JOURNAL OF MODERN SCIENCE
1/61/2025
www.jomswsge.com
DOI: 10.13166/jms/202386

Dorota Siemieniecka
Nicolaus Copernicus University in Toruń, Poland
ORCID iD: 0000-0002-0745-9960

Joanna Grubicka
Pomeranian University in Słupsk, Poland
ORCID iD: 0000-0001-7934-6044

PŁEĆ I WYKSZTAŁCENIE A ŚWIADOMOŚĆ ZAGROŻEŃ ZWIĄZANYCH Z KORZYSTANIEM Z INTERNETU – PERSPEKTYWA RELACJI INTERPERSONALNYCH

Abstract

Objectives: The aim of the article is to determine how the level of education and gender influence the awareness of threats related to the use of digital technologies, with particular emphasis on the issue of interpersonal relationships.

Material and methods: Research tool: Original questionnaire *Awareness of Internet threats and gender and education – online relationships questionnaire* developed for the needs of the study. The research paradigm included quantitative and qualitative approaches aimed at examining Internet user behavior in the context of potential threats related to Internet addiction.

The research sample consisted of 550 people selected randomly. The statistical analysis used Spearman's rho correlation coefficient to examine relationships between variables, as well as the Mann-Whitney test to compare groups with different demographic characteristics.

Results: The research results and conclusions from the analyzed literature indicate the need to implement educational activities in schools and broad public education through mass media (social campaigns). These activities should cover not only topics related to technological cyber threats, but also the issues of cyberbullying.

Conclusions: The research also showed significant differences in the awareness of threats between genders and the impact of education on the perception of these threats. Women are more aware of the risks of meeting new people online than men, which is confirmed by statistical analyses.

Streszczenie

Cel pracy: Artykuł dotyczy wpływu płci i wykształcenia na świadomość zagrożeń związanych z korzystaniem z internetu. Celem badań jest określenie, czy poziom wykształcenia oraz płeć korelują ze świadomością zagrożeń płynących z technologii cyfrowych w wymiarze relacji interpersonalnych. W badaniach zastosowano metody ilościowe i jakościowe. Wyniki wskazują na istotne różnice w świadomości zagrożeń między płciami oraz wpływ wykształcenia na ich postrzeganie. Kobiety cechuje wyższa świadomość zagrożeń związanych z poznawaniem nowych osób w internecie niż mężczyzn. Badania zostały przeprowadzone na próbie 550 internautów. Tekst poświęcony jest edukacji w zakresie cyberbezpieczeństwa w wymiarze jednostkowym i społecznym.

Celem artykułu jest określenie, czy poziom wykształcenia oraz płeć mają związek ze świadomością zagrożeń wynikających z korzystania z technologii cyfrowych. Analizy te wpisują się w problematykę relacji interpersonalnych.

Materiał i metody: W badaniach wykorzystano *Autorski Kwestionariusz Świadomość zagrożeń internetowych a płeć i wykształcenie – kwestionariusz relacji online* opracowany na potrzeby tej analizy. Paradygmat badawczy łączy podejście

ilościowe z jakościowym. Zbadano zachowania użytkowników internetu w kontekście potencjalnych zagrożeń związanych z korzystaniem z sieci.

Próba badawcza składała się z 550 osób, które zostały dobrane metodą losową. W analizie statystycznej zastosowano współczynnik korelacji rho-Spearmana w celu zbadania zależności między zmiennymi, a także test Manna-Whitneya w celu porównania grup o różnych cechach demograficznych.

Wyniki: Wyniki badań oraz wnioski z analizowanej literatury wskazują na konieczność wdrożenia działań edukacyjnych już na wczesnych etapach edukacji szkolnej. Działania te powinny obejmować nie tylko zagadnienia związane z cyberzagrożeniami technologicznymi, lecz także dotyczące cyberprzemocy.

Wnioski: Badania wykazały istotne różnice w świadomości zagrożeń między płciami oraz wpływ wykształcenia na postrzeganie zagrożeń. Kobiety cechuje wyższy poziom świadomości zagrożeń wynikających z poznawania nowych osób w przestrzeni internetu.

Keywords: *gender, education, awareness of threats, cyberbullying, online security, research results*

Słowa kluczowe: *płeć, wykształcenie, świadomość zagrożeń, cyberprzemoc, bezpieczeństwo w sieci, wyniki badań*

Wprowadzenie

Wynalezienie półprzewodników w XX w. oraz rozwój protokołów komunikacyjnych, takich jak TCP/IP, przyczyniły się do powstania internetu i zwiększenia wydajności komputerów (Białek, 2022). Powstanie internetu zmieniło relacje interpersonalne i komunikację społeczną. Stał się on nie tylko narzędziem służącym do wysyłania prostych wiadomości (pierwszym wysłanym słowem było *LOGIN*) (Adamski, 2012, s. 33), lecz także platformą potrzebną do pracy, służącą dostępowi do wiedzy, narzędziem umożliwiającym wymianę informacji i budowanie relacji międzyludzkich (Jastrzębska, 2020).

Każda technologia wpływa na środowisko życia człowieka i je odmienia. Dziś używa się określenia *homo digitalis*, odnoszącego się do człowieka żyjącego w świecie technologii cyfrowych, oraz sformułowania *homo connectus*, oznaczającego człowieka zalogowanego (Wysocka-Pleczyk, 2014). Odmienne wzorce przekazywania informacji wynikające z braku dostępu do komunikacji niewerbalnej między nadawcą a odbiorcą, w połączeniu

z zaburzeniami osobowości, zachowaniami toksycznymi oraz innymi problemami (również wynikającymi z sytuacji jednostki – np. przeżywanej frustracji, niezadowolenia z własnej sytuacji życiowej – cechującej się nieumiejętnością rozładowania emocji, uzależnieniem od alkoholu lub innych substancji i in.), a także subiektywne odczucie anonimowości, prowadzą do sytuacji,w których niektórzy użytkownicy internetu przekraczają granice prywatności, szacunku oraz bezpieczeństwa emocjonalnego innych osób, a także naruszają przepisy prawa. Anna Miotk podkreśla, że *poczucie anonimowości i równoczesny brak poczucia kontaktu z żywą osobą po drugiej stronie ekranu powodują większą agresję z naszej strony* (IAB, 2016/2017, s. 10).

Zagrożenia płynące z transformacji cyfrowej – aspekty społeczne

Transformacja cyfrowa niesie ze sobą wiele zagrożeń, które mogą prowadzić do kryzysu społeczeństwa cyfrowego. Przedstawione problemy mają jedynie charakter sygnalny. W raportach europejskich (ENISA, 2024) opisuje się wzrost częstotliwości występowania cyberzagrożeń, takich jak: oprogramowanie szantażujące (*ransomware*), złośliwe oprogramowanie (*malware*), zagrożenia dla danych (*threats against data*), zagrożenia dla dostępności: ataków typu Denial of Service (DoS) (*threats against availability*), manipulacja i zakłócanie informacji (*information manipulation and interference*), ataki na łańcuch dostaw (*supply chain attacks*). Wśród nich wymienia się również inżynierię społeczną (*social engineering*). Jak piszą autorzy *Raportu o zagrożeniach. Ochrona przed kluczowymi zagrożeniami w obecnych czasach*: *główną motywacją napastników wciąż pozostaje uzyskiwanie przychodów: złośliwe oprogramowanie pojawia się tam, gdzie są pieniądze* (CISCO, 2019, s. 3). Niektóre z nich mogą być jednak wykorzystywane przez osoby nękające (w kontekście relacji interpersonalnych, motywowane przyczynami osobistymi).

