Elżbieta Żywucka-Kozłowska
https://orcid.org/0000-0002-6039-5580
Wydział Prawa i Administracji
Uniwersytet Warmińsko-Mazurski w Olsztynie

Robert Dziembowski
https://orcid.org/0000-0002-1697-637X
Wydział Prawa i Administracji
Uniwersytet Warmińsko-Mazurski w Olsztynie

Społeczeństwo informacyjne w perspektywie wybranych aktów prawnych Unii Europejskiej

Słowa kluczowe: pedofilia, Unia Europejska, rozporządzenie, dyrektywa, przestępczość internetowa, komunikatory internetowe
Key words: pedophilia, European Union, regulation, directive, Internet crime, instant messaging

Wstęp

Społeczeństwo informacyjne zdaniem Mariana Golki (2005: 254) to „[…] takie, którego najważniejszą cechą jest produkcja, gromadzenie i obieg informacji, co jest uznawane za niezbędny warunek jego funkcjonowania". Trudno sobie wyobrazić współczesny świat bez komputerów, prasy, baz danych oraz szeregu różnego rodzaju informacji, klasyfikowanych według różnych kryteriów. Michał Goliński (2005) podkreśla w związku z terminem „społeczeństwo informacyjne", że brak jest obecnie jego definicji, która byłaby powszechnie akceptowana. Jakkolwiek by nie rozumieć przedmiotowego pojęcia, jest zawsze kojarzone po pierwsze ze społeczeństwem, po drugie z informacją. Bogata literatura naukowa dotycząca społeczeństwa informacyjnego nie tylko sięga do jego początków, ale także opisuje jego cechy (Goban-Klas i Sienkiewicz 1999; Castells 1996; Borowiec 2009; Babik i Rykaczewska-Wiorogórska 1998; Wierzbołowski 2006; Muraszkiewicz 2004).

Społeczeństwo informacyjne a prawo

W XXI wieku najbardziej pożądanym dobrem o uniwersalnym charakterze jest informacja. Oczywiste jest, że treść poszukiwanej informacji jest uzależniona od określonego wycinka rzeczywistości społecznej, prawnej, gospodarczej

i/lub politycznej. Jest to jedynie przykładowe wyliczenie, którego katalog wydaje się być otwarty z racji stale postępującego rozwoju ludzkości, a co za tym idzie, kreowania coraz to nowych obszarów ludzkich zainteresowań i potrzeb. Najbardziej widocznym przejawem szybko przepływających informacji jest handel elektroniczny. Popyt i podaż to jedno, jednak w perspektywie przekazu ofert, umów i postanowień najważniejsza jest informacja, czyli treść interesująca strony transakcji.

Dyrektywa o handlu elektronicznym

Zgodnie z postanowieniami Dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 roku w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (tak zwanej dyrektywy o handlu elektronicznym; zob. w bibliografii: Dyrektywa 2000/31/WE), celem nadrzędnym jest dążność do właściwego funkcjonowania rynku wewnętrznego w drodze zapewnienia swobodnego przepływu usług społeczeństwa informacyjnego między państwami członkowskimi Unii Europejskiej (art. 1). W art. 2 tejże dyrektywy zawarto definicje legalne, w tym informacji handlowej, usługodawcy, konsumenta. Z punktu widzenia przedmiotowych rozważań szczególne znaczenie ma informacja handlowa, będąca „[…] każdą formą informacji przeznaczoną do promowania, bezpośrednio lub pośrednio, towarów, usług lub wizerunku przedsiębiorstwa, organizacji lub osoby prowadzącej działalność handlową, gospodarczą, rzemieślniczą lub wykonującą zawód regulowany" (art. 2). Z przepisu tego wynika wprost, że możliwe są wszystkie formy, co należy rozumieć jako otwarty katalog. Dyrektywa nie ogranicza żadnej formy, traktując je na równi.

Koordynacja usług społeczeństwa informacyjnego w ramach Wspólnoty Europejskiej stała się nie tylko faktem, ale przede wszystkim koniecznością. Zgodnie z zapisem art. 3 pkt 2 Dyrektywy 2000/31/WE „Państwa Członkowskie nie mogą z powodów wchodzących w zakres koordynowanej dziedziny ograniczać swobodnego przepływu usług społeczeństwa informacyjnego pochodzących z innego Państwa Członkowskiego". Koordynacja ta dotyczy określonego wycinka rzeczywistości społeczno-gospodarczej, to jest handlu elektronicznego. Przy wymianie handlowej konieczna jest komunikacja między stronami umowy, co nie wymaga komentarza. Komunikacja oznacza w tym przypadku przede wszystkim porozumienie co do przedmiotu umowy, czyli usługi. Dyrektywa jednak przewiduje wyjątek od zasady swobodnego przepływu usług, a co za tym idzie – także informacji, w określonych przypadkach, które wskazano w art. 2, w pkt 4. Najprościej rzecz ujmując, dotyczą one: bezpieczeństwa powszechnego; ochrony życia i zdrowia ludzkiego; ochrony porządku publicznego, w tym ścigania przestępstw oraz zapobiegania im; walki z nienawiścią, dyskryminacją rasową i religijną; ochrony godności człowieka; ochrony konsumentów i inwestorów.

