ACTA IURIDICA RESOVIENSIA Nr 1(48)/2025
ISSN 2720-0574 DOI: 10.15584/actaires.2025.1.2

**Dawid Chaba**

Uniwersytet Komisji Edukacji Narodowej w Krakowie
ORCID: 0000-0002-2385-3466

**Piotr Lebelt**

Uniwersytet Komisji Edukacji Narodowej w Krakowie
ORCID: 0009-0001-1020-6702

# PRYWATNOŚĆ W SIECI – WYZNACZENIE OBSZARU BEZPIECZEŃSTWA W SOCIAL MEDIA I *E-COMMERCE*

## Wprowadzenie

W dobie wszechobecnej cyfryzacji kwestia prywatności w sieci nabiera szczególnego znaczenia. Polacy chętnie korzystają z mediów społecznościowych, dzieląc się swoim życiem osobistym, poglądami i zainteresowaniami. Jednocześnie handel elektroniczny, jako drugi z filarów internetowego życia, dynamicznie się rozwija, przy czym konsumenci dokonują zakupów online, udostępniając swoje dane osobowe i preferencje zakupowe. Kluczowym problemem jest napięcie między korzyściami płynącymi z aktywności online a zagrożeniami dla prywatności. Prywatność, rozumiana jako prawo do ochrony danych osobowych i swobody w zakresie decydowania o ich ujawnianiu, stała się zagrożona w erze internetu, gdzie granice między przestrzenią publiczną a prywatną są coraz trudniejsze do zachowania. Media społecznościowe, handel elektroniczny rodzą ryzyko naruszenia prywatności, kradzieży tożsamości, manipulacji czy dyskryminacji, jako że dane osobowe są gromadzone, przetwarzane i wykorzystywane przez firmy, a czasem nawet udostępniane podmiotom trzecim.

W obliczu tych wyzwań niezbędne jest wypracowywanie nowych mechanizmów ochrony prywatności, które uwzględnią specyfikę polskiego rynku cyfrowego. Polskie prawo, choć dostosowane do ogólnych wymogów europejskich (RODO), wymaga dalszych uszczegółowień i dostosowań do specyfiki lokalnych platform społecznościowych i sklepów internetowych. Konieczne jest znalezienie równowagi między ochroną prywatności a swobodą prowadzenia działalności gospodarczej w sieci.

W niniejszym artykule ujęto główne zagrożenia dla prywatności w polskich mediach społecznościowych i handlu elektronicznym. Omówiono problem ochrony danych osobowych w *e-commerce*, wpływ mediów społecznościowych na prywatność użytkowników oraz korzyści i ryzyko związane z udostępnianiem danych osobowych w sieci.

W Polsce i na świecie obserwuje się dynamiczne zmiany w prawodawstwie mające na celu wzmocnienie ochrony danych osobowych, co ma kluczowe znaczenie nie tylko dla ochrony prywatności, ale także dla zaufania konsumentów i stabilności rynków cyfrowych. Teza niniejszego artykułu koncentruje się na stwierdzeniu, że istniejące regulacje prawne dotyczące ochrony prywatności w Polsce, mimo że są krokiem w dobrym kierunku, wymagają dalszych modyfikacji lub całkowicie nowych rozwiązań regulacyjnych. Takie zmiany są niezbędne, aby skutecznie odpowiadać na nowe wyzwania i zagrożenia, które pojawiają się wraz z rozwojem nowych technologii i zmieniającymi się praktykami społecznymi i gospodarczymi.

## Poufność w mediach społecznościowych i w handlu elektronicznym

Internet, będący fundamentem współczesnego świata, oferuje dostęp do sieci ponad 5,4 mld osób, co stanowi około 67% globalnej populacji. W Europie 80% ludności ma dostęp do internetu, a w Polsce odsetek ten wynosi 78%[1]. Internet służy Polakom nie tylko do przeglądania stron czy wysyłania poczty elektronicznej, ale również do korzystania z serwisów społecznościowych. Niemniej coraz większa świadomość zagrożeń dla prywatności skłania użytkowników do podejmowania działań ochronnych, takich jak czyszczenie historii przeglądarek czy blokowanie ciasteczek. Przy czym każde korzystanie z internetu wiąże się z udostępnianiem danych. Wiele informacji dzielimy świadomie, inne – nieświadomie. Dane te, mimo pozornej chaotyczności, są używane przez różne podmioty – od reklamodawców po instytucje rządowe.

Prawo do prywatności, uznawane za jedno z praw człowieka pierwszej generacji, odgrywa zasadniczą rolę w większości współczesnych systemów prawnych, zabezpieczając prywatność życia jako odrębne dobro prawne[2]. W literaturze spotyka się dwa główne nurty dotyczące prywatności. Pierwszy z nich podkreśla potrzebę rozszerzenia ochrony prywatności, podczas gdy drugi proponuje jej ograniczenie, argumentując to koniecznością m.in. działania instytucji państwowych na

[1] *Worldwide digital population 2024*, https://www.statista.com/statistics/617136/digital-population-worldwide/ (10.05.2024); *Digital Around The World*, https://datareportal.com/global-digital-overview (10.05.2024).

[2] B. Banaszak, A. Preisner, *Prawa i wolności obywatelskie w Konstytucji RP*, Warszawa 2002, s. 41.

rzecz bezpieczeństwa narodowego i społecznego[3]. W kontekście kulturowym i społecznym definicja prywatności może się różnić, obejmując zakres interakcji, dystansu społecznego i poziomu izolacji, jakie są preferowane przez jednostki[4].

Międzynarodowe i regionalne ramy prawne, takie jak Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności czy Karta praw podstawowych Unii Europejskiej, jak również krajowe przepisy, na. polska Konstytucja z 1997 r. i rozporządzenie o ochronie danych osobowych, zapewniają ochronę życia prywatnego, czci i dobrego imienia każdej osoby.

Podjęcie tematyki prawnej ochrony prywatności w sieci w Polsce nieuchronnie prowadzi do rozpoznania wpływu ogólnego rozporządzenia o ochronie danych osobowych, znanego powszechnie jako RODO[5]. To kluczowe rozporządzenie, które weszło w życie w całej Unii Europejskiej w maju 2018 r., stanowi fundamentalną oś dla przepisów dotyczących prywatności i ochrony danych osobowych zarówno na poziomie lokalnym, jak i międzynarodowym. RODO nie tylko ujednoliciło sposób, w jaki należy chronić dane osobowe w Unii Europejskiej, ale także wyznaczyło nowe standardy globalne w zakresie prywatności[6].

