JOURNAL OF MODERN SCIENCE
3/63/2025
www.jomswsge.com
DOI: 10.13166/jms/210127

KONRAD STAŃCZYK
Military University of Technology
in Warsaw, Poland
ORCID iD: 0000-0003-2788-5358

JOANNA GRUBICKA
Pomeranian University in Słupsk, Poland
ORCID iD: 0000-0001-7934-6044

CYBERBEZPIECZEŃSTWO A PRYWATNOŚĆ – DYLEMAT BEZPIECZEŃSTWA W ERZE CYFROWEJ

CYBERSECURITY AND PRIVACY – THE SECURITY DILEMMA IN THE DIGITAL AGE

Abstract

Objectives: The article analyzes key threats arising from privacy violations in the name of cybersecurity and presents data protection strategies that can help achieve a balance between these two aspects. It highlights challenges related to mass surveillance, user profiling, and legal regulations concerning information protection. The aim of the article is to examine the dilemma between cybersecurity and privacy and to identify strategies that enable their effective balance.

Material and methods: The article employs an analytical approach, including a literature review, an analysis of legal regulations, and case studies related to the conflict between cybersecurity and privacy. Available research, reports, and publications on personal data protection and digital environment regulations were analyzed. The study includes a statistical analysis of cybercrime trends, case studies of security breaches, and legal regulations aimed at finding a balance between security and privacy.

Results: The results indicate a growing scale of threats such as phishing, ransomware, and data breaches, affecting both individual users and organizations. The analysis shows that cybersecurity measures often require extensive data collection, raising concerns about potential privacy violations.

Conclusions: Cybersecurity and privacy can coexist through innovative technologies, appropriate regulations, and user education. Limiting mass surveillance requires minimizing data collection and advancing anonymization techniques. International cooperation is essential for effective data protection and combating cybercrime.

Keywords: *cybersecurity, privacy, cyber threats, data breaches, phishing, ransomware, legal regulations, personal data protection, surveillance*

Streszczenie

Cel pracy: Współczesna era cyfrowa stawia przed społeczeństwem złożony dylemat bezpieczeństwa – równowagę między cyberbezpieczeństwem a ochroną prywatności. Cyberbezpieczeństwo koncentruje się na ochronie danych i systemów przed zagrożeniami cyfrowymi, co często wiąże się z koniecznością monitorowania aktywności użytkowników i przetwarzania dużych ilości informacji, w tym danych osobowych. Z kolei prywatność jest fundamentalnym prawem jednostki, zapewniającym kontrolę nad jej danymi oraz sposobem ich wykorzystywania. Konflikt ten nabiera szczególnego znaczenia w kontekście masowej inwigilacji, profilowania użytkowników oraz regulacji prawnych dotyczących ochrony danych osobowych. Artykuł analizuje kluczowe zagrożenia wynikające z naruszeń prywatności w imię cyberbezpieczeństwa, a także przedstawia strategie ochrony danych, które mogą pomóc w osiągnięciu równowagi między tymi dwoma aspektami. Wskazuje również na wyzwania związane z masową inwigilacją, profilowaniem użytkowników oraz regulacjami prawnymi

dotyczącymi ochrony informacji. Celem opracowania jest analiza dylematu między cyberbezpieczeństwem a prywatnością oraz identyfikacja strategii umożliwiających ich skuteczne równoważenie.

Materiał i metody: W artykule zastosowano podejście analityczne, obejmujące przegląd literatury, analizę regulacji prawnych oraz studia przypadków dotyczące konfliktu między cyberbezpieczeństwem a prywatnością. Przeanalizowano dostępne badania, raporty oraz publikacje dotyczące ochrony danych osobowych i regulacji w środowisku cyfrowym. Badanie obejmuje analizę statystyczną trendów cyberprzestępczości, studia przypadków naruszeń bezpieczeństwa oraz regulacji prawnych mających na celu znalezienie równowagi między bezpieczeństwem a prywatnością.

Wyniki: Wyniki wskazują na rosnącą skalę zagrożeń, takich jak phishing, ransomware i wycieki danych, które dotykają zarówno użytkowników indywidualnych, jak i organizacje. Analiza pokazuje, że środki cyberbezpieczeństwa często wymagają intensywnego gromadzenia danych, co budzi obawy dotyczące naruszeń prywatności

Wnioski: Cyberbezpieczeństwo i prywatność mogą współistnieć dzięki innowacyjnym technologiom, odpowiednim regulacjom i edukacji użytkowników. Ograniczenie masowej inwigilacji wymaga minimalizacji zbieranych danych i rozwoju anonimizacji. Kluczowa jest także międzynarodowa współpraca dla skutecznej ochrony danych i zwalczania cyberprzestępczości.

Słowa kluczowe: *cyberbezpieczeństwo, prywatność, cyberzagrożenia, wycieki danych, phishing, ransomware, regulacje prawne, ochrona danych osobowych, inwigilacja, edukacja cyfrowa*

Wprowadzenie

Cyberbezpieczeństwo koncentruje się na ochronie danych i systemów przed nieuprawnionym dostępem, atakami oraz innymi formami zagrożeń, co wymaga gromadzenia i analizy dużej ilości informacji, w tym danych osobowych (Jaworski, 2024; Kosiński, 2015). Z kolei prywatność obejmuje prawo jednostki do nadzoru nad tym, jakie dane są gromadzone, w jaki sposób są wykorzystywane oraz komu mogą być udostępniane (Górka, 2018). Szybki rozwój technologii cyfrowych, rosnąca liczba cyberataków oraz coraz bardziej zaawansowane metody stosowane przez cyberprzestępców sprawiają, że znalezienie równowagi między tymi aspektami staje się wyzwaniem (Gerring, 2001). Odpowiednie podejście do tego problemu wymaga nie tylko szczegółowej analizy mechanizmów bezpieczeństwa i ochrony prywatności, lecz także opracowania

skutecznych strategii i narzędzi (Brathwaite, 2019), które pozwolą na minimalizowanie ryzyka przy jednoczesnym poszanowaniu praw użytkowników.

Tabela 1. *Stan i perspektywy badań nad cyberprzestępczością jako zagrożeniem bezpieczeństwa personalnego*

