# NOWE TECHNOLOGIE
## – współczesne wyzwania w obszarze
# prawa i bezpieczeństwa

Redakcja naukowa
**Marta POMYKAŁA**
**Marcin MERKWA**

OFICYNA
WYDAWNICZA
POLITECHNIKI RZESZOWSKIEJ

Wydano za zgodą Rektora

R e c e n z e n t
dr hab. Justyna LIPIŃSKA, prof. ASzWoj

R e d a k t o r  n a c z e l n y
Wydawnictw Politechniki Rzeszowskiej
dr hab. inż. Lesław GNIEWEK, prof. PRz

R e d a k t o r
Piotr CYREK

S k ł a d  i  ł a m a n i e
Mariusz TENDERA

P r o j e k t  o k ł a d k i
Joanna MIKUŁA

*cyberbezpieczeństwo, informatyzacja, nowoczesne technologie*
*prawo w Internecie, systemy informatyczne*

*Cybersecurity, Computerization, Modern technologies*
*Law on the Internet, IT systems*



ISBN 978-83-7934-447-5
e-ISBN 978-83-7934-470-3

Oficyna Wydawnicza Politechniki Rzeszowskiej
al. Powstańców Warszawy 12, 35-959 Rzeszów

Ark. wyd. 12,36. Ark. druk. 12,75.
Oddano do druku w czerwcu 2020 r. Wydrukowano w grudniu 2020 r.
Drukarnia Oficyny Wydawniczej, al. Powstańców Warszawy 12, 35-959 Rzeszów
Zam. nr 95/20

# SPIS TREŚCI

# WPROWADZENIE

Truizmem jest stwierdzenie, iż niemający precedensu w historii rozwój technologiczny, którego jesteśmy świadkami w ciągu ostatnich lat, wpłynął i wciąż wpływa na każdy aspekt naszego życia. Choć na temat, jak złożony jest to proces, jak zmieniał poszczególne obszary ludzkiej działalności, jak pod jego wpływem powstawały nowe i odchodziły do historii stare dziedziny gospodarki, napisano już bardzo wiele, warto jednak zauważyć, że problematyka prawa, a zarazem bezpieczeństwa, w sposób szczególny związana jest z zagadnieniem rozwoju techniki.

Wiąże się to przede wszystkim z inflacją prawa, z coraz większym skomplikowaniem systemów normatywnych, czego jedną z przyczyn jest bez wątpienia zmieniająca się rzeczywistość społeczna i postęp naukowy. Prawo cechuje również względna stabilność, której efektem może być pogłębiająca się przepaść pomiędzy regulacjami przyjmowanymi przez współczesne państwa, a zmieniającym się szybko i nieznającym granic światem technologii. Widzimy więc, że prawo jako system regulujący złożoną rzeczywistość w sposób możliwie stabilny, kształtuje rzeczywistość pozaprawną, jak i jest przez nią kształtowane.

Takie spojrzenie na prawo pozwala dostrzec szczególną rolę, którą ono pełni. Prawo jawić się więc może jako swoisty pomost pomiędzy rzeczywistością odkryć naukowych czy nowych rozwiązań technologicznych a światem wartości. I paradoksalnie to właśnie w dobie technologii ta rola wydaje się kluczowa. Niczym nieograniczony postęp technologiczny przestał być bowiem postrzegany jako moralnie obojętny fakt. Stał się procesem, który ze względu na swoje konsekwencje wymaga – i to coraz szerszej – regulacji. Widzimy to w szczególności w tych obszarach, w których wpływ technologii jest najbardziej dostrzegalny.

W niniejszej publikacji zawarte są próby ukazania wybranych zagadnień obrazujących wpływ technologii na prawo i bezpieczeństwo. Ze względu na fakt, iż temat podejmowany w tym miejscu jest niezwykle rozległy, wybór zagadnień musiał być arbitralny i stanowi jedynie przyczynek do bardziej pogłębionych studiów. Zwrócić należy również uwagę na fakt, że autorami tekstów zawartych w tej książce, są zarówno doświadczeni pracownicy naukowi, jak i studenci (przede wszystkim kierunku bezpieczeństwo wewnętrzne na Wydziale Zarządzania Politechniki Rzeszowskiej). Jednakże wydaje się, że wspomniane wyżej cechy publikacji stanowią też jej największą zaletę – pozwoliły bowiem na ukazanie wybranych problemów, które naszkicują Czytelnikowi kilka istotnych zagadnień z bardzo różnych perspektyw.

W początkowych tekstach podjęta zastała próba nakreślenia kluczowych wyzwań, jakie postęp technologiczny kreuje w obszarze prawa. Ukazane zostały m.in.

zagadnienia z zakresu prawa autorskiego, zamówień publicznych czy prawa konstytucyjnego, zwrócono również uwagę na wpływ nowych technologii na koncepcję praw człowieka. Dalej – we fragmencie poświęconym bezpieczeństwu podjęto próbę nakreślenia nowych rodzajów zagrożeń dla bezpieczeństwa i porządku publicznego w obszarze cyberprzestępczości. Rozważania kolejnych rozdziałów poświęcone zostały skimmingowi, stalkingowi, wyłudzeniom dokonywanym za pośrednictwem portali społecznościowych, a także inwigilacji. Osobne materiały poświęcono również Krajowemu Systemowi Cyberbezpieczeństwa oraz porównaniu zasad odpowiedzialności karnej za cyberprzestępstwa w Polsce, Wielkiej Brytanii i Stanach Zjednoczonych.

*Marta Pomykała*
*Marcin Merkwa*

# NOWE TECHNOLOGIE A PRAWO

# PRAWNE ASPEKTY LINKOWANIA UTWORÓW

(*Marta Pomykała*)

Wraz z rozwojem Internetu nastąpił rozwój specyficznych narzędzi technicznych, które służą do udostępniania różnorodnych treści za pośrednictwem sieci. Charakterystyczną formą pozwalającą na dość szerokie i łatwe korzystanie z materiałów umieszczonych w Internecie są linki. Stosowanie linków znacznie upraszcza i przyspiesza przeszukiwanie materiałów w sieci; dzięki nim możliwe jest bowiem bezpośrednie przenoszenie się z jednej strony internetowej do szeregu kolejnych stron z zasobami informacyjnymi. Przenoszenie się poprzez system linków pozwala użytkownikowi pominąć żmudny i często czasochłonny proces wyszukiwania informacji źródłowych, gdyż już sam link stanowi skrót tej ścieżki. Linkiem mogą być połączone zarówno niezależne witryny internetowe, jak też różne strony tego samego serwisu. W wielu przypadkach linki prowadzą do zasobów informacyjnych chronionych prawem autorskim, dla których istnieją ograniczenia rozpowszechniania.

Link określa się także jako odesłanie internetowe, odnośnik albo hiperłącze. Jest to odwołanie do innego dokumentu lub innego miejsca w danym dokumencie, umożliwia wyświetlenie docelowej informacji poprzez proste kliknięcie w niego lub najechanie kursorem[1]. Od strony technicznej link wykorzystuje protokół http lub https. Może on pojawiać się w postaci adresu strony docelowej[2] albo ukrywać się pod określoną nazwą[3]. Częściej jako linki stosowane są różnorodne nazwy i oznaczenia, a dopiero pod nimi ukrywają się adresy internetowe. Linki tego typu stanowią elementarną część tekstu, są też bardziej naturalne i intuicyjne.

Linki są wyjątkowo popularnym elementem komunikowania się w sieci. Można nawet twierdzić, że są istotą komunikacji internetowej. Poprzez proste kliknięcie, a czasem tyko poprzez najechanie kursorem, pozwalają przenieść się bezpośrednio z przeglądanej strony do innej witryny internetowej lub jej wewnętrznej podstrony. Możliwe jest również przekierowanie od razu do konkretnego utworu (np. artykułu, utwory muzycznego), a nawet automatyczne rozpoczęcie pobierania tego utworu na dysk twardy komputera. Linkowanie ogranicza podejmowanie jakichkolwiek czynności wyszukiwawczych przez internautę,

---

[1] https://pl.wikipedia.org/wiki/Hiperłącze (dostęp: 20.09.2020 r.).

[2] Jest to czysty link, który pojawia się w formie adresu URL, czyli takiego adresu, który znajdujemy w pasku przeglądarki.

[3] W tym przypadku linkiem jest sam tekst, w który należy kliknąć w celu przekierowania do innej strony.

znacznie przyspiesza proces wyszukiwania informacji i upraszcza zapoznanie się z nią[4].

Linki pełnią wiele szczegółowych funkcji. Zasadniczą funkcją linka jest z pewnością jego funkcja techniczna, umożliwiająca faktyczne spięcie ze sobą dwóch różnych miejsc w Internecie. Z tej funkcji bezpośrednio wypływa jednak druga, polegająca na ułatwieniu komunikacji. Linkowanie stron znacznie przyspiesza proces rozpowszechniania informacji, zapewniając natychmiastowy dostęp do nich. Można także mówić o funkcji uwiarygadniającej, jeżeli połączenia do strony prowadzą z miejsc pewnych i sprawdzonych, co stanowi przekonującą wskazówkę o prawdziwości danych zamieszczonych na stronie. Natomiast funkcja pozycjonująca związana jest z budowaniem odpowiedniej pozycji strony w przeglądarkach internetowych. Trudno dziś już wyobrazić sobie informację internetową bez linkowania[5].

W praktyce stosowane są także różne rodzaje linków. Najczęściej rozróżnia się linki proste od tzw. linków głębokich. Pierwsze z nich oznaczają jedynie umieszczenie adresu innej strony internetowej w tekście. Takie linki można porównać do umieszczenia informacji o źródle, pełnią one bowiem identyczną rolę jak bibliografia w tekście drukowanym. Dodatkowo jednak link taki może pełnić funkcję nawigacyjną pomiędzy stronami internetowymi, może bowiem – po kliknięciu – przenosić użytkownika bezpośrednio do innych serwisów lub innych stron. Zwykle jednak chodzi o stronę główną lub początkową danego serwisu.

Linki głębokie (*deep links*) także przenoszą do innych witryn, lecz przekierowanie następuje nie do strony głównej jakiegoś serwisu, ale do jednej z jego wewnętrznych podstron. Klikając w taki link użytkownik przenosi się bezpośrednio do plików, materiałów, czy dokumentów zamieszczonych wewnątrz serwisu z całkowitym pominięciem strony głównej tego serwisu. Niektórzy użytkownicy wyraźnie wskazują, że nie godzą się na taką formę linkowania, uzasadniając że narusza to ich interesy, stanowiąc przejaw nieuczciwej konkurencji lub naruszając prawa autorskie. Faktem jest, że przechodząc do wewnętrznych stron serwisu z ominięciem jego strony głównej, następuje również ominięcie reklam i materiałów promocyjnych tam umieszczonych, a to rzeczywiście może wpływać na zmniejszenie zysków właściciela serwisu[6].

Bardziej skomplikowaną formą linkowania są linki w ramkach (*framed links*, framing). Wyświetlają się one jako dodatkowa ramka obejmująca treść strony, do

---

[4] Zob.: Ł. Maryniak, *Zakazane linkowanie?*, https://www.pwi.us.edu.pl/kategorie/prawo-technologii-i-internetu/245-zakazane-linkowanie (dostęp: 20.09.2020 r.).

[5] *Co to jest link building? Kilka słów o linkowaniu,* cz. 1, https://delante.pl/co-to-jest-link-building-kilka-slow-o-linkowaniu-cz-1-vlog-robie-seo-12/ (dostęp: 20.09.2020 r.)

[6] W. Szpringer, *Linking, framing, meta-tagi (perspektywa konkurencji),* http://vagla.pl/skrypts/w_szpringer_linking_framing.pdf (dostęp: 20.09.2020 r.).
S. Żyrek, *Zamieszczanie na stronach internetowych hiperłączy umożliwiających uzyskanie dostępu do utworów chronionych prawem autorskim* – wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.02.2014 r., C-466/12, Nils Svensson i in. przeciwko Retriever Sverige AB, „Europejski Przegląd Sądowy" 2019, nr 3, s. 49.

której prowadzi odesłanie. Ramka wprowadza podział witryny na widoczne na ekranie elementy, oddziela też treść witryny od części pochodzącej z podlinkowanej strony. Charakterystyczne dla tej formy linkowania jest to, że podlinkowana strona, a zwykle tylko jej fragment, jest widoczna na stronie linkującej. Użytkownik może zatem nawet nie mieć świadomości, że jest to forma linkowania. Istnieje więc duża możliwość wprowadzenia go w błąd. Prawie zawsze bowiem korzystanie z tego typu linków wiąże się z naruszeniem integralności podlinkowanej strony, a tam gdzie stanowi przekierowanie do zupełnie innego serwisu występuje spore ryzyko naruszenia prawa do decydowania i sposobie korzystania z utworu[7].

Kolejnym przykładem wykorzystania linków są natomiast odesłania wbudowane (*embedded likns*, embeding). Przybierają one postać jednego z elementów strony internetowej, na której są prezentowane. Oznacza to osadzenie treści stron opublikowanych w zewnętrznych serwisach lub na innych stronach tego samego serwisu na stronie embedującej. Obiekty embedowane umieszczane są w postaci interaktywnych elementów i bezpośrednio wzbogacają witrynę embedującą. *Embedded likns* nie są częścią strony, na którą zostały embedowane, lecz na pewno wzbogacają ją, a technicznie ujmując pochodzą z innej strony. W porównaniu do zwykłego linkowania, embeding pozwala na wyświetlenie całej strony embedowanej na stronie embedującej (np. pliku muzycznego zamieszczonego na innej witrynie), bez konieczności wchodzenia na stronę źródłową. W przypadku zastosowania tej techniki może nastąpić zatem naruszenie praw autorskich, w zakresie prawa do rozpowszechniania utworu[8]. Może też nastąpić pominięcie ograniczeń w dostępności treści strony (tzw. *paywalla*), ustawionych w celu pobierania od użytkowników opłat za udostępnienie utworów[9].

Korzystanie z linków i zasady odnoszące się do linkowania nie zostały wprost uregulowane w przepisach prawa. Należy więc posługiwać się w tym zakresie obowiązującymi regulacjami. W zależności od konkretnych okoliczności, do procesu linkowania i jego konsekwencji mogą mieć zastosowanie regulacje z zakresu prawa autorskiego, prawa o zwalczaniu nieuczciwej konkurencji, prawa prasowego, a także z zakresu ochrony dóbr osobistych. Problem linków i charakteru prawnego linkowania był już kilkakrotnie przedmiotem rozważań sądów, doczekał się również licznych refleksji w literaturze przedmiotu.

Polska ustawa o prawie autorskim[10] nie zawiera jakiejś odrębnej kompleksowej regulacji odnoszącej się do Internetu, a obejmującej poszczególne aspekty korzystania z utworów za pośrednictwem sieci, w tym także zasad linkowania utworów. Od 2003 r. w art. 50 ust. 3 tej ustawy wyodrębniono jednak w ramach tzw.

---

[7] Zob. M. Porzeżyński, *Użycie linków a naruszenie praw własności intelektualnej w świetle orzecznictwa Trybunału Sprawiedliwości UE*, „Kultura Popularna" 2015, nr 1, s. 137.

[8] B. Mazurek, *Wolność słowa w Internecie wobec praw autorskich po obu stronach Atlantyku* [w:] *In Search of the Euro-Atlantic Doctrine of Freedom of Speech*, red. M. Urbańczyk, Ł.D. Bartosik, N. Zagórska, ArchaeGraph Wydawnictwo Naukowe, Poznań–Łódź 2019, s. 205–206.

[9] S. Żyrek, *Zamieszczanie na stronach internetowych hiperłączy*…, s. 49.

[10] Ustawa z dnia z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn. Dz.U. z 2019 r., poz. 1231 ze zm.).

pól eksploatacji w zakresie rozpowszechniania utworów publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym[11]. W tym opisowym, choć jednocześnie szerokim i dość enigmatycznym określeniu, mieszczą się różne formy korzystania z utworu w środowisku informatycznym. Internet stanowi w tym przypadku nie jedyne, ale z pewnością najważniejsze medium rozpowszechniania utworu w przestrzeni wirtualnej[12]. Warto przypomnieć, że zastosowane przez polskiego ustawodawcę sformułowanie „udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym" jest konsekwencją implementacji międzynarodowych i unijnych dokumentów dotyczących prawa autorskiego, w szczególności traktatu WIPO o prawie autorskim[13] oraz dyrektywy 2001/29/WE[14]. Jak podkreślono w uzasadnieniu do ustawy nowelizującej, coraz powszechniejsze wykorzystywanie technologii cyfrowej powoduje nieodwracalną zmianę sposobów i zakresu eksploatacji utworów. Nigdy bowiem dotąd wytwory kultury czy nauki nie były tak łatwo dostępne i to na tak masową skalę, a dodatkowo przy tak niewielkich kosztach. Zjawisko to niesie niewątpliwie szereg pozytywnych konsekwencji poprzez zdecydowane poszerzenie możliwości dostępu do utworów, ale powoduje również istotne zagrożenie naruszaniem praw autorskich i to na niespotykaną dotąd skalę. Poważnym zagrożeniem staje się zwłaszcza wykorzystywanie chronionych dóbr bez zgody uprawnionych podmiotów[15].

Ustawodawca nie definiuje pojęcia pól eksploatacji utworu. W literaturze prawa autorskiego przyjmuje się, że są to pewne wyodrębnione (pod względem technicznym lub ekonomicznym) formy wykorzystywania z dzieła. Nowe pola eksploatacji pojawiają się, gdy dla rozpowszechniania lub zwielokrotniania utworu stosuje się inne sposoby techniczne, kiedy pojawia się możliwość zaspokojenia potrzeb różnego kręgu odbiorców, kiedy określone rozpowszechnianie utworu ma odrębne znaczenie ekonomiczne lub nowy zasięg terytorialny, albo gdy rozpowszechniania dokonuje inny podmiot niż ten który je rozpoczął[16]. Udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym pojawiło się zatem obok takich – tradycyjnych już – pól eksploatacji jak: wytwarzanie utworu określoną techniką, wprowadzanie do obrotu, publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie, nada-

---

[11] Nowelizacja została wprowadzona z dniem 1 stycznia 2003 r. – ustawa z dnia 28 października 2002 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych (Dz.U. z 2002 r., nr 197, poz. 1662 ze zm.).

[12] Por. J. Marcinkowska, A. Matlak, *Treść Prawa autorskiego* [w:] *Prawo autorskie a postęp techniczny*, red. J. Barta, R. Markiewicz, Universitas, Kraków 1999, s. 112 i n.

[13] Zob. art. 8 Traktatu Wipo o Prawie Autorskim (Dz.U. UE. L. z 2000 r., nr 89, s. 8).

[14] Zob. art. 3 dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. UE L z 2001 r., nr 167, s. 10).

[15] Uzasadnienie ustawy z dnia 28 października 2002 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych, System Informacji Prawnej LEX, 2020.

[16] A. Matlak, *Prawo autorskie w społeczeństwie informacyjnym*, Zakamycze, Kraków 2004, s. 104.

wanie i reemitowanie. Rozwój techniczny i technologiczny zawsze był najistotniejszym czynnikiem poszerzania się pól eksploatacji. Skoro zatem w przypadku udostępniania utworu w Internecie można mówić o odrębnym polu eksploatacji, to do działalności na tym polu należy stosować wszystkie wspólne zasady regulujące korzystanie z praw autorskich na poszczególnych polach eksploatacji. Wprowadzenie zasad odmiennych wymagałoby ingerencji ustawodawcy.

W myśl powyższego twierdzenia do linków i linkowania należy odnosić aktualnie obwiązujące przepisy prawa. Nie jest to jednak takie proste, z uwagi na różnorodność tworzenia linków i odmienne cele ich wykorzystywania. To właśnie ta swoistość linków powoduje, że trudno je jednoznacznie zakwalifikować. Mogą one bowiem, w zależności od sytuacji, posiadać cechy charakterystyczne dla kilku czynności, które w prawie autorskim kwalifikowane są zupełnie odmiennie, a prawidłowa ich realizacja wymaga wypełnienia zupełnie innych przesłanek. Wobec braku jednoznacznego rozstrzygnięcia w przepisach prawa można przyjąć, że linki powinny być traktowane jako oznaczenie utworu albo jako substytut utworu[17]. Jak już wcześniej zauważono, ze względu na sposób budowania wyróżnia się linki proste i linki głębokie, wypełniające w praktyce nieco inne funkcje. O ile te pierwsze częściej klasyfikowane są jako specyficzne dla środowiska internetowego oznaczenia utworów, to te drugie z kolei częściej stanowią przykład uznawania linków za substytut utworów.

Przyjmując pierwsze stanowisko, należy zauważyć, że link pełni przede wszystkim funkcję informacyjną, jest zatem informacją o tym, gdzie zamieszczony został wskazany utwór. Konsekwencją takiego rozumowania jest przyjęcie, że linkowanie nie wymaga zgody autora, którego utwór został podlinkowany. Zawsze bowiem możliwe jest wskazanie, gdzie dany utwór się znajduje. To tak jakby umieścić informację o adresie biblioteki czy księgarni, w której dana książka jest dostępna, albo galerii, która wystawia obraz czy rzeźbę. Przyjmuje się, że linki spełniają tutaj funkcję informacyjną, ponieważ – tak samo jak w powyższych przypadkach – wskazują, w jaki sposób dotrzeć do utworu oryginalnego. W przypadku tradycyjnej informacji o utworze – w odróżnieniu od linku – dotarcie do niego wymaga jeszcze wielu czynności i rzadko kiedy może zostać zrealizowane od razu. W przypadku linku, zwłaszcza takiego, który przybiera postać interaktywną, przejście do innego utworu nie wymaga jednak szczególnego wysiłku i w większości przypadków może nastąpić od razu. Taka argumentacja dotyczy zwłaszcza linków głębokich, które ze względu na swoją specyfikę przenoszą bezpośrednio do poszukiwanych treści i poza jednym kliknięciem na ogół nie wymagają żadnej dodatkowej aktywności od użytkownika. Linki proste, przenosząc jedynie do strony początkowej serwisu, a nie do samego utworu, na ogół takiej możliwości przejścia nie dają. Przeniesienie do wskazanego utworu wymaga tutaj podjęcia dodatkowego wysiłku i podjęcia pewnego trudu poszukiwania. Linki proste nie budzą zatem na ogół wątpliwości co do ich wyłącznie informacyjnego charakteru, może

[17] Zob. Ł. Goździaszek, *Prawo blogosfery*, Wydawnictwo C.H. Beck, Warszawa 2014, s. 73.

to być jednak kwestionowane w przypadku linków głębokich. Warto także podkreślić, że szczegółowe adresy internetowe, które są istotą linków, coraz częściej pojawiają się również w utworach mających tradycyjną formę, np. pisemną. Nie mają one jednak postaci interaktywnej, wypełniają więc w zasadzie wyłącznie funkcję informacyjną. Jednak przy obecnym rozpowszechnieniu urządzeń, za pośrednictwem których istnieje możliwość podłączenia do Internetu (jak tablety czy smartfony), także i w tym przypadku dotarcie do informacji zawartej w linku nie wymaga żadnych szczególnie skomplikowanych działań. Wystarczy wpisanie linku w oknie przeglądarki internetowej urządzenia mającego dostęp do Internetu i zaakceptowanie kliknięciem tego wyboru. Linki internetowe różnią się od takich odesłań jedynie większą i szerszą funkcjonalnością, wynikającą z bezpośredniego zamieszczenia na stronie internetowej i korzystania z dostępu do Internetu[18].

Drugie stanowisko przyjmuje założenie znacznie bardziej radykalne. Zakłada bowiem, że link „to niejako substytut utworu w takim sensie, że jednakowe znaczenie ma posługiwanie się linkiem i utworem, do którego prowadzi link”[19]. A zatem, w sensie prawnym czynność linkowania należy zrównywać z rozpowszechnieniem utworu, jest ono bowiem formą udostępnienia utworu za pośrednictwem sieci. Zgodnie z art. 17 ustawy o prawie autorskim wyłączne prawo do rozporządzania utworem na wszystkich polach eksploatacji przysługuje twórcy, o ile nie zostało ono ograniczone lub wyłączone innymi przepisami. Konsekwencją takiego podejścia jest więc wymaganie uzyskania zgody twórcy lub innego uprawnionego na korzystanie z utworu poprzez sporządzenie linku. Przyrównywanie linkowania do rozpowszechniania utworu wynika zapewne z łatwości dotarcia do utworu poprzez link, zwłaszcza, że linkowanie co do zasady umożliwia dostęp do całego utworu, a nie tylko do jego fragmentu. W takiej sytuacji ma miejsce płynne, wręcz odruchowe, przechodzenie do stron internetowych zawartych w linkach. Korzystający z linka może nawet nie mieć świadomości przechodzenia od utworów jednych autorów do utworów innych autorów, w szczególności przypadku zastosowania techniki framingu bądź embedingu, w przypadku których treść objęta linkiem – najczęściej obraz – jest widoczna na stronie linkującej bez konieczności przechodzenia do strony źródłowej[20].

Wyjaśniając jaki charakter mają linki, należy odwoływać się nie tylko do źródeł krajowych, ale także do źródeł międzynarodowych. Internet jest przecież medium o zasięgu ogólnoświatowym, niemieszczącym się w ramach wyłącznie krajowej regulacji. Warto więc sięgnąć do orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE). Problem linkowania pojawił się tutaj już wielokrotnie i był rozpatrywany w kontekście naruszenia prawa do publicznego

[18] Ł. Goździaszek, *Prawo blogosfery*…, s. 73.
[19] Tamże, s. 73.
[20] Por. K. Klafkowska-Waśniowska, *Zamieszczanie odesłań internetowych a zakres praw autorskich majątkowych*, „Białostockie Studia Prawnicze” 2015, z. 19, s. 54.

udostępnienia utworu, o którym mówi art. 3 ust 1 dyrektywy 2001/29/WE[21]. Należy jednak podkreślić, że kwestia ustalenia charakteru prawnego linkowania nie była nigdy podstawowym przedmiotem rozstrzygnięcia. Sądy odnosiły się do niej jedynie w kontekście konkretnego stanu faktycznego, zwykle jednak dość specyficznego i wąsko zarysowanego, miało to więc wpływ na ostateczne rozstrzygnięcie i zakres czynionych rozważań. W kilku przypadkach rozważania te sięgały jednak do kwestii podstawowych i były na tyle istotne, że można je uznać za próbę ustalenia ogólnych zasad korzystania z linków.

TSUE w orzeczeniu wydanym w sprawie *Svensson*[22] sformułował tezę, że nie stanowi czynności publicznego udostępnienia, w rozumienia art. 3 ust. 1 dyrektywy 2001/29/WE udostępnienie na stronie internetowej linków, na które można kliknąć, odsyłających do utworów chronionych, wolno dostępnych na innej stronie internetowej[23]. W uzasadnieniu wskazano, że pojęcie publicznego udostępnienia utworu łączy w sobie dwie przesłanki wymagające łącznego spełnienia, pierwsza z nich to udostępnienie utworu, druga natomiast to udostępnienie utworu publiczności. Fakt udostępniania linków, na które można kliknąć, umożliwiających dostęp do utworów chronionych należy uznać za „podanie do wiadomości" i, w konsekwencji, za „czynność publicznego udostępniania". Aby natomiast utwór chroniony był rzeczywiście udostępniany publiczności, to zgodnie z art. 3 ust. 1 dyrektywy 2001/29 pojęcie „publiczność" należy rozumieć jako nieokreśloną liczbę potencjalnych odbiorców, a ponadto powinna to być dość znaczna liczba osób. TSUE w tym orzeczeniu sformułował również tezę, że zezwolenie podmiotów prawa autorskiego na udostępnienie utworu nie jest konieczne w przypadku braku udostępnienia utworu nowej publiczności. Podkreślił, że nową publiczność stanowi taka publiczność, która nie została wzięta pod uwagę przez podmioty uprawnione, w momencie gdy zezwoliły na pierwotne udostępnienie utworu, przy czym miało miejsce udostępnienie tych samych utworów co przy udostępnieniu pierwotnym i nastąpiło ono w oparciu o tę samą technologię co udostępnienie pierwotne[24].

W innym orzeczeniu, w sprawie *GS Media*[25], TSUE podkreślił, że aby ustalić, czy fakt umieszczenia w witrynie internetowej hiperłączy odsyłających do utworów chronionych – swobodnie dostępnych w innej witrynie internetowej bez

---

[21] Zgodnie z art. 3 ust 1 dyrektywy 2001/29/WE: Państwa Członkowskie powinny zapewnić autorom wyłączne prawo do zezwalania lub zabraniania na jakiekolwiek publiczne udostępnianie ich utworów, drogą przewodową lub bezprzewodową, włączając podawanie do publicznej wiadomości ich utworów w taki sposób, że osoby postronne mają do nich dostęp w wybranym przez siebie miejscu i czasie.

[22] Wyrok Trybunału Sprawiedliwości UE z dnia 13 lutego 2014 r. (C-466/12, Nils Svensson i inni v. Retriever Sverige AB, LEX nr 1424770.

[23] Wyrok C-466/12, Svensson, pkt 32.

[24] Wyrok C-466/12, Svensson, pkt 20–28.

[25] Wyrok TS z dnia 8 września 2016 r., C-160/15, GS Media BV v. Sanoma Media Netherlands BV, Playboy Enterprises International INC. I Britt Geertruidzie Dekker, Lex nr 2099013.

zezwolenia podmiotu praw autorskich – stanowi „publiczne udostępnianie" w rozumieniu art. 3 ust. 1 dyrektywy 2001/29/WE, należy określić, czy te hiperłącza zostały udostępnione bez celu zarobkowego przez osobę, która nie wiedziała lub nie mogła racjonalnie wiedzieć o bezprawnym charakterze publikacji tych utworów w tej innej witrynie internetowej, czy też przeciwnie, wspomniane hiperłącza zostały udostępnione w celu zarobkowym, w której to sytuacji należy domniemywać istnienie tej wiedzy[26]. Taka interpretacja dyrektywy ma zapewniać wysoki poziom ochrony autorów, dając możliwość występowania podmiotom praw autorskich nie tylko przeciwko pierwotnej publikacji ich utworów w Internecie, ale także przeciwko każdemu, kto zamieści w celach zarobkowych hiperłącze do utworu bezprawnie opublikowanego. Ma chronić również w sytuacji, gdy hiperłącze umożliwia dostęp do utworu opublikowanego bezprawnie przez osobę, która wiedziała bądź powinna wiedzieć o tym fakcie oraz w sytuacji, gdy umieszczony link umożliwia użytkownikom witryny internetowej, w której ten link się znajduje, obejście ograniczeń zastosowanych w witrynie, w której znajduje się chroniony utwór, w celu ograniczenia dostępu jedynie dla klientów tejże witryny, a więc w takich sytuacjach, w których można domniemywać celowe i świadome działanie podmiotu umieszczającego link. Orzeczenie to poszerza interpretację przyjętą przez TSUE w sprawie *Svensson* o kwestie zarobkowego wykorzystania publikacji zawierających hiperłącza.

Natomiast w orzeczeniu w sprawie *Land Nordrhein-Westfalen*[27] TSUE wyraził przekonanie, że funkcją linków jest zagwarantowanie prawidłowego funkcjonowania Internetu, dzięki umożliwieniu szerokiego rozpowszechniania informacji w sieci i zapewnieniu pełnej dostępności do ogromnej ilości informacji. Prawa zapewnione w art. 3 ust. 1 dyrektywy 2001/29/WE mają charakter gwarancyjny i pozwalają podmiotom praw autorskich na podjęcie kroków wobec potencjalnych użytkowników ich utworów, rozważających publiczne udostępnienie tych utworów, tak aby zakazać im takich działań. Udostępnienie utworu poprzez zamieszczenie na stronie internetowej linku, który odsyła do utworu udostępnionego wcześniej za zgodą podmiotu praw autorskich, oznacza zachowanie prewencyjnego charakteru praw przysługujących temu podmiotowi, ponieważ jeżeli autor nie życzy już sobie udostępniania swojego utworu na odnośnej stronie internetowej, może usunąć utwór ze strony internetowej, na której został on pierwotnie udostępniony. W takim przypadku linki odsyłające do utworu także przestaną być aktywne. Należy więc odróżnić udostępnienie za pomocą linku od udostępnienia poprzez bezpośrednie umieszczenie utworu na innej stronie internetowej, ponieważ w takim przypadku utwór mimo usunięcia go ze strony pierwotnego udostępnienia, na które autor wyraził zgodę, pozostaje aktywny na innej stronie, niezależnie od uprzedniej zgody autora i pomimo wszelkich jego działań uniemożliwiających

[26] Wyrok C-160/15, GS Media BV, pkt 55.

[27] Wyrok Trybunału Sprawiedliwości UE z dnia 7 sierpnia 2018 r., C-161/17 Land Nordrhein-Westfalen v. Dirkowi Renckhoffowi, Lex nr 2600244.

dalsze udostępnianie utworu[28]. Zaprezentowane stanowisko TSUE wyraził również w innych swoich orzeczeniach[29].

W świetle przytoczonych przykładów orzecznictwa TSUE uzasadnione jest twierdzenie, że umieszczenie linku do utworu chronionego prawem autorskim nie może być traktowane jako udostępnienie utworu, naruszające majątkowe prawa autorskie. Przede wszystkim bowiem takie udostępnienie utworu nie stanowi udostępnienia utworu nowej publiczności. Treści umieszczone już wcześniej za zgodą uprawnionego na ogólnodostępnej stronie, stają się dostępne dla wszystkich użytkowników Internetu, a ten powinien być traktowany jako jedno medium, podobnie jak choćby telewizja. Internautów nie należy różnicować na odbiorców poszczególnych portali czy stron, tak samo jak nie różnicuje się grupy telewidzów ani czytelników[30]. Kolejne udostępnienie za pomocą tego samego medium nie zwiększa już liczby potencjalnych odbiorców utworu. A zatem nie może stanowić naruszenia praw autorskich umieszczenie linku do powszechnie dostępnych treści. Odmienne stanowisko w tej kwestii byłoby zaprzeczeniem podstawowej funkcjonalności Internetu, wynikającej właśnie z zastosowania interaktywnych odesłań, jako źródła ułatwiającego dotarcie do informacji[31]. Dopóki nie zmienia się techniczna forma udostępnienia utworu, to również nie można mówić o udostępnieniu utworu nowej publiczności.

W literaturze z zakresu prawa autorskiego zwraca się jednak uwagę, że kryterium nowej publiczności nie wynika z powszechnie obowiązujących przepisów prawa, a jest efektem posłużenia się nieaktualnym glosariuszem do konwencji berneńskiej, pochodzącym z 1980 r. Glosariusze takie nie stanowią aktu prawa powszechnie obowiązującego, a konkluzje wynikające z dokumentu pochodzącego z lat 80. XX wieku nie zostały opracowane z myślą o nowych mediach i nie odpowiadają zmianom, technologicznym, które nastąpiły w od tego czasu[32]. Zastosowanie kryterium nowej publiczności, choć pozwala na wyprowadzenie zdroworozsądkowego rozstrzygnięcia konkretnych spraw będących przedmiotem rozstrzygnięć TSUE, jest krytykowane w literaturze przedmiotu za pewne niekonsekwencje, które powstają przy próbie zastosowania tego kryterium do innych stanów faktycznych. S. Żyrek zwraca uwagę na paradoks pojawiający się, gdyby koncepcję tę zastosować również do kopii utworu zamieszczonej na jednej stronie internetowej bez zgody uprawnionego, podczas gdy na innej stronie ten sam utwór został udostępniony przez uprawnionego bez ograniczeń. Wskazuje, że w takiej sytuacji nie występowałoby publiczne udostępnienie waśnie ze względu na brak nowej publiczności[33]. Na inne zaskakujące i trudne do akceptacji konsekwencje

---

[28] Wyrok C-161/17, Land Nordrhein-Westfalen, pkt 40–44.
[29] C-348/13, C-136/09, C-279/13.
[30] Zob. M. Porzeżyński, *Użycie linków a naruszenie praw własności intelektualnej*…, s. 142.
[31] Zob. tamże, s. 144.
[32] S. Żyrek, *Zamieszczanie na stronach internetowych*…, s. 54 oraz cytowana tam literatura.
[33] Tamże, s. 56.

posługiwania się kryterium nowej publiczności zwraca uwagę R. Markiewicz. Sygnalizuje on, że kryterium to nie nadaje się do wykorzystania przy innych rodzajach publicznego udostępniania utworu, jak chociażby w przypadku wydania książki, ponieważ należałoby uznać, że inny wydawca, drukując i wydając za pośrednictwem tych samych kanałów dystrybucji taką samą książkę na takich samych warunkach, nie narusza monopolu autorskiego[34].

TSUE słusznie wykazał, że w przypadku zamieszczenia na stronie internetowej linku do utworu chronionego prawem wyłącznym, uprawnionemu nie jest odbierane prewencyjne prawo do kontroli dostępności tego materiału poprzez usunięcie go z pierwotnej strony. W efekcie usunięcia utworu z pierwotnej strony internetowej, przestaje on być dostępny poprzez link, i to niezależnie od tego, jaką formę przyjmie link, a więc zarówno wówczas, gdy będzie to link głęboki przenoszący bezpośrednio do strony, na której utwór był udostępniony, jak i w przypadku framingu oraz embedingu, gdy utwór udostępniony na pierwotnej stronie otwiera się bezpośrednio na stronie zawierającej link. Powoduje to, iż dostęp do utworu za pomocą linka staje się niemożliwy i następuje faktyczne zablokowanie dostępności pierwotnie udostępnionej treści. Trudno dowodzić w takim przypadku, iż poprzez linkowanie nastąpiło samodzielne rozpowszechnienie utworu, wymagające zgody uprawnionego. Takie rozpowszechnienie powinno być bowiem niezależne i niepowiązane bezpośrednio z udostępnieniem na stronie pierwotnej, jak ma to miejsce w przypadku umieszczenia utworu bezpośrednio na innej niż pierwotna stronie internetowej.

TSUE podkreślił jednak, że zarobkowe działanie udostępniającego linki do opublikowanych bezprawnie utworów, może skutkować odpowiedzialnością udostępniającego taki utwór; od takiej osoby wymagana jest bowiem większa staranność przy sprawdzaniu źródeł publikowanych treści. Niezależnie od naruszenia prawa autorskiego, linkowanie może być uznane za bezprawne w świetle zasad kodeksu cywilnego, prowadząc chociażby do naruszenia dóbr osobistych określonego podmiotu. Poprzez udostępnienie linku do pewnych stron czy utworów, następuje wybór określonych treści spośród ogromu materiałów dostępnych w Internecie i nakierowanie na nie użytkownika, który inaczej być może nigdy by się z nimi nie zapoznał. Umieszczający linki selekcjonuje i udostępnia takie materiały, które najczęściej służą wzmocnieniu jego własnego przekazu zawartego w innych umieszczonych w Internecie materiałach[35]. Odpowiedzialność udostępniającego link do takich materiałów zależy więc od tego czy jego działanie jest bezprawne. Odpowiada to polskiej konstrukcji pomocnictwa i podżegania[36].

---

[34] R. Markiewicz, *Svensson a sprawa polska*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2014, z. 4, s. 59.

[35] Szerzej: M. Piaskowska, F. Piesiewicz, *Problematyka naruszenia dóbr osobistych w postaci czci a udostępnianie treści pochodzących od osób trzecich za pośrednictwem hiperlinków*, „Studia Prawnicze" 2018, nr 2, s. 105.

[36] R. Markiewicz, *Svensson a sprawa polska*…, s. 61.

Reasumując należy stwierdzić, że umieszczanie linków internetowych nadal budzi wiele wątpliwości. Brak jednoznacznego ustalenia ich charakteru w przepisach prawa pozostawia otwartą drogę do różnych interpretacji, zarówno w kontekście prawa unijnego, jak i prawa krajowego. Pomimo pewnych niekonsekwencji, przyjęta w orzecznictwie TSUE linia orzecznictwa, bardziej skłania do przyjęcia stanowiska, że linki należy traktować jako swoiste dla Internetu oznaczenie utworu, a nie jako formę udostępnienia utworu. Osobną kwestią pozostają natomiast cywilnoprawne skutki wynikające z umieszczenia linku w Internecie, dotyczące odpowiedzialności za naruszenie dóbr osobistych. Należy też poprzeć wyrażone niejednokrotnie w literaturze stanowisko, że kwestie ochrony praw autorskich w Internecie wymaga poważnej i dość szerokiej ingerencji ustawodawcy, uwzględniającej specyfikę tego medium.

## Bibliografia


*Coś to jest building? Kilka słów o linkowaniu*, cz. 1, https://delante.pl/co-to-jest-link-building-kilka-slow-o-linkowaniu-cz-1-vlog-robie-seo-12/ (dostęp: 20.09.2020 r.)

Goździaszek Ł., *Prawo blogosfery*, Wydawnictwo C.H. Beck, Warszawa 2014.

https://pl.wikipedia.org/wiki/Hiperłącze (dostęp: 20.09.2020 r.).

Klafkowska-Waśniowska K., *Zamieszczanie odesłań internetowych a zakres praw autorskich majątkowych*, „Białostockie Studia Prawnicze" 2015, s. 19.

Marcinkowska J., Matlak A., *Treść Prawa autorskiego* [w:] *Prawo autorskie a postęp techniczny*, red. J. Barta, R. Markiewicz, Universitas, Kraków 1999.

Markiewicz R., *Svensson a sprawa polska*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2014, z. 4.

Maryniak Ł., *Zakazane linkowanie?*, https://www.pwi.us.edu.pl/kategorie/prawo-technologii-i-internetu/245-zakazane-linkowanie (dostęp: 20.09.2020 r.).

Matlak A., *Prawo autorskie w społeczeństwie informacyjnym*, Zakamycze, Kraków 2004.

Mazurek B., *Wolność słowa w Internecie wobec praw autorskich po obu stronach Atlantyku* [w:] *In Search of the Euro-Atlantic Doctrine of Freedom of Speech*, red. M. Urbańczyk, Ł.D. Bartosik, N. Zagórska, ArchaeGraph Wydawnictwo Naukowe, Poznań–Łódź 2019.

Piaskowska M., Piesiewicz F., *Problematyka naruszenia dóbr osobistych w postaci czci a udostępnianie treści pochodzących od osób trzecich za pośrednictwem hiperlinków*, „Studia Prawnicze" 2018, nr 2.

Porzeżyński M., *Użycie linków a naruszenie praw własności intelektualnej w świetle orzecznictwa Trybunału Sprawiedliwości UE*, „Kultura Popularna" 2015, nr 1/2015.

Szpringer W., *Linking, framing, meta-tagi (perspektywa konkurencji)*, http://vagla.pl/skrypts/w_szpringer_linking_framing.pdf (dostęp: 20.09.2020 r.).

Żyrek S., *Zamieszczanie na stronach internetowych hiperłączy umożliwiających uzyskanie dostępu do utworów chronionych prawem autorskim* – wprowadzenie i wyrok Trybunału Sprawiedliwości z 13.02.2014 r., C-466/12, Nils Svensson i in. przeciwko Retriever Sverige AB, „Europejski Przegląd Sądowy" 2019, nr 3.

# Prawodawstwo

Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. UE L z 2001 r., nr 167, s. 10).

Traktat Wipo o Prawie Autorskim (Dz.U. UE. L. z 2000 r., nr 89, s. 8).

Ustawa z dnia 28 października 2002 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych (Dz.U. z 2002 r., nr 197, poz. 1662 ze zm.).

Ustawa z dnia z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn. Dz.U. z 2019 r., poz. 1231 ze zm.).

Uzasadnienie ustawy z dnia 28 października 2002 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych, System Informacji Prawnej LEX, 2020.

# Orzecznictwo

Wyrok Trybunału Sprawiedliwości UE z dnia 13 lutego 2014 r. (C-466/12, Nils Svensson i inni v. Retriever Sverige AB, LEX nr 1424770.

Wyrok Trybunału Sprawiedliwości UE z dnia 7 sierpnia 2018 r., C-161/17 Land Nordrhein-Westfalen v. Dirkowi Renckhoffowi, Lex nr 2600244.

Wyrok TS z dnia 8 września 2016 r., C-160/15, GS Media BV v. Sanoma Media Netherlands BV, Playboy Enterprises International INC. I Britt Geertruidzie Dekker, Lex nr 2099013.

# PRAWNA OCHRONA WIZERUNKU W SIECI

(*Elżbieta Kurzępa*)

## Wprowadzenie

Wizerunek stanowi jedno z dóbr osobistych człowieka, podlegające ochronie prawnej zarówno na gruncie prawa prywatnego, jak również prawa publicznego. O ile jeszcze kilkanaście lat temu ochrona wizerunku i skuteczność rozwiązań w tym zakresie stanowiła przede wszystkim problem osób znanych, funkcjonujących w szeroko rozumianej przestrzeni publicznej (np. polityków, artystów wykonawców, sportowców), o tyle obecnie problem naruszenia wizerunku dotyczyć może w zasadzie każdej osoby, co związane jest z powszechnym dostępem do Internetu i łatwością rozpowszechniania w sieci dowolnych treści, także tych ingerujących w prawa osób trzecich. Zdarza się, że tego typu sytuacje spowodowane są umyślnym działaniem człowieka, ale także nierzadkie są przypadki, kiedy to nieświadomość w zakresie zasad ochrony wizerunku i możliwości jego rozpowszechniania oraz niefrasobliwość użytkowników Internetu powodują, że dochodzi do naruszenia tego dobra osobistego. Szczególne ryzyko rozpowszechniania wizerunku w Internecie wiąże się ze specyfiką sieci, z której stosunkowo trudno definitywnie usunąć pliki, na których utrwalono wizerunek. Jeśli chodzi o obecne krajowe rozwiązania w zakresie ochrony wizerunku, to są one przewidziane przede wszystkim na gruncie prawa cywilnego, prawa autorskiego, jak również prawa karnego. Pojawia się pytanie, czy są one wystarczające i skuteczne w czasach powszechnego dostępu do Internetu, kiedy to wizerunek jest tym dobrem, które w świecie wirtualnym wykorzystywane jest nie tylko jako narzędzie, czy element rozrywki oraz informacji, ale coraz częściej jako źródło potencjalnego zarobku.

## Definicja wizerunku

Rozważania w zakresie prawnej ochrony wizerunku w sieci należy rozpocząć od przedstawienia definicji wizerunku. Zaznaczyć trzeba, że w żadnym akcie normatywnym nie określono legalnej definicji tego dobra prawnego, jednak dość rozbudowana w tym zakresie linia orzecznicza, jak i poglądy doktryny, są stosunkowo jednolite. Zwrócić należy także uwagę, że w rozumieniu potocznym pojęcie „wizerunek" jest szersze, aniżeli to stosowane w nauce prawa. Według *Słownika języka polskiego PWN* wizerunek należy rozumieć jako czyjąś podobiznę na rysunku, obrazie, zdjęciu itp., a także sposób, w jaki dana osoba jest postrzegana

i przedstawiana[1]. Także w *Wielkim słowniku języka polskiego* zdefiniowano „wizerunek" jako podobiznę kogoś lub czegoś, a także sposób, w jaki dana osoba lub rzecz jest odbierana[2]. W powszechnym rozumieniu wizerunek odnosi się więc nie tylko do sposobu postrzegania ludzi, ale również rzeczy.

Z kolei według poglądów doktryny prawa autorskiego wizerunek oznacza zwykle wytwór niematerialny, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby (lub danych osób). Wizerunek utrwalony może być przez malarski portret, rysunek, fotografię. Ponadto, zgodnie ze stanowiskiem Sądu Najwyższego, wizerunek poza dostrzegalnymi dla otoczenia cechami fizycznymi, tworzącymi wygląd danej jednostki i pozwalającymi – jak się określa – na jej identyfikację wśród innych ludzi, może obejmować dodatkowe utrwalone elementy związane z wykonywanym zawodem jak charakteryzacja, ubiór, sposób poruszania się i kontaktowania z otoczeniem[3]. Wizerunek to takie cechy twarzy i całej postaci, które pozwalają zidentyfikować jakąś osobę jako określoną jednostkę fizyczną[4]. Wizerunek definiuje się ponadto w nauce prawa autorskiego jako wytwór niematerialny, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby lub danych osób. Obok klasycznych portretów malarskich są to także fotografie i karykatury[5]. Do tradycyjnych nośników wizerunku zakwalifikować zatem należy fotografię, utrwalenie audiowizualne, rzeźby, szkice, obrazy, Wskazać jednocześnie należy, że opis danej osoby, dokonany za pomocą innej metody niż środki plastyczne, nie tworzy jej wizerunku w rozumieniu prawa. Jak podnosi się w doktrynie prawa autorskiego poza zakresem pojęcia wizerunku powinien pozostawać chociażby „dźwięczny wizerunek" (określany również jako „wizerunek audialny"), rozumiany jako charakterystyczny głos danej osoby umożliwiający jej rozpoznanie[6]. Pojawiają się jednak w tej kwestii stanowiska przeciwne, według których wyróżnić jednakże należy tzw. wizerunek dźwięczny (głosowy), oznaczający określony charakterystyczny sposób mówienia, brzmienia, tembr głosu[7]. Biorąc jednak pod uwagę, że wizerunek kojarzyć raczej należy z plastycznym przedstawieniem cech danej osoby, trudno uznać ten pogląd (raczej niedominujący w doktrynie prawa autorskiego) za właściwy. Nawiązując do wyżej zaprezentowanych definicji wizerunku należy zaznaczyć, że nie będzie stanowił wizerunku literacki opis osoby, choćby

---

[1] https://sjp.pwn.pl/szukaj/wizerunek.html (dostęp: 4.09.2020 r.).

[2] https://www.wsjp.pl/index.php?id_hasla=11573&ind=0&w_szukaj=wizerunek (dostęp: 4.09. 2020 r.).

[3] J. Barta, R. Markiewicz (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, wyd. V, Warszawa 2011, System Informacji Prawnej LEX (dostęp: 4.09.2020 r.).

[4] K. Stefaniuk, *Naruszenie prawa do wizerunku przez rozpowszechnianie podobizny*, „Państwo i Prawo" 1970, nr 1, s. 64.

[5] J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Prawa autorskie i prawa pokrewne. Komentarz*, Kraków 2005, s. 628.

[6] D. Flisak (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, system Informacji Prawnej „LEX" (dostęp: 4.09.2020 r.).

[7] J. Sieńczyło-Chlabicz, *Rozpowszechnianie wizerunku osób powszechnie znanych*, „Przegląd Prawa Handlowego" 2003, nr 9, s. 40.

przedstawiający ją za pomocą słowa w szczególnie dokładny i trafny sposób, choć i w tym zakresie pojawiają się w doktrynie odmienne zdania[8].

Należy zaznaczyć, że wizerunkiem będzie takie skonkretyzowane ustalenie obrazu fizycznego, które można zwielokrotnić i rozpowszechnić. Tym różnić się będzie ono od pojęcia obrazu, wyglądu człowieka, będącego elementem jego tożsamości[9].

Jeżeli chodzi o pojęcie wizerunku pojawiające się w orzecznictwie sądów powszechnych, to definiuje się go m.in. jako podobiznę człowieka na obrazie, fotografii lub utrwaloną w inny sposób. Takie dobro osobiste przysługuje tylko człowiekowi i nie ma swojego odpowiednika w postaci dobra przysługującego osobie prawnej[10]. Wizerunek stanowi szeroko pojętą podobiznę człowieka, a więc konkretyzację i ustalenie obrazu fizycznego jednostki, zdatną do zwielokrotniania i rozpowszechniania. Wizerunek w sensie prawnym nie jest więc tożsamy z wyglądem fizycznym człowieka, stanowi przedstawienie i konkretyzację tego wyglądu. Wizerunek nie musi stanowić fotograficznego odwzorowania obrazu danego człowieka, może skupiać się, jak ma to miejsce na przykład w przypadku karykatury, jedynie na pewnych charakterystycznych dla danej jednostki elementach. Jednakże warunkiem koniecznym uznania danego przedstawienia wyglądu człowieka za wizerunek stanowiący chronione dobro osobiste, jest możliwość jego przypisania do określonej osoby, identyfikacja tej osoby za pomocą danego wizerunku. Identyfikacja taka może nastąpić bezpośrednio lub pośrednio poprzez dołączone wskazówki, kontekst sytuacyjny, w jakim jest umieszczona podobizna danej postaci, czy podpis umieszczony pod zdjęciem[11]. Wizerunek określany jest także jako dostrzegalne, fizyczne cechy człowieka, tworzące jego wygląd i pozwalające na identyfikację danej osoby wśród innych ludzi bądź też: skonkretyzowane ustalenie obrazu fizycznego człowieka, zdatne do zwielokrotnienia i rozpowszechnienia. Na gruncie art. 81 ustawy o prawie autorskim i prawach pokrewnych przyjmuje się, że wizerunek to wytwór niematerialny, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby (lub osób)[12].

Biorąc pod uwagę wyżej określone definicje wizerunku prezentowane w doktrynie oraz orzecznictwie, stwierdzić należy, że wizerunek w kontekście sieci Internet stanowić zwykle będzie utrwaloną na fotografii cyfrowej lub w formie zapisu audiowizualnego podobiznę człowieka, zapisaną następnie w formie pliku elektronicznego, choć rzecz jasna nie można wykluczyć innego sposobu plastycznego wyrażenia fizycznej strony danej osoby (np. karykatury). Rozpowszechniany

---

[8] J. Sieńczyło-Chlabicz (red.), *Prawo własności intelektualnej*, wyd. 1, Warszawa 2009, s. 237.

[9] Taki trafny pogląd wyraziła T. Grzeszczak [w:] *Prawo autorskie. System Prawa Prywatnego*, t. 13, red. J. Barta, Warszawa 2017, s. 783.

[10] Wyrok Sądu Apelacyjnego w Warszawie z dnia 1 sierpnia 2019 roku, sygn. akt V ACa 501/18, LEX nr 2726845, System Informacji Prawnej „LEX" (dostęp: 5.09.2020 r.).

[11] Wyrok Sądu Apelacyjnego w Warszawie z dnia 9 marca 2018 roku, sygn. akt VI ACa 1694/16, LEX nr 2524902, System Informacji Prawnej „LEX" (dostęp: 5.09.2020 r.).

[12] Wyrok Sądu Apelacyjnego w Krakowie z dnia 19 kwietnia 2016 roku, sygn. akt I ACa 1826/15, LEX nr 2041781, System Informacji Prawnej „LEX" (dostęp: 5.09.2020 r.).

w sieci wizerunek człowieka najczęściej pojawiać się będzie w kontekście informacyjnym, rozrywkowym, zarobkowym, choć zdarza się, że także w celach przestępczych.

## Prawna ochrona wizerunku w kontekście sieci Internet

Ochrona wizerunku zagwarantowana jest w polskim porządku prawym na gruncie co najmniej trzech dziedzin prawa, mianowicie w przepisach prawa cywilnego, autorskiego i karnego. Warto jednocześnie zaznaczyć, że regulacje te co do zasady nie wykluczają się wzajemnie, przez co umożliwiają bardziej kompleksową ochronę.