Kolejne niebezpieczeństwa wiążą się z manipulacjami związanymi z wykorzystaniem AI i szeroko rozumianą dezinformacją. Rozwój mediów społecznościowych sprzyja szerzeniu dezinformacji i manipulacji, co może prowadzić do polaryzacji społecznej (NASK, 2024). Algorytmy stwarzają warunki

do powstawania bańki informacyjnej (więcej o tym w rozmowie z J. Kreftem w: Małek, Mórawski, 2021), której rezultatem jest niemożność podejmowania społecznego dialogu (opartego na poszanowaniu innych punktów widzenia) zmierzającego do wypracowania wspólnej wizji rozwiązań. Nadmiar komunikatów emocjonalnych (które nie są ukierunkowane na fakty) oraz wynikające z nich konsekwencje uniemożliwiają zdrowy osąd sytuacji. Brakuje również transparentności działań instytucji w sieci.

Następnym aspektem jest cyfryzacja codziennego życia i wynikająca z niej utrata prywatności. Dane osobowe są gromadzone i dysponują nimi firmy oraz instytucje. Jednak konsekwencje wykorzystania danych osobowych najczęściej ponosi jednostka. Osoby nękające często publikują dane osobowe swoich ofiar. Za pośrednictwem narzędzi sieciowych śledzona jest aktywność (Siemieniecka, Skibińska, Majewska, 2020). Istnieje ryzyko inwigilacji rozmów w sieci, kontroli i łamania praw człowieka. W relacjach interpersonalnych zdarzenia te mają również miejsce.

Transformacja cyfrowa wiąże się także z wykluczeniem cyfrowym i społeczno-cyfrowym. Zjawisko ignorowania przez grupę rówieśników w sieci jest również formą przemocy. Badania wskazują, że *wykluczone cyfrowo to dziś […] osoby najstarsze, w mniejszym stopniu osoby o niskim poziomie wykształcenia oraz osoby o złej sytuacji materialnej […]. Ponad połowa osób (55%), które nigdy nie korzystały z sieci, mieszka na obszarach wiejskich* (Orange, 2021).

Technologie mogą również wpływać na likwidację wielu stanowisk pracy i bezrobocie (badania CBOS ukazują, że wśród bezrobotnych najliczniejszą grupę stanowią osoby wykluczone cyfrowo). Ta sytuacja kolejno przyczynia się do powstawania nierówności ekonomicznych, społecznych i ubóstwa. Sytuacja tych osób pogarsza się poprzez niemożność dostępu do usług świadczonych jedynie drogą elektroniczną. Brak realizacji podstawowych potrzeb (np. poczucia bezpieczeństwa) grup społecznych wpływa na wzrost przestępczości oraz uzależnienie. Ludzie tracą sens podejmowania działań.

Ponadto intensywne korzystanie z technologii może powodować liczne problemy zdrowotne, takie jak wady postawy (problemy z kręgosłupem), problemy z krążeniem, uzależnienia, depresję, bezsenność, czy zaburzenia odżywiania (Wojtkowska, Hewiak, Gąsiorowska, 2023). Oglądane materiały i treści również nie pozostają obojętne dla sfery psychicznej człowieka.

W obliczu tych niebezpieczeństw pojawiają się także kwestie etyczne związane z nowymi technologiami, w tym te dotyczące rozwoju sztucznej inteligencji. Dane medyczne są gromadzone przez systemy i przez nie analizowane, dostęp do nich może być złamany. Innym zagrożeniem jest to, że informacje generowane przez AI mogą być personalizowane w taki sposób, aby uzyskać zamierzoną reakcję grup osób. Mogą w ten sposób kształtować opinię publiczną. Kryzys społeczeństwa cyfrowego przejawia się w rosnącej izolacji społecznej, polaryzacji poglądów, a także podziałach ekonomicznych i społecznych (Auleytner, Grewiński, 2020, s. 15).

Bezpieczeństwo osobiste a nowe technologie

Istnieje jeszcze jeden aspekt, na który wpływ mają nowe technologie, a dotyczy on bezpieczeństwa osobistego oraz relacji międzyludzkich w sieci. Bezpieczeństwo jednostki wobec zjawisk cyberzagrożeń i cyberprzemocy może zależeć od różnych czynników: wiedzy (również tej związanej z posługiwaniem się technologią), umiejętności, zastosowania jej w praktyce, kompetencji cyfrowych oraz umiejętności społecznych. Kontakty online mają podobny status do tych w świecie rzeczywistym, jednak charakteryzują się specyficznymi cechami. Brak komunikacji *face to face* sprawia, że obraz innej osoby budujemy na podstawie jej zachowań autoprezentacyjnych w sieci oraz własnych wyobrażeń na jej temat. W literaturze mówi się o zjawisku *cyfrowej autoprezentacji* (Plichta, Pyżalski, Barlińska, 2018, s. 117). Luba Ślósarz (2021, s. 227) zwraca uwagę, że *sygnały dotyczące wyglądu i sygnały pozawerbalne są dużo wyższe, niż gdy oceniający widzą zdjęcie czy emotikony*.

W przestrzeni sieci *atrakcyjny wygląd zewnętrzny jest jednym z ważniejszych komponentów autoprezentacji i często może okazać się kluczem do sukcesów interpersonalnych* (Plichta, Pyżalski, Barlińska, 2018, s. 117), ale również może być on *czynnikiem powiązanym z występowaniem zjawiska cyberprzemocy* (Amnesty International, 2023). Badania wskazują, że kobiety częściej doświadczały bullyingu ze względu na wygląd (w grupie kobiet: 53,3%, w grupie dziewcząt: 74,7%, w grupie mężczyzn: 38,3%, w grupie chłopców: 55%) (Amnesty International, 2023).

Ocena osoby poznanej przez internet może być powierzchowna, ponieważ jesteśmy podatni na wpływ pierwszego wrażenia, które związane jest z psychologicznym zjawiskiem aureoli (efektem halo). Dodatkowo mamy tendencję do przypisywania pozytywnych cech osobom, które opisują siebie w sposób korzystny, co może zniekształcać nasze postrzeganie.

Ponadto, jak przyznaje J. Grohol, *[…] osoby spędzające zbyt dużo czasu w sieci mogą być narażone na występowanie poważnych problemów, a np. nadmierne korzystanie z internetu stanowić może jedną z form ucieczki od problemów […] i samotności* (Grohol, 1999).

W literaturze przedmiotu funkcjonują dychotomiczne podejścia odnoszące się do wpływu nowych mediów na życie człowieka. Budowanie i podtrzymywanie relacji społecznych, to przejawy korzystnego oddziaływania nowoczesnych technologii cyfrowych (Bębas, Jędrzejko, 2017), jednak relacje te mogą również mieć charakter toksyczny i destruktywny (Grubicka, Kompowska-Marek, 2024). Budowanie relacji z innymi oraz ich znaczenie dla człowieka podkreślają w swoich pracach Daniel Goleman i Karl Albrecht, wskazując na rolę rozwoju inteligencji społecznej oraz jej aspektów, takich jak umiejętności interpersonalne i empatia, które stanowią ważne czynniki wpływające na interakcje społeczne.