Taka regulacja pozwala państwom członkowskim na podejmowanie inicjatyw zmierzających do eliminacji społecznie szkodliwych czy niebezpiecznych działań.

Dyrektywa 2000/31/WE określa także wymogi formalne informacji (art. 5), w tym: nazwę usługodawcy; adres geograficzny siedziby usługodawcy, łącznie z jego adresem poczty elektronicznej, umożliwiającym szybki kontakt oraz bezpośrednie i skuteczne porozumiewanie się; dane rejestrowe, o ile usługodawca podlega wpisowi do rejestru; oraz – jeśli działalność jest uzależniona od uprzednio wydanego zezwolenia – dane o zezwoleniu wraz z danymi organów nadzoru.

W dalszej części dyrektywy zdefiniowano informację handlową (art. 6) oraz umowy zawierane drogą elektroniczną (art. 9 i n.). Zgodnie z przyjętym rozwiązaniem niektóre umowy zostały wyłączone z katalogu umów, jakie mogą być zawarte w drodze elektronicznej. Nie budzi zastrzeżeń zapis o wyłączeniu umów dotyczących przenoszenia praw do nieruchomości, poza umową najmu, która może być zawarta w drodze elektronicznej. Ponadto wyłączono także umowy z dziedziny prawa rodzinnego, spadkowego, poręczenia oraz takich umów, dla których wymagana jest zgoda sądu, władz publicznych lub zawodów związanych z wykonywaniem władzy publicznej. Pomijając szczegóły dotyczące zawierania umów drogą elektroniczną, należy wyraźnie podkreślić, iż istotą wprowadzenia tej możliwości prowadzenia handlu (elektronicznego) jest szybka komunikacja i zrozumiały przekaz informacji. Nie sposób nie zauważyć, że Unia Europejska z jednej strony dąży do ujednolicenia systemu rozwiązań prawnych w państwach członkowskich, do swobody przepływu towarów i usług, swobody przepływu informacji, z drugiej zaś daje tworzącym ją państwom margines swobody w kwestiach istotnych dla porządku publicznego, ochrony i bezpieczeństwa osób i mienia. Pewnym mankamentem jest wielojęzyczność, co – jak nietrudno dostrzec – w niektórych sytuacjach stanowić może istotny problem we właściwej (to jest zrozumiałej) komunikacji między stronami. Nie chodzi przy tym o kontakty oficjalne, konwencyjne, lecz takie, które nie mają takiego przymiotu. Wychodząc naprzeciw temu, wielu usługodawców opracowuje umowy w różnych językach, tak by ich warunki były zrozumiałe dla usługobiorcy (kontrahenta).

Ogólne rozporządzenie o ochronie danych

Kolejnym aktem prawnym istotnym podczas rozważania kwestii społeczeństwa informacyjnego jest Rozporządzenie Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (tak zwane ogólne rozporządzenie o ochronie danych; zob.: Rozporządzenie 2016/679; Fajgielski 2018; Jagielski 2010). Dotyczy ono ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, co jest jednym z najważniejszych praw Karty praw podstawowych Unii Europejskiej (2012) oraz Traktatu o funkcjonowaniu Unii Europejskiej (2012). W art. 4 wskazanego wyżej rozporządzenia zdefiniowano dane osobowe, przez które rozumie się:

> […] informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (Rozporządzenie 2016/679).

Identyfikacja rozumiana jest tu jako tożsamość określonego podmiotu. Rozszerzenie czynników (elementów) identyfikacyjnych w pewnym stopniu stanowi odwołanie do współczesnych możliwości identyfikacji człowieka w perspektywie interdyscyplinarnej nauki. Owa interdyscyplinarność przejawia się w ścisłych związkach nauk penalnych, nauk medycznych, ekonomii, ale też innych, chociażby psychologii czy socjologii. W przywołanym akcie prawnym prawodawca definiuje także inne pojęcia, choćby dane biometryczne, dane genetyczne czy dane dotyczące zdrowia, jak również naruszenie ochrony danych osobowych.

Przy dzisiejszych osiągnięciach technologicznych informacje stanowią cenne źródło wiedzy, w szczególności te, do których dostęp jest prosty i powszechny. Sieć informatyczna pozwala na szybką komunikację, szybkie przekazywanie danych różnego rodzaju, w tym także danych osobowych. Klasycznym przykładem są zbiory danych zwane bazami, w których są gromadzone i przetwarzane choćby dane dotyczące podmiotów gospodarczych, dane o stanie zdrowia w systemach należących do szpitali czy poradni specjalistycznych, a także podstawowej opieki zdrowotnej. Dane osobowe są praktycznie wszędzie – od urzędu stanu cywilnego, w którym rejestruje się urodzenia, zawarcia związków małżeńskich czy zgony, po wszelkiego rodzaju wyszukiwarki systemowe, w których wystarczy wpisać nazwisko, by uzyskać informację, co prawda niekompletną, o konkretnej osobie. Ogólne rozporządzenie o ochronie danych, podobnie jak inne akty prawa Unii Europejskiej, jest elementem wdrażania ujednoliconych przepisów w systemach prawa państw członkowskich. Ochrona informacji o osobie (dane osobowe) stanowi podstawę bezpieczeństwa człowieka w sieci informatycznej. Wszechobecne media społecznościowe stały się nieodłącznym elementem funkcjonowania globalnego społeczeństwa, bez nich trudno sobie wyobrazić współczesną komunikację interpersonalną (Van de Belt i in. 2012; Szczepańczyk 2014; Cyrek 2016; Steculа 2017; Kaleta 2018).

