mgr Krzysztof Żerebiec
Menedżerska Akademia Nauk Stosowanych w Warszawie
ORCID: 0009-0009-7175-8154

https://doi.org/10.29316/9788368103243_15

CYBERBEZPIECZEŃSTWO A OCHRONA DANYCH OSOBOWYCH

CYBERSECURITY AND PERSONAL DATA PROTECTION

Streszczenie

Problem badawczy postawiony w niniejszym rozdziale dotyczy kwestii tego, jak istotna jest świadomość zagrożeń użytkowników sieci wobec obecnych wyzwań w obszarze ochrony danych osobowych w cyberprzestrzeni. Przyjęta hipoteza zakłada, że w przypadku ochrony danych osobowych w cyberprzestrzeni, gdzie przenosi się całe funkcjonowanie społeczeństwa i obrót gospodarczy, kluczowe znaczenie ma świadomość zagrożeń u użytkowników Internetu. Do analiz wykorzystano badanie dokumentów, aktów prawa i dostępnej literatury przedmiotu.

Słowa kluczowe: dane osobowe, cyberprzestrzeń, cyberzagrożenia, bezpieczeństwo

Abstract

The research problem addressed in this chapter concerns the extent to which user awareness of threats is significant in the face of current challenges in the field of personal data protection in cyberspace. The adopted hypothesis assumes that in the context of personal data protection in cyberspace, where the functioning of society and economic transactions are increasingly transferred, the key factor is the awareness of threats among Internet users. The analysis is based on the examination of documents, legal acts, and the available subject literature.

Keywords: personal data, cyberspace, cyberthreats, security

Wstęp

Cieszymy się światem połączonym w sieci na wiele sposobów, ponieważ daje nam nowe możliwości i perspektywy, ale otwiera też zupełnie nowe terytoria niepokoju, zagrożenia i przemocy, gdyż poczucie przewidywalności świata zanika[1]. Rozważania nad problematyką ochrony danych osobowych w sieci wymagają zdefiniowania pojęcia cyberbezpieczeństwa i cyberprzestrzeni. Najogólniej mówiąc zagrożenia cyberbezpieczeństwa to zagrożenia cyberprzestrzeni i w cyberprzestrzeni. Konieczne jest wyodrębnienie cech konstytutywnych pojęcia cyberprzestrzeni – zdefiniowanie tego pojęcia, co jest elementem niniejszego opracowania.

Przez wyzwania cyberbezpieczeństwa z jednej strony można rozumieć techniczne komponenty cyberbezpieczeństwa zaś z drugiej strony merytoryczne zagrożenia dla cyberbezpieczeństwa. Zagrożenia dla cyberbezpieczeństwa są bardzo liczne i z każdym dniem dochodzą nowe vide kwestia funkcjonowania rozwiniętych zaawansowanych modeli AI (Artificial Intelligence) jak Chat GPT 4.0.

W ciągu ostatniej dekady jesteśmy świadkami przenoszenia, właściwie wszystkich dziedzin ludzkiej aktywności tak indywidualnej jak i społecznej, tak publicznej jak i prywatnej do sieci. Upowszechnienie się bankowości internetowej, szybki rozwój e-handlu oraz rozwój mediów społecznościowych, które dla coraz większej populacji stają się podstawowym źródłem informacji sprawia, że wraz z różnymi aktywnościami społecznymi również przestępczość i patologie społeczne przenoszą się do sieci. Znaczenie Internetu dla funkcjonowania infrastruktury, w tym infrastruktury krytycznej państw rozwiniętych sprawia, że sieć staje się miejscem wojny hybrydowej. Skuteczny atak hakerski może sparaliżować oficjalne strony rządowe, ale również ruch kolejowy, funkcjonowanie systemu bankowego czy systemu dystrybucji energii elektrycznej. Ataki takie niejednokrotnie podejmowała Rosja w stosunku do Estonii czy Ukrainy. Przykładem ataków hakerskich na firmy i agencje rządowe takie jak FBI (Federal Bureau of Investigation), Pentagon, Novell, Pacific, Bell jest Kevin Mitnick, który zdecydowaną większość ataków przeprowadził korzystając z naiwności ludzi oraz metod socjotechniki. Mawiał on „łamałem ludzi, nie hasła”[2]. Firma

[1] S. Zuboff, *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, Zysk i S-ka, Poznań 2019, s. 14.

[2] E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, dz. cyt., s. 95.

może posiadać najnowsze technologie i sprzęt oraz mieć wyszkolony personel, ale wobec takich ludzi jak Kevin Mitnick wciąż pozostaje niezabezpieczona. Technika jego działania okazała się być bardzo skuteczna, doprowadził do wielu włamań komputerowych jak również wszedł w posiadanie setek poufnych informacji.

Mimo wielu publikacji dotyczących bezpieczeństwa w cyberprzestrzeni nie ma jednej i obowiązującej definicji cyberprzestrzeni, traktowanej jako środowisko bezpieczeństwa użytkujących ją jednostek.

Pojęcie cyberbezpieczeństwa

Cyberprzestrzeń jest pewną przestrzenią wirtualną (niefizyczną). Sam termin cyberprzestrzeń w aspekcie etymologicznym jest hybrydą i pochodzi ze złożenia nazw *space* (ang. przestrzeń) i *cybernetics* (ang. cybernetyka)[3]. *Cyberspace*, czyli cyberprzestrzeń jako przestrzeń wirtualna może być definiowana na wiele sposobów. Istnieją zarówno definicje prawne cyberprzestrzeni (konieczne z uwagi na szereg aktów prawa obowiązującego powszechnie jak i prawa wewnętrznego), które formułują zadania w zakresie ochrony cyberprzestrzeni. Przykładem takiej definicji jest ujęcie ustawowe, zgodnie z którym cyberprzestrzeń to cyfrowa przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[4].

Kolejna definicja cyberprzestrzeni, która jest powszechnie cytowana została sformułowana przez Departament Obrony USA, według którego cyberprzestrzeń to: „globalna domena środowiska informacyjnego składająca się ze współzależności (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, a także osadzone w nich procesory i kontrolery”[5].

Wykorzystując tę definicję cyberprzestrzeni można wprowadzić pojęcie cyberbezpieczeństwa jako bezpieczeństwa procesów przetwarzania informacji (danych) w cyberprzestrzeni. W oczywisty sposób pojęcie cyberbezpieczeństwa

---

[3] W. Gogołek, W. Cetera, *Leksykon tematyczny: zarządzanie, IT,* Wydział Dziennikarstwa i Nauk Politycznych. Uniwersytet Warszawski, Warszawa 2014, s. 207.

[4] *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2002 r. Nr 156, poz. 1301), art. 2. ust 1b.

[5] E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2016, s. 71-72.

dotyczy również przetwarzania w cyberprzestrzeni danych, informacji szczególnej kategorii, jakimi są dane osobowe.

Inna definicja cyberprzestrzeni podkreśla socjologiczny aspekt funkcjonowania Internetu. Zgodnie z nią cyberprzestrzeń stanowi wirtualną iluzję świata rzeczywistego, której podstawą działania są systemy teleinformatyczne (w praktyce systemy komputerowe połączone siecią) i która jej użytkownikom służy do wymiany, gromadzenia i udostępniania informacji za pomocą komputerów lub telefonów. Cyberprzestrzeń oferuje ogromne możliwości, m.in. e-learning, e-administrację, telepracę, etc.[6] W tym rozumieniu cyberprzestrzeń stanowi przestrzeń społeczną (wirtualną, niefizyczną), która służy do interakcji jej użytkowników, internautów[7].