Wizerunek traktowany jest wprawie cywilnym jako jedno z dóbr osobistych człowieka, a ochrona tychże dóbr osobistych zagwarantowana została na gruncie art. 23–24 ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny[13]. Wizerunek jako dobro osobiste człowieka określono w przepisach art. 23 k.c., w myśl którego dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Należy zwrócić uwagę, że ustawodawca nie określił legalnej definicji dóbr osobistych, choć taka rzecz jasna pojawia się w doktrynie prawa cywilnego. Aktualnie dominującą w doktrynie koncepcją dóbr osobistych jest koncepcja posługująca się kryterium obiektywnym, odwołującym się do przyjętych w społeczeństwie ocen[14]. Zgodnie z tą koncepcją dobra osobiste są wartościami o charakterze niemajątkowym, wiążącymi się z osobowością człowieka, uznanymi powszechnie w społeczeństwie. Dla istnienia dobra osobistego i uznania, że doszło do jego naruszenia, znaczenie mają oceny społeczne, analiza z punktu widzenia rozsądnego człowieka; nie ma tu znaczenia subiektywne przekonanie zainteresowanego[15]. Niewłaściwe byłoby zatem opieranie oceny, czy doszło do naruszenia dobra osobistego, jedynie na odczuciach podmiotu, którego one dotyczą, zwłaszcza że czasem odczucia konkretnego człowieka odbiegają bardzo istotnie od norm ogólnych[16].

Zaznaczyć trzeba, że dobra osobiste wyszczególnione w powołanym powyżej art. 23 k.c. mają jedynie charakter przykładowy, a więc określony przez ustawodawcę katalog nie jest katalogiem zamkniętym. W doktrynie prawa cywilnego

---

[13] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2019 r., poz. 1145 ze zm.) (dalej jako: k.c.).

[14] K. Pietrzykowski (red.), *Kodeks cywilny*, t. I: *Komentarz do art. 1–449[1]*, wyd. 6, Warszawa 2011, s. 119.

[15] J. Ciszewski, P. Nazaruk (red.), *Kodeks cywilny. Komentarz*, Warszawa 2019, System Informacji Prawnej „LEX" (dostęp: 5.09.2020 r.).

[16] M. Fraus, M. Habdas (red.), *Kodeks cywilny*, t. I: *Część ogólna (art. 1–125)*, Warszawa 2018, System Informacji Prawnej „LEX" (dostęp: 5.09.2020 r.).

podkreśla się także, że objęcie ochroną wynikającą z art. 23 i 24 k.c. treści godzących w dobra osobiste dostępne w Internecie nie budzi wątpliwości, zwłaszcza że szeroki zasięg informacji i poczucie anonimowości użytkowników sprawiają, iż bardzo łatwo dochodzi do naruszenia szczególnie tak wrażliwych dóbr osobistych jak cześć, godność, wizerunek czy nazwisko[17].

Biorąc zatem pod uwagę przepisy kodeksu cywilnego nie ulega wątpliwości, że wizerunek jest dobrem osobistym człowieka chronionym na gruncie wyżej powołanego aktu prawnego, także w sytuacji naruszenia tego dobra w Internecie, co coraz częściej ma miejsce ze względu na przeniesienie się dużej części życia społecznego właśnie na grunt tego medium komunikacyjnego. Należy zauważyć, że ustawodawca nie precyzuje w kodeksie cywilnym, jakie czynności uważa się za naruszenie poszczególnych dóbr osobistych, określając jedynie rozwiązania w zakresie ochrony. Wydaje się, że takim naruszeniem wizerunku będzie chociażby takie jego utrwalenie (np. za pomocą fotografii), które przedstawia go w sposób niekorzystny dla danej osoby, ośmieszający, ingerujący w sferę intymną, bez zgody danej osoby. Niewątpliwie naruszeniem wizerunku będzie również takie jego przedstawienie, które przybiera charakter pornograficzny[18]. Jeśli chodzi o wizerunek osób publicznych, to przyjmuje się, że naruszeniem wizerunku, o którym mowa na gruncie art. 23–24 k.c., będzie także podszycie się osoby trzeciej za daną osobą publiczną, a więc wykorzystanie tzw. sobowtóra i wprowadzenie w ten sposób w błąd odbiorców[19]. Nie ulega wątpliwości, że wyżej opisane sposoby naruszenia dobra osobistego, jakim jest wizerunek, często mają miejsce w sieci, gdyż rozpowszechnianie zdjęć czy filmów z utrwalonym wizerunkiem w sposób, który to dobro narusza, nierzadko odbywa się właśnie w Internecie, w szczególności w serwisach informacyjnych, tzw. portalach plotkarskich czy portalach społecznościowych. Warto przytoczyć w tym miejscu tezę wyroku Sądu Apelacyjnego w Warszawie z dnia 19 września 2018 roku (sygn. akt VI ACa 528/17), w myśl której: wizerunek podlega ochronie również na gruncie art. 24 k.c. jako dobro osobiste, a więc jako pewna wartość idealna związana ściśle z osobowością człowieka, podlegająca ochronie na tych samych zasadach, jak godność osobista, dobre imię, czy prywatność. W tym wypadku przedmiotem ochrony jest nie monopol eksploatacyjny samego wizerunku, jak w wypadku ochrony przewidzianej przez prawo autorskie, a sfera wartości idealnych przypisanych dobrom osobistym jednostki. Naruszenie następuje wówczas poprzez opublikowanie podobizny jednostki w kontekście stanowiącym o naruszenie jej dobrego imienia lub prywatności. W tym wypadku publikacja wizerunku stanowi w istocie przejaw naruszenia prawa osobistości i w takim kontekście, to jest naruszenia wskazywanych

---

[17] P. Modrzejewski, *Odpowiedzialność innych podmiotów niż sprawca za naruszenie dóbr osobistych w Internecie*, „Przegląd Prawa Handlowego" 2017, nr 3, s. 50–58.

[18] M. Barta, R. Markiewicz, *Wokół prawa do wizerunku* [w:] *Zagadnienia prawa własności intelektualnej. Profesorowi Stefanowi Grzybowskiemu pracownicy Instytutu Wynalazczości i Ochrony Własności Intelektualnej w darze*, Kraków 2002, s. 11.

[19] M. Fraus, M. Habdas (red.), *Kodeks cywilny…*

w pozwie dóbr osobistych w postaci dobrego imienia i godności osobistej, publikacja ta powinna być rozpatrywana[20]. Wydaje się zatem, biorąc pod uwagę treść powyższego orzeczenia, że nie każde naruszenie przepisów ustawy oprawie autorskim i prawach pokrewnych z zakresu ochrony wizerunku stanowić będzie jednoczesne naruszenie wizerunku jako dobra osobistego określonego na gruncie art. 23 k.c. i uzasadniać będzie wystąpienie z roszczeniami skumulowanymi na gruncie tych dwóch aktów prawnych. Powstaje jednocześnie wątpliwość, czy aby nie każde naruszenie monopolu eksploatacyjnego wizerunku i bezprawnego jego rozpowszechnienie, mimo że niegodzące w godność osobistą i dobre imię, stanowi jednoczesne naruszenie prawa do prywatności, także uznawanego za jedno z dóbr osobistych.

Warto zaznaczyć, że nie każde wykorzystanie wizerunku będzie bezprawne i będzie stanowiło podstawę wystąpienia z roszczeniami określonymi na gruncie art. 24 k.c. Jasne jest, że w szczególności zgoda uprawnionego będzie okolicznością wyłączającą bezprawność. W orzecznictwie sądów powszechnych podnosi się, że zgoda na rozpowszechnienie wizerunku nie musi być dla swej ważności udzielona na piśmie, jednakże nie może budzić wątpliwości, że zgoda taka została udzielona. Oznacza to, że osoba, która udziela zgody musi mieć pełną świadomość nie tylko co do formy przedstawienia jej wizerunku, ale także czasu, miejsca publikacji, zestawienia z innymi wizerunkami, jak również towarzyszącego komentarza[21]. Zgoda wyrażona przez osobę, której wizerunek zostanie utrwalony i rozpowszechniony wyłącza zatem możliwość powołania się na przepisy art. 23–24 k.c., chyba została ona udzielona w innym zakresie, niż ostatecznie został wykorzystany przez osobę trzecią (np. udzielono zgody na utrwalenie i opublikowanie wizerunku w formie fotografii na prywatnym profilu na portalu społecznościowym, natomiast ostatecznie fotografię wykorzystano na stronie internetowej sklepu w celach reklamowych).

Ponadto, działaniem, które wyłączy bezprawność w zakresie wykorzystania wizerunku będzie działanie w oparciu o przepisy innych aktów prawnych, np. art. 81 ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych, które szczegółowo określone zostaną poniżej, a które uzależniają możliwość rozpowszechniania wizerunku od zgody osoby na nim przedstawionej, chyba że jest nią osoba powszechnienie znana i jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych lub gdy chodzi o wizerunek osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza[22]. Skoro przepisy ustawy o prawie autorskim i prawach pokrewnych co do zasady określają wymóg uzyskania zgody na rozpowszechnienie wizerunku, pojawia się

[20] LEX nr 2616080, System Informacji Prawnej „LEX" (dostęp: 5.09.2020 r.).

[21] Wyrok Sądu Apelacyjnego w Warszawie z dnia 7 maja 2014 roku, I ACa 1686/13 http://orzeczenia.waw.sa.gov.pl/content/$N/154500000000503_I_ACa_001686_2013_Uz_2014-05-07_002 (dostęp: 6.09.2020 r.).

[22] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2019 r., poz. 1231).

pytanie o możliwość naruszenia wizerunku jedynie poprzez jego utrwalenie bez zgody jego posiadacza (bez dodatkowego jego rozpowszechniania) i wystąpienie w takiej sytuacji z roszczeniami przewidzianymi w art. 24 k.c. Kodeks cywilny nie udziela jednoznacznej odpowiedzi na takie pytanie. Wydaje się zatem, że okoliczności utrwalenia wizerunku należy poddać każdorazowej ocenie w kontekście ewentualnej odpowiedzialności cywilnej. Nie ulega raczej wątpliwości, że utrwalenie wizerunku osoby w sytuacji krępującej, intymnej, np. w formie fotografii, nawet nierozpowszechnione, naruszać może dobro osobiste człowieka. Inaczej natomiast należy ocenić utrwalenie wizerunku w formie rodzinnej fotografii umieszczonej następnie w rodzinnym albumie, nawet bez uzyskania wyraźnej zgody na takie utrwalenie.

Warto także wspomnieć, że bezprawność naruszenia dobra osobistego w postaci wizerunku wyłączona będzie również poprzez działanie w oparciu o przepisy art. 279 i art. 280 ustawy z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego, dotyczące możliwości wydania listu gończego za oskarżonym, w stosunku do którego wydano postanowienie o tymczasowym aresztowaniu i który ukrywa się[23]. W myśl art. 280 § 1 pkt 2 k.p.k. list gończy powinien zawierać m.in. dane o osobie, które mogą ułatwić jej poszukiwanie, a przede wszystkim personalia, rysopis, znaki szczególne, miejsce zamieszkania i pracy, z dołączeniem w miarę możliwości fotografii poszukiwanego. Nie ulega wątpliwości, że w przypadku poszukiwania listem gończym rozpowszechnianie wizerunku oskarżonego nie będzie stanowić naruszenia jego dobra osobistego. Warto zaznaczyć, że publikacja listów gończych odbywa się obecnie przede wszystkim na stronach internetowych organów ścigania, rzadziej na portalach internetowych innych podmiotów lub w tradycyjnej prasie. Gdyby jednak list gończy zawierający publikację wizerunku oskarżonego nie został z takiej strony internetowej usunięty już po uchyleniu listu gończego, wówczas w istocie nastąpi naruszenie prawa do wizerunku oskarżonego[24].

Wspomnieć należy także o przepisach ustawy z dnia 26 stycznia 1984 roku – Prawo prasowe, które co do zasady wyłączają możliwość publikowania w prasie wizerunku i innych danych osobowych osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe, jak również wizerunku i innych danych osobowych świadków, pokrzywdzonych i poszkodowanych, chyba że osoby te wyrażą na to zgodę (art. 13 ust. 2)[25]. Wyjątek od tej zasady istnieje wyłącznie wówczas, gdy właściwy prokurator lub sąd zezwoli, ze względu na ważny interes społeczny, na ujawnienie wizerunku i innych danych osobowych osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe (art. 13 ust. 3).

---

[23] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2020 r., poz. 30) (dalej jako: k.p.k.).

[24] Podobnie: wyrok Sądu Apelacyjnego w Gdańsku Wydział I Cywilny z dnia 5 grudnia 2012 roku, sygn. akt I ACa 626/12, http://orzeczenia.gdansk.sa.gov.pl/content/$N/151000000000503_I_ACa_000626_2012_Uz_2012-12-05_001 (dostęp: 6.09.2020 r.).

[25] Ustawa z dnia 26 stycznia 1984 roku – Prawo prasowe (t.j. Dz.U. z 2018 r., poz. 1914 ze zm.).

Należy podkreślić, powołując stanowisko Sądu Najwyższego, że przez pojęcie prasy rozumieć należy także publikacje rozpowszechniane za pomocą Internetu, jeżeli spełniają one wymagania określone w art. 7 ust. 2 ustawy z 1984 r. – Prawo prasowe. Dotyczy to nie tylko sytuacji, gdy internetowej publikacji towarzyszy publikacja tradycyjna, drukowana, stanowiąca inną, elektroniczną jej postać online, ale także przypadków, gdy istnieje tylko publikacja w formie elektronicznej, ale zachowuje cechy prasy: określoną periodyczność, nie tworzy zamkniętej, jednorodnej całości, ma stały tytuł (nazwę), kolejny numer i datę. Chodzi tu o regularnie rozpowszechniane za pomocą Internetu biuletyny, serwisy i inne periodyki”[26].

Wobec tego można stwierdzić, że określone na gruncie art. 13 ustawy Prawo prasowe regulacje dotyczące możliwości publikacji w prasie wizerunku osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe, dotyczą także publikacji ukazujących się w Internecie.

Jeżeli chodzi o roszczenia, z którymi wystąpić może osoba, której prawo do wizerunku zostało naruszone, także przez publikacje ukazujące się w sieci, to przewidziane zostały one na gruncie art. 24 k.c. W myśl jego § 1 ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności, ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. Ponadto, zgodnie z postanowieniami art. 24 § 2 k.c., jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

Wyżej powołane przepisy przyznają zatem możliwość osobie poszkodowanej wystąpienia z pięcioma rodzajami roszczeń: o ustalenie, o zaniechanie naruszeń, o usunięcie skutków naruszenia, o zadośćuczynienie i o zapłatę sumy na cel społeczny, dla dochodzenia dwóch ostatnich wymagana jest dodatkowo przesłanka winy podmiotu dokonującego naruszenia[27]. W doktrynie podnosi się, że możliwa pozostaje kumulacja roszczenia o zadośćuczynienie z niemajątkowymi środkami ochrony. Możliwa jest też kumulacja zadośćuczynienia z roszczeniem odszkodowawczym o wynagrodzenie szkody majątkowej[28]. Ponadto, zgodnie z art. 24 § 3 k.c. przepisy § 1 i 2 nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym. Wydaje się, że roszczenia określone na gruncie kodeksu cywilnego oraz ustawy o prawie

---

[26] Wyrok Sądu Najwyższego z dnia 24 czerwca 2014 roku, sygn. akt I CSK 532/13, LEX nr 1540023, System Informacji Prawnej „LEX” (dostęp: 6.09.2020 r.).

[27] A. Kidyba (red.), *Kodeks cywilny. Komentarz*, t. I: *Część ogólna*, wyd. II, Warszawa 2012, System Informacji Prawnej „LEX” (dostęp: 6.09.2020 r.).

[28] K. Pietrzykowski (red.), *Kodeks cywilny*.., s. 170.

autorskim i prawach pokrewnych, w zależności od ich rodzaju, mogą mieć charakter alternatywny (np. roszczenie o zadośćuczynienie pieniężne oparte na przepisach kodeksu cywilnego i ustawy o prawie autorskim) bądź charakter kumulatywny (np. zadośćuczynienie, przeproszenie i odszkodowanie za wyrządzoną szkodę majątkową), choć poglądy doktryny w tym zakresie nie są jednolite[29].

Odrębną regulacją z zakresu ochrony wizerunku, także odnoszącą się do ochrony wizerunku w sieci, która została już wspomniana w powyższych rozwiązaniach, stanowiącą alternatywę, czy też uzupełnienie dla przepisów kodeksu cywilnego, są przepisy art. 81 ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych. Regulacja ta odnosi się do zasad rozpowszechniania wizerunku, nie odnosząc się natomiast do kwestii samego utrwalania wizerunku i jego dopuszczalności. W myśl art. 81 ust. 1 wyżej powołanej ustawy rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. Nie licząc wyjątków określonych w kolejnych przepisach niniejszego artykułu, w zasadzie zawsze rozpowszechnianie cudzego wizerunku, także w Internecie, wymaga zgody osoby, której wizerunek ma być rozpowszechniony.

Pojawia się rzecz jasna pytanie o definicję rozpowszechniania wizerunku, której ustawodawca nie określił na gruncie art. 81. Definicja utworu rozpowszechnionego została natomiast przedstawiona w przepisach art. 6 pkt 3 ustawy, w myśl którego utworem rozpowszechnionym jest utwór, który za zezwoleniem twórcy został w jakikolwiek sposób udostępniony publicznie. Należy więc stosować tę definicję analogicznie w zakresie terminu „rozpowszechnianie wizerunku". Zatem wywołanie fotografii przedstawiającej wizerunek danej osoby i umieszczenie jej w rodzinnym albumie, nie będzie wykazywało cech rozpowszechnienia. Z kolei umieszczenie fotografii/obrazu w galerii sztuki, czy też wyemitowanie nagrania w telewizji, z pewnością stanowić będzie rozpowszechnienie wizerunku w rozumieniu ustawy o prawie autorskim i prawach pokrewnych. Jeśli chodzi o rozpowszechnianie wizerunku w Internecie, to z pewnością większość sytuacji, w których wizerunek danej osoby (zwykle fotografia w formie cyfrowej) umieszczany jest na stronach internetowych różnych portali (społecznościowych, informacyjnych, rozrywkowych), z racji specyfiki tego medium stanowić będzie jego rozpowszechnienie. Zaznaczyć należy, podążając za stanowiskiem Sądu Apelacyjnego w Krakowie, wyrażonym w wyroku z dnia 20 lipca 2004 roku (sygn. akt ACa 564/04), iż za rozpowszechnianie wizerunku uznać należy zamieszczenie na stronie portalu internetowego tzw. głębokiego linku (*deep link*) umożliwiającego użytkownikom tego portalu bezpośrednie (tj. z pominięciem struktury nawigacyjnej strony głównej innego portalu) otwarcie rekomendowanej witryny, na której znajdowało się zdjęcie powódki[30].

---

[29] Tamże, s. 171.

[30] https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/i-aca-564-04-wyrok-sadu-apelacyjnego-w-krakowie-520235834 (dostęp: 7.09.2020 r.).

Zaznaczyć należy, że dobrem chronionym na gruncie art. 81 ustawy o prawie autorskim i prawach pokrewnych jest autonomia każdej osoby w zakresie swobodnego rozstrzygania, czy i w jakich okolicznościach jej wizerunek może być rozpowszechniony[31].

Ogólną zasadą wyrażoną na gruncie art. 81 ust. 1 ustawy o prawie autorskim i prawach pokrewnych jest zasada, że rozpowszechnienie wizerunku wymaga zgody osoby na niej przedstawionej. W orzecznictwie panuje raczej zgodny pogląd, iż zgoda na rozpowszechnianie wizerunku nie może być abstrakcyjna i musi być niewątpliwa, czyli osoba jej udzielająca musi mieć pełną świadomość formy przedstawienia wizerunku, miejsca i czasu publikacji, zestawienia z innymi wizerunkami i towarzyszącego komentarza[32]. Zgoda osoby na rozpowszechnianie jej wizerunku w mediach musi zostać udzielona wyraźnie i nie może być domniemywana. Musi być udzielona wprost oraz w sposób niewątpliwy. Powinna określać warunki i płaszczyzny dopuszczalnego wykorzystania wizerunku. Zgodę można wyrazić też ustnie, jednak okoliczność jej udzielenia musi wówczas zostać wykazana na podstawie dowodów[33].

Rozpowszechnianie wizerunku w sieci, jeżeli nie obejmuje wyjątków, o których będzie mowa poniżej, każdorazowo powinno zatem być poprzedzone uzyskaniem wyraźnej zgody osoby przedstawianej. Oczywiście, z punktu widzenia ewentualnego postępowania sądowego i kwestii dowodowych, pożądane byłoby odebranie zgody na piśmie, choć nie zawsze jest to możliwe, czy zwyczajowo przyjęte w danych warunkach. Słusznie podnosi się w literaturze przedmiotu, że prawo do decydowania o rozpowszechnianiu wizerunku nie ulega wyczerpaniu z chwilą pierwszego udostępnienia wizerunku publiczności, a o każdym kolejnym udostępnieniu wizerunku w innych okolicznościach, który już raz za odpowiednią zgodą został rozpowszechniony, każdorazowo wymaga zgody osoby przedstawionej[34]. W świetle tego poglądu za chybione należy zatem uznać stanowisko Sądu Najwyższego, zawarte w wyroku z 2 lutego 1967 roku (sygn. akt I CR 496/66) zgodnie z którym dalsza publikacja fotografii określonej osoby jest dopuszczalna bez jej zgody, pod warunkiem wskazania pierwotnego źródła publikacji i bez wprowadzania zmian w publikowanym zdjęciu[35]. W wyroku tym Sąd Najwyższy do kwestii rozpowszechniania wizerunku zastosował zasady regulujące korzystanie z utworu w ramach tzw. dozwolonego użytku, do czego brak jest normatywnych podstaw. Wobec powyższych twierdzeń uznać należy, że co do zasady tak popularna w dzisiejszych czasach każdorazowa publikacja np. na portalach społecznościowych wizerunków osób trzecich, które nie są częścią większej całości,

---

[31] J. Barta, R. Markiewicz (red.), *Ustawa o prawie autorskim…*

[32] Wyrok Sądu Apelacyjnego w Gdańsku z dnia 29 października 2018 roku, sygn. akt V ACa 829/17, LEX nr 269034, System Informacji Prawnej „LEX" (dostęp: 7.09.2020 r.).

[33] Wyrok Sądu Apelacyjnego w Warszawie z dnia 3 października 2018 roku, sygn. akt V ACa 655/17, LEX nr 2581117, System Informacji Prawnej „LEX" (dostęp: 7.09.2020 r.).

[34] W Machała, R.M. Sarbiński (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Warszawa 2019, System Informacji Prawnej „LEX" (dostęp: 7.09.2020 r.).

[35] LEX nr 561, System Informacji Prawnej „LEX" (dostęp: 7.09.2020 r.).

powinna być poprzedzona uzyskaniem ich wyraźnej zgody. Ponadto, raz udzielona zgoda na rozpowszechnienie wizerunku w danych okolicznościach (np. na profilu przedsiębiorcy w ramach portalu społecznościowego w celach reklamowych), nie daje przyzwolenia na dalsze rozpowszechnianie wizerunku w innych okolicznościach i na innych zasadach.

Tak jak wspomniano powyżej, ustawa o prawie autorskim i prawach pokrewnych przewiduje wyjątki od zasady, iż rozpowszechnienie wizerunku wymaga zgody osoby na nim przedstawionej. Te wyjątki określono na gruncie art. 81 ust. 2 ustawy, w myśl którego zezwolenia nie wymaga rozpowszechnianie wizerunku: 1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych; 2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza. Ponadto, w art. 81 ust. 1 zastrzeżono, że w braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. W tym ostatnim przypadku wyobrazić można sobie sytuację, kiedy od osoby pozującej do portretu, fotografii czy rzeźby, po uiszczeniu umówionej na jej rzecz zapłaty, nie wymaga się co do zasady zgody na rozpowszechnienie wizerunku i umieszczenie elektronicznych zapisów takich wizerunków w sieci. Jeżeli jednak osoba pozująca wyraźnie zastrzegła, że pomimo zapłaty nie godzi się na rozpowszechnianie jej wizerunku, wówczas zaprezentowane powyżej domniemanie nie obowiązuje. Warto jednak zaznaczyć, że w orzecznictwie uznaje się, iż przyjęcie umówionej zapłaty za pozowanie nie wyłącza możliwości dochodzenia przez osobę przedstawioną roszczeń na podstawie art. 23 i 24 k.c., jeśli na skutek publikacji wizerunku doszło do naruszenia innych dóbr osobistych, takich jak np. godność, cześć lub dobre imię[36].

Jeżeli chodzi z kolei o wyłączenie potrzeby uzyskiwania zgody na rozpowszechnianie wizerunku osób powszechnienie znanych, to możliwe jest to wyłącznie w sytuacji, kiedy wizerunek wykonano w związku z pełnieniem przez takie osoby funkcji publicznych, w szczególności politycznych, społecznych, zawodowych. Ustawodawca nie wskazuje legalnej definicji „osoby powszechnie znanej", jednak w doktrynie podnosi się, że przy ustaleniu, czy dana osoba jest powszechnienie znana, istotne znaczenie ma sprawowanie przez nią funkcji politycznych lub społecznych, popularność osiągana poza własnym środowiskiem ze względu na prowadzoną działalność zawodową, amatorską, hobbystyczną, sportową. Nie ma znaczenia rodzaj działalności, który spowodował, że osoba stała się powszechnie znana[37]. Słusznie podnosi się także w literaturze tematu, że człowiek może się stać osobą powszechnie znaną poprzez swoją działalność społeczną, naukową, polityczną, literacką, a także przez swoje życie prywatne[38]. Nie ulega wątpliwości,

[36] Wyrok Sądu Apelacyjnego w Warszawie z dnia 20 czerwca 2002 roku, sygn. akt I ACa 1358/01, LEX nr 111366, System Informacji Prawnej „LEX (dostęp: 7.09.2020 r.).
[37] K. Stefaniuk, *Naruszenie prawa do wizerunku…*, s. 71.
[38] J. Sieńczyło-Chlabicz, *Rozpowszechnianie wizerunku osób…*, s. 41.

że w obecnych czasach, wiele osób, które nie prezentują na zewnątrz swoich działań zawodowych, naukowych czy politycznych, ale właśnie swoją prywatność, szczególnie w sieci, zyskuje status osób powszechnie znanych (np. tzw. youtuberzy).

Brak wymogu uzyskania zgody wyżej określonych osób na rozpowszechnienie wizerunku dotyczyć będzie wyłącznie sytuacji, gdy wizerunek wykonano w związku z pełnieniem przez nie funkcji publicznych, w szczególności politycznych, społecznych, zawodowych. Poza tym, co nie wynika wprost z przepisu ustawy, jednak podnoszone jest w doktrynie, wykorzystanie takiego wizerunku powinno być związane z przedstawianiem (relacjonowaniem) wykonywania przez portretowanego funkcji zawodowych, społecznych lub politycznych. Wyłącza to zatem możliwość wykorzystywania bez zgody zainteresowanego jego wizerunku m.in. na pocztówkach, w kalendarzach czy w działalności reklamowej[39]. Wobec wyżej zaprezentowanych poglądów jasne jest, że utrwalone wizerunki osób powszechnie znanych mogą być rozpowszechniane w sieci bez konieczności uzyskania ich zgody, wyłącznie w kontekście wykonywania przez nich funkcji, w związku z którymi wizerunki te zostały utrwalone. Wykluczone jest zatem np. posłużenie się fotografią znanego sportowca bez jego zgody wykonaną w trakcie zawodów nie w celach informacyjnych (np. w serwisie internetowym o charakterze informacyjnym), ale w kampanii reklamowej producenta odzieży sportowej. Nie ulega także wątpliwości, że utrwalanie wizerunków osób powszechnie znanych, jednak w sytuacjach prywatnych i ich rozpowszechnianie bez zgody osób na nich przedstawionych, wykracza poza dozwolone ramy określone w art. 81 ust. 2 ustawy o prawie autorskim i prawach pokrewnych. Zatem publikacje na internetowych portalach plotkarskich zdjęć z wizerunkiem znanych polityków, wykonanych z ukrycia np. w trakcie prywatnych uroczystości, uznać należy za naruszające wyżej powołane przepisy ustawy o prawie autorskim i prawach pokrewnych.

W końcu dopuszczalne jest, w świetle obowiązujących przepisów prawa autorskiego, rozpowszechnianie wizerunku osoby stanowiącej jedynie szczegół jakiejś całości, takiej jak zgromadzenie, krajobraz, publiczna impreza, bez uzyskania zgody tej osoby. Zwykle tego typu sytuacje będą miały miejsce w przypadku publikacji fotografii lub nagrań ukazujących relacje/ujęcia z imprez masowych, zgromadzeń, uroczystości religijnych, na których wizerunek danej osoby jest jedynie elementem całości. Takie relacje pojawiają się zwykle w tradycyjnej prasie, telewizji, jak również sieci Internet, na różnego rodzajach serwisach informacyjnych. Słusznie podnosi Sąd Apelacyjny we Wrocławiu, że dla zastosowania art. 81 ust. 2 ustawy o prawie autorskim i prawach pokrewnych rozstrzygające znaczenie ma ustalenie w strukturze przedstawienia relacji między wizerunkiem osoby domagającej się ochrony a pozostałymi elementami jego treści. Co za tym idzie – rozpowszechnianie wizerunku nie wymaga zezwolenia, jeśli stanowi on jedynie element akcydentalny lub akcesoryjny przedstawionej całości,

[39] J. Barta, R. Markiewicz (red.), *Ustawa o prawie autorskim*…

tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia[40].

Zwykle celem takich publikacji jest nie przedstawienie wizerunku konkretnej osoby, ale udokumentowane pewnego zdarzenia o charakterze społecznym czy politycznym. Pewien problem stanowić mogą natomiast takie utrwalenia wizerunków, które co prawda dotyczą wydarzeń o charakterze masowym i w ich trakcie zostały wykonane, ale jednak kluczowy jest właśnie ten wizerunek konkretnej osoby, natychmiast przykuwający wzrok odbiorcy. Wydaje się, że każdorazowo takie utrwalenie i rozpowszechnienie wizerunku (zwykle w formie fotografii), oceniać należy przez pryzmat jego relacji do całości prezentowanego w mediach materiału. Jeżeli takie utrwalenie wizerunku stanowi jedno z wielu prezentowanych ujęć przedstawiających w sposób szeroki dane wydarzenie, to raczej trudno traktować je jako naruszające normy art. 82 ust. 1 ustawy o prawie autorskim i prawach pokrewnych. Jeśli zaś stanowi główny element takie relacji, to trudno mówić w takim przypadku o wyjątku od zasady określonej w wyżej wymienionym przepisie. Wówczas konieczne jest uzyskanie zgody osoby, której wizerunek rozpowszechniono.

Jeśli chodzi natomiast o roszczenia, jakie na gruncie ustawy o prawie autorskim i prawach pokrewnych przysługują w związku z naruszeniem prawa do rozpowszechniania wizerunku (tj. rozpowszechnienia bez wymaganej w danych okolicznościach zgody), to art. 83 tejże ustawy odsyła do art. 78 ust. 1. W takiej sytuacji należy uznać, że osoba, której wizerunek został rozpowszechniony wbrew zasadom określonym w art. 81 ustawy o prawie autorskim i prawach pokrewnych może żądać zaniechania tego działania. W razie dokonanego naruszenia może także żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności aby złożyła publiczne oświadczenie o odpowiedniej treści i formie. Z kolei jeżeli naruszenie było zawinione, sąd może przyznać twórcy odpowiednią sumę pieniężną tytułem zadośćuczynienia za doznaną krzywdę lub – na żądanie twórcy – zobowiązać sprawcę, aby uiścił odpowiednią sumę pieniężną na wskazany przez twórcę cel społeczny. Tak jak wskazano już w niniejszej publikacji, w pewnych sytuacjach możliwy będzie zbieg wyżej wymienionych roszczeń z roszczeniami określonymi na gruncie art. 24 k.c. Chodzi o przypadki, kiedy bezprawne rozpowszechnianie wizerunku danej osoby stanowić będzie jednocześnie naruszenie jej dóbr osobistych chronionych właśnie na gruncie prawa cywilnego.

Wskazać w końcu należy, że wizerunek chronią również przepisy ustawy z dnia 6 czerwca 1997 roku – Kodeks karny, aczkolwiek w nieco węższym zakresie niż przepisy prawa cywilnego czy autorskiego[41]. Penalizacja zachować godzących w to dobro osobiste nastąpiła na gruncie rozdziału XXIII k.k., dotyczącego

---

[40] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 30 stycznia 2014 roku, sygn. akt I ACa 1452/13, LEX nr 1425612, System Informacji Prawnej „LEX" (dostęp: 7.09.2020 r.).

[41] Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny (t.j. Dz.U. z 2020 r., poz. 1444) (dalej jako: k.k.).

przestępstw przeciwko wolności. Ochrona wizerunku przewidziana został po pierwsze w art. 190a § 2 k.k. Warto wskazać, że przepisy art. 190a zostały dodane przez art. 1 pkt 2 ustawy z 25 lutego 2011 r. o zmianie ustawy – Kodeks karny (Dz.U. poz. 381), która weszła w życie 6 czerwca 2011 roku. Nie ulega wątpliwości, że nowy typ przestępstwa związany jest także z postępem technologicznym, w tym powszechnym dostępem do sieci Internet, która niejednokrotnie staje się również sferą występowania zachowań przestępczych.

Art. 190a § 1 k.k. dotyczy przestępstwa uporczywego nękania (tzw. *stalkingu*), a karą za niego przewidzianą jest kara pozbawienia wolności od 6 miesięcy do lat 8. Z kolei, zgodnie z przepisami art. 190a § 2 k.k. tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej. W przepisie § 2 kryminalizowane jest zatem podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub innych jej danych osobowych albo innych danych, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej. Penalizowane będzie w ten sposób zjawisko „przywłaszczenia" tożsamości pokrzywdzonego[42]. Przepis art. 190a § 2 k.k. przewiduje dwie czynności sprawcze. Pierwsza – to podszywanie się pod inną osobę, a więc udawanie innej osoby, wprowadzanie w błąd otoczenia co do swojej tożsamości, podawanie się za kogoś innego. Druga polega na wykorzystywaniu wizerunku lub innych danych osobowych, a więc robieniu użytku z tych danych[43]. Z kolei w art. 190a § 3 k.k. określono przestępstwo kwalifikowane ze względu na skutek, jakim jest targnięcie się pokrzywdzonego na własne życie. Do wyczerpania znamion tego czynu dochodzi także wówczas, gdy próba samobójcza nie zakończyła się śmiercią pokrzywdzonego. Jeżeli chodzi o stronę podmiotową przestępstwa z art. 190a § 2 k.k., to odpowiedzialności za ten czyn podlega sprawca działający w zamiarze bezpośrednim kierunkowym – mający na celu wyrządzenie innej osobie szkody majątkowej lub osobistej. Jeżeli sprawcy nie przyświeca osiągnięcie tego celu, jego zachowanie nie jest kryminalizowane[44]. Wówczas pozostaje możliwość ewentualnej ochrony na gruncie przepisów kodeksu cywilnego czy ustawy o prawie autorskim i prawach pokrewnych. Wydaje się, że znamiona przestępstwa z art. 190a § 2 k.k. wypełniać będzie w szczególności zachowanie polegające np. na założeniu konta na portalu społecznościowym jako inna osoba, z wykorzystaniem wizerunku tej innej osoby (przede wszystkim utrwalonym na fotografii) w celu podszycia się pod tą osobę, aby wyrządzić jej szkodę osobistą, np. ośmieszyć czy upokorzyć w oczach osób trzecich. W takiej sytuacji osoba pokrzywdzona może skorzystać

---

[42] M. Budyn-Kulig i in., *Kodeks karny. Komentarz aktualizowany*, System Informacji Prawnej „LEX" (dostęp: 8.09.2020 r.).

[43] V. Konarska-Wrzosek (red.), *Kodeks karny. Komentarz*, wyd. II, Warszawa 2018, System Informacji Prawnej „LEX" (dostęp: 8.09.2020 r.).

[44] J. Giezek (red.), *Kodeks karny. Część szczególna. Komentarz*, System Informacji Prawnej „LEX" (dostęp: 8.09.2020 r.).

z ochrony gwarantowanej na gruncie wspomnianego wyżej przepisu kodeksu karnego, ale również kodeksu cywilnego (nie ulega wątpliwości, że sprawca naruszył jej dobra osobiste), czy ustawy o prawie autorskim i prawach pokrewnych (doszło do bezprawnego rozpowszechnienia wizerunku).

Wspomnieć należy równie o przepisach art. 191a § 1 k.k., ważnego z punktu widzenia ochrony wizerunku, w myśl którego: kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Powołany wyżej przepis określa zatem dwa penalizowane typy zachowań. Typ pierwszy to utrwalanie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej, z użyciem w tym celu przemocy, groźby bezprawnej lub podstępu. Typ drugi to rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody[45]. Zauważyć należy, że dobrem atakowanym w przypadku typu pierwszego będzie, jak podnosi się w doktrynie, wolność osoby od znoszenia stanu spowodowanego zachowaniem drugiej osoby używającej przemocy, groźby bezprawnej lub podstępu godzącego rażąco w sferę życia prywatnego i intymnego. W wypadku typu drugiego przedmiotem ataku jest wolność do dysponowania swoim wizerunkiem, w szczególności gdy jego rozpowszechnienie godzi rażąco w sferę życia prywatnego i intymnego[46]. Nie ulega wątpliwości, że drugi typ czynności przestępczej jest obecnie bardzo często realizowany właśnie poprzez rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody właśnie w sieci Internet. To niestety to medium komunikacyjne daje możliwość łatwego i powszechnego dostępu do zamieszczonych w nim plików znacznej liczbie osób, co niestety w przypadku działań przestępczych jest jednym z celów. Tę prawidłowość zauważył również Sąd Najwyższy, który w swoim wyroku z dnia 13 kwietnia 2016 roku stwierdził, że rozpowszechnianie wizerunku stanowiące znamię przestępstwa z art. 191a k.k. w praktyce wyłącznie następuje za pomocą mediów elektronicznych, co samo w sobie w najmniejszym stopniu nie obniża stopnia szkodliwości społecznej takiego czynu[47].

## Podsumowanie

Wobec wyżej zaprezentowanych rozwiązań uznać należy, że w polskim porządku prawnym przewidziano stosunkowo szeroką ochronę wizerunku, tratowanego przede wszystkim jako jedno z najważniejszych dóbr osobistych człowieka. Coraz większy postęp technologiczny, a przede wszystkim powszechny dostęp do

[45] W. Wróbel, A Zoll (red.), *Kodeks karny. Część szczególna*, t. II, cz. I: *Komentarz do art. 117–221a*, Warszawa 2017, System Informacji Prawnej „LEX" (dostęp na dzień 8.09.2020 r.).

[46] Tamże.

[47] Wyrok Sądu Najwyższego z dnia 13 kwietnia 2016 roku, sygn. akt II KK 304/15, LEX nr 2019608, System Informacji Prawnej „LEX" (dostęp: 8.09.2020 r.).

Internetu, spowodowały pojawienie się nowych możliwości w zakresie rozpowszechniania wizerunku, w szczególności tego utrwalonego na cyfrowych fotografiach czy nagraniach audiowizualnych. Wykorzystanie wizerunku w sieci dokonywane jest zwykle w celach informacyjnych, edukacyjnych, naukowych, rozrywkowych, czy zarobkowych. Jeżeli odbywa się ono zgodnie z obowiązującymi normami prawnymi, to nawet, mimo iż czasem zadziwia czy szokuje, jest wyłączną sprawą osoby, której wizerunek utrwalono i rozpowszechniono. Niestety, bardzo często posłużenie się cudzym wizerunkiem w Internecie odbywa się z naruszeniem obowiązujących reguł prawnych, a nawet przybiera charakter przestępczy. Wydaje się, że zagrożenie tego typu działaniami nie wynika natomiast z niedostatecznych rozwiązań systemowych, ale często z niewiedzy, niefrasobliwości i nieświadomości dużej części społeczeństwa w zakresie możliwości i zasad ochrony wizerunku.

Jak wskazano w niniejszym rozdziale, wizerunek chroniony jest przede wszystkim na gruncie przepisów prawa cywilnego, prawa autorskiego, jak również prawa karnego. O ile przepisy kodeksu cywilnego przewidują ochronę wizerunku jako dobra osobistego człowieka nie zawężając jej do ściśle określonych sytuacji i umożliwiając tym samym sięganie po tę ochronę także w sytuacji samego utrwalenia wizerunku, które narusza chociażby dobre imię przedstawionej osoby, o tyle przepisy ustawy o prawie autorskim i prawach pokrewnych dotyczą wyłącznie sytuacji bezprawnego rozpowszechniania wizerunku, co w zasadzie oznacza rozpowszechnianie go bez zgody przedstawianej osoby. Biorąc pod uwagę wizerunek przedstawiany w sieci, najczęściej to właśnie przepisy z zakresu prawa autorskiego stanowić będą podstawę roszczeń kierowanych w stosunku do osób bezprawnie rozpowszechniających cudzą podobiznę, choć jak podnoszono w publikacji, niewykluczony jest ich zbieg z roszczeniami określonymi na gruncie art. 24 k.c. W końcu zaznaczyć należy, że pewne zachowania dotyczące bezprawnego wykorzystania cudzego wizerunku, nierzadko szokujące i wkraczające dodatkowo w najbardziej intymną sferę człowieka, zostały spenalizowane i określone na gruncie art. 190a i art. 191a k.k. Warto zaznaczyć, że odpowiedzialność karna sprawców takich przestępstw nie wyklucza pociągnięcia ich również do odpowiedzialności cywilnej.

Reasumując, w dobie powszechnego dostępu do Internetu, który stał się codziennym narzędziem pracy, jak i rozrywki, a często – niestety – miejscem występowania wielu nadużyć, wiedza w zakresie własnych uprawnień i obowiązków dotyczących zasad wykorzystywania wizerunku oraz sposobu ich egzekwowania jest kluczowa, by uniknąć ewentualnej nieuczciwości w tej sferze ze strony osób trzecich, czy też nie narazić siebie na odpowiedzialność w tym zakresie. Warto także dodać, że z racji specyfiki tego medium, nierozważne udostępnianie wizerunku w sieci, powodować będzie zwykle bardziej dotkliwe i długofalowe skutki, niż w przypadku innych środków masowego przekazu.

# Bibliografia

Barta J., Czajkowska-Dąbrowska M., Ćwiąkalski Z., Markiewicz R., Traple E., *Prawa autorskie i prawa pokrewne. Komentarz*, Kraków 2005.

Barta J., Markiewicz R. (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, wyd. V, Warszawa 2011, System Informacji Prawnej „LEX".

Barta M., Markiewicz R., *Wokół prawa do wizerunku* [w:] *Zagadnienia prawa własności intelektualnej. Profesorowi Stefanowi Grzybowskiemu pracownicy Instytutu Wynalazczości i Ochrony Własności Intelektualnej w darze*, Kraków 2002.

Budyn-Kulig M. i in., *Kodeks karny. Komentarz aktualizowany*, System Informacji Prawnej „LEX".

Ciszewski J., Nazaruk P. (red.), *Kodeks cywilny. Komentarz*, Warszawa 2019, System Informacji Prawnej „LEX".

Flisak D. (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, system Informacji Prawnej „LEX".

Fraus M., Habdas M. (red.), *Kodeks cywilny. Tom I. Część ogólna (art. 1–125)*, Warszawa 2018, System Informacji Prawnej „LEX".

Giezek J. (red.), *Kodeks karny. Część szczególna. Komentarz*, System Informacji Prawnej „LEX".

Grzeszczak T. [w:] J. Barta (red.), *Prawo autorskie. System Prawa Prywatnego. Tom 13*, Warszawa 2017.

Kidyba A. (red.), *Kodeks cywilny. Komentarz. Tom I. Część ogólna*, wyd. II, Warszawa 2012, System Informacji Prawnej „LEX".

Konarska-Wrzosek V. (red.), *Kodeks karny. Komentarz*, wyd. II, Warszawa 2018, System Informacji Prawnej „LEX".

Machała W., Sarbiński R.M. (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Warszawa 2019, System Informacji Prawnej „LEX".

Modrzejewski P., *Odpowiedzialność innych podmiotów niż sprawca za naruszenie dóbr osobistych w Internecie*, „Przegląd Prawa Handlowego" 2017, nr 3.

Pietrzykowski K. (red.), *Kodeks cywilny. Tom I. Komentarz do art. 1–449[1]*, wyd. 6, Warszawa 2011.

Sieńczyło-Chlabicz J. (red.), *Prawo własności intelektualnej*, wyd. 1, Warszawa 2009.

Sieńczyło-Chlabicz J., *Rozpowszechnianie wizerunku osób powszechnie znanych*, „Przegląd Prawa Handlowego" 2003, nr 9.

Stefaniuk K., *Naruszenie prawa do wizerunku przez rozpowszechnianie podobizny*, „Państwo i Prawo" 1970, nr 1.

Wróbel W., Zoll A. (red.), *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–221a*, Warszawa 2017, System Informacji Prawnej „LEX".

# Prawodawstwo

Ustawa z dnia 23 kwietnia 1964 roku – Kodeks cywilny (Dz.U. z 2019 r., poz. 1145 ze zm.).

Ustawa z dnia 26 stycznia 1984 roku – Prawo prasowe (tekst jedn. Dz.U. z 2018 r., poz. 1914 ze zm.).

Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (tekst jedn. Dz.U. z 2019 r., poz. 1231).

Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny (tekst jedn. Dz.U. z 2020 r., poz. 1444).

Ustawa z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego (tekst jedn. Dz.U. z 2020 r., poz. 30).

# Orzecznictwo

Wyrok Sądu Najwyższego wyroku z 2 lutego 1967 roku, sygnatura akt I CR 496/66, LEX nr 561, System Informacji Prawnej „LEX".

Wyrok Sądu Najwyższego z dnia 24 czerwca 2014 roku, sygn. akt I CSK 532/13, LEX nr 1540023, System Informacji Prawnej „LEX".

Wyrok Sądu Najwyższego z dnia 13 kwietnia 2016 roku, sygn. akt II KK 304/15, LEX nr 2019608, System Informacji Prawnej „LEX".

Wyrok Sądu Apelacyjnego w Warszawie z dnia 20 czerwca 2002 roku, sygnatura akt I ACa 1358/01, LEX nr 111366, System Informacji Prawnej „LEX".

Wyrok z dnia 20 lipca 2004 roku Sądu Apelacyjnego w Krakowie, sygn. akt ACa 564/04 https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/i-aca-564-04-wyrok-sadu-apelacyjnego-w-krakowie-520235834.

Wyrok Sądu Apelacyjnego w Gdańsku Wydział I Cywilny z dnia 5 grudnia 2012 roku, sygn. akt I ACa 626/12 http://orzeczenia.gdansk.sa.gov.pl/content/$N/151000000000503_I_ACa_000626_2012_Uz_2012-12-05_001

Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 30 stycznia 2014 roku, sygn. akt I ACa 1452/13, LEX nr 1425612, System Informacji Prawnej „LEX".

Wyrok Sądu Apelacyjnego w Warszawie z dnia 7 maja 2014 roku, I ACa 1686/13 http://orzeczenia.waw.sa.gov.pl/content/$N/154500000000503_I_ACa_001686_2013_Uz_2014-05-07_002

Wyrok Sądu Apelacyjnego w Krakowie z dnia 19 kwietnia 2016 roku, sygn. akt I ACa 1826/15, LEX nr 2041781, System Informacji Prawnej „LEX" .

Wyrok Sądu Apelacyjnego w Warszawie z dnia 9 marca 2018 roku, sygn. akt VI ACa 1694/16, LEX nr 2524902, System Informacji Prawnej „LEX".

Wyrok Sądu Apelacyjnego w Warszawie z dnia 19 września 2018 roku, sygn. akt VI ACa 528/17, LEX nr 2616080, System Informacji Prawnej „LEX".

Wyrok Sądu Apelacyjnego w Warszawie z dnia 3 października 2018 roku, sygn. akt V ACa 655/17, LEX nr 2581117, System Informacji Prawnej „LEX".

Wyrok Sądu Apelacyjnego w Gdańsku z dnia 29 października 2018 roku, sygn. akt V ACa 829/17, LEX nr 269034, System Informacji Prawnej „LEX".

Wyrok Sądu Apelacyjnego w Warszawie z dnia 1 sierpnia 2019 roku, sygn. akt V ACa 501/18, LEX nr 2726845, System Informacji Prawnej „LEX".

# Netografia

https://sjp.pwn.pl/szukaj/wizerunek.html
https://www.wsjp.pl/index.php?id_hasla=11573&ind=0&w_szukaj=wizerunek

# PRAWNY ASPEKT POSTACI FIKCYJNYCH W GRACH MMORPG

(*Piotr Łosowski*)

## Wprowadzenie

Wraz z postępem technologicznym oraz rozwojem Internetu stają przed nami nowe wyzwania oraz zagadnienia, które są powodem do dyskusji i sporów w świetle doktryn prawa autorskiego. Do zagadnień budzących wiele pytań należy m.in. status prawny postaci świata wirtualnego. Temat ten jest bardzo aktualny nie tylko wśród graczy, ale również coraz częściej pojawia się na nagłówkach tytułów artykułów prasy codziennej.

W niniejszym rozdziale zostanie przedstawiona próba podsumowania obecnych poglądów na temat postaci wirtualnych oraz ich miejsca w prawie autorskim, zdefiniowanie pojęcia gry, wyjaśnienia, czym są gry MMORPG oraz ich krótka charakterystyka, omówienie wizerunku postaci fikcyjnych ze szczególnym uwzględnieniem ich istoty. Ponadto poruszono zagadnienie handlu kontami oraz przedmiotami wirtualnymi w odniesieniu do realnej sytuacji oraz prawnych aspektów takiego postępowania.

## Pojęcie gry komputerowej MMORPG

Zgodnie z powszechnymi przekonaniami gra oznacza czynność o wcześniej ustalonych zasadach, bierze w niej udział jedna lub więcej osób. Gra jest to rozgrywka o określonych regułach, do których każdy uczestnik musi się dostosować, w przeciwnym razie zostanie on wyeliminowany z grona uczestników rozgrywki. Jest to rozegranie, które posiada określony i ustalony wcześniej wachlarz zasad przebiegu gry, zapisane i wbudowane definicje sukcesu oraz porażki. To, z czym mamy do czynienia w grze, ma charakter wirtualny, posiada inny status niż świat rzeczywisty. Zbiór wszystkich zasad oraz reguł sprawia, że gra funkcjonuje i daje nam ujrzeć różnice od innych tego typu rozgrywek[1].

Mamy do czynienia z wieloma rodzajami gier, między innymi:

- akcji,
- RPG,

[1] R. Konarski, *Gra komputerowa jako przejaw wolności człowieka. Wybrane zagadnienia prawne*, Wrocław 2016, s. 16

- przygodowe,
- MMORPG.

Właśnie na tym ostatnim typie rozgrywek chcielibyśmy się skupić i przedstawić jej specyfikację. Jest to typ gry komputerowej w którym uczestniczy wielu graczy za pośrednictwem Internetu, zapewniania szeroki wachlarz interakcji między różnymi graczami wykraczające poza to co gwarantują nam zwykłe gry sieciowe. Dostęp do gier MMORPG najczęściej jest zapewniany przez twórcę gry[2]. Rozgrywki tego rodzaju są popularne na całym świecie. Gry MMORPG w większości przypadków są darmowymi tworami z ewentualnym dostępem do sklepu, który pozwala kupić wirtualne przedmioty za walutę w grze (oczywiście za prawdziwe pieniądze). Jednak gracz nie jest zmuszony do tego typu działań, może cieszyć się rozgrywką bez żadnych mikrotransakcji, aczkolwiek wykupienie wirtualnej waluty w grze pozwala graczowi zdobywać wyższe poziomy znacznie szybciej i daje możliwość cieszenia się z unikatowych przedmiotów, które potem mogą urosnąć do gigantycznych sum. Istnieją też gry MMORPG. które wymagają od nas konta premium. bez którego nie będziemy mogli uczestniczyć w rozgrywkach. Tego typu gier jest znacznie mniej niż tych darmowych, lecz cieszą się równie wysokim zainteresowaniem wśród graczy. Obecnie gry MMORPG uznaje się za podgrupę gier MMO, chociaż to właśnie MMORPG z tej grupy pojawiło się jako pierwsze.

Do najważniejszych cech tego typu rozgrywek należą:

- szeroka komunikacja,
- rozbudowany tryb walki, jednocześnie z wieloma graczami na różnych płaszczyznach,
- handel oraz szeroka ekonomia,
- proces rozwijania postaci, przyrost umiejętności oraz poziomu postaci poprzez zdobywanie punktów doświadczenia,
- system gildii i bractw do których gracze mogą dołączyć,
- admini, którzy prowadzą pracę nadzorcze na serwerami i graczami[3].

## Gra MMORPG a prawo własności wirtualnej

Twórcy pojęcia „postać fikcyjna” porównują świat wirtualny do świata realnego. Efektem tego działania jest przekonanie, że gracz rozgrywki MMORPG ma prawo nabywać struktury świata wirtualnego, takie jak np. odzież, obszary lądowe, domy, lądy czy też przedmioty potrzebne do funkcjonowania w danym świecie – na zasadach, które istnieją w świecie rzeczywistym, jednak w rzeczywistości owe elementy są wytworem graficznym umieszczonym w danej grze. Dlatego w grach typu MMORPG dokonywanie transakcji odbywa się poprzez wykorzystanie wirtualnego środka płatności. Efekty takich zakupów można zobaczyć w świecie

[2] E. Traple, *Wprowadzenie – gry komputerowe w świetle prawa*. Warszawa 2015, s. 12.
[3] Wikipedia Wolna encyklopedia, https://pl.wikipedia.org/wiki/MMORPG (dostęp: 06.05.2020 r.).

realnym, niektóre struktury wirtualnej rzeczywistości, takie jak np. broń, zbroja czy bardzo rzadki artefakt, często zostają sprzedawane na różnych aukcjach internetowych. Jeśli gracz odpowiednio się natrudzi, może zdobyć rzadki przedmiot, którego cena może osiągnąć nawet kilka tysięcy złotych. Przykładem może być postać fikcyjna w grze *World of Warcraft*, której cena osiągnęła 10 tys. USD[4]. Na samym szczycie, jeśli chodzi o rekordową sprzedaż rzeczy wirtualnej plasuje się gra *Entropia universe*, a konkretniej – chodzi o świat zwany *Planet Calypso.* Jest to pierwszy i najstarszy świat, w którym można zamieszkać w grze. W 2011 roku podjęto decyzje, żeby ją sprzedać wraz ze wszystkimi istniejącymi detalami w owej krainie. Całość wyceniono na ogromną kwotę 6 milionów USD. Zadziwiające jest to, iż chętny na zakup owej krainy znalazł się bardzo szybko i transakcja została zrealizowana jeszcze tego samego roku[5]. Ciekawy przypadek miał miejsce w Chinach, gdy sąd nakazał firmie „Red Moon" przywrócić graczowi stracone przedmioty na skutek włamania hackerskiego. Była to bardzo znana sprawa określana jako „first virtual property rights dispute case".

Przedsiębiorstwa, które udostępniają gry MMORPG, zastrzegają sobie w swoich regulaminach, że wszystko, co zostało stworzone w świecie wirtualnym, jest cały czas własnością podmiotu udostępniającego grę graczom. Tego typu zastrzeżenia regulaminów pozostawiają w sprzeczności z polskim prawem autorskim. Nie jest wiadomo, kto w takich sytuacjach jest podmiotem pierwotnego prawa autorskiego[6].