W kontekście monitorowania aktywności użytkowników w internecie istotne jest omówienie plików *cookies*, które funkcjonują od połowy lat 90. Pierwszy dokument normujący ich użycie datowany jest na 1997 r. Pliki *cookies* umożliwiają komunikację między przeglądarkami a stronami internetowymi oraz zapisywanie preferencji użytkownika, takich jak dane logowania, aby nie wpisywać ich za każdym razem podczas odwiedzania strony. Z czasem rozszerzono ich zastosowanie o inne funkcje personalizacji, np. ustalanie wielkości czcionki czy układu strony. Specyfikacja ciasteczek była wielokrotnie aktualizowana, ale pojawiły się też problemy z zarządzaniem i usuwaniem tych plików. Teoretycznie każde ciasteczko posiada datę ważności, która decyduje o jego usunięciu, lecz w praktyce okres ten może być bardzo zróżnicowany – od kilku godzin do lat. Rosnące funkcjonalności *cookies* i ich niemal nieograniczone stosowanie spowodowało problemy z ochroną prywatności użytkowników, co wykorzystali reklamodawcy do śledzenia ich aktywności online. Ochrona własnej prywatności wymagała od użytkowników internetu wiedzy i czasu na dostosowanie ustawień przeglądarki, co okazało się niewystarczające. W 2009 r. Unia Europejska podjęła kroki regulacyjne, wprowadzając dyrektywę 2009/136/EC, która wymagała od administratorów stron informowania użytkowników o plikach *cookies* oraz uzyskania

[3] J. Niklas, *Prywatność w internecie*, „Infos zagadnienia społeczno-gospodarcze" 2014, nr 13(173), s. 2.

[4] B. Banaszak, A. Preisner, *Prawa i wolności*…, s. 41.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

[6] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019, poz. 1781).

ich wyraźnej zgody na ich używanie. Był to ważny krok w kierunku uporządkowania przepisów i zwiększenia kontroli użytkowników nad swoimi danymi. Jednak dyrektywa pozostawiła dużą swobodę w implementacji, co ograniczyło jej efektywność. W praktyce informacyjne banery często nie dostarczały pełnej wiedzy o zapisywanych danych, skłaniając użytkownika do szybkiego zatwierdzenia wszystkich plików *cookies*, zamiast zapewniać pełną kontrolę nad tym procesem[7]. Z uwagi m.in. na ten fakt opracowano wspomniane już RODO.

Regulacje unijne dotyczące ochrony danych osobowych mają szeroki zakres stosowania, obejmujący takie sytuacje, jak zakupy internetowe, aplikacje o pracę czy ubieganie się o kredyt bankowy. Obowiązują one zarówno podmioty unijne, jak i te spoza Unii, np. takie giganty, jak Facebook czy Amazon, które prowadzą działalność na terenie Unii Europejskiej. W ramach ogólnego rozporządzenia o ochronie danych unijne prawo precyzuje zarówno okoliczności, w których dane mogą być zbierane i przetwarzane, jak i sytuacje, które wymagają zgody na przetwarzanie danych, oraz możliwości jej cofnięcia. RODO umożliwia również sprzeciw wobec używania danych do celów marketingu bezpośredniego, a także korygowanie nieprawidłowych informacji dotyczących osoby.

W Polsce wprowadzenie RODO wymagało licznych zmian w krajowych ustawach, takich jak ustawa o ochronie danych osobowych[8], oraz innych aktów regulujących specyficzne aspekty gospodarki i administracji publicznej. Polskie prawodawstwo musiało zostać dostosowane do wymogów RODO, co spowodowało istotne zmiany zarówno w zakresie praw jednostek, jak i obowiązków podmiotów przetwarzających dane osobowe. Kluczowym elementem tych regulacji jest zwiększenie przejrzystości procesów przetwarzania danych oraz wzmocnienie praw osób, których dane dotyczą, do ich kontroli, w tym prawa do bycia zapomnianym, prawa do dostępu do danych, a także prawa do ich sprostowania i usunięcia[9]. RODO rozszerza definicję danych osobowych, w tym o adresy IP oraz pliki *cookies*, co ma kluczowe znaczenie w kontekście cyfrowym, gdzie dane biometryczne zyskują na popularności jako metody autentykacji. Niemniej współczesne podejście do prywatności wymaga nie tylko ochrony prawnej, ale również świadomego zarządzania danymi osobowymi, szczególnie w dobie cyfryzacji, gdzie internet staje się areną życia społecznego, zawodowego i edukacyjnego.

Uzupełnieniem RODO jest rozporządzenie ePrivacy, które koncentruje się na ochronie prywatności w komunikacji elektronicznej i ma zastąpić dyrektywę 2002/58/WE. Choć wciąż jest ono przygotowywane, jego głównym celem jest zwiększenie ochrony użytkowników urządzeń końcowych, takich jak komputery,

[7] K. Dziedzic, *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie. Kompletny poradnik krok po kroku,* „Komputer Świat" 2018, nr 1(95), s. 5.

[8] E. Milczarek, *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie*, Warszawa 2020, s. 41.

[9] M.T. Osypowicz, *Wpływ standardów Rady Europy i Unii Europejskiej na zapewnienie bezpieczeństwa danych osobowych w państwach członkowskich*, Kielce 2021, s. 78.

telefony czy tablety, przed nadmierną ingerencją w ich prywatność. Podejmowane są działania, by chronić takie informacje, jak historia przeglądarki, ruch na stronach czy lokalizacja w celach marketingowych[10].