Obszar badań	Stan badań	Perspektywy rozwoju	Ośrodki/Fundacje
wpływ cyberprzestępczości na bezpieczeństwo personalne	– Interpol: 75% cyberataków dotyczy danych osobowych (2022) (ENISA, 2022) – NASK: wzrost incydentów cyberprzestępczych o 35% (2023) (NASK, 2023) – ENISA: zagrożenia takie jak phishing, ransomware, ataki na dane biometryczne (ENISA, 2023)	– rozwój systemów ochronnych, takich jak AI i ML – międzynarodowa współpraca w harmonizacji przepisów – wzmocnienie edukacji cyfrowej	– Interpol – NASK (Polska) – ENISA (Unia Europejska)
zagrożenia psychologiczne i społeczne	– wzrost badań nad wpływem cyberprzestępczości na zdrowie psychiczne – analiza stresu i depresji jako skutków cyberprzemocy	– rozwój interdyscyplinarnych badań łączących psychologię, technologię i prawo – opracowanie programów wsparcia dla ofiar cyberprzestępczości	– Centrum Badań nad Cyberprzestępczością Uniwersytet w Cambridge. – Centrum Badań nad Cyberprzestępczością UMK Toruń – Fundacja Bezpieczne Dzieci Online (Polska) (Fundacja Dajemy Dzieciom Siłę, 2025)
rozwój technologii ochronnych	– wdrażanie zaawansowanych systemów monitorowania zagrożeń (AI, ML) – badania nad skutecznością wieloskładnikowego uwierzytelniania i szyfrowania danych	– automatyzacja systemów bezpieczeństwa w czasie rzeczywistym – wykorzystanie AI do przewidywania i zapobiegania zagrożeniom	– OpenAI (USA) – IBM Research Labs
edukacja i świadomość cyfrowa	– badania wskazujące na niski poziom świadomości użytkowników jako kluczowy czynnik ryzyka (ENISA, 2023) – kampanie edukacyjne na temat cyberhigieny	– wprowadzenie edukacji cyfrowej na wszystkich poziomach edukacji – organizacja globalnych kampanii podnoszących świadomość zagrożeń	ESET Foundation; – CyberPeace Institute (Szwajcaria) Akademia NASK (Cyberprofilaktyka NASK 2025)
międzynarodowa współpraca	– wzrost liczby wspólnych działań Interpolu, Europolu i ENISA w ściganiu cyberprzestępców – brak pełnej harmonizacji przepisów w skali globalnej;	– harmonizacja przepisów dotyczących ochrony danych – rozwój międzynarodowych zespołów reagowania na incydenty (CERT)	– Europol – CERT Polska
ochrona grup szczególnie narażonych	– badania nad ochroną dzieci, osób starszych i pracowników służby zdrowia – wzrost liczby ataków na osoby niedoświadczone technologicznie	– opracowanie programów wsparcia i ochrony dla grup wrażliwych – rozwój technologii ochronnych dedykowanych dla tych grup	– UNICEF (projekty cyfrowe) (UNICEF 2000) – Fundacja Panoptykon (Polska) (Panoptykon, 2024)

Źródło: opracowanie własne na podstawie: Raport ENISA, Threat Landscape Report 2023: Emerging Trends in Cybersecurity, report 2023, https://www.enisa.europa.eu/ (dostęp: 1.01.2025); https://cyberprofilaktyka.pl/; (dostęp: 3.12.2025); Fundacja Dajemy Dzieciom Siłę, https://fdds.pl/, https://fdds.pl/co-robimy/dbamy-o-bezpieczenstwo-dzieci-w-internecie.html (dostęp 1.01.2025); https://panoptykon.org/ (dostęp: 3.01.2025).

Tabela 1. ukazuje obecny stan wiedzy i badań w tej dziedzinie oraz wskazuje kluczowe obszary zainteresowania badaczy, przykłady zagrożeń oraz potencjalne kierunki rozwoju w obszarze ochrony bezpieczeństwa personalnego. Uwzględnia również instytucje i organizacje zaangażowane w badania nad cyberprzestępczością, które odgrywają istotną rolę w rozwoju praktycznych i teoretycznych aspektów tego zagadnienia. Takie zestawienie pozwala lepiej zrozumieć obecne wyzwania oraz kierunki działań niezbędnych do zwiększenia ochrony współczesnego człowieka w środowisku cyfrowym.

Konflikt interesów między cyberbezpieczeństwem a prywatnością

Cyberprzestępczość ma głęboki wpływ na życie współczesnego człowieka, którego codzienność coraz bardziej opiera się na technologiach cyfrowych (Deibert, 2013). Od sfery osobistej po społeczną i zawodową, skutki działań przestępczych w cyberprzestrzeni są odczuwalne na wielu płaszczyznach. Jak zauważa Kevin Mitnick: *Największym zagrożeniem dla bezpieczeństwa jest człowiek. Możemy stworzyć najlepsze technologie, ale to od użytkowników zależy ich skuteczność* (Mitnick, 2002). To ludzki czynnik często decyduje o skuteczności zabezpieczeń i podatności na ataki. Taki układ umożliwia kompleksową analizę wpływu działań przestępczych w cyberprzestrzeni na życie współczesnego człowieka. Uwzględnienie różnych kategorii pozwala lepiej zrozumieć, w jaki sposób cyberzagrożenia oddziałują na jednostki, społeczeństwa oraz całe gospodarki. Przedstawione w Tabeli 2 przykłady ilustrują realne konsekwencje, podkreślając konieczność podejmowania działań zapobiegawczych oraz edukacyjnych w celu minimalizacji ryzyka i skutków cyberprzestępczości. Raporty NASK o stanie bezpieczeństwa w cyberprzestrzeni RP z lat 2020–2023 ukazują dynamiczny wzrost liczby incydentów oraz ewolucję zagrożeń w Polsce. W 2020 r. zgłoszono ok. 20 tys. incydentów (CSIRT GOV, 2023), podczas gdy w 2023 r. liczba ta przekroczyła 33 tys., (CSIRT GOV Polska, 2023), co oznacza wzrost o 65% w ciągu czterech lat. Phishing, który dominował w 2020 r. (35% zgłoszeń), w 2023 r. stanowił 43% wszystkich ataków, a ransomware, wcześniej marginalny, wzrósł do 19% (CSIRT GOV Polska, 2023).

Najbardziej narażone sektory to bankowość, służba zdrowia, sektor prywatny oraz instytucje państwowe. W 2020 r. głównym celem cyberprzestępców była bankowość, gdzie atakowano dane finansowe i systemy płatności. W 2023 r. szczególną uwagę przyciągnęły placówki medyczne, które doświadczyły licznych ataków ransomware, prowadzących do paraliżu działalności i wycieków danych pacjentów. Sektor prywatny z kolei zmagał się z kradzieżą danych klientów i pracowników, a instytucje państwowe były celem ataków na dane strategiczne i kampanii dezinformacyjnych. Użytkownicy indywidualni stanowili coraz większą grupę ofiar cyberprzestępczości – od 50% incydentów w 2020 r., do 67% w 2023 r. (Związek Pracodawców Branży Internetowej IAB Polska, Money, 2023). Wśród najczęstszych zagrożeń znalazły się wyłudzenia danych osobowych, oszustwa finansowe oraz przejęcia kont w mediach społecznościowych. Raporty wskazują również na niską świadomość społeczeństwa w zakresie cyberhigieny, która mimo wzrostu liczby kampanii edukacyjnych pozostaje kluczowym wyzwaniem. Utrata danych osobowych stanowi jedno z najpoważniejszych zagrożeń współczesnego świata cyfrowego, gdyż dotyka zarówno jednostek, jak i całych organizacji (Związek Pracodawców Branży Internetowej IAB Polska, Money, 2023). Skala i charakter tych incydentów różnią się w zależności od obszaru, obejmując użytkowników indywidualnych, instytucje służby zdrowia oraz firmy. Tabela 2 przedstawia przykłady naruszeń w tych kategoriach, wskazując ich skutki oraz konkretne przypadki, które obrazują realne zagrożenia związane z cyberprzestępczością. Taki podział umożliwia lepsze zrozumienie problemu i podkreśla konieczność dostosowywania strategii ochrony w zależności od specyfiki każdego sektora.