## Istota postaci fikcyjnej w grach MMORPG

Zgodnie z definicją Katarzyny Grzybczyk postać fikcyjna to „wytwór wyobraźni autora, który żyje podobnie jak istota ludzka: nosi jakieś imię, ma swój wizerunek, charakter, uczucia, życie prywatne, a czasem może mieć prawo do swojego honoru". Cechy te mogą również odnosić się do awatara. Twory fikcyjne, jakimi są postacie, można traktować jako nierozłączną część utworu lub jako istoty, które zachowują się według własnych zasad. Szczególnie można to zauważyć w grach typu MMORPG, gdzie uczestnik gry tworzy postać, która ma charakter indywidualny, może różnić się od reszty postaci w danym świecie[7]. Doskonałym przykładem jest gra *Second Life*, gdzie gracz sam tworzy swoje awatary i bierze udział w budowie wirtualnego świata. Ma prawo do korzystania z wirtualnych pieniędzy albo zakupu coraz to lepszych przedmiotów. Staje się on panem swojej postaci, chociaż wykorzystuje przy tym środki, które zapewnia mu gra. Oczywiste więc jest, że producenci gier w pewien sposób chcą się zabezpieczyć przed

---

[4] I. Matusiak, *Postacie świata wirtualnego w prawie autorskim,* Warszawa 2009, s. 37.

[5] https://www.komputerswiat.pl/gamezilla/artykuly/10-najdrozszych-wirtualnych-przedmiotow-w-historii- gier-wideo/0ggk5gn (dostęp: 8.05.2020 r.).

[6] I. Matusiak, *Postacie świata wirtualnego*…, s. 38

[7] https://www.rp.pl/artykul/642442-awatar--bohater--fikcja--gra--komputer--second-life--Tarzan.html (dostęp: 08.05.2020 r.)

sytuacjami, gdzie gracz zamierza zmienić poczynania swojego bohatera. Autorzy gry ochraniają się różnego typu regulaminami, w których zastrzegają sobie, że wszystko co jest wykreowane w owym świecie należy do nich. Tutaj powstaje problem, gdyż jest to sprzeczne z polskim prawem autorskim i często dochodzi do sporów na linii producent gry a gracz[8].

Mając na uwadze sposób powstania awataru w grze typu MMORPG, możemy mówić, że postać fikcyjna jest alter ego osoby, która ją tworzy. Podobna zależność zachodzi w dziełach literackich, gdzie często autor książki utożsamia się z danym bohaterem fikcyjnym. Zatem można stwierdzić, że zachodzi tutaj szczególna więź emocjonalna uczestnika gry z jego awatarem. Więź ta może mieć wpływ na losy postaci, może ona działać w indywidualny sposób, kształtować cechy, których nie mają inne awatary wirtualne. Awatar może zawierać elementy osobiste stworzone przez członka gry; ta zależność może potwierdzić indywidualny charakter postaci fikcyjnej[9].

Stanowisko Sądu Najwyższego z dnia 31 grudnia 1974 r., zgodnie z którym „ochronie prawa autorskiego podlega nie temat, lecz jego indywidualizacja (postać i koncepcja bohatera oraz innych postaci, ich losy, określone sytuacje, opisy itd.)”[10]. Zatem postać fikcyjna z połączeniem tworu plastycznego oraz literackiego może być podmiotem prawa autorskiego. Postać w grze może być personą indywidualną, dzięki ściśle określonym cechom może być uznawana jako utwór. W momencie objęcia postaci ochroną prawno-autorską, chociażby jako utworu plastycznego, jego komercyjne wykorzystanie będzie wymagać określenia podmiotu prawa autorskiego do utworu-awatara, pokazania pól eksploatacji, na których można korzystać z awatara oraz sposobu wykonania autorskich praw osobistych[11].

W grach MMORPG nie można odrzucić przypadku, występują tutaj takie sytuacje, gdy uczestnik gry kieruje swoją postacią świadomie oraz zgodnie z wcześniejszymi planami. Zdarza się, że gracze tego typu gier dążą do takich samych, często wspólnych celów. Takowe zachowania często wymagają od gracza szeregu przemyśleń i nie można tutaj mówić o elemencie przypadku, który w jakiś sposób wpływa na przebieg gry. Można powiedzieć, że mamy do czynienia z pewnego rodzaju scenariuszem gry komputerowej. Scenariuszem, który zważywszy na rodzaj gry jest cały czas tworzony. Jest tutaj spory dysonans między zwykłą grą komputerową a grą MMORPG; twórcy tych pierwszych gier znają scenariusz od początku do samego końca, podczas, gdy w grach typu MMORPG spotykamy się z otwartym scenariuszem rozgrywki. W drugim typie gier scenariusz tworzą

---

[8] https://www.komputerswiat.pl/gamezilla/aktualnosci/awatar-prawnie-nieokreslony/me7sdl5 (dostęp: 08.05.2020 r.).

[9] I. Matusiak, *Postacie świata wirtualnego*…, s. 40.

[10] Wyrok Sądu Najwyższego z dnia 31 grudnia 1974 r. (I CR 659/74), niepubl.; J. Barta, R. Markiewicz, *Prawo autorskie, przepisy, orzecznictwo, umowy międzynarodowe*, Warszawa 1997, s. 678.

[11] I. Matusiak, *Postacie świata wirtualnego*…, s. 41.

wszyscy uczestnicy gry. Dokładny schemat nie jest do końca znany, tak samo jak jego akcja[12].

Zbudowany komputerowo twór graficzny, jakim jest postać, może przypominać w większym lub mniejszym stopniu uczestnika rozgrywki i może być rozpoznawalny w społeczności innych postaci wirtualnych. Zjawisko to jest widocznie wśród osób powszechnie znanych. Bazując na grze *Second Life* swoje wizerunki, podobizny mają artyści, sportowcy czy też niektórzy z byłych posłów Sejmu RP. Postacie zawierają charakterystyczne cechy ubioru (np. charakterystyczne włosy Elvisa Presley`a czy też pumpy kojarzone z znanym raperem MC Hammerem) – wtedy nie ma wątpliwości, kogo przedstawia dana postać[13].

Postać wirtualna oprócz wyglądu posiada ściśle określony życiorys, który zbliżony jest do tego rzeczywistego osoby siedzącej przed komputerem. Ta zależność sprzyja identyfikacji osoby, która prowadzi swoją postać w świat wirtualny. Postać może w takim ujęciu tworzyć wirtualną konkretyzację obrazu fizycznego – obrazu w szerszym znaczeniu. Wizerunek w małym znaczeniu ograniczałby się tylko i wyłącznie do tzw. wizerunku plastycznego. Używanie określenia „wirtualny" wskazuje na okoliczność występowania wizerunku. Nie ma żadnych ograniczeń prawnych odnośnie do technik przedstawiania postaci[14].

## Handel kontami oraz przedmiotami wirtualnymi

Szerokie grono osób zaczęło szukać sposobów, aby ominąć barierę dotyczącą handlu kontami wirtualnymi. Pojawił się pomysł tworzenia osobnego konta do każdej gry, później ulegały one sprzedaży, dochodziło do podziału kontem na kilka osób i tak dalej. W taki sposób tworzył się pewnego rodzaju pomysł na szybki zarobek. Nie tak dawno doszło do aresztowania 24-latka z Piekar Śląskich w związku z nielegalną sprzedażą kont z grami na platformie Allegro. Otóż po wpisaniu w wyszukiwarkę tytułu pożądanej przez nas gry, pojawiały się oferty kupna gry w cenie rynkowej oraz oferty kupna za część ceny, przykładowo 10 zł. Tego typu aukcje nie zawierały fizycznego nośnika do gry czy też klucza wirtualnego, lecz oferowały jedynie dostęp do konta, na którym znajdowała się owa rozgrywka. Oczywiście nie była to sprzedaż konta z możliwością zmiany danych do zalogowania się i przeniesieniem zawartości konta. Osoba kupująca konto dostawała do niej login i hasło, a po udanym zalogowaniu (nie zawsze było to możliwe, gdyż często w jednym momencie więcej niż jeden użytkownik chciał się zalogować na dane konto) dochodziło do przejścia w tryb offline, aby system nie mógł wykryć przestępstwa[15].

Rodzi się pytanie: czy ten przypadek był nielegalny? Trzeba wyjaśnić, że to co zrobił wspomniany mieszkaniec Piekar Śląskich (robi to również wiele innych

[12] Tamże, s. 41.
[13] Tamże, s. 42.
[14] Tamże, s. 42.
[15] https://prawointernetu.eu/handel-kontami-do-gier-czy-jest-legalny/ (dostęp: 8.09.2020 r.).

osób), nie jest powtórną odsprzedażą kont z grami od jednej osoby do drugiej. W tej sytuacji dochodzi do wielokrotnej sprzedaży dostępu do tego samego konta. Rodzi to sytuację, gdy jeden nośnik z grą, po wieloetapowym złamaniu zabezpieczeń został skopiowany na tysiące innych nośników (płyt CD/DVD), które później dostałyby się do sprzedaży. O bezprawności tego ostatniego działania przesądziła w 1994 roku ustawa o prawie autorskim i prawach pokrewnych, która uporządkowała w sposób niebudzący wątpliwości kwestie praw autorskich.

Warto przytoczyć pierwsze trzy ustępy ustawy o prawie autorskim i prawach pokrewnych:

1. „Kto bez uprawienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca dopuszcza się czynu określonego w ust.1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.
3. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu lub działalność przestępną, określoną w ust. 1 organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5”[16].

Powstaje pytanie, czy legalnie możemy odsprzedać nasze konto, postacie czy też przedmioty wirtualne innej osobie. Stworzył się pewien dualizm w podejściu do tematu, czy gra komputerowa (w tym również postać) może zostać odsprzedana na rynku wtórnym. W odpowiedzi na to pytanie szybko pojawia się problem w związku z brzmieniem treści art. 51 ust. 3 ustawy o prawie autorskim i prawach pokrewnych. W myśl tego przepisu: „Wprowadzenie do obrotu oryginału albo egzemplarza utworu na terytorium Europejskiego Obszaru Gospodarczego wyczerpuje prawo do zezwalania na dalszy obrót takim egzemplarzem na terytorium Rzeczypospolitej Polski, z wyjątkiem jego najmu lub użyczenia”.

Należy zwrócić uwagę, iż przepis mówi o obrocie oryginałem lub numerem utworu. Generalnie można przyjąć, że mowa tutaj o materialnym nośniku, na którym danym utwór został zapisany. Ustawa, o której mowa wyżej, weszła w życie w roku 1994. Wówczas 90% sprzedaży wszelkiego rodzaju odbywała się materialnych nośnikach takich jak kasety magnetofonowe czy trochę później płyty CD/DVD. Obecnie najbardziej powszechną metodą sprzedaży utworów jest sprzedaż internetowa/cyfrowa. Dotychczasowe podejście zmienił jednak wyrok Trybunału Sprawiedliwości UE z dnia 3 lipca 2012 r. w sprawie o sygn. akt C-128/11; to interpretacja Trybunału: „Należy następnie przypomnieć, że przysługujące podmiotowi praw autorskich prawo do rozpowszechniania zostaje wyczerpane zgodnie z art. 4 ust. 2 dyrektywy 2009/24 przy pierwszej sprzedaży na terytorium Unii kopii jego programu komputerowego przez ten podmiot praw autorskich lub za jego zgodą, niezależnie od tego, czy jest to kopia materialna czy też niematerialna.

[16] https://prawointernetu.eu/handel-kontami-do-gier-czy-jest-legalny/ (dostęp: 8.09.2020 r.).

Wynika z tego, że zgodnie z tym przepisem i pomimo istnienia postanowień umownych zakazujących dalszego zbywania, podmiot danego prawa autorskiego nie może sprzeciwić się odsprzedaży tej kopii".

Przewrotne podejście Trybunału daje nam do zrozumienia, że do wyczerpania prawa dochodzi również w stosunku do odsprzedaży cyfrowej kopii gry bądź programu. Trybunał prawdopodobnie miał na myśli postanowienia regulaminów, które zakazują tego typu działań. Przykładowo platformy bardzo często zamieszczają zapis, że nie kupujemy gier, a jedynie dostęp do nich. Jednak, jakby miało to wpływać na prawo wynikające z art. 51 ust. 3 ustawy o prawie autorskim i prawach pokrewnych. Reguła ta dotyczy rzecz jasna sytuacji, gdzie sprzedajemy dostęp do programu czy gry jednej osobie, po czym tracimy go na zawsze. Dokładnie tak, jak mamy to w sytuacji sprzedaży fizycznego nośnika gry[17].

Współcześnie handel wirtualnymi przedmiotami w grach komputerowych stał się niezwykle popularny. Spowodowane jest to rosnącą powszechnością gier, w których niemalże każdy ma możliwość wzięcia udziału. Istnieje liczna grupa graczy, która jest w stanie ponieść wysokie koszty, byle tylko zdobyć rzadką zbroję czy unikatowy miecz. Od kilku lat kwestia handlu przedmiotami wirtualnymi budzi kontrowersje w naszym kraju, mimo że żadna z ustaw nie określa wprost konsekwencji podatkowych związanych z handlem przedmiotami wirtualnymi. W ostatnich latach swoją opinię przedstawiły regionalne Izby Skarbowe m.in. w Łodzi, Poznaniu, Bydgoszczy oraz Katowicach.

Tarcze, magiczne amulety czy antyczne miecze oraz wiele innych wirtualnych rzeczy (itemów) w świecie gier kosztują tyle samo co w świecie rzeczywistym, a czasami ceny dochodzą nawet do setek tysięcy złotych. Gdy handel przedmiotami wirtualnymi ma charakter zorganizowany i ciągły oraz staje się regularnym źródłem dochodu, to w myśl ustawy o podatku dochodowych od osób fizycznych mamy do czynienia z przesłanką do założenia działalności gospodarczej.

Jeśli handel przedmiotów wirtualnych odbywa się w sposób zorganizowany oraz ma na celu zarobek, wpisuje się w definicję działalności gospodarczej określoną w art. 5 pkt 6 ustawy o PIT, a to oznacza, iż opodatkowany jest przychód osiągany przez podatnika, jeśli przepisy nie przewidują odpowiedniego zwolnienia lub nie włączają go z opodatkowania. Tak właśnie jest w przypadku sprzedaży wirtualnych przedmiotów przez ich posiadaczy. Rzecz jasna innej ocenie podlega sytuacja, gdy podatnik dopuści się sprzedaży jednorazowej lub gdy mamy do czynienia ze sprzedażą sporadyczną, nie planując pozyskiwania w ten sposób stałych dochodów. Sytuacja zmienia się, gdy podatnik pozyskuje regularny dochód poprzez handel wirtualnymi przedmiotami.

Aby osoby, które prowadzą działalność gospodarczą były podatnikami VAT, musi dojść do obrotu wirtualnymi przedmiotami, które będą uznane jako świadczenie usług. Transakcję tego typu rzeczy według przepisów należy uważać za

[17] https://prawointernetu.eu/handel-kontami-do-gier-czy-jest-legalny/ (dostęp: 8.09.2020 r.).

handel usług elektronicznych w rozumieniu art. 2 pkt 26 ustawy o VAT. Zatem stawka podatku wynosi 23%. Jeśli doszło do zdarzenia, gdzie osoba sprzedająca przedmioty wirtualne nie przekroczyła w danym roku kwoty 200 tysięcy zł, może skorzystać ze zwolnienia podatkowego z VAT na podstawie art. 113 ustawy o VAT[18].

## Zakończenie

Jak zaznaczono na wstępie rozdziału, celem rozważań było przedstawienie zagadnień prawno-autorskich, które dotyczyły postaci wirtualnych w grach komputerowych, ukazanie funkcjonowania gry komputerowej typu MMORPG. W aspekcie prawnym temat postaci fikcyjnych w grach MMORPG budzi wiele wątpliwości, z pewnością potrzebne są przepisy prawne, które pozwoliłyby nam regulować tę sferę Internetu. Postęp technologiczny ulega dzisiaj intensywnej dynamizacji, owe działania mogą więc korzystnie wpłynąć na szeroko pojęty rozwój sfery świata wirtualnego. Dzięki rozwojowi grafiki komputerowej stale wzrasta również zapotrzebowanie na kolejne ulepszone postacie. Warto wspomnieć, iż odsprzedaż kont z grami nie powinna być nielegalna. Firmy, które uciekają od tego, zapewne w przyszłości zostaną zmuszone przez przepisy unijne do wdrożenia udogodnień pozwalających na odsprzedaż gry bez sprzedaży całego konta. Z uwagi na szybki rozwój tej sfery organy państwowe i skarbowe mogą zacząć się przyglądać handlowi itemów w celu rozliczania jej dla potrzeb podatkowych.

## Bibliografia

Barta J., Markiewicz R., *Prawo autorskie, przepisy, orzecznictwo, umowy międzynarodowe*, Warszawa 1997.

Konarski R., *Gra komputerowa jako przejaw wolności człowieka*, Wrocław 2013.

Matusiak I., *Postacie świata wirtualnego w prawie autorskim*, Warszawa 2009.

Traple E., *Wprowadzenie – gry komputerowe w świetle prawa*, Warszawa 2015.

## Orzecznictwo

Wyrok Sądu Najwyższego z 31.12.1974 r. (I CR 659/74), niepubl.

## Netografia

https://www.komputerswiat.pl/gamezilla/artykuly/10-najdrozszych-wirtualnych-przedmiotow-w-historii- gier-wideo/0ggk5gn

[18] https://br-kwapisz.pl/czy-handel-wirtualny-nosi-znamiona-dzialalnosci-gospodarczej/ (dostęp: 09.09.2020 r.).

https://www.rp.pl/artykul/642442-awatar--bohater--fikcja--gra--komputer--second-life--Tarzan.html
https://br-kwapisz.pl/czy-handel-wirtualny-nosi-znamiona-dzialalnosci-gospodarczej/
https://prawointernetu.eu/handel-kontami-do-gier-czy-jest-legalny/
Wikipedia Wolna encyklopedia, https://pl.wikipedia.org/wiki/MMORPG

# AUKCJA ELEKTRONICZNA W NOWYM PRAWIE ZAMÓWIEŃ PUBLICZNYCH

(z dnia 11 września 2019 r.)

(*Andrzej Kiełtyka*)

„Zamówienia" w systemie zamówień publicznych to umowy odpłatne, zawierane między zamawiającym a wykonawcą, których przedmiotem jest nabycie przez zamawiającego, od wybranego wykonawcy, robót budowlanych, dostaw lub usług[1]. Zamówienia publiczne to ogromne przedsięwzięcie wspomagające rozwój gospodarczy kraju, umożliwiające poprawę jakości zamawianych dostaw, usług i robót budowlanych, wsparcie innowacyjności, realizowanie polityki społecznej i strategii państwa. Zamówienia publiczne są zasadniczą formą udziału sektora publicznego w gospodarce.

W dniu 11 września 2019 r. uchwalono nową ustawę – Prawo zamówień publicznych[2]. Zastąpiła ona wielokrotnie nowelizowaną ustawę z 29 stycznia 2004 roku[3]. Zgodnie z ustawą z 11 września 2019 r. Przepisy wprowadzające ustawę Prawo zamówień publicznych nowe prawo zamówień publicznych, co do zasady, wejdzie w życie 1 stycznia 2021 r. (art. 109)[4].

W uzasadnieniu do projektu ustawy z 29 stycznia 2004 r.[5] podniesiono, że obowiązująca uprzednio ustawa z 10 czerwca 1994 r. o zamówieniach publicznych[6], wskutek zmian społeczno-gospodarczych w kraju oraz rozwoju rynku zamówień publicznych, wciągu ostatnich lat, była wielokrotnie nowelizowana, co spowodowało brak przejrzystości, spójności i precyzji przepisów. Nieczytelność i brak precyzji prawa sprzyjał powstawaniu niekorzystnych zjawisk – w tym świadomemu łamaniu zasad wydatkowania środków publicznych. Przyjęcie nowej ustawy, zmierzając do ograniczenia takich praktyk, było między innymi elementem realizacji zadań zawartych w „Strategii Antykorupcyjnej Rządu". Jednocześnie stworzenia nowego spójnego aktu prawnego, regulującego problematykę zamówień publicznych, wymagał proces harmonizacji prawa z wymogami Unii

---

[1] Definicja ustawowa zawarta w art. 7 pkt. 32 ustawy z 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2019 r., poz. 2019).

[2] Dz.U. z 2019 r., poz. 2019.

[3] Tekst jedn. Dz.U. z 2019 r., poz. 1843.

[4] Dz.U. z 2019 r., poz. 2020. Do postępowań o udzielenie zamówienia, o których mowa w ustawie uchylonej, wszczętych i niezakończonych przed dniem 1 stycznia 2021 r. stosuje się przepisy dotychczasowe (art. 90 ust. 1).

[5] Projekt ustawy z 7 listopada 2003 r., Sejm IV Kadencji, druk nr 2218.

[6] Tekst jedn. Dz.U. z 2002 r., nr 72, poz. 664 ze zm.

Europejskiej, objęcie przepisami ustawy nowych grup podmiotów oraz zwiększająca się corocznie wielkość środków wydawanych w trybie ustawy. Usunięcie rozbieżności w zakresie harmonizacji prawa było szczególnie istotne, gdyż od osiągnięcia pełnej zgodności polskiego prawa z regulacjami Unii Europejskiej zależał nieskrępowany dostęp polskich wykonawców do europejskiego rynku zamówień.

Ustawa z 2004 r. przewiduje przeprowadzenie licytacji elektronicznej (art. 74 i n.) oraz aukcji elektronicznej (art. 91a i n.)[7]. W znaczeniu językowym oba te wyrazy to niewątpliwie synonimy[8]. W znaczeniu prawa zamówień publicznych różnią się istotnie. Przede wszystkim licytacja elektroniczna zaliczana jest (jeszcze obecnie – do 1 stycznia 2021 r.) do jednego z trybów postępowania o zamówienie (obok: przetargu nieograniczonego, przetargu ograniczonego, negocjacji z ogłoszeniem, negocjacji bez ogłoszenia, dialogu konkurencyjnego, zamówienia z wolnej ręki i zapytania o cenę)[9]. Tryb zamówienia publicznego to sposób prowadzenia postępowania o zamówienie publiczne, przy jednoczesnym spełnieniu określonych w ustawie warunków.

Zamawiający mógł przeprowadzić licytację elektroniczną przy nabywaniu dostaw, usług lub robót budowlanych, jeżeli wartość zamówienia była niższa od tzw. progów unijnych określonych w przepisach[10].

---

[7] Art. 74 ustawy z 2004 r. ustawa z 7 kwietnia 2006 r. o zmianie ustawy Prawo zamówień publicznych oraz ustawy o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz.U. z 2006 r., nr 79, poz. 551). Na skutek nowelizacji tryb udzielenia zamówienia, nazywany dotychczas aukcją elektroniczną, został „przemianowany" z dniem 25 maja 2006 r. na licytację elektroniczną. Nazwa aukcja elektroniczna obowiązywała odtąd dla procedury uregulowanej w art. 91a – 91c ustawy.

[8] Zob. M. Bańko (red.), *Inny słownik języka polskiego*, t. I, Wydawnictwo Naukowe PWN, Warszawa 2000, s. 51, 764: definicja: „Publiczna sprzedaż jakichś rzeczy, których właścicielem staje się ten, kto oferuje najwyższą cenę".

[9] W ustawie z dnia 11 września 2019 r. tryb udzielenia zamówienia publicznego w postaci licytacji elektronicznej nie występuje.

[10] Wydanych na odstawie art. 11 ust. 8 ustawy: „Minister właściwy do spraw gospodarki określi, w drodze rozporządzenia, kwoty wartości zamówień oraz konkursów, od których jest uzależniony obowiązek przekazywania ogłoszeń Urzędowi Publikacji Unii Europejskiej, mając na względzie obowiązujące w tym zakresie przepisy prawa Unii Europejskiej": rozporządzenie Ministra Rozwoju z dnia 16 grudnia 2019 r. w sprawie kwot wartości zamówień oraz konkursów, od których jest uzależniony obowiązek przekazywania ogłoszeń Urzędowi Publikacji Unii Europejskiej, ustawodawca uzależnił zatem zastosowanie tego trybu od wartości planowanych zakupów, bez względu na ich przedmiot (dostawa, usługa czy robota budowlana).
W ustawie z 11 września 2019 r. progi unijne ustalono w art. 3 ustawy. Przez progi unijne należy rozumieć kwoty wartości zamówień lub konkursów określone w:
- art. 4 i art. 13 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE (Dz. Urz. UE L 94 z 28.03.2014 r., s. 65 z ze zm.),
- art. 15 dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE z 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającej dyrektywę 2004/17/WE (Dz. Urz. UE L 94 z 28.03.2014 r., s. 243 ze zm.),

Cechą odróżniającą tryb licytacji elektronicznej od innych procedur była możliwość wielokrotnego składania oferty cenowej w formie tzw. postąpienia[11], co oznaczało, że cena oferty była uzależniona od ofert innych uczestników licytacji, a każde kolejne postąpienie (tańsza oferta) podlegało automatycznej klasyfikacji. Zamawiający nie mógł ingerować w tę klasyfikację, dlatego też musiał zapewnić do licytacji urządzenia, które samodzielnie klasyfikują postąpienia w czasie rzeczywistym. Zamawiający był obowiązany do zapewnienia odpowiedniego formularza z dostępem online[12], za pomocą którego wykonawcy składali postąpienia. Urząd Zamówień Publicznych stworzył platformę do prowadzenia licytacji elektronicznych – jest ona dostępna pod adresem: licytacje.uzp.gov.pl.[13]. Ustawa wdrażała szereg dyrektyw Unii Europejskiej[14]. Zasadniczo utrzymano katalog zasad

- art. 8 dyrektywy 2009/81/WE Parlamentu Europejskiego i Rady z 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniającej dyrektywy 2004/17/WE i 2004/18/WE (Dz. Urz. UE L 216 z 20.08.2009 r., s. 76, ze zm.),
- aktualizowane w aktach wykonawczych Komisji Europejskiej, wydawanych odpowiednio na podstawie art. 6 ust. 5 dyrektywy 2014/24/UE, art. 17 ust. 4 dyrektywy 2014/25/UE i art. 68 dyrektywy 2009/81/WE.

[11] „Postąpienie" jest to kwota, o jaką zmienia się proponowana cena podczas licytacji. Termin ekonomiczny. https://sjp.pl/post%C4%85postąpienie (dostęp: 31.08.2020 r.).

[12] Online (*online*, pierwotnie *on-line* z ang. dosł. „na linii") – zwykle status osoby, serwera lub innego podmiotu związanego z dostępem do łączy komunikacyjnych (np. Internetu), który informuje o dostępności – aktywności. Przeciwieństwem trybu online jest tryb offline. https://pl.wikipedia.org/wiki/Online (dostęp: 31.08.2020 r.).

[13] Por.: I. Skubiszak-Kalinowska, E. Wiktorowska, *Prawo zamówień publicznych. Komentarz aktualizowany*, LEX/el. 2020; J.E. Nowicki, M. Kołecki, *Prawo zamówień publicznych. Komentarz*, wyd. IV, Wolters Kluwer Polska 2019; W. Dzierżanowski, J. Jerzykowski, M. Stachowiak, *Prawo zamówień publicznych. Komentarz*, wyd. VII Wolters Kluwer Polska 2018 – tezy do art. 74 ustawy z 2004 r.

[14] Dyrektywę Parlamentu Europejskiego i Rady 2014/24/UE z 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającą dyrektywę 2004/18/WE (Dz. Urz. UEL94 z 28 marca 2014 r., s. 65 ze zm.); dyrektywę Parlamentu Europejskiego i Rady 2014/25/UE z 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającą dyrektywę 2004/17/WE (Dz. Urz. UEL 94 z 28 marca 2014 r., s. 243 ze zm.); dyrektywę Parlamentu Europejskiego i Rady 2009/81/WE z 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniającą dyrektywy 2004/17/WE i 2004/18/WE (Dz. Urz. UEL 216 z 20 sierpnia 2009 r., s. 76, ze zm.); dyrektywę Rady 89/665/EWG z 21 grudnia 1989 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do stosowania procedur odwoławczych w zakresie udzielania zamówień publicznych na dostawy i roboty budowlane (Dz. Urz. WE L 395 z 30 grudnia 1989 r., s. 33 ze zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 6, t.1, str. 246); dyrektywę Rady 92/13/EWG z 25 lutego 1992 r. koordynującą przepisy ustawowe, wykonawcze i administracyjne odnoszące się do stosowania przepisów wspólnotowych w procedurach zamówień publicznych podmiotów działających w sektorach gospodarki wodnej, energetyki, transportu i telekomunikacji (Dz. Urz. WE L 76 z 23 marca 1992 r., s. 14 ze zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 6, t. 1, s. 315).

udzielania zamówień publicznych, wzbogacając go o zasadę ochrony danych osobowych[15].

Natomiast aukcja elektroniczna nie jest trybem postępowania o zamówienie publiczne. Zasady organizacji aukcji elektronicznej określa art. 91a i nast. ustawy z 2004 r. Jeżeli postępowanie jest prowadzone w trybie przetargu nieograniczonego, przetargu ograniczonego lub negocjacji z ogłoszeniem, zamawiający po dokonaniu oceny ofert w celu wyboru najkorzystniejszej oferty przeprowadza aukcję elektroniczną, jeżeli przewidział to w ogłoszeniu o zamówieniu, zaproszeniu do potwierdzenia zainteresowania lub w ogłoszeniu o ustanowieniu systemu kwalifikowania wykonawców, oraz jeżeli można w sposób precyzyjny określić treść specyfikacji istotnych warunków zamówienia oraz złożono co najmniej dwie oferty niepodlegające odrzuceniu.

W przypadku gdy zamawiający postanowił przeprowadzić aukcję elektroniczną, w ogłoszeniu o zamówieniu lub specyfikacji istotnych warunków zamówienia określa co najmniej:

- elementy, których wartości będą przedmiotem aukcji elektronicznej, pod warunkiem że elementy te są wymierne i mogą być wyrażone w postaci liczbowej lub procentowej,
- wszelkie ograniczenia co do przedstawianych wartości, wynikające z opisu przedmiotu zamówienia,
- informacje, które zostaną udostępnione wykonawcom w trakcie aukcji elektronicznej oraz, w stosownych przypadkach, termin ich udostępnienia,
- informacje dotyczące przebiegu aukcji elektronicznej;
- warunki, na jakich wykonawcy będą mogli licytować oraz, w szczególności, minimalne wysokości postąpień, które, w stosownych przypadkach, wymagane będą podczas licytacji,
- informacje dotyczące parametrów wykorzystywanego sprzętu elektronicznego, rozwiązań i specyfikacji technicznych w zakresie połączeń.

Kryteriami oceny ofert w toku aukcji elektronicznej są wyłącznie kryteria określone w specyfikacji istotnych warunków zamówienia i zaproszeniu do aukcji elektronicznej, umożliwiające automatyczną ocenę oferty bez ingerencji zamawiającego, wskazane spośród kryteriów, na podstawie których dokonano oceny ofert przed otwarciem aukcji elektronicznej.

Aukcja elektroniczna może być jednoetapowa lub wieloetapowa. Aukcja elektroniczna nie jest odrębnym trybem postępowania o udzielenie zamówienia publicznego, lecz swoistą dogrywką elektroniczną, która następuje po dokonaniu

[15] Nr 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4 maja 2016 r., s. 1 ze zm.).

oceny ofert w sytuacjach określonych w art. 91a ust. 1 ustawy z 2004 roku[16]. Przepisy Prawa zamówień publicznych nie definiują pojęcia aukcji elektronicznej. Aukcja elektroniczna nie jest trybem, lecz sposobem wyboru oferty[17]. Rozwiązanie to ma na celu zwiększenie konkurencyjności pomiędzy wykonawcami ubiegającymi się o udzielenie zamówienia publicznego, a tym samym otrzymywanie przez zamawiających jeszcze korzystniejszych ofert[18].

Według uzasadnienia do projektu nowej ustawy z 11 września 2019 r.: „Ustawa przewiduje w zakresie aukcji elektronicznej rozwiązania odpowiadające dotychczasowym. Wprowadzone zmiany w stosunku do przepisów dotychczas obowiązujących mają wyłącznie charakter porządkujący i dostosowujący. Przepisy o aukcji elektronicznej wdrażają w projekcie ustawy postanowienia art. 35 dyrektywy klasycznej[19] oraz art. 53 dyrektywy sektorowej”[20]. Systematyka ustawy porządkuje przepisy oraz zwiększa jej przejrzystość[21].

Art. 227 ustawy z 11 września 2019 r. określa czynności poprzedzające wybór najkorzystniejszej oferty poprzez stosowanie aukcji elektronicznej.

W przypadku postępowań o udzielenie zamówienia prowadzonych w trybie przetargu nieograniczonego[22], przetargu ograniczonego[23] lub negocjacji z ogłoszeniem[24], zamawiający może przewidzieć w ogłoszeniu o zamówieniu, że wybór najkorzystniejszej oferty zostanie poprzedzony aukcją elektroniczną, jeżeli warunki

---

[16] Zob. I. Skubiszak-Kalinowska, E. Wiktorowska, *Prawo zamówień…*; tezy do art. 91a ustawy z 2004 r.

[17] Zob. J.E. Nowicki, M. Kołecki, *Prawo zamówień*…; tezy do art. 91a ustawy z 2004 r.

[18] Zob. W. Dzierżanowski, J. Jerzykowski, M. Stachowiak, *Prawo zamówień publicznych. Komentarz*, wyd. VII Wolters Kluwer Polska 2018; tezy do art. 91a ustawy z 2004 r.

[19] Dyrektywa 2014/24/UE z 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (art. 53: „Podmioty zamawiające mogą stosować aukcje elektroniczne, w których przedstawiane są nowe, obniżane ceny lub nowe wartości dotyczące niektórych elementów ofert. W tym celu podmioty zamawiające organizują aukcje elektroniczne w formie powtarzalnego procesu elektronicznego, który następuje po przeprowadzeniu wstępnej pełnej oceny ofert, umożliwiającego ich klasyfikację za pomocą metod automatycznej oceny. Niektóre zamówienia na usługi i niektóre zamówienia na roboty budowlane, których przedmiotem są prace intelektualne, takie jak projekt robót budowlanych i których nie można sklasyfikować za pomocą metod automatycznej oceny, nie mogą być przedmiotem aukcji elektronicznych”).

[20] Dyrektywa 2014/25/UE z 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (treść przepisu art. 35 zbliżona do przytoczonej wyżej).

[21] Z uzasadnienia do projektu ustawy. Sejm VIII Kadencji, druk nr 3624.

[22] Art. 132 ustawy z 11 września 2019 r. „Przetarg nieograniczony to tryb udzielenia zamówienia, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani wykonawcy”.

[23] Art. 140 ustawy z 11 września 2019 r. „Przetarg ograniczony to tryb udzielenia zamówienia, w którym w odpowiedzi na ogłoszenie o zamówieniu, wnioski o dopuszczenie do udziału w postępowaniu mogą składać wszyscy zainteresowani wykonawcy, a oferty mogą składać wyłącznie wykonawcy zaproszeni do składania ofert”.

[24] Art. 152 ustawy z 11 września 2019 r. „Negocjacje z ogłoszeniem to tryb udzielenia zamówienia, w którym w odpowiedzi na ogłoszenie o zamówieniu, wnioski o dopuszczenie do udziału w postępowaniu mogą składać wszyscy zainteresowani wykonawcy, zamawiający zaprasza wykonaw-

zamówienia, w szczególności opis przedmiotu zamówienia, są określone w dokumentach zamówienia w sposób precyzyjny i świadczenia mogą być sklasyfikowane za pomocą metod automatycznej oceny oraz złożono co najmniej dwie oferty niepodlegające odrzuceniu.

Zamawiający może przeprowadzić aukcję elektroniczną w celu uzyskania nowych, obniżonych cen lub nowych wartości w zakresie niektórych elementów ofert, podlegających ocenie w ramach kryteriów oceny ofert.

W zakresie sposobu przeprowadzenia aukcji elektronicznej to jest ona przeprowadzana przy użyciu systemu teleinformatycznego w formie powtarzalnego procesu elektronicznego, umożliwiającego klasyfikację ofert za pomocą metod automatycznej oceny, po wstępnym badaniu i ocenie ofert zgodnie z kryteriami udzielania zamówienia i przypisaną im wagą. Aukcja elektroniczna nie ma zastosowania do zamówień na usługi lub roboty budowlane, gdzie przedmiotem są świadczenia o charakterze intelektualnym, których nie można sklasyfikować za pomocą metod automatycznej oceny[25].

W art. 229 ustawy z 11 września 2019 r. określono elementy ofert będące podstawą aukcji elektronicznej. W szczególności aukcja elektroniczna może opierać się na następujących elementach ofert:

- cenach, jeżeli jedynym kryterium oceny ofert w postępowaniu jest cena;
- cenach lub nowych wartościach elementów ofert wskazanych w dokumentach zamówienia, jeżeli kryteriami oceny ofert w postępowaniu są kryteria jakościowe albo najniższy koszt.

Ustawa określa także treść ogłoszenia o zamówieniu lub dokumentów zamówienia w przypadku przeprowadzania aukcji elektronicznej. W przypadku przeprowadzania aukcji elektronicznej w ogłoszeniu o zamówieniu lub w dokumentach zamówienia określa się co najmniej:

- elementy, których wartości będą przedmiotem aukcji elektronicznej, pod warunkiem że elementy te są wymierne i mogą być wyrażone w postaci liczbowej lub procentowej;
- wszelkie ograniczenia co do przedstawianych wartości, wynikające z opisu przedmiotu zamówienia;
- informacje, które zostaną udostępnione wykonawcom w trakcie aukcji elektronicznej, oraz, w stosownych przypadkach, termin ich udostępnienia;
- informacje dotyczące przebiegu aukcji elektronicznej;
- warunki, na jakich wykonawcy będą mogli licytować, w szczególności minimalne wartości postąpień, które wymagane będą podczas licytacji;

---

ców dopuszczonych do udziału w postępowaniu do składania ofert wstępnych, prowadzi z nimi negocjacje w celu ulepszenia treści ofert wstępnych, ofert składanych na etapie negocjacji, po zakończeniu których zaprasza wykonawców do składania ofert ostatecznych. Zamawiający może udzielić zamówienia na podstawie ofert wstępnych bez negocjacji, o ile wskaże w ogłoszeniu o zamówieniu, że zastrzega sobie taką możliwość".

[25] Art. 228 ustawy.

- informacje dotyczące parametrów wykorzystywanego sprzętu elektronicznego, rozwiązań i specyfikacji technicznych w zakresie połączeń.

Aukcja elektroniczna może być przeprowadzona jednoetapowo lub wieloetapowo[26].

### Zaproszenie do udziału w aukcji elektronicznej; termin otwarcia aukcji elektronicznej

Zamawiający zaprasza do udziału w aukcji elektronicznej jednocześnie wszystkich wykonawców, którzy złożyli oferty niepodlegające odrzuceniu, przy użyciu połączeń elektronicznych wskazanych w zaproszeniu. W zaproszeniu zamawiający informuje wykonawcę o:

- wyniku badania i oceny oferty tego wykonawcy;
- minimalnych wartościach postąpień składanych w toku aukcji elektronicznej;
- terminie otwarcia aukcji elektronicznej;
- terminie i warunkach zamknięcia aukcji elektronicznej;
- sposobie oceny ofert w toku aukcji elektronicznej;
- formule matematycznej, która zostanie wykorzystana w aukcji elektronicznej do automatycznego tworzenia kolejnych klasyfikacji na podstawie przedstawianych nowych cen lub wartości;
- harmonogramie dla każdego etapu aukcji elektronicznej, jeżeli zamawiający zamierza zamknąć aukcję elektroniczną na podstawie art. 237 pkt 3[27].

Z wyjątkiem przypadków, gdy najkorzystniejsza oferta jest wybierana na podstawie ceny, formuła matematyczna, która zostanie wykorzystana w aukcji elektronicznej do automatycznego tworzenia kolejnych klasyfikacji na podstawie przedstawianych nowych cen lub wartości uwzględnia wagi przypisane poszczególnym kryteriom oceny ofert w celu dokonania wyboru najkorzystniejszej oferty, wskazanym w ogłoszeniu o zamówieniu lub dokumentach zamówienia, a w przypadku dopuszczenia ofert wariantowych określa się odrębną formułę dla każdego wariantu. Termin otwarcia aukcji elektronicznej nie może być krótszy niż dwa dni robocze od dnia przekazania zaproszenia.

W toku aukcji elektronicznej zamawiający na bieżąco przekazuje każdemu wykonawcy informacje umożliwiające mu ustalenie pozycji jego oferty w klasyfikacji ofert, w szczególności informacje o uzyskanej punktacji oraz o punktacji oferty, która uzyskała najwyższą liczbę punktów. Zamawiający, jeżeli zostało to przewidziane w dokumentach zamówienia, może w ustalonym przez siebie czasie ogłaszać liczbę uczestników danego etapu aukcji elektronicznej. Do momentu zamknięcia aukcji elektronicznej nie ujawnia się informacji umożliwiających identyfikację wykonawców biorących udział w danym etapie aukcji elektronicznej[28].

---

[26] Art. 230, 231 ustawy.
[27] Zamawiający zamyka aukcję elektroniczną po zakończeniu ostatniego, ustalonego etapu.
[28] Art. 233 ustawy.

Zasady składania postąpień w aukcji elektronicznej: w toku aukcji elektronicznej wykonawcy za pomocą formularza umieszczonego na stronie internetowej, umożliwiającego wprowadzenie niezbędnych danych w trybie bezpośredniego połączenia z tą stroną, składają kolejne korzystniejsze postąpienia, podlegające automatycznej ocenie i klasyfikacji. Postąpienia, pod rygorem nieważności, składane są w formie elektronicznej (art. 234 ustawy).

Oferta wykonawcy przestaje wiązać w zakresie, w jakim złoży on korzystniejszą ofertę w toku aukcji elektronicznej. W takiej sytuacji bieg terminu związania ofertą nie ulega przerwaniu.

W przypadku, gdy awaria systemu teleinformatycznego spowoduje przerwanie aukcji elektronicznej, zamawiający wyznacza termin kontynuowania aukcji elektronicznej na następny dzień roboczy przypadający po usunięciu awarii, z uwzględnieniem stanu ofert po ostatnim zatwierdzonym postąpieniu.

Zamawiający zamyka aukcję elektroniczną: w terminie określonym w zaproszeniu do udziału w aukcji elektronicznej; jeżeli w ustalonym terminie nie zostaną zgłoszone nowe postąpienia; po zakończeniu ostatniego, ustalonego etapu.

Zamawiający po zamknięciu aukcji elektronicznej dokonuje oceny ofert w oparciu o kryteria oceny ofert wskazane w ogłoszeniu o zamówieniu i w dokumentach zamówienia, z uwzględnieniem wyników aukcji elektronicznej[29].

Treść Specyfikacji Warunków Zamówienia (SWZ) winna zawierać informację o przewidywanym wyborze najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230[30], jeżeli zamawiający przewiduje aukcję elektroniczną[31].

Zamawiający może udzielić zamówienia w dziedzinach obronności i bezpieczeństwa w trybie przetargu ograniczonego lub negocjacji z ogłoszeniem. W takich przypadkach zamawiający może wybrać najkorzystniejszą ofertę z zastosowaniem aukcji elektronicznej. Przepisy art. 227–238 (dotyczące aukcji elektronicznej) stosuje się odpowiednio[32].

Na stronie internetowej Urzędu Zamówień Publicznych[33] znajduje się platforma służąca do przeprowadzania aukcji elektronicznych – zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych[34], jako sposobu dokonywania wyboru najkorzystniejszej oferty m.in., w postępowaniach prowadzonych w trybie przetargu nieograniczonego, przetargu ograniczonego lub negocjacji z ogłoszeniem.

Korzystanie z systemu jest bezpłatne. Zamawiający chcący korzystać z systemu muszą uprzednio dokonać rejestracji. Raz dokonana rejestracja umożliwia

---

[29] Art. 238 ustawy.

[30] Art. 230. Treść ogłoszenia o zamówieniu lub dokumentów zamówienia w przypadku przeprowadzania aukcji elektronicznej.

[31] Art. 134 pkt 12 ustawy.

[32] Art. 410 ustawy.

[33] https://aukcje.uzp.gov.pl/index.php/page/selflearn/page/9 (dostęp: 28.08.2020 r.).

[34] Zasady funkcjonowania platformy będą musiały być dostosowane do przepisów ustawy z dnia 11 września 2019 r., po jej wejściu w życie. Zmiany jednak prawdopodobnie będą mało istotne.

prowadzenie wielu aukcji. W przypadku wykonawców, rejestracji każdorazowo dokonuje zamawiający prowadzący aukcję elektroniczną.

Celem ułatwienia korzystania z platformy, przygotowano samouczek interaktywny zawierający podpowiedzi dla zainteresowanych. Zawiera on następująca problematykę: wymagania systemu, rejestrację, hasło i login, aukcję elektroniczną, ramy czasowe aukcji, czas systemowy, podpis elektroniczny, rodzaj wiadomości przesyłane na pośrednictwem systemu.

W dniu 25 maja 2018 r. w związku z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) uległ zmianie Regulamin Platformy Aukcji Urzędu Zamówień Publicznych.

Zalecają, by używać do wykorzystania na platformie przeglądarek internetowych: Mozilla Firefox[35] oraz Google Chrome[36]. Winny być stosowane najnowsze wersje tych przeglądarek.

Z uwagi na fakt, że postąpienia, które wykonawcy są zobligowani podpisać elektronicznie, są generowane w postaci dokumentu PDF[37], wykonawcy biorący udział w aukcji elektronicznej winni dysponować oprogramowaniem umożliwiającym odczytywanie plików w tym formacie. Oprogramowanie takie wykonawcy mogą pobrać bezpłatnie ze strony internetowej[38].

Ponadto wykonawcy chcący składać oferty w toku aukcji elektronicznej muszą dysponować urządzeniami technicznymi oraz oprogramowaniem służącymi do obsługi podpisu elektronicznego. Wymóg dysponowania podpisem elektronicznym nie dotyczy zamawiającego.

Rejestracja jest obowiązkowa dla zamawiających, którzy chcą przeprowadzić własną aukcję. Podczas rejestracji, wypełniając odpowiedni formularz, określają swój LOGIN i HASŁO, które umożliwią korzystanie ze wszystkich funkcji platformy

Login to określenie identyfikujące użytkownika w systemie. W polu tym można wpisać dowolną nazwę. Musi być ona jednak unikalna. Utracony login nie jest możliwy do odtworzenia.

Hasło służy weryfikacji tożsamości osoby próbującej zalogować się na dane konto. Stanowi zabezpieczenie przed dostępem osób niepowołanych. System bada, czy wprowadzane hasło jest bezpieczne. Hasło bezpieczne to hasło długie, składające się z różnego rodzaju znaków (wielkie litery, małe litery, cyfry, inne znaki). Utracone hasło może być odtworzone.

Aukcja elektroniczna służy do wyboru oferty elektronicznej. Może być zastosowana w przetargu nieograniczonym, przetargu ograniczonym lub w negocja-

---

[35] http://www.mozilla-europe.org/pl/firefox/ (dostęp: 28.08.2020 r.).
[36] http://www.google.pl/chrome (dostęp: 28.08.2020 r.).
[37] *Portable Document Format.*
[38] http://get.adobe.com/reader/ (dostęp: 28.08.2020 r.).

cjach z ogłoszeniem, po przeprowadzeniu całkowitej oceny ofert. Informacja o zastosowaniu aukcji elektronicznej musi zawierać ogłoszenie o zamówieniu oraz w specyfikacja warunków zamówienia. Zamawiający wskazuje w ogłoszeniu o zamówieniu adres strony internetowej, na której będzie prowadzona aukcja elektroniczna. Kryteria oceny ofert stosowane w toku aukcji elektronicznej oraz sposób obliczania punktacji w ramach tych kryteriów muszą być identyczne z tymi, które były stosowane podczas oceny ofert w części tradycyjnej.

Aukcja zostaje otwarta w terminie wyznaczonym przez zamawiającego. Zamknięcie aukcji następuje w terminie zamknięcia albo w momencie, gdy przez czas określony przez zamawiającego nie zostaną złożone nowe postąpienia.

Zamawiający może przewidzieć, że w aukcji zostanie zastosowana tzw. dogrywka. Przewidzenie jej spowoduje, że w przypadku, gdy w momencie upływu terminu zamknięcia aukcji (lub okresu bezczynności) dwie lub więcej ofert miałoby uzyskać taką samą, a jednocześnie najwyższą punktację, aukcja nie zostanie zamknięta, lecz przedłużona o czas wskazany przez zamawiającego.

Początkowo w praktyce udzielania zamówień publicznych instytucja aukcji elektronicznej nie była zbyt często wykorzystywana. Sytuacja ta po części była spowodowana ograniczonym dostępem zamawiających do oprogramowania umożliwiającego prowadzenie aukcji elektronicznych (wszystkie działające na rynku platformy były płatne), a po części ogólnym brakiem zaufania do instrumentów elektronicznych. Aby to zmienić, w grudniu 2009 r. Urząd Zamówień Publicznych udostępnił do dyspozycji Platformę Aukcji Elektronicznych – pierwszy w Polsce w pełni bezpłatny system aukcyjny służący do prowadzenia aukcji elektronicznych zgodnie z ustawą – Prawo zamówień publicznych[39].

Aukcja elektroniczna jest nowoczesną i sprawdzoną formą realizowania zamówień publicznych. Świadczy o tym to, że w zasadzie przepisy zawarte w poprzednim akcie prawnym, który zostanie uchylony z dniem 1 stycznia 2021 r., nie zostały istotnie zmienione. Rekomendują ją także uregulowania międzynarodowe. Wykorzystanie środków komunikacji elektronicznej obniża koszty procedury zamówień publicznych oraz zapewnia prawidłowość i przejrzystość podejmowanych czynności. Uważa się, że stosowanie systemu aukcji elektronicznej powoduje oszczędności sięgające 20% wartości zamówienia[40].

## Bibliografia

Dzierżanowski W., Jerzykowski J., Stachowiak M., *Prawo zamówień publicznych. Komentarz,* wyd. VII Wolters Kluwer Polska 2018.

[39] M. Szymczak, *Aukcja elektroniczna. Praktyczny poradnik dla użytkowników Platformy Aukcji Elektronicznej*, UZP, Warszawa 2009. https://www.uzp.gov.pl/__data/assets/pdf_file/0018/24714/Aukcja_elektroniczna_poradnik.pdf (dostęp: 28.08.2020 r.).

[40] Tamże.

Nowicki J.E., Kołecki M., *Prawo zamówień publicznych. Komentarz*, wyd. IV, Wolters Kluwer Polska 2019.

Skubiszak-Kalinowska I., Wiktorowska E., *Prawo zamówień publicznych. Komentarz aktualizowany*, LEX/el. 2020.

Szymczak M., *Aukcja elektroniczna. Praktyczny poradnik dla użytkowników Platformy Aukcji Elektronicznej*, UZP, Warszawa 2009.

# Prawodawstwo

Dyrektywa 2014/24/UE z 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE.

Dyrektywa 2014/25/UE z 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (treść przepisu art. 35 zbliżona do przytoczonej wyżej).

Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniającą dyrektywy 2004/17/WE i 2004/18/WE (Dz. Urz. UEL 216 z 20 sierpnia 2009 r., s. 76, ze zm.).

Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz. Urz. UEL94 z 28 marca 2014 r., s. 65, ze zm.)

Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylającą dyrektywę 2004/17/WE (Dz. Urz. UEL 94 z 28 marca 2014 r., s. 243, ze zm.).

Dyrektywa Rady 89/665/EWG z 21 grudnia 1989 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do stosowania procedur odwoławczych w zakresie udzielania zamówień publicznych na dostawy i roboty budowlane (Dz. Urz. WE L 395 z 30 grudnia 1989 r., s. 33 ze zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 6, t. 1, s. 246).

Dyrektywa Rady 92/13/EWG z 25 lutego 1992 r. koordynującą przepisy ustawowe, wykonawcze i administracyjne odnoszące się do stosowania przepisów wspólnotowych w procedurach zamówień publicznych podmiotów działających w sektorach gospodarki wodnej, energetyki, transportu i telekomunikacji (Dz. Urz. WE L 76 z 23 marca 1992 r., s. 14, ze zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 6, t. 1, s. 315).

Ustawa z 7 kwietnia 2006 r. o zmianie ustawy Prawo zamówień publicznych oraz ustawy o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz.U. z 2006 r., nr 79, poz. 551).

# Netografia

http://get.adobe.com/reader/
http://www.google.pl/chrome
http://www.mozilla-europe.org/pl/firefox/
https://aukcje.uzp.gov.pl/index.php/page/selflearn/page/9
https://www.uzp.gov.pl/__data/assets/pdf_file/0018/24714/Aukcja_elektroniczna_poradnik.pdf

# E-MEDIACJA JAKO NOWOCZESNA TECHNOLOGIA ROZWIĄZYWANIA SPORÓW

*(Katarzyna Purc-Kurowicka)*

Nowoczesne technologie są obecnie największą siłą napędzającą gospodarkę. Umożliwiają szybszą, o wiele tańszą oraz lepszą pod względem jakościowym produkcję w porównaniu do poprzednich lat. Panująca sytuacja na rynkach wymaga od przedsiębiorstw nieustannego rozwoju, czyli szybkiego pojmowania i wdrażania zdobytej wiedzy. Nowe technologie znacznie poprawiają jakość oferowanych usług czy produktów i obniżają koszty. Jeszcze kilka lat temu dostęp do nowoczesnych technologii miały nieliczne grupy, ale aktualnie każdy człowiek w różny sposób z nich korzysta.

W ciągu ostatnich lat Internet zrewolucjonizował wiele aspektów naszego życia, dzięki czemu pojawiła się także możliwość wykorzystania globalnej sieci w zakresie rozwiązywania sporów[1]. E-mediacja, zwana też mediacją elektroniczną daje stronom konfliktu możliwość przeprowadzenia postępowania mediacyjnego online, czyli za pośrednictwem poczty elektronicznej, telefonu czy wideokonferencji. Jest to alternatywna metoda zarządzania konfliktem, w stosunku do postępowania sądowego, odzwierciedlająca mediację prowadzoną „twarzą w twarz". Służy ona zarówno rozwiązaniu sporu, jak i utrzymaniu dobrej relacji pomiędzy stronami oraz ułatwia stronom znalezienie satysfakcjonujących ich rozwiązań i zawarcie ugody na odległość, za pośrednictwem Internetu, przy użyciu elektronicznych środków komunikacji.

Obecnie społeczeństwo żyje w świecie coraz bardziej zmechanizowanym i skomputeryzowanym, w którym wymiana informacji jest szybka i sprawna. Dzięki powstaniu Internetu zmienił się sposób komunikacji i przede wszystkim szybkość i dokładność uzyskiwanych informacji. Bardzo popularne są zwłaszcza wszelkie nowoczesne technologie internetowe, które sprawdzają się również w miejscach pracy. Nowoczesne komputery i urządzenia biurowe znacznie przyspieszają czas pracy i poprawiają jej jakość. Mają wpływ na nasz styl życia, pracę oraz oczywiście relacje z innymi ludźmi. Ułatwiają nasze życie i czynią je wygodniejszym, bezpieczniejszym oraz łatwiejszym. Dlatego strony i mediatorzy coraz częściej z nich korzystają przy rozwiązywaniu sporów.