A zatem najbardziej fundamentalne rozumienie pojęcia cyberbezpieczeństwa to rozumienie go jako bezpieczeństwa cyberprzestrzeni, cyberbezpieczeństwo to bezpieczeństwo dotyczące przetwarzania informacji i danych w przestrzeni wirtualnej funkcjonującej dzięki cyfrowemu systemowi teleinformatycznemu w postaci komputerów połączonych siecią Internet. Skrótowa i syntetyczna definicja cyberbezpieczeństwa występująca w literaturze przedmiotu oraz w polskich dokumentach[8] określa cyberbezpieczeństwo „mianem bezpieczeństwa technologii informatycznych i definiowane jest jako odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne”[9]. Cyberbezpieczeństwo nie dotyczy bowiem jedynie zabezpieczenia pewnej technologii *in abstracto*, co może być zadaniem np. służby kontrwywiadu, lecz zapewnieniu bezpieczeństwa funkcjonowania przestrzeni wirtualnej, która funkcjonuje w oparciu o technologie informatyczne. Dodajmy tu, że w ogólnym przypadku tak rozumiane cyberbezpieczeństwo obejmuje zarówno bezpieczeństwo infrastruktury materialnej zapewniającej przetwarzanie

[6] Tamże, s. 73.

[7] M. Radochoński, B. Przywara, *Jednostka, grupa, cybersieć: psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*, Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania, Rzeszów 2004, s. 157.

[8] K. Bakalarczyk-Burakowska, J. Nowicka, *Cyberbezpieczeństwo a ochrona danych osobowych*, [w:] *Społeczeństwo jako uczestnik bezpieczeństwa*, red. J. Nowicka, dz. cyt., s. 32.

[9] *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, s. 28.

danych przez systemy teleinformatyczne (hardware) jak i bezpieczeństwo samej przestrzeni wirtualnej (software). Dla ustalenia uwagi autor podkreśla tu, że w tej pracy rozważana będzie wyłącznie problematyka cyberbezpieczeństwa w rozumieniu software. Analogicznie jak w przypadku pojęcia bezpieczeństwa narodowego i bezpieczeństwa wewnętrznego, również w przypadku cyberbezpieczeństwa można i należy mówić o cyberbezpieczeństwie w rozumieniu statycznym (jako pewnym optymalnym stanie funkcjonowania w cyberprzestrzeni) jak i o cyberbezpieczeństwie w rozumieniu dynamicznym i procesowym (jako pewnym procesie obejmującym zespół działań), którego celem jest zapewnienie niezakłóconego i wolnego od niepożądanych działań zewnętrznych funkcjonowania procesów przetwarzania danych w cyberprzestrzeni. Powszechna cyfryzacja i przenoszenie wszelkiej aktywności do globalnej sieci Internetu spowodowały jego powszechność. W rezultacie w Internecie pojawili się wszyscy, dobrzy i źli, zwykli ludzie oraz różne organizacje oraz wielkie globalne korporacje[10] co spowodowało, że cyberprzestrzeń nie pozostała wolna od różnego rodzaju zagrożeń.

Znaczenie terminu cyberbezpieczeństwa wskazuje na konstytutywne cechy tego pojęcia, które należy również rozumieć jako ogół działań, metod, procedur i technik, które mają na celu zapewnienie ochrony cyberprzestrzeni przed nieautoryzowanym dostępem, atakami, uszkodzeniami i kradzieżą danych w cyberprzestrzeni. Tak rozumiane cyberbezpieczeństwo jest dynamicznym procesem i stanowi zbiór działań, których celem jest zapewnienie odporności cyberprzestrzeni przed niepożądanymi, bezprawnymi działaniami. Cyberbezpieczeństwo to obszar bezpieczeństwa, którego znaczenie z racji postępu technologicznego systematycznie wzrasta[11]. Celem takich działań jest cyberbezpieczeństwo rozumiane jako stan równowagi, w którym przetwarzane w cyberprzestrzeni dane są zabezpieczone poprzez odpowiednie procedury w ten sposób, że są one zabezpieczone przed bezprawną ingerencją w zakresie poufności, autentyczności, wiarygodności i minimalizacji prawdopodobieństwa uzyskania dostępu do nich przez podmioty nieuprawnione do tego.

[10] R. Szpyra, *Cyberbezpieczeństwo militarne w amerykańskiej praktyce*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2016, s. 7.

[11] K. Bakalarczyk-Burakowska, J. Nowicka, *Cyberbezpieczeństwo a ochrona danych osobowych*, [w:] *Społeczeństwo jako uczestnik bezpieczeństwa*, red. J. Nowicka, dz. cyt., s. 32.

W innym jeszcze rozumieniu problematyka cyberbezpieczeństwa jest to problematyka zapewnienia bezpieczeństwa przetwarzania danych w przestrzeni teleinformatycznej (cyberprzestrzeni). Jest to bardzo szeroka tematyka z uwagi na różnorodność zagrożeń dla bezpieczeństwa cyberprzestrzeni. Nie chodzi przy tym wyłącznie o wyzwania techniczne związane z przetwarzaniem danych cyfrowych. poważnym wyzwaniem jest analiza całych wolumenów danych i przetwarzanie ich na masową skalę[12].

Kolejny aspekt rozumienia pojęcia cyberbezpieczeństwa obejmuje instytucjonalne cyberbezpieczeństwo. Instytucje służące zapewnieniu cyberbezpieczeństwa to z jednej strony jednostki organizacyjne i organy władzy publicznej, których celem jest zapewnienie bezpieczeństwa przetwarzania danych w przestrzeni teleinformatycznej, zaś z drugiej strony instytucje służące zapewnieniu cyberbezpieczeństwa, to ogół aktów prawnych (aktów prawa międzynarodowego oraz prawa UE wtórnego, ustaw i rozporządzeń wykonawczych do nich) oraz aktów prawa wewnętrznego (Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024), których celem jest zapewnienie bezpieczeństwa przetwarzania danych w sieci. Przykładem takiej instytucji jest omawiane już powyżej Rozporządzenie Parlamentu Europejskiego i Rady.

W zakresie instytucji, których celem jest zapewnienie cyberbezpieczeństwa, kluczowe znaczenie spośród polskich aktów normatywnych ma Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa[13].

Współczesne zagrożenia w cyberprzestrzeni

Postępująca konwergencja technologii informatycznych, telekomunikacyjnych i mediów, a w konsekwencji infosfery, socjosfery i technosfery przyniosła nową jakość w postaci fenomenu cyberprzestrzeni[14]. Istnieje wiele ujęć określających to pojęcie: cyberprzestrzeń to Internet, jego zasoby i usługi oraz użytkownicy. Utożsamiane jest ono z wirtualną rzeczywistością generowaną przez komputer, sieć i Internet[15]. Cyberprzestrzeń jest wymiarem aktywności,

[12] J. Kurek, *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big data*, dz. cyt., s. 198.

[13] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2018 r. poz. 1560).

[14] P. Sienkiewicz, *Ontologia cyberprzestrzeni*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, t. 9, nr 13, 2015, s. 89-91.