Przegląd badań na temat wpływu wykształcenia i płci na świadomość różnych zagrożeń związanych z korzystaniem z internetu

W badaniach CBOS (2019) autorzy piszą, że *o obecności online decyduje przede wszystkim wiek, a dopiero w drugiej kolejności wykształcenie, które ma znaczenie, głównie jeśli chodzi o starszych respondentów (55+)* (CBOS, 2019, s. 1). Jeśli chodzi o wiek, to najliczniejszą grupę użytkowników internetu stanowią osoby w wieku 18–24 lata (100) oraz 25–34 lata (99). Najmniej liczną osoby 65 plus (26). Biorąc pod uwagę wykształcenie, wśród użytkowników dominują osoby z wyższym wykształceniem (95) i gimnazjalnym (93).

Badania te wskazują, że mężczyźni nieznacznie więcej czasu przeznaczają na aktywność w sieci niż kobiety (średnio: 14,21 i 11,59 godz.) (CBOS, 2019).

W raporcie *Bezpieczeństwo w sieci, nowe technologie i AI* (2023) czytamy, że 72% badanych internautów czuje się w internecie bezpiecznie (Związek Pracodawców Branży Internetowej IAB Polska, Money, 2023). Mężczyźni lepiej oceniają stan swojej wiedzy na temat bezpieczeństwa niż badane kobiety. Kobiety odczuwają niższy poziom bezpieczeństwa niż mężczyźni. 79% respondentów pozytywnie ocenia swój poziom wiedzy na temat bezpieczeństwa w sieci (Związek Pracodawców Branży Internetowej IAB Polska, Money, 2023). Ponadto połowa badanych osób nie doświadczyła oszustwa w internecie. Autorzy raportu stwierdzają, że *Im większa wiedza na temat bezpieczeństwa w sieci, tym większe poczucie bezpieczeństwa w sieci*. Wskazuje to na istotną rolę edukacji w zakresie cyberbezpieczeństwa (Związek Pracodawców Branży Internetowej IAB Polska, Money, 2023).

W raporcie CERT (2023) autorzy zwracają uwagę na wzrost świadomości dotyczącej cyberzagrożeń, który przypisują kampaniom informacyjnym w mediach, co potwierdzają dane dotyczące zgłoszeń związanych z bezpieczeństwem w sieci. W 2022 r. zespół CERT Polska odnotował ponad 34-proc. wzrost zarejestrowanych incydentów cyberbezpieczeństwa oraz prawie 178-proc. wzrost wszystkich zgłoszeń (CERT, 2023).

W raporcie *Bezpieczeństwo Cyfrowe Polaków – Oszustwa internetowe i zagrożenia komunikacji mobilnej. Jak bronić się przed oszustwami internetowymi?* (SMSAPI, 2024) czytamy, że co piąty Polak był ofiarą przestępców w internecie, a zagrożonymi grupami są osoby powyżej 50 roku życia. Polacy czerpią wiedzę na temat cyberprzestępstw z mediów (69,4%), od znajomych i rodziny (53,6%), z grup social mediowych i forów internetowych (43,8%), popularnych platform społecznościowych (FB, TikToka, Instagrama) (35,5%), szkoleń w pracy (21,6%), konferencji, szkoleń, webinarów (12,7%). 8,7% badanych nie szuka informacji na ten temat (SMSAPI, 2024, s. 30). Łukasz Tomczyk (2014) zauważa, że *niestety wzrost sprzedaży urządzeń typu tablet lub smartfon nie jest skorelowany z wiedzą ich użytkowników w zakresie poprawnego użytkowania, zabezpieczenia oraz z ilością powstającego złośliwego oprogramowania* (Tomczyk, 2014, s. 283). Natomiast wyniki badań przeprowadzonych przez Centrum Badań Marketingowych Indicator na zlecenie Google (Google Blog Polska, 2022) wskazują na rosnącą

świadomość Polaków w zakresie podstawowych zasad cyberbezpieczeństwa. Aż 95% respondentów nie otwiera załączników od nieznajomych, a 91% unika podejrzanych stron. Mimo to tylko 25% Polaków uczestniczy w szkoleniach dotyczących cyberbezpieczeństwa (Google Blog Polska, 2022). Autorzy raportu wyróżniają wśród grupy badanych respondentów trzy kategorie: Newbies (56,9%), Normcores (13,8%) i Geeks (29,3%). Newbies to osoby z niską świadomością zagrożeń, głównie starsze. Normcores mają podstawową wiedzę o cyberzagrożeniach, natomiast Geeks orientują się w zagrożeniach i stosują metody ochrony. Geeks to grupa o najwyższym poziomie kompetencji w zakresie wiedzy o cyberzagrożeniach (Google Blog Polska, 2022). Weryfikacja dwuetapowa jest znana 66% badanych, ale tylko 50% z nich ją stosuje. Jednakże znajomość bardziej złożonych zagrożeń jest niska: o ataku *ransomware* słyszało jedynie 16% Polaków, a o ataku DDoS – 21%. Mimo to większość (79%) nie pozwala na podłączanie obcych urządzeń do swoich komputerów (Google Blog Polska, 2022).

W zakresie zabezpieczeń 44% badanych tworzy kopie zapasowe danych, a tylko 17% korzysta z menedżerów haseł (Google Blog Polska, 2022). Warto zauważyć, że 43% użytkowników stosuje różne hasła do różnych usług internetowych. Średnia długość hasła wynosi 10,85 znaku. Polacy czerpią wiedzę o cyberbezpieczeństwie głównie z internetu (66%), a tylko 16% korzysta z literatury fachowej (Google Blog Polska, 2022).

Warto zauważyć, że pomimo rosnącej świadomości podstawowych zasad bezpieczeństwa w sieci nadal występują braki w wiedzy dotyczącej bardziej zaawansowanych zagrożeń i metod ochrony. Przygotowanie społeczeństwa do przeciwdziałania cyberzagrożeniom niestety nie jest wystarczające i wymaga ciągłego uzupełniania wiedzy. Nowe technologie to obszar charakteryzujący się bardzo dynamicznymi zmianami. Jak wskazują badania, w szkoleniach z zakresu cyberbezpieczeństwa brała udział co czwarta osoba badana (Google Blog Polska, 2022). Fakt, że w więcej niż czterech szkoleniach brało udział 2% kobiet i 4% mężczyzn (Google Blog Polska, 2022; Klonowska, Stawicka, 2018) może sugerować, że mężczyźni są bardziej zaangażowani w edukację związaną z nowymi technologiami, ale brak jest szczegółowych danych, które jednoznacznie potwierdziłyby różnice między płciami.

Raporty badawcze wskazują na istnienie zróżnicowanych sposobów korzystania z internetu pomiędzy kobietami i mężczyznami. Niestety, nadal brakuje

publikacji poświęconych *stricte* różnicom płciowym w kontekście wiedzy na temat cyberzagrożeń. W dostępnych analizach badawczych wiedza jest zwykle oceniana na podstawie znajomości terminów zagrożeń lub ma charakter deklaratywny. Można zauważyć, że zjawiska cyberprzemocy technologicznej (obejmującej szerszy zakres działań w sieci) stanowią oddzielną kategorię wobec cyberprzemocy (przemocy skierowanej wobec jednostki).