---

[1] Zob. M. Grabowski, E-*mediacja jako metoda rozwiązywania sporów w handlu elektronicznym*, http://arbitraz.laszczuk.pl/_adr/243/E-mediacja_jako_metoda_rozwiazywania_sporow_w_handlu_elektronicznym.pdf

Stosowanie Internetu jako środka komunikacji w praktyce prowadzi do dwóch podstawowych różnic. Po pierwsze, przeprowadzanie procedur online różni się od tradycyjnych metod mediacji w większości przypadków tekstową formą komunikacji, a po drugie – asynchronią. Zdarza się, że telekonferencja jest czasami używana jako wspierający środek komunikacji, jednak e-mediacja z reguły ogranicza się do e-maili i tekstowych form komunikacji na *chatach* internetowych. Z tego względu wykluczone są zwykle z niej takie elementy, jak język ciała i ton głosu[2].

Aktualne metody określane jako *online dispute resolution* (ODR) służą przede wszystkim rozwiązywaniu sporów typowych dla Internetu, np. wynikających z powszechnie zawieranych transakcji handlowych. Jednak nie oznacza to, że potencjał globalnej sieci nie może być wykorzystany także w zakresie rozwiązywania wszelkiego rodzaju konfliktów, w których do tej pory posługiwano się tradycyjnymi metodami mediacji[3].

E-mediacja, podobnie jak mediacja tradycyjna, charakteryzuje się podstawowymi zasadami, takimi jak poufność, dobrowolność, odformalizowanie, samodzielność w podejmowaniu decyzji, akceptowalność, czy neutralność i bezstronność mediatora. Podobnie jak do mediacji tradycyjnej mogą być do niej kierowane sprawy, w których toczy się już postępowanie sądowe (mediacja sądowa), jak również te, co do których strony zdecydowały się na prowadzenie mediacji na podstawie umowy przed skierowaniem sprawy do sądy lub w toku postępowania sądowego (mediacja umowna).

Korzyści wynikających z e-mediacji, jako pozasądowego sposobu rozwiązywania sporu, jest wiele. Zasadnicza, to przede wszystkim szybkie i wygodne rozstrzygnięcie konfliktu. Kiedy stronom zależy na jak najszybszym ułożeniu sobie życia ponownie, na powrocie do względnej równowagi, czy na rozstrzygnięciu konkretnych kwestii – to e-mediacja jest pożądana jako metoda, która szybko przynosi rezultaty. Z tego względu, że e-mediacja odbywa się w sieci, wszyscy uczestnicy mogą się zalogować na posiedzenie mediacyjne w dowolnym czasie i z dowolnego miejsca. Czas e-mediacji jest zawsze krótszy niż postępowania sadowego, albowiem w sprawach cywilnych sąd wyznacza czas jej trwania na okres do trzech miesięcy, a w sprawach karnych nie powinna trwać dłużej niż miesiąc[4]. Dodatkowo elastyczność terminów spotkań z mediatorem jest nieporównywalnie większa, niż ta związana z zawiadomieniem o terminie rozprawy. Jednak zasadnicze znaczenie w tym zakresie ma okoliczność, że e-mediacja pozwala na korzystanie z narzędzi elektronicznych, które ułatwiają i usprawniają kontakt pomiędzy

---

[2] M. Wasylkowska-Michór, *Mediacja elektroniczna w sprawach transgranicznych* [w:] *Mediacje w społeczeństwie otwartym*, red. M. Tabernacka, R. Raszewska-Skałecka, Wrocław 2012, s. 286.

[3] S. Kordasiewicz, *Historyczna i międzynarodowa pespektywa mediacji*, [w:] *Mediacje. Teoria i praktyka*, red. E. Gmurzyńska, R. Morka, Warszawa 2009, WoltersKluwer, Warszawa 2009, s. 48.

[4] Art. $183^{10}$§ 1 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2019 r., poz. 1460 ze zm.) i art. 23a § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. z 2018 r., poz. 1987 ze zm.).

stronami i mediatorem. Możliwość skorzystania z poczty elektronicznej i telefonu przy ustalaniu terminu i miejsca posiedzenia mediacyjnego, czy zorganizowanie wideokonferencji w sytuacjach, gdy strony mają siedzibę, czy miejsce zamieszkania poza miejscem działalności mediatora, znacznie przyspiesza i ułatwia przeprowadzenie mediacji i jest najbardziej efektywną formę przeprowadzenia postępowania mediacyjnego. Oczywiście to od stron zależy, czy skorzystają z tej formy kontaktu, albowiem do pojednania się w e-mediacji konieczna jest, tak samo jak w mediacji tradycyjnej, dobra wola strony[5].

Następną zaletą wynikającą z e-mediacji jest asynchroniczna komunikacja, która pozwala stronom konfliktu na prowadzenie dyskusji, w której nie oczekuje się natychmiastowej odpowiedzi. Podczas e-mediacji mediator może przeformułować wypowiedź jednej ze stron, zanim dotrze ona do drugiej strony, w taki sposób, aby nie zaostrzać konfliktu. Dzięki globalnej sieci mediator może prowadzić mediację w sposób wahadłowy i umożliwić stronom przemyślenie sytuacji, czy zdobycie dodatkowych informacji sprzyjających ugodzie w trakcie jednego posiedzenia. Podczas posiedzenia e-mediacyjnego każda ze stron może dowiedzieć się, jakie są motywy działania drugiej strony. Zdarza się, że strony konfliktu dowiadują się w trakcje mediacji czegoś nowego, co pozwala inaczej spojrzeć na drugą stronę, czy na cały konflikt i ułatwia zawarcie ugody. E-mediacja rozwija świadomość stron dotyczącą potrzeby tworzenia różnorodnych rozwiązań, zmniejsza też przywiązanie stron do swoich stanowisk i tworzy rozwiązania przy użyciu przetargu biorącego pod uwagę interesy stron. Dzięki skorzystaniu z procedury mediacyjnej podmioty w niej uczestniczące mogą aktywniej i efektywniej uczestniczyć w realizowaniu swoich celów oraz zadań[6].

W klasycznym postepowaniu mediacyjnym z reguły mamy do czynienia z trzema stronami, z których trzecia to neutralny mediator. Natomiast w e-mediacji wyróżnia się cztery, a nawet pięć stron, z czego czwarta to technologia, np. e-mail, *chat roomy*, czy wideokonferencja, a piąta to dostawca technologii, np. właściciel strony internetowej, która oferuje narzędzia umożliwiające prowadzenie mediacji[7]. W tradycyjnych mediacjach ustalenie terminu posiedzenia stanowi czasami duży problem, w szczególności, jeżeli w mediacji poza stronami biorą udział ich pełnomocnicy. Oznacza to bowiem, że termin posiedzenia musi pasować 5 osobom, a w przypadku dwóch mediatorów biorących udział w mediacji 6 osobom. W takim wypadku e-mediacja jest najlepszym narzędziem, bowiem łatwiej każdemu znaleźć czas na podłączenie się do sieci, niż na przyjazd i bezpośrednią rozmowę. E-mediacja umożliwia stronom samodzielne negocjowanie porozumienia,

---

[5] Art. $183^8$§ 2 k.p.c. stanowi, że „mediacji nie prowadzi się, jeżeli strona w terminie tygodnia od dnia ogłoszenia lub doręczenia jej postanowienia kierującego strony do mediacji nie wyraziła zgody na mediację". Szerzej na temat braku motywacji stron do wypracowani porozumienia zob.: M. Kaźmierczak, J. Kaźmierczak, *Mediacja rodzinna. Praktyczny poradnik*, Difin, Warszawa 2015, s. 125.

[6] A. Binsztok (red.), *Sztuka skutecznego prowadzenia mediacji – zagadnienia prawne i ekonomiczne*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2012, s. 15.

[7] M. Wasylkowska-Michór, *Mediacja elektroniczna w sprawach…*, s. 287.

a strony, które samodzielnie ustaliły warunki porozumienia, mają większą kontrolę nad ostatecznym wynikiem ugody. Brak ingerencji sądu, jako podmiotu o cechach arbitralnych, zdecydowanie zmniejsza antagonizmy i wzmaga naturalną potrzebę porozumienia[8].

E-mediacja, podobnie jak mediacja tradycyjna, ułatwia osiąganie porozumienia w drodze negocjacji poprzez stopniowe zbliżenie stanowisk i wypracowanie zasad akceptowanych przez obie strony. W sądzie nie ma na to miejsca. W e-mediacji straty i zyski są bardziej przewidywalne w porównaniu z sytuacją, w której sprawa zostaje skierowana do sądu. W efekcie wzmacnia to poczucie własnej kompetencji i możliwości w odróżnieniu od sytuacji, kiedy strony powierzają reprezentowanie swoich interesów osobom trzecim. Najistotniejszą sprawą jest jednak fakt, że podczas e-mediacji same strony konfliktu szukają rozwiązań dla nich odpowiednich – nie mediatorzy, nie pełnomocnicy, czy sąd. To z kolei uczy strony samodzielnego rozwiązywania problemów w przyszłości. Strony jako „właściciele" konfliktu mają prawo do wyboru stylu reagowania na konflikt i do kontroli nad jego przebiegiem i zakończeniem, a także do wyboru metody mediacji[9].

Niestety, mediacja w sieci stwarza też zagrożenie dla ochrony prywatności i zasady poufności mediacji, albowiem w praktyce nie ma możliwości zagwarantowania, że jedna ze stron konfliktu nie skopiuje zapisu toczącej się rozmowy i nie wykorzysta go w przyszłości[10]. Jednak takiej gwarancji nie ma też i w mediacjach tradycyjnych, podczas których strony mogą nagrać przebieg posiedzenia. W obu przypadkach istotne jest, aby obowiązująca mediatora zasada poufności zawarta w art. $183^4$ k.p.c., wzmacniała komfort odbywanych posiedzeń i mobilizowała strony do aktywnego i nieskrępowanego wyrażania własnych poglądów, co często nie jest możliwe podczas postępowania sądowego, gdzie strony są sparaliżowane przez stres.

Istotną korzyścią e-mediacji jest okoliczność, że podczas posiedzeń w sieci strony zachowują pomiędzy sobą większy dystans i redukują siłę negatywnych emocji podczas komunikacji. Taki element w ogóle nie jest brany pod uwagę w postępowaniu sądowym, a przecież decyzyjność stron wpływa na osiągnięcie satysfakcji psychicznej, bowiem porozumienie osiągnięte w wyniku mediacji obejmuje również kwestie proceduralne i psychologiczne, które nie zawsze mogą być rozstrzygnięte na drodze sądowej[11]. W wymiarze psychologicznym e-mediacja przede wszystkim kształtuje pożądane cechy i postawy stron konfliktu oraz zaspokaja ich wewnętrzne potrzeby w postaci szacunku, wysłuchania, docenienia,

---

[8] K. Flaga-Gieruszyńska, *Kilka uwag o mediacji jako instrumencie efektywnego rozstrzygania sporów gospodarczych* [w:] *Arbitraż i mediacja. Praktyczne aspekty stosowania przepisów*, red. J. Olszewski, TNOiK, Rzeszów 2007, s. 86.

[9] A. Kalisz, A. Zienkiewicz (red.), *Elementy teorii konfliktu i rozwiązywania sporów* [w:] *Mediacja sądowa i pozasądowa. Zarys wykładu*, WoltersKluwer, Warszawa 2014, s. 59.

[10] S. Kordasiewicz, *Historyczna i międzynarodowa*…, s. 48.

[11] Szerzej na temat satysfakcji z mediacji zob.: J.M. Łukasiewicz, *Naczelne zasady mediacji* [w:] *Zarys metodyki pracy mediatora w sprawach cywilnych*, red. A.M. Arkuszewska, J. Plis, Wolters Kluwer, Warszawa 2014, s. 87.

akceptacji, przeproszenia, zrozumienia, tolerancji, czy wyładowania negatywnych emocji[12]. E-mediacja pozwala na odkrywanie ukrytych interesów stron i umożliwia wymianę poglądów, w sposób dopasowany do specyfiki swojej sytuacji, co w budynku sądu jest w dużym zakresie ograniczone. Jednakże w tego typu procedurach łatwiej o zablokowanie procesu mediacji, bowiem każda ze stron może przestać reagować na wiadomości i pytania. W niebezpośredniej komunikacji strony mogą łatwiej przekazywać sobie błędne lub nieprawdziwe informacje. Dlatego w e-mediacji niezmiernie ważne jest, aby mediator utrzymywał stały kontakt ze stronami i czuwał nad zachowaniem pozytywnych relacji między zainteresowanymi. Brak komunikacji werbalnej powoduje duże trudności ze zbudowaniem i utrzymaniem życzliwych relacji pomiędzy stronami, czy zapewnieniem właściwej atmosfery prowadzenia rozmów[13].

Z powyższego względu niezmiernie ważny jest wybór odpowiedniego mediatora do danego rodzaju sprawy, który będzie w stanie utrzymać pomiędzy stronami łączące je stosunki lub zakończy je w spokojnej atmosferze, pozbawionej agresji i wrogości. E-mediacje daje taką możliwość, gdyż wybór odpowiedniego mediatora jest niezależny od ograniczeń geograficznych. Dzięki sprawnemu mediatorowi zostaje wyeliminowana konfrontacja i dążenie do wygrania przez którąś ze stron. Jest to tym bardziej ważne, że w przypadku rodziny wygrana oznacza najczęściej przegraną dla pozostałych członków rodziny (w tym dzieci), a w wielu przypadkach jest przegraną dla wszystkich. Walka przed sądem nie pozwala na zachowanie równowagi pomiędzy stronami, co powoduje podział na wygranych i przegranych, a to oznacza dalsze kłopoty dla rodziny, nawet po jej rozpadzie. Rodzą się emocje charakterystyczne dla przegranych takie jak: żal, poczucie pokrzywdzenia, złość, bezradność, chęć odwetu, sabotowania warunków postanowienia sądowego itp. Siła tych emocji jest najczęściej duża i paraliżuje trwałość postanowień sądu. Sprawy wracają kolejny raz na wokandę i cała historia walki o wygraną powtarza się[14]. W przypadku konfliktów towarzyszących rozwodowi e-mediacja może prowadzić do uniknięcia rywalizacji w postępowaniu sądowym oraz ułatwić rodzicom kooperację w kwestiach związanych z opieką nad dziećmi[15]. E-mediacja rodzinna dla skonfliktowanych członków rodzin to szansa, że rezygnując z procedury sądowej, będą mogli rozwiązywać swoje spory polubownie, w mniej sformalizowanej atmosferze, poszukując rozwiązań dostosowanych do szczególnych potrzeb swoje rodziny[16]. W tym przypadku e-mediacja służy

---

[12] Szerzej na ten temat: A. Kalisz, A. Zienkiewicz (red.), *Elementy teorii konfliktu.…*, s. 44.

[13] S. Kordasiewicz, *Historyczna i międzynarodowa...*, s. 49.

[14] H. Przybyła-Basista, *Proces mediacji rodzinnych – od teorii do praktyki*, „Mediator" 2002, nr 21, s. 11.

[15] Szerzej na temat mediacji rozwodowych: A. Milne, J. Folberg, *The theory and practice of divorce mediation: an overview* [In:] *Divorce mediation. Theory and practice*, eds. J. Folberg, A. Milne, The Guilford Press, New York–London 1988, s. 12.

[16] Na temat efektywności procesu mediacji rodzinnych zob.: H. Przybyła-Basista, *Mediacje rodzinne w konflikcie rozwodowym. Gotowość i opór małżonków a efektywność procesu mediacji*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2006, s. 161.

zatem zmniejszeniu lub wygaszeniu konfliktu istniejącego między stronami, co jest tym łatwiejsze do osiągnięcia, że osoby dotychczas pozostające w konflikcie są równouprawnionymi partnerami w rozmowie, w poszukiwaniu rozwiązania dzielącego ich sporu i nie muszą ze sobą rozmawiać bezpośrednio[17].

Jednym z najkorzystniejszych profitów e-mediacji, jest jej tani koszt. Jest to metoda rozwiązywania konfliktów opłacalna w porównaniu z kosztami związanymi z procesem sądowym, czy nawet mediacją tradycyjną. W przypadku e-mediacji żaden z jej uczestników nie musi nigdzie się udawać, żeby w niej uczestniczyć. Wystarczy, że za pomocą odpowiedniego środka komunikacji elektronicznej przyłączy się do dyskusji. Dzięki temu koszty e-mediacji nie będą obejmowały chociażby kosztów dojazdów mediatora do miejsca spotkania, czy kosztów wynajęcia lokalu. W klasycznym postępowaniu mediacyjnym strony z reguły obciążone są kosztami związanymi z wynagrodzeniem mediatora, ale także pozostałymi, tj. koniecznymi do przeprowadzenia mediacji. E-mediacja umożliwi ich uniknięcie. Koszty mediacji online nie zostały uregulowane odrębnie, dlatego należy do niej stosować te same przepisy co w przypadku mediacji tradycyjnych. Oznacza to, że w sprawach cywilnych, w tym rodzinnych, gospodarczych i z zakresu prawa pracy, koszty e-mediacji reguluje rozporządzenie Ministra Sprawiedliwości z dnia 20 czerwca 2016 r. w sprawie wysokości wynagrodzenia i podlegających zwrotowi wydatków mediatora w postępowaniu cywilnym[18]. Natomiast w sprawach karnych art. 619 § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, który kosztami postępowania mediacyjnego obciąża Skarb Państwa[19].

Z powyższego jednoznacznie wynika, że nowe technologie w zasadniczym stopniu wpływają na codzienne życie. Praktycznie nie można już znaleźć takiej dziedziny ludzkiej działalności, w której informatyka i jej narzędzia nie znajdowałyby zastosowania. Ma to miejsce także i w mediacjach, w których wykorzystywanie informatyki jest jak najbardziej uzasadnione, chociażby ze względu na fakt, że „materiałem roboczym" w przedmiotowej dziedzinie są dane, czy informacja, a potrzeba zapewnienia przejrzystości w prowadzeniu mediacji zmusza do zastosowania informatyki w maksymalnym możliwym zakresie[20]. Ważnym aspektem tej nowej technologii w prowadzeniu mediacji jest nie tylko zapewnienie stronom postępowania możliwości skorzystania z udogodnień, jakie niesie za sobą informatyzacja[21], ale również bezpieczeństwa takiego postępowania. Z tego względu

---

[17] A. Pietrzkiewicz, *Mediacje rodzinne w polskim systemie prawnym*, Wyższa Szkoła Biznesu i Przedsiębiorczości w Ostrowcu Świętokrzyskim, Ostrowiec Świętokrzyski 2016, s. 237.

[18] Dz.U. z 2016 r., poz. 921 ze zm.

[19] Dz.U. z 2018 r., poz. 1987 ze zm.

[20] K. Wojsyk, *Oddziaływanie prawa nowych technologii na funkcjonowanie wymiaru sprawiedliwości w społeczeństwie informacyjnym – aspekty społeczne* [w:] *Informatyzacja postępowania sądowego i administracji publicznej*, red. J. Gołaczyński, Warszawa 2010, s. 169.

[21] Pojęcie to zostało wprowadzone do polskiego porządku prawnego ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U. z 2020 r., poz. 3465 ze zm.). Pojęcia tego nie należy mylić z komputeryzacją, o czym szerzej S. Kotecka, *Informatyzacja postępowania cywilnego w Polsce* [w:] *Informatyzacja postępowania…*, s. 3 i 4.

e-mediacja powinna zapewniać ogólną sprawność, a także rzetelność i kulturę w traktowaniu pojedynczego obywatela[22]. Powinna wiązać się z realizacją podstawowych publicznych praw podmiotowych obywateli, a więc także z realizacją prawa podmiotowego do zapewnienia obywatelowi bezpieczeństwa wewnętrznego.

Mediacja prowadzona za pośrednictwem elektronicznych środków komunikacji stanowi jeden z etapów informatyzacji społeczeństwa. Jej wprowadzenie jest wymuszone aktualnym poziomem rozwoju technik informatycznych, które wkraczają do różnych dziedzin życia społecznego, w tym także do obrotu prawnego pozasądowego, jak i sądowego[23]. Informatyzacja, jako środek zapewniający praktyczną skuteczność pracy mediatora, stała się istotnym środkiem ochrony i nadzoru nad podstawowymi gwarancjami obywatela w państwie prawa[24]. Jednakże należy mieć na uwadze, że nowoczesne technologie pełnią istotną rolę w mediacji, ale jedynie wspierają mediatorów i w żadnym wypadku system teleinformatyczny nie zastąpi człowieka. Należy podkreślić, że system teleinformatyczny zawsze będzie pełnił służebną rolę względem czynności podejmowanych przez mediatorów. Dzięki wykorzystaniu nowych technologii poprawia się efektywności prowadzenia mediacji i zwiększą się ich skala.

Znaczenie mediacji online rośnie i można przypuszczać, że wzrost ten będzie systematyczny, przede wszystkim ze względu na dynamiczny rozwój globalnej społeczności użytkowników sieci. O rozwoju tej dziedziny świadczy także wzrastająca liczba nowych dostawców tego typu energii. Nowoczesne technologie, w tym Internet, wyraźnie zapewniają skuteczną ochronę prawną osobom korzystającym z e-mediacji.

## Bibliografia

Binsztok A. (red.), *Sztuka skutecznego prowadzenia mediacji – zagadnienia prawne i ekonomiczne*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2012.

Boć J., *O bezpieczeństwie wewnętrznym* [w:] *Bezpieczeństwo wewnętrzne w działaniach terenowej administracji publicznej*, red. A. Chajbowicz, T. Kocowski, Wrocław 2009.

Cieślak S., *Elektroniczne postępowanie upominawcze*, „Monitor Prawniczy" 2010, nr 7.

Flaga-Gieruszyńska K., *Kilka uwag o mediacji jako instrumencie efektywnego rozstrzygania sporów gospodarczych* [w:] *Arbitraż i mediacja. Praktyczne aspekty stosowania przepisów*, red. J. Olszewski, Rzeszów 2007.

---

[22] J. Boć, *O bezpieczeństwie wewnętrznym* [w:] *Bezpieczeństwo wewnętrzne w działaniach terenowej administracji publicznej*, red. A. Chajbowicz, T. Kocowski, Wrocław 2009, s. 25.

[23] S. Cieślak, *Elektroniczne postępowanie upominawcze*, „Monitor Prawniczy" 2010, nr 7, s. 359.

[24] A. Pyszny, *Informatyzacja sądownictwa – szansa czy zagrożenie dla wymiaru sprawiedliwości*, [w:] *Elektroniczne aspekty wymiaru sprawiedliwości: materiały z Konferencji zorganizowanej przez Instytut Prawa Wydziału Zamiejscowego Nauk o Społeczeństwie w Stalowej Woli w Katolickim Uniwersytecie Lubelskim Jana Pawła II*, red. G. Tylec, J. Misztal-Konecka, Bydgoszcz––Lublin 2009, s. 67.

Grabowski M., E-*mediacja jako metoda rozwiązywania sporów w handlu elektronicznym*, http://arbitraz.laszczuk.pl/_adr/243/E-mediacja_jako_metoda_rozwiazywania_sporow_w_handlu_elektronicznym.pdf

Kalisz A., Zienkiewicz A. (red.), *Elementy teorii konfliktu i rozwiązywania sporów* [w:] *Mediacja sądowa i pozasądowa. Zarys wykładu*, WoltersKluwer, Warszawa 2014.

Kaźmierczak M., Kaźmierczak J., *Mediacja rodzinna. Praktyczny poradnik*, Difin, Warszawa 2015.

Kordasiewicz S., *Historyczna i międzynarodowa pespektywa mediacji* [w:] *Mediacje. Teoria i praktyka*, red. E. Gmurzyńska, R. Morka, WoltersKluwer, Warszawa 2009.

Kotecka S., *Informatyzacja postępowania cywilnego w Polsce*, [w:] *Informatyzacja postępowania sądowego i administracji publicznej*, red. J. Gołaczyński, Warszawa 2010.

Łukasiewicz J.M., *Naczelne zasady mediacji* [w:] *Zarys metodyki pracy mediatora w sprawach cywilnych*, red. A.M. Arkuszewska, J. Plis, WoltersKluwer, Warszawa 2014.

Milne A., Folberg J., *The theory and practice of divorce mediation: an overview* [In:] *Divorce mediation. Theory and practice*, eds. J. Folberg A., Milne, The Guilford Press 1988, New York–London 1988.

Pietrzkiewicz A., *Mediacje rodzinne w polskim systemie prawnym*, Wyższa Szkoła Biznesu i Przedsiębiorczości w Ostrowcu Świętokrzyskim, Ostrowiec Świętokrzyski 2016.

Przybyła-Basista H., *Mediacje rodzinne w konflikcie rozwodowym. Gotowość i opór małżonków a efektywność procesu mediacji*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2006.

Przybyła-Basista H., *Proces mediacji rodzinnych – od teorii do praktyki*, „Mediator" 2002, nr 21.

Pyszny A., *Informatyzacja sądownictwa – szansa czy zagrożenie dla wymiaru sprawiedliwości* [w:] *Elektroniczne aspekty wymiaru sprawiedliwości: materiały z Konferencji zorganizowanej przez Instytut Prawa Wydziału Zamiejscowego Nauk o Społeczeństwie w Stalowej Woli w Katolickim Uniwersytecie Lubelskim Jana Pawła II*, red. G. Tylec, J. Misztal-Konecka, Bydgoszcz–Lublin 2009.

Wasylkowska-Michór M., *Mediacja elektroniczna w sprawach transgranicznych* [w:] *Mediacje w społeczeństwie otwartym*, red. M. Tabernacka, R. Raszewska-Skałecka, Gaskor, Wrocław 2012.

Wojsyk K., *Oddziaływanie prawa nowych technologii na funkcjonowanie wymiaru sprawiedliwości w społeczeństwie informacyjnym – aspekty społeczne* [w:] *Informatyzacja postępowania sądowego i administracji publicznej*, red. J. Gołaczyński, Warszawa 2010.

## Prawodawstwo

Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (tekst jedn. Dz.U. z 2019 r., poz. 1460 ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jedn. Dz.U. z 2018 r., poz. 1987 ze zm.)

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U. z 2020 r., poz. 345 ze zm.).

# PRAWNE ASPEKTY GŁOSOWANIA ELEKTRONICZNEGO W POLSCE

(*Wojciech Gryzik*)

## Wprowadzenie

Wybory w państwach demokratycznych odgrywają bardzo ważną rolę. Od czasu II wojny światowej znaczenie przeprowadzania wyborów w państwach demokratycznych ma ciągłą tendencję wzrostową. Od lat 60. liczba przeprowadzonych wyborów na wszystkich szczeblach i do wszystkich organów wzrosła ponad dwukrotnie. Wzrost częstotliwości wyborów w państwach Unii Europejskiej jest związany z wyborami do Parlamentu Europejskiego. Udział w wyborach w państwach demokratycznych jest jednym z praw podstawowych wszystkich obywateli. W Polsce prawa wyborcze zapisane są w Konstytucji Rzeczypospolitej Polskiej. Dzielą się one na bierne (prawo do kandydowania) i czynne (prawo wybierana) prawo wyborcze. Znaczenie wyborów, podobnie jak frekwencja wyborcza w Polsce stale rośnie, co jest związane z rozwojem społeczeństwa obywatelskiego oraz większym zainteresowaniem obywateli z kwestiami politycznymi[1].

## Alternatywne metody głosowania w polskim prawie

Głosowanie elektroniczne jest jedną z alternatywnych procedur głosowania, obok głosowania korespondencyjnego, przez pełnomocnika oraz mobilnej urny wyborczej. W Polsce kodeks wyborczy dopuszcza jedynie głosowanie osobiste, korespondencyjne oraz głosowanie przez pełnomocnika. Metodę głosowania elektronicznego (*e-voting*), czyli oddanie własnego głosu za pomocą specjalnej maszyny elektronicznej znajdującej się w lokalu wyborczym lub w wyznaczonych miejscach publicznym. W tym przypadku głosujący, podobnie jak w tradycyjnej metodzie, musi udać się do lokalu wyborczego lub specjalnie wyznaczonego do tego punktu. Przykładem państwa, w którym powszechnie wykorzystuje się maszyny do głosowania są Stany Zjednoczone Ameryki. Początki powszechnego wykorzystywania maszyn do głosowania elektronicznego w USA sięgają lat 80. XX wieku. Pomimo dość długiego czasu, od kiedy Amerykanie mogą oddawać głosy w sposób elektroniczny, system oraz maszyny do głosowania nie pozostają bez

[1] M. Chrzanowski, *Podstawowe zasady prawa wyborczego do organów stanowiących jednostek samorządu terytorialnego,* Białystok 2018, s. 12–13.

wad. Najlepszym tego przykładem mogą być wybory prezydenckie w 2000 roku. Różnica otrzymanych głosów pomiędzy dwoma głównymi kandydatami w stanie Floryda wyniosła zaledwie 1784 głosy, co stanowiło mniej niż pół procenta oddanych głosów. W wyniku tego przeprowadzono ponownie maszynowe liczenie głosów, co spowodowało zmniejszenie przewagi George'a W. Busha nad Al Gore. W związku z tym kandydat demokratów złożył skargę do Sądu Najwyższego Florydy, który nakazał ponowne przeliczenie nieważnych głosów w kilku hrabstwach. Po ręcznym przeliczeniu głosów okazało się, że co prawda nadal zwycięzcą pozostał George W. Bush, lecz jego przewaga zmniejszyła się do 537 głosów. Przyczyną tego był błąd maszyn wyborczych, które część oddanych prawidłowo głosów uznały za nieważne[2]. Poza e-votingiem wyróżnia się także i-voting, który zakłada możliwość oddania głosu w sposób zdalny za pomocą Internetu, bez konieczności opuszczania miejsca zamieszkania lub z dowolnej lokalizacji. Głosowanie elektroniczne zaliczane jest do szerszej grupy zwanej e-demokracją. Zaletami głosowania elektronicznego są między innymi: możliwość zastosowania w wyborach powszechnych oraz referendach, niski koszt obsługi wyborów (brak konieczności zwoływania komisji wyborczej), możliwość glosowania osób znajdujących się poza miejscem zamieszkania oraz poza granicami kraju. Wadą elektronicznego systemu jest konieczność stworzenia odpowiedniego systemu informatycznego zdolnego zapewnić bezpieczeństwo oraz zapobiec fałszerstwom, a także konieczność zachowania zasad prawa wyborczego ze szczególnym uwzględnieniem zasady tajności głosowania, której przestrzeganie w przypadku głosowania elektronicznego jest najtrudniejsze[3].

W Polsce w porównaniu z innymi krajami Unii Europejskiej nie prowadzono obszernych badań poświęconych technikom głosowania elektronicznego. Badania, które zostały wykonane, dotyczyły jedynie specjalnych maszyn do głosowania, które miały być umieszczone w lokalach wyborczych, nie zaś możliwości głosowania poza lokalem lub przez Internet. Pierwszą próbę glosowania przez Internet podjęto w 2008 roku, kiedy to odpowiedzialny za zmiany ordynacji wyborczych w ówczesnym rządzie Waldy Dzikowski zapowiedział, że możliwe jest wprowadzenie głosowania przez Internet już w wyborach do Europarlamentu w 2009 roku, czego jednak nie udało się wykonać. Problematyką wprowadzenia zmian w kodeksie wyborczym i uruchomieniem sprawnego systemu wyborczego zajęły się Państwowa Komisja Wyborcza oraz specjalnie powołany zespół w Ministerstwie Spraw Wewnętrznych i Administracji. Prace zostały zawieszone ze względu na problemy techniczne[4].

---

[2] M. Radajewski, *Weryfikacja ważności wyników wyborów na przykładzie sprawy Bush v. Gore*, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2016, s. 343–344.

[3] K. Duda, *E-voting jako forma demokracji bezpośredniej. Dotychczasowe doświadczenia i ich konsekwencje*, „Refleksje Pismo Naukowe Studentów i Doktorantów WNPiD UAM" 2011, nr 4, s. 161.

[4] J. Zbieranek, *Alternatywne procedury głosowania w Polsce na tle państw Unii Europejskiej*, Studia BAS, 2011, nr 3(27), s. 114-115.

Konstytucja Rzeczypospolitej Polskiej nie określa w żaden sposób metody głosowania elektronicznego. Ustawa zasadnicza jednoznacznie nie dopuszcza oraz nie zakazuje wprowadzenia takiej możliwości. Kwestia związana e-wyborami została całkowicie pominięta przez polski porządek prawny, co wiąże się z datą ogłoszenia Konstytucji, gdyż w tamtych czasach temat głosowania elektronicznego nie był poddawany dyskusji społecznej i politycznej. W wyniku tego decyzja o możliwości wprowadzenia innych metod głosowania jest zależna jedynie od decyzji sejmu i zmiany kodeksu wyborczego, jednak z zachowaniem wszystkich konstytucyjnych zasad wyborczych[5]. W polskim prawie wyborczym aktualnie nie ma wzmianki o metodzie głosowania elektronicznego. Kodeks wyborczy dopuszcza jedynie możliwość oddania głosu osobiście w lokalu wyborczym, korespondencyjnie w przypadku osoby niepełnosprawnej oraz przez pełnomocnika, również w przypadku osoby niepełnosprawnej i osoby, która ukończyła 75 lat. Art. 39 wyraźnie mówi, że głosowanie odbywa się w lokalu obwodowej komisji wyborczej. Wprowadzenie głosowania elektronicznego musiałoby się wiązać ze zmianą kodeksu wyborczego, który dawałby możliwość oddania głosu spoza określonego lokalu wyborczego[6].

## Głosowanie elektroniczne a zasady wyborcze

Największym wyzwaniem, przed którym stoi polski ustawodawca, jest utworzenie sprawnie działającego systemu informatycznego, który będzie w stanie zagwarantować przestrzeganie podstawowych zasad prawa wyborczego, któremu podlegają wszystkie metody głosowania, zaliczając do tego katalogu głosowanie elektroniczne. Konstytucja Rzeczypospolitej Polskiej wyróżnia pięć podstawowych zasad wyborczych. Należą do nich: zasada powszechności, równości, bezpośredniości, proporcjonalności oraz tajności[7].

## Zasada powszechności

Zasada ta wyznacza ściśle określony krąg osób, które mają uprawnienia do udziału w wyborach. Jest ona uznawana za najważniejszą zasadę wyborczą w krajach demokratycznych. Zasada ta daje prawo wszystkim obywatelom Polski, którzy najpóźniej w dniu wyborów ukończyli 18 lat, mają obywatelstwo polskie oraz nie zostały im odebrane prawa wyborcze. Głosowanie elektroniczne w żadnym stopniu nie łamie zasady powszechności, a wręcz przeciwnie, daje możliwość udziału w wyborach osobą, które nie mają możliwości udania się do lokalu

---

[5] M. Musiał-Karg, *Głosowanie elektroniczne jako alternatywna metoda uczestnictwa w wyborach – opinie Polaków*, Political Preferences, Poznań 2015, nr 10, s. 90.

[6] Ustawa z dnia 5 stycznia 2011 r., Kodeks wyborczy (stan prawny na dzień 10 sierpnia 2019 r.).

[7] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483 ze zm.).

wyborczego z różnorakich powodów. Można więc założyć, że wprowadzenie głosowania elektronicznego w znacznym stopniu przyczyni się do wzrostu frekwencji wyborczej. Ważne jest, aby taki sposób oddania głosu był możliwy jako alternatywna metoda, a nie jako główna i tradycyjna, ponieważ uniemożliwiłoby to oddanie głosu osobom, które nie mają dostępu do Internetu, których wbrew pozorom w Polsce jest znaczna liczba i tyczy się głównie osób starszych (dotyczy jedynie głosowania przez Internet, a nie poprzez system informatyczny w lokalu wyborczym). Byłoby to złamaniem zasady powszechności, gdyż uniemożliwiłoby wzięcie udziału w wyborach przez określony krąg ludzi[8].

## Zasada równości

Zasada równości w kontekście prawa wyborczego ma trzy aspekty: równość materialną, równość formalną oraz równość szans. Równość materialna polega na tym, że każdy oddany glos ma taką samą siłę. Równość formalna odnosi się do równej liczby głosów, jaką może oddać każdy wyborca. Równość szans polega na zapewnieniu przez ustawodawcę równej dla wszystkich procedury wyborczej, tyczy się ona biernego prawa wyborczego i daje wszystkim kandydatom i komitetom wyborczym równe szanse. Z punktu widzenia głosowania elektronicznego zasada równości zostanie zachowana. Głosowanie elektroniczne nie wpłynie na aspekt równych szans oraz aspekt materialny. Zmiana sposobu głosowania z tradycyjnego nie ma żadnego wpływu na siłę głosu wyborców.

Wyzwaniem, jakie stoi przed ustawodawcą, jest zapewnienie zachowania aspektu formalnego, aby każdy wyborca posiadał taką samą liczbę głosów. Problemem równości formalnej przy stosowaniu głosowania elektronicznego jest możliwość oddania przez wyborcę dwóch głosów, w sposób tradycyjny i elektroniczny. W Estonii problem tez został rozwiązany poprzez wprowadzenie głosowania wcześniejszego, które umożliwia zmianę głosu oddanego za pomocą Internetu, w sposób tradycyjny, co wiąże się z unieważnieniem wyboru dokonanego w głosowaniu elektronicznym. Metoda ta znacznie zwiększa bezpieczeństwo wyborów, jednak nie eliminuje całkowicie podatności na manipulacje związane ze zmianą głosów. Sposobem na zabezpieczenie głosowania elektronicznego jest wprowadzenie potwierdzeń treści oddanego głosu, które następnie można porównać z wynikami po zakończeniu głosowania, podanego przez system wyborczy. Wprowadzenie takich metod zabezpieczenia wyborów może jednak kolidować z zasadą tajności głosowania[9].

[8] M. Chrzanowski, *Podstawowe zasady prawa wyborczego...*, s. 54–58.

[9] M. Rulka, *E-Voting, a zasady prawa wyborczego. Analiza prawnopowównawcza*, „Przegląd Sejmowy" 2017, nr 3, s. 76–78.

## Zasada bezpośredniości

Do najważniejszej funkcji zasady bezpośredniości należy umożliwienie oddania głosu przez wyborcę osobiście w sposób bezpośredni, bez udziału osób trzecich. Zasadę tę można podzielić na trzy części. Jako pierwsze, zasada bezpośrednich wyborów zakłada wybory jednostopniowe, co oznacza wyłonienie zwycięzcy poprzez oparcie na głosach oddanych przez wyborców. Drugą częścią jest zagwarantowanie wyborcy możliwości oddania głosu na konkretnego kandydata, a nie na komitet wyborczy lub partię polityczną. Jako trzecią część uznaje się oddanie głosu w określonym lokalu wyborczym, osobiście, bez udziału pośrednika. Zasada bezpośredniości nie stanowi przeszkody dla wprowadzenia głosowania elektronicznego. Jednym z problemów, który wymaga rozwiązania, jest rozstrzygnięcie, czy głosowanie osobiste wymaga udania się do lokalu wyborczego, a także, czy głos oddany w sposób elektroniczny oddany jest samodzielnie, a nie przez kogoś innego, np. członka rodziny. Zasada bezpośrednich wyborów może budzić również wątpliwości związane z oddaniem głosu za pomocą określonej maszyny lub Internetu. Uznaje się, że zasada bezpośredniości dotyczy jedynie woli wyborcy a nie sposobu, w jaki oddaje się głos. Mając na uwadze powyższe, uznać można, że wprowadzenie głosowania elektronicznego jest zgodne z zasadą bezpośredniości[10].

## Zasada tajności głosowania

Zasada tajności umożliwia każdemu wyborcy oddanie głosu na dowolnego kandydata, bez obawy o jakiekolwiek konsekwencje z tym związane. Zasada ta uważana jest jako prawo wyborcy, a nie jego obowiązek. Władza ma za zadanie zapewnić wyborcy jedynie, aby oddany głos nie był znany dla innych osób. W tradycyjnym głosowaniu problem ten rozwiązany jest przez udostępnienie indywidualnego miejsca, umożliwiającego samodzielne oddanie głosu. Z punktu widzenia wyborcy zasada tajności uznawana jest jako przywilej; zostało to potwierdzone przez Trybunał Konstytucyjny: „W sytuacji, gdy wyborca decyduje się na głosowanie poza lokalem obwodowej komisji wyborczej, świadomie rezygnuje z tej gwarancji tajności głosowania stwarzanej przez państwo, przejmując jednocześnie obowiązek zorganizowania sobie we własnym zakresie odpowiednich warunków zapewniających tajność głosowania”[11]. Wypowiedź ta odnosi się bezpośrednio do głosowania korespondencyjnego, lecz może być również stosowana w przypadku i-votingu, ponieważ w obydwu przypadkach głosowanie odbywa nie poza lokalem wyborczym. Trudnym problemem jest rozwiązanie obowiązku tajności głosowania, jaki spoczywa na władzy publicznej. Jako rozwiązanie można

[10] M. Chrzanowski, *Podstawowe zasady prawa wyborczego...*, s. 167–179.
[11] Wyrok TK z 20 lipca 2011 r., sygn. akt K 9/11 ( Dz.U. z 2011 r., nr 149, poz. 889).

uznać częściową rezygnację przez wyborcę z zasady tajności głosowania. Polegałoby to na otrzymaniu potwierdzenia oddania głosu. I-voting, podobnie jak głosowanie korespondencyjne, nie łamie w rażący sposób zasady tajności, gdyż w obydwu przypadkach wyborca zgadza się częściowo ograniczyć swoją anonimowość. Zasada ta jest najtrudniejsza do zagwarantowania przy metodzie głosowania elektronicznego. Można jednak uznać tę metodę za zgodną z prawem w przypadku, gdy pozostają jeszcze inne sposoby na oddanie głosu, które są pełni tajne oraz do momentu, gdy nie zostanie wynaleziony sposób zapewnienia pełnej anonimowości[12].

## Zasada wolnych wyborów

Zasada wolnych wyborów zakłada, że każdy, kto posiada prawo wyborcze może w pełni z niego skorzystać, nie jest on w żaden sposób ograniczany ani zmuszany w sposób fizyczny lub psychiczny. Udział lub brak udziału w wyborach nie niesie za sobą również żadnych konsekwencji lub przywilejów. Aby wybory były w pełni uznane za wolne, muszą być spełnione cztery warunki. Jako pierwszy dopuszczeni do udziału, na równych prawach, powinni być wszyscy obywatele posiadający prawa wyborcze, bez względu na ich wyznanie, poglądy, kolor skóry oraz inne. Drugim warunkiem jest umożliwienie wyborcom dokonania realnego wyboru, a więc wybór spośród co najmniej dwóch kandydatów. Kolejnym warunkiem jest okresowość wyborów, co jest równoznaczne z ustaleniem kadencji i regularne powtarzanie wyborów. Jako ostatni warunek uznaje się ogłoszenie wyników wyborów oraz potwierdzenie ich ważności przez sąd. Zasada ta w żaden sposób nie koliduje z metodą głosowania elektronicznego. Jedynym warunkiem, jaki musi spełniać system informatyczny obsługujący i-voting, jest możliwość oddania głosu nieważnego, przez możliwość wybrania kilku kandydatów lub żadnego, tak jak jest to możliwe w głosowaniu tradycyjnym. Ważne jest więc, by system wyborczy umożliwiał zaznaczenie kilku opcji lub żadnej, a nie zmuszał wyborcy do wybrania konkretnie jednego kandydata. Uznaje się bowiem, że większość nieważnych głosów to nie błąd wyborcy przy wypełnianiu karty, lecz celowe oddanie nieważnego głosu[13].

## Podsumowanie

Głosowanie elektroniczne jest jedną z alternatywnych metod głosowania, występujących w kilku krajach na świecie, między innymi w Estonii czy Szwajcarii, a także w innych krajach na świecie w różnym wymiarze dostępności i poziomowi rozwoju, jednak w tych dwóch europejskich państwach działa sprawnie już od wielu lat. Głosowanie elektroniczne podzielić na dwa rodzaje: e-voting oraz

[12] M. Rulka, *E-Voting, a zasady prawa wyborczego...*, s. 79–80.
[13] M. Chrzanowski, *Podstawowe zasady prawa wyborczego...*, s. 234–235.

i-voting. Pierwszy z nich polega na oddaniu głosu w lokalu wyborczym lub innym wyznaczonym do tego miejscu, przy pomocy specjalnego urządzenia. Pozwala to natychmiastowe uzyskanie odpowiedzi, czy oddany głos został zarejestrowany przez system i czy jest oddany w sposób wiążący. Jednak metoda ta wymusza na wyborcy, jak w głosowaniu tradycyjnym udanie się do lokalu wyborczego. Znacznie wygodniejszą pod tym względem formą jest i-voting, który zakłada głosowanie z wykorzystaniem Internetu, bez konieczności udania się do lokalu wyborczego, z dowolnego miejsca w kraju lub z zagranicy. Konstytucja Rzeczypospolitej Polskiej nie reguluje w żaden sposób metody elektronicznego głosowania. Może się to wiązać z datą uchwalenia obecnie obowiązującej Konstytucji oraz bardzo mało rozpowszechnionym jak na tamten czas głosowaniu elektronicznym. Oznacza to, że polska ustawa zasadnicza nie reguluje zakazu wprowadzenia alternatywnych metod głosowania. Kodeks wyborczy poza tradycyjnym głosowaniem wyróżnia również możliwość głosowania przez pośrednika i głosowanie korespondencyjne. Wprowadzenie głosowania elektronicznego w Polsce jest możliwe po zmianie prawa wyborczego, wiążącego się z dodaniem kolejnej alternatywnej metody oddania głosu. Z punktu widzenia podstawowych zasad wyborczych nie ma większych przesłanek zakazujących lub niedopuszczających tej metody głosowania. Jedyną zasadą mogącą budzić wątpliwości jest zasada tajności wyborów, wiążąca się z koniecznością zapewnienia wyborcy możliwości oddania głosu w sposób anonimowy. Rozwiązaniem tego problemu jest stworzenie odpowiedniego, bezpiecznego systemu informatycznego, który pozwoli respektować wszystkie zasady prawa wyborczego. Wprowadzenie głosowania elektronicznego w Polsce może nieść za sobą wiele zalet, jak i również wad. Oczywistą zaletą może być upowszechnienie i zwiększenie dostępu do wyborów przez osoby najmłodsze oraz przebywające poza granicami kraju. Istotną zaletą tego systemu byłaby także jego powszechność i łatwość oddania głosu bez konieczności udania się do lokalu wyborczego. Głosowanie elektroniczne ma także wady oraz problemy, które należy rozwiązać w celu sprawnego funkcjonowania systemu. Największym wyzwaniem stojącym przed twórcami jest zapewnienie wysokiego poziomu bezpieczeństwa systemu komputerowego obsługującego głosowanie elektroniczne, co niewątpliwie wiązać się będzie z wysokimi kosztami, oraz bezwzględne zapewnienie poszanowania polskiego prawa, a w szczególności podstawowych zasad wyborczych.

## Bibliografia

Chrzanowski M., *Podstawowe zasady prawa wyborczego do organów stanowiących jednostek samorządu terytorialnego,* Białystok 2018.

Duda K., *E-voting jako forma demokracji bezpośredniej. Dotychczasowe doświadczenia i ich konsekwencje,* „Refleksje. Pismo Naukowe Studentów i Doktorantów WNPiD UAM" 2011, nr 4.

Musiał-Karg M., *Głosowanie elektroniczne jako alternatywna metoda uczestnictwa w wyborach – opinie Polaków*, „Political Preferences", Poznań 2015, nr 10.

Radajewski M., *Weryfikacja ważności wyników wyborów na przykładzie sprawy Bush v. Gore*, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2016.

Rulka M., *E-Voting, a zasady prawa wyborczego. Analiza prawnoporównawcza*, Przegląd Sejmowy, 2017, nr 3.

Zbieranek J., *Alternatywne procedury głosowania w Polsce na tle państw Unii Europejskiej*, Studia BAS, 2011, nr 3(27).

## Prawodawstwo

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483 ze zm.).

Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (tekst jedn. Dz.U. z 2020 r., poz. 1319).

## Orzecznictwo

Wyrok TK z 20 lipca 2011 r., sygn. akt K 9/11 (Dz.U. z 2011 r., nr 149, poz. 889).

# PRAWNE ASPEKTY TRANSHUMANIZMU

(*Anna Mroczkowska*)

## Wstęp

Termin „transhumanizm" w jego obecnym znaczeniu utworzył Max More. W eseju *Transhumanizm: Towards a Futurist Philosophy* zdefiniował on transhumanizm jako trend naukowy i filozoficzny, którego celem jest stworzenie człowieka pozbawionego ludzkich ograniczeń. Stworzenie super-człowieka, istoty będącej hybrydą wykorzystującą biotechnologie, nanotechnologie i neurotechnologie. Transhumanizm przejawia pewne cechy humanizmu, takich jak szacunek dla rozumu i nauki, nacisk na postęp i nastawienie na człowieczeństwo, a nie nadprzyrodzoną wiarę w przyszłe życie. Nie ogranicza się on zatem wyłącznie do badania technicznych zagadnień, lecz rozpatruje również dylematy natury filozoficznej i moralnej. Transhumanizm wykracza poza ramy humanizmu rozpoznając oraz przewidując radykalne zmiany w przyrodzie oraz życiu społecznym, wynikające z rozwoju nauki oraz technologii[1].

Na przestrzeni dziejów powstało sporo koncepcji, które dotyczyły rozwoju człowieka i gatunku ludzkiego. Jedną z bardziej znanych koncepcji była myśl Friedricha Nietschego, który wskazywał na powstanie nadczłowieka. Jednak, jak wskazuje Max More, Nietsche nie postulował wykorzystania techniki w przemianie człowieka, aczkolwiek jego metaforyczny język inspiruje część obecnych transhumanistów.

Czołowi reprezentanci transhumanizmu to: Max More, Natasha Vita-More, Anders Sandberg, jak również Nick Bostrom. Część z tych osób związana jest z Future od Humanity Institute (Uniwersytet Oxford) albo z organizacją Humanity+[2].

Wraz z rozwojem myśli, ale przede wszystkim praktyki biotechnologicznej powstaje wyzwanie dla prawa cywilnego, zarówno w aspekcie krajowym, jak również międzynarodowym i globalnym. Wyzwanie to jest dwukierunkowe, z jednej strony prawo musi sankcjonować nowe, pożyteczne rozwiązania w obszarze szeroko pojętej biomedycyny, ale także stawić czoła takim problemom jak choćby klonowanie ludzi, co obecnie przez prawo jest zabronione.

Ponieważ transhumanizm jest dopiero rozwijającym się nurtem, gdzie rozwiązania technologiczne stosowane obecnie nie nadążają za myślą czy ideą, dla-

---

[1] K. Szymański, *Transhumanizm*, „Kultura Wartości" 2015, nr 13, s. 134.

[2] Tamże, s. 134.

tego też rozwiązania prawne również w tym obszarze są fragmentaryczne i obecnie nie obejmują całości zagadnień, które będą poruszane w pracy.

## Transhumanizm w działaniu

Transhumanizm jest w swojej idei ukierunkowany na maksymalne wykorzystanie technologii w procesie kreowania ludzkiej ewolucji biotechnologicznej. Transhumaniści wskazują, iż człowiek powinien bezkrytycznie przyjmować wszelkie możliwe udoskonalenia oferowane przez inżynierów. Wszystkie powstające urządzenia służą polepszeniu życia i w związku z tym powinno się z nich korzystać. Dzięki temu technologia będzie w stanie zapewnić człowiekowi możliwość dłuższego oraz zdrowszego życia, polepszenia jego pamięci, jak i zdolności intelektualnych, udoskonalenia doznań zmysłowych, a także ogólnie uzyskania większej możliwości kontroli swojego życia[3].

Jak wskazują tranhumaniści, ostatecznym celem ewolucji transhumanistycznej, jest tzw. kondycja postczłowiecza. Według Nicka Bostroma, wielu transhumanistów chce podążać w życiu drogą, która doprowadzi ich do tego, iż staną się postludźmi, gdyż chcą uzyskać intelektualne szczyty, których nikt do tego czasu nie osiągnął. Ludzie ci chcą być odporni na choroby, wiecznie młodzi oraz pełni życia. Chcą mieć władzę nad własnymi pragnieniami, emocjami oraz stanami psychicznymi, nie czuć negatywnych myśli czy zmęczenia. Chcą mieć większą zdolność do przeżywania miłości, przyjemności czy wrażeń estetycznych. Choć z drugiej strony wskazują oni, iż postczłowiek nie będzie ostatecznym etapem tej ewolucji. Max More nie wskazuje również ostatecznego momentu udoskonalania człowieka.

Wiadomo, że już obecnie dzięki technice można stworzyć mechaniczne protezy, które są prawie tak sprawne jak biologiczne kończyny. Postulowana przez transhumanistów ewolucja ma zostać oparta na różnorodnej technologii. Jak wskazuje Nick Bostrom, jednym z jej kierunków ma być budowa tzw. awatarów, czyli sztucznych ciał, które w całości zbudowane są z mechanicznych elementów, w których istotną rolę odgrywał będzie ośrodek centralny. Centralnym ośrodkiem „naczynia" będzie ludzka osobowość, która zostanie wprowadzona do awatara. Naukowcy, którzy są skupieni w projekcie 2045 uważają, iż w stosunkowo bliskim czasie będą wstanie dokonać transferu ludzkiej świadomości na dysk twardy, który następnie zostanie umieszczony w naczyniu nazywanym awatarem. W efekcie tego ludzkie życie ulegnie istotnemu wydłużeniu[4].

Inną możliwością ścieżki ewolucji jest ewolucja na bazie biotechnologii. Przewiduje się, iż dzięki rozwojowi nauk medycznych będzie możliwa taka modyfikacja DNA, że ludzkie życie ulegnie istotnemu wydłużeniu, jak również uda się uwolnić ludzi od chorób, nowotworów i innych problemów zdrowotnych.

[3] Tamże, s. 134.
[4] Tamże, s. 134.

W związku z czym w aktualnych transhumanistycznych rozważaniach konkretna forma albo postać postczłowieka nadal pozostaje niedookreślona. Postczłowiek może być zarówno sztuczną inteligencją w komputerze, programem, sztucznym poruszającym się po świecie awatarem czy istotą biologiczną, tak jak obecny człowiek, tylko że z wieloma modyfikacjami biotechnologicznymi albo zmienionym DNA. Wszystko zależne jest od rozwoju nauk zapewniających narzędzia do dalszej ewolucji. Dla transhumnistów liczą się tylko skutki ewolucji biotechnologicznej oraz realizacja ich postulatów, ale sposób dojścia do celu nie ma znaczenia.

Nick Bostrom wskazuje, iż zdolności postczłowieka będą dalece wykraczały poza zdolności homo sapiens i transludzi, którzy są formą przejściową. Postczłowiek to istota, której ogląd wychodzi mocno poza poznawcze możliwości człowieka. Takie udoskonalenie jest możliwe dzięki ingerencji w biologiczny organizm człowieka[5].