[15] J. Nowicka, red., *Społeczeństwo jako uczestnik bezpieczeństwa*, dz. cyt., s. 12.

w której wszelkie działania odbiegają charakterem od środowiska fizycznego[16]. Obok środowiska lądowego, morskiego, powietrznego jak i kosmicznego jest to nowy wymiar, w którym można prowadzić działania[17].

Cyberprzestrzeń charakteryzuje się następującymi cechami[18]:

- niezależnością od miejsca,
- niezależnością od odległości,
- niezależnością od czasu,
- niezależnością od granic,
- względną anonimowością,
- możliwością ustalenia sprzętu, nie osoby.

Można zatem twierdzić, że zapewnia anonimowość, aterytorialność, systematyczność i globalny zasięg[19]. Cyberprzestrzeń spełnia również inne ważne funkcje i kilka podstawowych zostanie wyróżnionych[20]:

- funkcja informacyjna, która określa, iż jest ona przestrzenią ciągłej wymiany informacji, i pozwala na szybkie uzyskanie informacji z niemalże każdego aspektu życia człowieka czy też nauk,
- funkcja ludyczna (rozrywkowa), której istota pozwala na zaspokajanie potrzeb człowieka związanych z rozrywką czy oderwaniem się od codziennych zajęć,
- funkcja stymulująca, stanowiąca inspirację odbiorców do aktywnego odbioru treści znajdujących się w cyberprzestrzeni,
- funkcja wzorcotwórcza, odnosząca się do zjawisk tworzenia nowych standardów, ideałów czy też stylów życia, które obserwujemy wraz z rozwojem cywilizacyjnym,
- funkcja interpersonalna, gdzie stanowi przestrzeń mieszania się kultur, gromadząc przy tym różne idee oraz informacje z całego świata, gdzie

[16] A. Chrząszcz, J. Nowicka, red., *Współczesny wymiar bezpieczeństwa państwa*, Wydawnictwo Wyższej Szkoły Menedżerskiej, Warszawa 2021, s. 143.

[17] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, Przegląd Teleinformatyczny, nr 1(2), 2018, s. 59-72.

[18] T. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego, t. 8, nr 15, 2016, s. 11.

[19] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, Przegląd Teleinformatyczny, nr 1(2), 2018, dz. cyt., s. 60.

[20] P. Sienkiewicz, *Ontologia cyberprzestrzeni*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, t. 9, nr 13, 2015, dz. cyt., s. 61.

dochodzi do zacierania się różnic pomiędzy kulturami. Jest również obszarem ciągłych starć i konfliktów, a także przestrzenią, w której obecne są wirtualne byty.

Każda z wymienionych funkcji może być realizowania zarówno dla celów budowania bezpiecznej przestrzeni, jak i dla działań destrukcyjnych w tym obszarze.

Coraz większe znaczenie ma wojna informacyjna, zmasowane i profilowane ataki informacyjne prowadzone szczególnie intensywnie w mediach społecznościowych podczas kampanii wyborczych. Przykładem mogą być tu kampania przed referendum brexitowym i przed wyborami prezydenckimi w USA, w których wygrał D. Trump. Zatem z uwagi na fakt, że następuje migracja do Internetu wszystkich dziedzin ludzkiej aktywności, wraz z tą migracją do sieci i cyberprzestrzeni przenoszą się również zagrożenia. Podstawowe rodzaje wybranych cyberzagrożeń przedstawiono w tabeli 1.

Tabela 1. Podstawowe rodzaje cyberzagrożeń

Zjawisko	Cechy charakterystyczne
Cyberprzemoc	Wykorzystanie cyberprzestrzeni w celu wymuszenia odbioru niepożądanych komunikatów zawierających informacje (dane, obrazy, treści) sprzecznych z wartościami adresata.
Cyberprzestępstwo	Wykorzystanie cyberprzestrzeni w celu dokonania ataków kryminalnych pospolitych i zorganizowanych skierowanych na zasoby osób prywatnych i/lub organizacji (instytucji).
Cyberinwigilacja	Wykorzystanie cyberprzestrzeni w celu kontroli i/lub pozyskania informacji o zachowaniach i działaniach obywateli (społeczności, społeczeństwa) (efekt *Big Brother).*
Cyberterroryzm	Wykorzystanie cyberprzestrzeni w celu działań terrorystycznych (państwowych i pozapaństwowych).
Cyberautorytaryzm	Wykorzystanie cyberprzestrzeni w życiu politycznym państwa w sprzeczności z zasadami demokracji liberalnej (przeciwieństwem – cyberdemokracja).
Cyberwojna	Wykorzystanie cyberprzestrzeni w celu realizacji działań politycznych realizowanych przez siły zbrojne (*cyberwarriors)* i skierowane na zasoby i struktury państwa przeciwnika (również w działaniach innych niż wojna).

Źródło: P. Sienkiewicz, *Ontologia cyberprzestrzeni,* Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, t. 9. nr 13, 2015, s. 97.

Dostęp do sieci jest powszechny, więc coraz częściej zostaje wykorzystywany przeciwko społeczeństwu, które jest narażone na wiele działań,

określanych jako przestępczość cybernetyczna[21]. Zagrożenia te mają charakter zarówno zagrożenia typową przestępczością kryminalną przeciwko mieniu, której celem jest wyłudzenie mienia (oszustwa internetowe i kradzieże), wyłudzenia kredytów i pożyczek, możliwe dzięki uzyskanym w sieci danym osobowym jak i z przestępczością przeciw wolności seksualnej i obyczajności (rozpowszechnianie treści pedofilskich). Sieć stała się idealnym miejscem prania brudnych pieniędzy przy wykorzystaniu technologii blockchain, zapewniającej wysoki poziom anonimowości. Internet wykorzystywany jest do werbowania najemników, finansowania działalności terrorystycznej i szeregu innych przestępstw. Cyberterroryzm jest formą terroryzmu wykorzystującą cyberprzestrzeń jako pole działania. Celem nadrzędnym jest wywołanie paniki lub zastraszenia, tak aby osiągnąć zamierzenia polityczne lub zmusić władze do konkretnych działań[22]. Sprawą mniejszej wagi, lecz dokuczliwą jest masowe profilowanie użytkowników sieci (w szczególności mediów społecznościowych) i po uzyskaniu ich danych osobowych następuje przekazanie im masowo odpowiednio targetowanego spamu.

Identyfikacja i klasyfikacja zagrożeń i wyzwań dla cyberbezpieczeństwa powinna zostać oparta o ich podział z uwagi na kryterium podmiotowe i przedmiotowe. W tym pierwszym przypadku zagrożenia dzielimy w oparciu o to czy stanowią zagrożenia dla osób fizycznych i prawnych – podmiotów prawa prywatnego, czy też stanowią one zagrożenia dla państwa, jego obronności, organów konstytucyjnych, stabilności ustroju, procesu wyborczego etc. Innymi słowy zagrożenia te polegają na takiej ingerencji zewnętrznej w proces przetwarzania danych, które godzą w pewne interesy publiczne – bezpieczeństwo publiczne, proces wyborczy, obronność danego państwa jak i takie, które godzą w interesy prywatne – dobra majątkowe osób fizycznych i jednostek organizacyjnych jak również ich dobra osobiste (godność, dobre imię). I tak zagrożenia bezpieczeństwa osobistego i majątkowego podmiotów prawa prywatnego – osób fizycznych i prawnych będących użytkownikami sieci są praktycznie zawsze związane z bezprawnym przetwarzaniem danych osobowych osób fizycznych w zabronionym celu. Druga klasa zagrożeń obejmuje zagrożenia dla obrotu społeczno-gospodarczego oraz infrastruktury (w tym infrastruktury

[21] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki, organizacji, państwa*, CeDeWu, Warszawa 2020, s. 203.