Pojęcie świadomości cyberzagrożeń

Słowo *świadomość* jest definiowane w *Słowniku Języka Polskiego* PWN (2024) jako *zdawanie sobie sprawy z czegoś , wspólne dla określonej grupy ludzi poglądy i cele, stan przytomności, charakterystyczna dla człowieka zdolność poznawania i oceniania siebie i otoczenia.*

W kontekście cyberzagrożeń *świadomość* można rozumieć jako gotowość podjęcia działań w obliczu możliwych zdarzeń w przestrzeni internetu i narzędzi cyfrowych. Polega ona na zdolności do szybkiego rozpoznawania sytuacji zagrażającej (potencjalnie niebezpiecznej), jej oceny klasyfikowanej jako zagrażającej i prawidłowego reagowania w sytuacji jej doświadczenia. Na podstawie wiedzy (lub oprogramowania) osoba jest w stanie ocenić ryzyko wystąpienia danego zagrożenia. Świadomość obejmuje: identyfikację zagrożenia, rozumienie jego istoty i potencjalnych skutków (analiza ryzyka) (Grupa, 2024). W działanie wpisany jest schemat właściwego reagowania (podjęcia działania ochronnego lub minimalizującego skutki) (Grupa, 2024). Świadomość dotyczy przewidywania konsekwencji wynikających z różnych form cyberprzemocy oraz planowanie i podejmowanie działań ochronnych z myślą o przyszłości. Świadomość wymaga nabycia wiedzy na temat funkcjonowania mediów i technologii (na czym polega dany problem, jego przyczyna, z czego on wynika i jakie niesie konsekwencje) i umiejętności podejmowania działań jednostkowych zorientowanych na zachowanie bezpieczeństwa. Ważna jest profilaktyka zagrożeń, a także możliwości podjęcia działań zaradczych.

Świadomość wiąże się z nabyciem kompetencji cyfrowych, takich jak: umiejętność bezpiecznego korzystania z internetu, komunikacji cyfrowej i rozwiązywania problemów cyfrowych (Duda, 2024). Zwraca się uwagę, że *według*

danych Information Commissioner's Office – brytyjskiego odpowiednika UODO, tylko 8% zagrożeń nie jest związanych z działaniem czynnika ludzkiego. 92% zależy od […] ludzi. Ludzie mają więc istotny wpływ na bezpieczeństwo […] i mogą być najsłabszym ogniwem w strukturze (Stech, 2019). Ważna jest również znajomość przepisów prawnych oraz umiejętność postępowania w sytuacjach wymagających zgłaszania aktów cyberprzemocy. Osoba świadoma wie, jak dokumentować incydenty oraz jakie podejmować działania zmierzające do minimalizacji skutków przemocy. Bardzo ważnym aspektem jest opanowanie lęku i zarządzanie własnym stresem w sytuacjach doświadczania przemocy. Osoba świadoma wie, jak zapewnić sobie wsparcie i pomoc w swoim otoczeniu osobistym i instytucjonalnym (wsparcie emocjonalne, pomoc służb). Świadomość cyberzagrożeń wiąże się również z krytycznym myśleniem oraz adaptacyjnym podejściem do trudnych sytuacji doświadczanych w otoczeniu narzędzi cyfrowych. Oznacza to, że ważnym decyzjom polegającym na zaufaniu do innych osób lub napływającym informacjom powinny towarzyszyć podejście refleksyjne i weryfikacyjne (Penszko, Wasilewska, 2024, s. 16). Świadomość pozwala na planowanie działań mających na celu unikanie sytuacji zagrożenia (również w przyszłości) i minimalizowanie ich możliwych skutków (minimalizacja ryzyka). Jest to myślenie, które można opisać następująco: *posiadam wiedzę, dzięki której wiem, co może mnie spotkać, i jestem świadomy sytuacji i możliwych następstw, rozpoznaję zagrożenia, potrafię skutecznie planować swoje działania tak, by chronić siebie i innych, moja postawa jest aktywna, dlatego mam potrzebę wzbogacania swojej wiedzy, po to by umieć radzić sobie z dziś nieprzewidywalnymi, przyszłymi sytuacjami, znam swoje prawa i wiem, kto w razie potrzeby może udzielić mi pomocy.* Świadomość zagrożeń wymaga dostosowywania się do zmiennego środowiska, jakim są media i nowoczesne technologie, w których ciągle pojawiają się nowe zjawiska i formy przemocy. W świadomość zagrożeń wpisane jest także działanie uświadamiające innych. Można zgodzić się ze stwierdzeniem, że *Świadomość zagrożenia jest podstawowym elementem silnego systemu cyberbezpieczeństwa* (Kozłowski, 2017).

Badania dotyczące zagrożeń płynących z patologicznych relacji interpersonalnych w sieci

Badania wykazują, że sprawcami przemocy częściej są mężczyźni (Mullen i in.., 2009; Groth, 2010; Woźniakowska-Fajst, 2019). Przemocy ze względu na płeć doświadczało 71,8% kobiet, podczas gdy w przypadku mężczyzn zjawisko to dotyczyło 32,9% badanych (Amnesty International, 2023).

Badania Amnesty International (2023) przeprowadzone na próbie 1088 osób ujawniły brak pomocy instytucji państwowych oraz wsparcia ze strony administratorów portali internetowych w sytuacjach doświadczania cyberprzemocy przez użytkowników internetu. Osoby doświadczające cyberprzemocy często nie otrzymują wsparcia (Amnesty International, 2023). Zgłoszenia do administratorów odbywają się za pośrednictwem podanych na stronie maili lub formularzy. Reakcja na zgłoszenia jest zbyt późna (Amnesty International, 2023). Raport NASK i DyżurnyNET (Szczęsna i in., 2023), w którym badaniami objęto 32 serwisy internetowe, podaje, że 23 z 32 serwisów nie ma w swoim regulaminie informacji na temat czasu rozpatrywania zgłoszeń dotyczących nadużyć. Nie ma jednolitych regulacji w tej kwestii, a czas reakcji zależy od konkretnego serwisu; czasami może wynosić 48 godzin, a innym razem 72 godziny (Szczęsna i in., 2023). Szybka reakcja administratora serwisu na zgłoszenia cyberprzemocy jest istotna, ponieważ przez cały czas oczekiwania (na odpowiedź i reakcję wobec sprawcy) ofiara doświadcza stresu, który może prowadzić do pogorszenia jej stanu psychicznego. Szybka interwencja i reakcja na cyberprzemoc jest konieczną formą ochrony ofiary przed dalszymi atakami i eskalacją działań sprawcy. Wyniki badań pokazują, że 1 na 10 osób doświadcza cyberprzemocy, a młode kobiety doświadczają jej aż dwukrotnie częściej (Amnesty International, 2023). Ponadto aż 87% badanych wielokrotnie doświadczało cyberprzemocy (Amnesty International, 2023). Wśród możliwych sposobów indywidualnej ochrony osoby badane wymieniały: ograniczone zaufanie podczas korzystania z internetu (77,8%), chronienie swoich danych (85,3%), nieotwieranie podejrzanych e-maili (86,7%) oraz ograniczenie dostępu innym w sieciach społecznościowych do informacji osobistych i zdjęć (Amnesty International, 2023).