Społeczeństwo XXI wieku przyzwyczaiło się, na swój specyficzny sposób, do życia „w sieci". Niewątpliwie stanowi to znaczne ułatwienie w pracy (obecnie niezwykle częstej w dobie pandemii COVID-19), w kontaktach z innymi ludźmi, ale także w załatwianiu różnych spraw, w tym tych o urzędowym charakterze. Niestety, prócz wymienionych zalet są też negatywne strony cyberprzestrzeni i wszechogarniających sieciowych informacji, w których nie brakuje nieprawdziwych, niczym nieuzasadnionych wiadomości, rewelacji czy doniesień. Informacyjny chaos kreowany przez fake newsy stał się wręcz powszechny. Administratorzy nie nadążają z usuwaniem treści sprzecznych

z przedmiotowym rozporządzeniem. Przetwarzanie danych osobowych, będących informacją o szczególnym charakterze, wymaga zgody osoby. Prawo państw członkowskich, jak i prawo Unii Europejskiej, przewiduje zakaz przetwarzania szczególnej kategorii danych, o których mowa w art. 9 Rozporządzenia 2016/679. Jest to możliwe tylko w określonych przypadkach, wskazanych w tym akcie prawnym. Do tychże przypadków zalicza się między innymi zgodę podmiotu, potrzebę ochrony zdrowia osoby (dane medyczne), realizację orzeczeń sądowych i związanych z tym działań organów ścigania czy przetwarzanie dla celów naukowych. Katalog warunków oczywiście jest szerszy, co wyraźnie wynika z treści ogólnego rozporządzenia o ochronie danych. Warto zaznaczyć, że polskie rozwiązania prawne dotyczące ochrony danych osobowych są zbieżne z postanowieniami prawa Unii Europejskiej (Barta i in. 2011; Litwiński i in. 2018; Hoc i Szewc 2014; Kuczma 2017).

Inne regulacje dotyczące bezpieczeństwa w cyberprzestrzeni

Wśród regulacji w przedmiocie bezpieczeństwa w cyberprzestrzeni na szczególną uwagę zasługuje Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (zob. w bibliografii: Dyrektywa 2016/1148) oraz powiązane z nią dokumenty, a mianowicie:

- Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (zob. Rozporządzenie 2018/151);
- Decyzja wykonawcza Komisji (UE) 2017/179 z dnia 1 lutego 2017 r. ustanawiająca procedury niezbędne do funkcjonowania grupy współpracy zgodnie z art. 11 ust. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (zob. Decyzja 2017/179);
- Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (zob. Komunikat 2017);
- Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (zob. Zalecenie 2017/1584);

- Wspólny komunikat do Parlamentu Europejskiego i Rady – Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej (zob. Wspólny komunikat 2017);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (zob. Rozporządzenie 910/2014);
- Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (zob. Decyzja 2013/488/UE);
- Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (zob. Dyrektywa 2013/40/UE);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (zob. Rozporządzenie 526/2013);
- Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (zob. Wspólny komunikat 2013).

Wybrane zagrożenia

Cyberbezpieczeństwo jest pojęciem, które na stałe wpisało się w systemy bezpieczeństwa wszystkich państw współczesnego świata. Tym samym wpisało się w indywidualne bezpieczeństwo informacji kreowanych przez człowieka. Członkowie społeczeństwa są autorami wszystkich informacji, bez względu na to, jakiej sfery aktywności człowieka informacje te dotyczą. Żadna informacja nie powstaje poza ludzkim umysłem, każda ma określoną treść, określoną intencję. W Sieci występują wszystkie rodzaje informacji, od tych zupełnie neutralnych po takie, które wyczerpują znamiona przestępstw. Wymienione wyżej akty prawne dotyczą szeroko rozumianego bezpieczeństwa w wirtualnej przestrzeni. Monitorowanie Internetu stało się codziennością i narzędziem walki z cyberzagrożeniami. Państwa-członkowie Unii Europejskiej przyjęły także model transgranicznej kontroli w tym względzie. Informacje anonimowe w istocie takimi nie są, bowiem w każdym czasie można zidentyfikować urządzenie, z którego zostały przesłane. Odrębną kwestią jest ustalenie autora przekazu, co zdecydowanie leży w kompetencjach właściwych służb (Lubaszewski 2007; Lipiński i Bernardelli 2018; Nacher 2014; Kosiński 2015; Lach 2011); rola organów ścigania w identyfikacji osoby sprawcy przestępstwa dokonanego w sieci teleinformatycznej jest kluczowa.