Dla transhumanistów, przejściowym etapem między człowiekiem a postczłowiekiem jest transczłowiek. W tej sytuacji termin „transhuman" (transczłowiek) odnosi się do istoty miedzy człowiekiem a postczłowiekiem. Źródło słowa trashuman sięga do futurysty FM-2030, nazywanego także Ferejdun M. Esfandiar. Stworzył on ten skrót od „transitional human" (człowiek przejściowy). Nazywając transludźmi pierwsze przejawy istot, które powstaną z nowej ewolucji, FM zakłada, iż symbolem transludzi będą protezy, operacje plastyczne, intensywne wykorzystanie technologii komunikacyjnych, kosmopolityczność czy mobilny tryb życia, korzystanie z in vitro, ateizm a także odrzucenie tradycyjnych wartości. Choć część osób wskazuje, że to stanowisko jest nadinterpretacją, ponieważ nie istnieją przesłanki, z racji których można by było określać się mianem transludzi, gdy zostanie przeprowadzony zabieg chirurgiczny. Można także stać się transczłowiekiem i zachować tradycyjne wartości oraz zasady społeczne[6].

W związku z tym ścierają się dwie koncepcje, które pokazują, iż sami transhumaniści mają problem ze zdefiniowaniem kim naprawdę będzie ten transczłowiek.

Max More wskazuje na tzw. siedem poprawek do ludzkiego życia biologicznego i są nimi[7]:

- poprawka 1: nie będzie się dłużej tolerować starzenia oraz śmierci. Zmieniają geny, manipulując komórkami, używając syntetycznych organów oraz wszystkich koniecznych środków, człowiek obdarzy się większą żywotnością,
- poprawka 2: rozszerzy się zasięg ludzkich zmysłów przy użyciu biotechnologicznych oraz obliczeniowych środków. Przekroczy się zdolności percepcji wszelkich innych stworzeń, jak również rozwinie się nowe zmysły, żeby w jeszcze większym stopniu docenić oraz zrozumieć otaczający świat,

[5] Tamże, s. 138.
[6] Tamże, s. 138.
[7] Tamże, s. 141.

- poprawka 3: udoskonali się organizację oraz pojemność neuronową, rozbuduje się pamięć roboczą oraz polepszy inteligencję,
- poprawka 4: uzupełni się korę metamózgiem. Jest to rozproszona sieć czujników, przetworników informacji, jak również inteligencji, co zwiększy samoświadomość oraz pozwoli przestrajać emocje,
- poprawka 5: nie będzie się już niewolnikiem genów. Nastąpi samo programowanie genetyczne, dzięki czemu zostanie osiągnięte mistrzostwo w panowaniu nad biologicznymi oraz neurologicznymi procesami. Zostaną naprawione wszystkie indywidualne oraz gatunkowe wady,
- poprawka 6: przebuduje się wzorce motywacyjne, jak również emocjonalne reakcje w sposób, który zostanie uznany za zdrowy,
- poprawka 7: stale rozwijając biotechnologiczną doskonałość, jednocześnie będzie się dążyć do większej integracji naszej zaawansowanej technologii z nami samymi.

Według przeciwników tego nurtu taka wizja przyszłości jest niemożliwa do przewidzenia. Ponieważ nie można wykluczyć, iż to, co z założenia ma doprowadzić do wiecznego szczęścia, zdrowia, nieśmiertelności albo dobrobytu, w ostatecznej rzeczywistości będzie początkiem zagłady ludzkości, w szeroko rozumianym sensie. Samoreplikujące się, coraz mocniej świadome postępu technicznego jednostki ludzkie byłyby coraz mocniej przekonane o swojej własnej doskonałości oraz niezniszczalności. Najwięcej zastrzeżeń mają tutaj teologowie, którzy w przeciwieństwie do zwolenników tej ideologii uważają, iż nie da się takiej filozofii pogodzić z chrześcijaństwem, ponieważ to człowiek w niej staje się Bogiem. Dla chrześcijan wizja świata, w którym postęp technologiczny staje się Dobrą Nowiną, jest nie do zaakceptowania. Uwalnianiem człowieka od cierpienia oraz od śmierci zająć się miał Bóg, a nie człowiek. W takiej rzeczywistości praktycznie jakakolwiek religia wydaje się bezsensowna. Przeciwnicy tej drogi zwracają uwagę, na sytuację, w której władzę nad tą technologią przejęli by ludzie rządni władzy, w efekcie czego mogłoby to doprowadzić do tyrani[8].

Natomiast biokonserwatyści, do których zalicza się między innymi Leona Kassa, Jurgena Habermasa, C.S. Lewisa, Francisca Fukuyamę czy Michaela Sandela wskazują, iż idea ulepszenia gatunku ludzkiego, szczególnie przy pomocy ingerencji wywołującej zmiany genetyczne, za moralnie wątpliwą albo nawet niedopuszczalną. Jednakże nie kwestionują oni metod ulepszenia, w tym ryzyka związanego z nieznanymi konsekwencjami ich zastosowania. Odnoszą się sceptycznie do samej idei transhumanizmu, poprzez krytykę jej celów.

Chociaż przykładowo idea genetycznego projektowania potomstwa pozostaje w tej chwili w sferze science fiction, to prowadzona debata etyczna zwraca uwagę na bardzo wiele poważnych problemów związanych z kierunkiem oraz granicami stosowania osiągnięć postępu biotechnologicznego. Ingerencja genetyczna

[8] K. Całus, *Transhumanizm – wizja nowego człowieka*, Uniwersytet Humanistyczno-Przyrodniczy w Częstochowie, Częstochowa 2018, s. 240.

w ludzką prokreację może być przedmiotem wielu kontrowersji ze sporem o status moralny zarodka albo embrionu. Żeby uwypuklić problemy specyficzne dla samej idei ulepszania można przyjąć założenie, iż ulepszanie genetyczne mogłoby w przyszłości być realizowane za pomocą metod przed zapłodnieniem, czyli selekcji właściwych gamet albo modyfikacji genetycznych zarodka albo embrionu.

Istnieje wiele metod biomedycznego ulepszania kondycji psychicznej albo fizycznej człowieka po jego urodzeniu, do których zaliczyć należy stosowanie farmakoterapii (przykładowo beta-blokerów czy środków dopingujących), terapii genowej, a także operacji. W przypadku takiej formy ulepszania istnieje określona osoba, która korzysta dzięki interwencjom, które mają poprawić jej kondycję zdrowotną albo życiową. Z kolei ulepszanie przed urodzeniem nie zakłada istnienia określonej osoby, która sama ma coś zyskać na poszczególnej ingerencji, ale oparta jest na założeniu, iż pojawienie się albo niepojawienie się na świecie osobników, o określonych predyspozycjach będzie dla rodziców albo populacji lepsze.

Należy także podkreślić, iż postęp techniczny i technologiczny dają coraz to nowsze możliwości wykorzystania sztucznej inteligencji. Dobrym przykładem jest tutaj dr Scott-Morgan, który zachorował na stwardnienie zanikowe boczne. Chory w tej przypadłości zachowuje w pełni władzę umysłową, ale stopniowo traci kontrolę nad swym ciałem. Jednakże osoba ta nie poddała się i dokonała przy współpracy wielu naukowców wielu zmian w swoim ciele.

Liczba modyfikacji, którym poddał swe ciało dr Scott-Morgan jest ogromna, Specjalny egzoszkielet obudowujące jego ciało daje możliwość stanięcia znowu na nogi. Jego mózg zostanie podłączony bezpośrednio do komputera, a twarz, która jest sparaliżowana zastąpi hiperrealistyczny awatar, który ma nie tylko mówić, ale również poprzez ruchy awatara naukowiec będzie mógł wyrażać emocje w czasie prowadzenia rozmowy[9].

W roku 2018 dr Scott-Morgan został poddany wielu operacjom, które zmodyfikowały jego układ pokarmowy, w takim sposób, żeby nie musiał polegać na opiekunach w czasie jedzenia albo korzystania z toalety. Operacje te były wysokiego ryzyka, przede wszystkim dla osoby w jego stanie.

Następnie Scott-Morgan zdecydował się na laryngoterapię, czyli zabieg polegający na oddzieleniu przełyku od tchawicy. Było to konieczne, ze względu na paraliż górnej części ciała, co wpływało na funkcjonowanie przełyku. Ważne było, aby ślina chorego nie przedostawała się do jego płuc, jednak efektem ubocznym takiego zabiegu była utrata możliwości mówienia. Jednakże i z tym problemem postarano się uporać. Zwrócono się do Lamy Nachman, dyrektor działu Anticipatory Computing w Intel Labs, osoby, która opracowała także zaawansowany system mowy dla profesora Stephena Hawkinga. W efekcie opracowano moduł prywatnej sztucznej inteligencji, która w pewnym sensie uczy się sposobu wyrażania myśli oraz formułowania zdań przez chorego. Sztuczna inteligencja ma przemawiać za dr. Scotta-Morgana. Jednak z drugiej strony chory będzie wybierał słowa

[9] https://www.komputerswiat.pl/artykuly/redakcyjne/czlowiek-cyborg-to-nie-science-fiction-to-rzeczywistosc/9s9jd2v

zaproponowane przez sztuczną inteligencję, ponieważ to system będzie musiał się w pewnym stopniu domyślać się,o co chodzi choremu.

Warto także wskazać, iż egzoszkielet Scotta-Morgana jest nieustannie rozbudowywane i ma w przyszłości praktycznie całkowicie przywrócić choremu zdolność poruszania się. W dalszych planach jest połączenie systemu ACAT z systemami BCI, czyli interfejsami mózg – komputer, w efekcie czego możliwe będzie sterownie maszyną dosłownie przy pomocy myśli. Fale mózgowe człowieka przetłumaczone zostaną na właściwe instrukcje, a maszyna wykona pokreślone działanie. Dr. Scott – Morgan ma szansę zostać pierwszym człowiekiem cyborgiem. Podobne pomysły ma firma Neuralink należąca do Elona Muska. Chce ona połączyć mózg z komputerem za pomocą chipu. Na razie wszczepiono taki chip świni. W przyszłości taki układ ma pomagać osobom sparaliżowanym[10].

Z pewnością postęp technologiczny w tym obszarze będzie stanowił poważne wyzwanie dla prawa cywilnego. Może pojawić się pytanie prawne, czy słowa i czynności podejmowane przez sztuczną inteligencję są na pewno odzwierciedleniem dosłownych myśli ludzkiego mózgu czy tylko interpretacją sztucznej inteligencji.

## Transhumanizm, a aspekt prawny

Idea transhumanizmu budzi nie tylko wiele obaw etycznych, ale także wiele problemów natury prawnej. W chwili obecnej system prawny nie musi się jeszcze mierzyć ze wszystkimi wyzwaniami. Wydaje się obecnie, iż powstanie jak to transhumaniści określają, postczłowieka, jest obecnie nie możliwe. Droga do tej idei widzie przez wiele rozwiązań technologicznych, które już obecnie są stosowane. W związku z czym prawo musi odpowiadać na dynamiczny rozwój biotechnologii.

Pojawia się również dużo zagadnień, które są związane przykładowo z wyrażeniem zgody na modyfikacje genowe. Trzeba pamiętać, iż materiał genetyczny jest szczególnym nośnikiem informacji, który dotyczy zarówno właściciela, członków jego rodzina, zstępnych, wstępnych, ale także całej ludzkości.

Od strony prawnej istotne są następujące obszary związane z materiałem genetycznym[11]:

- opis tego nowego oraz wyjątkowego przedmiotu ochrony prawnej, jakim jest materiał genetyczny człowieka. W ramach rozważań, czym jest prawo do materiału genetycznego człowieka analizuje się nie tylko wpływ odkrycia genomu ludzkiego na życie człowieka, na postępowanie sądowe, ale także wskazuje się najistotniejsze zagrożenia związane z wykorzystaniem materiału genetycznego człowieka do różnorodnych celów

[10] https://tvn24.pl/biznes/tech/elon-musk-chce-laczyc-mozg-z-komputerem-poki-co-chip-wszczepiono-swini-4677821

[11] D. Krekora-Zając, *Prawo do materiału genetycznego człowieka*, LexisNexis, Warszawa 2014 (lex.pl).

- trzeba także poddać analizie charakter prawny materiału genetycznego człowieka. Trzeba znaleźć odpowiedź na pytanie, czy istnieje prawo do materiału genetycznego, a jeżeli tak, to jaki ono ma charakter, ponieważ zagadnienie związane z materiałem genetycznym jest istotne dla praktycznych problemów związanych z rozwojem genetyki oraz konieczności ingerencji w nią prawa.
- powinno wskazać się metody regulacji prawnej prawa do materiału genetycznego człowieka i co jest z tym związane, ocena przydatności klasycznych instytucji prawa cywilnego w odniesieniu do prawnej regulacji materiału genetycznego człowieka. Trudność w regulacji prawnej takiego zagadnienia polega z jednej strony na tym, że niełatwe jest regulowanie materii, która tak szybko ulega istotnym zmianom, a z drugiej strony istnieje nieustannie szereg kontrowersji etycznych, które są związane z biomedycyną. Bardzo dobrze ukazuje to problematyka badań embrionalnych komórkami macierzystymi, która nadal budzi wiele kontrowersji. Wielu znanych przedstawicieli doktryny prawa prowadziło oraz nadal prowadzi spór nad kształtem regulacji, które dotyczą tychże badań

Genetyk W. Szybalski, pytany o możliwość regulacji prawnej zagadnień biomedycznych wskazał, że „Kontrolować to trzeba, ale najlepiej gdyby wam się udało stworzyć prawo z terminem, to znaczy, że w ciągu najbliższego roku nie będzie można zamrażać zarodków, po roku nauka pójdzie do przodu i za rok nowa regulacja". Jednakże taki pogląd wydaje się być ciężki do zaakceptowania z wielu powodów. Głównie prawo, a w szczególności prawo cywilne, reguluje określone zagadnienia dopiero po obserwacji wieloletniej praktyki. Dlatego prawo cywilne miało i musi mieć charakter, co do zasady, wtórny do praktyki, sankcjonując określone działania. Trzeba wskazać, iż ważną cechą prawa jest pewność oraz stałość. Cechy te zapewniają obywatelom bezpieczeństwo, czyli są fundamentalne dla całego systemu prawnego. Pewność prawa nie może być pogodzona z jego zmiennością[12].

Istotnym obszarem w rozwoju eksperymentalnej biotechnologii są kwestie związane z klonowaniem ludzi.

Pierwsze próby uporządkowania tematyki klonowania człowieka na poziomie globalnym zostały podjęte przez ONZ. W literaturze przedmiotu wskazuje się, iż ONZ poniosła w tym obszarze porażkę, gdyż akty, które w następstwie jej działalności wydano, nie zostały ratyfikowane przez wszystkie kraje członkowskie. Mowa tutaj o trzech deklaracjach bioetycznych, które zostały przygotowane przez ONZ dla Wychowania, Nauki i Kultury (UNESCO): Powszechnej Deklaracji w sprawie genomu ludzkiego i prawach człowieka z dnia 11 listopada 1997 roku, Międzynarodowej Deklaracji o danych genetycznych z 16 października 2003 roku jak również Powszechnej Deklaracji w sprawie bioetyki i praw człowieka z 19 października 2005 roku, choć tylko pierwszy z nich wprost mówi o klonowaniu.

[12] Tamże.

W art. 11 Powszechnej Deklaracji w sprawie genomu ludzkiego i prawach człowieka znajduje się zakaz reprodukcyjnego klonowania istot ludzkich. Jednakże przepis ten milczy w sprawie klonowania terapeutycznego, co może wskazywać, iż istnieje powszechny sprzeciw tylko co do pierwszego ze sposobów klonowania[13].

Jednocześnie z UNESCO kwestią klonowania zajmowała się Światowa Organizacja Zdrowia (WHO). Dokonała ona analizy posiedzeń Zgromadzenia Ogólnego Narodów Zjednoczonych w obszarze klonowania przedstawiając swoje obserwacje w postaci Raportu z dnia 16 grudnia 2014 roku. Wskazano, iż trzeba utworzyć definicję pojęcia klonowanie. Poza tym wskazano, iż w zależności od przynależności kulturowej, tematyka klonowania człowieka jest postrzegana różnorodnie. Przykładowo państwa Ameryki Północnej opowiadają się za słusznością klonowania, z kolei większość krajów europejskich chciałaby wprowadzenia zakazu tej procedury[14].

W Polsce, gdzie dorobek jak również skala badań genetycznych są znaczne, istniało słabe zainteresowanie społeczne problemami związanymi z klonowaniem. Literatura z tego obszaru to przede wszystkim doniesienia o wydarzeniach, które miały miejsce w innych państwach. Jednakże nie można wziąć pod uwagę tego, iż system prawa krajowego w istotnej mirze zależy również od prawa międzynarodowego. W związku z tym trzeba wskazać, iż Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, która jest najistotniejszym aktem systemu prawa krajowego, spina jednocześnie działania innych systemów normatywnych, jak przykładowo prawo międzynarodowe. Przejmując oraz akceptując ich sprawdzone zasady staje się miedzy innymi źródłem prawnie obowiązującego systemu wartości. Niezależnie od postanowień wstępu, przykładowo o zachowaniu przyrodzonej godności człowieka albo chrześcijańskiej genezie polskiej kultury , Konstytucja zawiera wiele przepisów bezpośrednio traktujących o istocie życia ludzkiego. W art. 38 wskazuje na podstawową zasadę prawnej ochronny życia. Według art. 39 nikt nie może być poddany eksperymentom naukowym, w tym także medycznym, bez dobrowolnie wyrażonej zgody, jak również przewiduje się, iż nikt nie może być poddany nieludzkiemu albo poniżającemu traktowaniu. Jednakże czy przykładowo słowo nikt rozciąga się także na zarodek albo też sztucznie stworzone życie?[15]

Należy także podkreślić, iż elementem rozwoju transhumanizmu jest rozwój sztucznej inteligencji i robotyzacja. Proces ten wiąże się także ze zmianami prawnymi, które próbuje się w ostatnim czasie powoli wprowadzać, zarówno w obszarze sztucznej inteligencji, jak również praw robotów.

Kwestia praw robotów, na wzór praw człowiek, obecnie pozostaje w sferze fantastyki, jednakże zaczyna już się toczyć debata na ten temat. Zwolennicy jak

---

[13] A. Bałaban, E. Michałkiewicz-Kądziela, *Prawne aspekty klonowania człowieka*, Uniwersytet Szczeciński, Szczecin 2019, s. 17.

[14] Tamże, s. 17.

[15] Tamże, s. 22–23.

również przeciwnicy takiego podejścia wskazują, że sztuczna inteligencja nie może równać się człowiekowi, oraz że obecnie sztuczna inteligencja nie jest w stanie odwzorować działania ludzkiego mózgu. Jednakże niektóre państwa postanowiły nadać sztucznej inteligencji pewną namiastkę ludzkich praw. Można tutaj wymienić kilka takich przypadków. Japonia przyznała prawo stałego pobytu w Tokio sztucznej inteligencji, której nadano imię Mirai. Ta sztuczna inteligencja jest botem, który został stworzony na podobieństwo siedmioletniego chłopca, ale nie ma sztucznego ciała. Inaczej jest w przypadku Sophi, która została stworzona przez Hanson Robotics. Sophia jest najbardziej znanym robotem na świecie, otrzymała ona obywatelstwo Arabii Saudyjskiej. Natomiast wiosną 2017 roku w Belgii, wydano akt urodzenia robotowi pod imieniem i nazwiskiem Fran Pepper[16].

Nadanie aktu urodzenia robotowi czy przyznawanie mu obywatelstwa nie oznacza obecnie nabycia przez maszynę takich praw, jakie mają ludzie. W związku z tym na razie roboty nie mają zdolności do czynności prawnych, nie mogą kupować w sklepach, wynajmować mieszkań i nie płaci im się za to co robią (przykładowo Fran Pepper pracuje w recepcji uniwersytetu PXL). Także z jednej strony roboty i sztuczna inteligencja nie posiadają realnych praw, to z drugiej strony może się to z czasem zmienić. Komisja Europejska w sprawozdaniu, które zostało opublikowane w 2017 roku nie wykluczyła tego, iż wyjątkowo zaawansowane maszyny mogą się w przyszłości stać osobami elektronicznymi. Sama nazwa wskazuje, że zbliża się roboty do ludzi. Indyjski dokument Report of Task Force on Artificial Intelligence wskazuje, iż przepisy dotyczące osób używających systemów, które są oparte na sztucznej inteligencji powinny być stosowane do maszyn autonomicznych, a twórcy oraz projektanci sztucznej inteligencji powinni dbać o przestrzeganie przepisów prawa. Sygnalizuje się, iż w przyszłości trzeba będzie się zmierzyć z pytaniem o prawa oraz obowiązki bytów autonomicznych. Polska również włącza się w ten trend. 13 czerwca 2018 roku Sophia była w Krakowie i otrzymała indeks krakowskiej AGH. Prorektor tej uczelni, prof. J. Lis wskazał, że ten gest miał być symbolem, ale również sygnałem, iż AGH jest gotowe na wyzwania, które niesie ze sobą sztuczna inteligencja.

Prawo karne jest polem, przez które na sztuczną inteligencję można patrzeć dwojako. Pojawia się pytanie, kto będzie odpowiedzialny za szkody, które zostały wyrządzone przez AI albo roboty. Już obecnie samochody autonomiczne powodują pierwsze wypadki, co jest wyzwaniem dla obecnego prawa, również karnego. Obecnie sztuczna inteligencja nie ma odpowiedzialności karnej. Jednakże wraz z jej rozwojem ludzkość będzie się mierzyła z tym zagadnieniem. Z drugiej strony sztuczna inteligencja może zostać wykorzystana jako narzędzie egzekwowania prawa. Sztuczna inteligencja jest w stanie analizować wzory zachowań jednostek

[16] https://lexrobotica.pl/2018/10/22/aspekty-prawne-zwiazane-z-rozwojem-sztucznej-inteligencji/#more-257

albo nawet całych grup ludzi oraz wykrywać anomalie mogące świadczyć o prawdopodobieństwie wystąpienia naruszenia prawa[17].

## Podsumowanie

Podsumowując należy wskazać, iż istotą transhumanizmu jest jego mocna wiara w człowieka oraz postęp nauki. Transhumaniści są przekonani, iż człowiek nie musi zgadzać się na rolę, która została przewidziana dla niego na tym świecie przez naturę. Może on rzucić jej wyzwanie i stać się kimkolwiek zechce. Nie musi cierpieć, umierać czy być jakimkolwiek więźniem różnych relacji społecznych. Transhumanizm wyrasta z humanizmu, czyli filozofii skupiającej się na człowieku, która jest nastawiona na jego potrzeby oraz aspiracje. Jednakże dopiero transhumanizm postawił sobie za cel nie tylko zrozumienie człowieka, ale również jego przemianę, dosłowną, jak również zmianę natury świata w celu dostosowania natury do potrzeb człowieka[18].

Natomiast w aspekcie prawnym, największym wyzwaniem tej idei jest to, że rozwiązania technologiczne, które mogą być potencjalnie stosowane wyprzedzają myśl prawną w tym obszarze. Dobrym tego przykładem jest problem związany z klonowaniem ludzi. Obecnie jest to zabronione, jednakże wydaje się, iż myśl technologiczna jest o krok od możliwości dokonania tej czynności. W efekcie czego pomimo formalnego prawnego zakazu, dojdzie do sklonowania człowieka. Jak wówczas będzie można pogodzić zakaz klonowania z prawem człowieka do urodzenia, do istnienia? Te i wiele innych aspektów, które nie zostały tutaj poruszone, będą z pewnością obiektem wielu debat prawnych i poszukiwania rozwiązań, które będą musiały sprostać rozwojowi biotechnologii, co w długiej perspektywie może doprowadzić, jak to transhumaniści ujęli, do powstania transczłowieka.

## Bibliografia

Bałaban A., Michałkiewicz-Kądziela E., *Prawne aspekty klonowania człowieka*, Uniwersytet Szczeciński, Szczecin 2019.

Całus K., *Transhumanizm – wizja nowego człowieka*, Uniwersytet Humanistyczno-Przyrodniczy w Częstochowie, Częstochowa 2018.

Krekora-Zając D., *Prawo do materiału genetycznego człowieka*, LexisNexis, Warszawa 2014.

Szymański K., *Transhumanizm*, „Kultura Wartości" 2015, nr 13.

[17] https://lexrobotica.pl/2018/10/22/aspekty-prawne-zwiazane-z-rozwojem-sztucznej-inteligencji/#more-257

[18] K. Całus, *Transhumanizm – wizja nowego człowieka.…*, s. 252.

# Netografia

https://lexrobotica.pl/2018/10/22/aspekty-prawne-zwiazane-z-rozwojem-sztucznej-inteligencji/#more-257

https://www.komputerswiat.pl/artykuly/redakcyjne/czlowiek-cyborg-to-nie-science-fiction-to-rzeczywistosc/9s9jd2v

https://tvn24.pl/biznes/tech/elon-musk-chce-laczyc-mozg-z-komputerem-poki-co-chip-wszczepiono-swini-4677821

# NOWE TECHNOLOGIE I STARA TEORIA – KILKA UWAG O WPŁYWIE NOWYCH TECHNOLOGII NA KONCEPCJĘ PRAW CZŁOWIEKA

(*Marcin Merkwa*)

## Wprowadzenie

Koncepcja praw człowieka należy do tych idei, które w stopniu niemożliwym do przecenienia wpłynęły na współczesne systemy prawne. Właściwie każdy porządek prawny współczesnych państw demokratycznych odzwierciedla założenia leżące u podstaw idei niezbywalnych praw jednostki. W szczególności normy konstytucyjne ufundowane są bardzo często na uznaniu przyrodzonej godności jednostki, która jest źródłem przysługujących jej praw. Praw człowieka mają przy tym wiele wymiarów. Choć sama idea wyrażona została w pełnej postaci w oświeceniu, to kluczową role w systemach prawnych poszczególnych państw, ale i w prawie międzynarodowym, odgrywa właściwie dopiero od zakończenia II wojny światowej. Przy czym w okresie tych 70 lat prawa człowieka przestały być jedynie filozoficzną koncepcją, zakorzenioną w liberalizmie, doświadczeniach wojny czy też chrześcijaństwie i wyrażoną w Powszechnej Deklaracji Praw Człowieka, a stały się, jak już wspomniano, podstawą porządków prawnych państw istniejących, podstawą, która obejmuje już nie tylko najbardziej rudymentarne prawa takie jak praw do życia, ale i np. prawa socjalne. Rozwinęło się przy tym międzynarodowe prawo humanitarne, a prawa człowieka stały się znaczącym elementem współczesnej kultury. Z tego względu, ale również dlatego, że prawa jednostki to najczęściej najbardziej podstawowe uprawnienia, w mniej lub bardziej świadomy sposób realizowane w życiu codziennym, można dostrzec związek pomiędzy ideą praw człowieka i jej jurydyzacją a technologią. Rozwój technologii przekształca bowiem świat na skale dotąd niespotykaną. Nowe rozwiązania, takie jak chociażby Internet, nie tylko wpływają na kulturę czy ekonomię, ale również na prawa człowieka: dostarczają narzędzia pozwalające np. na lepsze wykrywanie i przeciwdziałanie naruszeniom praw człowieka[1], ale i tworzą wyzwania tak dla badaczy, jak i dla legislatorów czy organów stosujących prawo.

[1] Ciekawy przykład wykorzystania to zautomatyzowane wyszukiwanie naruszeń praw człowieka poprzez analizę zdjęć zamieszonych w Internecie. Szerzej: G. Kalliatakis, S. Ehsan, K.D. McDo-

W dalszej części pracy ukazane zostaną przykłady dwóch obszarów, w których mamy do czynienia z intensywnym rozwojem technologii, który to rozwój może wpłynąć (choć w różnym stopniu) na prawa człowieka, tak na ich rozumienie, jak i stosowanie. Oczywiście wskazane zagadnienia nie wyczerpują analizowanej problematyki; ze względu na ograniczenia rozdziału nie podejmuję się na przykład analizy problemów z obszaru biotechnologii, jednakże wydaje się, że nawet krótkie uproszczone przedstawienie dwóch interesujących obszarów pozwoli wykazać tezę, zgodnie z którą rozwój technologii postrzegany być powinien nie tylko jako szansa na lepszą ochronę praw człowieka i/lub zagrożenie dla tych fundamentalnych praw, ale również jako czynnik, który może doprowadzić do istotnych zmian sposobu pojmowania niezbywalnych praw jednostki.

## Nowe technologie i stara teoria

Jednym z częściej dyskutowanych ostatnimi laty zagadnień jest problem pojazdów autonomicznych. I choć dyskusje te dotyczą w przeważającej mierze ewentualnej odpowiedzialności karnej i/lub cywilnej w przypadku wypadków, w których uczestniczyć mogą takie pojazdy, to cały czas pojawiają się nowe zagadnienia, z których niektóre mogą mieć związek z prawami człowieka. Wynika to przede wszystkim z tego, iż właściwie bez przerwy pojawiają się nowe możliwości ich zastosowania: od całkowicie autonomicznych środków transportu osób (np. w komunikacji miejskiej), po drony, które wykorzystywane być mogą zarówno do celów rekreacyjnych, jak i do transportu osób czy mienia, a w końcu do celów militarnych (w kontekście dronów warto również wskazać, iż urządzenia te mogą przyjąć bardzo różny stopień zaawansowania, mamy bowiem bojowe bezzałogowe pojazdy, jak i dziecięce zabawki, jednakże nawet w tym ostatnim przypadku mogą być one wyposażone w funkcje takie jak automatyczny powrót do miejsca startu, które choć nie świadczą o autonomii tych urządzeń, to jednak dają możliwość odbywania części lotu bez nadzoru ludzkiego operatora).

Analizując problem autonomicznych pojazdów D. Iwan wskazuje na trzy zagadnienia, które stanowią wyzwanie, jakie rozwój omawianej technologii może postawić przed prawodawcami. Jest to problem bezpieczeństwa, cyberbezpieczeństwa i prywatności[2]. Z perspektywy praw człowieka kluczowe wydaje się rozważenie problemu prawa do prywatności. Nie wdając się w szczegółowe analizy warto przypomnieć, że kluczowym dokumentem powszechnego systemu praw człowieka jest Międzynarodowy Pakt Praw Obywatelskich i Politycznych[3]. W art.

---

nald-Maier, *A Paradigm Shift: Detecting Human Rights Violations Through Web Images*, https://arxiv.org/abs/1703.10501 (dostęp: 31.08.2020 r.).

[2] D. Iwan, *Autonomous Vehicles – a New Challenge to Human Rights?*, „Adam Mickiewicz University Law Review" 2019, 9.

[3] Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 19 grudnia 1966 r. (Dz.U. z 1977 r., nr 38, poz. 167).

17 dokumenty czytamy, że „Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję, ani też na bezprawne zamachy na jego cześć i dobre imię", ponadto, zgodnie z ust. 2 „Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami". Warto podkreślić, że autorzy Paktu nie zdefiniowali pojęcia prywatności, wymienili jedynie dobra, które są chronione[4]. Z perspektywy omawianego zagadnienia najistotniejsze wydaje się „życie prywatne". Termin ten jest pojęciem bardzo szerokim i definiowany jest z reguły poprzez otwarte wyliczenie tych sytuacji, które mogą być uznane za należące do „życia prywatnego". Do tej kategorii należą m.in. kwestie dotyczące zabiegów medycznych czy tożsamości jednostki, jednakże dla omawianego zagadnienia kluczowe wydaje się zaliczenie do tej grupy prawa jednostki do ochrony tych informacji, które odnoszą się do jej osoby[5]. Nie ma bowiem wątpliwości, iż autonomiczne pojazdy będą gromadzić znaczną ilość informacji nt. ich użytkowników.

W literaturze przedmiotu zwraca się uwagę, że wprowadzenie pojazdów autonomicznych jako powszechnego środka transportu skutkować musi koniecznością rozważenia trzech obszarów związanych z prywatnością: autonomii jednostki, danych osobowych i nadzoru[6]. Opisując problem autonomii jednostki D.J. Glancy zwraca uwagę na wiele aspektów tego zagadnienia; od problemów psychologicznych po marketingowe. Przy czym istotne wydaje się uznanie, że kluczowe dla zapewnienia autonomii jednostki jest wprowadzenie systemów, które pozwolą osobom korzystającym z tego typu pojazdów zapoznać się z warunkami ich użytkowania i wyrazić świadomą zgodę na nie. Autorka zwraca uwagę, że posiadanie danych o jednostce, która w pojeździe się znajduje, o położeniu pojazdu w przestrzeni, ale i o celu podróży, może prowadzić np. do tworzenia nowych form spersonalizowanej reklamy, a także grozi ryzykiem podejmowania przez władze prób monitorowania zachowania tak poszczególnych osób, jak i grup społecznych. Kluczowe wydaje się więc zapewnienie możliwości podejmowania świadomych decyzji dotyczących korzystania z autonomicznych pojazdów. Wskazane wyżej kwestie dotyczące m.in. marketingu związane są ściśle z drugim obszarem definiowanym przez Glancy, a mianowicie z ochroną danych osobowych. Nie ma wątpliwości, że korzystanie z autonomicznych pojazdów będzie prowadzić do generowania znacznych ilości danych, które mogą być wykorzystywane nie tylko w reklamie, ale i użyte np. przez władzę zarówno do poszukiwania sprawców przestępstw, jak i w ramach działań prewencyjnych. Ze względu na specyfikę rzeczy

[4] Szerzej: J. Uliasz, *Konstytucyjna ochrona prywatności w świetle standardów* międzynarodowych, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2018, s. 47.

[5] Zob. A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, *Komentarz do art. 17 MPPOiP* [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, red. R. Wieruszewski, Lex 2012.

[6] D.J. Glancy, P*rivacy in Autonomous Vehicles,* 52 „Santa Clara L. Rev." 1171, 2012, s. 1187 i n., https://digitalcommons.law.scu.edu/lawreview/vol52/iss4/3 (dostęp: 07.09.2020 r.).

jaką jest samochód, nie można pominąć tego, iż informacja np. o miejscu zaparkowania pojazdu może dostarczyć również danych np. o przyszłych zachowaniach jednostki (np. o sklepie, do którego się udaje) czy zamożności[7].

Czy zbieranie tak znacznej ilości danych może dać możliwość prowadzenia nadzoru nad pojedynczymi osobami, a także nad społeczeństwem, na skalę dotąd niespotykaną? Wbrew pozorom wydaje się, że nie. Sądzę, że z analogiczną sytuacją mieliśmy i wciąż mamy do czynienia w przypadku telefonów komórkowych. Można nawet uznać, że pozwalają one na zebranie znacznie większej ilości danych niż autonomiczny samochód. Wydaje się więc, że zasadne są argumenty, iż potencjalne korzyści związane z bezpieczeństwem[8], a wynikające z wprowadzenia autonomicznych pojazdów, nie znajdą przeciwwagi w postaci niedającego się uniknąć naruszenia prywatności użytkowników. Jednakże stwierdzenie takie może być zasadne tylko przy założeniu wdrożenia odpowiednich regulacji, do czego w znaczącym stopniu przyczynić się może np. aktywność UE. Autonomiczne pojazdy są dobrym przykładem technologii, której rozwój wymusi szereg zmian legislacyjnych, w tym przepisów z obszaru praw człowieka, jednakże raczej nie zredefiniuje to sposobu rozumienia praw człowieka. Z drugiej strony ukazać można problem uznania dostępu do Internetu za podstawowe prawo człowieka – kwestia ta może bowiem doprowadzić do rozszerzenia katalogu podstawowych praw i wolności. Związane jest to na naturą problemu, który będzie dyskutowany w dalszej kolejności; nie chodzi bowiem o objęcie nowych zjawisk (autonomicznych pojazdów) obowiązującymi już normami (oczywiście przy odpowiedniej ich modyfikacji) lub ewentualnie utworzenie nowych norm będących rozwinięciem już obowiązujących, lecz o sytuacje, w której stosunkowo nowo powstała technologia prowadzi do skodyfikowania nowych uprawnień.

Już w 2016 roku ONZ uznała w rezolucji, iż państwa zakłócające dostęp do Internetu dopuszczają się naruszenia międzynarodowego prawa praw człowieka[9]. Warto wyraźnie zaznaczyć, że wspomniana rezolucja nie określa dostępu do Internetu jako podstawowego prawa człowieka, stwierdza jedynie o braku legalności działania podejmowanego przez państwo, które za cel ma ograniczenie dostępu do niego. W związku z tym pojawia się pytanie, czy dostęp do Internetu może być uznany za prawo przynależne każdemu człowiekowi?

Zacznijmy od uwagi, że w literaturze przedmiotu pojawia się często teza, iż dotychczasowe regulacje zapewniają ramy, w których można umieścić nowe technologie. W kontekście dyskusji dotyczącej dostępu do Internetu wskazuje się przede wszystkim na art. 19 Powszechnej Deklaracji Praw Człowieka, zgodnie z którym „Każda jednostka ma prawo do wolności poglądów i wypowiedzi; prawo

---

[7] Tamże, s. 1196.

[8] T.B. Lee, *Self-driving cars are a privacy nightmare. And it's totally worth it*, 21.05.2013, https://www.washingtonpost.com/news/wonk/wp/2013/05/21/self-driving-cars-are-a-privacy-nightmare-and-its-totally-worth-it/?arc404=true (dostęp: 07.09.2020 r.).

[9] Zgromadzenie Ogólne ONZ, *The promotion, protection and enjoyment of human rights on the Internet*, 27 Czerwca 2016, A/HRC/32/L.20.A/HRC/32/L.20.

to obejmuje nieskrępowaną wolność posiadania poglądów oraz poszukiwania, otrzymywania i przekazywania informacji oraz idei, wszelkimi środkami i bez względu na granice". Krytycy uznania dostępu do Internetu za podstawowe prawo człowieka zwracają m.in. uwagę, że Internet jest jedynie narzędziem, które pozwala ludziom korzystać z uregulowanych praw i wolności, np. z swobody wypowiedzi[10]. Zwolennicy argumentują, że powszechny niemonitorowany i niecenzurowany, ale także darmowy dla osób ubogich dostęp do sieci uzasadnić można poprzez odwołanie do natury Internetu. Nie jest on bowiem li tylko narzędziem pozwalającym realizować prawa człowieka, jest medium, które wpływa na rzeczywistość w sposób niemający precedensu w dotychczasowej historii. Zwraca na to uwagę m.in. M. Reglitz pisząc, iż uznanie, że Internet pozwala jedynie na realizację praw jest niedocenieniem tego, w jaki sposób to medium wpłynęło na sposób komunikacji czy gromadzenia danych. Internet, a właściwie wolny do niego dostęp, jest bardzo często warunkiem *sine qua non* korzystania z podstawowych praw. Reglitz pisze: „(…) Internet jest zarówno konieczny do realizacji kluczowych praw człowieka, jak i stanowi narzędzie wzmacniające demokrację. Tak pojmowany dostęp do Internetu uzasadnia postrzeganie go jako odrębnego prawa, które nie może być zredukowane do innych praw (np. swobody wypowiedzi)"[11].

Uznanie dostępu do Internetu jako praw człowieka można uzasadnić na kilka sposobów. Można to uczynić np. poprzez przytoczone już odwołanie do natury Internetu, który jest znacznie bardziej demokratyczny niż inne media. W ostatnich latach wiele było przypadków, w których masowe ruchy społeczne wpływały na politykę poszczególnych państw unaoczniając siłę społeczeństwa obywatelskiego. Przyjmując, że takie działania były możliwe przede wszystkim dzięki Internetowi, i pamiętając, że Powszechna Deklaracja Praw Człowieka daje, w art. 21, prawo każdemu człowiekowi do „uczestniczenia w rządzeniu swym krajem bezpośrednio lub poprzez swobodnie wybranych przedstawicieli", trudno wyobrazić sobie w dzisiejszym świecie równie skuteczny sposób wpływania na decyzje demokratycznych państw, na organizację jednostek czy wyrażanie opinii w sposób, który może rzeczywiście wpłynąć na politykę. Drugi argument, który przytacza Reglitz, zasadza się na uznaniu, że Internet jest środkiem koniecznym do realizacji niektórych podstawowych praw człowieka, w szczególności wolności wyrażania opinii i prawa stowarzyszania się (art. 19 i 20 PDPCz) realizowanych w świecie wirtualnym. Przy czym autor zwraca uwagę, że dostęp do Internetu nie jest po prostu środkiem umożliwiającym lepszą realizację wskazanych praw (choć i w te kwestii jego rola jest nie do przecenienia). Brak dostępu do Internetu oznacza pozbawienie określonych osób lub grup społecznych możliwości uczestniczenia w debacie publicznej. Trzeci argument na rzecz dyskutowanej tezy zasadza się

[10] T.D. Sniadecki, *A Road compared to a Horse: An Examination of Internet Access as a Human Right*, Honors Projects 283, https://scholarworks.gvsu.edu/honorsprojects/283 (dostęp: 07.09. 2020 r.).

[11] M. Reglitz, *The Human Right to Free Internet Access*, „Journal of Applied Philosophy" 2020, Vol. 37, Issue 2, s. 4.

na uznaniu kluczowej roli Internetu w ochronie podstawowych praw człowieka. W tym ujęciu Internet jawi się jako wyjątkowe narzędzie do ochrony kluczowych interesów jednostki i jako taki może być uznany za prawo podlegające ochronie.

Musimy przy tym pamiętać, że uznanie zasadności dostępu do Internetu za podstawowe prawo człowieka prowadzi do pytań, które z pozoru tylko mogą mieć charakter pytań technicznych, a które w rzeczywistości są pytaniami o naturę ewentualnego nowego prawa. Dotyczą one np. kosztów infrastruktury, szczególnie jeśli przyjmiemy, że zapewnienie dostępu do Internetu związane będzie ze spełnieniem pewnych wymagań technicznych, w szczególności dotyczących prędkości przesyła danych. Mówiąc inaczej: czy ludzie powinni mieć prawo dostępu do Internetu czy też do szybkiego Internetu. Ze względu na fakt, iż różnica pomiędzy rozmiarem pliku tekstowego, a plikiem wideo z 10 minutami nagrania jest nie do pominięcia, a także biorąc pod uwagę sposób funkcjonowania ludzi w Internecie, sposób odbierania treści, ich rodzaj, można uznać, że pytania takie są nadzwyczaj zasadne.

Rozważając problem uznania dostępu do Internetu za podstawowe prawo człowieka musimy mieć również na uwadze, że w związku z ogólnoświatową pandemią dyskusja na ten temat nie jest już sporem akademickim o to, czy dostęp do sieci spełnia wszystkie kryteria pozwalające uznać go za prawo lub czy dostęp ów jest jedynie narzędziem pozwalającym realizować określone prawa czy też sam powinien taki status otrzymać. W czasach, w których znaczna część pracy przeniesiona została do Internetu, w których nauka odbywa się bardzo często tylko zdalnie, w których to Internet służy jako podstawowe medium komunikacji władz z obywatelami[12] wydaje się zasadne stwierdzenie, że pozostaje już tylko pytanie nie o to, czy Internet powinien być uznany za podstawowe praw człowieka, ale jak należy tę kwestię uregulować. Wartym podkreślenia jest, że kwestie związane z uznaniem dostępu do Internetu za podstawowe prawa człowieka ogniskują wiele zagadnień, które pojawiają się w debacie o prawach człowieka i nowych technologiach. Tak jak zostało już wspomniane, Internet z jednej strony przynosi nowe zagrożenia, co widoczne jest np. w dyskusji o nowych rozwiązaniach w obszarze prawa do prywatności. Z drugiej strony daje nowe możliwości np. dokumentowania naruszeń praw człowieka: w czasach gdy praktycznie każdy człowiek wyposażony jest w przenośną kamerę podłączona do sieci dokumentowanie przypadków naruszeń praw człowieka jest zdecydowanie łatwiejsze (i widać to było tak w Kenii, jak i w Syrii czy również USA[13]).

---

[12] J.J. Berry, *COVID-19 exposes why access to the internet is a human right*, https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/

[13] T.F. McInerney, *How New Technologies Are Holding Human Rights Abusers Accountabl*e, https://www.worldpoliticsreview.com/articles/28921/in-the-fight-for-human-rights-technology-is-now-a-powerful-tool (dostęp: 07.09.2020 r.).

# Podsumowanie

Zagadnienia omówione powyżej mają różną naturę, a także w inny sposób wpływać mogą na międzynarodowe prawo praw człowieka i na krajowe porządki prawne. Wydaje się, że rozwój autonomicznych pojazdów generuje problemy, które rozwiązane mogą być przy wykorzystaniu istniejących mechanizmów (odpowiednio zmodyfikowanych). Z drugiej strony debata nad dostępem do Internetu może doprowadzić do rozszerzenia katalogu praw człowieka, choć nie będzie to radykalna zmiana samej koncepcji. Jednakże wielu badaczy zwraca uwagę, że rozwój biotechnologii i sztucznej inteligencji może doprowadzić do radykalnego zredefiniowania podstaw koncepcji praw człowieka. Jest to oczywiście dyskusja o przyszłości, jednakże już dziś można zauważyć zjawisko odwrotne: w literaturze zwraca się bowiem uwagę na interesujący fakt, iż rozwój nowych technologii może, w pewnym zakresie, odbywać się w ramach zakreślonych poprzez uwzględnienie międzynarodowych standardów ochrony praw człowieka. Zwracają na to uwagę autorzy raportu *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*[14], którzy próbowali prześledzić tworzenie normatywnych standardów dla systemów opartych o sztuczną inteligencję. Wskazując na kluczowe obszary, które są przedmiotem zainteresowania badaczy (takie jak prywatność, bezpieczeństwo czy brak dyskryminacji) stwierdzono, że naukowcy niezajmujący się na co dzień problematyką praw jednostki, coraz częściej odwołują się do międzynarodowych standardów praw człowieka w celu umocowania zasad funkcjonowania sztucznej inteligencji. Autorzy raportu zwracają uwagę, że dla tak szybko rozwijanej technologii „prawo praw człowieka oferuje atrakcyjnie ugruntowany zbiór koncepcji, które mogą być podstawą oceny powstających technologii". Przy czym problem określenia zasad funkcjonowania sztucznej inteligencji jawi się również jako impuls, który może do szeroko określonych ram koncepcji praw człowieka wnieść konkretne rozwiązania, a także zarysować nowe obszary, które mogą być przedmiotem badań. Z analizowanego raportu wynika również, że tak jak wśród osób zajmujących się problematyką praw człowieka można wskazać na znaczną świadomość problemów, które niesie z sobą rozwój AI, tak i badacze sztucznej inteligencji zdają się dostrzegać rolę praw człowieka. Oczywiście trudno jest w tym momencie wyrokować, w jakim zakresie prawa człowieka kształtować będą standardy funkcjonowania systemów opartych o sztuczna inteligencję. Można jednak założyć, że jest prawdopodobne iż tak się stanie, co nie tylko pozwoli „dowartościować" koncepcję niezbywalnych praw jednostki, ale również wykazać jej znaczenie we współczesnym świecie między innymi dzięki ukazaniu roli, jaką odgrywać mogą wypracowane standardy ochrony praw człowieka.

---

[14] J. Fjeld, N. Achten, H. Hilligoss, A. Nagy, M. Srikumar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, Berkman Klein Center Research Publication No. 2020-1, https://ssrn.com/abstract=3518482 (dostęp: 07.09. 2020 r.).

# Bibliografia

Berry J.J., *COVID-19 exposes why access to the internet is a human right*. Tekst dostępny na stronie: https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/

Fjeld J., Achten N., Hilligoss H.,Nagy A, Srikumar M., *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, Berkman Klein Center Research Publication No. 2020-1. Tekst dostępny na stronie: https://ssrn.com/abstract=3518482

Glancy D.J., P*rivacy in Autonomous Vehicles*, 52 „Santa Clara L. Rev." 2012, 1171.

Gliszczyńska-Grabias A., Sękowska-Kozłowska K., *Komentarz do art. 17 MPPOiP* [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, red. R. Wieruszewski, Lex 2012.

Iwan D., *Autonomous Vehicles – a New Challenge to Human Rights?*, „Adam Mickiewicz University Law Review" 2019, 9.

Kalliatakis G., Ehsan S., McDonald-Maier K.D., *A Paradigm Shift: Detecting Human Rights Violations Through Web Images*. Artykuł dostępny na stronie: https://arxiv.org/abs/1703.10501

Lee T.B., *Self-driving cars are a privacy nightmare. And it's totally worth it*, 21.05.2013. Artykuł dostępny na stronie: https://www.washingtonpost.com

McInerney T.F., *How New Technologies Are Holding Human Rights Abusers Accountabl*e. Tekst dostępny na stronie: https://www.worldpoliticsreview.com/articles/28921/in-the-fight-for-human-rights-technology-is-now-a-powerful-tool

Reglitz M., *The Human Right to Free Internet Access*, „Journal of Applied Philosophy" 2020, Vol. 37, Issue 2.

Sniadecki T.D., *A Road compared to a Horse: An Examination of Internet Access as a Human Right*, Honors Projects 283. Tekst dostępny na stronie: https://scholarworks.gvsu.edu/honorsprojects/283

Uliasz J., *Konstytucyjna ochrona prywatności w świetle standardów* międzynarodowych, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2018.

# Inne

Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 19 grudnia 1966 r. (Dz.U. z 1977 r., nr 38, poz. 167).

Zgromadzenie Ogólne ONZ, *The promotion, protection and enjoyment of human rights on the Internet*, 27 czerwca 2016 r., A/HRC/32/L.20.A/HRC/32/L.20.

# NOWE TECHNOLOGIE
# A BEZPIECZEŃSTWO

# KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA – ZAGADNIENIA WYBRANE

(*Elżbieta Kosior*)

## Wprowadzenie

Rozwój technologii cyfrowej, w której wiodącą rolę odegrał Internet zmienił otaczającą nas rzeczywistość w każdym wymiarze. Internet traktowany jest jako jedno z najważniejszych osiągnięć naszej cywilizacji, a „technologiczna rewolucja, w której kluczową rolę odgrywa…, to nie tylko początek końca współczesnych systemów politycznych, ale też początek końca człowieka, jakiego znamy. Człowiek przyszłości nie będzie już indywidualistą, ale elementem globalnego roju. Świat przyszłości to wspólnota monitorowana przez algorytmy i sprzężona w cyberprzestrzeni”[1]. I chociaż aktualność zachowują słowa historyka technologii Melvina Kranzberga „Technologia nie jest ani dobra, ani zła, ani obojętna”[2] nie sposób wyobrazić sobie dzisiejszego świata bez globalnej sieci połączeń, bez komunikacji, dla której odległość geograficzna przestała mieć znaczenie. Cybertechnologia zmieniła nieodwracalnie model funkcjonowania współczesnego państwa, które w strategicznych obszarach, gospodarczym, finansowym, politycznym, ale również międzynarodowym stało się sprawniejsze. Dlatego też niezawodność i stabilność sieci teleinformatycznych stała się nie tylko priorytetem, ale i wyzwaniem dla podmiotów odpowiedzialnych za system bezpieczeństwa państwa.

Rozwiązania techniczne, funkcjonalne i organizacyjne zabezpieczające cyberprzestrzeń przed niepożądanymi zdarzeniami wymagały zmian legislacyjnych na poziomie europejskim i krajowym. Usystematyzowanie i ujednolicenie przepisów obowiązujących w dziedzinie bezpieczeństwa cybernetycznego stało się koniecznością wobec wzrastającej liczby cyberzagrożeń. Nowatorskie podejście do tematu zaproponował ustawodawca europejski w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych[3]. Ustawa z dnia

---

[1] G. Lewicki *Internet, koniec człowieka jakiego znamy*, „Rzeczpospolita” z 2 kwietnia 2017 roku, https://www.rp.pl/Plus-Minus/303309929-In https://www.technologystories.org/first-and-second-laws/ternet-Koniec-czlowieka-jakiego-znamy.html (dostęp: 07.09.2020 r.).

[2] E. Schatzberg, *Pierwsza zasada Kranzberga*, *Technology's Stories* vol. 6, No. 4, https://www.technologystories.org/first-and-second-laws(dostęp: 07.09.2020 r.) i tam cytowany Melvin Kranzberg, „Technology and History: 'Kranzberg's Laws'”, *Technology and Culture* 27: 3 (lipiec 1986).

[3] Dz. Urz. UE. L nr 194 z 19.07.2016, s. 1–30).

5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa[4] implementowała do polskiego porządku prawnego wspomnianą powyżej dyrektywę. Otwarta, bezpieczna i chroniona cyberprzestrzeń pojawia się w strategii bezpieczeństwa cybernetycznego Unii Europejskiej, nakładając jednocześnie na kraje członkowskie obowiązek opracowania krajowych strategii ochrony sieci i informacji[5].

Rozdział prezentuje zarówno cel ustawodawcy europejskiego dążącego do ujednolicenia norm prawnych chroniących cyberprzestrzeń, jak też charakteryzuje najważniejsze zapisy polskiej ustawy oraz Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

## Problem bezpieczeństwa cybernetycznego w wybranym ustawodawstwie europejskim

Poziom technologii IT, szczególnie technologii informacyjno-komunikacyjnej (ang. *Information and Communication Technology*, ICT), stał się wyznacznikiem potęgi współczesnych państw, zarówno w relacjach społecznych, jak też w stosunkach międzynarodowych. Powszechny dostęp do Internetu przyczynił się do powstania globalnego społeczeństwa informacyjnego, dla którego przetwarzanie i wymiana informacji przestały być zależne od odległości[6]. W każdym obszarze życia społecznego i gospodarczego odnotowano postęp związany z niczym nieskrępowanym dostępem do informacji i możliwością ich wykorzystania. Z jednej strony Internet uczy, bawi, ułatwia codzienne funkcjonowanie chociażby poprzez dostęp do wysoko rozwiniętych usług z dziedziny bankowości, finansów, telekomunikacji, informatyki, handlu itd. Z drugiej zaś strony upowszechnienie Internetu, wzajemne oddziaływania w cyberprzestrzeni stworzyły zagrożenia w wymiarze wcześniej nieznanym, tak dla jednostki i społeczeństwa, jak i struktur państwa.

Termin cyberprzestrzeni funkcjonuje zarówno w literaturze przedmiotu, jak też w aktach prawnych[7]. Definiowanie cyberprzestrzeni jako globalnej wirtualnej

---

[4] Tekst jedn. Dz.U. z 2020 r., poz. 1369.

[5] Wspólny Komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów; Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52013JC0001) (dostęp: 4.09.2020 r.).

[6] Więcej na temat społeczeństwa informacyjnego S. Buregwa-Czuma, K. Garwol, *Definicje, właściwości i funkcje społeczeństwa informacyjnego*,Cejsh.icm.edu.pl, Vol. 6, s. 30–37, „Dydaktyka Informatyki" 2011.