Inne badania (Siemieniecka, Skibińska, 2019, 2019a) wykazały, że wśród najczęściej wymienianych form doświadczonej przemocy w internecie są: wysyłanie wiadomości przez komunikator, aby kogoś obrazić/wystraszyć; wysyłanie SMS-ów, żeby dokuczyć/sprawić przykrość/wystraszyć inną osobę; włamanie do poczty internetowej/komunikatora innej osoby i ujawnienie jej tajemnic; agresja werbalna i obrażanie słowne w realnej rzeczywistości; umieszczanie w internecie / rozsyłanie znajomym zdjęć osoby; wyzywanie innych osób podczas rozmów na czacie; komentowanie wypowiedzi na forum internetowym, żeby ośmieszyć / sprawić przykrość / wystraszyć inną osobę; korzystanie bez zgody właściciela, rozsyłanie z jego telefonu / konta internetowego / komunikatora nieprzyjemnych informacji do innych osób; obrażanie/wyzywanie podczas gier online; ujawnienie w internecie czyjejś prywatnej rozmowy/zdjęcia wbrew woli tej osoby; wysłanie umyślne materiału z wirusem komputerowym do innej osoby w celu śledzenia tej osoby, kradzieży jej danych lub destrukcji jej systemu operacyjnego czy oprogramowania (Siemieniecka, Skibińska, 2019, 2019a). Wymienione kategorie również są obecne w raporcie *Cyberprzemoc wobec kobiet w Polsce* (Spurek, 2024). W świetle doniesień tego raportu wśród najczęściej doświadczanych form cyberagresji kobiety doświadczały: wyzwisk i obelg (37% obserwowało, 14% doświadczało), poniżania, obrażania, wyszydzania, wyśmiewania (37% dostrzegało, 11% doświadczało), negatywnych, obraźliwych komentarzy na temat członków rodziny kobiety (26% obserwowało, 6% doświadczało), propozycji seksualnych (20% obserwowało, 10% doświadczało), przesyłania wiadomości o charakterze seksualnym (6% obserwowało, 10% doświadczało), otrzymywania obscenicznych fotografii, np. narządów płciowych (9% doświadczało), tworzenia fałszywej tożsamości z zamiarem oszukania (24% obserwowało, 7% doświadczało), zastraszania (13% obserwowało, 6% doświadczało), uporczywego nękania (12% obserwowało, 5% doświadczało), memów, grafik, zdjęć, fotomontaży o wulgarnym wydźwięku z wizerunkiem kobiet, które nie wyraziły na to zgody (26% obserwowało, 4% doświadczało), upublicznienia osobistych informacji na temat kobiety (19% obserwowało, 4% doświadczało), tworzenia fałszywych profili podważających kompetencje (23% obserwowało, 3% doświadczało), tworzenia fałszywego profilu o wydźwięku erotycznym (17% obserwowało, 2% doświadczało), nawoływania do przemocy wobec

kobiety (12% obserwowało, 2% doświadczało), upubliczniania informacji na temat życia intymnego kobiety i gróźb tego dotyczących (10% obserwowało, 2% doświadczało), gróźb śmierci, uszkodzenia ciała (8% obserwowało, 2% doświadczało), gróźb najścia w miejscu zamieszkania (6% obserwowało, 2% doświadczało), gróźb najścia / czekania pod szkołą / pracą (6% obserwowało, 2% doświadczało), udostępniania intymnych zdjęć i nagrań bez wiedzy i zgody kobiety (11% obserwowało, 1% doświadczał), gróźb gwałtu lub innego rodzaju przemocy seksualnej (7% obserwowało, 1% doświadczał); (Spurek, 2024, s. 96). Wymienione zagrożenia można ująć w grupy problemowe: agresję słowną i poniżanie (100% obserwowało, 31% doświadczało), molestowanie seksualne (obserwowało 26%, doświadczało 29%), zastraszanie i nękanie (obserwowało 25%, doświadczało 11%), upublicznianie informacji i fałszywe tożsamości (obserwowało 100%, doświadczało 20%), groźby i przemoc (obserwowało 20%, doświadczało 3%). Większość wymienionych form przemocy mieści się w opisie zachowań wskazujących na nękanie lub cyberstalking. W literaturze rys psychologiczny i kryminologiczny osób nękających został szczegółowo opisany (Mullen i in., 2009; Woźniakowska-Fajst, 2019).

Przytoczone badania pokazują skalę zjawiska przemocy wobec kobiet. Fakt, że aż 71,8% kobiet doświadczyło przemocy ze względu na płeć, wskazuje na potrzebę wdrożenia skutecznych interwencji wobec sprawców cyberprzemocy w przestrzeni cyfrowej (Amnesty International, 2023) i realizacji postulowanych w literaturze rozwiązań (szybkiego reagowania administratorów na zgłoszenia aktów przemocy) (Amnesty International, 2023; Szczęsna i in., 2023).

W tym kontekście zasadne jest pytanie, czy płeć oraz wykształcenie mają wpływ na świadomość zagrożeń związanych z nawiązywaniem nowych znajomości w internecie.

Metodologia badań

Celem badania jest ustalenie, czy między kobietami a mężczyznami istnieją różnice w świadomości zagrożeń związanych z poznawaniem nowych osób przez internet oraz zbadanie tego, w jaki sposób poziom wykształcenia wpływa na świadomość zagrożeń związanych z korzystaniem z internetu.

W badaniach przyjęto następujące hipotezy badawcze:

H1: Im wyższy poziom wykształcenia, tym większa świadomość zagrożeń związanych z poznawaniem nowych osób przez internet.

H2: Kobiety są bardziej niż mężczyźni świadome zagrożeń związanych z poznawaniem nowych osób przez internet.

Badanie zostało przeprowadzone na próbie 550 osób w okresie od 2 lutego do 15 czerwca 2024 r. Uczestników rekrutowano za pośrednictwem mediów społecznościowych oraz platform internetowych.

W badaniach zastosowano autorski kwestionariusz online, który składał się z kilku sekcji, zorientowanych na ocenę relacji między płcią, wykształceniem a świadomością zagrożeń związanych z korzystaniem z internetu, ze szczególnym uwzględnieniem perspektywy relacji interpersonalnych. Kwestionariusz podzielono na trzy główne części. Pierwszą sekcję stanowiły informacje demograficzne. Sekcja ta zawierała pytania dotyczące płci, wieku, poziomu wykształcenia oraz miejsca zamieszkania. Celem tej części było zebranie podstawowych danych o respondentach, które pozwoliłyby na analizę z uwzględnieniem różnych grup społecznych.

Druga sekcja koncentrowała się na aktywności online użytkowników. Pytania dotyczyły dziennego czasu spędzanego w sieci oraz rodzajów podejmowanych aktywności, takich jak korzystanie z mediów społecznościowych, granie w gry online, zakupy internetowe czy edukacja zdalna. Zawierała również pytania o urządzenia używane do łączenia się z internetem, np. smartfony, tablety i komputery. Celem tych pytań było określenie wzorców użytkowania sieci przez badanych oraz zbadanie ich potencjalnego wpływu na relacje społeczne.

Trzecia, najważniejsza sekcja dotyczyła świadomości zagrożeń związanych z korzystaniem z internetu. Respondenci byli pytani o swoje postrzeganie ryzyka związanego z cyberprzemocą, phishingiem, kradzieżą danych osobowych

oraz możliwością utraty prywatności. W tej części badano także znajomość narzędzi ochronnych, takich jak oprogramowanie antywirusowe czy narzędzia do kontroli rodzicielskiej. Respondenci oceniali również, na ile ich korzystanie z internetu wpływa na relacje z innymi ludźmi – zarówno w kontekście prywatnym, jak i zawodowym.

Kwestionariusz zawierał zarówno pytania zamknięte (np. na skali Likerta), które umożliwiały uproszczoną analizę statystyczną, jak i pytania otwarte, dające respondentom możliwość pełniejszego wyrażenia opinii na temat zagrożeń i korzyści wynikających z użytkowania sieci.

Pozyskane dane poddano analizie statystycznej przy użyciu współczynnika korelacji rho-Spearmana, oraz testu Manna-Whitneya, co pozwoliło na określenie siły i kierunku zależności między zmiennymi. Wyniki analizy przedstawiono w formie tabel. Tego typu badania, jak również raporty dotyczące cyberprzemocy, wskazują na potrzebę dalszej edukacji społeczeństwa w zakresie bezpiecznego korzystania z internetu oraz na konieczność wprowadzenia bardziej efektywnych regulacji prawnych i mechanizmów ochrony ofiar.