Równie ważnym zagadnieniem są działania o znamionach czynów karalnych za pośrednictwem komunikatorów internetowych instalowanych w urządzeniach

mobilnych (telefony, tablety, laptopy). Swoboda komunikowania się, w tym zamieszczania informacji w różnych miejscach w Sieci, podlega swoistej kontroli, monitorowaniu, co wskazano powyżej. Pozwala to na identyfikację niebezpieczeństwa i podjęcie działań eliminujących. Rozmiary naruszeń prawa w tym względzie były asumptem do powstania Komunikatu Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości (zob. Komunikat 2007). Z treści tego dokumentu, niebędącego aktem o normatywnym charakterze, co należy zaznaczyć, wynika ogólna polityka, której celem jest poprawa koordynacji walki z cyberprzestępczością. Owo zintensyfikowanie działań ma nie tylko charakter o zasięgu europejskim, ale także międzynarodowym, jak i krajowym. Działania te obejmują między innymi: współpracę z innymi państwami (niebędącymi państwami członkowskimi Unii Europejskiej), działania informacyjne o zagrożeniach w wirtualnej przestrzeni, ujednolicenie prawa i definicji dotyczących przedmiotowej sfery. Rezultatem publikacji wspomnianego komunikatu są przede wszystkim dwie dyrektywy, a mianowicie: Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (zob. Dyrektywa 2011/93/UE) oraz wspomniana już Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW.

Pierwsza z wymienionych regulacji, Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r., dotyczy w najszerszym znaczeniu ochrony jednostki ludzkiej przed nadużyciami w sferze seksualnej. Szczególne znaczenie dla przedmiotowych rozważań ma treść jej art. 6. Przepis ten stanowi o karalności nagabywania dzieci do celów seksualnych. Określenie „nagabywanie" należy rozumieć jako każdą formę indywidualnego kontaktu werbalnego, nie tylko bezpośredniego, ale także za pośrednictwem jakiegokolwiek środka przekazu, w tym sieci teleinformatycznych. Tak szeroka interpretacja pojęcia dozwala na kwalifikowanie każdego zachowania, którego celem jest nawiązanie kontaktu osoby dorosłej z osobą małoletnią w celach seksualnych (Carr 2005; Gruchoła 2011; Mierzwińska-Lorencka 2012; Tomkiewicz 2012; Sikorski 2018; Badźmirowska-Masłowska 2013; Wróbel-Delegacz 2018).

Statystyki policyjne państw Unii Europejskiej, jak i innych państw świata dowodzą, że mimo szeroko zakrojonych działań prewencyjnych w zakresie zapobiegania przestępczości seksualnej obserwuje się tendencję wzrostową w tym względzie, w szczególności tej, w której pokrzywdzonymi są osoby małoletnie. Pedofilia znana jest ludzkości od wieków i występuje, podobnie jak dawniej, w każdym społeczeństwie świata. Internet otworzył nowe możliwości w komunikacji między ludźmi. Jak każda innowacja, ma też negatywne strony, w tym anonimowość, dzięki której wszystko staje się w pewnym sensie łatwiejsze. Owa łatwość sprawia, że człowiek dorosły w kilka sekund staje się nastolatkiem, a ten ostatni raptem starzeje się, zawyżając metrykalny wiek, by uzyskać dostęp do stron przeznaczonych dla osób pełnoletnich. Cyfrowe społeczeństwo,

bo tak można określić populację XXI wieku, jest na swój sposób uzależnione od kontaktów za pośrednictwem Internetu. Większość ludzi, bez względu na wiek, korzysta z mediów społecznościowych. Komunikatory, czaty czy fora są miejscem spotkań, wymiany poglądów, ale też zawierania znajomości. Zamieszczanie fotografii i publikowanie informacji o wydarzeniach natury prywatnej stało się normą. Fałszywa tożsamość umożliwia kreowanie siebie samego w sposób inny niż w rzeczywistości. W taki sposób, prymitywny i prosty, pedofile poszukują dzieci, które, z reguły nieświadome zagrożenia, dają się zwieść obietnicom przyjaźni i zrozumienia (Baker i Duncan 1985; Arnaldo 2001; Beech i in. 2008; Balfe i in. 2015; Webb i in. 2008; McCarthy 2010). Ustawodawstwa poszczególnych państw szczególną ochroną obejmują osoby małoletnie przed każdą formą przemocy, w tym przed wykorzystywaniem seksualnym. Wyżej wymienione regulacje prawa unijnego są wyrazem wspólnej polityki prawnej w przedmiocie ochrony dzieci i młodzieży.

W innej regulacji prawnej Unii Europejskiej, jaką jest Dyrektywa Parlamentu Europejskiego i Rady 2011/36/UE z dnia 5 kwietnia 2011 r. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępująca decyzję ramową Rady 2002/629/WSiSW (zob. Dyrektywa 2011/36/UE), przepis art. 15 traktuje o ochronie dzieci będących ofiarami przestępstwa handlu ludźmi. Pomijając kwestie natury prawnej, nie sposób nie dostrzec związku pomiędzy przestępnym procederem a komunikacją interpersonalną. By doszło do handlu, jakiegokolwiek, muszą być dwie strony – sprzedający i kupujący. Niestety, coraz częściej to właśnie Internet staje się narzędziem służącym do szybkiej wymiany informacji. Oczywiste jest, że tego rodzaju komunikowanie przybiera formy ukryte, co należy rozumieć jako swoisty kod językowy. Przestępstwo handlu ludźmi jest ścigane w każdym systemie prawnym, co nie budzi wątpliwości. Ma charakter ponadpaństwowy, co oznacza, że społeczność międzynarodowa w sposób jednoznaczny podejmuje działania natury prawnej zmierzające tak do zapobiegania, jak i zwalczania tego rodzaju przestępczości (Jasiński i Karsznicki 2003; Warylewski 2000; Sakowicz 2006). Handel ludźmi ma różne oblicza. W sieci wirtualnej pojawiają się ogłoszenia rekrutujące do wszelkiego rodzaju pracy, jak też składane są propozycje współpracy czy wymiany. Treść tychże jest tak skomponowana, że nie budzi niepokoju, a oferowane warunki pracy czy współpracy, jak i wymiany rozumiane są jako atrakcyjne (Andrees 2006; Karsznicki 2009; Jasiński i Karsznicki 2003; Radoniewicz 2011; Fehér 1996).