[22] Tamże, s. 105.

krytycznej). W doktrynie używa się w tym przypadku pojęcia cyberterroryzm. Jego nadrzędnym celem jest dezinformacja oraz prowadzenie walki psychologicznej[23].

Kolejna klasa zagrożeń obejmuje zagrożenia dla stabilności politycznej państwa, instytucji państwa, procesów wyborczych etc. W przypadku tych zagrożeń używane bywa pojęcie wojny hybrydowej, która w obecnych realiach międzynarodowych ma coraz większe znaczenie. Praktyki określane mianem wojny hybrydowej (wojna propagandowa, manipulowanie opinii publicznej, intensywna propaganda wykorzystująca boty i farmy trolli) są prowadzone intensywnie przez Rosję, KRLD (Koreańska Republika Ludowo-Demokratyczna) i w pewnej mierze również Chiny. Zagrożenia wreszcie z uwagi na ich źródło można podzielić na wewnętrzne (generowane przez podmioty zlokalizowane w obrębie państwa/społeczności), która padła ofiara ataku i zewnętrzne (gdy pochodzi z terytorium obcego państwa). W praktyce zagrożenia dotyczące drugiej kategorii i trzeciej przenikają się wzajemnie z uwagi na globalny charakter sieci i stąd podział ten nie rości sobie pretensji do bycia podziałem logicznym (rozłącznym i wyczerpującym)[24]. Zagrożenia prywatnych interesów osób fizycznych i prawnych w cyberprzestrzeni są zwykłą ekstrapolacją przestępstw znanych ludzkości od zarania dziejów do cyberprzestrzeni. Są to kradzieże pieniędzy i papierów wartościowych z rachunków bankowych, kart płatniczych, wyłudzenia kredytów i pożyczek (w Internecie dokonywane często dzięki wyłudzeniu danych osobowych i kradzieży tożsamości). Cyberprzestrzeń jest również miejscem naruszenia dóbr osobistych i zniesławiania poprzez rozpowszechnianie określonych treści. Internet z uwagi na anonimowość i multimedialność są idealnym medium służącym przestępcom do rozpowszechniania treści pedofilskich i tzw. hard porno jak również stręczycielstwa, szantażu obyczajowego i szeregu innych przestępstw przeciw wolności seksualnej obyczajowości. Internet stworzył również szeroką przestrzeń działania dla stalkerów. Ta problematyka wiąże się ściśle z kwestią wyłudzania i kradzieży danych osobowych, co jest w praktyce powszechne w sieci i z czym mimo szeregu regulacji tak międzynarodowych jak i krajowych nie potrafiono

[23] E. Lichocki, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Wydawnictwo Akademii Marynarki Wojennej, Gdynia 2011, s. 34.

[24] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, portal winntbg.bg.agh.edu.pl, https://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf, [dostęp: 11.04.2023].

sobie poradzić. Należy podkreślić, że rozwój cyberprzestępczości związany jest z powstawaniem coraz skuteczniejszych narzędzi przeznaczonych do celów przestępczych[25]. Przestępstwa te mogą być dokonywane przy użyciu legalnych środków (np. zwykłego serwisu ogłoszeniowego), ale również poprzez zastosowanie instrumentów, których użycie (niezależnie od motywacji i celu) jest przestępstwem, a zatem przy wykorzystaniu wirusów, trojanów i robaków komputerowych, których samo używanie stanowi przestępstwo stypizowane w kodeksie karnym. W tym drugim przypadku mamy do czynienia ze zbiegiem przestępstw, stosowanie malware jest przestępstwem przeciw integralności systemu teleinformatycznego, zaś wyłudzanie danych użytkownika sieci i wyłudzenie za ich pomocą pożyczki jest zwykłym oszustwem stypizowanym w przepisach art. 286 kk. Do drugiej klasy zagrożeń w cyberprzestrzeni należy zagrożenie związane z przestępstwami przeciw obrotowi społeczno-gospodarczemu. Jest to pranie pieniędzy (dziś skutecznie dokonywane przy wykorzystaniu technologii blockchain), nielegalne rynki internetowe – rynek bukmacherski, czarny rynek broni i narkotyków w tzw. darknecie itp.

Współczesne pojęcie wojny hybrydowej i cyberterroryzmu dotyczy jednak działań realizowanych w cyberprzestrzeni, które godzą w infrastrukturę krytyczną (funkcjonowanie systemów bankowych, rynków finansowych, linii przesyłowych energii, elektrowni oraz funkcjonowanie organów władzy publicznej, urzędów etc.). Oznacza to, że ataku można dokonać z każdego miejsca na Ziemi. Cyberwojna jest konfliktem asymetrycznym[26]. Takie działania realizowane przez hakerów działających z własnej inicjatywy lub na zlecenie innego państwa i w jego imieniu mogą sparaliżować instytucje państwa, działanie linii przesyłowych czy transportu, zakłócić proces wyborczy czy doprowadzić do wypadków i katastrof[27]. Szczególnym zagrożeniem jest cyberatak, którego celem jest uniemożliwienie działania sieci w danym regionie. Przestają wówczas funkcjonować wszystkie struktury, których funkcjonowanie jest zależne od działania sieci. Inny rodzaj poważnego zagrożenia dla bezpieczeństwa

[25] E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, dz. cyt., s. 108.

[26] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki*, *organizacji, państwa*, dz. cyt., s. 213.

[27] J. Kowalewski, M. Kowalewski, *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, portal core.ac.uk, https://core.ac.uk/download/pdf/235207549.pdf, [dostęp: 11.04.2023].

całego państwa to wykorzystanie cyberprzestrzeni (a w szczególności forów, mediów społecznościowych etc. do siania zamętu i dezinformacji przy użyciu płatnych trolii oraz coraz częściej botów generujących wpisy). Na wielką skalę i skutecznie działania takie prowadzi Rosja wykorzystując słynna petersburską farmę trolii, założonej przez samego J. Prigożyna znanego dzisiaj jako szefa zbrodniczej grupy Wagnera. Działania trolii i botów są tanie i niesłychanie wydajne. Skutecznie wpłynęły na wynik referendum brexitowego i pierwszą elekcję Trumpa. Ponadto trudno je zwalczać, produkowanie najgłupszych nawet antyszczepionkowych wpisów czy fake newsów i ich rozpowszechnianie nie jest zabronione. Ten rodzaj zagrożenia jeszcze w wyższym stopniu zrealizował się w działaniach, które symbolizuje afera Cambridge Analytica. Firma ta posługiwała się namierzaniem behawioralnym, żeby przekazywać określone, popierające Trumpa treści, odpowiadające określonym wyborcom z bardzo osobistych powodów[28]. Masowa manipulacja propagandowa wyborcami, którym trolle (lub coraz częściej boty, gdyż jest to tańsze) przesyłają sprofilowane pod ich kątem informacje (targetowanie odbyło się przy wykorzystaniu profili na Facebooku i Twitterze) prowadzi do skutecznego wpływania na wynik wyborów[29].