Sieć internetowa, rozumiana jako globalna platforma łącząca komputery, zapewnia użytkownikom dostęp do różnorodnych usług i treści, zasadniczo nie wymagając za nie dodatkowych opłat. Niezbędnym warunkiem korzystania z tego medium jest jednak wysyłanie oraz odbieranie danych. Wynajem infrastruktury internetowej jest kosztem, który musi być pokryty bez względu na cele operacyjne strony. W odpowiedzi na te wyzwania twórcy treści przyjmują głównie dwa modele zarabiania. Pierwszy z nich zakłada, że użytkownik uiszcza opłatę jednorazową lub regularną, co zapewnia mu dostęp do treści, a twórcy – stałe źródło dochodu. Drugi model, dominujący na rynku, opiera się na darmowym dostępie do treści i generowaniu przychodów poprzez reklamy. Sektor reklamy cyfrowej jest dynamicznie rozwijającym się rynkiem z prognozowanymi wydatkami sięgającymi 870 mld USD w 2027 r., co stanowi znaczny wzrost w porównaniu do 506 mld USD w 2021 r.[11] Wystarczy prześledzić model działania jednej z funkcjonujących platform, tj. Facebooka. Platforma ta, założona w 2004 r., szybko zdobyła dominującą pozycję na rynku dzięki ogromnej liczbie aktywnych użytkowników. Chociaż główna usługa Facebooka jest bezpłatna, firma generuje wysokie zyski poprzez dokładne profilowanie użytkowników. Materiały publikowane przez użytkowników są analizowane w celu identyfikacji ich zainteresowań, co umożliwia platformie dostosowanie przekazywanych treści do indywidualnych preferencji odbiorców. Takie podejście nie tylko przyciąga użytkowników do dłuższego przebywania na stronie, ale również umożliwia reklamodawcom skuteczniejsze dotarcie do docelowych grup klientów.

Niewątpliwie media społecznościowe, będące integralną częścią życia codziennego wielu osób, stanowią równocześnie źródło licznych zagrożeń dla prywatności. Ich dynamiczny rozwój i wszechobecność stawiają użytkowników w obliczu potencjalnych naruszeń ich danych osobowych, często wynikających z nieświadomego udostępniania informacji prywatnych w przestrzeni publicznej. Media społecznościowe, choć pełnią rolę platform do wymiany myśli i doświadczeń, mogą też stać się narzędziem do nieautoryzowanego śledzenia, profilowania oraz manipulacji.

Charakterystyka zagrożeń dla prywatności w mediach społecznościowych obejmuje m.in. niekontrolowany zasięg publikacji danych, możliwość ich kopiowania i nieautoryzowanego wykorzystania przez inne osoby lub firmy[12]. Szerokie spektrum informacji, które użytkownicy niejednokrotnie nieświadomie udostępniają, jak lokalizacja, preferencje osobiste, dane kontaktowe czy zdjęcia, może być

[10] S. Kotecka-Kral, *Postulaty de lege ferenda dotyczące ochrony prywatności użytkowników usług Over-the-Top w Unii Europejskiej*, „Przegląd Prawa i Administracji" 2020, nr 120, t. 1, s. 292.

[11] *Digital advertising spending worldwide from 2021 to 2027*, https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/ (25.05.2024).

[12] *What Does Facebook Know About You Really?*, https://www.socialmediatoday.com/news/what-does-facebook-know-about-you-really/546502/ (14.05.2024).

wykorzystywane nie tylko do celów marketingowych, ale też w bardziej złośliwy sposób, w tym do kradzieży tożsamości czy cyberprzemocy[13].

Przykłady naruszeń prywatności w mediach społecznościowych są liczne i zróżnicowane. Jednym z bardziej znaczących przypadków, który miał miejsce na arenie międzynarodowej, było wykorzystanie danych z Facebooka przez firmę Cambridge Analytica, co skutkowało manipulacją wyborczą[14]. W Polsce również dochodziło do przypadków naruszeń, gdzie dane osobowe były wykorzystywane bez zgody użytkowników, co prowadziło do interwencji organów ochrony danych osobowych i nałożenia sankcji na odpowiedzialne podmioty[15]. Konsekwencje takich naruszeń są dwojakie – z jednej strony prowadzą do utraty zaufania do platform, z drugiej stanowią poważne zagrożenie dla integralności osobistej i prywatności.

W kontekście rosnącej świadomości zagrożeń dyskusja na temat potrzeby wprowadzenia specyficznych regulacji dla mediów społecznościowych nabiera na znaczeniu. Obecne przepisy, mimo że częściowo adresują kwestie związane z ochroną danych osobowych, często okazują się niewystarczające wobec szybkiego tempa ewolucji technologii cyfrowych[16]. Wiele głosów w debacie publicznej i naukowej podnosi, że istnieje pilna potrzeba wprowadzenia bardziej precyzyjnych i rygorystycznych regulacji, które będą skuteczniej chronić użytkowników mediów społecznościowych przed nieautoryzowanym dostępem do ich danych i wykorzystaniem ich[17]. Proponowane zmiany mogłyby obejmować m.in. wprowadzenie bardziej transparentnych zasad dotyczących tego, jak dane są zbierane, przetwarzane i udostępniane, zwiększenie kontroli użytkowników nad ich danymi, a także wprowadzenie surowszych sankcji dla platform, które naruszają przepisy o ochronie danych osobowych[18].

Należy zwrócić uwagę, że Meta, właściciel Facebooka, zarządza również innymi platformami komunikacyjnymi, takimi jak Instagram czy komunikator WhatsApp. Informacje zebrane z tych źródeł są również wykorzystywane do tworzenia dokładnych profili użytkowników w celu dostosowania treści zarówno na stronach internetowych, jak i w aplikacjach mobilnych. Nie tylko Meta czerpie korzyści z analizowania i wykorzystywania danych swoich użytkowników. Google, będący operatorem najczęściej używanej wyszukiwarki internetowej, stosuje podobne

[13] J. Tyburska, *Kryterium legalności zgody na przetwarzanie danych osobowych w obrocie elektronicznym*, „Człowiek w Cyberprzestrzeni" 2020, nr 3, s. 1–2.

[14] *Facebook pod ostrzałem za możliwy wyciek danych. Zajmą się nim władze USA i Unii Europejskiej*, https://businessinsider.com.pl/firmy/strategie/facebook-wyciek-danych-manipulacja-wyborami-w-usa-przez-rosje/fjwvbgs (11.05.2024).

[15] E. Milczarek, *Prywatność wirtualna*…, s. 67.

[16] I. Ładysz, *V edycja konferencji naukowej z serii „Bezpieczna Młodzież" – „Młodzież wobec współczesnych zagrożeń. Prawda i fałsz w cyberprzestrzeni" – Wrocław, 13 czerwca 2023 r.*, „Rocznik Bezpieczeństwa Międzynarodowego" 2023, nr 17(1), s. 192.