Komunikowanie się w XXI wieku za pomocą Internetu nie przedstawia żadnych trudności nie tylko w języku podstawowym podmiotu (ojczystym), ale także w innych, nieznanych. Służą temu narzędzia cyfrowe, takie jak translatory językowe. Co prawda nie są doskonałe, ale tłumaczenie z jednego języka na inny pozwala na ogólne zrozumienie treści. Niejednokrotnie pomaga to w popełnianiu nadużyć, w tym także przestępstwa, jakim jest handel ludźmi, i stanowi dla sprawcy przestępstwa podstawowe narzędzie służące jego realizacji. Internetowe ogłoszenia o rekrutacji do prostych zajęć, niewymagających znajomości języka, wysoko wynagradzanych przy braku innych wymagań

są charakterystyczne dla ukrytego celu ogłoszeniodawcy. Niestety, takie ogłoszenia cieszą się znacznym zainteresowaniem osób szukających zatrudnienia nie tylko w Polsce, ale także za granicą.

Podsumowanie

Społeczeństwo XXI wieku jest nie bez powodu określane jako informacyjne. We współczesnej rzeczywistości nie wymaga uzasadnienia teza, że cyfryzacja odgrywa znaczną rolę. Wraz z postępem w dziedzinie informatyki koniecznością stały się regulacje natury prawnej. Prawo krajowe poszczególnych państw zawiera stosowne rozwiązania w tym zakresie. Unia Europejska, dostrzegając potrzebę wspólnej polityki także w tym względzie, podjęła starania w kierunku ujednolicenia warunków dostępności do otwartego Internetu, czego wyrazem jest Rozporządzenie Parlamentu Europejskiego i Rady Europy (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii (zob. Rozporządzenie 2015/2120). W treści tego rozporządzenia, w punkcie pierwszym, wskazano:

> Niniejsze rozporządzenie ma na celu ustanowienie wspólnych zasad mających na celu zagwarantowanie równego i niedyskryminacyjnego traktowania transmisji danych w ramach świadczenia usług dostępu do internetu oraz związanych z tym praw użytkowników końcowych. Ma ono na celu ochronę użytkowników końcowych oraz równocześnie zagwarantowanie nieprzerwanego funkcjonowania ekosystemu internetowego stanowiącego siłę napędową innowacji. Reformy w dziedzinie roamingu powinny zachęcić użytkowników końcowych do swobodnego korzystania z usług łączności elektronicznej podczas podróży w Unii oraz z czasem stać się czynnikiem ujednolicania cen i innych warunków w Unii (Rozporządzenie 2015/2120).

Wolny, otwarty dostęp do Internetu jest prawem, co podkreślono w zacytowanym powyżej zapisie, na państwa członkowskie zaś nałożono obowiązek polegający na umożliwieniu dostępu do Sieci na takich samych zasadach. W tym akcie prawnym zasadnicze regulacje dotyczą niedyskryminacyjnego dostępu oraz cen detalicznych usług ogólnounijnego roamingu, co przekłada się na komunikację między członkami społeczeństwa. Nie zawsze komunikacja ta służy dobrym celom, niekiedy ma inny charakter, w tym też przestępczy. Internet w wymiarze medium komunikacyjnego nie jest jednolity. W literaturze przedmiotu wymienia się trzy typy w tym względzie, a mianowicie typ: konwersacyjny, korespondencyjny oraz hipertekstowy (Grzenia 2006: 43). Wszystkie wymienione typy komunikacji internetowej mogą służyć dobrym, pozytywnym celom, jak i tym społecznie niepożądanym, nagannym i karygodnym.

Agnieszka Szewczyk (2011) akcentuje popularność komunikacji internetowej, podkreślając jej specyficzne formy, w tym także niewerbalne. Słusznie zauważa Stanisław Juszczyk (2011), że Internet stał się nową przestrzenią społeczną, w której współczesny człowiek realizuje swoje potrzeby. Potrzeby te, jak wiadomo, są różne, jak choćby potrzeba akceptacji, zrozumienia, ale też poszerzania wiedzy oraz zainteresowań. Wszystko to jest możliwe w Sieci, bez potrzeby wychodzenia z domu. Internet stał się dzisiejszym oknem na świat, ale też i drzwiami, przez które można się dostać do bibliotek, uczelni, na sale wykładowe, nie mówiąc już o scenach teatrów, wnętrzach galerii sztuki czy muzeów:

> Cybersztuka, stanowiąc ekspresję cyberkultury, może być jednocześnie interpretowana jako awangarda technospołeczeństwa, które wypowiada się w sposób najpełniejszy, wykorzystując nowe media cyfrowe i technologie komunikacyjne. Zasadne już jest mówienie o pewnym przesunięciu w stronę nowej formacji kulturowej, co niektórzy nazywają epoką postmediów. […] Cybersztuka i cyberkultura oparte są zatem na grze i kombinacji wielu mediów digitalnych, odbywającej się przy wszechstronnym wykorzystaniu komputera, który uznać można za uniwersalną maszynę, narzędzie i zarazem medium postmedialne (Zawojski 2010: 149).