Anne Applebaum w swoich pracach wielokrotnie podkreślała, że triumf prawicowych autorytaryzmów i populizmów w drugiej dekadzie XXI wieku jest w znacznym stopniu spowodowany wykorzystaniem możliwości Internetu w zakresie dezinformacji i propagandy. Tego zagrożenia, które jest szczególnie trudne do efektywnego zwalczania nie może dzisiaj lekceważyć żadne państwo, godzi ono w najbardziej podstawowe zasady porządku ustrojowego a walka z fake newsami i dezinformacją na Facebooku jest łatwa w Rosji czy Chinach, gdzie można ją prowadzić przy wykorzystaniu instytucji prawa karnego lub blokady serwisu, ale bardzo trudna w demokratycznych państwach prawnych[30].

---

[28] S. Galloway, *Wielka czwórka. Ukryte DNA: Amazon, Apple, Facebook i Google*, tłum. J. Kubiak, Dom Wydawniczy REBIS, Poznań 2018, s. 135.

[29] *Wywiad z dr. Michałem Kosińskim: Zgłaszali się do mnie autokraci, żeby im pomóc w wyborach. Z Polski też – program Świat, którym żyjemy*, portal wyborcza.pl, https://wyborcza.pl/10,82983,22715049,zglaszali-sie-do-mnie-autokraci-zeby-im-pomoc-w-wyborach-z.html, [dostęp: 13.04.2023].

[30] A. Applebaum, *Zmierzch demokracji: zwodniczy powab autorytaryzmu*, Wydawnictwo Agora, Warszawa 2020, s. 143-145.

Historia Państwa Islamskiego (ISIS) pokazuje też, że media społecznościowe (Facebook) mogą też zostać wykorzystane bezpośrednio do werbunku członków grup terrorystycznych i jest to metoda tania i skuteczna. Wykradanie danych w Internecie to zarówno wykradanie danych użytkowników indywidualnych w celu dokonania oszustwa czy kradzieży tożsamości jak i zorganizowane szpiegostwo przemysłowe oraz dotyczące technologii wojskowych i obronnych. Słynna akcja Izraela przeciw Iranowi (*Stuxnet)* polegająca na czasowym sparaliżowaniu irańskiego programu jądrowego poprzez zatrzymanie przez robaka komputerowego pracy wirówek wzbogacających uran do postaci, w której mógł on być wykorzystywany w bombie jądrowej, pokazuje w jaki sposób działania wojenne przenoszą się w znacznej mierze z przestrzeni fizycznej i rzeczywistej do cyberprzestrzeni. Potencjalni przestępcy z racji tego, iż są w większości anonimowi w sieci czują się praktycznie bezkarni a osoby poszkodowane bezradne[31]. Zagrożenia polegające na rozpowszechnianiu złośliwego oprogramowania, atakach internetowych na witryny, kradzieży danych etc. łamiące zabezpieczenia informacji godzą w pierwszy aspekt powyżej zdefiniowanego bezpieczeństwa teleinformatycznego. Z drugiej strony przestępczość godząca w użytkowników sieci i naruszająca zasady bezpieczeństwa teleinformatycznego w aspekcie podmiotowym, może polegać na działaniach niezwiązanych z przełamywaniem zabezpieczeń systemów teleinformatycznych, kradzieżą danych czy rozpowszechnianiem malware. Sieć stała się terenem działań terrorystów, szczególnie z ISIS wykorzystujących legalnie działające portale społecznościowe do werbowania członków, przygotowywania i finasowania działalności terrorystycznej. Klasycznym przykładem tego typu przestępczości jest również działanie pedofili wykorzystujących Internet do pozyskania dziecięcej pornografii i zawierania znajomości z małoletnimi. Jolanta Zmarzlik uważa, że dzieci „są łatwymi ofiarami, ponieważ nie mają dostatecznego doświadczenia są ufne i naiwne, a także, niestety, bardzo często samotne w swoich domach, szkołach i coraz mniej bezpiecznych podwórkach”[32]. Ten rodzaj zagrożeń bezpieczeństwa cybernetycznego wiąże się z przekazywaniem, oferowaniem i udostępnianiem zabronionych treści za pomocą legalnych, co do zasady środków.

[31] Z. Ciekanowski, *Współczesne zagrożenia bezpieczeństwa państwa. Cz. 1*, dz. cyt., s. 57.

[32] J. Zmarzlik, *Internetowe znajomości – lek na samotność w realnym świecie*, Dziecko Krzywdzone. Teoria, badania, praktyka, t. 4, nr 4, 2005, s. 70.

Zagrożenia bezpieczeństwa teleinformatycznego pierwszego rodzaju są generowane głownie przez działania celowe, z których najczęstszym jest tworzenie i rozprzestrzenianie złośliwego oprogramowania, (które działając automatycznie zmienia funkcjonowanie zainfekowanych nim systemów bez wiedzy i zgody użytkowników, co w języku potocznym jest nieściśle określane jako „wirus komputerowy"), oraz przeprowadzane zdalnie bezprawne manipulacje w obcych systemach określane potocznie jako „ataki komputerowe". Mogą to być zarówno ataki paraliżujące pracę określonych wybranych za cel ataku systemów lub ataki mające na celu wykradnięcie danych i oszustwa internetowe. Cyberprzestępczość ewoluuje i dostosowuje swoje narzędzia oraz techniki do postępu technologicznego[33]. Wprowadzając pojęcie zagrożeń bezpieczeństwa cyberprzestrzeni należy zwrócić uwagę na różnoraki charakter tych zagrożeń i wiążącą się z tym faktem konieczność wypracowania rozwiązań wielopłaszczyznowych, z jednej strony wykorzystujących instytucje prawa karnego i administracyjnego, z drugiej zaś edukację obywateli i uświadamianie im tych zagrożeń a także obecność w mediach społecznościowych i aktywne przeciwstawianie się propagandzie i dezinformacji za pomocą tych mediów, które są jej nośnikiem. Zauważmy bowiem, że walka z cyberatakami będącymi atakami terrorystycznymi, czyli włamaniami do systemów odpowiadających za funkcjonowanie infrastruktury (a w szczególności infrastruktury krytycznej) odbywa się w oparciu o przepisy krajowego prawa karnego (i konwencji międzynarodowych). Jednak współczesnym zagrożeniem cyberbezpieczeństwa jest w dużym stopniu propaganda i dezinformacja szerzona za pomocą mediów społecznościowych. Ma ona na celu zarówno ingerencję w konkretne procesy wyborcze jak i rozpowszechnianie nieprawdziwych informacji. W demokratycznym państwie prawnym nie jest możliwe cenzurowanie prewencyjne treści zamieszczanych w Internecie. Z drugiej zaś strony propagowanie w mediach społecznych absurdalnych i oszczerczych treści pod adresem np. Hillary Clinton czy Unii Europejskiej (może być to również skuteczność szczepionek), nie jest możliwe do sankcjonowania w trybie karnym czy administracyjnym. Tu zatem przeciwnik a konkretnie Rosja czy Chiny ma zdecydowaną przewagę w sytuacji, gdy około 30% populacji czerpie informacje o świecie z Facebooka czy Twittera, zamykając się w swoich bańkach społecznościowych, fake newsy rozpowszechniane na Facebooku i Twitterze przez trolli i boty, są

[33] M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 1-2.

zwielokrotniane i przekazywane dalej przez użytkowników tych mediów kolejnym osobom, tak w obrębie bańki jak i poza nią. Walka z taką dezinformacją (stanowiącą kluczowy element wojny hybrydowej) jest niezwykle trudna, *Scam* staje się coraz popularniejszym oszustwem internetowym i nie ma wątpliwości, że pomimo blokowania takich stron, kluczem do sukcesu w walce z takimi zagrożeniami jest odpowiednia świadomość zagrożeń u użytkowników sieci, która może być uzyskana jedynie poprzez ich właściwą edukację[34]. Najnowsze dane o poziomie cyberprzestępczości w 2022 roku pozwalają stwierdzić, że liczba incydentów dynamicznie rośnie. Ma to miejsce od pandemii, kiedy szereg aktywności przeniesiony został do sieci i tak już pozostało. Konkretyzując, w 2022 roku do CERT Polska zgłoszono aż o 176% więcej incydentów (przypadków zagrożenia cyberbezpieczeństwa) niż w roku 2021[35]. W 2022 roku zgłoszono aż 320 tys. przypadków zagrożeń cyberbezpieczeństwa.