Tabela 2. *Skala i skutki utraty danych osobowych*

Obszar	Przykłady naruszeń	Skutki	Przykłady
użytkownicy	włamania na konta e-mail lub społecznościowe	kradzież tożsamości, nieautoryzowane transakcje finansowe	wycieki danych z Facebooka (2019) – 533 mln użytkowników (BBC.com, 2018)
	phishing i wyłudzenia danych osobowych	utrata oszczędności, oszustwa kredytowe	kampanie phishingowe z fałszywymi stronami bankowymi
	nieautoryzowane udostępnienie prywatnych danych	naruszenie prywatności, stres emocjonalny	afera Cambridge Analytica (2016) (BBC.com, 2018)
służba zdrowia	wyciek danych pacjentów z systemów szpitalnych	utrata wrażliwych informacji medycznych, naruszenie poufności	atak ransomware WannaCry (2017) – dotknął systemy NHS w Wielkiej Brytanii (Theverge.com, 2017)
	brak zabezpieczeń w elektronicznych kartotekach	możliwość użycia danych do oszustw	wyciek danych pacjentów z klinik estetycznych w USA (2021)
	ataki ransomware na placówki medyczne	zakłócenia działalności, paraliż systemów	ataki ransomware w niemieckich szpitalach (2020) (Zdanet.com, 2021)
firmy	włamania do baz danych klientów	utrata poufnych informacji handlowych, straty finansowe	wyciek danych LinkedIn (2021) 700 mln rekordów (Edition.cnn 2021)
	wycieki informacji handlowych i pracowniczych	naruszenie reputacji, koszty prawne i naprawcze	wyciek danych Equifax (2017) – 147 mln klientów (Equifax, 2021)
	ataki na infrastrukturę IT firm	przerwy w działalności, utrata danych operacyjnych	atak na Colonial Pipeline (2021) – paraliż dostaw energii w USA (Nytimes.com 2021)

Źródło: opracowanie własne na podstawie: D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe, Prawo w działaniu*. Sprawy karne, 53/2023, s. 98–100.

Każdy z przypadków wymienionych w Tabeli 2 ukazuje mechanizmy działania przestępców, skalę problemu oraz konsekwencje dla użytkowników i organizacji, podkreślając tym samym znaczenie skutecznych strategii ochrony danych w cyfrowym świecie. Analiza tych przykładów pozwala lepiej zrozumieć wyzwania stojące przed współczesnym społeczeństwem i organizacjami w kontekście bezpieczeństwa informacji. Afera Cambridge Analytica to jeden z najgłośniejszych skandali związanych z ochroną danych osobowych w historii, który ujawniono w 2016 r. Firma Cambridge Analytica, specjalizująca się w analizie danych, bezprawnie pozyskała dane ok. 87 mln użytkowników Facebooka, wykorzystując je do profilowania psychograficznego i precyzyjnego targetowania reklam politycznych. Działania te odegrały kluczową rolę w kampanii wyborczej Donalda Trumpa w USA

oraz w referendum dotyczącym brexitu w Wielkiej Brytanii. Dane te zostały pozyskane za pośrednictwem aplikacji *This Is Your Digital Life*, stworzonej przez Aleksandra Kogana, badacza z Uniwersytetu w Cambridge. Aplikacja deklarowała zbieranie danych na potrzeby badań akademickich i umożliwiała użytkownikom wypełnianie quizów psychologicznych. Jednak oprócz danych użytkowników, gromadziła również informacje o ich znajomych na Facebooku, co znacząco zwiększyło skalę naruszenia prywatności. W efekcie, choć aplikację pobrało jedynie ok. 300 tys. osób, dane aż 87 mln użytkowników znalazły się w rękach Cambridge Analytica (BBC.com, 2018). Skandal wywołał ogromne kontrowersje na całym świecie i stał się symbolem naruszenia prywatności w epoce cyfrowej. Firma Cambridge Analytica została oskarżona o wykorzystanie danych bez zgody użytkowników, a Facebook – o brak odpowiednich zabezpieczeń oraz niewystarczającą transparentność w zakresie przetwarzania danych. W wyniku skandalu Mark Zuckerberg, założyciel Facebooka, został przesłuchany przed Kongresem Stanów Zjednoczonych, a platforma społecznościowa nałożyła na siebie dodatkowe środki bezpieczeństwa danych. Incydent ten przyczynił się do zaostrzenia przepisów dotyczących ochrony danych osobowych, takich jak RODO w Unii Europejskiej, oraz do wzrostu świadomości na temat prywatności i cyberbezpieczeństwa w sieci. Afera Cambridge Analytica pozostaje punktem odniesienia w debacie o odpowiedzialności platform cyfrowych za ochronę danych użytkowników, jednak już w 2019 r. Facebook ponownie znalazł się w centrum uwagi, gdy doszło do jednego z największych naruszeń danych osobowych w historii platformy. W wyniku błędów w zabezpieczeniach dostępne publicznie stały się dane osobowe ok. 533 mln użytkowników z 106 krajów, w tym numerów telefonów, dat urodzenia, adresów e-mail oraz lokalizacji. Wyciek dotyczył również ok. 2,7 mln użytkowników z Polski (Money, 2021). Dane te zostały udostępnione na forum hakerskim, gdzie mogły być wykorzystywane do oszustw, phishingu, a także innych działań przestępczych, takich jak kradzież tożsamości. Przyczyną wycieku były nieprawidłowe konfiguracje systemów bazy danych oraz niewystarczająca ochrona mechanizmów dostępu do informacji. Incydent ten podkreślił znaczenie odpowiednich zabezpieczeń oraz problem braku przejrzystości w przetwarzaniu danych osobowych przez duże platformy społecznościowe. Był również impulsem do zwiększenia nacisku

na przestrzeganie regulacji, takich jak RODO, oraz na edukację użytkowników w zakresie ochrony prywatności online.

Ataki ransomware na niemieckie szpitale stanowią jeden z najbardziej niepokojących przykładów cyberprzestępczości, która bezpośrednio zagraża zdrowiu i życiu ludzi. W 2020 r. doszło do serii ataków ransomware, które sparaliżowały działanie kilku niemieckich placówek medycznych, w tym szpitala uniwersyteckiego w Düsseldorfie (zdnet.com, 2020). Ataki te wymusiły wyłączenie systemów IT, co uniemożliwiło placówkom dostęp do krytycznych danych pacjentów oraz korzystanie z systemów diagnostycznych i zarządzania. Jednym z najtragiczniejszych skutków był przypadek pacjentki, która z powodu braku możliwości udzielenia pomocy w szpitalu w Düsseldorfie została przewieziona do innej placówki, co spowodowało krytyczne opóźnienie w leczeniu. Był to pierwszy udokumentowany przypadek, w którym atak ransomware miał bezpośredni wpływ na śmierć pacjenta. Po atakach w Niemczech wiele placówek na całym świecie zaczęło bardziej inwestować w cyberbezpieczeństwo, uświadamiając sobie, jak kluczowe jest zabezpieczenie systemów IT dla funkcjonowania opieki zdrowotnej. Ataki ransomware na szpitale wywołały debatę na temat konieczności lepszego zabezpieczenia infrastruktury krytycznej, w tym placówek medycznych. W odpowiedzi na te wydarzenia, Niemcy oraz inne kraje podjęły kroki mające na celu zwiększenie ochrony infrastruktury medycznej, w tym wdrażanie zaawansowanych systemów szyfrowania i tworzenie dedykowanych zespołów ds. cyberbezpieczeństwa. Ataki ransomware na niemieckie szpitale ukazują, jak cyberprzestępczość wykracza poza sferę finansową, bezpośrednio zagrażając zdrowiu i życiu ludzi. To ostrzeżenie dla wszystkich krajów, jak krytyczne znaczenie ma cyberbezpieczeństwo w sektorze opieki zdrowotnej. Atak na Colonial Pipeline, który miał miejsce w maju 2021 r., jest jednym z najbardziej znaczących incydentów cyberprzestępczości w historii infrastruktury krytycznej Stanów Zjednoczonych. Colonial Pipeline to jedna z największych sieci rurociągów paliwowych w USA, zaopatrująca w paliwo wschodnie wybrzeże kraju. Atak ransomware przeprowadzony przez grupę hakerską DarkSide (nytimes.com, 2024) doprowadził do wstrzymania działalności systemu transportu paliwa na kilka dni, powodując chaos w dostawach i wzrost cen paliw. Hakerzy wykorzystali oprogramowanie ransomware, które zainfekowało