Charakterystyka próby badawczej

Dobór próby do badań: Grupa badawcza została dobrana na podstawie różnych kryteriów demograficznych, takich jak wiek, płeć, miejsce zamieszkania, wykształcenie, status rodzinny oraz aktywność zawodowa. Dobór próby miał na celu uzyskanie reprezentatywnych wyników, odzwierciedlających przekrój społeczny użytkowników internetu, a także zbadanie ich świadomości zagrożeń związanych z nawiązywaniem nowych znajomości online. Liczba uczestników badania wyniosła $N = 550$. Wiek: 25–31 lat (n = 180; 32,7%), 32–39 lat (n = 155; 28,2%), 18–24 lata (n = 130; 23,6%), 40–50 lat (n = 61; 11,1%), powyżej 50 lat ($n = 24$; 4,4%). Płeć: kobieta (n = 303; 55,1%), mężczyzna (n = 247; 44,9%). Miejsce zamieszkania: miasto do 50 tys. mieszkańców (n = 174; 31,6%), miasto do 150 tys. mieszkańców (n = 166; 30,2%), wieś ($n = 115$; 20,9%), miasto powyżej 150 tys. mieszkańców ($n = 95$; 17,3%). Wykształcenie: średnie ($n = 231$; 42,0%), wyższe – licencjat/inżynier ($n = 201$; 36,5%).wyższe – magister ($n = 99$; 18,0%),

podstawowe (n = 19; 3,5%). Status rodzinny respondentów: posiadająca/y partnera (n = 239; 43,5%), w związku małżeńskim (n = 161; 29,3%), samotna/y (n = 105; 19,1%), rozwiedziona/y (n = 45; 8,2%). Aktywność zawodowa: pracuję (n = 341; 62,0%), uczę się / studiuję i pracuję (n = 72; 13,1%), nie pracuję (n = 44; 8,0%), studiuję (n = 36; 6,5%), uczę się (n = 30; 5.5%), urlop macierzyński / wychowawczy (n = 27; 4,9%).

Badanie dotyczyło wpływu płci i wykształcenia na świadomość zagrożeń związanych z korzystaniem z internetu. W analizie uwzględniono zmienne demograficzne, a mianowicie: wiek, płeć, miejsce zamieszkania, wykształcenie, status rodzinny oraz aktywność zawodową. Wiek uczestników badania był zróżnicowany, przy czym najliczniejszą grupę stanowiły osoby w wieku 25–31 lat (32,7%), a najmniej liczną grupę – respondenci powyżej 50. roku życia (4,4%). Kobiety stanowiły 55,1% populacji badanej, co sugeruje, że w badaniu wzięła udział większa liczba kobiet niż mężczyzn (44,9%). Pod względem wykształcenia najliczniejszą grupę stanowiły osoby mające wykształcenie średnie (42,0%), a najmniej liczną – podstawowe (3,5%). Warto również zauważyć, że 62% badanych było aktywnych zawodowo, co może przekładać się również na sposób, w jaki badani postrzegają zagrożenia związane z internetem.

H1: Im wyższy poziom wykształcenia, tym większa świadomość zagrożeń związanych z poznawaniem nowych osób przez internet – uzyskane wyniki sugerują przyjęcie hipotezy, że wraz ze wzrostem wykształcenia istotnie wzrasta świadomość zagrożeń związanych z poznawaniem nowych osób przez internet.

Wyniki analizy korelacji rho-Spearmana

W celu określenia siły i kierunku zależności między zmienną *wykształcenie* a zmienną *czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet* wykorzystano współczynnik korelacji monotonicznej rho-Spearmana. Uzyskane wyniki przedstawiono w tabeli (Tabela 1).

Tabela 1. *Wyniki analizy korelacji rho-Spearmana*

					95% CI		
Zmienna 1	Zmienna 2	*n*	*rho*		Lower	Upper	*p*
Wykształcenie	Czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet	550	0,07	*	-0,02	0,16	0,048

H_1: korelacja dodatnia

* $p < 0,05$, ** $p < 0,01$, *** $p < 0,001$

Wyniki analizy korelacji rho-Spearmana wskazują na występowanie istotnej zależności między zmienną *ykształcenie* a zmienną *czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet*, *rho* = 0,07*, 95% CI [-0,02; 0,16], p = 0,048, n = 550. Siła korelacji okazała się bardzo mała, kierunek korelacji okazał się pozytywny – wraz ze wzrostem wykształcenia istotnie wzrasta świadomość zagrożeń związanych z poznawaniem nowych osób przez internet.

H2: Kobiety są bardziej niż mężczyźni świadome zagrożeń związanych z poznawaniem nowych osób przez internet – uzyskane wyniki sugerują przyjęcie hipotezy, że kobiety wykazują większą świadomość zagrożeń związanych z poznawaniem nowych osób w porównaniu z grupą mężczyzn.

Porównanie dwóch grup (zmienna niezależna: *płeć*)

Podstawowe statystyki opisowe dotyczące zmiennej *czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet*, z podziałemze względu na zmienną *płeć*, przedstawiono w tabeli (Tabela 2).

Tabela 2. *Podstawowe statystyki opisowe – podział ze względu na zmienną płeć*

	Płeć	*N*	*M*	*SD*	*Me*	Min.	Maks.	*IQR*
Czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet	Kobieta	303	3,66	0,515	4,00	1,00	4,00	1,00
	Mężczyzna	247	3,51	0,555	4,00	1,00	4,00	1,00

N – liczba ważnych obserwacji, *M* – średnia, *SD* – odchylenie standardowe, *Me* – mediana, Min. – wartość minimalna, Maks. – wartość maksymalna, *IQR* – rozstęp międzykwartylowy

Wyniki testu Manna-Whitneya

W celu określenia istotności różnic między dwiema grupami (*Czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet* – zmienna zależna; *płeć* – zmienna niezależna) wykorzystano test Manna-Whitneya. Uzyskane wyniki przedstawiono w tabeli (Tabela 3).

Tabela 3. *Wyniki testu Manna-Whitneya – istotność różnic między dwoma grupami (zmienna niezależna: Płeć)*

					95% CI	
Zmienna	*U*		*p*	r_{rb}	Lower	Upper
Czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet	42,605,00	***	<0,001	0,14	0,04	0,23

H_1: kobieta > mężczyzna
* $p < 0,05$, ** $p < 0,01$, *** $p < 0,001$

Wyniki testu Manna-Whitneya w zakresie zmiennej *czy słyszał/a Pan/Pani lub czytał/a o zagrożeniach związanych z poznawaniem nowych osób przez internet* wskazują na występowanie istotnie wyższych wartości w grupie kobiet (M = 3,66, SD = 0,515, Me = 4, IQR = 1), w porównaniu z grupą mężczyzn (M = 3,51, SD = 0,555, Me = 4, IQR = 1), U = 42605***, p <0,001, r_{rb} = 0,14, 95% CI [0,04; 0,23], n = 550. Siła obserwowanego efektu (r_{rb}) okazała się mała. Wyniki wskazują, że kobiety są bardziej świadome zagrożeń związanych z poznawaniem nowych osób w internecie.