Według CERT Polska najczęściej spotykanym obecnie rodzajem zagrożenia cyberbezpieczeństwa jest oszustwo komputerowe (przede wszystkim są to ataki phishing)[36]. W roku 2022 zaraportowano aż 34955 takich przypadków. Zagrożenia bezpieczeństwa związane z malware (złośliwym oprogramowaniu) uplasowały się na drugim miejscu wśród zagrożeń cyberbezpieczeństwa. Takie ataki stanowiły jednak jedynie 3408 przypadki.

Wyzwania ochrony danych osobowych w cyberprzestrzeni

Związek problematyki cyberbezpieczeństwa z ochroną danych osobowych jest ścisły i stanowi jedno z największych wyzwań w zakresie polityki ochrony danych osobowych, polityki, która wynika wprost z zasad polskiej konstytucji oraz traktatów unijnych i umów międzynarodowych oraz ustaw jak to już było wcześniej omawiane. Można wręcz stwierdzić, że ochrona danych osobowych w sieci stanowi jedno z najpoważniejszych wyzwań dla cyberbezpieczeństwa. Jest tak dlatego, że rozwój Internetu sprawił, że faktyczne zadania ochrony danych osobowych, sprowadzają się przede wszystkim do ochrony danych osobowych przetwarzanych w sieciach teleinformatycznych. Funkcjonowanie tak

[34] *Uwaga na Bitcoin Revolution i Profit Revolution*, portal cryps.pl, https://cryps.pl/ostrzezenie/uwaga-na-scam-bitcoin-revolution, [dostęp: 13.04.2023].

[35] *Wzrost zagrożeń cyberbezpieczeństwa*, portal gdpr.pl, https://gdpr.pl/wzrost-zagrozen-cyberbezpieczenstwa, [dostęp: 13.04.2023].

[36] *Kampanie phishingowe na serwisy pocztowe*, portal cert.pl, https://cert.pl/posts/2023/04/phishing-webmail, [dostęp: 13.04.2023].

sklepów internetowych, bankowości internetowej, mediów społecznościowych jak i różnego rodzaju serwisów usługowych oparte jest o prowadzenie w systemach teleinformatycznych wielkich baz danych dotyczących użytkowników sieci. Środki nadzoru, poczynając od Google, zdominowały obszar gromadzenia i przetwarzania informacji, zwłaszcza informacji o ludzkich zachowaniach. Wiedzą o nas wiele, natomiast nasz dostęp do ich wiedzy jest niewielki[37]. Ochrona danych osobowych we współczesnym świecie jest prawie tożsama z ochroną danych w sieci. Wynika to z faktu, że cyberprzestrzeń stała się miejscem, w którym dane osobowe są przetwarzane w stopniu niespotykanym do tej pory w dziejach oraz nieporównywalnym ze skalą przetwarzania danych osobowych przetwarzanych offline (np. zawartych w papierowych rejestrach czy ewidencjach)[38]. Zauważmy, że współcześnie wszystkie istotne rejestry jak KRS, rejestr skazanych czy księgi wieczyste funkcjonują online. Te gigantyczne ilości danych osobowych wymagają zabezpieczenia i zabezpieczenie ich jest znacznie trudniejsze niż zabezpieczenie papierowego rejestru, gdzie dane są przechowywane w postaci tradycyjnego zapisu[39]. Wyobraźmy sobie skutki ingerencji hakerów, którzy np. modyfikują zapisy ksiąg wieczystych. Przedsiębiorcy działający w sieci gromadzą w postaci baz danych wielkie zbiory danych osobowych użytkowników serwisów internetowych. W związku z tym powstaje zagrożenie wyciekiem tych danych lub pozyskaniem ich przez podmioty nieuprawnione do tego. Wielokrotnie notowano wielkie wycieki danych osobowych użytkowników sklepów internetowych, wielkich serwisów aukcyjnych, serwisów randkowych, a nawet wojskowych w służbie czynnej. Jest chyba oczywiste, w jak dużym stopniu stanowi to zagrożenie dla osób, których dane dotyczą jak i w przypadku danych osobowych funkcjonariuszy publicznych dla interesu państwa i bezpieczeństwa narodowego. Można tu dla ilustracji powagi i skali problemu podać przykład podwójnego wycieku danych osobowych Politechniki Warszawskiej w 2020 roku, gdzie wyciek danych obejmował takie dane jak imiona i nazwiska studentów i pracowników, dane

[37] S. Zuboff, *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, Zysk i S-ka, Poznań 2019, s. 268.

[38] K. Bakalarczyk-Burakowska, J. Nowicka, *Ochrona danych osobowych w cyberprzestrzeni,* [w:] *Współczesne zagrożenia bezpieczeństwa państwa,* red. Z. Ciekanowski, Wydawnictwo Państwowej Szkoły Wyższej im. Jana Pawła II w Białej Podlaskiej, Biała Podlaska, 2020.

[39] T. Stawecki, *Rejestry publiczne: funkcje instytucji*, Wydawnictwo LexisNexis, Warszawa 2005, s. 13.

ich dowodów osobistych oraz numery PESEL[40]. Takie dane w rękach przestępców mogą służyć do tzw. kradzieży tożsamości i wyłudzeń pożyczek lub kredytów bankowych o czym często nieświadoma niczego ofiara dowiaduje się dopiero z chwilą rozpoczęcia egzekucji komorniczej z tytułu niespłaconej pożyczki lub raty, której nie wzięła.