systemy Colonial Pipeline. Zablokowano dostęp do kluczowych danych, a w zamian za ich odblokowanie żądano okupu w wysokości 4,4 mln dolarów, który został zapłacony przez firmę w kryptowalutach. Cyberatak zmusił firmę do tymczasowego wstrzymania działalności, co spowodowało przerwy w dostawach paliwa i zakłócenia w funkcjonowaniu stacji benzynowych w wielu stanach (nytimes.com, 2024). Atak na Colonial Pipeline stał się punktem zwrotnym w dyskusji o bezpieczeństwie infrastruktury krytycznej. Wydarzenie to uwidoczniło znaczenie cyberbezpieczeństwa dla ciągłości funkcjonowania podstawowych usług i wywołało debatę na temat roli państwa oraz firm prywatnych w ochronie przed tego typu zagrożeniami. Incydent ten pokazał, że cyberprzestępczość może mieć realne, fizyczne konsekwencje, oddziałując na całe społeczeństwo i gospodarkę. Atak na Colonial Pipeline jest ostrzeżeniem, że infrastruktura krytyczna na całym świecie wymaga stałych inwestycji w zabezpieczenia cyfrowe oraz szybkiej reakcji na nowe zagrożenia. Wybrane przykłady, przedstawione w Tabeli 2, zostały dobrane z uwagi na ich różnorodność oraz zdolność do ukazania wielowymiarowych aspektów cyberzagrożeń i ich konsekwencji w świecie współczesnym. Każdy z opisanych przypadków ilustruje odmienny obszar zagrożeń: naruszenie prywatności danych (afera Cambridge Analytica), błędy w zabezpieczeniach platform cyfrowych (wyciek danych z Facebooka w 2019 r.), wpływ cyberprzestępczości na życie ludzkie (ataki ransomware na niemieckie szpitale) oraz zagrożenia dla infrastruktury krytycznej (atak na Colonial Pipeline). Przykłady te pokazują, jak różnorodne są cele i metody cyberprzestępców, a także jak poważne mogą być konsekwencje ich działań. Podkreślają również skalę problemu – od naruszeń prywatności jednostek po globalne skutki, takie jak zakłócenia dostaw paliw czy zagrożenia dla zdrowia i życia ludzi. Analiza tych przypadków pomaga zrozumieć, jak istotne są mechanizmy obronne, takie jak regulacje prawne (np. RODO), inwestycje w zabezpieczenia oraz edukacja w zakresie ochrony danych osobowych. Dzięki temu zestawieniu możliwe jest wskazanie obszarów wymagających szczególnej uwagi i działań zapobiegawczych, zarówno na poziomie jednostek, jak i całych organizacji. Wybrane przykłady nie tylko dokumentują skutki cyberprzestępczości, ale również inspirują do poszukiwania skutecznych strategii przeciwdziałania

jej zagrożeniom. To właśnie dzięki takim analizom można lepiej przygotować się na wyzwania w dynamicznie zmieniającym się środowisku cyfrowym.

Wymienione incydenty ukazują różnorodność i skalę zagrożeń w cyberprzestrzeni, wynikających m.in. z luk w zabezpieczeniach, niewystarczających procedur bezpieczeństwa oraz braku świadomości użytkowników. Analiza tych wydarzeń podkreśla znaczenie inwestycji w zaawansowane technologie ochronne, regularnych aktualizacji systemów oraz rozwijania mechanizmów szybkiego reagowania na incydenty (Banasiński, 2023).

Analiza dynamiki cyberprzestępczości w Polsce

KSIP, jako centralny system informacyjny policji, odgrywa kluczową rolę w gromadzeniu, analizie i udostępnianiu danych dotyczących przestępczości, w tym cyberprzestępstw. Jego zasoby pozwalają na identyfikację trendów oraz wyznaczanie obszarów wymagających szczególnej uwagi zarówno w działaniach operacyjnych, jak i prewencyjnych. W kontekście niniejszej analizy wybór Słupska nie był przypadkowy i wynikał z kilku istotnych czynników. Uzasadnienie doboru Słupska jako studium przypadku oparto na przesłankach metodologicznych i empirycznych. Słupsk ma status miasta na prawach powiatu, co zapewnia ekspozycję na pełne spektrum spraw miejskich i policyjnych typowych dla ośrodków średniej wielkości oraz zwiększa trafność zewnętrzną wniosków (BDL/TERYT; por. Gerring, 2001). W ujęciu statystycznym Słupsk mieści się w klasie *miast średnich* (20–100 tys. mieszkańców) przyjmowanej w badaniach GUS i literaturze przedmiotu; najnowsze dane miejskie wskazują 76 522 mieszkańców (stan na 24.04.2025), co potwierdza jego reprezentatywność dla tej kategorii (GUS; UM Słupsk). Stopień upowszechnienia usług cyfrowych w Polsce – 9,5 mln klientów stacjonarnego dostępu do internetu w 2023 r. – pokazuje, że wzorce korzystania z usług i ekspozycji na ryzyka w ośrodkach średniej wielkości są porównywalne z trendami krajowymi (UKE, 2023). Profil zagrożeń obserwowany w skali kraju, z dominacją phishingu (ok. 65% incydentów obsłużonych przez CERT Polska w 2022 r.), jest spójny z obrazem europejskim, w którym wśród kluczowych

kategorii utrzymują się ransomware oraz wektory oparte na socjotechnice (ENISA ETL, 2023; por. także CERT Polska, 2023). Położenie Słupska w województwie pomorskim i jego funkcje administracyjno-gospodarcze generują heterogeniczną ekspozycję na ryzyko w przekroju użytkowników indywidualnych, MŚP i sektora publicznego. Z perspektywy doboru przypadków Słupsk odpowiada kryterium *przypadku typowego* (ang. *typical case*), co sprzyja ostrożnej analitycznej generalizacji wniosków do populacji polskich miast średnich, przy jednoczesnym zakotwiczeniu analiz w udokumentowanych trendach krajowych i europejskich (Gerring, 2001; Śleszyńska, 2017; GUS; UKE, 2024; CERT Polska, 2023; ENISA, 2023). Tak ujęte studium przypadku pozwala nie tylko porównywać lokalne trendy z danymi ogólnopolskimi, ale też oceniać skuteczność wdrażanych strategii i ich potencjalną implementację w ośrodkach o podobnej strukturze społeczno-gospodarczej, a w konsekwencji – identyfikować obszary wymagające dalszych działań prewencyjnych i legislacyjnych. Dane z lat 2013–2018, pochodzące z KSIP Analit. (dane analityczne KSIP), KSIP WWW oraz Biuletynu Statystycznego, wskazują na dynamiczny wzrost liczby cyberprzestępstw w Polsce. W szczególności liczba oszustw internetowych (art. 286 § 1 kk) wzrosła z 16 556 przypadków w 2013 r. do 35 525 w 2018 r., co podkreśla rosnące znaczenie problematyki bezpieczeństwa cyfrowego i konieczność wdrażania skutecznych mechanizmów ochrony. W Słupsku, mimo mniejszej skali, zauważalny jest podobny trend wzrostowy, szczególnie w zakresie oszustw internetowych oraz nieautoryzowanego dostępu do informacji (art. 267 § 1 kk). Z kolei dane z okresu 2019–2023 (KSIP Analit. – dane analityczne z KSIP, KSIP WWW, Biulet. Stat. – dane z Biuletynu Statystycznego) potwierdzają dalszy wzrost liczby przestępstw. W Polsce w 2022 r. oszustwa internetowe osiągnęły rekordową liczbę 65 037 przypadków, podczas gdy w Słupsku zanotowano 1239 takich incydentów, co stanowiło znaczący wzrost w stosunku do poprzednich lat. Przestępstwa związane z nękaniem (art. 190a kk) utrzymywały wysoki poziom, a ich liczba w Słupsku wzrosła o 30% w ciągu dekady. Łącznie w latach 2013–2023 w Polsce odnotowano ponad 200 tys. przypadków cyberprzestępstw, z czego Słupsk odpowiadał za ok. 0,6% wszystkich zgłoszonych incydentów. Szczególnie wyraźny był wzrost przestępstw związanych z fałszowaniem pieniędzy (art. 310 kk) oraz propagowaniem faszyzmu