[17] A. Pawlak, *The right to privacy in the era of artificial intelligence* [w:] *Human rights – evolution in the digital era*, red. M. Sitek, J. Bonet Navarro, Józefów 2021, s. 109.

[18] J. Czopek, *Bezpieczeństwo i ochrona prywatności młodzieży w Internecie w kontekście edukacji medialnej*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Pedagogika" 2016, nr 12, s. 67–73.

metody do profilowania użytkowników, oferując im reklamy i oferty skrojone na miarę ich potrzeb i zainteresowań[19]. Facebook, będący platformą służącą zarówno do prywatnej komunikacji, jak i do poszukiwania informacji o aktualnych wydarzeniach czy nowych produktach, stanowi szczególnie interesujący przykład. Zgodnie z badaniami przeprowadzonymi przez Pew Research Center większość użytkowników tego serwisu konsumuje treści, w tym informacje prasowe, w sposób przypadkowy[20]. Zarządzanie treściami na Facebooku oparte jest na algorytmach, które decydują, które informacje są użytkownikowi prezentowane w danym momencie, co czyni go biernym odbiorcą treści. W przeciwieństwie do tego, korzystanie z wyszukiwarki wymaga aktywnej interakcji ze strony użytkownika, który musi określić, jakiego rodzaju dane chce wyszukać. Wyszukiwarka nie ma możliwości przewidywania indywidualnych zapytań. Z kolei platforma społecznościowa, mając dostęp do obszernej bazy treści publikowanych przez użytkowników, może oferować nowe informacje dostosowane do zainteresowań odbiorców bez konieczności wpisywania specyficznych zapytań. Chociaż początkowe założenie profilu w mediach społecznościowych wymaga pewnego wysiłku, treści są następnie dostarczane użytkownikom automatycznie. Dla wielu z nich Facebook staje się głównym źródłem informacji, przyciągającym swoją łatwością obsługi i ciągłym dostępem do nowych danych. W zamian użytkownicy nieustannie, często nieświadomie, udostępniają informacje na temat swoich preferencji i zachowań.

Handel elektroniczny, będący jednym z szybciej rozwijających się sektorów gospodarki, również niesie z sobą liczne wyzwania związane z ochroną danych osobowych klientów. Sklepy internetowe, platformy zakupowe oraz inne formy *e-commerce* zbierają i przetwarzają ogromne ilości danych, co stawia przed nimi szczególne wymagania dotyczące ich zabezpieczania i przestrzegania praw konsumentów do prywatności.

Analiza problemów związanych z ochroną danych osobowych w *e-commerce* ujawnia kilka kluczowych obszarów ryzyka. Po pierwsze, sklepy internetowe często gromadzą więcej informacji, niż jest to niezbędne do realizacji transakcji[21]. Po drugie, dane te mogą być przechowywane przez nadmiernie długi okres lub wykorzystywane w sposób, którego konsumenci nie zaakceptowali[22]. Po trzecie, niezabezpieczone bazy danych są narażone na ataki cybernetyczne, co może prowadzić do wycieku wrażliwych informacji osobowych i finansowych[23].

---

[19] *Meta przeanalizuje, co robisz na Facebooku i WhatsApp, aby szkolić AI. „To dla waszego dobra"*, https://android.com.pl/tech/738480-ai-whatsapp-facebook-meta-dane/ (29.05.2024).

[20] https://www.pewresearch.org/tools-and-resources/ (28.05.2024).

[21] G. Gregorczyk, *Jak (i czy) dzieci i młodzież chronią swoją prywatność? O edukacji na temat ochrony danych osobowych i cyfrowej tożsamości. Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków 2018, s. 130.

[22] *Kiedy usuwamy dane osobowe*, https://www.rp.pl/biznes/art39235301-kiedy-usuwamy-dane-osobowe (27.05.2024).

[23] E. Milczarek, *Prywatność wirtualna*…, s. 73.

Systemy zabezpieczeń stosowane przez platformy *e-commerce* obejmują zaawansowane technologie szyfrowania danych, uwierzytelnianie wieloskładnikowe, a także monitorowanie transakcji w czasie rzeczywistym w celu wykrywania i zapobiegania nieautoryzowanym operacjom. Dzięki takim środkom platformy *e-commerce* starają się minimalizować ryzyko oszustw i zapewniać bezpieczne środowisko zakupowe dla użytkowników. Niemniej istnieją również istotne ograniczenia i luki w obecnych systemach zabezpieczeń, które mogą stanowić zagrożenie dla konsumentów. Luki te mogą wynikać z błędów programistycznych, braku aktualizacji oprogramowania czy niewłaściwego zarządzania danymi przez użytkowników. Cyberprzestępcy nieustannie opracowują nowe metody obejścia zabezpieczeń[24].

Analiza orzecznictwa polskich sądów w kontekście ochrony danych osobowych pokazuje, jak prawo jest interpretowane i stosowane w praktyce. Polskie sądy w swoich wyrokach coraz częściej odwołują się do zasad i wartości wprowadzonych przez RODO, co demonstruje wpływ europejskiej doktryny prawnej na krajowe prawodawstwo[25]. Z jednej strony sądy w Polsce podkreślają znaczenie ochrony danych osobowych jako fundamentalnego prawa człowieka, z drugiej strony muszą równoważyć te prawa z innymi prawami i wolnościami, w tym z wolnością wypowiedzi i prawem do informacji[26].

Porównanie polskich i europejskich praktyk dotyczących zabezpieczenia transakcji online wskazuje na stosunkowo dobrą harmonizację przepisów wynikającą z implementacji RODO i innych regulacji unijnych, takich jak dyrektywa o prywatności i łączności elektronicznej[27]. W Polsce, podobnie jak w innych krajach Unii, przedsiębiorcy działający w obszarze *e-commerce* są zobowiązani do stosowania odpowiednich środków technicznych i organizacyjnych mających na celu ochronę zbieranych danych osobowych. Obejmuje to m.in. szyfrowanie danych, regularne audyty bezpieczeństwa oraz wdrażanie procedur reagowania na incydenty bezpieczeństwa.

## Argumenty i kontrargumenty dla zmian

Debata na temat regulacji ochrony danych osobowych jest złożona i wielowymiarowa, gdyż dotyka podstawowych wolności jednostki oraz potrzeby zapewnienia bezpieczeństwa publicznego i gospodarczego. Dyskusja ta oscyluje między

[24] G. Gregorczyk, *Jak (i czy) dzieci i młodzież*…, s. 133.