[7] Zob.: Wstęp do uchwały nr 125 Rady Ministrów z dnia 22 października 2019 roku w sprawie Strategii cyberbezpieczeństwa RP na lata 2019–2024, według której: „Cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne, określone w artykule 3 pkt 3 ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2019 r., poz. 700 i in.), wraz z powiązaniami między nimi oraz relacjami z użytkownikami – zgodnie z artykułem 2 ust. 1b ustawy z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2019 r., poz. 1932)".

przestrzeni informacyjnej, w której odbywa się komunikacja między komputerami połączonymi w sieć internetową[8], czy też „świata sprzężonych ze sobą sieci komputerowych z wszelkimi możliwościami jej eksploatacji[9], podkreśla jej strategiczne znaczenie dla systemu bezpieczeństwa państwa podlegającego szczególnej ochronie. To właśnie w tym obszarze pojawiają się zagrożenia, które w konsekwencji mogą doprowadzić do destabilizacji struktur państwowych. Zagrożenia w sieci stały się na tyle realne, że w powszechnym obiegu znalazły się pojęcia takie jak: cyberwojna, cyberterroryzm, cyberszpiegostwo, cyberkonflikt, cybersabotaż, czy cyberprzestępstwo. Stały się one wyzwaniem dla cyberbezpieczeństwa definiowanego ustawowo jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

W Unii Europejskiej przyjęto, że: „Bezpieczeństwo cybernetyczne ogólnie odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci i tę infrastrukturę uszkodzić. Bezpieczeństwo cybernetyczne polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji”[10].

Rosnący dostęp do Internetu również na obszarach niezurbanizowanych obrazują dane Internet World Stats z 2020 roku[11] przedstawione w tabeli 1, z których wynika, że Europa odnotowała na przestrzeni ostatnich 20 lat największy wzrost upowszechnienia Internetu.

Podobny obraz wyłania się z danych Eurostatu za 2018 rok, wskazujących na wzrost odsetka gospodarstw domowych w Unii Europejskiej, posiadających dostęp do Internetu w ostatnich 10 lat. I tak oto:

- do 2018 r. odsetek gospodarstw domowych w UE-28 posiadających dostęp do sieci zwiększył się do 89% – wzrost o 29 punktów procentowych w porównaniu z 2008 r.,
- w 2018 r. z dostępu do szerokopasmowego Internetu korzystało 86% gospodarstw domowych w UE-28, co oznacza, że odsetek ten był o 38 punktów procentowych wyższy niż w 2008 r. (48%),

---

[8] *Słownik języka polskiego*, http://sjp.pwn.pl/sjp/cyberprzestrzen-2353915...

[9] A. Golonka, *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne*, s.64, https://sp.ka.edu.pl/numery/2016-1/studia-prawnicze-rim-2016-1-golonka.pdf i tam cytowany R. Łukasiewicz, *Rozwój informatyczny a cyberterroryzm* [w:] *Wojna z terroryzmem w XXI wieku*, red. B. Hołyst, K. Jałoszyński, A. Letkiewicz, Szczytno 2009, s. 110.

[10] *Strategia cyberbezpieczeństwa Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, Bruksela, 2013,www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf (dostęp: 04.09.2020 r.).

[11] INTERNET *USAGE STATISTICS. The Internet Big Picture. World Internet Users and 2020 Population Stats*, www.internetworldstats.com (dostęp: 05.09.2020 r.).

- odsetek osób w wieku od 16 do 74 lat w UE-28, którzy zamawiali lub kupowali towary lub usługi przez Internet na potrzeby prywatne, w 2018 r. wyniósł 60%[12].

Tabela 1. Światowe wykorzystanie Internetu i statystyka ludności
(szacunki za II kwartał roku 2020)

| **Regiony świata** | **Ludność (szac. 2020)** | **Populacja (%)** | **Internauci (30 czerwca 2020 r.)** | **Współczynnik penetracji (% pop.)** | **Rozwój 2000-2020** | **Świat (%)** |
|---|---|---|---|---|---|---|
| Afryka | 1,340,598,447 | 17,2% | 566,138,772 | 42,2% | 12,441% | 11,7% |
| Azja | 4.294.516.659 | 55,1% | 2.525.033.874 | 58,8% | 2,109% | 52,2% |
| **Europa** | **834,995,197** | **10,7%** | **727,848,547** | **87,2%** | **592%** | **15,1%** |
| Ameryka Łacińska / Karaiby | 654,287,232 | 8,4% | 467,817,332 | 71,5% | 2,489% | 9,7% |
| Bliski Wschód | 260,991,690 | 3,3% | 184,856,813 | 70, 8% | 5,527% | 3,8% |
| Ameryka Północna | 368,869,647 | 4,7% | 332,908,868 | 90, 3% | 208% | 6,9% |
| Oceania / Australia | 42,690,838 | 0,5% | 28,917,600 | 67,7% | 279% | 0,6% |
| **Ogółem** | **7,796,949,710** | **100%** | **4,833,521,806** | **62%** | **1239%** | **100%** |

Wraz z dynamiką rozwoju sieci teleinformatycznych w Europie, zwiększyła się świadomość zagrożeń, jakie towarzyszą zarówno osobom prywatnym, jak też podmiotom publicznym przy korzystaniu z nieograniczonego dostępu do Internetu i usług cyfrowych. Państwa Unii Europejskiej odnotowując jeden z najwyższych poziomów upowszechnienia Internetu na świecie, stały się szczególnym celem ataków cybernetycznych, ponosząc związane z tym rozliczne konsekwencje. Pomimo świadomości zagrożeń cyberprzestrzeni, polityka Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego ewoluowała na przestrzeni wielu lat, dostrzegając tak naprawdę wymiar tego problemu dopiero w 2013 roku.

W dniu 14 lutego 2013 roku Komisja Europejska wraz z Wysokim Komisarzem Unii ds. Zagranicznych i Polityki Bezpieczeństwa, we Wspólnym Komunikacie do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów przedstawiła strategię bezpieczeństwa cybernetycznego Unii Europejskiej „Otwarta, bezpieczna i chroniona cyberprzestrzeń”[13]. Obserwując siłę Internetu i jego wpływ na wszystkie aspekty życia społecznego i gospodarczego podkreślono, że cyberprzestrzeń powinna pozostać

[12] Dane statystyczne dotyczące gospodarki cyfrowej i społeczeństwa cyfrowego – gospodarstwa domowe i osoby fizyczne, www.ec.europa.eu (dostęp: 05.09.2020 r.).

[13] Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia bezpieczeństwa cybernetycznego Unii

otwarta i wolna, bo tylko taka stanowi forum dla wymiany informacji i pomysłów w skali światowej, tylko taka gwarantuje realizację praw podstawowych i wolność słowa oraz daje społeczeństwom szansę na walkę o bardziej demokratyczne i sprawiedliwe rządy – co uwidoczniło się podczas „arabskiej wiosny". Technologie cyfrowe dynamizując wzrost gospodarczy w krajach Unii, wpływają bezpośrednio na poprawę jakości życia jej mieszkańców. Uzasadniając potrzebę opracowania strategii bezpieczeństwa cybernetycznego stwierdzono, że wraz ze wzrostem wymiernych korzyści, jakie daje Internet, staje się on coraz bardziej podatny na zagrożenia, tworząc u jego użytkowników poczucie niepewności. Tempo wzrostu incydentów w cyberprzestrzeni, zarówno umyślnych, jak i niezamierzonych, zakłócających działanie sieci energetycznych, sieci telefonii komórkowych, dostaw wody czy usług zdrowotnych zaktywizowało działania poszczególnych rządów do opracowania strategii bezpieczeństwa cybernetycznego.

Prezentując założenia strategii cyberbezpieczeństwa Unii Europejskiej, Komisja Europejska wraz z Wysokim Przedstawicielem Unii zarysowała następujący program:

- osiągnięcie odporności na zagrożenia cybernetyczne poprzez zaangażowanie zarówno organów publicznych, jak i sektora prywatnego w poprawę zdolności, zwiększenia zasobów i usprawniania procedur zapobiegających incydentom w cyberświecie;
- radykalne ograniczenie cyberprzestępczości poprzez stworzenie rygorystycznego i skutecznego prawa;
- opracowanie polityki obronnej i rozbudowa zdolności bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony UE, wykorzystując w tym względzie współdziałanie cywilnych i wojskowych koncepcji dotyczących ochrony krytycznych zasobów cybernetycznych;
- rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego poprzez między innymi wspieranie jednolitego rynku produktów związanych z bezpieczeństwem w sieci, popytem na produkty o wysokim poziomie bezpieczeństwa oraz uruchomienie platformy publiczno-prywatnej dla rozwiązań w dziedzinie bezpieczeństwa sieci i informacji, które mogą być wykorzystane w Europie.

Odwołując się do konieczności radykalizacji przepisów prawnych zwalczających cyberprzestępczość, autorzy strategii odnieśli powyższe do:

- dyrektywy 2011/93/UE o zwalczaniu wykorzystywania seksualnego dzieci w Internecie;
- dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne (zawierającej normy przestępstw komputerowych);
- powołania Europejskiego Centrum do spraw Walki z Cyberprzestępczością (EC3) w ramach Europolu.

---

Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52013JC0001 (dostęp: 05.09.2020 r.).

Unia Europejska zapewniła wsparcie działań państw członkowskich poprzez przyjęcie skoordynowanego i opartego na współpracy podejścia, skupiającego organy ścigania i organy sądowe oraz inne, zainteresowane podmioty z sektora publicznego i prywatnego z UE i spoza jej granic[14]. Strategia unijna uznała za powinność każdego państwa członkowskiego utworzenie struktur przeznaczonych do działań w zakresie podniesienia odporności cybernetycznej, cyberprzestępczości i obrony. Uznano, że państwa członkowskie na poziomie krajowym powinny stworzyć własne strategie bezpieczeństwa cybernetycznego, w których zostaną określone role i obowiązki poszczególnych organów krajowych. W końcowych wnioskach autorzy strategii uznali, że wizja w niej przedstawiona zostanie zrealizowana jedynie na zasadzie partnerstwa między wieloma podmiotami, co może doprowadzić do uczynienia środowiska internetowego w UE najbezpieczniejszym na świecie przy jednoczesnej ochronie i wspieraniu praw obywateli.

Strategia cyberbezpieczeństwa, której główne założenia przywołano powyżej, była pierwszym kompleksowym rozwiązaniem obejmującym wszystkie aspekty tego problemu. Bez wątpienia wpływ na opracowanie i zdynamizowanie działań Unii w tej sferze miały wydarzenia związane z cyberatakami w kwietniu i maju 2007 roku w Estonii, które powszechnie przypisuje się rosyjskim hakerom[15] oraz ataki na rządowe strony internetowe i serwery w Gruzji podczas konfliktu gruzińsko-rosyjskiego w 2008 roku[16].

Wpływ konfliktu ukraińsko-rosyjskiego z 2014 roku, w którym odnotowano cyberataki na sieć energetyczną Ukrainy były z kolei asumptem do uszczegółowienia założeń Strategii bezpieczeństwa cybernetycznego Unii w zakresie cyberobrony. 18 listopada 2014 roku Rada Unii Europejskiej zatwierdziła Ramy polityki UE w zakresie cyberobrony, skoncentrowane wokół wspólnej polityki bezpieczeństwa i obrony (WPBiO)[17]. Za priorytetowe uznano:

- wspieranie rozwijania związanych z WPBiO zdolności państw członkowskich w zakresie cyberobrony,
- usprawnienie ochrony sieci łączności związanych z WPBiO wykorzystywanych przez podmioty UE,
- propagowanie współpracy i synergii cywilno-wojskowych z szerzej pojętymi politykami cybernetycznymi UE, odpowiednimi instytucjami i agencjami UE, a także z sektorem prywatnym,
- badania i technologia we współpracy z sektorem prywatnym i środowiskiem naukowym,
- poprawa możliwości w zakresie szkolenia, kształcenia i ćwiczeń,

[14] Tamże.
[15] *Estonia – pierwsza ofiara cybernetycznej wojny*, https://wiadomosci.onet.pl/tylko-w-onecie/estonia-pierwsza-ofiara-cybernetycznej-wojny/t3czdg5 (dostęp: 05.09.2020 r.).
[16] *Cyberatak na Gruzję*, https://kopalniawiedzy.pl/Gruzja-Rosja-atak,5438(dostęp 05.09.2020 r.).
[17] *Ramy polityki UE w zakresie cyberobrony*, https://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pl/pdf (dostęp: 05.09.2020 r.).

- zacieśnianie współpracy z odpowiednimi partnerami międzynarodowymi, a w szczególności z NATO[18].

Zapewnienie bezpieczeństwa łączności elektronicznej, infrastruktury oraz usług łączności elektronicznej, w szczególności ich integralności, dostępności i poufności stało się motywem przewodnim Rozporządzenia 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)[19], na mocy którego rozszerzono i doprecyzowano rolę europejskiej Agencję ENISA, stanowiącej specjalistyczne centrum ds. cyberbezpieczeństwa w Europie.

Rozporządzenie przydzieliło Agencji rolę ośrodka wiedzy wspierającego Instytucje Unii i państwa członkowskie w podnoszeniu poziomu bezpieczeństwa w sieci. Niezależnie od sektorowych regulacji prawnych, chroniących cyberprzestrzeń, już w 2013 roku rozpoczęła się procedura tworzenia kompleksowego rozwiązania dotyczącego cyberbezpieczeństwa w Unii Europejskiej, któremu nadano wymiar dyrektywy.

„Sieci oraz systemy i usługi informatyczne pełnią ważną rolę w społeczeństwie, a ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i społecznej, w szczególności dla funkcjonowania rynku wewnętrznego" – tymi słowami ustawodawca europejski rozpoczyna dyrektywę nr 2016/1148 NIS (*Network and Information Systems Directive*) z 6 lipca 2016 roku poświęconą działaniom na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[20]. Uzasadniając cel uchwalenia tego najważniejszego obecnie aktu europejskiego, wyznaczającego kierunki cyberbezpieczeństwa, w preambule wskazano, że „skala, częstotliwość oraz wpływ incydentów w zakresie bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Systemy te mogą się również stać obiektem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie ich działania. Tego typu incydenty mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników oraz powodować poważne straty w gospodarce Unii... Obecne zdolności nie są wystarczające do zapewnienia wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii. Państwa członkowskie bardzo się różnią pod względem poziomu gotowości, co powoduje niejednolite podejście w ramach Unii. Prowadzi to do nierównego poziomu ochrony konsumentów i przedsiębiorców oraz negatywnie wpływa na ogólny poziom bezpieczeństwa sieci i systemów informatycznych w Unii"[21].

---

[18] Tamże.

[19] 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, motyw 1 (Dz. Urz. UE.L 2013, nr 165, s. 41).

[20] 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 z dnia 6 lipca 2016 r. (Dz. Urz. UE.L nr 194, s. 1).

[21] Tamże.

Dyrektywa w sposób kompleksowy i międzysektorowy reguluje zagadnienia związane z bezpieczeństwem w cyberprzestrzeni, zobowiązując państwa członkowskie do zapewnienia minimalnego poziomu zdolności krajowych w tej dziedzinie poprzez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcie krajowych strategii w zakresie cyberbezpieczeństwa[22].

Zagadnienia prawne skupiają się wokół trzech wiodących tematów:

- instytucji, jakie powinny powstać we wszystkich państwach członkowskich,
- współpracy na poziomie europejskim,
- zobowiązań w zakresie bezpieczeństwa sieci i informacji.

Dyrektywa NIS wyposażyła organy publiczne w precyzyjnie określone narzędzia do przeciwdziałania i reagowania na incydenty w cyberprzestrzeni. Dotyczy to obowiązkowego raportowania, skoordynowania przepływu informacji czy też zinstytucjonalizowania współpracy CSIRT-ów[23]. Państwa członkowskie zostały zobowiązane do uchwalenia narodowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych określającej cele strategiczne i konkretne działania z zakresu polityki, które należy wdrożyć[24].

## Krajowe regulacje prawne w dziedzinie cyberbezpieczeństwa

Dyrektywa UE NIS z 2016 roku wyznaczyła okres 2 lat na wprowadzenie jej zapisów do porządku prawnego państw członkowskich. 5 lipca 2018 roku uchwalono ustawę o Krajowym systemie cyberbezpieczeństwa, z mocą obowiązywania od 28 sierpnia 2018 roku[25]. Jest to pierwszy akt prawny regulujący całościowo problem bezpieczeństwa w cyberprzestrzeni na poziomie krajowym, obejmując zagadnienia rozproszone przed jej uchwaleniem w różnych ustawach[26]. Celem ustawodawcy, zapisanym w art. 3, było zapewnienie:

- niezakłóconego świadczenia usług kluczowych i usług cyfrowych,

---

[22] Uzasadnienie projektu ustawy o Krajowym systemie cyberbezpieczeństwa http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505 (dostęp: 05.09.2020 r.).

[23] Więcej na ten temat Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa, https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/

[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148..., motyw 29.

[25] Tekst jedn. Dz.U. z 2020 r., poz. 1369.

[26] Czytaj przykładowo: Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (tekst jedn. Dz.U. z 2019 r., poz. 796), ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn Dz.U. z 2019 r., poz. 1398), ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tj. Dz.U. z 2019 r., poz. 2460), ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (tj. Dz.U. z 2019 r., poz. 2357).

- osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Zakresem przedmiotowym objęto trzy grupy problemów:

- organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu,
- sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy,
- zakres Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej (której dotyczy rozdział 13 ustawy).

Przedstawiając legalne definicje najistotniejszych pojęć ustawodawca odnosi je zarówno do zakresu podmiotowego, jak i przedmiotowego, sankcjonując przy tym działające od lat w ramach swojej właściwości trzy podmioty na poziomie krajowym, zajmujące się reagowaniem na incydenty komputerowe, które w dyrektywie 2016/1148 zostały określone jako CSIRT (ang. *Computer Security Incident Response Teams*). W Polsce są to CSIRT GOV, czyli Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, CSIRT MON, czyli System Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej oraz CSIRT NASK, czyli NC Cyber Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy[27]. Wprowadzając kilka kategorii incydentów: poważny, istotny, krytyczny i incydent w podmiocie publicznym dokonano jego rozróżnienia w zależności od rodzaju podmiotu zgłaszającego i stopnia jego oddziaływania (progów). Jako potencjalną przyczynę wystąpienia incydentów wskazano poziom zagrożenia cyberbezpieczeństwa. Wprowadzono pojęcie usługi kluczowej, która ma szczególne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienionej w wykazie usług kluczowych (art. 2 pkt 16), przydzielając operatorom tych usług w 3 rozdziale szczególne obowiązki, podobnie jak operatorom usług cyfrowych (rozdział 4).

Operatorzy usług kluczowych to firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej z dziedziny energetyki, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej, wobec których organ właściwy (ministerstwo danego sektora) wydał decyzję o uznaniu za operatora usługi kluczowej. Dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe, które mają określona sytuację prawną (osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, mające siedzibę

[27] Uzasadnienie projektu ustawy o Krajowym systemie cyberbezpieczeństwa, s. 17, http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505 (dostęp: 05.09.2020 r.).

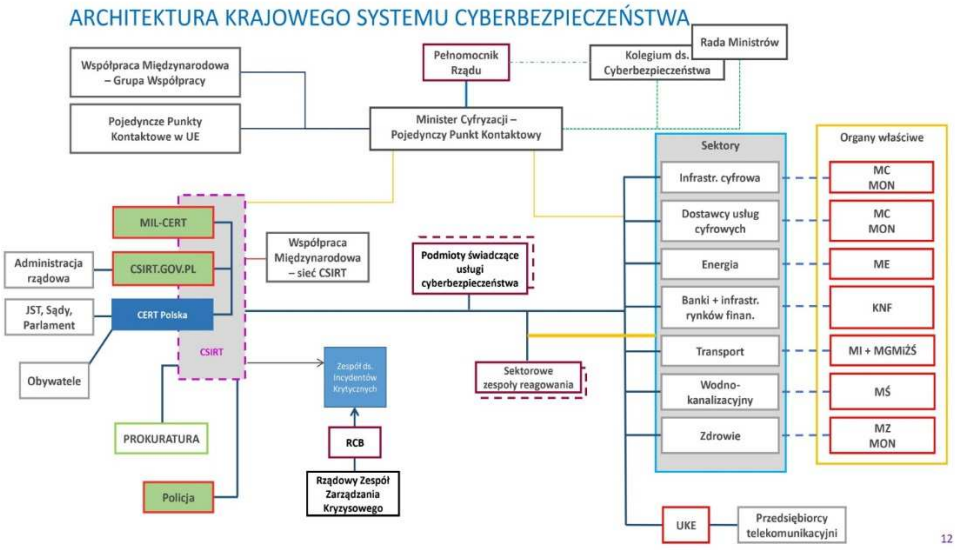
lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej.

W rozdziale 14 ustawodawca zawarł przepisy dotyczące kar pieniężnych, które mogą być nałożone na operatorów usług kluczowych i dostawców usług cyfrowych za zaniechanie ustawowych obowiązków. Wysokość kar uzależniona jest od rodzaju przewinienia i zagrożenia dla dobra chronionego, niemniej jednak przewidziano, przy łącznym spełnieniu (opisanych w ustawie) kryteriów karę 1 000 000 zł, jako karę najwyższą, którą nakłada organ właściwy do spraw cyberbezpieczeństwa.

W strukturach systemu cyberbezpieczeństwa znalazły się następujące podmioty:

1) organy właściwe,
2) CSIRT poziomu krajowego,
3) operatorzy usług kluczowych i dostawców usług cyfrowych,
4) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa
5) podmioty świadczące usługi z zakresu cyberbezpieczeństwa (CSIRT komercyjne),
6) Rządowe Centrum Bezpieczeństwa (w zakresie zarządzania kryzysowego i ochrony infrastruktury krytycznej)
7) przedsiębiorcy telekomunikacyjni
8) administracja publiczna.

Wzajemne zależności przedstawia schemat udostępniony przez Departament Bezpieczeństwa i Zarządzania Kryzysowego, Ministerstwo Energii[28], oparty na art. 4 ustawy.




[28] www. gov.pl

Przydzielenie szczegółowych kompetencji i obowiązków poszczególnym podmiotom budującym system cyberbezpieczeństwa następuje w kolejnych artykułach ustawy, w rozdziałach od 3 do 10. Z kolei w rozdziale 11. przydzielono funkcje nadzorcze nad operatorami usług kluczowych, dostawcami usług cyfrowych i podmiotami świadczącymi usługi.

Na podstawie art. 68 ustawy Rada Ministrów podjęła w dniu 22 października 2019 r uchwałę zatwierdzającą Strategię cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 opracowaną przez Ministerstwo Cyfryzacji[29].

Strategia na lata 2019–2024 jest kontynuacją i rozszerzeniem działań, podejmowanych przez administrację rządową, mających na celu podniesienie poziomu bezpieczeństwa cybernetycznego w Rzeczypospolitej Polskiej, zastępuje jednocześnie Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022[30].

Głównym celem Strategii jest zwiększenie odporności systemów informacyjnych operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na cyberzagrożenia, jak też zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń. Powyższe ma wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) i szpiegowskim w cyberprzestrzeni[31]. „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jest spójna z prowadzonymi działaniami dotyczącymi systemów teleinformatycznych operatorów infrastruktury krytycznej oraz uwzględnia potrzeby zapewnienia zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych”[32].

## Podsumowanie

Cyberbezpieczeństwo i cyberzagrożenie stały się pojęciami współzależnymi. Wzrost liczby cyberataków, nowe rodzaje incydentów ingerujących i destabilizujących cyberprzestrzeń aktywizują państwa do doskonalenia obrony zarówno w znaczeniu technologicznym, organizacyjnym, jak i prawnym.

---

[29] Uchwała nr 125 Rady Ministrów w sprawie Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (MP z 2019 r., poz.1037).

[30] Uchwała nr 52/2017 Rady Ministrów z dnia 27.04.2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

[31] Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, 2. Kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej, s. 6 (M.P. z 2019 r., poz. 1037).

[32] Tamże.

Upowszechnienie Internetu i usług cyfrowych potwierdziło z kolei, że nie jest możliwe takie „uszczelnienie" systemu, które wyeliminowałoby zagrożenia w cyberprzestrzeni.

W Polsce obserwuje się wzrost liczby incydentów, ustawowo określanych jako zdarzenia, mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo.

I tak oto w 2019 roku odnotowano 6484 incydenty, co dało wzrost w stosunku do 2018 roku o 73% (3739 incydentów). Phishing stanowił ok. 54,2% wszystkich incydentów złośliwe oprogramowanie stanowiło ok. 14,9% incydentów, a „obraźliwe i nielegalne treści", w tym spam to 12,1% wszystkich zarejestrowanych spraw[33]. Z raportu CERT Polska (ang. *Computer Emergency Response Team*) zaobserwować można niepokojący trend zwiększania się liczby rozpowszechnianych nieprawdziwych informacji, tzw. *fake newsów*. Kojarzone dotychczas z wewnętrzną rywalizacją polityczną przybierają obecnie zdecydowanie inny charakter wojny informacyjnej ukierunkowanej na wywołanie negatywnych emocji[34].

Krajowy system bezpieczeństwa w cyberprzestrzeni zyskał wymiar ustawowy i wraz z aktami wykonawczymi[35] stworzył nowy model zarządzania zagrożeniami dla cyberbezpieczeństwa. Ustawa, „buduje" platformę do współdziałania szeregu podmiotów ze sfery publicznej, jak też podmiotów komercyjnych w dziedzinie monitorowania zagrożeń i reagowania na incydenty. Zakreślenie precyzyjnych obowiązków dla operatorów usług kluczowych i dostawców usług cyfrowych, nadzór i kontrola właściwych organów nad realizacją zadań w zakresie cyberbezpieczeństwa, możliwość nałożenia kar pieniężnych za zaniechanie ustawowych obowiązków pozwalają sądzić, że obowiązujące prawo wpłynie na poprawę odporności państwa na cyberzagrożenia.

Zarówno rozwiązania przyjęte przez ustawodawcę unijnego, jak też krajowego nie mogą być uznane za ostateczne i optymalne, co uzasadnia poszukiwanie nowych rozwiązań legislacyjnych. 17 kwietnia 2019 roku Parlament Europejski i Rada (UE) wydały Rozporządzenie 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[36].

Uzasadnieniem dla przyjęcia nowego Aktu o cyberbezpieczeństwie było min. zwiększenie ryzyka w cyberprzestrzeni, a tym samym podatności ogółu społeczeństwa na cyberzagrożenia, w szczególności osób bardziej na nie podatnych, takich jak dzieci – wide moduł 3 Rozporządzenia. Nasilające się cyberataki wymagają

---

[33] *Krajobraz bezpieczeństwa polskiego Internetu*. Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (dostęp: 05.09.2020 r.).

[34] Tamże, s. 41–43.

[35] Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r., poz. 2479).

[36] Dz.U. UE.L.2019.151.15 z dnia 07.06.2019 r.

zdaniem ustawodawcy unijnego zwiększenia ochrony przed nimi zarówno społeczeństwa, jak i gospodarki. Nowe regulacje wyposażają Europejską Agencję w mandat uprawniający do funkcjonowania i posiadania środków umożliwiających jej rozwój. Rozszerzone zostały kompetencje ENISY o certyfikację, która ma z jednej strony poprawić poziom bezpieczeństwa, z drugiej zaś zaangażować podmioty komercyjne do inwestowania w cyberbezpieczeństwo.

W odniesieniu do prawa krajowego, minister cyfryzacji 8 września 2020 skierował do konsultacji społecznych projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, obejmujący:

- rozszerzenie zakresu podmiotowego o przedsiębiorców telekomunikacyjnych i dostawców usług zaufania (objętych wyłączeniem na mocy art. 1 ust. 2 pkt 1 i 2 dotychczasowej ustawy),
- wprowadzenie pojęcia incydentu telekomunikacyjnego,
- powołanie Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego, czyli CSIRT Telco,
- dokonywanie na wniosek członka Kolegium ds. Cyberbezpieczeństwa oceny ryzyka dostawcy sprzętu lub oprogramowania teleinformatycznego, istotnego dla cyberbezpieczeństwa. Ocena ryzyka na poziomie wysokim będzie wiązała się z zakazem wprowadzania sprzętu, oprogramowania i usług danego dostawcy, który w ciągu 5 lat od ogłoszenia komunikatu zobowiązany będzie do wycofania się z rynku. Status ryzyka umiarkowanego lub niskiego przyznany krajowym podmiotom będzie oznaczał zakaz wprowadzenia do użytkowania nowych produktów danej firmy, a podmioty z wysokim ryzykiem będą wyłączone z zamówień publicznych,
- wprowadzenie znaczących kar pieniężnych za używanie sprzętu i oprogramowania z wysokim ryzykiem (do 3% całkowitego obrotu światowego dla podmiotów prywatnych i do 100 000 zł dla publicznych).
- stworzenie większej liczby sektorowych CSIRT oraz operacyjnych centrów bezpieczeństwa SOC.

W uzasadnieniu do proponowanych zmian Ministerstwo Cyfryzacji powołało się na zobowiązania unijne w zakresie podniesienia bezpieczeństwa sieci telekomunikacyjnych oraz na usprawnienie funkcjonowania najważniejszych instytucji w systemie cyberbezpieczeństwa RP. Po zakończeniu procedury legislacyjnej znowelizowana ustawa wejdzie w życie 21 grudnia 2020 roku.

Czy rozwiązania prawne zaproponowane w noweli do ustawy przyniosą wymierny skutek dla szeroko rozumianego bezpieczeństwa w cyberprzestrzeni nie sposób przewidzieć. Pewne natomiast jest to, że prawo związane z tą dziedziną nie jest stabilne i takim być nie może. Rozwoju cybertechnologii nie można zatrzymać, podobnie jak nie można przewidzieć skali zagrożeń w cyberprzestrzeni. To właśnie tempo zmian zachodzących w tej sferze bezpieczeństwa będzie wyznaczało kierunek prawodawstwa europejskiego i krajowego. Zaznaczyć należy, że prawo związane z cyberbezpieczeństwem jest pojęciowo skomplikowane, a w związku z tym same akty prawne stają się nieczytelne. Niejednoznaczność

zapisów, wielopodmiotowość struktury systemu cyberbezpieczeństwa i wielowątkowość ustawy oznaczają, że można spodziewać się problemów interpretacyjnych, wymagających wykładni prawnej. Jak podkreślono powyżej system bezpieczeństwa w cyberprzestrzeni nie jest doskonały. Stworzenie kompleksowych regulacji prawnych, opracowanie odpowiednich procedur, które mają ów system uszczelnić, przygotowanie „zaplecza" technologicznego nie spełnią swojej roli, jeżeli prawo nie będzie należycie rozumiane i respektowane. Udział jednostki w kształtowaniu bezpiecznej cyberprzestrzeni staje się oczywisty, jeżeli zważy się na procent zdarzeń niepożądanych, incydentów wymierzonych właśnie w dobra prawne osób fizycznych.

Wolna, otwarta i bezpieczna cyberprzestrzeń powinna wszak stać się priorytetem nie tylko dla państwa, ale też każdego z nas z osobna, bowiem właśnie tam przenieśliśmy większą część swojej aktywności z dawnego świata realnego[37].

## Bibliografia

Buregwa-Czuma S., Garwol K., *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, „Dydaktyka Informatyki" 2011, Vol. 6.

Golonka A., *Cyberprzestępczość – międzynarodowe standardy zwalczania zjawiska a polskie regulacje karne*, „Studia Prawnicze. Rozprawy i Materiały" 2016, nr 1/18.

Kranzberg M., *Technology and History: 'Kranzberg's Laws*, "Technology and Culture" 1986, No. 27/3.

Łukasiewicz R., *Rozwój informatyczny a cyberterroryzm* [w:] *Wojna z terroryzmem w XXI wieku*, red. B. Hołyst, K. Jałoszyński, A. Letkiewicz, Szczytno 2009.

Sitek M., *Prawne ramy bezpieczeństwa jednostki w cyberprzestrzeni*, „Journal of Modern Science" 2/2018, Vol. 37.

## Prawodawstwo

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 z dnia 6 lipca 2016 r.).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (tekst jedn. Dz.U. z 2019 r., poz. 2357).

Ustawa z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2019 r., poz. 1932).

Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tekst jedn. Dz.U. z 2019 r. Dz.U. z 2019 r., poz. 2460).

Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U. z 2019 r., poz. 700 i in.).

[37] M. Sitek, *Prawne ramy bezpieczeństwa jednostki w cyberprzestrzeni*, Journal of Modern Science", 2/2018, Vol. 37, s. 179.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jedn. Dz.U. z 2019 r. poz. 1398).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (tekst jedn. Dz.U. z 2019 r., poz. 796).

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, motyw 1 (Dz. Urz. UE.L 2013, nr 165, s. 41).

Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r., poz. 2479).

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, 2. Kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej, s. 6 (M.P. z 2019 r., poz. 1037).

Uchwała nr 125 Rady Ministrów w sprawie Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (MP z 2019 r., poz. 1037).

Uchwała nr 52/2017 Rady Ministrów z dnia 27.04.2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 roku w sprawie Strategii cyberbezpieczeństwa RP na lata 2019–2024.

## Inne

*Dane statystyczne dotyczące gospodarki cyfrowej i społeczeństwa cyfrowego – gospodarstwa domowe i osoby fizyczne*, www.ec.europa.eu (dostęp: 05.09.2020 r.).

*Krajobraz bezpieczeństwa polskiego Internetu*. Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (dostęp: 05.09.2020 r.).

Krajowy system cyberbezpieczeństwa – gov.pl

*Ramy polityki UEw zakresie cyberobrony*, https://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pl/pdf

„Strategia cyberbezpieczeństwa Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", Bruksela,2013,www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf

Uzasadnienie projektu ustawy o Krajowym systemie cyberbezpieczeństwa, s. 17, http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505

*Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństw*a, https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/

Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52013JC0001.

Wspólny Komunikat Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", https://eur-lex.europa.eu/legal-content/PL/ TXT/?uri=CELEX%3A52013JC0001.

## Netografia

*Cyberatak na Gruzję*, https://kopalniawiedzy.pl/Gruzja-Rosja-atak,5438

*Estonia – pierwsza ofiara cybernetycznej* wojny https://wiadomosci.onet.pl/tylko-w-onecie/estonia-pierwsza-ofiara-cybernetycznej-wojny/t3czdg5

INTERNET *USAGE STATISTICS. The Internet Big Picture. World Internet Users and 2020 Population Stats*, www.internetworldstats.com

Lewicki G., *Internet, koniec człowieka jakiego znamy*, „Rzeczpospolita" z 2 kwietnia 2017 r., https://www.rp.pl/Plus-Minus/303309929-Inhttps://www.technologystories.org/first-and-second-laws/ternet-Koniec-czlowieka-jakiego-znamy.html

Schatzberg E., *Pierwsza zasada Kranzberga*, „Technology's Stories" Vol. 6, No. 4, https://www.technologystories.org/first-and-second-laws

*Słownik języka polskiego*, http://sjp.pwn.pl/sjp/cyberprzestrzen-2353915

# ANALIZA I PORÓWNANIE ODPOWIEDZIALNOŚCI KARNEJ ZA CYBERPRZESTĘPSTWA W RZECZYPOSPOLITEJ POLSKIEJ, ZJEDNOCZONYM KRÓLESTWIE WIELKIEJ BRYTANII I IRLANDII PÓŁNOCNEJ ORAZ STANACH ZJEDNOCZONYCH AMERYKI

(*Krzysztof Nowakowski*)

## Wprowadzenie

W ciągu ostatnich dekad olbrzymi skok technologiczny odcisnął trwałe piętno na społeczeństwie, powodując w nim nieodwracalne zmiany. Nowe technologie dały ludzkości nieograniczony dostęp do globalnej komunikacji, olbrzymich zasobów informacji oraz nowych, wcześniej nieosiągalnych udogodnień. Jednak wraz z nowymi technologiami pojawiły się również nowe rodzaje przestępstw, które początkowo marginalne, szybko zaczęły stanowić zagrożenie dla gwałtownie rosnącej liczby osób korzystających z Internetu i systemów informatycznych[1]. To z kolei wymusiło na systemach prawnych szybkie, a przez to dość chaotyczne i nieustandaryzowane, dostosowanie się do nowych rodzajów przestępstw i zagrożeń. W dzisiejszych czasach jesteśmy świadkami nieustannego wyścigu pomiędzy szybko rozwijającymi się technologiami, których negatywnym efektem jest powstawanie zarówno nowych cyberprzestępstw, jak i nowych sposobów popełniania ich, a, z natury powolnymi, systemami legislacyjnymi próbującymi nadążyć za technologią[2].

## Problematyczna natura cyberprzestępczości

Z powodu samej struktury globalnej sieci telekomunikacyjnej cyberprzestępstwa stanowią jedno z najcięższych wyzwań stawianych przed organami postępowania karnego. Internet zapewnia przestępcom anonimowość oraz globalny

[1] CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html (dostęp: 11.08.2020 r.).

[2] M. Zbrojewska, V. Mosorov, S. Biedron, T. Panskyi, *Jak definiujemy cyberprzestępstwo?*, „Informatyka. Automatyka. Pomiary w Gospodarce i Ochronie Środowiska" 2016, t. 2, s. 64–68.

zasięg, co w efekcie sprawia, że ściganie i karanie cyberprzestępców jest znacznie utrudnione.

Pierwszym poważnym problemem w zwalczaniu cyberprzestępczości w Polsce jest charakterystyka prawa stanowiąca, że nawet w przypadku zarejestrowania przestępstwa dokonywanego przeciwko bezpieczeństwu informacji, postępowanie karne nie jest wszczynane z urzędu. Dopiero bezpośredni wniosek od pokrzywdzonego jest w stanie rozpocząć proces karny przeciwko przestępcy[3].

Kolejnym problemem jest znalezienie, rozpoznanie oraz zgromadzenie odpowiedniego materiału dowodowego[4]. Środowisko sieciowe jest bardzo skomplikowanym, otwartym i zatłoczonym miejscem popełnienia przestępstwa, w którym łatwo jest pozostać niezauważonym. Konsekwencją powyższych cech jest łatwość, z jaką przestępcy są w stanie zatrzeć za sobą ślady po przeprowadzeniu ataku. Technologie wirtualizacji, konteneryzacji, wykorzystywania botnetu, zmienianie adresów MAC karty sieciowej, użycie serwisów VPN i wiele innych technik, potrafi skutecznie zamaskować przestępcę w ruchu sieciowym. Dodatkowo czyszczenie rejestrów maszyn, które zostały zaatakowane, sprawia, że często nie pozostają żadne ślady po hackerze i jego szkodliwych działaniach[5].

Nawet w przypadku zebrania materiału dowodowego wystarczającego do potwierdzenia winy przestępcy można napotkać kolejne problemy. Zebrane dowody wskazują jedynie maszynę, konkretniej zaś, jej identyfikatory, zazwyczaj adres IP oraz adres MAC karty sieciowej. Mając te dane, organy ścigania muszą znaleźć osobę, do której atakująca maszyna należy, a następnie potwierdzić, że to ta osoba dokonywała danego przestępstwa, co pozwoli na wystosowanie zarzutów i sprowadzanie oskarżonego przed oblicze sądu.

W tym miejscu trafiamy na główny problem związany ze zwalczaniem hackerstwa. Jedną z największych różnic pomiędzy „tradycyjną" przestępczością a cyberprzestępczością jest odległość, z jakiej może być ona dokonywana. W przypadku „tradycyjnych" przestępstw skala zasięgu jest zazwyczaj lokalna bądź regionalna, zdecydowana większość z nich dokonywana jest na terenie tej samej jurysdykcji karnej co dokonująca ich osoba. Cyberprzestępstwa mogą być dokonywane z dowolnego miejsca na globie posiadającego połączenie z Internetem, co sprawia, że ściganie i postawienie osoby odpowiedzialnej przed sądem jest niejednokrotnie niemożliwe[6].

---

[3] T. Prauzner, *Prawo a bezprawie w Internecie*, Prace Naukowe Akademii im. Jana Długosza w Częstochowie, „Edukacja Techniczna i Informatyczna" 2009, t. 4, s. 297–302.
INFOR Prawo, *Czym jest cyberprzestępstwo?*, www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,2,Czym-jest-cyberprzestepstwo.html (dostęp: 04.08.2020 r.).

[4] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawne i kryminalistyczne*, rozdz. V, Uniwersytet w Białymstoku, Białystok 2017.

[5] H.L. Armstrong, P.J. Forde, *Internet anonymity practices in computer crime*, „Information Management & Computer Security" 2003, Vol. 11, No. 5, p. 209–215.

[6] IKMJ, *Cyberbezpieczeństwo w Polsce – statystyki*, ikmj.com/cyberbezpieczenstwo-w-polsce-statystyki/ (dostęp: 04.08.2020 r.). Mediarecovery. *Malware okiem prawnika – część pierwsza*, mediarecovery.pl/malware-okiem-prawnika-czesc-pierwsza/ (dostęp: 05.08.2020 r.).

# System prawny a cyberprzestępczość – Polska

Podstawowym dokumentem definiującym przestępstwa i wykroczenia związane z cyberprzestępczością oraz odpowiedzialność za nie jest polski kodeks karny, szczególnie zaś Dział XXIII – „Przestępstwa o ochronie danych osobowych" oraz Dział XXV – „Przestępstwa przeciwko mieniu". Na podstawie tych Działów możemy podzielić przestępstwa komputerowe na trzy podgrupy[7]:

- przestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanych informacji – jest to najszersza grupa przestępstw obejmująca m.in:
  - nielegalny dostęp do systemu – art. 267 § 1 i 2 k.k. Ta grupa w przeważającej części składa się z działań polegających na łamaniu haseł i innych zabezpieczeń elektronicznych w celu włamania się do systemu ofiary. Zazwyczaj przestępstwa te występują w połączeniu z innymi, np. kradzieżą danych cyfrowych, gdyż samo włamanie się jest tylko pojedynczym elementem ataku hackerskiego. Osoby orzeczone winnymi powyższych przestępstw mogą zostać poddane karze grzywny bądź pozbawienia wolności do lat 2,
  - naruszenie tajemnicy informacji – art. 267 § 1 i 2 k.k. Najpopularniejszą metodą tzw. sniffingu są ataki hackerskie przeprowadzane jedną z metod należących do rodziny ataków „Man in the Middle". W atakach tych przestępca podszywa się pod urządzenie będące częścią sieci komunikacyjnej pomiędzy dwiema ofiarami (np. klientem i bankiem), dzięki czemu może przechwycić wrażliwe informacje. Osoby dopuszczające się tego typu przestępstw podlegają karom analogicznym jak opisane w poprzednim przypadku,
  - naruszenie integralności danych – art. 268 oraz 268a k.k. W tej kategorii znajdziemy wszystkie przestępstwa skutkujące zniszczeniem lub korupcją danych. Najczęściej spotykanymi wirusami wykorzystywanymi w takich atakach są robaki bądź konie trojańskie, zaś celami ataków są duże firmy i instytucje publiczne, gdzie uszkodzenie wrażliwych danych może mieć poważne finansowe konsekwencje. Kodeks karny przewiduje do 3 lat pozbawienia wolności za tego typu działalność hackerską,
  - naruszenie integralności systemu operacyjnego – art. 269 k.k. Bardzo obszerna podgrupa działalności przestępczej, która częściej skupia się na atakowaniu instytucji zamiast prywatnych osób. W jej skład wchodzą ataki typu DDOS bądź flood, wymagające specjalistycznej wiedzy i olbrzymich zasobów, liczących nieraz dziesiątki tysięcy maszyn.

[7] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawne i kryminalistyczne*, rozdz. IV, Uniwersytet w Białymstoku, Białystok 2017, rozdział IV, Mediarecovery, *Cyberprzestępczość – odpowiedzialność karna*, mediarecovery.pl/cyberprzestepczosc-odpowiedzialnosc-karna/ (dostęp: 05.08.2020 r.).

Ataki te mają na celu zablokowanie możliwości świadczenia usług przez dane systemy, najczęściej serwerowe i mogą być bardzo dewastujące zarówno dla firm, jak i instytucji państwowych. Ze względu na swoją skalę i wymagane wyszkolenie techniczne, osoby odpowiedzialne za te przestępstwa są niezwykle trudne do uchwycenia przez służby ścigania, gdy się to jednak stanie, przestępcom grozi od 3 miesięcy do 5 lat więzienia,

- cyberszpiegostwo – art. 130 § 3 k.k. W rozumieniu paragrafu jako działanie szpiegowskie przeciwko Rzeczypospolitej Polskiej na rzecz obcego wywiadu, niezwiązane ze szpiegostwem przemysłowym. W zależności od wyroku sądu winny tego przestępstwa może otrzymać karę pozbawienia wolności od 6 miesięcy do 8 lat,

- drugą, mniejszą grupą, są przestępstwa związane z treścią informacji publikowanej za pomocą Internetu, wyróżnić wśród nich możemy:
  - wykorzystanie mediów telekomunikacyjnych na szkodę małoletniego – art. 200a oraz art. 202 k.k. Do tej podgrupy zaliczamy tworzenie i rozpowszechnianie treści pornograficznych z udziałem osób małoletnich, wykorzystywanie środków telekomunikacji do spotkania z osobą małoletnią w celu odbycia stosunku seksualnego, wykorzystując wymuszenie bądź oszustwa oraz składanie propozycji obcowania płciowego osobie małoletniej. Za powyższe czyny grozi do 3 lat więzienia,
  - przestępstwa przeciwko czci – art. 212 § 2 oraz art. 216 k.k. W skład tej podgrupy zaliczyć możemy wszelkie przestępstwa polegające na znieważeniu bądź zniesławieniu osób prywatnych i publicznych z wykorzystaniem środków telekomunikacyjnych, traktowanych jako środki masowego przekazu. Kodeks karny przewiduje kary grzywny, ograniczenia wolności lub jej pozbawienie do roku,
- trzecią grupą przestępstw są przestępstwa, które medium Internetu traktują instrumentalnie. Do tej grupy zaliczymy takie przestępstwa jak: oszustwo, naruszenie praw własności intelektualnej, cyberstalking, kradzież tożsamości i inne, zaś ich kwalifikacja prawna zależy od rodzaju kwalifikacji tradycyjnego odpowiednika tych przestępstw.

# System prawny a cyberprzestępczość – Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej

Najważniejszym dokumentem dotyczącym cyberprzestępczości w Wielkiej Brytanii jest „Computer Misuse Act”[8] wydany w 1990 roku, stanowiący fundament orzekania wyroków w sprawach związanych z cyberprzestępczością. Przez lata powyższy dokument był wielokrotnie aktualizowany oraz rozwijany, ponadto w życie weszły inne akty, które odnoszą się do cyberprzestępczości tylko jako do pobocznego aspektu przestępstwa, któremu te akty są poświęcone, nie stanowi ona jednak ich sedna. Do takich aktów należą m.in. „Police and Justice Act”, „Interception of Communications Act” i „Terrorism Act”[9].

Analogicznie jak w Polsce, tak i w Wielkiej Brytanii jesteśmy w stanie rozróżnić cyberprzestępstwa na ściśle związane z atakami informatycznymi (*cyber-centric*) odpowiadające pierwszej grupie wcześniejszego podziału cyberprzestępstw, jak i na przestępstwa wykorzystujące informatykę i pokrewne jej technologie instrumentalnie (*cyber-enabled*), które zostaną pominięte w opisie[10].

Computer Misuse Act adresuje przestępstwa związane z cyberbezpieczeństwem w trzech sekcjach, opisujących kolejno[11]:

1. Nieautoryzowany dostęp do komputera – obejmujący wymuszenie na komputerze wykonania jakiejkolwiek funkcji mającej za zadanie nieautoryzowany dostęp. Warunkiem możliwości wystąpienia przestępstwa jest wymóg świadomego działania przeciwko zabezpieczeniom. Osobom odpowiedzialnym za te czyny grozi do 2 lat więzienia.
2. Nieautoryzowany dostęp z zamiarem popełnienia lub ułatwienia popełnienia dalszych przestępstw – dotyczy to osób dokonujących przestępstwa z punktu pierwszego, z zamiarem wyrządzenia dodatkowych szkód przeciwko komputerowi, jego użytkownikowi bądź danym znajdującym się na maszynie. W tej grupie zawrzeć można większość przestępstw przeciwko bezpieczeństwu informacji, jak i kradzież danych. CMA przewiduje do 5 lat więzienia za tego typu przestępstwa.
3. Nieautoryzowane działania mające na celu utrudnienie lub lekkomyślne utrudnienie działania komputera – jest to kolejna bardzo obszerna grupa, w której można zawrzeć wszystkie ataki hackerskie typu DDOS, flood, trojany, robaki, wirusy i inne. Sekcja ta była dwukrotnie nowelizowana, najpierw w 2006 roku przez „Police and Justice Act”, następnie zaś w roku

[8] UK Public General Acts, *Computer Misuse Act*, 1990, c. 18.

[9] L. Trevelyan, *Computer hacking and the criminal law*, www.inbrief.co.uk/offences/hacking-of-computers/ (dostęp: 12.08.2020 r.).

[10] Crown Prosecution Service, *Cybercrime – prosecution guidance.* www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (dostęp: 11.08.2020 r.).

[11] H. Graceful, *UK Cyber Crime Law*, https://gracefulsecurity.com/uk-cyber-crime-law/ (dostęp: 22.08.2020 r.).

2015 przez „Serious Crime Act", które wprowadziły dwie podsekcje, odpowiednio:

- ✓ 3A – Działania bez upoważnienia powodujące poważne szkody lub stwarzające ryzyko takich szkód – również ten zapis obejmuje bardzo szeroki zakres przestępstw związany z cyberprzestępczością, Przykładem działania, do którego ten akt się odnosi, może być wykorzystywanie ataków hackerskich do celów terrorystycznych mogących powodować uszczerbek na zdrowiu bądź utratę życia. Akt ten oddaje w ręce sędziego orzekającego wyrok całe spektrum możliwych kar, gdyż osoby oskarżone o to przestępstwo mogą zostać ukarane zarówno grzywną, jak i nawet dożywotnim pozbawieniem wolności.
- ✓ 3ZA – Wytwarzanie, dostarczanie lub pozyskiwanie artykułów do wykorzystania w przestępstwach opisywanych w sekcjach 1, 3 lub 3A – wymogiem powstania przestępstwa jest świadome działanie mające na celu popełnienie przestępstwa, artykuły wytworzone w celach technicznych bądź naukowych, wykorzystane później podczas popełniania przestępstwa nie są objęte tą sekcją. Kara z powyższe przestępstwo zależy od rejonu Wielkiej Brytanii, na którym zostanie wydany wyrok, nie przekracza jednak 2 lat pozbawienia wolności.

## System prawny a cyberprzestępczość – Stany Zjednoczone Ameryki

Stany Zjednoczone Ameryki mają jeden z najbardziej obszernych i rozwiniętych systemów prawnych w kwestii karania cyberprzestępstw. W odróżnieniu od wcześniej opisanych państw waga i odpowiedzialność karna większości przestępstw związanych z hackerstwem jest ściśle związana z oszacowanymi stratami materialnymi poniesionymi przez poszkodowanego.

Głównym dokumentem legislacyjnym w Stanach Zjednoczonych Ameryki dotyczącym cyberprzestępczości jest „Computer Fraud and Abuse Act" (CFAA)[12], obejmujący nieautoryzowany dostęp do systemu komputerowego, Początkowo akt ten odnosił się wyłącznie do własności rządowej, jednak z czasem zostały do niego dodane liczne poprawki, które rozszerzyły jego zakres na niemal wszystkie urządzenia elektroniczne znajdujące się na terenie państwa[13].

Powagę popełnionego cyberprzestępstwa oraz kary za nie grożące dzieli się na pięciostopniową skalę, gdzie przestępstwo pierwszego stopnia jest karane najsurowiej.

1. Cyberprzestępstwo pierwszego stopnia występuje, gdy poniesione szkody lub wartość uszkodzonego sprzętu wynosi ponad 10 tys. USD. Traktowane

[12] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[13] FindLaw, *Hacking Laws and Punishments*, criminal.findlaw.com/criminal-charges/hacking-laws-and-punishments.html (dostęp: 28.08.2020 r.).

jest jako przestępstwo typu B, za które grozi do 20 lat pozbawienia wolności i/lub grzywna do 15 tys. USD[14].

2. Drugi stopień dotyczy szkód szacowanych na ponad 5 tys. USD, traktowane jest jako przestępstwo typu C i grozi za nie do 10 lat pozbawienia wolności i/lub grzywna do 10 tys. USD.
3. Trzeci stopień opisuje działania powodujące szkodę na szacowaną kwotę powyżej 1000 USD lub lekkomyślne działania stwarzające ryzyko poniesienia poważnych obrażeń ciała innej osoby. Ten stopień cyberprzestępstw traktowany jest jako przestępstwo typu D, grożące pozbawieniem wolności do 5 lat i/lub grzywną o wartości 5000 USD.
4. Cyberprzestępstwa czwartego stopnia dotyczą sytuacji, w których szacowane straty wynoszą powyżej 500 USD. Ten stopień nie jest już traktowany jako przestępstwo, lecz wykroczenie typu A, za które grozi do roku pozbawienia wolności i/lub 2000 USD grzywny.
5. Ostatnim, najniższym stopniem cyberprzestępstw jest stopień piąty, którego dotyczą wszelkie sprawy, gdzie szacowana kwota strat wynosi mniej niż 500 USD. Te cyberprzestępstwa traktowane są jako wykroczenia typu C, które karane są pozbawieniem wolności do 6 miesięcy i/lub grzywną do 1000 USD.

W procesach karnych szacunkowa wartość start w sprzęcie elektronicznym bądź usługach cyfrowych obliczona jest poprzez:

- wartość rynkową,
- jeśli nie jest możliwa naprawa bądź odzyskanie, to koszt ponownego wytworzenia bądź zastąpienia,
- 250 USD, jeśli nie można w sposób zadowalający oszacować ich wartości,
- prywatne dane osobowe szacowane są na 1500 USD.

Prawo zezwala sądowi na zażądanie od osoby skazanej za przestępstwo komputerowe zapłacenia podwójnej kwoty zysku oskarżonego z tego przestępstwa, zamiast zapłacenia grzywny.

Zgodnie z zapisami CFAA cyberprzestępstwo związane z niepoprawnym wykorzystaniem komputerów jest popełniane przez osobę, gdy:

- uzyskuje dostęp do urządzenia bez autoryzacji,
- uzyskuje dostęp lub używa urządzenia w celu uruchomienia funkcji, nie posiadając autoryzacji do tego,
- lekkomyślnie lub z premedytacją zakłóca bądź powoduje awarię usług komputerowych dla autoryzowanych użytkowników,
- lekkomyślnie lub z premedytacją powoduje uszkodzenia bądź zakłócenia działania sprzętu komputerowego.

[14] E. Spitzer, *What Is a Felony? Definition, Classifications and Examples*: https://www.thoughtco.com/what-is-a-felony-4590195 (dostęp: 28.08.2020 r.).

Cyberprzestępstwem jest również niewłaściwe wykorzystanie danych komputerowych. Osoba popełnia takie przestępstwo, gdy:

- uzyskuje nieautoryzowany dostęp do systemu w celu ujawnienia bądź skopiowania danych przechowywanych, komunikowanych lub wytwarzanych przez komputer,
- lekkomyślnie lub z premedytacją i bez autoryzacji przechwytuje bądź zbiera dane przeznaczone do wykorzystania przez maszynę,
- świadomie otrzymuje lub przesyła dane uzyskane poprzez popełnienie cyberprzestępstwa,
- wykorzystuje lub udostępnia dane, o których wie lub podejrzewa, że zostały uzyskane poprzez popełnienie cyberprzestępstwa.