Wnioski

Ważnym wnioskiem płynącym z przeprowadzonych badań jest potwierdzenie hipotezy mówiącej o korelacji pomiędzy poziomem wykształcenia a większą świadomością zagrożeń związanych z poznawaniem nowych osób przez internet. Uzyskany współczynnik korelacji rho = 0,07, choć wskazuje na bardzo niską siłę, jest jednak statystycznie istotny (p = 0,048). Można wiązać ten wynik z faktem, że kobiety częściej niż mężczyźni padają ofiarami cyberbullyingu (np. nękania przez internet). Badania wykazały również istotne różnice między kobietami a mężczyznami w zakresie świadomości zagrożeń związanych z internetem. Kobiety uzyskały wyższą średnią (M = 3,66) w porównaniu z mężczyznami (M = 3,51), co potwierdzają wyniki testu Manna-Whitneya (U = 42605, p < 0,001). To może sugerować, że kobiety są bardziej ostrożne i świadome potencjalnych zagrożeń w sieci. Możliwe, że rzadziej są one skłonne podejmować zachowania ryzykowne. Wyniki analizy korelacji sugerują, że wyższy poziom wykształcenia wiąże się z większą świadomością zagrożeń. Ważny jest dostęp do filmów, kampanii edukacyjnych oraz doświadczeń innych osób, a także szkoleń realizowanych w pracy (SMSAPI, 2024). Choć mężczyźni, jak wskazują badania, w większym stopniu niż kobiety interesują się technologiami i częściej dokształcają się w tym obszarze (Google Blog Polska, 2022), to jednak kobiety są bardziej świadome zagrożeń wynikających z kontaktów z innymi. Ta świadomość może być związana z częstszym doświadczaniem przez nie

cyberprzemocy (Spurek, 2024; Woźniakowska-Fajst, 2019) w charakterze świadka i ofiary oraz posiadanymi kompetencjami społecznymi.

Zakończenie

Edukacja jest istotnym elementem budowania świadomości społecznej. Bezpieczeństwu służy również budowanie środowiska społecznego, w którym każda osoba może zwrócić się o pomoc i ją otrzymać.

Na wczesnym etapie edukacji należy wdrażać działania profilaktyczne zorientowane na rozwijanie poczucia własnej wartości, zdolności, umiejętności komunikacyjnych (w tym formułowania riposty, zachowań asertywnych). Świadomość cyberzagrożeń wymaga zdolności rozpoznawania i reagowania na trudne sytuacje (również w charakterze świadka). W kontekście nowych technologii ważne jest kształtowanie aktywnych postaw w poszukiwaniu i aktualizacji swojej wiedzy oraz umiejętności. Dodatkowo istotne jest rozwijanie empatii, etycznego i odpowiedzialnego korzystania z technologii. Ważna jest również edukacja w zakresie prawa. Nauczanie w tym obszarze wymagałoby przedstawiania konkretnych sytuacji problemowych i możliwości rozwiązań. Materiały powinny mieć formy syntetycznych, łatwych do zapamiętania memów, filmów, rolek popularyzowanych w mediach społecznościowych.

Istnieje potrzeba przeprowadzenia dalszych, pogłębionych badań nad czynnikami demograficznymi w kontekście świadomości cyberzagrożeń. Warto rozszerzyć przyszłe analizy o uwzględnienie zróżnicowanych kategorii, takich jak poziom wiedzy na temat cyberzagrożeń (warunkujący ich rozpoznawanie), umiejętności oraz ich zastosowanie w trudnych sytuacjach. Interesujące byłyby analizy procesu predykcji następstw oraz procesu rozwiązywania problemów w kontekście różnic płciowych, a także motywacji warunkującej podejmowanie przez jednostkę działań związanych z ochroną siebie i innych. Ciekawym aspektem byłoby również badanie czynników emocjonalnych i środowiskowych, które kształtują świadomość cyberzagrożeń.

References

Adamski, A. (2012). *Media w analogowym i cyfrowym świecie. Wpływ cyfrowej rewolucji na rekonfigurację komunikacji społecznej*. Warszawa: Dom Wydawniczy Elipsa.

Amnesty International. (2023). *Cyberprzemoc krzywdzi naprawdę. Prawie co piąta młoda dziewczyna doświadczyła cyberprzemocy*. Pobrano z https://www.amnesty.org.pl/badania-prawie-co-piata-mloda-dziewczyna-doswiadczyla-cyberprzemocy/ (dostęp: 08.03.2025).

Auleytner J., Grewiński M. *Pandemia koronawirusa i ryzyka społeczne z nią związane a chaos w zarządzaniu państwem – dokąd zmierzamy?* Pobrano z https://izss.uken.krakow.pl/wp-content/uploads/sites/13/2023/01/Julian-Auleytner-Miroslaw-Grewinski-Pandemia-koronawirusa-i-ryzyka-spoleczne-z-nia-zwiazane-a-chaos.pdf (dostęp: 08.03.2025).

Bębas, S., Jędrzejko, M. Z. (2017). *Cyberprzestrzeń – próba diagnozy głównych zagrożeń*. W: S. Bębas, M.Z. Jędrzejko, K. Kasprzak, A. Szwedzik, A. Taper (red.), *Cyfrowe dzieci: zjawisko, uwarunkowania, kluczowe problemy*. Warszawa: Oficyna Wydawnicza Aspra-JR.

Białek, A. (2022). *Jak powstał Internet – historia wynalazku, bez którego nie wyobrażamy sobie życia. National Geographic Polska.* Pobrano z https://www.national-geographic.pl/technologia/jak-powstal-internet-historia-wynalazku-bez-ktorego-nie-wyobrazamy-sobie-zycia/ (dostęp: 08.03.2025).

CISCO (2019). *Raport o zagrożeniach. Luty 2019. Ochrona przed kluczowymi zagrożeniami w obecnych czasach*. Pobrano z https://www.cisco.com/c/dam/global/pl_pl/assets/pdfs/pl_cybersecurityseries_thrt_01_0219_r2-2.pdf (dostęp: 08.03.2025).

CBOS. (2019). *Korzystanie z Internetu – komunikat z badań* (Nr 95). Warszawa: CBOS. ISSN 2353-5822.

CERT Polska. (2023). *Krajobraz bezpieczeństwa polskiego Internetu w 2022 roku*. NASK. Pobrano z https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp: 08.03.2025).

Duda, D. (2024). *Kompetencje cyfrowe użytkowników cyberprzestrzeni newralgicznym komponentem systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Praca doktorska. WAT. Pobrano z https://bip.wat.edu.pl/bip/dokumenty/postepowania-awansowe/dduda/rozprawa_doktorska_d_duda.pdf (dostęp: 08.03.2025).

Google Blog Polska. (2022, 25 listopada). *Jesteśmy coraz bardziej świadomi zagrożeń w sieci. Technologia, produkty, kultura i informacje z Google*. Pobrano z https://polska.googleblog.com/2022/11/jestesmy-coraz-bardziej-swiadomi.html (dostęp: 08.03.2025).

Grądzki, W. (2023). *Współczesne wyzwania społeczeństwa informacyjnego*. Journal of Modern Science, 52(3), 458-477. https://doi.org/10.13166/jms/174419

Grochala, M. (2023, 25 kwietnia). Efekt halo, czyli jaki wpływ ma pierwsze wrażenie? *Lifestyle i wydarzenia*. Lancerto. Pobrano z https://www.lancerto.com/pl/blog/efekt-halo-czyli-jaki-wplyw-ma-pierwsze-wrazenie (dostęp: 08.03.2025).

Grohol, J.M. *Internet addiction guide. Internet addiction guide*. 1999 [updated 2005, April 16; cited 2011 April 20]; Pobrano z http: //psychcentral.com/ netaddiction/ (dostęp: 08.03.2025).

Groth, J. (2010). Cyberstalking – perspektywa psychologiczna. *Forum Oświatowe*, *2*(43).