[25] Por. *Orzeczenia polskich sądów w sprawach związanych z ochroną danych osobowych*, https://perfectinfo.pl/orzeczenia-polskich-sadow-w-sprawach-zwiazanych-z-ochrona-danych-osobowych/ (30.05.2024).

[26] E. Milczarek, *Prywatność wirtualna*…, s. 74.

[27] Dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. UE L 2002, nr 201, poz. 37).

różnymi poglądami, które często są sprzeczne, co stanowi istotne wyzwanie dla prawodawców i społeczeństwa.

Argumenty za zaostrzeniem przepisów o ochronie danych często podkreślają wzrost zagrożeń wynikających z rozwijających się technologii, takich jak *big data*, sztuczna inteligencja czy internet rzeczy, które mogą prowadzić do nadużyć i nieautoryzowanego wykorzystania danych osobowych[28]. Zwolennicy tej perspektywy argumentują, że tylko przez zaostrzenie regulacji można skutecznie chronić prywatność obywateli przed nadmiernym nadzorem i komercjalizacją ich danych osobowych. Podkreślają, że w dobie cyfrowej każda luka w ochronie danych może skutkować poważnymi konsekwencjami, takimi jak kradzież tożsamości, oszustwa finansowe czy manipulacja różnego typu[29]. Kontrargumenty z kolei wskazują na ryzyko nadmiernej regulacji, która może hamować innowacyjność i rozwój gospodarczy. Krytycy zaostrzania przepisów o ochronie danych zauważają, iż zbyt rygorystyczne prawo może ograniczyć zdolność firm do wykorzystywania danych w celu poprawy i personalizacji usług, co jest kluczowe w konkurencyjnej gospodarce cyfrowej[30]. Podnoszą również, że nadmierne regulacje mogą prowadzić do znacznego wzrostu kosztów dla przedsiębiorstw, szczególnie dla małych i średnich firm, które mogą nie być w stanie sprostać wymogom regulacyjnym[31].

Generalizując, analiza możliwych konsekwencji zaostrzenia przepisów ochrony danych pokazuje, że każde działanie w tej dziedzinie musi być starannie wyważone. Z jednej strony zaostrzenie przepisów może zwiększyć ochronę prywatności i zredukować ryzyko nadużyć, co jest niezbędne dla zachowania zaufania społecznego. Z drugiej strony może ograniczyć zdolności operacyjne przedsiębiorstw, co negatywnie wpłynie na innowacyjność i efektywność ekonomiczną. Mowa zatem o równowadze między prywatnością a bezpieczeństwem w sieci, która jest fundamentalnym elementem tej debaty. Równowaga ta jest niezbędna do zapewnienia, że prawa i wolności jednostek są chronione, jednocześnie umożliwiając skuteczną walkę z przestępczością cyfrową i innymi zagrożeniami dla bezpieczeństwa. Kluczowe staje się tutaj znalezienie takich rozwiązań regulacyjnych, które będą elastyczne i zdolne do adaptacji w szybko zmieniającym się środowisku technologicznym, zachowując przy tym fundamentalne prawa do prywatności i ochrony danych osobowych.

---

[28] W. Dubis, M. Daćków, *Prawo do bycia zapomnianym w internecie – za życia i po śmierci?* [w:] *Non omnis moriar: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane*, t. 1, red. J. Gołaczyński, J. Mazurkiewicz, J. Turłukowski, D. Karkut, Wrocław 2015, s. 174–175.

[29] B. Baran, K. Południak-Gierz, *Perspektywa regulacji prawa do bycia" zapomnianym" w Internecie: zarys problematyki*, „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego, Nauki Społeczne" 2017, nr 17(2), s. 155.

[30] K. Cłapińska, *Prywatność vs. świat wirtualny: ochrona praw jednostki w dobie Internetu*, „Studia Prawa Publicznego" 2023, nr 43(3), s. 160–161.

[31] W. Dubis, M. Daćków, *Prawo do bycia zapomnianym*…, s. 174–175.

Sklepy internetowe standardowo zbierają takie informacje, jak imię i nazwisko, adres, numer telefonu, adres e-mail, historia zakupów, preferencje zakupowe, a czasami dane dotyczące lokalizacji czy urządzenia, z którego korzysta klient. Te dane są wykorzystywane do realizacji zamówień oraz dokonywania rozliczeń pomiędzy stronami umowy, co jest jak najbardziej konieczne i leży w interesie obydwu stron, lecz poza tym również do personalizacji ofert, analizy zachowań klientów i targetowania reklam, co znacznie częściej jest potrzebne wyłącznie stronie sprzedażowej[32].

Nie można zapominać, że udostępnianie danych osobowych w sieci niesie ze sobą również pewne korzyści zarówno dla konsumentów, jak i dla przedsiębiorców. Personalizacja usług, którą umożliwia analiza danych, pozwala na dostosowanie ofert do indywidualnych potrzeb i preferencji klientów. Dzięki temu konsumenci otrzymują rekomendacje produktów, które mogą ich zainteresować, a także oferty promocyjne dopasowane do ich historii zakupów.

W przypadku handlu elektronicznego zapamiętywanie takich danych osobowych, jak adres czy numer telefonu, znacznie ułatwia i przyspiesza proces składania zamówień. Klienci nie muszą za każdym razem ręcznie wprowadzać tych informacji, co oszczędza czas i zwiększa wygodę zakupów. Z uwagi na powyższe wielu konsumentów świadomie akceptuje pewien poziom utraty prywatności w zamian za korzyści płynące z personalizacji usług i wygody zakupów. Badania pokazują, że konsumenci są skłonni udostępniać swoje dane osobowe, jeśli mają poczucie, że przyniesie im to konkretne korzyści, takie jak lepsze oferty czy szybsza obsługa[33]. Należy jednak pamiętać, że akceptacja utraty prywatności nie oznacza zgody na nieograniczone gromadzenie i wykorzystywanie danych osobowych.