Osobną grupą cyberprzestępstw, z własną skalą kar, są przestępstwa popełniane przy pomocy komputera bądź sieci komputerowej:

- tymczasowe lub stałe usunięcie, zatrzymanie lub wyłączenie programów, danych bądź oprogramowania,
- spowodowanie awarii maszyny bądź systemu operacyjnego,
- zmienienie lub wymazanie programów, danych bądź oprogramowania,
- stworzenie bądź zmodyfikowanie finansowego instrumentu, bądź elektronicznego transferu pieniężnego,
- stworzenie lub spowodowanie stworzenia nieautoryzowanej kopii danych cyfrowych, programów bądź oprogramowania.

Wszystkie czynności opisane powyżej są przestępstwem pod warunkiem, że osoba je wykonująca nie posiada odpowiednich uprawnień i autoryzacji do ich wykonania. Przestępstwa te w większości traktowane są jako wykroczenia typu B (kary opisane w liście wcześniejszej) z dwoma wyjątkami, występującymi, tylko jeśli oszacowane straty wynoszą ponad 2500 USD:

1. Jeśli osoba działała lekkomyślne, lekceważąc konsekwencje swoich czynów, działanie to traktowane jest jako wykroczenie typu A.
2. Jeśli osoba działała złośliwie, działanie to traktowane jest jako przestępstwo typu D.

Ostatnim najpoważniejszym przestępstwem dokonywanym za pomocą sieci telekomunikacyjnej są działania terrorystyczne. Cyberterroryzm w USA definiowany jest jako popełnienie cyberprzestępstwa przy użyciu komputera lub sieci komputerowej z zamiarem zastraszenia bądź przymuszenia populacji cywilnej, lub jednostki rządowej. Działanie takie traktowane jest jako przestępstwo typu B i jeśli stosowane jest przeciwko agencji bezpieczeństwa publicznego, to prawo wymusza zastosowanie co najmniej 5-letniego, obowiązkowego pozbawienia wolności[15].

[15] C. Reinhart, *Penalties for computer hacking*, OLR Research Report. 2012-R-0254.

# Podsumowanie

Stany Zjednoczone Ameryki posiadają najbardziej rozbudowane prawo karne związane z przestępczością cyfrową, podzielone logicznie, zgodnie z przyjętym dogmatem powagi przestępstwa będącym szacowaną szkodą działania hackera. Podział ten pozwala tylko na niewielką elastyczność w kwestii orzekania wyroków, zapewnia jednak przejrzysty system pozwalający łatwo oszacować możliwy wymiar kary za konkretne działanie. Prawo USA podchodzi bardzo rygorystycznie do karania cyberprzestępstw, które często powodują szkody finansowe łatwo przekraczające górne granice przewidzianej skali. Tak rozbudowane i dokładne prawo może mieć historyczne korzenie w fakcie, że USA jest kolebką współczesnych technologii, a co za tym idzie, przestępstw związanych z nimi. To właśnie w Stanach Zjednoczonych Ameryki pojawiały się pierwsze głośne przypadki ataków hackerskich, przez co system prawny musiał zacząć dostosowywać prawo do nowych wyzwań znacznie wcześniej[16].

Wielka Brytania podchodzi do kwestii odpowiedzialności karnej w sposób znacznie mniej skategoryzowany, opisując niemal wszystkie cyberprzestępstwa w trzech, bardzo ogólnych sekcjach oraz pozwalając na znacznie swobodniejszy dobór kar przez sądy wydające wyrok na osobach skazanych za dane przestępstwa. Porównanie systemu prawnego w kwestii cyberprzestępczości Wielkiej Brytanii z systemem prawnym Stanów Zjednoczonych Ameryki wypada na niekorzyść Zjednoczonego Królestwa. Zastosowanie niewielu sekcji definiujących cyberprzestępstwa, obejmujących szeroki zakres możliwych szkodliwych działań, wraz z niesprecyzowanym podziałem kar, może doprowadzić do sytuacji błędnego ocenienia działań i niedostosowania kary do odpowiadającego jej czynu. W skrajnych przypadkach może doprowadzić to do zbyt srogiego ukarania czynu będącego wykroczeniem lub zbyt łagodnego potraktowania poważnego przestępstwa, gdyż oba przestępstwa znajdują się w tej samej sekcji przewidującej jeden zakres kar.

Polski kodeks karny opisuje przestępstwa związane z wykorzystaniem technologii informatycznych w sposób dokładny, dzieląc je kilka rozróżnialnych kategorii, opisywanych w różnych artykułach. Dzięki samej strukturze dokumentu udaje się uniknąć potencjalnego problemu z rozbiciem prawa na różne akty, jak to ma miejsce w pozostałych opisywanych państwach. Polski system prawny w kwestii cyberbezpieczeństwa wypada lepiej niż system Wielkiej Brytanii, dzięki znacznie większemu zróżnicowaniu opisywanych rodzajów przestępstw. Pozwala to na znacznie dokładniejsze dobranie kar do konkretnych przypadków wyroków. Jednak w porównaniu z USA, w polskim prawie nadal brakuje jednolitego i przejrzystego systemu orzekania, jak poważne jest przewinienie i jak wielką karę skazany powinien otrzymać.

---

[16] A. Grzebska, *Rozwój cyberprzestępczości w Stanach Zjednoczonych Ameryki. Kazus Kevina Mitnicka*, UJ, Kraków 2018.

Analogicznie porównanie wygląda, jeśli przyjrzeć się wielkości kar, jakie grożą za cyberprzestępczość. Najsurowsze kary stosowane są w Stanach Zjednoczonych Ameryki, potem w Polsce, najłagodniej zaś przestępstwa oceniane są w Wielkie Brytanii, z wyjątkiem sekcji 3A, która dopuszcza karę dożywotniego pozbawienia wolności.

## Bibliografia

Armstrong H.L., Forde P.J., *Internet anonymity practices in computer crime*, Information Management & Computer Security, 2003, Vol. 11, No. 5.

Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

Computer Misuse Act. UK Public General Acts 1990.

Grzebska A., *Rozwój cyberprzestępczości w Stanach Zjednoczonych Ameryki. Kazus Kevina Mitnicka*, UJ, Kraków 2018.

Prauzner T., *Prawo a bezprawie w Internecie*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Edukacja Techniczna i Informatyczna" 2009, t. 4.

Reinhart C., *Penalties for computer hacking*, OLR Research Report. 2012-R-0254.

Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawne i kryminalistyczne*, Uniwersytet w Białymstoku, Białystok 2017.

Zbrojewska, M. Mosorov, V. Biedron, S. Panskyi, T., *Jak definiujemy cyberprzestępstwo?*, „Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" 2016, t. 2.

## Prawodawstwo

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r., nr 88, poz. 553).

## Netografia

Crown Prosecution Service, *Cybercrime – prosecution guidance*, www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku*, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html

FindLaw, *Hacking Laws and Punishments*, criminal.findlaw.com/criminal-charges/hacking-laws-and-punishments.html

Graceful H., *UK Cyber Crime Law*, https://gracefulsecurity.com/uk-cyber-crime-law/

IKMJ, *Cyberbezpieczeństwo w Polsce – statystyki*, ikmj.com/cyberbezpieczenstwo-w-polsce-statystyki

INFOR Prawo, *Czym jest cyberprzestępstwo?*, www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,2,Czym-jest-cyberprzestepstwo.html

Mediarecovery, *Cyberprzestępczość – odpowiedzialność karna*, mediarecovery.pl/cyberprzestepczosc-odpowiedzialnosc-karna/

Mediarecovery. *Malware okiem prawnika – część pierwsza*, mediarecovery.pl/malware-okiem-prawnika-czesc-pierwsza/

Spitzer E., *What Is a Felony? Definition, Classifications, and Examples*, https://www.thoughtco.com/what-is-a-felony-4590195

Trevelyan L., *Computer hacking and the criminal law*, www.inbrief.co.uk/offences/hacking-of-computers/

# WYBRANE PROBLEMY BEZPIECZEŃSTWA BANKOWOŚCI TERMINALOWEJ

(*Ewa Pondel*)

## Rozwój bankowości elektronicznej i jej zagrożenia

Rynek usług bankowych ulega ciągłym i dynamicznym zmianom, wynikającym w szczególności z rozwoju nowoczesnych technologii informatycznych. Posiadanie konta bankowego, posługiwanie się na co dzień kilkoma kartami płatniczymi, korzystanie z bankomatów i terminali do akceptowania kart płatniczych, używanie komputera i smartfonu w celu realizacji coraz liczniejszej gamy usług bankowych stało się naturalne i oczywiste dla większości uczestników obrotu gospodarczego. Wyraźnie można też zauważyć, że obrót bezgotówkowy w coraz większym stopniu wypiera i zastępuje obrót gotówkowy. W niektórych krajach rozważana jest nawet całkowita rezygnacja z obrotu gotówkowego. Niekwestionowanym liderem w tej kwestii jest Szwecja, gdzie szacuje się, że już dzisiaj obrót gotówkowy sięga zaledwie kilkunastu procent ogółu transakcji. Całkowita rezygnacja z obrotu gotówkowego ma jednak zarówno zwolenników, jak i przeciwników, istnieje bowiem obawa wykluczenia niektórych grup obywateli (zwłaszcza osób starszych mających problem z płynnym korzystaniem z nowoczesnych technologii) oraz obcokrajowców (turystów, imigrantów, nieprzygotowanych na takie radykalne rozwiązania)[1]. Wydaje się jednak, że zmiany takie są nieodwracalne i będą następować, ale stopniowo wraz ze zmianami pokoleniowymi.

Mając na uwadze dynamiczną cyfryzację współczesnego społeczeństwa i postęp w rozwoju technologii informatycznych, można stwierdzić, że w dzisiejszej bankowości bankowość elektroniczna odgrywa zasadniczą rolę. Jak stwierdzają A. Janc i G. Kotliński, jest to system wykorzystujący rozwiązania informatyczne do obsługi transakcji klientów banku, zarówno osób indywidualnych, jak też wielkich podmiotów gospodarczych[2]. Jest to zatem forma usług świadczonych przez banki na rzecz klientów, polegająca na umożliwieniu dostępu do rachunku bankowego i innych usług bankowych na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak: komputer, telefon,

[1] https://www.fxmag.pl/artykul/rosnace-obawy-szwedow-wobec-obrotu-bezgotowkowego (dostęp: 12.06.2020 r.).

[2] A. Janc, G. Kotliński, *Wykorzystanie bankowości elektronicznej w rozwoju usług*, „Miesięcznik Finansowy Bank" 1999, nr 9, s. 33.

bankomat, terminal, odbiornik telewizji cyfrowej[3]. Obecnie ten rodzaj bankowości jest najprężniej rozwijającym się sektorem usług finansowych. Dominującymi formami bankowości elektronicznej stały się: bankowość internetowa, bankowość mobilna oraz bankowość terminalowa.

Bankowość internetowa oznacza dostęp do informacji i transakcji bankowych w dowolnym miejscu i w dowolnym czasie. Bankowość mobilna umożliwia komunikację klientów z bankiem za pomocą telefonu komórkowego, tabletu lub innego urządzenia przenośnego. Z kolei bankowość terminalowa polega na dokonywaniu transakcji bankowych, z wykorzystaniem urządzeń takich jak bankomaty i terminale do akceptowania kart płatniczych[4]. Podstawowym elementem bankowości terminalowej są karty płatnicze.

Bankowość terminalowa jest najstarszą i nadal bardzo powszechną formą bankowości elektronicznej. Wydaje się jednak, że wraz z rozwojem bankowości mobilnej oraz ograniczaniem obrotu gotówkowego na rzecz płatności elektronicznych jej znaczenie stopniowo będzie się zmniejszać. Podstawowym urządzeniem umożliwiającym korzystanie z usług banku w ramach bankowości terminalowej są bankomaty[5]. Urządzenia te są wyposażone w czytniki paska magnetycznego lub mikroprocesora, co umożliwia dokonywanie operacji bankowych przy użyciu kart płatniczych. Bankomaty znajdują się w miejscach publicznych, a klient banku przy ich pomocy może samodzielnie dokonywać określonych operacji. Najprostsze bankomaty umożliwiają jedynie operacje wypłaty gotówki, bardziej zaawansowane umożliwiają również sprawdzenie stanu konta, dokonanie wpłaty gotówki, a nawet zrobienie przelewu. Te pierwsze działają na ogół jedynie w trybie offline, te drugie wykorzystują połączenia online i łączą się z bankiem bezpośrednio, dając możliwość natychmiastowej autoryzacji transakcji[6].

Jedną z nowszych technologii stosowanych w bankowości terminalowej jest biometria, czyli skanowanie układu krwionośnego palca w bankomatach[7]. Inną formą bankowości terminalowej są elektroniczne punkty sprzedaży, tzw. POS (*Point of Sale*). Dają one możliwość dokonania transakcji zakupu w punktach handlowych, korzystających z elektronicznych czytników kart płatniczych. Urządzenia te nie są jednak samodzielnymi kanałami bankowości terminalowej, służą jedynie

---

[3] M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, Komisja Nadzoru Bankowego, Warszawa 2014, https://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf (dostęp: 9.06.2019 r.).

[4] A. Nowacka, M. Szewczyk-Jarocka, *Bezpieczeństwo usług bankowości elektronicznej w opinii klientów banków spółdzielczych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 307, s. 61–63.

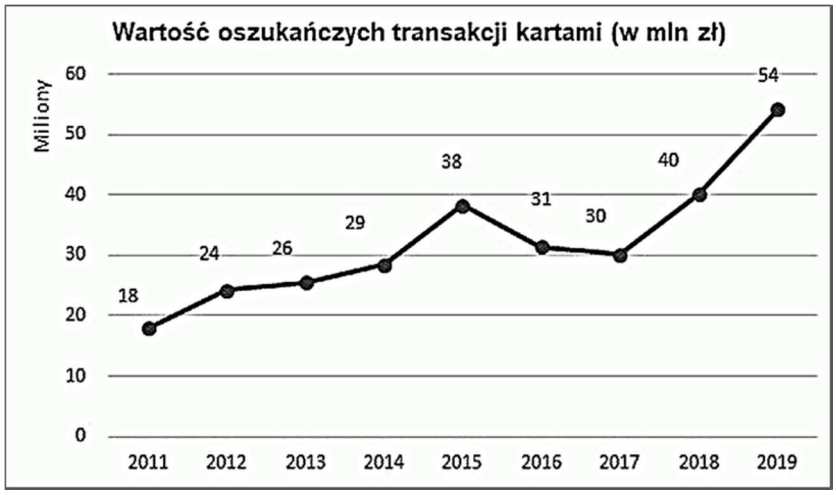
[5] M. Krzysztoszek, *Bankowość elektroniczna w teorii i praktyce*, Komisja Nadzoru Bankowego, Warszawa 2017, s. 6–7.

[6] Szerzej na temat budowy i działania bankomatu zob. P. Opitek, *Skimming. Aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Wydawnictwo C.H. Beck, Warszawa 2017, s. 49 i n.

[7] https://www.automatykabankowa.pl/biometria-w-bankomatach-coraz-bardziej-popularna-na-swiecie-ale-2/ (dostęp: 12.06.2020 r.).

do autoryzacji płatności dokonywanej przez klienta (sprawdzenie dostępności środków na rachunku bankowym klienta)[8].

Bankowość terminalowa, wykorzystująca komunikację za pośrednictwem sieci informatycznych, nie jest wolna od zagrożenia przestępczością, nazywaną powszechnie cyberprzestępczością. Cyberprzestępczość to zbiorcza nazwa przestępczości wykorzystującej nowoczesne technologie informatyczne do ataku na wszelkie dobra chronione prawem[9]. Wraz z rozwojem sieci bankomatów zaczęło dochodzić do ataków na te urządzenia, co wynika z faktu, że w ich szufladach potencjalnie mogą znajdować się znaczne kwoty gotówki. Przestępcy podejmują najróżniejsze próby zagarnięcia pieniędzy z bankomatu. P. Opitek wskazuje, że tego rodzaju przestępczość przybiera dwie zasadnicze postaci: oszustw bankomatowych, mających na celu obejście zabezpieczeń poprzez dokonanie pewnych manipulacji w systemie urządzenia oraz mechanicznych ataków na bankomaty poprzez kradzieże, włamania bądź napaści na osoby obsługujące bankomaty[10]. Korzyści z popełnienia takich przestępstw są niewspółmiernie wysokie, zwłaszcza w stosunku do nakładów poniesionych na ich przygotowanie i dokonanie. Jedną z najpopularniejszych a zarazem najbardziej rozpowszechnionych form przestępczości skierowanej przeciwko bankomatom jest skimming.




Rys. 1. Wartość oszukańczych transakcji kartami w latach 2011–2019

Źródło: https://alebank.pl/kieszonkowcy-i-oszusci-niestety-tez-czekaja-na-turystow/

[8] M. Polasik, *Bankowość elektroniczna istota – stan – perspektywy*, CeDeWu, Warszawa 2012, s. 21.

[9] I. Oleksiewicz, M. Pomykała, *Problemy dostosowania prawa polskiego do prawa międzynarodowego i unijnego w zakresie zwalczania cyberprzestępczości* [w:] *Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy prawno-kryminologiczne*, red. E.W. Pływaczewski, W. Filipkowski, Z. Rau, Wolters Kluwer Business, Warszawa 2015, s. 856.

[10] P. Opitek, *Skimming. Aspekty*…, s. 52.

Warto podkreślić, że według danych NBP wartość transakcji przy użyciu fałszywych kart płatniczych z roku na rok niepokojąco wzrasta. Podczas gdy w roku 2011 było to 18 mln zł, to w 2019 r jest to już 54 mln zł (rys. 1).

## Skimming

Etymologia pojęcia „skimming" została zaczerpnięta z języka angielskiego. Czasownik *skim* znaczy *musnąć* (zbierać z powierzchni)[11]. Należy zaznaczyć, że w obowiązujących przepisach prawa nie występuje legalna definicja skimmingu. Warto jednak sięgnąć w tym zakresie do literatury przedmiotu; zjawisko to było bowiem wielokrotnie analizowane. K. Mikołajczyk określa skimming jako bezprawne skopiowanie informacji z paska magnetycznego umieszczonego na karcie płatniczej oraz przechwycenie przypisanego jej kodu PIN, bez wiedzy i woli użytkownika karty w celu wykonania duplikatu służącego do obciążenia rachunku bankowego posiadacza[12]. R. Janowicz twierdzi, że skimming to nielegalna operacja polegająca na skopiowaniu zawartości paska podczas transakcji dokonywanej przez prawowitego posiadacza karty[13]. J. Wójcik podaje, że skimming polega na przechwyceniu kodu PIN oraz danych z paska magnetycznego karty w celu wykonania jej duplikatu, który służyć będzie do wypłaty pieniędzy z cudzego rachunku bankowego[14]. Należy zauważyć, że wszystkie transakcje dokonane przy użyciu kopii kart obciążają prawowitego posiadacza karty, niejednokrotnie przy jego nieświadomości.

W szerokim ujęciu skimming to nie tylko skopiowanie paska magnetycznego karty każdą z dostępnych metod i przechwycenie PIN-u, ale również przetwarzanie tych informacji, a następnie ich wykorzystanie do operacji za pomocą karty-klonu lub w środowisku CNP (ang. *card not present*), tj. bez fizycznego użycia karty, np. do transakcji w sieci lub transakcji typu MOTO (ang. *Mail Order, Telephone Order*)[15]. Skradzione dane kartowe mogą zostać ponadto wystawione na sprzedaż na specjalnych stronach internetowych stanowiących cybernetyczny czarny rynek.

Skimming, jako przestępcze wykorzystanie skopiowanych kart, należy do najgroźniejszych przestępstw związanych z bankowością elektroniczną. Proceder ten jest dość szybki i prosty, nie wymaga podejmowania skomplikowanych metod działania. Przy pomocy urządzeń, które stosunkowo łatwo można zakupić za pośrednictwem Internetu, można skopiować całą zawartość paska magnetycznego

---

[11] https://dictionary.cambridge.org, skim/ Cambridge – Cambridge University Press (dostęp: 12.06.2020 r.).

[12] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 104.

[13] R. Janowicz, R. Klepacz, *Pieniądz elektroniczny na świecie, istota i zastosowanie elektronicznej portmonetki*, Warszawa 2002, s. 135; J. Kosiński, *Paradygmat cyberprzestępczości*, Warszawa 2015, s. 159.

[14] J. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008, s. 375.

[15] P. Opitek, *Skimming. Aspekty…*, s. 64.

karty i zapisać ją na innej karcie-klonie. Dane kart są bowiem zapisywane na paskach magnetycznych bez żadnego szyfrowania. Skopiowanie karty jest łatwe i zajmuje zaledwie kilka sekund.

Uwzględniając sposób postępowania sprawców oraz miejsce, gdzie dochodzi do popełnienia czynu zabronionego, można rozróżnić dwa rodzaje skimmingu:

- skimming bankomatowy (podstawowy),
- skimming w punktach handlowo-usługowych.

Szczególnie groźną odmianą skimmingu jest skimming bankomatowy. W tym celu przestępcy instalują w bankomatach specjalistyczne urządzenia służące do pozyskiwania danych z paska magnetycznego kart oraz kodów PIN. Urządzenia takie mogą być montowane zarówno na bankomatach, jak i w ich wnętrzu. K. Mikołajczyk określa takie nielegalnie zamontowane urządzenie skanujące kartę płatniczą mianem *skimmera*[16]. Opisując działanie skimmera, należy stwierdzić, że jest to urządzenie będące specjalnie przygotowaną nakładką bankomatową, umożliwiającą pobieranie informacji przez przestępców z pasków magnetycznych zapisanych na karcie płatniczej. Nakładce może towarzyszyć dodatkowa klawiatura, nałożona na właściwą klawiaturę bankomatu, zapisująca wpisywane numery PIN lub kamera śledząca palce na klawiaturze[17]. Zrejestrowane informacje są najczęściej transmitowane drogą radiową i służą do produkcji fałszywych kart, z pomocą których możliwe jest pobieranie gotówki z kont klientów banków za pośrednictwem bankomatów.

Rys. 2. Kopiowanie zawartości paska magnetycznego za pomocą urządzeń zainstalowanych na bankomacie –skimming bankomatowy

Źródło: https://www.policja.pl/pol/aktualnosci/11364,dok.html (dostęp: 12.08.2020 r.).

[16] K. Mikołajczyk, *Przestępstwa związane z wykorzystaniem…*, s. 108.

[17] P. Konieczny, *Bankomat i video z instalacji skimmera*, Niebezpiecznik.pl.2010-05-09 (dostęp: 02.02.2018 r.).

Natomiast skimming w punktach usługowych polega na tym, że karty są kopiowane podczas dokonywania transakcji nimi, czyli w sklepach, restauracjach, klubach, na stacjach paliwowych oraz we wszelkich innych miejscach. Nieuczciwy sprzedawca, dysponując odpowiednim urządzeniem, może skopiować pasek karty na zapleczu, pod ladą sklepową, a nawet na oczach nieświadomego niczego klienta.


Rys. 3. Kopiowanie zawartości paska magnetycznego za pomocą urządzeń naręcznych – skimming w punktach handlowo usługowych

Źródło: https://www.policja.pl/pol/aktualnosci/11364,dok.html (dostęp: 12.08.2020 r.).

Obecny postęp technologiczny pozwala na tworzenie skanerów bardzo małych rozmiarów, zwłaszcza takich, które w całości mieszczą się w dłoni, czy w kieszeni i są niewidoczne dla potencjalnej ofiary[18]. Takie urządzenia mogą służyć do skanowania karty nawet na oczach nieświadomego jej posiadacza – przyszłej ofiary. Należy stwierdzić z pełnym przekonaniem, że niezależnie od typu bankomatów czy terminali oraz zabezpieczeń na nich stosowanych, przestępcy są w stanie przystosować wszystkie te urządzenia do swoich potrzeb.

## Cash trapping

Inną, równie niebezpieczną metodą okradania użytkowników kart płatniczych jest Cash trapping. Określenie pochodzi od angielskich słów: *cash* – gotówka, *trap* – pułapka, co w dosłownym tłumaczeniu na język polski oznacza „pułapka na pieniądze".

Cash trapping nie jest nową metodą działania przestępczego. W Europie metoda ta pojawiła się już przed kilkoma laty, ale w Polsce stosowana jest od niedawna. Cash trapping polega na tym, że przestępca instaluje we wnętrzu bankomatu specjalną listwę klejową, która blokuje możliwość wydostania się banknotów

[18] www.policja.pl>aktualności (dostęp:12.06.2020 r.).

z bankomatu, przy czym ma to miejsce podczas prawidłowo przeprowadzonej transakcji[19]. Pieniądze po prostu przyklejają się do specjalnie skonstruowanego urządzenia pokrytego klejem i pozostają w bankomacie. W praktyce wygląda to w ten sposób, że osoba zainteresowana wybraniem swoich środków pieniężnych, udaje się do bankomatu, wpisuje PIN i wysokość żądanej kwoty, poprawnie autoryzując w ten sposób transakcję, i oczekuje na zleconą wypłatę. Niestety, w wyniku działania przestępczego pieniądze nie wydostają się z bankomatu, lecz przyklejają się do zamontowanej przez oszustów listwy klejowej i zostają zatrzymane wewnątrz. Nieświadomy klient banku oddala się od bankomatu w przekonaniu, że doszło do awarii sytemu bankowego, bankomat się zepsuł i odchodzi. Złodziej natomiast oczekuje w oddali na ruch klienta, podchodzi do bankomatu i odbiera bez trudu skradzione pieniądze.

Proceder ten zbiera żniwo w galopującym tempie w Europie, szczególnie narażone są bankomaty w Wielkiej Brytanii[20]. W tym miejscu należałoby zadać pytanie, czy polskie bankomaty mają problem z metodą cash trapping i jak wielka jest skala tego zjawiska? Z pełną stanowczością należy stwierdzić, że tak. Wnioskowanie to wynika ze zwielokrotnienia ostrzeżeń, jakie wysyłają banki polskie do swoich klientów, o konieczności zachowania czujności i ostrożności przy bankomatach w trakcie wypłat.

Udowodnienie cash traapingu sprawia ogromne trudności, ponieważ według banku transakcja przebiegła prawidłowo. Dobrym sposobem zapewnienia ochrony przed tym procederem może być monitoring wizyjny zainstalowany w pobliżu bankomatu. Istnieją też mechanizmy, które utrudniają sam atak, ale wymagają one interwencji serwisu i sprzętowej aktualizacji. Mając wątpliwość co do bezpieczeństwa danego bankomatu, zwłaszcza widząc niepokojące wypukłości czy uszkodzenia, warto zrezygnować z przeprowadzenia transakcji i udać się w inne miejsce. Należy, niestety, wziąć pod uwagę, że przestępcy wymyślają kolejne coraz nowsze sposoby i metody kradzieży pieniędzy z bankomatów. Wraz z uszczelnianiem zabezpieczeń stosowanych przez banki pojawiają się nowsze i oryginalniejsze pomysły na kradzież.

## Jackpotting

Jackpotting to jeszcze jeden sposób na kradzież pieniędzy z bankomatu. Polega na opróżnieniu wszystkich kaset z gotówką bez konieczności posiadania jakiejkolwiek karty płatniczej. Nazwa „jackpotting" została zapożyczona od maszyn hazardowych, które „wyrzucają" gotówkę po wygranej.

Atak jackpotting przeprowadzany jest poprzez włamanie się do oprogramowania bankowego w bankomacie, celem zainstalowania oprogramowania

[19] https://cashless.pl.>cashlesspedia (dostęp: 10.09.2019 r.).
[20] https:// association – ecure-transactions. eu EAST/European Payment Terminal Crime Raport (dostęp: 10.09.2019 r.).

kontrolującego urządzenie. Sama metoda jest dość prosta w realizacji. Polega na tym, że oszust podszywając się pod pracownika banku, podłącza się do bankomatu za pomocą laptopa albo nawet smartfona, wgrywa odpowiednie oprogramowanie i przejmuje kontrolę nad bankomatem. Następnie zdalnie uruchamia wypłatę gotówki, którą w późniejszym czasie podejmuje inna osoba. Do oodebrania gotówki angażawane są tzw. słupy; często zostają nimi osoby nisko wykwalifikowane, których rola sprowadza się właśnie do odebrania pieniędzy i przelania ich na wskazane konto.

Jackpotting jest stosunkowo prostym sposobem kradzieży pieniędzy, wykorzystującym luki w zabezpieczeniach. Do kradzieży pieniędzy z bankomatu wystarczy człowiek przebrany za pracownika technicznego banku, który nie wzbudza podejrzeń osób postronych, pobiera gotowkę i przelewa ją na inne konto[21]

## Działania banków mające na celu zapewnienie bezpieczeństwa bankowości terminalowej

Nieodłącznym problemem, z jakim stykają się banki wobec przestępczości skierowanej przeciwko bankowości elektronicznej, w tym również bankowości terminalowej, jest zapewnienie właściwego poziomu bezpieczeństwa i konieczność utrzymania zaufania klienta. Problem bezpieczeństwa pozostaje aktualny niezależnie od rodzaju usług świadczonych przez bank. Zapewnienie bezpieczeństwa w przypadku korzystania z nowoczesnej bankowości oznacza nie tylko kwestie sprzętowe i technologiczne, ale również działania logistyczne oraz zagwarantowanie właściwych rozwiązań prawnych.

Nie można wprost wskazać sposobów, których stosowanie zagwarantuje stuprocentowe bezpieczeństwo bankowych usług elektronicznych. Jak wskazuje J. Grzywacz, najważniejszą kwestią w przypadku bankowości internetowej jest zaimplementowanie przez bank następujących funkcjonalności: natychmiastowego potwierdzenia tożsamości osób realizujących transakcję, stosowania skutecznego systemu szyfrowania transmisji informacji i zapewnienie jej całkowitej poufności, odpowiedniego zabezpieczenia serwera instytucji będącej dostawcą internetowych usług finansowych przed nielegalnym dostępem, zabezpieczenia serwera przed celowymi atakami przeprowadzonymi zarówno z zewnątrz (Internetu), jak i od środka (sieć lokalna)[22].

Obecnie banki stosują szereg zabezpieczeń mających zagwarantować bezpieczeństwo transakcji elektronicznych. Bezpieczeństwo kanału internetowego zapewnia szyfrowana transmisja danych za pomocą protokołu SSL. Wcześniej proste uwierzytelnianie oparte było na tokenie, dziś jednak stopniowo następuje likwi-

[21] https://www.securelist.pl (dostęp: 22.06.2020 r.).

[22] J. Grzywacz, *Bankowość elektroniczna w przedsiębiorstwie*, Oficyna Wydawnicza SGH, Warszawa 2016, s. 119.

dacja tej usługi. Zastępują ją certyfikaty użytkownika, klucze kryptograficzne, karty haseł, karty magnetyczne (urządzenia elektroniczne lub mechanizmy cyfrowe), podpis elektroniczny (cyfrowy). Często również stosowane są dodatkowe metody zwiększające bezpieczeństwo, tzw. zapory ogniowe, czyli *firewalle*. Ich zadaniem jest ochrona systemu przed bezpośrednimi atakami hakerów, poprzez uniemożliwienie niedozwolonego sposobu komunikacji z serwerem z innych portów TCP/IP. Oprócz tego system rejestruje wszelkie czynności użytkownika oraz inne przeprowadzone operacje systemowe (np. próby logowania do systemu, odczyt historii konta, wykonywanie przelewu). Zapisywane dane obejmują również adres IP użytkownika. W przypadku trzykrotnego (najczęstsza opcja) podania złych danych autoryzacyjnych następuje automatyczna blokada konta. Natomiast przy braku aktywności użytkownika przez określony czas (zwykle kilka minut) inicjowane jest automatycznie zakończenie sesji i następuje wylogowanie[23].

Oprócz rozwiązań stosowanych w przypadku wszystkich transakcji w bankowości elektronicznej, warto zwrócić uwagę na zabezpieczenia wykorzystywane wyłącznie w bankowości terminalowej i montowane w nowoczesnych bankomatach. Ciekawym rozwiązaniem jest wykorzystanie technologii biometrycznych. Technologie biometryczne używane przez banki to przykładowo: skan tęczówki oka, geometria twarzy, geometria dłoni, odcisk palca oraz rejestracja głosu[24]. Bankomaty biometryczne wykorzystują autoryzację biometryczną przy realizacji transakcji bankomatowej. Danych biometrycznych nie można skopiować ani podejrzeć, a przez to wyeliminowane zostaje ryzyko przestępczego wykorzystania kart bankowych, jak ma to miejsce w przypadku skimmingu. Jednocześnie zastosowanie biometrii usprawnia też sam proces autoryzacji i zwiększa komfort korzystania z bankomatu. Nie jest konieczne podawanie numeru PIN, mniejsze jest ryzyko zatrzymania i zablokowania karty w razie jego pomyłki[25].

Innym rozwiązaniem, będącym odpowiedzią na dość wysokie ryzyko skimmingu w klasycznych bankomatach, jest zmiana w budowie bankomatu, polegająca na zastosowaniu dużych ekranów z dotykowym panelem oraz płaskiej obudowy. Taka konstrukcja panelu frontowego utrudnia przestępcom instalację kamer czy nakładek na czytniki. Powszechne staje się także montowanie coraz większej ilości kamer w okolicy bankomatu. Instalowane są kamery, które robią zdjęcia podczas zakładania kont, monitorują obszar za osobą korzystającą z bankomatu, osobne kamery znajdują się też na podajniku banknotów. Te pierwsze monitorują, czy w trakcie transakcji ktoś nie przychwytuje danych klienta, te ostatnie natomiast służą do zweryfikowania, czy klient rzeczywiście odebrał gotówkę[26].

---

[23] www.policja.pl >aktualności (dostęp: 12.06.2020 r.).

[24] A. Jasiński, *Bank jako ośrodek nowoczesnych technologii. Ewolucja bankowych technik zabezpieczeniowych i ich wpływ na architekturę współczesnych banków*, „Czasopismo Techniczne. Architektura" z. 4-A/2007, s. 81

[25] R. Lewandowski, *Biometria – nowe zastosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 152 i n.

[26] https://www.automatykabankowa.pl/jak-bedzie-wygladal-bankomat-przyszlosci/ (dostęp: 12.06. 2020 r.).

Jednym z nowszych rozwiązań stosowanych między innymi w bankomatach jest technologia NFC (*Near Field Communication*). Jest to bezdotykowa i bezprzewodowa technologia komunikacyjna, która wykorzystuje fale radiowe w celu udostępniania cyfrowych informacji i wysyłania ich na odległość do 20 centymetrów[27]. Opiera się ona na systemie Android 2.3 i dostępna jest w większości nowszych smartfonów. Zastosowanie jej w bankomatach powoduje, że stają się one kompatybilne ze smartfonami, co umożliwia realizację transakcji bankomatowych bez użycia jakiejkolwiek karty, a z wykorzystaniem smartfonu do autoryzacji. W praktyce telefon wyposażony w NFC współpracuje z odpowiednimi aplikacjami bankowymi, jego zbliżenie do bankomatu, wyposażonego również w NFC, powoduje nawiązanie transmisji i błyskawiczne przekazanie danych, telefon pełni tutaj funkcję karty płatniczej. Przy pomocy telefonu wyposażonego w NFC mogą być dokonywane również wszelkie inne płatności, wszędzie tam gdzie mają zastosowanie karty płatnicze (np. w terminalach POS)[28]. Warto podkreślić, że użycie telefonu w miejsce karty płatniczej stanowi ograniczenie groźby skimmingu.

Bardzo wygodną usługą udostępnianą przez banki dla posiadaczy kont bankowych są również płatności BLIK-iem. Usługa ta wykorzystywana jest w Polsce od 2015 r. Jest to forma płatności wykorzystująca odpowiednią aplikację mobilną. Posiadacz konta bankowego musi zainstalować na swoim smartfonie aplikację mobilną danego banku, za pomocą której będzie mógł realizować płatności w punktach handlowych stacjonarnych i internetowych, wypłaty z bankomatów, będzie także mógł przesyłać pieniądze innym osobom. Przelew środków pieniężnych następuje we wszystkich tych przypadkach bez użycia karty płatniczej. Do wykonania przelewu konieczne jest jedynie wygenerowanie 6-cyfrowego kodu BLIK i potwierdzenie nim wykonania transakcji w aplikacji mobilnej w telefonie. Ważność kodu trwa około 2 minuty, a każdy kod służy do zaakceptowania tylko jednej transakcji. Zapewnia to stosunkowo duże bezpieczeństwo transakcji. Eliminowana jest dzięki temu możliwość podejrzenia stosowanego kodu czy zeskanowania danych osobowych[29].

## Prewencja kryminalna w zakresie bankowości terminalowej

Bardzo istotną rzeczą, zwiększającą bezpieczeństwo użytkowników usług bankowości terminalowej oraz zmniejszającą ryzyko nieuprawnionego zagarnięcia środków płatniczych z konta bankowego przy wykorzystaniu bankomatu, jest zachowanie określonych, a nierzadko po prostu elementarnych, zasad postępowania przy korzystaniu z bankomatu.

---

[27] https://pl.wikipedia.org/wiki/Komunikacja_bliskiego_zasi%C4%99gu (dostęp: 12.06.2020 r.).

[28] M. Polasik, *Perspektywy rozwoju mobilnych płatności NFC na rynku polskim*, Annales Universitatis Mariae Curie-Skłodowska. Sectio H, Vol. XLVIII/2014, s. 197 i n.

[29] J. Wolna, *Rozwój systemów płatności mobilnych w Polsce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 239, s. 168–169.

W przypadku transakcji dokonywanych za pomocą terminali naręcznych, powszechnie stosowanych w hipermarketach, w restauracjach, czy na stacjach benzynowych, najprostszym sposobem ochrony przed działaniem przestępczym jest stałe monitorowanie swojej karty podczas przeprowadzania transakcji z jej użyciem. W przypadku płatności kartą płatniczą nie należy, a nawet nie wolno, tracić jej z oczu. Obowiązkiem realizującego transakcję (akceptanta) w przypadku, gdy nie posiada terminalu przenośnego, jest poinformowanie posiadacza, aby ten udał się do miejsca, gdzie znajduje się terminal stacjonarny, w celu autoryzacji płatności. Niedopuszczalnym zachowaniem akceptanta jest natomiast oddalenie się z kartą w miejsce niewidoczne dla klienta. Jeśli jednak taka sytuacja jest niezbędna (np. z uwagi na brak zasilania w miejscu transakcji), wówczas użytkownik karty ma prawo udać się do miejsca, gdzie akceptant będzie realizował transakcję. Można nawet stwierdzić, że takie postępowanie to wyraz odpowiedzialności za własne bezpieczeństwo. Bezwzględnie natomiast należy unikać sytuacji, gdy transakcja z użyciem karty odbywa się w miejscu niewidocznym dla użytkownika, np. na zapleczu restauracji, sklepu itp.

Na coraz większe bezpieczeństwo transakcji bankomatowych duży wpływ ma również coraz powszechniejsze stosowanie profesjonalnych zabezpieczeń antyskimmingowych. Warto podkreślić, że w ostatnich latach znacznie zmniejszyła się liczba ujawnionych przypadków skimmingu. Badania przeprowadzone przez firmę RBR wykazały że już ponad 40% bankomatów w Europie jest wyposażona w rozwiązania antyskimmingowe. Zabezpieczenia te są bardziej popularne w Europie Środkowej i Wschodniej niż w Zachodniej. Rozwiązania antyskimmingowe są stosowane w 58% urządzeń w Europie Środkowej i Wschodniej, podczas gdy w Europie Zachodniej zawiera je tylko 32% urządzeń[30].

Jak wynika z badań przeprowadzonych przez ekspertów z Kaspersky Lab, w użyciu nadal pozostaje wiele bankomatów z przestarzałym i niezabezpieczonym oprogramowaniem. Stąd zatem błędy w konfiguracji sieci oraz brak fizycznego zabezpieczenia krytycznych części bankomatu[31]. Analizując problem bezpieczeństwa bankowości terminalowej, należy więc zadać pytanie, jak przeciwdziałać atakom na bankomaty? Wyniki badań pokazują, że chociaż producenci próbują opracowywać coraz lepiej zabezpieczone bankomaty, to wiele urządzeń jest przestarzałych i słabo chronionych. Oszuści bardzo szybko to dostrzegają i wykorzystują takie luki w zabezpieczeniach bankomatów. Olga Koczetowa uważa, że bezpośrednie ataki na takie urządzenia znacznie skracają drogę do rzeczywistych pieniędzy[32].

Niezwykle ważna jest także czujność i obserwacja urządzenia podczas dokonywania transakcji. Współczesne społeczeństwo jest już dostatecznie świadome zagrożeń związanych z użytkowaniem kart płatniczych i przy zachowaniu minimum ostrożności korzystający z bankomatu jest w stanie zauważyć dodatkowe

[30] http://wwwautomatykabankowa.pl (dostęp: 23.06.2020 r.).
[31] http://r.kaspersky.pl/qtsqK (dostęp: 20.06.2020 r.).
[32] http://www.kaspersky.pl/nowosci (dostęp: 20.06.2020 r.).

urządzenie dołączone do bankomatu lub widoczną modyfikację terminala „POS" (w postaci dodatkowego czytnika, zewnętrznej karty pamięci itp.). W przypadku zaistnienia jakiegoś problemu przy bankomacie nie należy podejmować żadnej operacji finansowej, warto natomiast powiadomić bank oraz Policję.

Zawsze też warto na bieżąco sprawdzać saldo swojego rachunku bankowego. Dzięki takiemu zabiegowi, gdy karta zostanie skopiowana i użyta, zaalarmuje użytkownika już pierwsza transakcja dokonana przez osoby trzecie.

## Podsumowanie

Metody i sposoby działania przy realizacji przestępstw bankomatowych bardzo szybko ewoluują, dostosowując się zarówno do technicznych możliwości będących w dyspozycji grup, jak i okazji osiągnięcia tą drogą maksymalnych zysków. Omawiana działalność ma często zasięg międzynarodowy, począwszy od niezgodnego z prawem wykorzystania elektronicznych instrumentów płatniczych, kończąc na przypadkach używania narzędzi cyfrowych do obrotu towarami niebezpiecznymi, środkami odurzającymi, bronią i materiałami wybuchowymi.

Postęp technologiczny sprzyja nie tylko klientom banków i posiadaczom kart płatniczych, przynosząc coraz to nowe sposoby zabezpieczeń. Nowinki technologiczne wykorzystują również przestępcy, nieustannie modyfikując i dostosowując swoje środki działania i narzędzia. Fakt, że urządzenia oraz umiejętności potrzebne do uprawiania tego procederu są coraz bardziej dostępne i łatwiejsze do zdobycia, sprawia, że korzyści z popełniania przestępstw na szkodę systemów kart płatniczych są niewspółmiernie większe od nakładów poniesionych na przygotowanie i dokonanie tych przestępstw. Niestety, należy również podkreślić relatywnie niskie zagrożenie ewentualną karą. Dlatego też nawet duże zorganizowane grupy przestępcze, dostrzegając w tego typu przestępstwach więcej korzyści, modyfikują, a nieraz wręcz przestawiają profil swojej działalności, np. prania brudnych pieniędzy czy też handlu bronią i narkotykami, na fałszowanie kart płatniczych czy okradanie klientów banków.

Na skuteczność zapewnienia bezpieczeństwa bankowości terminalowej ogromny wpływ mają działania takich instytucji jak organy ścigania, w tym wyspecjalizowane komórki do zwalczania cyberprzestępczości, banki, producenci urządzeń bankomatowych. Szczególnie ważna jest wymiana informacji, wzajemna współpraca oraz działalność edukacyjna uczestników obrotu kartami głównie akceptantów i posiadaczy kart płatniczych.

Z punktu widzenia skuteczności zwalczania skimmingu korzystniejsze będzie przeciwdziałanie temu zjawisku, tzw. polityka prewencyjna niż usuwanie jej skutków.

Warto również zauważyć, że zarówno problemy bezpieczeństwa bankowości terminalowej, jak i stabilność ekonomiczna, społeczna państwa są bardzo skomplikowaną materią, a wyznaczone instytucje publiczne, odpowiedzialne za ich

sprawne funkcjonowanie, nie zawsze nadążają za szybkim postępem technologicznym w tym obszarze.

# Bibliografia


Górnisiewicz M., Obczyński R., Pstruś M., *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, Komisja Nadzoru Bankowego, Warszawa 2014.

Grzywacz J.., *Bankowość elektroniczna w przedsiębiorstwie*, Oficyna Wydawnicza SGH, Warszawa 2016.

Janc A., Kotliński G., *Wykorzystanie bankowości elektronicznej w rozwoju usług*, „Miesięcznik Finansowy Bank" 1999, nr 9.

Janowicz R., Klepacz R., *Pieniądz elektroniczny na świecie, istota i zastosowanie elektronicznej portmonetki*, Warszawa 2002.

Jasiński A., *Bank jako ośrodek nowoczesnych technologii. Ewolucja bankowych technik zabezpieczeniowych i ich wpływ na architekturę współczesnych banków*, „Czasopismo Techniczne. Architektura" z. 4-A/2007.

Konieczny P., *Bankomat i video z instalacji skimmera*, Niebezpiecznik.pl.2010-05-09.

Kosiński J., *Paradygmat cyberprzestępczości*, Warszawa 2015.

Krzysztoszek M., *Bankowość elektroniczna w teorii i praktyce*, Komisja Nadzoru Bankowego, Warszawa 2017.

Lewandowski R., *Biometria – nowe zastosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17.

Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej – skimming*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10.

Nowacka A., Szewczyk-Jarocka M., *Bezpieczeństwo usług bankowości elektronicznej w opinii klientów banków spółdzielczych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 307.

Oleksiewicz I., Pomykała M., *Problemy dostosowania prawa polskiego do prawa międzynarodowego i unijnego w zakresie zwalczania cyberprzestępczości* [w:] *Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy prawno-kryminologiczne*, red. E.W. Pływaczewski, W. Filipkowski, Z. Rau, Wolters Kluwer Business, Warszawa 2015.

Opitek P., *Skimming. Aspekty kryminalistyczne. Cyberprzestępczość w bankowości elektronicznej*, Wydawnictwo C.H.Beck, Warszawa 2017.

Polasik M., *Bankowość elektroniczna istota – stan – perspektywy*, CeDeWu, Warszawa 2012.

Polasik M., *Perspektywy rozwoju mobilnych płatności NFC na rynku polskim*, Annales Universitatis Mariae Curie-Skłodowska. Sectio H, vol. XLVIII/2014.

Wolna J., *Rozwój systemów płatności mobilnych w Polsce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 239.

Wójcik J., *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008.

# WYŁUDZENIA DOKONYWANE ZA POŚREDNICTWEM PORTALI SPOŁECZNOŚCIOWYCH JAKO ZAGROŻENIE BEZPIECZEŃSTWA W SIECI

(*Paweł Michalak*)

## Wprowadzenie

Powstanie portali społecznościowych było przełomem w rozwoju komunikacji społeczeństwa, dało to wiele korzyści oraz szeroki zakres możliwości. Wraz z atutami portali zaczęły pojawiać się ich negatywne strony. Liczba zagrożeń istniejących w *social media* sprawiła, że podzielono je na wiele rodzajów, a te zaś na osobne gałęzie. Społeczeństwo komunikujące się w Internecie nie zdaje sobie często sprawy, na jak wiele zagrożeń jest narażonych. Niekiedy wynika to z niewiedzy w zakresie bezpiecznego korzystania z sieci, ale również ze słabego poziomu zabezpieczeń swoich dóbr zamieszczonych na portalach społecznościowych.

Jedną z grup osób tworzących zagrożenia są oszuści internetowi. Osoby wykorzystujące *social media* do oszustw istnieją od czasu powstania portali. Odkryto bowiem, że ogromna liczba osób w jednym miejscu staje się idealnym polem do działania, jednak muszą się wykazywać coraz większą kreatywnością, perfekcją i sposobami na nielegalnym pozyskiwaniu dóbr.

W rozdziale omówiono jeden z rodzajów zagrożeń w sieci, mianowicie wyłudzeń dokonywanych za pośrednictwem portali społecznościowych oraz konsekwencji dla oszustów internetowych egzekwowanych przez polskie prawo. Opisane zostały metody wyłudzeń, które dokonywane są najczęściej oraz przeanalizowane artykuły z aktów prawnych, mające zapewnić bezpieczeństwo obywatelom oraz działać prewencyjnie.

## Oszustwa dokonywane na portalach społecznościowych

### Wstępny zarys teoretyczny

Na początku należy skupić się na pojęciu wyłudzenia internetowego oraz na działaniach podejmowanych przez oszustów. Zjawisko to nazywane jest *phishingiem*. By dokonać efektywnego wyzyskania poufnych danych osób korzystających z portali społecznościowych należy stosować praktyki socjotechniczne (ang.

*Social engineering*). Użytkownicy ulegają szkodliwemu działaniu wyspecjalizowanych programów i algorytmów funkcjonujących bez wiedzy właściciela konta. Przejęcie profilu bądź skopiowanie danych może doprowadzić do realnego zagrożenia zaczynając od niszczenia dobrej opinii użytkownika, kończąc na całkowitym przejęciu profilu w celach marketingowych (kasowanie danych użytkownika i tworzenie reklam dla znajomych poszkodowanego) lub dodawaniu materiałów kompromitujących go. W sytuacji przejęcia konta, dosyć nieprzyjemną może być sytuacja, gdzie wypływają obraźliwe treści, szantaż innych osób czy znęcanie się[1]. Czyny te są prawnie zabronione i opisane w art. 190a § 2 kodeksu karnego, grożą za nie kary pozbawienia wolności od 6 miesięcy do 8 lat dla osoby podszywającej się pod wizerunek osoby poszkodowanej w celach wyrządzenia szkody materialnej lub pogorszenia opinii[2].

Niebezpieczeństwa dotykające danych osobistych zostały zaobserwowane również przez organy Unii Europejskiej po 2009 roku, co było powodem do wydania opinii. Ustalała ona konieczność ujednolicenia zasad wykorzystujących dane osobowe przez administratorów portali oraz reklamodawców. Opinia wskazuje powinność kasowania danych użytkownika przez zarządcę portalu zaraz po usunięciu konta. Wynika to z tego, że wiele portali zamieszcza zawiłe, obszerne i skomplikowane regulaminy, które mają na celu wprowadzenie w błąd użytkownika przez specyficzne zawarte w nich warunki. W większości przypadków użytkownicy nie mają świadomości na co się zgadzają akceptując warunki umowy[3].

## Metody i rodzaje wyłudzeń na portalach społecznościowych

Aby skutecznie dokonywać wyłudzeń w sieci sprawcy są zmuszani do nieustannego wymyślania nowych metod. Tworzy to ogromne zagrożenie dla użytkowników portali, a także utrudnia zwalczanie internetowych przestępców. Gdy organy ścigania opanują metody i techniki na ujęcie sprawcy, ten zdąży już posługiwać się innym sposobem kradzieży. W historii funkcjonowania *social media* powstało bardzo wiele typów oszustw, a poniższe zestawienie prezentuje najczęściej używane techniki.

**Kradzież tożsamości** – stosunkowo prosta metoda wyłudzenia polegająca na wykradaniu danych osobowych (np. numer PESEL, numery kart, informacji o kontach bankowych) lub działaniach mających zaszkodzić dobremu imieniu ofiary. Osoby wykradające dane wrażliwe mogą posłużyć się nimi do otworzenia nowego rachunku bankowego lub kradzieży środków z istniejącego rachunku lub opłacić inne swoje rachunki kosztem poszkodowanego[4]. Zdarzają się również sytuacje gdzie publikowane z konta użytkownika są materiały zachęcające do kliknięcia

[1] http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-39679cf9-0b59-4752-82c0-38d0bbd280ce/c/Gruber_Jozwiak_ZNPSL_Org._Zarz._63a_2012.pdf (dostęp: 05.05.2020 r.).

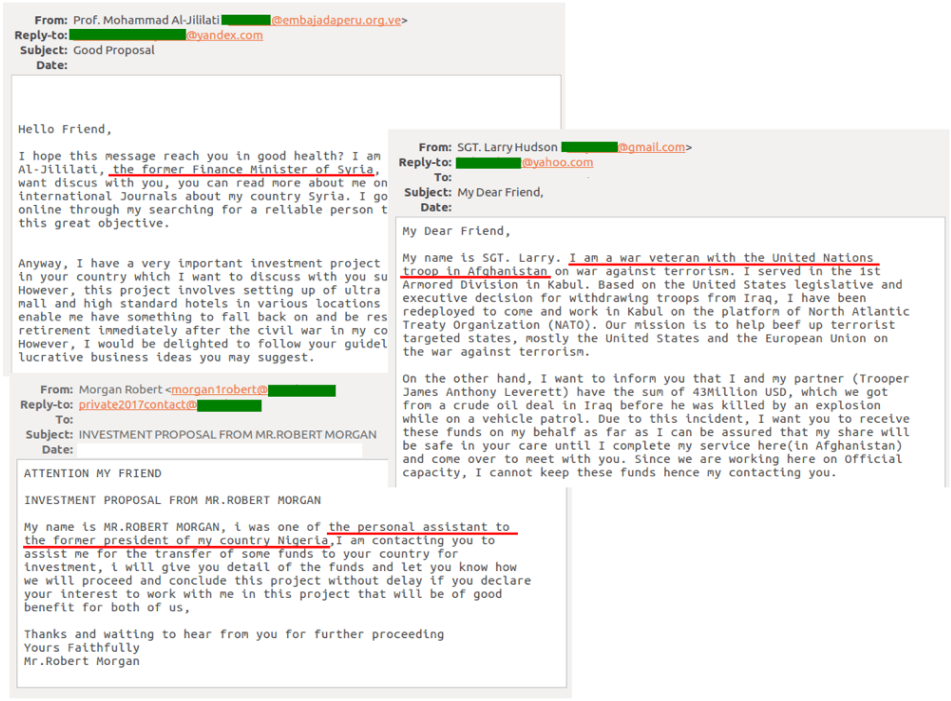
[2] Art. 190a ustawy z dnia 6 czerwca 1997r. Kodeks karny (Dz.U. z 1997 r., nr 88, poz. 553 ze zm.).

[3] K. Garwol, *Portale społecznościowe – szanse i zagrożenia dla młodego człowieka*, Wydawnictwo UR, Rzeszów 2016, s. 186–187.

[4] https://www.westernunion.com/pl/pl/fraudawareness/fraud-types.html (dostęp: 05.05.2020 r.).

w artykuł, który w rzeczywistości zawiera w sobie szkodliwe oprogramowania wykradając wrażliwe dane kolejnej osoby, która otworzy daną witrynę[5].

**Nigeryjski przekręt** – jeden z najbardziej klasycznych i najstarszych sposobów na wyłudzenie pieniędzy. Potencjalna ofiara otrzymuje wiadomość napisaną źle sformułowanym językiem polskim lub też w innym języku od osoby bogatej z innego kraju (afrykańskiego bądź azjatyckiego), która ma kłopoty w swoim kraju i potrzebuje pomocy obywatela Polski w celu założenia konta bankowego. Polega to na wymuszeniu uiszczenia drobnej opłaty manipulacyjnej lub podania numeru karty kredytowej w zamian za sporą sumę pieniędzy jako prowizję za pośrednictwo. Takie działanie pozwalało sprawcy na zyskanie owej opłaty manipulacyjnej, a w najgorszym przypadku, wyczyszczenia środków na koncie. Mimo tego, że sam pomysł brzmi niedorzecznie, to jest on skuteczny i posiada on kilkadziesiąt swoich odmian[6] (rys. 1).