lub nawoływaniem do nienawiści (art. 256 kk), choć w ostatnich latach w tej ostatniej kategorii odnotowano spadek liczby przestępstw. Porównanie obu okresów wskazuje na znaczny wzrost liczby cyberprzestępstw, co odzwierciedla coraz większą zależność społeczeństwa od technologii cyfrowych oraz rosnącą aktywność cyberprzestępców. Przestępstwa takie jak wyłudzanie danych osobowych i kradzież tożsamości (art. 267 § 2 kk) stanowiły ok. 15% wszystkich zgłoszonych incydentów w Słupsku, co wskazuje na konieczność wdrożenia bardziej zaawansowanych mechanizmów ochrony.

Analiza danych zarówno na poziomie lokalnym, jak i krajowym wskazuje na konieczność intensyfikacji działań w zakresie edukacji społecznej, rozwoju narzędzi wspierających działania policji oraz zwiększenia inwestycji w cyberbezpieczeństwo. Szczególną uwagę należy poświęcić zapobieganiu oszustwom internetowym oraz ochronie danych osobowych, które stanowią jedne z kluczowych obszarów zagrożeń we współczesnej cyberprzestrzeni. Uwzględnienie Słupska w analizie nie tylko dostarcza istotnych wniosków dla lokalnych instytucji odpowiedzialnych za bezpieczeństwo, ale także umożliwia sformułowanie bardziej uniwersalnych rekomendacji dotyczących skutecznych metod przeciwdziałania cyberprzestępczości na poziomie regionalnym i krajowym. Ponadtozauważalny wzrost liczby przestępstw oraz zróżnicowana dynamika ich występowania w poszczególnych kategoriach podkreślają znaczenie skutecznej implementacji działań operacyjnych oraz ciągłego rozwoju technologii wspierających bezpieczeństwo. Tylko kompleksowe podejście, łączące działania prewencyjne, zaawansowane narzędzia analityczne oraz współpracę instytucji publicznych i sektora prywatnego, może skutecznie ograniczyć skalę zagrożeń i zwiększyć odporność na cyberprzestępczość.

Balans między prywatnością a cyberbezpieczeństwem

Cyberbezpieczeństwo obejmuje szereg kluczowych działań, które mają na celu ochronę systemów informatycznych, danych oraz użytkowników przed zagrożeniami cyfrowymi. Jednym z priorytetowych aspektów jest ochrona systemów przed atakami hakerskimi, złośliwym oprogramowaniem i nieautoryzowanym dostępem. W tym celu stosowane są technologie takie jak firewalle, oprogramowanie antywirusowe oraz systemy wykrywania i zapobiegania włamaniom. Istotnym elementem jest także monitorowanie i wykrywanie zagrożeń, co obejmuje analizę ruchu sieciowego oraz zastosowanie zaawansowanych narzędzi, takich jak systemy SIEM, które umożliwiają bieżącą analizę i szybkie reagowanie na incydenty bezpieczeństwa. Z kolei ochrona prywatności koncentruje się na zapewnieniu przejrzystości w przetwarzaniu danych, minimalizacji zbieranych informacji oraz wdrażaniu odpowiednich mechanizmów kontroli dostępu. Regulacje prawne, takie jak RODO, nakładają na organizacje obowiązek informowania użytkowników o celach przetwarzania ich danych oraz zapewnienia możliwości ich usunięcia lub sprostowania. Ochrona prywatności obejmuje również technologie zabezpieczające, takie jak szyfrowanie danych, anonimizacja oraz polityki zarządzania zgodami, które umożliwiają użytkownikom kontrolę nad swoimi danymi osobowymi. W praktyce napięcie między cyberbezpieczeństwem a prywatnością jest widoczne w wielu obszarach. Na przykład wprowadzenie systemów monitoringu aktywności internetowej czy analizy ruchu sieciowego może znacznie zwiększyć poziom bezpieczeństwa, ale jednocześnie rodzi pytania o granice ingerencji w prywatność obywateli. Systemy nadzoru, takie jak PRISM stosowany przez amerykańską NSA, pokazują, jak zaawansowane narzędzia cyberbezpieczeństwa mogą prowadzić do masowej inwigilacji. Podobnie rozwój technologii biometrycznych, takich jak rozpoznawanie twarzy, budzi obawy o możliwość nadmiernej kontroli społeczeństwa. W celu znalezienia kompromisu między ochroną prywatności a cyberbezpieczeństwem, konieczne jest stosowanie strategii uwzględniających oba te aspekty. Przykładem może być wdrażanie uwierzytelniania dwuskładnikowego (2FA) zamiast metod biometrycznych, co pozwala na zwiększenie poziomu ochrony

bez nadmiernej ingerencji w dane osobowe. Ponadto stosowanie zasady minimalizacji danych oraz wdrażanie technik anonimizacji może zmniejszyć ryzyko naruszenia prywatności, jednocześnie pozwalając na skuteczne wykrywanie zagrożeń. Znaczenie znalezienia równowagi między tymi dwoma obszarami podkreślają również regulacje prawne oraz polityki organizacyjne. Przepisy RODO wprowadzają wymagania dotyczące przechowywania danych przez określony czas, co pozwala na realizację celów bezpieczeństwa bez nadmiernego gromadzenia informacji o użytkownikach. Jednocześnie instytucje odpowiedzialne za cyberbezpieczeństwo muszą dostosowywać swoje procedury do dynamicznie zmieniających się zagrożeń, co wymaga elastycznego podejścia do ochrony prywatności i stosowania innowacyjnych metod analizy danych. Rozwój technologii sztucznej inteligencji (SI) w ostatnich latach istotnie wpłynął zarówno na ewolucję cyberzagrożeń, jak i na doskonalenie narzędzi cyberbezpieczeństwa (Schneier, 2023). Z jednej strony algorytmy uczenia maszynowego umożliwiają cyberprzestępcom automatyzację ataków, personalizację kampanii phishingowych oraz generowanie treści dezinformacyjnych w skali masowej (Akhtar, Mian, 2021; Brundage i in., 2022). Z drugiej – te same technologie wspierają systemy detekcji anomalii, analizę predykcyjną incydentów oraz adaptacyjne mechanizmy reagowania, zwiększając skuteczność ochrony infrastruktury krytycznej i danych wrażliwych użytkowników (ENISA, 2021). Dynamiczny rozwój SI stawia jednak nowe wyzwania w obszarze ochrony prywatności, w tym konieczność zapewnienia transparentności działania algorytmów i minimalizacji ryzyka nadużyć w przetwarzaniu danych osobowych (Goodfellow, Bengio, Courville, 2016). Uwzględnienie tej problematyki w strategiach bezpieczeństwa cyfrowego jest zatem kluczowe dla kompleksowej ochrony internautów w warunkach transformacji technologicznej.