Niestety, pomimo obowiązywania RODO ochrona danych osobowych w polskim *e-commerce* pozostawia wiele do życzenia. Wiele platform nie informuje w sposób jasny i przejrzysty o tym, jakie dane zbiera, w jakim celu i komu je udostępnia. Często zgody na przetwarzanie danych są ukryte w długich i skomplikowanych regulaminach, a klienci nie mają realnej możliwości wyboru, czy chcą udostępnić swoje dane i jakie dane chcą przekazywać. Co więcej, ochrona danych rzadko stanowi priorytet firm i potencjalnie dochodzić może do wycieków danych, po czym konsumenci są narażeni na spam, niechciane reklamy i próby wyłudzenia. W ostatnich latach głośno było w mediach o wyciekach danych z popularnych sklepów internetowych, takich jak Morele.net czy Empik[34].

[32] E. Milczarek, *Prywatność wirtualna*…, s. 83.

[33] K. Cłapińska, *Prywatność vs. świat wirtualny*…, s. 160.

[34] Zob. *Rekordowa kara za wyciek danych. Sklep ma kłopoty*, https://www.money.pl/gospodarka/rekordowa-kara-za-wyciek-danych-sklep-ma-klopoty-6993387033082848a.html (29.06.2024); *Morele potwierdza, że wykradziono dane klientów*, https://niebezpiecznik.pl/post/morele-potwierdza-

W wyniku tych incydentów dane osobowe tysięcy klientów, w tym adresy e-mail, hasła czy adresy korespondencyjne, trafiły w niepowołane ręce. Skala problemu jest duża, a Urząd Ochrony Danych Osobowych (UODO) regularnie nakłada kary na przedsiębiorców za naruszenia RODO[35].

Mimo że RODO oraz ustawa o świadczeniu usług drogą elektroniczną stanowią ramy prawne dla ochrony danych osobowych w *e-commerce*, to w praktyce przepisy te są często interpretowane na korzyść przedsiębiorców, a konsumenci mają trudności z dochodzeniem swoich praw.

## Wpływ mediów społecznościowych na prywatność użytkowników

Mechanizmy śledzenia, profilowania i targetowania reklam w mediach społecznościowych są niezwykle zaawansowane. Platformy wykorzystują pliki *cookies*, piksele śledzące, a także analizują treści publikowane przez użytkowników, aby stworzyć szczegółowe profile behawioralne. Na podstawie tych profili reklamodawcy mogą kierować do użytkowników spersonalizowane reklamy, które są dopasowane do ich zainteresowań, wieku, płci czy lokalizacji[36]. I choć personalizacja reklam może być postrzegana jako korzyść, to mechanizmy śledzenia i profilowania budzą poważne obawy dotyczące prywatności. Użytkownicy często nie są świadomi, jakie dane są o nich gromadzone i w jaki sposób są wykorzystywane. Co więcej, algorytmy mediów społecznościowych mogą prowadzić do tworzenia tzw. baniek informacyjnych, gdzie użytkownicy są izolowani od różnorodnych poglądów i informacji[37].

Badania świadomości Polek i Polaków w zakresie cyberbezpieczeństwa przeprowadzone dla Google przez CBM Indicator wykazały, że Polacy są coraz bardziej świadomi zagrożeń związanych z prywatnością w sieci, ale jednocześnie nie podejmują wystarczających działań, by chronić swoje dane[38]. Inne badania wskazują, że algorytmy mediów społecznościowych mogą prowadzić do polaryzacji społeczeństwa i wzrostu dezinformacji[39]. Raporty organizacji pozarządowych,

---

ze-wykradziono-dane-klientow/ (29.06.2024); *Dane części klientów sklepu Empik.com w „głębokim ukryciu”*, https://zaufanatrzeciastrona.pl/post/dane-czesci-klientow-sklepu-empik-com-w-glebokim-ukryciu/ (29.06.2024).

[35] Zob. *Urząd ochrony danych osobowych*, https://uodo.gov.pl/342 (29.06.2024).

[36] K. Cłapińska, *Prywatność vs. świat wirtualny*…, s. 160.

[37] *Korzystasz z Google i Facebooka? Sprawdź, czy algorytm nie zamknął cię w bańce informacyjnej!*, https://cubegroup.pl/blog/korzystasz-z-google-i-facebooka-sprawdz-czy-algorytm-nie-zamknal-cie-w-bance-informacyjnej/ (11.05.2024).

[38] *Google, Ministerstwo Cyfryzacji, NASK i CERT Polska wspólnie dla bezpieczeństwa w internecie*, https://www.nask.pl/pl/aktualnosci/5186,Google-Ministerstwo-Cyfryzacji-NASK-i-CERT-Polska-wspolnie-dla-bezpieczenstwa-w-.html (30.05.2024).

[39] J. Bartlett, *Ludzie przeciw technologii: Jak Internet zabija demokrację (i jak ją możemy ocalić)*, Katowice 2019, s. 133–134.

takich jak Panoptykon czy Fundacja Helsińska, również zwracają uwagę na problem naruszania prywatności w mediach społecznościowych. Organizacje te alarmują, że platformy nie zawsze przestrzegają przepisów RODO, a użytkownicy mają ograniczone możliwości kontroli nad swoimi danymi[40].

Zbieranie danych w mediach społecznościowych musi być również analizowane przez pryzmat obowiązujących regulacji prawnych oraz zasad etyki cyfrowej. Regulacje takie jak RODO nakładają ścisłe wymagania dotyczące zgody na przetwarzanie danych oraz transparentności działań platform społecznościowych. Etyka cyfrowa z kolei podkreśla konieczność zachowania równowagi między korzyściami płynącymi z personalizacji a prawem użytkowników do prywatności[41].

## Podsumowanie

Zgromadzone informacje umożliwiają sformułowanie kilku kluczowych wniosków. Dotyczą one konieczności ciągłej aktualizacji i dostosowywania przepisów o ochronie danych osobowych w obliczu rozwijających się i zmieniających sposobów korzystania użytkowników z treści dostarczanych przez twórców i dostawców internetowych. W kontekście rosnącej roli technologii cyfrowych oraz złożoności współczesnych modeli biznesowych istnieje pilna potrzeba dostosowania regulacji do nowych wyzwań związanych z trendami i sposobem przetwarzania danych.