Medium bez granic, jakim jest Internet, podobnie jak wszystko, co nas otacza, podlega prawom współczesnych państw. Niektóre z regulacji prawnych w tym zakresie zostały w bardzo zwięzły sposób przywołane w niniejszej próbie spojrzenia na społeczeństwo informacyjne, które równie dobrze można określić jako cyfrowe. Nie bez powodu Agata Rutkiewicz (2018: 91), powołując się na innych autorów, pisze o „sieciakach", nowym pokoleniu, które wychowało się w otoczeniu komputerów i Internetu. To pokolenie i następne stworzą społeczeństwo, które nie obejdzie się bez technologii cyfrowej. Życie w przestrzeni realnej podlega regulacjom prawnym, tak samo jak jego inny, cyfrowy wymiar.

Bibliografia

Akty normatywne i inne dokumenty

Decyzja 2013/488/UE. 2013. Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2013/488/UE). [Online]. Dziennik Urzędowy Unii Europejskiej, L 274/1. Dostęp: https://eur-lex.europa.eu/legal-content/pl/TXT/PDF/?uri=CELEX:32013D0488&from=EN [6.09.2020].

Decyzja 2017/179. 2017. Decyzja wykonawcza Komisji (UE) 2017/179 z dnia 1 lutego 2017 r. ustanawiająca procedury niezbędne do funkcjonowania grupy współpracy zgodnie z art. 11 ust. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dziennik Urzędowy Unii Europejskiej, L 28/73. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32017D0179 [6.09.2020].

Dyrektywa 2000/31/WE. 2000. Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego. Dziennik Urzędowy Wspólnot Europejskich, L 178/1. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32000L0031 [6.09.2020].

Dyrektywa 2011/36/UE. 2011. Dyrektywa Parlamentu Europejskiego i Rady 2011/36/UE z dnia 5 kwietnia 2011 r. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępująca decyzję ramową Rady 2002/629/WSiSW. Dziennik Urzędowy Unii Europejskiej, L 101/1. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32011L0036 [6.09.2020].

Dyrektywa 2011/93/UE. 2011. Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW. Dziennik Urzędowy Unii Europejskiej, L 335/1. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32011L0093 [6.09.2020].

Dyrektywa 2013/40/UE. 2013. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW. Dziennik Urzędowy Unii Europejskiej, L 218/8. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32013L0040 [6.09.2020].

Dyrektywa 2016/1148. 2016. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dziennik Urzędowy Unii Europejskiej, L 194/1. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148 [6.09.2020].

Karta praw podstawowych UE. 2012. Karta praw podstawowych Unii Europejskiej. Dziennik Urzędowy Unii Europejskiej, C 326/391. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A12012P%2FTXT [6.09.2020].

Komunikat. 2007. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 [6.09.2020].

Komunikat. 2017. Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52017DC0476 [6.09.2020].

Rozporządzenie 526/2013. 2013. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004. Dziennik Urzędowy Unii Europejskiej, L 165/41. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32013R0526 [6.09.2020].

Rozporządzenie 910/2014. 2014. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE. Dziennik Urzędowy Unii Europejskiej, L 257/73. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910 [6.09.2020].

Rozporządzenie 2015/2120. 2015. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii. Dziennik Urzędowy Unii Europejskiej, L 310/1. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32015R2120#document1 [6.09.2020].

Rozporządzenie 2016/679. 2016. Rozporządzenie Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 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. Dziennik Urzędowy Unii Europejskiej, L 119/1. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679 [6.09.2020].

Rozporządzenie 2018/151. 2018. Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego

i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ. Dziennik Urzędowy Unii Europejskiej, L 26/48. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32018R0151 [6.09.2020].

Traktat o funkcjonowaniu UE. 2012. Traktat o funkcjonowaniu Unii Europejskiej. Dziennik Urzędowy Unii Europejskiej, C 326/49. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/pl/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN [6.09.2020].

Wspólny komunikat. 2013. Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013JC0001 [6.09.2020].

Wspólny komunikat. 2017. Wspólny komunikat do Parlamentu Europejskiego i Rady – Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017JC0450 [6.09.2020].

Zalecenie 2017/1584. 2017. Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę. Dziennik Urzędowy Unii Europejskiej, L 239/36. [Online]. EUR-Lex. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32017H1584 [6.09.2020].

Opracowania

Andrees, Beate. 2006. Praca przymusowa jako forma handlu ludźmi. W: Lasocik, Zbigniew (red.). *Handel ludźmi. Zapobieganie i ściganie*. Warszawa: Instytut Prawa Sądowego i Resocjalizacji Uniwersytetu Warszawskiego, s. 191–202.