W kontekście cyberzagrożeń istotnym problemem jest możliwość wykorzystania pozyskanych informacji w działaniach ofensywnych (Janczewski, 2019). Dane gromadzone przez urządzenia mobilne, sieci bezprzewodowe oraz systemy monitoringu mogą zostać użyte przez podmioty prowadzące działania hybrydowe, obejmujące manipulację informacyjną, szantaż czy ataki cybernetyczne. Coraz bardziej zaawansowane metody analizy danych umożliwiają budowanie szczegółowych profili jednostek, co może stanowić poważne zagrożenie dla ich prywatności i bezpieczeństwa. W związku z tym konieczne

jest wdrażanie skutecznych mechanizmów ochrony danych oraz zwiększanie świadomości użytkowników w zakresie zagrożeń wynikających z postępującej cyfryzacji. Pliki cookies są jednym z fundamentalnych elementów funkcjonowania internetu. Te niewielkie pliki przechowują duże ilości informacji o użytkownikach, umożliwiając dostosowanie witryn i stron internetowych do indywidualnych potrzeb. Dzięki nim strony internetowe mogą gromadzić dane dotyczące ustawień, historii przeglądania, języka oraz lokalizacji użytkownika, co pozwala na optymalizację działania stron. Przykładowo pliki cookies przesyłają informacje o preferencjach językowych, co pozwala serwerowi na wyświetlenie strony w odpowiednim języku, dostosowanym do ustawień użytkownika. Oprócz standardowych plików cookies istnieją bardziej zaawansowane technologie śledzenia, takie jak tagipixel, beacony ultradźwięków, odciski palców przeglądarki, a także nieusuwalne pliki cookie zombie, super cookies, dynamiczne cookies, Silverlight Isolated Storage i Indexed DB (Microsoft Edge, 2024). Te zaawansowane metody śledzenia są coraz bardziej kreatywne i skomplikowane, co ukazuje, jak cennym towarem stały się dane w cyfrowej epoce. Informacje te mogą być wykorzystywane do przejęcia kontroli nad rynkami, wpływania na opinię publiczną, a nawet do wygrywania wyborów.

W odpowiedzi na rosnące zagrożenia związane z masowym zbieraniem danych Unia Europejska wprowadziła regulacje w postaci RODO (GDPR) oraz dyrektywy e-prywatności (Dyrektywa 2002/58/WE). Celem tych inicjatyw jest uregulowanie praktyk śledzenia użytkowników i ochrona ich danych osobowych. Choć te regulacje mogą nie być w pełni wystarczające, stanowią istotny krok w kierunku ochrony prywatności użytkowników internetu. W odpowiedzi na te regulacje powstały narzędzia takie jak Cookiebot, które umożliwiają zgodne z RODO i dyrektywą e-prywatności korzystanie z plików cookies oraz innych technologii śledzących. Cookiebot zapewnia przejrzystość poprzez informowanie użytkowników o stosowanych technologiach i zbieranie ich zgody na śledzenie. System ten oferuje trzy główne funkcje: skan witryny, system zgody na pliki cookies oraz pełną kontrolę i przejrzystość. Skan witryny identyfikuje wszystkie typy technologii śledzących, w tym dynamiczne cookies, beacony ultradźwięków, tagipixel i odciski palców. System zgody dezaktywuje skrypty na stronie do momentu uzyskania zgody użytkownika, zgodnie z zasadą *uprzedniej zgody* wymaganą przez nowe przepisy. Comiesięczny skan generuje

raport, który daje właścicielowi witryny pełen wgląd w technologie śledzenia używane na stronie oraz możliwość zarządzania nimi zgodnie z wymogami RODO. Dzięki takim rozwiązaniom użytkownicy mają zapewnioną większą kontrolę nad swoimi danymi, a właściciele witryn mogą dostosować swoje działania do obowiązujących przepisów, co jest kluczowe w dzisiejszym, coraz bardziej uregulowanym środowisku cyfrowym (Grubicka, Matuska, 2023).

W swojej istocie tożsamość cyfrowa stanowi fundamentalny element zapewniający bezpieczeństwo w cyfrowym świecie, umożliwiający uwierzytelnianie użytkowników i autoryzację dostępu do zasobów oraz usług online, jednocześnie chroniąc integralność i autentyczność przekazywanych danych. Uchwalenie przez Sejm ustawy z 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej było następstwem wejścia w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania publicznego w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (eIDAS) (Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r.). Rozporządzenie eIDAS wprowadza nowy porządek prawny w obszarze usług zaufania, co spowodowało konieczność dostosowania prawa krajowego do nowych uwarunkowań. Jak wskazano w uzasadnieniu do ustawy, dotychczas w polskim prawie regulowana była w pełni jedynie instytucja podpisu elektronicznego, w tym szczególnie bezpiecznego podpisu elektronicznego oraz znakowania czasem. Rozporządzenie eIDAS rozszerza zakres dostępnych usług oraz nakłada na państwa członkowskie obowiązek ustanowienia nadzoru. Kwestie związane z nadzorem nad usługami zaufania oraz notyfikacją systemów elektronicznej identyfikacji stanowią główną treść nowej krajowej regulacji (Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r.). Ponadto rozporządzenie wprowadza nowy element, który nie jest zaliczany do usług zaufania – identyfikację elektroniczną w celu realizacji usług online. Celem jest zapewnienie posiadaczowi środka identyfikacji elektronicznej wydanego w jednym kraju członkowskim możliwości korzystania z publicznych usług online w innych krajach członkowskich. Artykuł 1 ustawy z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej określa krajową infrastrukturę zaufania, działalność dostawców usług zaufania,

w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych, tryb notyfikacji krajowego systemu identyfikacji elektronicznej oraz nadzór nad dostawcami usług zaufania. Zadaniem uchwalonej ustawy było przede wszystkim wyeliminowanie pojęć i instytucji nieznanych w rozporządzeniu eIDAS oraz dostosowanie terminologii krajowych aktów prawnych do terminów używanych w tym rozporządzeniu. Dodatkowo ustawa regulowała te obszary, które były niezbędne do umożliwienia stosowania rozporządzenia eIDAS w polskim porządku prawnym, takie jak wyznaczenie organu nadzoru oraz uchylenie ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (tekst jedn. Dz. U. z 2013 r., poz. 262 ze zm.), a także usunięcie istniejących odesłań do jej przepisów W kontekście powyższych regulacji i dostosowania prawa krajowego do wymogów rozporządzenia eIDAS, została wprowadzona także ustawa o aplikacji mObywatel (tekst jedn. Dz. U. z 2023 r., poz. 1234). Ustawa ta stanowi kontynuację wysiłków mających na celu cyfryzację usług publicznych oraz ułatwienie dostępu do dokumentów tożsamości w formie elektronicznej. Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel reguluje funkcjonowanie aplikacji mObywatel, która umożliwia obywatelom Polski dostęp do różnorodnych usług publicznych oraz dokumentów w formie elektronicznej (tekst jedn. Dz. U. z 2023 r., poz. 1234). Ustawa obejmuje takie elementy, jak dokument mObywatel, profil mObywatel, certyfikaty użytkownika oraz podpis elektroniczny weryfikowany przy użyciu certyfikatu użytkownika. Określa ona zasady działania aplikacji, regulując kwestie związane z bezpieczeństwem danych, ich przetwarzaniem oraz odpowiedzialnością za zgodność tych danych z rzeczywistymi dokumentami. Dzięki integracji z systemami publicznymi i bankowymi aplikacja mObywatel pozwala na bezpieczną identyfikację elektroniczną oraz na korzystanie z usług online zarówno w Polsce, jak i w innych krajach członkowskich Unii Europejskiej, zgodnie z zasadami określonymi przez rozporządzenie eIDAS (tekst jedn. Dz. U. z 2023 r., poz. 1234).