Obecnie obowiązujące przepisy, w tym RODO, nakładają na podmioty przetwarzające dane obowiązek informowania użytkowników o sposobach ich wykorzystywania. Jednak w praktyce komunikaty te są często sformułowane w sposób niejasny i nieprzystępny, co ogranicza realną kontrolę użytkowników nad ich własnymi danymi. Wobec powyższego konieczne jest wprowadzenie mechanizmów zwiększających transparentność tych procesów, co może obejmować tworzenie standaryzowanych raportów o przetwarzaniu danych, które powinny być publikowane cyklicznie przez platformy cyfrowe, uwzględniając m.in. kategorie odbiorców danych oraz cele ich wykorzystywania. Świadomość użytkowników na temat operowania ich danymi może poprawić wprowadzenie obowiązku udostępniania im szczegółowych historii operacji na ich danych, umożliwiających identyfikację podmiotów trzecich, którym dane zostały przekazane. Wykorzystanie nowych technologii także może się przyczynić do bardziej przejrzystego wykorzystywania danych użytkowników poprzez techniki umożliwiające audyt i śledzenie przepływu danych, np. technologii *blockchain* w kontekście zarządzania zgodami na przetwarzanie danych.

[40] Zob. *Bez pozasądowych organów nie wygramy z „prywatną cenzurą" w mediach społecznościowych*, https://panoptykon.org/pozasadowe-organy-moderacja-komentarz (25.05.2024).

[41] J. Bartlett, *Ludzie przeciw technologii*…, s. 134.

Zgodnie z art. 17 RODO użytkownicy mają prawo do usunięcia swoich danych (tzw. prawo do bycia zapomnianym[42]), jednak w praktyce jego egzekwowanie napotyka liczne bariery techniczne i prawne. Żeby zapewnić użytkownikom rzeczywistą kontrolę nad swoimi danymi, należy wprowadzić jednolite mechanizmy modyfikacji i usuwania danych, dostępne bezpośrednio na platformach internetowych takich jak Facebook, bez konieczności kontaktowania się z działem wsparcia. Poprawę przestrzegania RODO i zasad w nim zawartych, takich jak np. zasada minimalizacji danych, mogłoby zagwarantować nałożenie na administratorów obowiązku okresowego przeglądu przechowywanych informacji i automatycznego usuwania tych, które są zbędne, czy też rozszerzenie zakresu obowiązku informowania użytkowników o przetwarzaniu danych, możliwość ich edycji, a także trwałego usunięcia z baz danych.

Analiza problemu naruszeń przez podmioty przepisów o ochronie danych osobowych pokazuje, że dotychczasowe sankcje przewidziane w RODO, choć skuteczne po ich zastosowaniu, nie spełniają funkcji prewencyjnej. Aby zwiększyć skuteczność zapobiegania na przyszłość negatywnym skutkom nieprawidłowego lub niedozwolonego wykorzystania zebranych informacji, należy ustanowić progresywny system sankcji – uzależniony nie tylko od obrotu przedsiębiorstwa, ale także od skali naruszenia i liczby poszkodowanych użytkowników. Dodatkowo należałoby wprowadzić obowiązek odszkodowania bądź zadośćuczynienia dla użytkowników, których dane zostały naruszone, oraz zwiększyć kompetencje organów nadzorczych, takich jak UODO, w zakresie prowadzenia dochodzeń i nakładania administracyjnych kar finansowych.

RODO, będące obecnie podstawą ochrony danych w Europie, stanowi solidną podstawę ochrony danych osobowych, jednak wymaga uzupełnienia o nowe przepisy uwzględniające rozwój technologii przetwarzania danych, które wymagają m.in. precyzyjnych regulacji dotyczących profilowania użytkowników i automatycznego podejmowania decyzji. Rozwój nowych technologii oraz *e-commerce* umożliwia podejmowanie działań w sposób transgraniczy. Żeby zachować spójność i przewidywalność procesów wpływających na konsumentów, istnieje konieczność harmonizacji przepisów krajowych w obrębie Unii Europejskiej w celu uniknięcia rozbieżności interpretacyjnych między państwami członkowskimi. Nabiera to na znaczeniu szczególnie w kontekście widocznie zmieniających się praktyk biznesowych, kiedy to płatność za korzystanie z treści czy usługi cyfrowej przestaje przybierać formę pieniężną, a zastępuję ją możliwość korzystania przez przedsiębiorców z wprowadzonych przez użytkowników danych osobowych.

Warto wyznaczyć, iż w sytuacja rosnącego znaczenia ochrony danych osobowych konieczne jest zbadanie i wdrożenie innowacyjnych narzędzi oraz technologii,

[42] Zob. D. Chaba, J. Kluza, *Prawo do bycia zapomnianym a zatarcie skazania*, „Zeszyty Prawnicze" 2024, nr 24(2), s. 201–227.

które mogą znacząco zwiększyć kontrolę użytkowników nad swoimi danymi. Wśród takich rozwiązań warto wymienić:

- prywatność różnicową: umożliwia analizę danych w sposób zagregowany, co pozwala na identyfikację pojedynczych osób, jednocześnie dostarczając cennych informacji statystycznych,
- *blockchain*: zapewnia transparentność i niezmienność danych, co może być wykorzystane do tworzenia zdecentralizowanych systemów zarządzania zgodami na przetwarzanie danych,
- szyfrowanie homomorficzne: umożliwia przeprowadzanie obliczeń na zaszyfrowanych danych bez konieczności ich odszyfrowywania, co zwiększa bezpieczeństwo przetwarzania,
- techniki anonimizacji i pseudonimizacji: pozwalają na zastąpienie danych osobowych danymi zastępczymi, co utrudnia identyfikację osób.

Wdrożenie nowych rozwiązań prawnych i technologicznych powinno się odbywać w sposób przemyślany i zrównoważony, uwzględniający zarówno interesy jednostek, jak i potrzeby przedsiębiorstw oraz instytucji publicznych. Kluczowe jest zapewnienie odpowiednich mechanizmów nadzoru i egzekwowania przepisów, a także edukacja społeczeństwa na temat znaczenia ochrony danych osobowych.

## Bibliografia


Banaszak B., Preisner A., *Prawa i wolności obywatelskie w Konstytucji RP*, Warszawa 2002.

Baran B., Południak-Gierz K., *Perspektywa regulacji prawa do bycia" zapomnianym" w Internecie: zarys problematyki*, „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego. Nauki Społeczne" 2017, nr 17(2).

Bartlett J., *Ludzie przeciw technologii: Jak Internet zabija demokrację (i jak ją możemy ocalić)*, Katowice 2019.