Arnaldo, Carlos A. 2001. *Child Abuse on the Internet: Ending the Silence*. New York: Berghahn Books.

Babik, Wiesław, i Rykaczewska-Wiorogórska, Bogumiła. 1998. Telematyka – koncepcja i wykorzystanie w społeczeństwie informacyjnym. *Zagadnienia Informacji Naukowej*, 1 (71), s. 64–73.

Badźmirowska-Masłowska, Katarzyna. 2013. Ochrona małoletnich w środowisku mediów audiowizualnych, Internetu i innych usług on-line przed współczesnymi zagrożeniami w świetle dokumentów Rady Europy. Wybrane aspekty prawne. *Journal of Modern Science*, 16 (1), s. 59–100.

Baker, Anthony W., i Duncan, Sylvia P. 1985 Child Sexual Abuse: A Study of Prevalence in Great Britain. *Child Abuse and Neglect*, 4 (9), s. 457–467.

Balfe, Myles; Gallagher, Bernard; Masson, Helen; Balfe, Shane; Brugha, Ruairi; i Hackett, Simon. 2015. Internet Child Sex Offenders' Concerns about Online Security and Their Use of Identity Protection Technologies: A Review. *Child Abuse Review*, 6 (24), s. 427–439.

Barta, Janusz; Fajgielski, Paweł; i Markiewicz, Ryszard. 2011. *Ochrona danych osobowych: komentarz*. Warszawa: Wolters Kluwer.

Beech, Anthony R.; Elliott, Ian A.; Birgden, Astrid; i Findlater, Donald. 2008. The Internet and Child Sexual Offending: A Criminological Review. *Aggression and Violent Behavior*, 13 (3), s. 216–228.

Borowiec, Monika. 2009. Rola edukacji w kształtowaniu społeczeństwa informacyjnego. *Przedsiębiorczość – Edukacja*, 5, s. 37–47.

Carr, John. 2005. Internet a wykorzystywanie seksualne dzieci i pornografia dziecięca. Tłum. Agnieszka Nowak. *Dziecko Krzywdzone. Teoria, badania, praktyka*, 4 (4), s. 1–17.

Castells, Manuel. 1996. *The Rise of the Network Society: The Information Age*. Oxford: Blackwell.

Cyrek, Barbara. 2016. Media społecznościowe – nowa przestrzeń nauki. *Kognitywistyka i Media w Edukacji*, 2, s. 45–56.

Fajgielski, Paweł. 2018. *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wolters Kluwer.

Fehér, Lenke. 1996. *Frauenhandel*. Wien: SWA-Studienarbeit.

Goban-Klas, Tomasz, i Sienkiewicz, Piotr. 1999. *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Kraków: Wydawnictwo Postępu Telekomunikacji.
Golka, Marian. 2005. Czym jest społeczeństwo informacyjne? *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 4 (67), s. 253–265.
Gruchoła, Małgorzata. 2011. Ochrona małoletnich internautów jako zadanie i wyzwanie dla rodziny w państwach Unii Europejskiej. *Studia Gdańskie*, 28, s. 229–256.
Grzenia, Jan. 2006. *Komunikacja językowa w Internecie*. Warszawa: PWN.
Hoc, Stanisław, i Szewc, Tomasz. 2014. *Ochrona danych osobowych i informacji niejawnych*. Warszawa: CH Beck.
Jagielski, Mariusz. 2010. *Prawo do ochrony danych osobowych. Standardy europejskie*. Warszawa: Wolters Kluwer.
Jasiński, Filip, i Karsznicki, Krzysztof. 2003. Walka z handlem ludźmi z perspektywy Unii Europejskiej. *Państwo i Prawo*, 7, s. 84–96.
Juszczyk, Stanisław. 2011. Internet – współczesne medium komunikacji społecznej. *Edukacja i Dialog*, 5, s. 42–46.
Kaleta, Mateusz. 2018. Wykorzystanie mediów społecznych w procesach rekrutacji pracowników. *Intercathedra*, 2 (35), s. 143–150.
Karsznicki, Krzysztof. 2009. Analiza polskiego prawa pod kątem efektywności ścigania handlu ludźmi do pracy przymusowej. *Prokuratura i Prawo*, 7–8, s. 39–47.
Kosiński, Jerzy. 2015. *Paradygmaty cyberprzestępczości*. Warszawa: Difin.
Kuczma, Emilia. 2017. Cyber-dane osobowe jako dane osobowe nowej generacji. *Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z Nauk Społecznych*, 10, s. 61–73.
Lach, Arkadiusz. 2011. Przeszukanie na odległość systemu informatycznego. *Prokuratura i Prawo*, 9, s. 67–79.
Lipiński, Łukasz, i Bernardelli, Michał. 2018. Anonimowość w Internecie – identyfikacja płci użytkowników na podstawie historii odwiedzanych stron internetowych. *Collegium of Economic Analysis Annals*, 53, s. 147–162.
Litwiński, Paweł; Barta, Paweł; i Dörre-Kolasa, Dominika. 2018. *Ustawa o ochronie danych osobowych: komentarz*. Warszawa: CH Beck.
Lubaszewski, Wiesław. 2007. *Anonimowość w Internecie*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
McCarthy, Jennifer A. 2010. Internet Sexual Activity: A Comparison between Contact and Non-Contact Child Pornography Offenders. *Journal of Sexual Aggression*, 2 (16), s. 181–195.
Mierzwińska-Lorencka, Joanna. 2012. *Karnoprawna ochrona dziecka przed wykorzystaniem seksualnym*. Warszawa: Wolters Kluwer.
Muraszkiewicz, Mieczysław. 2004. Społeczeństwo informacyjne i praca. W: Sosińska-Kalata, Barbara; Materska, Katarzyna; i Gliński, Wiesław (red.). *Społeczeństwo informacyjne i jego technologie*. Warszawa: Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, s. 13–28.
Nacher, Anna. 2014. Teletechnologie, linie i cyfrowe ślady. Od sytuacjonizmu i land artu do sztuki mediów lokacyjnych. *Sztuka i Dokumentacja*, 11, s. 71–78.
Radoniewicz, Filip. 2011. Przestępstwo handlu ludźmi. *Prokuratura i Prawo*, 10, s. 134–155.
Rutkiewicz, Agata. 2018. Cyfryzacja w edukacji przedszkolnej. Cz. 1. *Refleksja*, 4, s. 88–93.
Sakowicz, Andrzej. 2006. Przestępstwo handlu ludźmi z perspektywy regulacji międzynarodowych. *Prokuratura i Prawo*, 3, s. 52–69.
Sikorski, Przemysław. 2018. Prawnokarne i prawnomiędzynarodowe regulacje związane z ochroną przed pedofilią w cyberprzestrzeni. *Teka Komisji Politologii i Stosunków Międzynarodowych*, 2 (13), s. 177–185.
Stecuła, Kinga. 2017. Zagrożenia związane z postępem techniki na przykładzie Facebooka. *Systemy Wspomagania w Inżynierii Produkcji*, 6, s. 223–232.
Szczepańczyk, Maciej. 2014. Innowacyjne sposoby wykorzystania mediów społecznościowych w komunikacji wewnętrznej i zewnętrznej organizacji. *Studia Ekonomiczne*, 183, cz. 2, s. 185–196.
Szewczyk, Agnieszka. 2011. Popularność form komunikacji internetowej. *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica*, 27 (643), s. 159–179.