Grubicka, J., Kompowska-Marek R. (2024). *Przestrzeń cyfrowa w ponowoczesności jednostka – technologia – profilaktyka*. Warszawa: Difin.

Grupa, E. (2024). Ocena ryzyka cybernetycznego, czyli jak zapobiegać i reagować na zagrożenia w sieci? Pobrano z https://www.grupae.pl/ocena-ryzyka-cybernetycznego-czyli-jak-zapobiegac-i-reagowac-na-zagrozenia-w-sieci/ (dostęp: 08.03.2025).

IAB Polska (2016/2017). *Internetowa kultura obrażania*. Pobrano z https://iab.org.pl/wp-content/uploads/2017/05/InternetowaKulturaObrazania_2016_2017_raport_20170511.pdf (dostęp: 08.03.2025).

Jastrzębska, J. (2020). Internet jako miejsce nawiązywania relacji interpersonalnych. Grupy społeczne w obszarze cyberprzestrzeni. *Kwartalnik Naukowy Fides Et Ratio*, *42*(2), 92–100. https://doi.org/10.34766/fetr.v42i2.277

Klonowska I., Stawnicka J. (2018). Płeć determinantem różnicującym pracę dzielnicowego: analiza badań krzyżowych : ujęcie społeczno-pedagogiczno-psychologiczne. Warszawa: Komenda Główna Policji, s. 305.

Kozłowski, A. (2017). *Świadomość zagrożenia to fundament cyberbezpieczeństwa (analiza)* Pobrano z https://cyberdefence24.pl/swiadomosc-zagrozenia-to-fundament-cyberbezpieczenstwa-analiza (dostęp: 08.03.2025).

Małek, M., Mórawski, K. (2021). Wywiad z prof. J. Kreftem. *Cyberprzestrzeń to lustrzane odbicie nierówności społecznych w rzeczywistości. IT@BANK*. Miesięcznik Finansowy BANK.

Mullen, P.E., Pathe, M., & Purcell, R. (2009). *Stalkers and their victims*. Cambridge: Cambridge University Press.

NASK (2024). *Polaryzacja społeczeństwa jako cel dezinformacji.* Pobrano z https://nask.pl/magazyn/polaryzacja-spoleczenstwa-jako-cel-dezinformacji/ (dostęp: 08.03.2025).

Orange (2021). *Wykluczenie społeczno-cyfrowe w Polsce.. Stan zjawiska, trendy, rekomendacje*. Pobrano z https://fundacja.orange.pl/app/uploads/2021/11/RAPORT_WYKLUCZENIE-SPOLECZNO-CYFROWE-W-POLSCE_2021.pdf (dostęp: 08.03.2025).

Penszko, P., Wasilewska, O. (2025). *Krytyczne myślenie, ocena wiarygodności informacji. Wnioski z międzynarodowych badań edukacyjnych i przeglądu literatury.* Instytut Badań Edukacyjnych. Pobrano z https://ibe.edu.pl/images/publikacje/Analizy-ibe-Krytyczne-myslenie-ocena-wiarygodnoci-informacji.pdf (dostęp: 08.03.2025).

Plichta, P., Pyżalski, J., Barlińska, J. (2018). Cyberprzemoc a kreowanie własnego wizerunku w internecie – co w ich mechanizmach zmienia niepełnosprawność młodych dorosłych osób. *Interdyscyplinarne Konteksty Pedagogiki Specjalnej*, *20*.

PWN. (2024). Świadomość. W: *Słownik języka polskiego PWN*. Pobrano z https://sjp.pwn.pl/slowniki/%C5%9Bwiadomo%C5%9B%C4%87.html (dostęp: 08.03.2025).

Siemieniecka, D., Skibińska, M. (2019). Cyberprzemoc w doświadczeniu studentów kierunków pedagogicznych WNP UMK w Toruniu – raport z badań. *Głos Uczelni*.

Siemieniecka, D. &Skibińska, M. (2019a). Stalking and cyberstalking as a form of violence. *Society. Integration. Education. Proceedings of the International Scientific Conference*, *3*, 403– 413.

Siemieniecka, D., Skibińska, M., Majewska K. (2020). *Cyberagresja – zjawisko, skutki, zapobieganie*. Toruń: Wydawnictwo Naukowe UMK.

SMSAPI (2024). *Bezpieczeństwo cyfrowe Polaków: Oszustwa internetowe i zagrożenia komunikacji mobilnej. Jak bronić się przed oszustwami internetowymi?* Pobrano z https://www.smsapi.pl/static/files/Bezpieczenstwo_cyfrowe_Polakow-Raport_SMSAPI_2024.pdf (dostęp: 08.03.2025).

Spurek, S. (2024). *Cyberprzemoc wobec kobiet w Polsce*. Raport z badań. Pobrano z https://sylwiaspurek.pl/wp-content/uploads/2024/06/raport-cyberprzemoc-10-online. (dostęp: 08.03.2025).

Stech, G. (2019). *Jak budować świadomość cyberzagrożeń.* Pobrano z https://www.computerworld.pl/article/2503889/jak-budowac-swiadomosc-cyberzagrozen.html (dostęp: 08.03.2025).

Szczęsna, A., Zalewska, E., Zegarow, P., Sowiński, P., Michałowski, A., Dąbrowski, M. (2023). *Od zgłoszenia do reakcji: Raport z badania szkodliwych treści w serwisach internetowych*. NASK Państwowy Instytut Badawczy. Pobrano z https://cyberpolicy.nask.pl/wp-content/uploads/2023/12/Od_zgloszenia_do_reakcji.pdf (dostęp: 08.03.2025).

Ślósarz, L. (2024). *Autoprezentacja a komunikacja zapośredniczona przez komputer*. Wrocław: Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu.

Tomczyk, Ł. (2014). Zagrożenia dla urządzeń mobilnych. W: J. Lizut (red.), *Zagrożenia cyberprzestrzeni: kompleksowy program dla pracowników służb społecznych* (s. 281– 287). Warszawa: Wyższa Szkoła Pedagogiczna im. Janusza Korczaka. Pobrano z https://cyberprofilaktyka.pl/pliki/4-zagrozenia_cyberprzestrzeni_produkt_finalny.pdf (dostęp: 07.01.2025).

Wojtkowska, A., Hewiak, E., Gąsiorowska, A. (2023). *Nadużywanie mediów elektronicznych przez dzieci i młodzież: badanie rozpowszechnienia problemu, jego determinantów i nowej interwencji profilaktycznej redukującej skalę problemu*. Pobrano z https://kcpu.gov.pl/wp-content/uploads/2024/01/FBS_Naduzywanie-mediow-elektronicznych-przez-dzieci-i-mlodziz-.pdf (dostęp: 02.01.2025).

Woźniakowska-Fajst, D. (2019). *Stalking i inne formy przemocy emocjonalnej. Studium kryminologiczne*. Warszawa: Wydawnictwo Uniwersytetu Warszawskiego.

Wysocka-Pleczyk, M. (2014). *Człowiek zalogowany – wirtualne społeczności 2*. Pobrano z https://open.icm.edu.pl/items/3cc80540-3717-4da7-b93b-dafe5713d3bf (dostęp: 02.11.2024).

Związek Pracodawców Branży Internetowej IAB Polska. Money (2023). *Bezpieczeństwo w sieci: nowe technologie i AI*. IAB Polska. Pobrano z https://money2.wpcdn.pl/raporty/bezpieczenstwo-w-sieci-nowe-technologie-i-ai.pdf (dostęp: 02.01.2025).