*Bez pozasądowych organów nie wygramy z „prywatną cenzurą" w mediach społecznościowych*, https://panoptykon.org/pozasadowe-organy-moderacja-komentarz (25.05.2024).

Chaba D., Kluza J., *Prawo do bycia zapomnianym a zatarcie skazania*, „Zeszyty Prawnicze" 2024, nr 24(2).

Cłapińska K., *Prywatność vs. świat wirtualny: ochrona praw jednostki w dobie Internetu*, „Studia Prawa Publicznego" 2023, nr 43(3).

Czopek J., *Bezpieczeństwo i ochrona prywatności młodzieży w Internecie w kontekście edukacji medialnej*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Pedagogika" 2016, nr 12.

*Digital Around The World*, https://datareportal.com/global-digital-overview (10.05.2024).

Dubis W., Daćków M., *Prawo do bycia zapomnianym w internecie – za życia i po śmierci?* [w:] *Non omnis moriar: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane*, t. 1, red. J. Gołaczyński, J. Mazurkiewicz, J. Turłukowski, D. Karkut, Wrocław 2015.

Dziedzic K., *Jak skutecznie zapewnić sobie anonimowość. Anonimowość w Internecie. Kompletny poradnik krok po kroku*, „Komputer Świat" 2018, nr 1(95).

*Facebook pod ostrzałem za możliwy wyciek danych. Zajmą się nim władze USA i Unii Europejskiej*, https://businessinsider.com.pl/firmy/strategie/facebook-wyciek-danych-manipulacja-wyborami-w-usa-przez-rosje/fjwvbgs (11.05.2024).

*Google, Ministerstwo Cyfryzacji, NASK i CERT Polska wspólnie dla bezpieczeństwa w internecie*, https://www.nask.pl/pl/aktualnosci/5186,Google-Ministerstwo-Cyfryzacji-NASK-i-CERT-Polska-wspolnie-dla-bezpieczenstwa-w-.html (30.05.2024).
Gregorczyk G., *Jak (i czy) dzieci i młodzież chronią swoją prywatność? O edukacji na temat ochrony danych osobowych i cyfrowej tożsamości. Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków 2018.
https://www.pewresearch.org/tools-and-resources/ (28.05.2024).
https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/ (25.05.2024).
*Kiedy usuwamy dane osobowe*, https://www.rp.pl/biznes/art39235301-kiedy-usuwamy-dane-osobowe (27.05.2024).
*Korzystasz z Google i Facebooka? Sprawdź, czy algorytm nie zamknął cię w bańce informacyjnej!*, https://cubegroup.pl/blog/korzystasz-z-google-i-facebooka-sprawdz-czy-algorytm-nie-zamknal-cie-w-bance-informacyjnej/ (11.05.2024).
Kotecka-Kral S., *Postulaty de lege ferenda dotyczące ochrony prywatności użytkowników usług Over-the-Top w Unii Europejskiej*, „Przegląd Prawa i Administracji" 2020, nr 120, t. 1.
Ładysz I., *V edycja konferencji naukowej z serii „Bezpieczna Młodzież" – „Młodzież wobec współczesnych zagrożeń. Prawda i fałsz w cyberprzestrzeni" – Wrocław, 13 czerwca 2023 r.*, „Rocznik Bezpieczeństwa Międzynarodowego" 2023, nr 17(1).
*Meta przeanalizuje, co robisz na Facebooku i WhatsApp, aby szkolić AI. „To dla waszego dobra"*, https://android.com.pl/tech/738480-ai-whatsapp-facebook-meta-dane/ (29.05.2024).
Milczarek E., *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie*, Warszawa 2020.
Niklas J., *Prywatność w internecie*, „Infos zagadnienia społeczno-gospodarcze" 2014, nr 13.
*Orzeczenia polskich sądów w sprawach związanych z ochroną danych osobowych*, https://perfectinfo.pl/orzeczenia-polskich-sadow-w-sprawach-zwiazanych-z-ochrona-danych-osobowych/ (30.05.2024).
Osypowicz M.T., *Wpływ standardów Rady Europy i Unii Europejskiej na zapewnienie bezpieczeństwa danych osobowych w państwach członkowskich*, Kielce 2021.
Pawlak A., *The right to privacy in the era of artificial intelligence* [w:] *Human rights – evolution in the digital era*, red. M Sitek, J. Bonet Navarro, Józefów 2021.
Tyburska J., *Kryterium legalności zgody na przetwarzanie danych osobowych w obrocie elektronicznym*, „Człowiek w Cyberprzestrzeni" 2020, nr 3.
*What Does Facebook Know About You Really?*, https://www.socialmediatoday.com/news/what-does-facebook-know-about-you-really/546502/ (14.05.2024).
*Worldwide digital population 2024*, https://www.statista.com/statistics/617136/digital-population-worldwide/ (10.05.2024).

## Streszczenie

Artykuł analizuje problematykę ochrony prywatności w kontekście mediów społecznościowych i handlu elektronicznego w Polsce. Omawia zmieniające się zagrożenia dla prywatności wynikające z postępu technologicznego i rosnącej obecności cyfrowej. Zostały w nim przedstawione aktualne przepisy, takie jak RODO, oraz ich wpływ na krajowe prawodawstwo, a także konieczność ich adaptacji w odpowiedzi na nowe wyzwania cyfrowe. Artykuł podkreśla potrzebę znalezienia równowagi między ochroną danych osobowych a innowacyjnością gospodarczą, zwracając uwagę na konsekwencje społeczne i prawne naruszeń prywatności. Proponowane są kierunki zmian w polskim prawodawstwie mające na celu lepszą ochronę użytkowników sieci.

*Słowa kluczowe:* dane osobowe, ochrona, użytkownik, regulacje, bezpieczeństwo, zagrożenia

## E-PRIVACY – DEFINING A SAFETY AREA IN SOCIAL MEDIA AND E-COMMERCE


### Summary

The article analyses the issue of privacy protection in the context of social media and e-commerce in Poland. It discusses the changing threats to privacy resulting from technological progress and growing digital presence. Current legislation, such as GDPR, and its impact on national legislation, as well as the need to adapt it in response to new digital challenges, are presented. The article emphasizes the need to find a balance between personal data protection and economic innovation, drawing attention to the social and legal consequences of privacy violations. Directions for amendments to Polish legislation for better protection of online users are proposed.



*Keywords:* personal data, protection, user, regulations, security, dangers