. .. Otwarte oprogramowanie pozwala też budować powiązania między sektorem IT oraz różnorodnymi środowiskami rozwijającymi i korzystającymi z technologii, a otwarte	Oprogramowanie musi działać na jakimś sprzęcie (np. RISC-V). Sprzęt również jest uzależniającym narzędziem kontroli. Nie ma prawdziwie otwartego rozwiązania, jeśli nie jest to połączenie wolnego oprogramowania i sprzętu, na którym działa. Podobnie wszystkie co raz bardziej popularne "gotowe" rozwiązania AI są narzędziem kontroli. Prawdziwą suwerenność mamy wtedy, gdy zupełnie niezależnie od świata zewnętrznego możemy wyprodukować -

		<p>Otwarte oprogramowanie pozwala też budować powiązania między sektorem IT oraz różnorodnymi środowiskami rozwijającymi i korzystającymi z technologii</p>	<p>wyparta przez ARMv64 i powoli wypierana przez ARM.</p> <p>Na horyzoncie pojawia się architektura RISC-V, którą można napisać samodzielnie w małym lub dużym układzie FPGA, obudować akceleratorami AI lub innymi dedykowanymi blokami funkcjonalnymi, a następnie wyprodukować masowo jako ASIC.</p> <p>Powinniśmy stworzyć i rozwijać inicjatywy DIY/FAB, które pozwolą na lokalną produkcję kompletnych urządzeń na podstawie otwartych schematów (blueprints).</p>	<p>architektury i projekty sprzętowe dają niezależność w projektowaniu, adaptacji, produkcji, i aplikacji całkowicie wolnych i niezależnych rozwiązań.</p>	<p>całkowicie od podstaw i samodzielnie - kompletne urządzenia / produkty w sposób zautomatyzowany - komponenty elektroniczne i elektroniczne, komponenty mechaniczne, oprogramowanie.</p>
6.	168	<p>W ostatnich latach przykładem takiego podejścia jest rozwój polskich, otwartych modeli językowych wykorzystywanych w metodach AI, oraz udział naszych inżynierów w otwartych inicjatywach narzędziowych, systemów operacyjnych OS/RTOS, rozwiązań IoT, itp.</p>	<p>LLM jest tylko popularnym terminem w ramach AI, ale przecież <i>open source</i> to systemy operacyjne (OS / RTOS), narzędzia, sterowniki, platformy, urządzenia, itp.</p>	<p>W ostatnich latach przykładem takiego podejścia jest rozwój polskich, otwartych modeli językowych wykorzystywanych w metodach AI, oraz udział naszych inżynierów w otwartych inicjatywach narzędziowych, systemów operacyjnych OS/RTOS, rozwiązań IoT, itp.</p>	<p>AI to tylko mały obszar, jest dużo więcej projektów, w których Polacy współtworzą otwarte narzędzia, architektury, systemy operacyjne (OS/RTOS), technologie IoT, itp.</p>
7.	169	Cel 1	<p>Brakuje programów wsparcia freelance. Jeśli rozwiązania są otwarte to powinny stosować</p>	<p>e) Stworzenie narzędzi wsparcia i rozwoju dla niezależnych specjalistów.</p>	<p>Przetargi wspomniane w punkcie C są znane z wdrożeń komercyjnych rozwiązań i niekoniecznie pasują do</p>



			rozwiązania wsparcia znane z tego obszaru (np. Bounty, LFX https://crowdfunding.lfx.linuxfoundation.org/ , kontrakty, itp).		świata <i>open source</i> , ponieważ zakładają udział dużych firm i pomijają niezależnych badaczy / inżynierów, których można zadaniować / rozliczać, bazując na innych metodach jak kontrakty, bounty, LFX, itp.
8.	170	Cel 2	Jest mowa tylko o otwartym oprogramowaniu nie ma mowy o sprzęcie. Wolne oprogramowanie działać na wolnym sprzęcie a nawet kompletnych dedykowanych urządzeniach produkowanych lokalnie na podstawie ogólnodostępnych schematów (blueprint).	<p>Cel 2. Poziom tworzenia i wykorzystania otwartego oprogramowania oraz sprzętu przez polskie firmy i polskich programistów jest wyższy.</p> <p>Co umożliwi realizację celu:</p> <p>a) Wprowadzenie instrumentu finansowania dla firm i inżynierów na tworzenie otwartego oprogramowania oraz sprzętu;</p> <p>b) Wsparcie rozwoju otwartych systemów sztucznej inteligencji oraz ich wdrażania w administracji publicznej;</p> <p>c) Wsparcie rozwoju otwartych rozwiązań dla administracji na poziomie lokalnym, połączone ze wsparciem dla lokalnych firm i gmin wdrażających oprogramowanie.</p>	Nie zapominajmy o sprzęcie oraz niezależnej produkcji i projektowaniu :-)
9.	171	4.7 Cyfrowa i zielona transformacja	Zielona transformacja obecnie przyczynia się do załamania gospodarki w EU podczas gdy inne kraje wykorzystują sytuację, zwiększając sprzedaż; stajemy się co raz bardziej uzależnionymi od	<p>Powinniśmy tutaj również włączyć rozwiązania <i>open source</i> (software i hardware), które każdy może będzie mógł zastosować a nawet samodzielnie wyprodukować (DIY) lub zlecić produkcję w lokalnym punkcie specjalistycznym (FAB), na zasadzie "jest specjalistycznym (FAB), na zasadzie "jest</p>	Zamiast ograniczać skuteczne rozwiązania, należy skupić się na opracowaniu nowych technologii, metod produkcji, odzyskiwania i ponownego wykorzystania surowców, a także planowanemu wydłużaniu życia produktów i możliwości ich naprawy

			<p>dostawców zewnętrznych konsumentami. Nie możemy kierować się ideologiami – w świecie technologii jest to destruktywne.</p>	<p>potrzebne” (need-to-have), co może zmniejszyć konsumpcjonizm, zwiększyć poziom świadomości i umiejętności społeczzeństwa, uniezależnić się od “toksycznych producentów” czy niestabilnych łańcuchów dostaw.</p>	<p>oraz ponownego zastosowania. Obecnie produkty są celowo postarzane, co warunkowane jest maksymalizacją zysków (gospodarka nieograniczonego wzrostu), pomijając wpływ na środowisko. Należy cyklicznie weryfikować i rozliczać efektywność ideologii często wprowadzanych siłowo, bez społecznej akceptacji.</p> <p>Należy wspierać i promować lokalne inicjatywy Open-Source/DIY/FAB.</p>
--	--	--	---	--	--

Dokument
podpisany przez
Wiesław
Paluszynski
Data: 2024.12.09
07:18:19 CET