Z nowoczesnego typu e-dowodu tożsamości można korzystać od 4 marca 2019 r. E-dowód jest projektem realizowanym przez ówczesne Ministerstwo Spraw Wewnętrznych i Administracji oraz Ministerstwo Cyfryzacji (Archiwumbip.mswia.gov.pl, 2018). Proces wymiany dowodów rozłożono na 10 lat i potrwa on do 2029 r. E-dowód osobisty ma różnorodne funkcje, takie jak udostępnienie informacji o posiadaczu, potwierdzenie tożsamości oraz

potwierdzanie obecności. Dzięki temu, bez aktywacji dodatkowych funkcji, e-dowód może służyć do potwierdzania tożsamości poprzez przyłożenie go do czytnika, co umożliwia wyświetlenie informacji potwierdzającej autentyczność dokumentu. Od 7 listopada 2021 r. funkcje e-dowodów zostały rozszerzone. Nowe e-dowody tożsamości wydawane po tej dacie zawierają dodatkowo obraz odcisku palca w warstwie elektronicznej oraz obraz podpisu własnoręcznego posiadacza e-dowodu w warstwie graficznej. Obraz odcisku palca dostępny jest dla służb granicznych, co umożliwia automatyczne przeprowadzanie kontroli paszportowej. E-dowody oferują także usługę profilu osobistego, powszechnie dostępnego środka identyfikacji elektronicznej, który umożliwia potwierdzanie tożsamości zarówno w usługach prywatnych, jak i publicznych. Profil osobisty zapewnia wyższy stopień wiarygodności niż profil zaufany, który również potwierdza tożsamość, ale jest ograniczony do kontaktów z administracją publiczną. Dzięki certyfikatowi identyfikacji i uwierzytelniania umieszczonemu w e-dowodzie administracja publiczna oraz usługi prywatne mogą jednoznacznie uwierzytelnić użytkownika online. Korzystanie z e-dowodu umożliwia instytucjom takim jak banki czy przychodnie potwierdzenie autentyczności dokumentu bez konieczności fizycznej obecności właściciela. E-dowód znacząco ułatwia kontakty z administracją publiczną za pośrednictwem internetu, umożliwiając logowanie do platform takich jak Gov.pl, portal pacjenta, składanie zeznań podatkowych czy zakładanie kont firmowych online. Ponadto e-dowód osobisty umożliwia korzystanie z podpisu osobistego – zaawansowanego podpisu elektronicznego, który może mieć taki sam skutek prawny jak podpis własnoręczny. Ten podpis, chroniony sześciocyfrowym numerem PIN, może być używany do podpisywania dokumentów elektronicznych zarówno w kontaktach z urzędami, jak i w relacjach prywatnych, pod warunkiem że obie strony wyrażą na to zgodę. Warstwa elektroniczna e-dowodu, umożliwiająca korzystanie z jego funkcji, może być aktywowana przez użytkownika po ustaleniu osobistych kodów PIN za pomocą kodu PUK, otrzymanego podczas odbierania dowodu. E-dowód może być używany do logowania w serwisach takich jak Gov.pl, przy czym niezbędne jest posiadanie urządzenia z funkcją NFC oraz odpowiedniego oprogramowania, np. aplikacji eDoApp. Aplikacja eDoApp umożliwia zdalne potwierdzanie tożsamości za pomocą smartfona i e-dowodu. Jest dostępna dla systemów Android i iOS,

a korzystanie z niej jest bezpłatne. Aby potwierdzić tożsamość, wystarczy zeskanować kod QR lub wpisać numer, przyłożyć e-dowód do smartfona z NFC i podać czterocyfrowy PIN (E-dowód w dłoni, 2024). Bezpieczeństwo użycia e-dowodu jest zapewnione przez protokół, który wymaga podania numeru dostępowego (CAN). Numer ten znajduje się w warstwie graficznej dowodu osobistego w postaci sześciu cyfr na awersie oraz kodu kreskowego na rewersie dokumentu. Ma to na celu uniemożliwienie dostępu do elektronicznych danych zawartych w dowodzie bez wiedzy i zgody posiadacza. Dodatkowo, aby skorzystać z certyfikatu identyfikacji i uwierzytelnienia lub podpisu osobistego, wymagane jest podanie odpowiednio kodu PIN1 lub PIN2, które użytkownik nadaje samodzielnie (e-Dowód, 2024). W kontekście bezpieczeństwa danych kluczowe jest wdrożenie rozwiązań opierających się na zasadach *privacy by design* i *privacy by default*. *Privacy by design* zakłada włączenie ochrony prywatności w sam proces tworzenia projektu, jego komponentów oraz zarządzania technologiami informacyjnymi i systemami przez cały cykl życia informacji. Z kolei *privacy by default* to zasada, według której systemy powinny mieć ustawienia domyślne maksymalnie chroniące prywatność użytkowników (Wiewiórowski, 2012). Umieszczenie w jednym miejscu tak wielu istotnych danych o obywatelu, jak ma to miejsce w przypadku e-dowodu, niesie za sobą ryzyko kradzieży tożsamości. Jak podkreśla Arkadiusz Lach, *może to być szczególnie groźne dla pokrzywdzonego, zwłaszcza w przypadku danych niezmiennych, takich jak data i miejsce urodzenia, czy trudnych do zmiany, jak nazwisko* (Lach, 2015). Skutki kradzieży tożsamości mogą być odczuwalne przez poszkodowanego jeszcze przez wiele lat po nieautoryzowanym wykorzystaniu jego danych (Lach, 2015). Dlatego ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel, która reguluje funkcjonowanie aplikacji mObywatel, kładzie szczególny nacisk na zasady bezpieczeństwa danych, sposób ich przetwarzania oraz odpowiedzialność za ich zgodność z rzeczywistymi dokumentami.

Zakończenie

Współczesne społeczeństwo zmaga się z wyzwaniem znalezienia równowagi między cyberbezpieczeństwem a ochroną prywatności. Rosnąca liczba cyberzagrożeń, takich jak phishing, ransomware i wycieki danych, wymaga skutecznych mechanizmów ochrony, jednak ich wdrożenie często wiąże się z koniecznością gromadzenia i przetwarzania dużych ilości danych osobowych. Powstaje więc konflikt między koniecznością zapewnienia bezpieczeństwa a ochroną prywatności jednostek. Analiza wykazała, że jednym z kluczowych problemów współczesnej cyberprzestrzeni jest masowa inwigilacja, profilowanie użytkowników oraz brak pełnej transparentności w zakresie przetwarzania danych. Aby skutecznie równoważyć oba aspekty, konieczne jest zastosowanie podejścia interdyscyplinarnego, łączącego technologie ochronne, regulacje prawne oraz działania edukacyjne. Rozwiązania oparte na zasadach *privacy by design* i *privacy by default* mogą pomóc w minimalizacji ryzyka naruszeń prywatności przy jednoczesnym zapewnieniu odpowiedniego poziomu bezpieczeństwa cyfrowego. Równie istotna jest współpraca międzynarodowa oraz harmonizacja regulacji prawnych, co pozwoli na skuteczniejszą walkę z cyberprzestępczością i zabezpieczenie danych osobowych użytkowników (Antczak, 2020).