Jeszcze poważniejszym wyciekiem danych osobowych, był wyciek danych osobowych pracowników wymiaru sprawiedliwości, sędziów, prokuratorów i asesorów z zasobów danych Krajowej Rady Sądownictwa i Prokuratury w Krakowie. W tym przypadku dane te obejmowały również dane adresowe i numery telefonów. Liczni sędziowie i prokuratorzy spotkali się z groźbami od osób, które pozyskały ich dane[41]. Pierwszym poważnym wyzwaniem w obszarze ochrony obrotu danymi osobowymi w cyberprzestrzeni jest zatem zabezpieczenie wielkich zbiorów danych (klientów, konsumentów, interesariuszy, pracowników) przed wyciekami. Drugie fundamentalne wyzwanie to kwestia ochrony przed wyłudzeniem danych osobowych poprzez phishing i scam. Te dwa ostatnie rodzaje malware służące do wyłudzania danych osobowych stanowią w ostatnich latach szczególnie szybko narastający problem. W przypadku phishingu oszukany otrzymuje link do fałszywej strony (np. swojego banku) i podaje tam swoje dane osobowe, np. dane dostępowe do konta tracąc środki pieniężne na rachunku. Scam natomiast to oszustwo poprzez podstawione osoby i strony sugerujące inwestowanie pieniędzy a w rzeczywistości służące oszustwu, wyłudzaniu pieniędzy w rozumieniu art. 286 kk. Często są one sygnowane używanym bezprawnie wizerunkiem znanej osoby, np. K. Wojewódzkiego, Sz. Hołowni, R. Lewandowskiego, itp.[42] W tym przypadku i w przypadku oszustw na tzw. amerykańskiego żołnierza wyzwaniem nie jest technologia, lecz ludzka psychika i świadomość z jej ograniczeniami. Żadne blokowanie stron nie pomoże, jeżeli użytkownik sieci będzie otwierać podejrzane linki

[40] *Wywiad z dr. Michałem Kosińskim: Zgłaszali się do mnie autokraci, żeby im pomóc w wyborach. Z Polski też – program Świat, którym żyjemy*, portal wyborcza.pl, https://wyborcza.pl/10,82983,22715049,zglaszali-sie-do-mnie-autokraci-zeby-im-pomoc-w-wyborach-z.html, [dostęp: 13.04.2023].

[41] *Wyciek danych z KSSiP. ABW opisała Rzecznikowi swe działania w sprawie,* portal bip.brpo.gov.pl, http://bip.brpo.gov.pl/pl/content/wyciek-danych-z-kssip-abw-opisala-rpo-swe-dzialania, [dostęp: 13.04.2023].

[42] *Cyberbezpieczeństwo a ochrona danych osobowych*, portal ine.org.pl, https://ine.org.pl/cyberbezpieczenstwo-a-ochrona-danych-osobowych, [dostęp: 13.04.2023].

a następnie podawać cyberprzestępcy dane osobowe i dostępowe. Łatwowierność, naiwność jest tu bezwzględnie wykorzystywana i tylko edukacja internautów w zakresie niebezpieczeństw może poprawić sytuację, należy opracować strategie szkoleniowe, prowadzić monitoring sieci i systemów, zapewnić szeroką kampanię informacyjną na temat zagrożeń bezpieczeństwa użytkowników w sieci[43].

Ściganie tego rodzaju wyłudzeń jest bardzo trudne i często lub zazwyczaj nieskuteczne, gdyż oszuści operują z innych krajów, z którymi niemożliwa jest faktyczna współpraca policyjna. Stąd prewencja i edukacja użytkowników sieci to podstawowe narzędzie zwalczania tego zagrożenia. O znaczeniu problemu mówi fakt, że w 2019 roku phishing stanowił ok. 54% wszystkich zarejestrowanych przez CERT Polska ataków[44].

Kolejne wyzwanie związane z ochroną danych osobowych w cyberprzestrzeni to problem profilowania konsumentów i analizowania metadanych. Jest to dokonywane masowo tak przez witryny, dostawców usług, przedsiębiorców oferujących swoje usługi w Internecie jak i organy administracji publicznej (w państwach autorytarnych choć nie tylko vide kazus Pegazusa w Polsce i na Węgrzech). Profilowanie konsumentów na podstawie analizy ich aktywności sieciowej jest zabronione, np. w przepisach RODO. W teorii profilowanie wymaga jasnej i wyraźnej zgody osoby, której dotyczy. W praktyce jest to czysta fikcja. Wszyscy użytkownicy sieci są nieustannie śledzeni i profilowani, co służy tworzeniu odpowiednio targetowanych reklam. Aktywność w świecie realnym jest nieustannie renderowana z naszych telefonów, samochodów, ulic, domów, sklepów, ciał, drzew, budynków, lotnisk, z całych miast wprost do sfery cyfrowej, gdzie wszystko to zaczyna żyć nowym życiem, jako dane gotowe do przerobienia na przewidywanie przyszłości[45]. Dzieje się to w mediach społecznościowych, ale nie tylko. Przepisy RODO pozostają tu martwe, gdyż przedsiębiorcy często wolą płacić wysokie kary niż rezygnować z pewnych praktyk. Z drugiej strony wielkie amerykańskie korporacje internetowe

[43] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki, organizacji, państwa*, dz. cyt., s. 256.

[44] CERT Polska, *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny 2019 z działalności CERT Polska*, portal cert.pl, https://cert.pl/uploads/docs/Raport_CP_2019.pdf, [dostęp: 13.04.2023].

[45] S. Zuboff, *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, Zysk i S-ka, Poznań 2019, s. 280.

nie zwracają większej uwagi na te regulacje i pomimo kar opłacalna jest dla nich taka działalność. Analiza metadanych jest ważną metodą pozyskiwania szeregu danych osobowych w tym wrażliwych np. danych o lokalizacji użytkownika i jego miejscu zamieszkania, naszym stanie zdrowia, poglądach politycznych, wyznaniu i preferencjach seksualnych. Śledząc aktywność sieciową użytkownika algorytmy AI (Artificial Intelligence) wykorzystywane przez media społecznościowe z łatwością uzyskują te dane. A są one teoretycznie objęte najwyższym poziomem ochrony (co do zasady objęte zakazem przetwarzania). Y. Harari stwierdził wręcz, że algorytmy na podstawie analizy metadanych (a nie pozyskiwania danych osobowych bezpośrednio) szybko poznają nas lepiej niż nasi najbliżsi w zakresie naszych często bardzo intymnych cech i preferencji. Uzyskane przez algorytmy AI i służące do tworzenia zindywidualizowanych reklam oraz niekiedy zmasowanej zindywidualizowanej propagandy politycznej dane, są przetwarzane przez algorytm AI w sposób w zasadzie niekontrolowany i rozwiązania prawne i instytucjonalne są tu w zasadzie bezradne. Już w ostatnich miesiącach kolejnym wyzwaniem dla ochrony danych osobowych okazało się działanie ChatGPT 4.0 – modelu językowego stanowiącego kolejny model językowy o niezwykłych możliwościach. W związku z łamaniem prawa UE przez działania ChatGPT 4.0 Włochy zakazały funkcjonowania tego programu pod koniec marca 2023. Działanie chatbota zostało zablokowane przez włoski organ ochrony danych osobowych. Obecnie polski organ ochrony danych osobowych pozostaje w kontakcie z włoskimi i unijnymi odpowiednikami. Wniosek jest jasny, wraz z rozwojem zaawansowanych rozwiązań technicznych liczba i poziom wyzwań dla ochrony danych osobowych w cyberprzestrzeni będą rosnąć[46].