Tomkiewicz, Małgorzata. 2012. Child grooming i sexting. Dziecko jako ofiara i sprawca nadużyć seksualnych w cyberprzestrzeni – wymiar prawnokarny zjawiska. *Prace Instytutu Profilaktyki Społecznej i Resocjalizacji*, 20, s. 49–65.
Van de Belt, Tom H.; Berben, Sivera A.; Samsom, Melvin; Engelen, Lucien J.; Schoonhoven, Lisette. 2012. Use of Social Media by Western European Hospitals: Longitudinal Study. *Journal of Medical Internet Research*, 3 (14), s. 1–9.
Warylewski, Jarosław. 2000. Karalność handlu żywym towarem w świetle nowego kodeksu karnego. *Palestra*, 7–8, s. 43–57.
Webb, Liane; Craissati, Jackie; i Keen, Sarah. 2008. Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters. *Sexual Abuse: A Journal of Research and Treatment*, 4 (19), s. 449–465.
Wierzbołowski, Józef. 2006. Społeczeństwo informacyjne a integracja Polski w ramach Unii Europejskiej. *Ekonomista*, 1, s. 27–52.
Wróbel-Delegacz, Wioletta. 2018. Grooming: zagrożenie dla bezpieczeństwa dzieci. *Doctrina. Studia społeczno-polityczne*, 15, s. 329–350.
Zawojski, Piotr. 2010. *Cyberkultura. Syntopia sztuki, nauki i technologii*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Netografia

Goliński, Michał. 2005. Społeczeństwo informacyjne – często (nie)zadawane pytania. *E-mentor*, 2 (9). [Online]. E-mentor. Dostęp: http://www.e-mentor.edu.pl/artykul/index/numer/9/id/130 [6.09.2020].

Streszczenie

Celem autorów artykułu jest przybliżenie problematyki funkcjonowania społeczeństwa informacyjnego w ramach obowiązujących regulacji prawnych Unii Europejskiej. Autorzy odnoszą się do najważniejszych aktów prawnych UE, takich jak rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej, dotyczących między innymi dostępu do otwartego Internetu oraz ochrony przed wykorzystywaniem danych osobowych. Ponadto wskazują na ważne zagrożenia płynące z funkcjonowania społeczeństwa informacyjnego, takie jak wykorzystywanie dzieci w celach seksualnych, pornografia dziecięca czy zjawisko handlu ludźmi.

Information Society in the Perspective of Selected Legal Acts of the European Union

Summary

The aim of the article is to present the issues of the information society functioning under the applicable legal regulations of the European Union. For this purpose, the authors refer to the most important legal acts of the EU, such as regulations of the European Parliament and of the Council of Europe concerning access to the open Internet and protection against the use of personal data. Moreover, the authors point to important threats resulting from the functioning of the information society, such as the exploitation of children for sexual purposes, child pornography and the phenomenon of human trafficking.