References

Akhtar, N., Mian, A. (2021). *Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey*. Cham: Springer.

Antczak, J. (2020). *Costs of Cyber-Security in a Business Entity*. Warszawa: Education of Economists and Managers.

Archiwumbip.mswia.gov.pl, https://archiwumbip.mswia.gov.pl/bip/sprawy-obywatelskie/25913,E-dowod.html (dostęp: 28.08.2024).

Banasiński, C. (red.) (2023). *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

BBC.com (2018), https://www.bbc.com/news/technology-43465968 (dostęp: 30.12.2024).

Brathwaite, S. (2019). *Cybersecurity Law Protect Yourself and Your Customers*. New York: Business Expert Press.

Brundage, M., Avin, S., Clark, J. (2022). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford: Oxford University Press.

Centrum Badań nad Cyberprzestępczością UMK Toruń, https://www.law.umk.pl/centrum-badan-nad-cyberprzestepczoscia/ (dostęp: 1.01.2025).

CERT Polska. (2023). *Krajobraz bezpieczeństwa polskiego internetu w 2022 roku*. NASK, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp: 13.08.2025).

CSIRT GOV Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjBgOyIvf2LAxWOJBAIHbkqGagQFnoECBMQAQ&url=https%3A%2F%2Fcsirt.gov.pl%2Fdownload%2F3%2F201%2FRaportostaniebezpieczenstwacyberprzestrzeniRPw2020.pdf&usg=AOvVaw1wpnjKH3KAAA1J1oDpECns&opi=89978449 (dostęp: 3.01.2025).

CSIRT GOV Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi (dostęp: 3.01.2025).

Cyberprofilaktyka NASK, https://cyberprofilaktyka.pl/ (dostęp: 3.01.2025).

Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto: International Journal of Communication

Edition.cnn, https://edition.cnn.com/2021/04/08/tech/linkedin-data-scraped-hacker-site/index.html (dostęp:30.12.2024)

E-dowód w dłoni, eDOApp w telefonie, https://www.gov.pl/web/cyfryzacja/e-dowod--w-dloni-edo-app-w-telefonie (dostęp: 28.08.2024).

e-Dowód – e-dowód – Portal Gov.pl, https://www.gov.pl/web/e-dowod (dostęp: 29.08.2024).

ENISA (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf?utm (dostęp: 13.08.2025).

Equifax, https://www.reuters.com/article/world/equifax-says-15-2-million-uk-records-exposed-in-cyber-breach-idUSKBN1CF2JR/ (dostęp: 30.12.2024).
European Union Agency for Cybersecurity (ENISA) (2021). *Artificial Intelligence and Cybersecurity: A State-of-the-Art Analysis, ENISA*, Athens.
Fundacja Dajemy Dzieciom Siłę, https://fdds.pl/, https://fdds.pl/co-robimy/dbamy-o-bezpieczenstwo-dzieci-w-internecie.html (dostęp: 3.01.2025).
Gerring, J. (2001). *Social science methodology: A criterial framework*, Cambridge: University Press.
Goodfellow, I., Bengio, Y., Courville, A. (2016). *Deep Learning*, MIT Press, Cambridge (MA).
Górka, M. (2018) *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa*. W: T. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem X*XI wieku. Łódź – Wrocław: Archae-Graph.
Grubicka, J., Matuska, E. (2023). *Bezpieczeństwo cyfrowe. Perspektywa organizacyjna*. Warszawa: Difin.
GUS (2012). *Miasta w liczbach 2012.* Warszawa: GUS, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5499/3/7/1/miasta_w_liczbach_2012_07_31_internet.pdf?utm (dostęp: 13.08.2025).
GUS BDL/TERYT. *Powiat m. Słupsk (2263000) – klasyfikacja jednostki*, https://bdl.stat.gov.pl/bdl/dane/teryt/jednostka/2842?utm (dostęp: 13.08.2025).
Janczewski, R.A. (2019). *Znaczenie cyberprzestrzeni w działaniach hybrydowych*. W: L. Elak i in. (red.). *Zagrożenia hybrydowe*. Warszawa: Bellona.
Jaworski, D.R. (red.) (2024). *Cyberprzestępczość i nowe technologie. Współczesne wyzwania nauk prawnych.* Warszawa: Difin.
Kosiński, J. (2015). *Paradygmaty cyberprzestępczości*. Warszawa: Difin.
Lach, A. (2015). *Karnoprawna reakcja na zjawisko kradzieży tożsamości*. Warszawa: Wolters Kluwer.
Mitnick, K. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: Wiley.
Money.pl, https://www.money.pl/gospodarka/wyciek-danych-z-facebooka-uodo-ostrzega-6626549045603008a.html (dostęp: 30.12.2024).
Nytimes.com https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html/ (dostęp: 30.12.2024).
Panoptykon, https://panoptykon.org/search?search=&sort_by=sort_by&sort_order=DESC&f%5B0%5D=content_type%3A84&f%5B1%5D=content_type%3A87 (dostęp: 30.12.2024).
Śleszyński, P. (2017). *Wyznaczenie i typologia miast średnich tracących funkcje społeczno-gospodarcze*, https://rcin.org.pl/Content/64381/PDF/WA51_83754_r2017-t89-z4_Przeg-Geogr-Sleszyns.pdf (dostęp: 13.08.2025).
UKE (2024). *Raport o stanie rynku telekomunikacyjnego w 2023 r.* Warszawa: Urząd Komunikacji Elektronicznej, https://bip.uke.gov.pl/ (dostęp: 13.08.2025).

Urząd Miejski w Słupsku (2025). *Dane statystyczne – stan na 24.04.2025 r.*, https://www.slupsk.pl/ratusz/dane-statystyczne?utm (dostęp: 14.08.2025).
PolskaRaport ENISA, Threat Landscape Report 2023: Emerging Trends in Cybersecurity, report 2023, https://www.enisa.europa.eu/ (dostęp: 8.03.2025).
Raport Interpol, https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report (dostęp: 8.03.2025).
Schneier, B. (2023). *Artificial Intelligence and Security: The Impact of AI on Cybersecurity*. Oxford: Oxford University Press.
Skoczylas, D. (2023). *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe, Prawo w działaniu*. Sprawy karne, 53, Prawo w Działaniu. Warszawa: Instytut Wymiar Sprawiedliwości.
Theverge.com, https://www.theverge.com/2017/5/14/15637888/authorities-wanna-cry-ransomware-attack-spread-150-countries (dostęp: 30.12.2024).
UNICEF (2020). *Children in the Digital World: Opportunities and Risks*. Nowy Jork.
Wiewiórowski, W.R. (2012). *Privacy by Design jako paradygmat ochrony prywatności*. W: G. Szpor (red.). *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*. Warszawa: Wydawnictwo C.H. Beck.
Zdanet.com, https://www.zdnet.com/article/ransomware-attacks-against-hospitals--are-having-some-very-grim consequences/ (dostęp: 30.12.2024).
Związek Pracodawców Branży Internetowej IAB Polska. Money (2023). *Bezpieczeństwo w sieci: nowe technologie i AI*. IAB Polska, https://money2.wpcdn.pl/raporty/bezpieczenstwo-w-sieci-nowe-technologie-i-ai.pdf (dostęp: 26.12.2024).

Akty prawne i orzecznictwo

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej); Dziennik Urzędowy L 201 , 31/07/2002 P. 0037 – 0047.
Rozporządzenie 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (tekst jedn. Dz. U. z 2023 r., poz. 1234).