Podsumowanie

Problemem badawczym postawionym w niniejszym rozdziale była kwestia jak istotna jest świadomość zagrożeń użytkowników sieci wobec obecnych wyzwań w obszarze ochrony danych osobowych w cyberprzestrzeni? Przyjęta hipoteza zakłada, że w przypadku ochrony danych osobowych w cyberprzestrzeni, gdzie przenosi się całe funkcjonowanie społeczeństwa i obrót

[46] *Polski UODO wystąpił do Włoch w sprawie ChatGPT. Zamierza zbadać chatbota*, portal cyfrowa.rp.pl, https://cyfrowa.rp.pl/globalne-interesy/art38274811-polski-uodo-wystapil-do-wloch-w-sprawie-chatgpt-zamierza-zbadac-chatbota, [dostęp: 13.04.2023].

gospodarczy kluczowe znaczenie ma świadomość zagrożeń u użytkowników Internetu. Żadne rozwiązania technologiczne nie zastąpią tej świadomości. Podstawowym wnioskiem z przeprowadzonych tu rozważań jest konstatacja, że ochrona danych osobowych w cyberprzestrzeni jest jednym z najważniejszych zadań w zakresie zapewnienia cyberbezpieczeństwa i stabilności cyberprzestrzeni. Ochrona danych osobowych nieuwzględniająca ich przetwarzania w Internecie i systemach teleinformatycznych byłaby czystą fikcją, gdyż cyberprzestrzeń stała się miejscem, w którym dane są przetwarzane na niespotykaną skalę. Zapewnienie przez organy państwa odpowiedniego poziomu zabezpieczenia przetwarzania danych osobowych w sieci wynika wprost z zasad konstytucyjnych określających prawo do prywatności jako prawo podstawowe człowieka. O ile pozyskiwanie w sieci danych osobowych bezpośrednio podlega w UE dobrej i wyczerpującej regulacji prawnej i instytucjonalnej, o tyle pozyskiwanie tych danych w cyberprzestrzeni przez analizę metadanych oraz przetwarzanie danych osobowych przez systemy AI takie jak chatbot GPT 4.0 stanowi nowe i bardzo poważne wyzwanie, wobec którego nie można być obojętnym. Na podstawie zanalizowanego materiału wtórnego, przyjmuje się, że hipoteza została potwierdzona.

Literatura

1. Aleksandrowicz T., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego, 2016, t. 8.
2. Applebaum A., *Zmierzch demokracji: zwodniczy powab autorytaryzmu*, Wydawnictwo Agora, Warszawa 2020.
3. Bakalarczyk-Burakowska K., Nowicka J., *Cyberbezpieczeństwo a ochrona danych osobowych* [w:] *Społeczeństwo jako uczestnik bezpieczeństwa*, J. Nowicka red., Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2022.
4. Ciekanowski Z., *Współczesne zagrożenia bezpieczeństwa państwa. Cz. 1,* Wydawnictwo Państwowej Szkoły Wyższej im Papieża Jana Pawła w Białej Podlaskiej, Biała Podlaska 2020.
5. Chrząszcz A., Nowicka J., red., *Współczesny wymiar bezpieczeństwa państwa*, Wydawnictwo Wyższej Szkoły Menedżerskiej, Warszawa 2021.
6. Galloway S., *Wielka czwórka. Ukryte DNA: Amazon, Apple, Facebook i Google*, tłum. J. Kubiak, Dom Wydawniczy REBIS, Poznań 2018.

7. Gogołek W., Cetera W., *Leksykon tematyczny: zarządzanie, IT*, Wydział Dziennikarstwa i Nauk Politycznych. Uniwersytet Warszawski, Warszawa 2014.
8. Kurek J., *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big data*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2021.
9. Lichocki E, *Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy*, Wydawnictwo Akademii Marynarki Wojennej, Gdynia 2011.
10. Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, Przegląd Teleinformatyczny, 2018/1(2).
11. Nowicka J., red., *Społeczeństwo jako uczestnik bezpieczeństwa*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2022.
12. Radochoński M., Przywara B., *Jednostka, grupa, cybersieć: psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*, Wydawnictwo Wyższej Szkoły Informatyki i Zarządzania, Rzeszów 2004.
13. Sienkiewicz P, *Ontologia cyberprzestrzeni*, Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki, 2015, t. 9, nr 13.
14. Siwicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013.
15. Stawecki T.*, Rejestry publiczne: funkcje instytucji*, Wydawnictwo LexisNexis, Warszawa 2005, s. 13.
16. Szczepaniuk E., *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2016.
17. Szpyra R., *Cyberbezpieczeństwo militarne w amerykańskiej praktyce*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2016.
18. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki, organizacji, państwa*, CeDeWu, Warszawa 2020.
19. Zmarzlik J., *Internetowe znajomości – lek na samotność w realnym świecie*, Dziecko Krzywdzone. Teoria, badania, praktyka 2005, t. 4, nr 4.
20. Zuboff S., *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, Zysk i S-ka, Poznań 2019.

Akty prawne

1. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Ministerstwo Cyfryzacji, Warszawa 2017.

2. *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2002 r. Nr 156, poz. 1301).
3. *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2018 r. poz. 1560).

Netografia

1. CERT Polska, *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny 2019*, portal cert.pl, https://cert.pl/uploads/docs/Raport_CP_2019.pdf, [dostęp: 13.04.2023].
2. *Cyberbezpieczeństwo a ochrona danych osobowych*, portal ine.org.pl, https://ine.org.pl/cyberbezpieczenstwo-a-ochrona-danych-osobowych, [dostęp: 13.04.2023].
3. *Kampanie phishingowe na serwisy pocztowe*, portal cert.pl, https://cert.pl/posts/2023/04/phishing-webmail, [dostęp: 13.04.2023].
4. Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, portal core.ac.uk, https://core.ac.uk/download/pdf/235207549.pdf, [dostęp: 11.04.2023].
5. *Polski UODO wystąpił do Włoch w sprawie ChatGPT. Zamierza zbadać chatbota*, portal cyfrowa.rp.pl, https://cyfrowa.rp.pl/globalne-interesy/art38274811-polski-uodo-wystapil-do-wloch-w-sprawie-chatgpt-zamierza-zbadac-chatbota, [dostęp: 13.04.2023].
6. Sienkiewicz P., *Wizje i modele wojny informacyjnej*, portal winntbg.bg.agh.edu.pl, https://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf, [dostęp: 11.04.2023].
7. *Uwaga na Bitcoin Revolution i Profit Revolution,* portal cryps.pl, https://cryps.pl/ostrzezenie/uwaga-na-scam-bitcoin-revolution, [dostęp: 13.04.2023].
8. Wyciek danych z KSSiP. ABW opisała Rzecznikowi swe działania w sprawie, portal bip.brpo.gov.pl, https://bip.brpo.gov.pl/pl/content/wyciek-danych-z-kssip-abw-opisala-rpo-swe-dzialania, [dostęp: 13.04.2023].
9. *Wywiad z dr. Michałem Kosińskim: Zgłaszali się do mnie autokraci, żeby im pomóc w wyborach. Z Polski też – program Świat, którym żyjemy*, portal wyborcza.pl, https://wyborcza.pl/10,82983,22715049,zglaszali-sie-do-mnie-autokraci-zeby-im-pomoc-w-wyborach-z.html, [dostęp: 13.04.2023].
10. *Wzrost zagrożeń cyberbezpieczeństwa*, portal gdpr.pl, https://gdpr.pl/wzrost-zagrozen-cyberbezpieczenstwa, [dostęp: 13.04.2023].

11. *Zawiadomienie pokrzywdzonych wyciekiem danych osobowych z platformy OKNO Politechniki Warszawskiej przeznaczonej dla studentów i pracowników uczelni – Prokuratura Okręgowa w Warszawie,* portal gov.pl, https://www.gov.pl/web/po-warszawa/zawiadomienie-pokrzywdzonych-wyciekiem-danych-osobowych-z-platformy-okno-politechniki-warszawskiej-przeznaczonej-dla-studentow-i-pracownikow-uczelni, [dostęp: 13.04.2023].