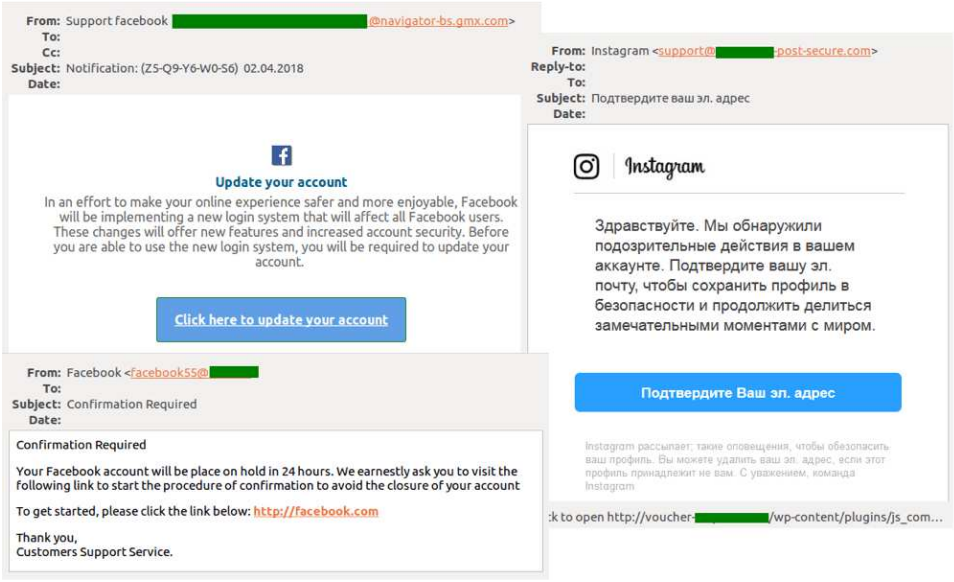

Rys. 1. Przykładowe wiadomości z wykorzystaniem „Nigeryjskiego przekrętu”

Źródło: https://plblog.kaspersky.com/phishing-spam-hooks/10141/(dostęp: 05.05.2020 r.).

[5] https://poradnikprzedsiebiorcy.pl/-wyludzanie-danych-osobowych-zagrozenia (dostęp: 05.05. 2020 r.).

[6] Tamże.

**Fałszywe powiadomienia z portali społecznościowych** – sposób polega na wysyłaniu przez oszustów fałszywych powiadomień pod adresem popularnych portali. W treści powiadomień poruszane są tematy ich znajomych lub aktywności. Rzeczą która odróżnia te powiadomienia od prawdziwych jest odnośnik phishingowy, który często jest trudny do odróżnienia. Włączając wadliwe powiadomienie ofiara jest zmuszona do uwierzytelnienia swoich danych i podania hasła na fałszywej stronie do logowania. Takie działanie otwiera furtkę sprawcom na swobodne wejście na profil społecznościowy ofiary[7] (rys. 2).




Rys. 2. Przykładowe próby uwierzytelnienia konta za pomocą fałszywego powiadomienia

Źródło: https://plblog.kaspersky.com/phishing-spam-hooks/10141/ (dostęp: 05.05.2020 r.).

**Metoda na BLIK** – początkowo polega na włamaniu się na konto poszkodowanego na portalu społecznościowym, a następnie wysyłaniu do najbliższych znajomych ofiary prośby o przelanie pieniędzy z różnych przyczyn. Równie znanym sposobem jest publikowanie na grupach osób sprzedaży losowego przedmiotu i prośba o przelanie pieniędzy BLIK-iem ponieważ oszust tłumaczy się, że przebywa za granicą, więc tradycyjny przelew będzie zbyt kosztowny. Sprawca prosi o podanie kodu i zatwierdzenie transakcji przez nieświadomą ofiarę, po czym doładowuje wirtualny portfel w serwisie Skrill[8]. Metoda ta bazuje głównie na ludzkiej naiwności i jest obecnie najczęściej stosowaną metodą na wyłudzanie pieniędzy (rys. 3).

[7] https://plblog.kaspersky.com/phishing-spam-hooks/10141/ (dostęp: 05.05.2020 r.).
[8] https://fintek.pl/przekret-blika-metoda-wyludzania-pieniedzy/ (dostęp: 05.05.2020 r.).


Rys. 3. Przykładowa wiadomość od oszusta posługującego się metodą BLIK

Źródło: http://www.policja.pl/pol/aktualnosci/184677,Nie-podawaj-kodu-BLIK.html (dostęp: 05.05.2020 r.).

**SCAM –** SCAM to oszustwo mające na celu wzbudzenie zaufania czy ciekawości poszkodowanego, a następnie wykorzystanie tego zaufania do wyłudzenia danych osobowych lub pieniędzy. SCAM-owy post charakteryzuje się szokującą, intrygującą, obrzydzającą treścią, a zwłaszcza emocjonującym nagłówkiem zachęcającym do kliknięcia na daną witrynę. Taki post zawiera również ciekawe zdjęcie nawiązujące do treści nagłówka. Często pojawia się znajomo brzmiąca postać z mediów, lecz w rzeczywistości nie chodzi o nikogo znanego. Pod nagłówkiem zamieszczany jest też krótki opis potęgujący wrażenie prawdziwości informacji. Najbardziej częstym zagrożeniem związanym ze SCAM-em jest zmanipulowanie odbiorcy do podania swoich danych, aby móc przeczytać artykuł, np. podanie e-maila, który zapewne trafi do SPAM-iarskiej bazy kontaktów, przez co skrzynka odbiorcza tej osoby zostanie zasypana dziwnymi wiadomościami lub reklamami. W przypadku podania numeru telefonu może okazać się, że będzie pobierana jednorazowa lub cykliczna opłata, którą będzie trudno dezaktywować. Niektóre strony posiadają również wirusa, który będzie udostępniał ten i inne posty na tablicy poszkodowanego tworząc łańcuch osób odwiedzających niebezpieczną stronę[9] (rys. 4).

[9] https://annamariawisniewska.pl/jakie-zagrozenia-czyhaja-na-ciebie-na-facebooku-scam-jako-jedno-z-nich/ (dostęp: 05.09.2020 r.).


Rys. 4. Przykładowy post SCAM-ujący na portalu Facebook

Źródło: https://annamariawisniewska.pl/jakie-zagrozenia-czyhaja-na-ciebie-na-facebooku-scam-jako-jedno-z-nich/ (dostęp: 05.09.2020 r.).


Rys. 5. Informacja nakazująca uiszczenie opłaty za „dezynfekcję” paczki

Źródło: opracowanie własne.

**Fałszywe strony** – osoby poszkodowane otrzymują wiadomość z linkiem informującym o braku zapłaty lub o konieczności dopłaty danej kwoty do rachunku. Po kliknięciu w link ukazuje się strona dostawcy np. usług telefonicznych, na której widnieje gotowy do wydruku przelew, gdzie trzeba tylko wpisać swoje dane i zapłacić rachunek. W rzeczywistości jest to niemalże identyczna strona internetowa, która różni się jedynie numerem konta bankowego, a oszuści zyskują pełną kwotę lub niewielką dopłatę, dzięki której są w stanie włamać się na konto bankowe i je wyczyścić[10] (rys. 5).

## Ochrona prawna obywateli przed oszustwami w sieci. Analiza przepisów prawnych

Obecnie polski system prawny nie posiada jednolitego aktu, w którym gromadziłyby się regulacje prawne dotyczące cyberprzemocy. Jednakże społeczeństwo nie pozostaje bez ochrony prawnej w przypadku zagrożeń w przestrzeni internetowej, ponieważ dostępne są dwie drogi: karna i cywilna. Należy uwzględnić to rozróżnienie dlatego, że liczba zagrożeń powodowanych za pomocą nowych technologii sprawia, iż kodeks karny nie jest rozbudowany do takiego stopnia, by objąć wszystkie przestępstwa popełniane w Internecie. Wówczas zgłoszenie przestępstwa w sieci, czyli skierowanie sprawy do postępowania karnego, jest niemożliwe. W takich przypadkach należy wykorzystać drogę cywilną, a dokładniej – drogę roszczeń odszkodowawczych.

W dalszej części rozdziału omówione zostały najbardziej powszechne formy cyberprzemocy powiązane bezpośrednio ze zjawiskiem wyłudzenia w sieci oraz sposoby dochodzenia odpowiedzialności prawnej sprawcy[11].

### Naruszenie dóbr osobistych, a w szczególności nazwiska lub pseudonimu i wizerunku oraz czci

Charakteryzuje się w działaniach mających na celu upublicznienie danych osobowych identyfikujących użytkownika (np. nazwisko, twarz lub pseudonim) bez zgody, wiedzy lub wbrew woli właściciela. Przybiera ono formy takie jak zamieszczanie fotografii lub filmów przedstawiających poszkodowanego na portalu społecznościowym. Przed takim rodzajem występku społeczeństwo chroni Konstytucja, a dokładnie art. 47, który mówi, że „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”[12]. W przypadku gdy ofiarą staje się dziecko dotyczy

[10] http://www.policja.pl/pol/aktualnosci/184568,Klikasz-w-link-i-mozesz-stracic-pieniadze.html (dostęp: 05.05.2020 r.).

[11] https://fundacja.orange.pl/files/user_files/user_upload/6.%20gdzie%20jest%20mimi/jak-reagowac-na-cyberprzemoc.pdf (dostęp: 05.05.2020 r.).

[12] Art. 47 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.

sytuacji art. 8 Konwencji o Prawach Dziecka, którego treść brzmi: „1. Państwa-Strony podejmują działania mające na celu poszanowanie prawa dziecka do zachowania jego tożsamości, w tym obywatelstwa, nazwiska, stosunków rodzinnych zgodnych z prawem, z wyłączeniem bezprawnych ingerencji. 2. W przypadku, gdy dziecko zostało bezprawnie pozbawione części lub wszystkich elementów swojej tożsamości, Państwa-Strony okażą właściwą pomoc i ochronę w celu jak najszybszego przywrócenia jego tożsamości”[13].

Artykuł ten wyjaśnia, że każde działanie mające na celu pozbawienie elementów tożsamości dziecka będzie skutkowało reakcją danego państwa i natychmiastową ochroną tej osoby. Następnym aktem prawnym zabezpieczającym użytkownika przed niebezpiecznymi działaniami jest kodeks cywilny, a dokładnie art. 23 oraz art. 24. Artykuł 23 dotyczy ochrony dóbr osobistych człowieka (również podczas aktywności na portalach społecznościowych) i niezależnie od przewidzianej ochrony w innych przepisach, obywatel pozostaje pod ochroną prawa cywilnego. Następny artykuł wyraża jasno, że jeżeli jakieś dobro (np. wizerunek, nazwisko) zostanie naruszone, wówczas poszkodowana osoba może domagać się usunięcia materiałów naruszających godność, a także na zasadach przewidzianych w kodeksie może również żądać rekompensaty w formie pieniężnej na własne cele lub wskazane cele społeczne[14]. Przykładem, gdzie występuje naruszenie dóbr osobistych, może być np. założenie (przez sprawcę) profilu na portalu społecznościowym, gdzie umieszczone będą obnażające zdjęcia osoby poszkodowanej.

## Naruszenie czci (zniesławienie, znieważenie)

W tym przypadku mowa jest o wszelkich czynnościach, które ingerują w życie prywatne oraz godność człowieka o charakterze lekceważącym oraz pogardliwym. Zazwyczaj do takich incydentów dochodzi za pośrednictwem portali społecznościowych, gdzie poszkodowana osoba zostaje publicznie ośmieszona i upokorzona. Inną formą znieważenia jest również wysyłanie wiadomości obrażających ofiarę przy użyciu np. fałszywych materiałów, zwłaszcza wulgarnych lub wysyłanie kompromitujących zdjęć i filmów. Gdy zachodzi taka sytuacja, zastosowanie swoje ma art. 212 oraz art. 216 kodeksu karnego oraz art. 8 Konwencji o Prawach Dziecka (jeżeli sprawa dotyczy osoby niepełnoletniej). Art. 212 dotyczy pomówienia podmiotu którym może być osoba, grupa osób, instytucja, osoba prawna lub jednostka organizacyjna i jasno opisuje sytuacje kiedy zachodzi dana sytuacja. Osobom, które dopuszczają się czynu określonego w tym artykule grozi grzywna lub kara ograniczenia wolności, natomiast, jeżeli sprawca dopuszcza się czynu za pomocą środków masowego komunikowania (np. zamieszczanie treści na Facebooku) podlega powyższej karze albo pozbawieniu wolności do roku. Uwzględniona jest również nawiązka na rzecz pokrzywdzonego, Polskiego Czer-

[13] Art. 8 Konwencji o Prawach Dziecka przyjętej przez Zgromadzenie Ogólne ONZ 20 listopada 1989 r.

[14] Art. 23, 24 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2019 r., poz. 1145).

wonego Krzyża lub na inny cel społeczny, jeżeli tak orzeknie sąd[15]. Podobnym artykułem jest art. 216 k.k., który dotyczy znieważenia osoby. Czyn też także jest prawnie zabronionym i za popełnienie go grozi kara grzywny lub kara ograniczenia wolności a w przypadku dokonania za pomocą środków masowej komunikacji grozi kara pozbawienia wolności do roku. Artykuł ten (w odróżnieniu od art. 212) uwzględnia odstąpienie wymierzenia kary przez sąd w przypadku, gdy osoba pokrzywdzona odpowie oskarżonemu w ramach samosądu (np. pobije oskarżonego lub znieważy go wzajemnie). Przykładową sytuacją może być umieszczenie przez sprawcę nieprawdziwych i obraźliwych treści na portalu społecznościowym pod adresem poszkodowanego.

## Włamania (w sieci)

Czynności dokonywane bezprawnie za pomocą Internetu na strony/profile strzeżone hasłami lub innymi typami zabezpieczeń polegają na złamaniu wyżej wymienionych blokad w celu uzyskania jakichś informacji, dodania lub usunięcia materiałów oraz zniszczenia/uszkodzenia treści na profilu poszkodowanej osoby. Aktami prawnymi w sytuacji zagrożenia prywatności są kodeks karny, a dokładnie jego art. 267 oraz 268a. Pierwszy artykuł odnosi się do uzyskania dostępu do informacji nieprzeznaczonych dla sprawcy. Określone jest, w jaki sposób naruszane jest prawo, a także określona jest sankcja karna za występek. Ustawodawca przewidział za ten czyn karę grzywny, ograniczenia wolności lub pozbawienia wolności do lat 2. Takiej samej karze podlega osoba, która używa podsłuchu do uzyskania informacji lub dzieli się tą informacją z inną osobą. Art. 268a odnosi się zaś do bezprawnej inwigilacji w dane informatyczne (jak np. prywatne wiadomości poszkodowanego), niszczenia, zmieniania i ingerencji w przesyłanie, gromadzenie, przetwarzanie tych danych. Za ten czyn ustawodawca przewiduje karę pozbawienia wolności do 3 lat. Natomiast w przypadku, gdy sprawca wyrządzi straty finansowe osobie poszkodowanej, ustawodawca ustalił karę pozbawienia wolności od 3 miesięcy do 5 lat. W przypadku, gdy taki incydent dotyczy osoby nieletniej, należy uwzględnić również art. 16. Konwencji o Prawach Dziecka, który wyraża jasno, że każde dziecko ma prawo do ochrony prawnej w memencie, gdy zostanie naruszona jego sfera prywatna (np. życie prywatne, honor, reputacja). Sytuacją, w jakiej zachodzi włamanie może być zdarzenie, gdy sprawca włamuje się na profil społecznościowy poszkodowanej osoby, a następnie usuwa zamieszczone tam materiały lub obraża i pomawia.

## Szantaż

Zgodnie z obowiązującym prawem szantażowanie jest przestępstwem. Czyn ten zachodzi w momencie, gdy sprawca po nielegalnym pozyskaniu danych (np. wykradnięcia prywatnych wiadomości z Facebooka) grozi poszkodowanemu, że

[15] Art. 212 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997 r., nr 88, poz. 553 ze zm.).

upubliczni te dane, gdy ten nie wykona jego żądań. Mimo że w kodeksie karnym słowo „szantaż" nie występuje ani razu, to czyn opisujący to słowo występuje w art. 191, który brzmi następująco: „§ 1. Kto stosuje przemoc wobec osoby lub groźbę bezprawną **w celu zmuszenia innej osoby do określonego działania**, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3". W przypadku, gdy dojdzie do publikacji tych materiałów, osoba pokrzywdzona może ubiegać się swoich praw w postępowaniu cywilnym, a dokładnie na podstawie art. 23 kodeksu cywilnego (artykuł omawiany przy przypadku naruszenia dóbr osobistych).

Powyższe przykłady zostały uwzględnione, ponieważ osoby poszkodowane doświadczają ich podczas wyłudzeń najczęściej. Jeżeli natomiast chodzi o akty prawne, które mają swoje zastosowanie w przypadkach oszustw, to jest ich większa liczba. Artykułem, od którego należy zacząć dochodzenia prawne po dokonanym oszustwie, jest art. 287 k.k., którego treść brzmi: „§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5". Jego zapis mówi jasno o czynie pozyskania korzyści majątkowej bez pozwolenia poszkodowanego, a także o przewidzianym środku karnym za występek. Następnym artykułem broniącym ofiarę ataku w sieci jest art. 107 k.w., którego zapis informuje, że sprawca dokuczając innej osobie złośliwie wprowadza ją w błąd lub w inny sposób niepokoi, podlega karze ograniczenia wolności, grzywnie do 1500 złotych albo karze nagany[16].

## Podsumowanie

W rozdziale ukazano, jak wiele zagrożeń w kontekście wyłudzeń istnieje na portalach społecznościowych. Mimo krótkiego czasu funkcjonowania *social media*, liczba zagrożeń mających wpływ na bezpieczne korzystanie drastycznie wzrosła, powodując, że społeczeństwo ma problemy w regularnym przeciwdziałaniu i dowiadywaniu się o sposobach ataków. Wzrost popularności portali społecznościowych oraz rozwój technologii sprawił, że ataki oszustów z każdym rokiem są coraz liczniejsze. W tekście ukazano wybrane popularne metody wyłudzeń. Prowadzone są kampanie społeczne mające na celu uświadamianie społeczeństwa, jak groźnym miejscem może być sieć w przypadku nieumiejętnego użytkowania. Prawo w przypadku dokonywania wyłudzeń działa jedynie po dokonaniu występku. Nie zabezpiecza obywatela przed staniem się ofiarą ataku. Społeczeństwo musi zdać sobie sprawę, że bez kształcenia w temacie bezpieczeństwa w sieci, naraża się na liczne niebezpieczeństwa. Należy podejmować formy przeciwdziałania atakom, takie jak chociażby instalowanie systemów antywirusowych, mających

[16] Art. 107 ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń (tekst jedn. Dz.U. z 2019 r., poz. 821).

ustrzec użytkownika przed fałszywym oprogramowaniem, a także zabezpieczanie kont internetowych logowaniem dwuskładniowym oraz stosowanie wielu haseł podczas zakładania profili na różnych stronach. Odpowiedzialne korzystanie z portali poprawi bezpieczeństwo własne i nie narazi użytkownika na niepożądane skutki.

## Bibliografia

Garwol K., *Portale społecznościowe – szanse i zagrożenia dla młodego człowieka*, Wydawnictwo UR, Rzeszów 2016.

## Prawodawstwo

Konwencja o Prawach Dziecka przyjęta przez Zgromadzenie Ogólne ONZ w dniu 20 listopada 1989 r. (Dz.U. z 1991 r., nr 120, poz. 527).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483 ze zm.).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (tekst jedn. Dz.U. z 2020 r., poz. 1740).

Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (tekst jedn. Dz.U. z 2019 r., poz. 821).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz.U. z 2020 r., poz. 1444).

## Netografia

https://fundacja.orange.pl/files/user_files/user_upload/6.%20gdzie%20jest%20mimi/jak-reagowac-na-cyberprzemoc.pdf

https://plblog.kaspersky.com/phishing-spam-hooks/10141/

http://www.policja.pl/pol/aktualnosci/184568,Klikasz-w-link-i-mozesz-stracic-pieniadze.html

http://www.policja.pl/pol/aktualnosci/184677,Nie-podawaj-kodu-BLIK.html

https://poradnikprzedsiebiorcy.pl/-wyludzanie-danych-osobowych-zagrozenia

https://fintek.pl/przekret-blika-metoda-wyludzania-pieniedzy/

https://www.westernunion.com/pl/pl/fraudawareness/fraud-types.html

http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-39679cf9-0b59-4752-82c0-38d0bbd280ce/c/Gruber_Jozwiak_ZNPSL_Org._Zarz._63a_2012.pdf

# PRAWNE REGULACJE STALKINGU INTERNETOWEGO W POLSKIM PRAWIE KARNYM

(*Paweł Gierłach*)

## Wprowadzenie

Postępujący rozwój cyberprzestrzeni to nie tylko nowe możliwości, ale także liczne wyzwania dla krajowych i międzynarodowych ustawodawców. Internet początkowo miał służyć przede wszystkim celom badawczym i edukacyjnym – w związku z tym cechował go brak zabezpieczeń. Jednakże wciąż rosnąca popularność sieci komputerowych oraz wzrost liczby użytkowników wpłynęły nie tylko na kształt istniejących stosunków prawnych, ale również przyczyniły się do powstania nowych form przestępczości, które zaczęto określać mianem cyberprzestępstw. Stosowanie zwyczajowych rozwiązań prawnych do cyberprzestrzeni okazało się niemożliwe[1].

Pojawiły się nowe rodzaje przestępstw – przestępstwa komputerowe (cyberprzestępstwa), do których zaliczyć można zarówno te skierowane przeciwko systemowi komputerowemu, jak i te popełnione przy jego użyciu[2]. W tej drugiej kategorii znajdują się m.in. przestępstwa obejmujące zamachy na tradycyjne dobra prawne dokonywane za pomocą nowoczesnych urządzeń, służących do cyfrowego gromadzenia i przetwarzania danych, przy czym sposób popełnienia przestępstwa (z wykorzystaniem tychże technologii) nie jest wskazany w ustawowym opisie danej odmiany przestępstwa rodzajowego[3]. W tej właśnie grupie znajduje się stalking, czy dokładnie stalking internetowy, czyli uporczywe nękanie innej osoby lub osoby jej najbliższej mające na celu wzbudzenie u niej uzasadnionego okolicznościami poczucia zagrożenia lub istotne naruszenie jej prywatności. Stalking internetowy może również polegać na złośliwym wykorzystywanie danych osobowych innej osoby celem narażenia jej na szkodę materialną lub osobistą.

Celem rozważań jest zaprezentowanie uregulowań prawnych przestępstwa stalkingu w polskim prawie karnym, ze szczególnym uwzględnieniem stalkingu

---

[1] I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 1.

[2] B. Fisher, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 24.

[3] P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, s. 52.

internetowego. Autor postara się przybliżyć krótko historię wprowadzenia stalkingu do katalogu przestępstw penalizowanych przez polskie prawo karne. Omówione zostaną także pojęcie, znamiona oraz tryb ścigania stalking.

## Rys historyczny i geneza wprowadzenia stalkingu do polskiego kodeksu karnego

W Polsce regulacje dotyczące prawnokarnej oceny stalkingu znajdują się jedynie w kodeksie karnym i zostały wprowadzone w 2011 roku[4]. Stało się to za sprawą ustawy nowelizującej kodeks karny, uchwalonej przez Sejm RP w dniu 25 lutego 2011 roku[5]. Ustawa weszła w życie po dwóch miesiącach od publikacji.

Stalking jest pojęciem, które przewija się w podręcznikach od lat. W jego lepszym zrozumieniu pomaga kodeks karny, gdzie w uzasadnieniu ustawy z 25 lutego 2011 r. (druk sejmowy nr 3553), dowiadujemy się, iż inicjatywą do wprowadzenia tego pojęcia była sprawna ochrona prawna wobec stalkingu[6].

Rozważania nad stalkingiem zaczęto w latach 80. XX wieku; w tym czasie ofiarami stalkingu padali głównie celebryci. Jedną z pierwszych ofiar stalkingu padła Jodie Foster. Aby zdobyć zainteresowanie aktorki prześladowca próbował przeprowadzić zamach na prezydenta USA Ronalda Regana.

W Polsce stalking zaobserwowano w latach 90. XX wieku. W roku 2009 przeprowadzono badania w celu rozpoznania skali zjawiska stalkingu w Polsce. Badania wykazały, że 9,9% badanych było ofiarą uporczywego nękania (badanie przeprowadzono na grupie 10 200 losowo wybranych osób)[7]. Badania wykazały, że sprawcy stosowali różne sposoby znęcania się nad ofiarami, najczęściej posługiwali się plotkami i oszczerstwami, posługiwali się również osobami trzecimi. „Stalkerzy" upodobali sobie także e-maile, SMS, portale społecznościowe, upublicznianie wizerunku czy robienie zdjęć z ukrycia.

Osoby pokrzywdzone w związku ze zdarzeniem stalkingu zgłaszały problemy natury emocjonalnej, psychicznej, przygnębienie, brak poczucia bezpieczeństwa, irytację, złość oraz strach. Zaburzenia, z jakimi borykały się osoby pokrzywdzone, to między innymi obawy wyjścia z domu, które odczuwało 30% osób; rozkojarzenie lub agresja występowały u co czwartej ofiary. Natomiast znaczna część pokrzywdzonych borykała się z zaburzeniami sfery psychiki. Próby i myśli samobójcze miała co dziewiąta osoba, 20% miało ataki paniki, a jedna na dziewięć osób natręctwa lub urojenia. Co czwarta ofiara wspominała o dolegliwościach fizycznych, połowa ofiar stalkingu musiała skorzystać z pomocy lekarskiej. Co dziewiąta osoba dotknięta stalkingiem musiała zmienić miejsce zamieszkania, a co szósta

[4] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. nr 88, poz. 553 ze zm.) (dalej jako: k.k.).
[5] Ustawa z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny (Dz.U. nr 72, poz. 381).
[6] Uzasadnienie do ustawy z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny, Sejm VI kadencji, druk sejmowy nr 3553, http://orka.sejm.gov.pl/Druki6ka.nsf
[7] Tamże.

zmuszona była do zmiany pracy. Jedna na dwie osoby pokrzywdzone stalkingiem unikała pewnych miejsc lub sytuacji, a około 40% ofiar pogorszeniu uległo życie zawodowe lub rodzinne[8].

Analiza wyników tych badań doprowadziła ustawodawcę do wniosku, iż istniejące w polskim prawie instrumenty prawne nie są wystarczające dla zabezpieczenia przed zachowaniami mieszczącymi się w ramach zjawiska stalkingu i niezbędne jest wprowadzenie nowych rozwiązań prawnych, zwłaszcza w zakresie kryminalizacji tego rodzaju zachowań. Wspomniana wyżej nowelizacja (dodanie do kodeksu karnego art. 190a) stała się odpowiedzią na wyniki przeprowadzonych badań.

Przed wejściem w życie przepisów art. 190a k.k. na gruncie polskiego prawa karnego do walki z nękaniem można było stosować niektóre z przepisów kodeksu karnego lub kodeksu wykroczeń[9], np. art. 107 k.w. (złośliwe niepokojenie); art. 207 k.k. (znęcanie się); art. 190 k.k. (groźba karalna), jednakże zasadniczy problem, jaki pojawiał się w walce z nękaniem, był taki, że zachowania sprawcy (niezwykle dolegliwe dla ofiary) często w ogóle nie były przestępstwami ani nawet wykroczeniami (wystawanie pod domem czy pracą, pisanie listów, zasypywanie SMS-ami czy mailami itp.), choć mogły stanowić dla ofiary znaczącą dolegliwość[10].

## Stalking i stalking internetowy – definicja, przedmiot ochrony, znamiona, tryb ścigania, wymiar kary

Ani polski kodeks karny, ani inny obowiązujący obecnie w Polsce akt prawny, nie definiuje stalkingu internetowego. Słowo „stalking" pochodzi z języka angielskiego i oznacza „skradanie się", „podchody"[11].

Legalna definicja stalkingu pojawiła się w polskim kodeksie karnym w 2011 roku i od tamtej pory treść dodanego wówczas przepisu art. 190a k.k. do dziś brzmi następująco:

„Art. 190a § 1. Kto przez uporczywe nękanie innej osoby doprowadza ją lub osobę jej najbliższą do uzasadnionego odczuwania strachu lub narusza jej prywatność, podlega karze pozbawienia wolności do lat 3.

§ 2. Tej samej karze podlega, kto złośliwie wykorzystuje dane osobowe innej osoby celem narażenia jej na szkodę materialną lub osobistą.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub § 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 12.

---

[8] Tamże.

[9] Ustawa z dnia 20 maja 1971 roku Kodeks wykroczeń (Dz.U. z 1971 r., nr 12, poz. 114 ze zm.).

[10] M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik, M. Mozgawa (red.), *Kodeks karny. Komentarz*, wyd. VII WoltersKluwer 2015 (M. Mozgawa, komentarz do art. 190a k.k.).

[11] https://pl.wikipedia.org/wiki/Stalking (dostęp: 13.04.2020 r.).

§ 4. Ściganie przestępstwa określonego w § 1 lub § 2 odbywa się na wniosek pokrzywdzonego".

Według zacytowanego powyżej artykułu stalkingiem są zachowania uporczywe polegające na nękaniu danej osoby, może to być także wykorzystanie danych osobowych w celu narażenia jej na szkodę materialną poprzez wykorzystanie jej danych w Internecie.

Będzie nim również tzw. przywłaszczenie wizerunku, czyli wskazane w § 2 „złośliwe wykorzystanie danych osobowych innej osoby celem narażenia jej na szkodę materialną lub osobistą" przy użyciu Internetu.

Za przedmiot ochrony przed stalkingiem oraz stalkingiem internetowym uznano podstawowe dobra człowieka, do których zaliczyć można godność, wolność i jego cześć. Poza tymi podstawowymi dobrami uwzględnić trzeba także, iż przedmiotem ochrony będzie w szczególności zdrowie człowieka, fizyczne oraz psychiczne, jego nietykalność cielesna, a także nienaruszalność korespondencji. Za przedmiot ochrony uznaje się wolność w zakresie samodzielnego decydowania informacjami o swoim życiu osobistym, danymi osobowymi oraz wolność dysponowania swoim wizerunkiem. Przestępstwo stalkingu, o którym mowa w art. 190a § 1 k.k. jest przestępstwem powszechnym. Może ono zostać popełnione przez każdego, kto jest zdolny do ponoszenia odpowiedzialności karnej. Co więcej, przedmiotem czynności wykonawczej może być również człowiek (czyli: inna osoba), na którego skierowane są działania sprawcy lub bliscy danej osoby. Przykładem takiego działania może być oddziaływanie na rodziców za pośrednictwem dzieci (rodzice są przedmiotem działania, ale „wykonuje się" je przez wpływ na dzieci)[12].

Czyny sprawcy objawiają się nękaniem wzbudzającym u ofiary poczucie naruszenia jej prywatności oraz zagrożenia. Uporczywość ta dzieli się na dwa elementy: po pierwsze, postępowanie sprawcy rozumiane jako postępowanie podmiotowe, czyli takie, które skupia się na nastawieniu psychicznym sprawcy (chęć postawienia na swoim, nieustępliwość itp.); po drugie, postępowanie sprawcy rozumiane jako stan obiektywny, czyli taki, który trwa przez pewien dłuższy czas[13]. Jednorazowe działanie sprawcy nie jest zatem stalkingiem – to uporczywość i wiążące się z nią upór, wielokrotność działania i wytrwałość są znakami, że do stalkingu dochodzi.

Działania sprawcy mają polegać na nękaniu, co w rozumieniu słownikowym oznacza ustawiczne dręczenie, trapienie, niepokojenie (czymś) kogoś; dokuczanie komuś, nie dawanie chwili spokoju[14].

Nękanie w sieci może przybrać różne formy. Może przybrać postać nękania za pomocą maili oraz wiadomości na portalach społecznościowych i polegać na:

- zamieszczaniu obraźliwych komentarzy na portalach społecznościowych lub forach, do których należy ofiara;

[12] Uzasadnienie do ustawy z dnia 25.2.2011 r. o zmianie ustawy – Kodeks karny.
[13] R.A. Stefański (red.), *Kodeks karny. Komentarz*, Warszawa 2018.
[14] S. Dubisz (red.), *Uniwersalny słownik języka polskiego*, t. II, Warszawa 2003, s. 1095.

- umieszczaniu w Internecie filmów oraz zdjęć z wizerunkiem ofiary lub groźby umieszczenia takich;
- nękaniu za pomocą aplikacji i portali randkowych;
- wykluczaniu pokrzywdzonego z grup np. poprzez zablokowania dostępu do komunikatora czy forum dyskusyjnego;
- rozsyłaniu przez stalkera drogą elektroniczną negatywnych opinii o ofierze do jej potencjalnych pracodawców i wiele innych.

Zachowanie sprawcy jest znamienne skutkiem, co oznacza, że ma ono wzbudzać u osoby prześladowanej uzasadnione okolicznościami poczucie zagrożenia lub istotnie naruszać jej prywatność[15].

Wzbudzenie u pokrzywdzonego poczucia zagrożenia winno być oceniane w sposób obiektywny, wynikający z analizy okoliczności dotyczących zachowania sprawcy, zaś przesłanką odpowiedzialności w tym przypadku jest wyłącznie poczucie zagrożenia, jakie powstałoby w danych okolicznościach u przeciętnej, racjonalnie myślącej osoby, której reakcja mogłaby zostać uznana za naturalną i niebudzącą wątpliwości[16].

Alternatywnym skutkiem uporczywego nękania – choć nie można wykluczyć wystąpienia obu łącznie – jest istotne naruszenie prywatności. Wprowadzenie tego odrębnego pojęcia zostało uzasadnione wynikami badań empirycznych, z których wynika, że stalking skutkować może naruszeniem życia prywatnego, obejmującym m.in. takie formy działania stalkera, jak: próby nawiązywania kontaktów z daną osobą, częste głuche lub nocne telefony, otrzymywanie niechcianych e-maili, listów oraz SMS-ów, pozostawianie wiadomości pod drzwiami, a także robienie zdjęć bez uprzedniego wyrażenia zgody[17].

Stalking, powszechnie znany i kojarzony jest przede wszystkim ze swym pierwszym, opisanym już typem podstawowym – uporczywym nękaniem. Tymczasem w paragrafie drugim art. 190a k.k. został wprowadzony odrębny typ podstawowy, który skrótowo można nazwać przestępstwem „przywłaszczenia tożsamości", a polegający na złośliwym wykorzystywanie danych osobowych innej osoby celem narażenia jej na szkodę materialną lub osobistą. Ta właśnie forma wydaje się niezwykle charakterystyczna dla stalkingu internetowego. Zachowanie stalkera polega na podszyciu się pod inną osobą poprzez wykorzystanie jej wizerunku lub innych danych osobowych, co w praktyce przejawiać się będzie m.in. zamieszczaniem zdjęć ofiary i komentarzy ujawniających informacje o niej w Internecie, zamawianiem na jej koszt niechcianych towarów i usług, a także rozpowszechnianiem informacji o pokrzywdzonym, np. w ramach tworzonych bez wiedzy i zgody ofiary kont na popularnych portalach społecznościowych[18].

---

[15] R.A. Stefański (red.), *Kodeks karny…*

[16] Uzasadnienie do ustawy z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny.

[17] A. Szelęgiewicz, *Stalking i przywłaszczenie tożsamości w polskim prawie karnym. Zagadnienia wybrane*, „Ius Novum" 2013, nr 3, s. 67.

[18] Tamże, s. 71.

Pisząc o stalkingu, należy wspomnieć o typie kwalifikowanym tegoż występku, opisanym w art. 190a § 3 k.k., zgodnie z którym o surowszej odpowiedzialności sprawcy decyduje następstwo, polegające na targnięciu się pokrzywdzonego na własne życie. Dla zastosowania dyspozycji art. 190a § 3 k.k. konieczne jest ustalenie, od strony przedmiotowej, związku przyczynowego między poszczególnymi zachowaniami mającymi postać nękania a targnięciem się pokrzywdzonego na własne życie[19].

Ostatni paragraf art. 190a k.k. wskazuje, iż przestępstwo uporczywego nękania w postaci wyrażonej zarówno w § 1 jak i § 2 art. 190a k.k. jest przestępstwem ściganym na wniosek pokrzywdzonego, zaś postać kwalifikowana przestępstwa nękania z art. 190a § 3 k.k. jest natomiast ścigana jest w trybie publicznoskargowym z urzędu.

Czyn, o którym mowa w art. 190a § 1 i § 2 k.k., zagrożony jest karą pozbawienia wolności do lat 3. Natomiast typ kwalifikowany, o którym stanowi art. 190a § 3 k.k., zagrożony jest karą pozbawienia wolności od lat 2 do lat 12.

## Podsumowanie

Od czasu wprowadzenia stalkingu do kodeksu karnego minęło ponad 9 lat. I choć pojawiały się w doktrynie głosy krytykujące sam sposób regulacji[20], z pewnością samo wprowadzenie do katalogu przestępstw nowego czynu zabronionego, było naturalnym i koniecznym następstwem zmian zachodzących w społeczeństwie i należy je ocenić pozytywnie.

Gwałtowny rozwój techniki i technologii wpłynął znacząco na życie społeczne i kulturalne, oddziałując często bardzo negatywnie na ludzkie zachowania i niejako stwarzając pole do popełniania nowych rodzajów przestępstw (np. stalkingu w Internecie). Permanentny postęp w dziedzinie nowoczesnych technologii przekłada się bowiem na coraz to doskonalsze sposoby i metody działań przestępnych, zaś sprawcy przestępstw to grupa, która bardzo szybko dostosowuje strategie przestępne do zmieniającej się rzeczywistości społecznej[21].

Żyjemy w czasach, w których dla wielu osób miarą statusu społecznego jest liczba znajomych na portalu społecznościowym, a cena, którą potencjalny nabywca jest w stanie zapłacić za wirtualny przedmiot, dostępny jedynie w sieciowej grze komputerowej, może przekraczać nawet kilka tysięcy złotych. Internet jest miejscem, w którym najszybciej i najłatwiej uzyskamy potrzebne informacje czy usługi; miejscem przetwarzanie możliwie jak największej ilości danych o pojedynczych osobach w rozmaitych systemach. Znakiem czasów stało się również, niestety, iż stał się on również nowym, ogromnym polem działalności przestępczej.

---

[19] M. Staręga, *Stalking jako nowy czyn zabroniony w polskim kodeksie karnym. Aspekt prawny oraz znaczenie społeczne*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" 2012, nr 94, s. 198.

[20] A. Szelęgiewicz, *Stalking i przywłaszczenie tożsamości…*, s. 65.

[21] M. Szczepaniec, *Komputer jako narzędzie przestępstwa*, „Zeszyty Prawnicze", 12.2/2012, s. 178.

Jedną z form tej działalności jest stalking internetowy. Z tego też względu, wprowadzenie do kodeksu karnego regulacji prawnych dotyczących stalkingu z pewnością było niezbędne.

## Bibliografia

Budyn-Kulik M., Kozłowska-Kalisz P., Kulik M., Mozgawa M. (red.), *Kodeks karny. Komentarz*, wyd. VII, WoltersKluwer, 2015.

Dubisz S. (red.), *Uniwersalny słownik języka polskiego*, t. II, Warszawa 2003.

Fisher B., *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000.

https://pl.wikipedia.org/wiki/Stalking

Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.

Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.

Staręga M., *Stalking jako nowy czyn zabroniony w polskim kodeksie karnym. Aspekt prawny oraz znaczenie społeczne*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach" 2012, nr 94.

Stefański R.A. (red.), *Kodeks karny. Komentarz*, Warszawa 2018.

Szczepaniec M., *Komputer jako narzędzie przestępstwa*, „Zeszyty Prawnicze" 2012, nr 12.2.

Szelęgiewicz A., *Stalking i przywłaszczenie tożsamości w polskim prawie karnym. Zagadnienia wybrane*, „Ius Novum" 2013, nr 3.

## Prawodawstwo

Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (tekst jedn. Dz.U. z 2019 r., poz. 821).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tekst jedn. Dz.U. z 2020 r., poz. 1444).

Ustawa z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny (tekst jedn. Dz.U. z 2011 r., nr 72, poz. 381).

# INWIGILACJA W SIECI

(*Adrian Martinez*)

## Wstęp

Postęp technologiczny, jaki nastąpił na przełomie XX i XXI wieku, spowodował, iż świat stał się dużo prostszy. Powstało wiele urządzeń takich jak: telefony, telewizja, komputery, czy Internet, które znacząco przyczyniły się do procesu globalizacji oraz sprawiły, że wiele rzeczy kiedyś niedostępnych stało się rzeczami powszechnymi. Szczególnie Internet jest urządzeniem przełomowym, który znacząco zmienił funkcjonowanie świata. Niestety, poza korzyściami, jakie daje technologia cyfrowa, Internet również przyczynia się do powstania wielu nowych poważnych zagrożeń. Jednym z nich jest inwigilacja. Jest to stosunkowo nowe zjawisko, lecz już w ostatnich latach stało się jednym z głównym tematów rozważań. Powodowane jest to faktem, iż inwigilacja narusza podstawowe prawa człowieka, w tym prawo do prywatności, co wywołuje wiele negatywnych reakcji ze strony ludzi.

W opracowaniu zostanie przedstawiony zarys teoretyczny inwigilacji, oraz według jakich aspektów prawnych inwigilacja jest zjawiskiem, które łamie prawo do prywatności. Następnie zostaną przedstawione dwie ustawy, które polski rząd wprowadził w ostatnich latach, a które dotyczą inwigilacji. Ustawy znacząco ułatwiły proces inwigilacji m.in. w sieci polskim organom ścigania oraz instytucjom bezpieczeństwa, co wywołało wiele burzliwych komentarzy na ten temat wśród obywateli. Dalej przeanalizowany zostanie proces inwigilacji stosowany przez największe firmy cyfrowe oraz ich wpływ na bezpieczeństwo danych użytkowników na przykładzie największego portalu społecznościowego, jakim jest Facebook, a w końcowej części rozdziału omówione będą podstawowe zasady, jakimi należy się kierować, by skutecznie chronić się przed inwigilacją.

## Inwigilacja – zarys teoretyczny

Inwigilacja jest to zespół czynności stosowanych do tajnej obserwacji, śledzenia zachowań ludzkich, działań lub informacji w celu wywierania wpływu, zarządzania lub kierowania. Najczęściej obserwacja jest prowadzona na odległość za pomocą sprzętów elektronicznych. Jest ona wykorzystywana w państwach totalitarnych jako narzędzie do nadzorowania obywateli i ingerowania w ich życie, jednak i w państwach demokratycznych coraz częściej znajduje zastosowanie do

gromadzenia danych wywiadowczych, zapobiegania przestępczości, ochrony procesu, osoby, grupy lub przedmiotu lub dochodzenia w sprawie przestępstwa. Jest również wykorzystywana przez organizacje przestępcze do planowania i popełniania przestępstw, przez przedsiębiorstwa do gromadzenia danych wywiadowczych na temat ich konkurentów, dostawców lub klientów oraz największe portale społecznościowe, które posiadają największe skupisko danych osobowych i wykorzystują je do wydobycia użytecznych informacji, takich jak osobiste zainteresowania, przyjaźnie i powiązania, potrzeby, przekonania, przemyślenia i działania. Przez największe organizacje pozarządowe dotyczące praw człowieka jak ONZ czy HRW poprzez inwigilacje jest łamane prawo do prywatności i staje się jednym z zagrożeń dla wolności słowa[1].

## Inwigilacja w sieci – aspekty prawne

Inwigilacja jest dosyć nowym zjawiskiem, lecz w ostatnich latach stała się głównym tematem dyskusji oraz wyrazem niezadowolenia wśród obywateli, co przyczyniło się również do fali protestów. Rozchodzi się o już wcześniej wspomniane prawo do prywatności, które według największych organizacji pozarządowych dotyczących praw człowieka jest wymieniane jako jeden z podstawowych praw człowieka. Według Powszechnej Deklaracji Praw Człowieka (art. 12) „Nikt nie może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję ani też atakom na jego honor i dobre imię. Każdy człowiek ma prawo do ochrony prawnej przeciwko takim ingerencjom i atakom”[2]. Dodatkowo prawo do prywatności jest wymieniane w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych (art. 17), Konwencji o Ochronie Prawo Człowieka i Podstawowych Wolności (art. 8), Karty Praw Podstawowych UE (art. 7). W Polsce prawo do prywatności zostało dokładnie opisane w Konstytucji RP z 1997r. (art. 47–51). Według art. 47 „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”. Konstytucja również wymienia wyjątki od odstąpienia z konstytucyjnych praw. Art. 31 ust 3 mówi „Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw”[3].

---

[1] https://en.wikipedia.org/wiki/Surveillance#cite_note-3 (dostęp: 08.05.2020 r.).

[2] Powszechna Deklaracja Praw Człowieka ONZ z dnia 10 grudnia 1948 r. (rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) )

[3] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. z 1997 r., nr 78, poz. 483).

Główne zagrożenia dotyczące prawa to prywatności to[4]:

- działania służb i administracji państwowej,
- zbieranie danych przez firmy,
- nadzór nad pracownikami,
- Internet i telefonia komórkowa,
- monitoring wizyjny,
- rozwój biometrii.

W polskim prawie początki inwigilacji miały miejsce w 2003 roku, kiedy to operatorzy telekomunikacyjni zostali zmuszeni przez Policję oraz służby specjalne do przechowywania oraz udostępniania im danych telekomunikacyjnych. Policja oraz służby specjalne miały wolną rękę w zakresie stosowania podsłuchów i pozyskiwania danych telekomunikacyjnych oraz określania katalogu zbieranych informacji i tryb ich niszczenia. Sytuacja taka miała miejsce do 2011 roku, kiedy prokurator generalny oraz Rzecznik Praw Obywatelskich zaskarżyli do Trybunału Konstytucyjnego przepisy dotyczące kompetencji inwigilacyjnych polskich instytucji bezpieczeństwa.

W 2014 r. Trybunał Konstytucyjny wydał orzeczenie, w którym zgodził się z faktem, iż sięganie przez służby oraz inne instytucje bezpieczeństwa bez jakiejkolwiek kontroli są niezgodne z konstytucją oraz wskazał 8 punktów, które należy zmienić w polskim prawie dotyczącym prawa do prywatności. Zgodnie z prawem Orzeczenie Trybunału Konstytucyjnego miało wejść w życie po upływie 18 miesięcy. Tyle czasu miał zatem rząd, by wprowadzić zmiany prawne. Jako że był to okres zbliżających się wyborów, prace nad zmianą ustawy rozpoczął ówczesny rząd PO, natomiast po wyborach, które wygrało PiS, powstał nowy projekt ustawy, który był bardzo podobny do tego sprzed wyborów. Tak ukształtowana reforma nie spełniła oczekiwań dotyczących kontroli nad dostępem do danych przez służby oraz instytucje bezpieczeństwa. Ustawa weszła w życie 7 lutego 2016 r. i została określona „ustawą inwigilacyjną". Reforma spotkała się z powszechną krytyką ze strony organizacji pozarządowych, Rzecznika Praw Obywatelskich, Naczelnej Rady Adwokackiej czy Biura Analiz Sejmowych. Nawet Biuro Trybunału Konstytucyjnego wydało oświadczenie, z którego wynika, że ustawa nie realizuje wyroku Trybunału Konstytucyjnego. Doszło również do fali protestów ze strony obywateli[5].

## Ustawa „inwigilacyjna"

Przyjęta ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw wprowadziła trzy fundamentalne zmiany dotyczące uprawnień

[4] https://panoptykon.org/sites/default/files/prawo-do-prywatnosci_kliniki_prezentacja.pdf (dostęp: 08.05.2020 r.).

[5] A. Nyzio, *Wokół „ustawy inwigilacyjnej". Geneza, przepisy i konsekwencje Ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*, „Jagielloński Przegląd Bezpieczeństwa" 2017, nr 1.

służb do pozyskiwania danych. Był to ułatwiony dostęp do danych internetowych, został wprowadzony pozorny system kontroli nad pobieraniem danych przez służby oraz została zmniejszona jeszcze bardziej przejrzystość działań służb. Oznaczało to, że nie dość, że ustawa nie zwiększyła aspektów dotyczących prywatności, to dodatkowo ułatwiła proces inwigilacji służbom oraz instytucjom[6].

Służby w ramach tzw. ustawy inwigilacyjnej uzyskały wszelaki dostęp do danych internetowych z tzw. bezpiecznego łącza od firm internetowych co oznacza brak jakichkolwiek ograniczeń z dostępem do masowej ilości danych. Przed wprowadzeniem ustawy dana instytucja musiała mieć powód, by moc uzyskać dane w postaci np. wykazania prowadzonego postepowania. Obecna reforma stanowi, iż sięganie po dane staje się możliwe „w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych", co nie określa konkretnych powodów pozyskania danych. Następna kwestia dotyczy rodzajów danych. W ustawie nie zostało określone, jakie typy danych mogą pobierać służby, co może oznaczać, iż w ich posiadaniu mogą znaleźć się dane niemające nic wspólnego z daną sprawą[7].

Cały mechanizm został poddany pozornej kontroli ze strony sądów. Dana instytucja w ramach takiej kontroli przekazuje sprawozdanie odpowiedniemu sądowi w okresach półrocznych, w których wykazuje liczbę pozyskania danych ich rodzaj, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane. Wyjątkiem w tej sprawie są dane abonenckie, które zostały odłączone z możliwości kontroli. W praktyce taki rodzaj kontroli może budzić wiele wątpliwości. Wynika to z faktu, iż sądy nie są w stanie poprawnie skontrolować działań dostając raporty co 6 miesięcy w masowych ilościach. Ustawa również nie nakłada obowiązku na sądy weryfikacji zasadności pobierania danych przez instytucje. Sędziowie mają w tej w kwestii pełną swobodę, co może oznaczać różny sposób kontroli ze strony różnych sądów.

Fundacja Panoptykon w 2017 r przeprowadziła badania dotyczące weryfikacji działań sądów w ramach kontroli instytucji. W większości przypadków sądy odmówiły udostepnienia informacji, natomiast udało się uzyskać informacje m.in z sądów okręgowych w Poznaniu oraz Gdańsku, gdzie tylko na podstawie suchych danych z tabel, z których nie wynika, czy pobieranie danych było konieczne, sądy uznały ich zasadność. Kwestia danych abonenckich również jest kontrowersyjna, ponieważ np. Policja może interesować się takimi danymi jak (np. imię i nazwisko, numer konta, adres zamieszkania, nr telefonu) bez jakichkolwiek ograniczeń oraz kontroli[8].

Ostatnią istotną kwestią, jaką zmieniła tzw. ustawa inwigilacyjna, jest ograniczenie zakresu publicznie dostępnych informacji o tym, jak często i po jakie kategorie danych telekomunikacyjnych sięgają uprawnione organy. Oznacza to, że

---

[6] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. z 2016 r., poz. 147).

[7] W. Klicki, *Rok z ustawą inwigilacyjną*, Fundacja Panoptykon, Warszawa 2017, s. 3–5.

[8] Tamże, s. 5–8.

zwykły obywatel nie uzyska już tego typu informacji w drodze dostępu do informacji publicznej i jest to argumentowane ochroną informacji niejawnych. Taka zmiana bardzo ogranicza kontrole społeczną nad funkcjonowaniem instytucji[9].

### Ustawa antyterrostyczna

Zaledwie pół roku po wejściu w życie ustawy „inwigilacyjnej" Sejm uchwalił kolejną ustawę zwiększającą kompetencje organów ścigania względem prywatności obywatela. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych skupia nowe uprawnienia instytucji bezpieczeństwa, a szczególnie ABW w kwestii inwigilacji. Nowe przepisy mają charakter zapobiegawczy względem zagrożeń terrorystycznych które w ostatnich latach przybrały szczególnie niebezpieczny charakter. Ustawa wchodziła w życie niedługo przed takimi wydarzeniami jak szczyt NATO oraz Światowe Dni Młodzieży, co było dodatkowym powodem, lecz sama ustawa jest nieprecyzyjna, dając wiele kompetencji władzom w kwestii inwigilacji oraz budząc wiele wątpliwości[10].

Według nowej reformy szef ABW wobec cudzoziemca może samodzielnie zadecydować o założeniu podsłuchu, zainstalowaniu kamery w domu albo uzyskać dostęp do korespondencji na e-mailu. Dodatkowo ABW, Policja oraz Straż Graniczna uzyskały uprawnienia do pobierania obrazu linii papilarnych, utrwalania wizerunku twarzy, a nawet materiału biologicznego (DNA) od cudzoziemców. Ustawa zmieniła również zasady sięgania po dane z baz danych publicznych różnych instytucji. Są one pobierane za pomocą teletransmisji, co oznacza utworzenie tzw. stałego łącza przez wszystkie instytucje publiczne oraz brak jakiejkolwiek kontroli w tym zakresie. ABW uzyskała również dostęp do kamer umieszczonych we wszystkich obiektach użyteczności publicznej. Po wejściu w życie ustawy zmienił się również sposób kupowania karty SIM. Konkretnie chodzi o rejestrację abonentów tzw. telefonicznych usług przedpłaconych. Oznacza to ze operatorzy komórkowi nie sprzedadzą takiej karty SIM bez weryfikacji oraz zapisania naszych danych osobowych, natomiast osoby, które posiadały taką kartę w dniu wejścia reformy dostały odpowiedni czas, by taką kartę zarejestrować u operatora komórkowego[11].

## GAFAM – światowy król danych

Analizując ww. ustawy można śmiało stwierdzić, że polskie służby mają bardzo szeroki zakres możliwości w kwestii dostępu do danych obywateli w szczególności jeśli chodzi o Internet. Służby wraz z wejściem w życie ustawy z dnia 15

---

[9] Tamże, s. 5–8.

[10] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2016 r., poz. 904).

[11] W. Klicki, *Ustawa antyterrorystyczna wchodzi w życie – co się zmienia*, „panoptykon.org", 01.07.2016, https://panoptykon.org/wiadomosc/ustawa-antyterrorystyczna-wchodzi-w-zycie-co-sie-zmienia (dostęp: 08.05.2020 r.).

stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw uzyskały wszelaki dostęp do danych internetowych z tzw. bezpiecznego łącza od firm internetowych, co oznacza brak jakichkolwiek ograniczeń z dostępem do masowej ilości danych. Sprawa ma się trochę inaczej, jeśli chodzi już o globalne korporacje cyfrowe. W tej kwestii polski rząd nie ma żadnych praw, a to takie firmy jak GAFAM posiadają największą ilość danych dotyczących miliardów ludzi.

GAFAM, czyli Google, Apple, Facebook, Amazon oraz Microsoft to największe firmy cyfrowe, które również są na szczycie największych spółek publicznych na świecie. Są to firmy, które zbudowały ogromną infrastrukturę zajmującą się obserwowaniem, analizowaniem i badaniem zachowań użytkowników, a następnie profilowaniem przy użyciu AI (sztucznej inteligencji), która na podstawie gromadzonych o nas danych próbuje przewidzieć nasze przyszłe potrzeby i preferencje oraz dostosować reklamy i pozycjonowanie treści pod konkretnego użytkownika. Coraz chętniej korzystamy z narzędzi, jakie udostępnia nam cyfrowy rynek: portale społecznościowe, komunikatory, sklepy internetowe oraz masa innych aplikacji, które są nam podsuwane, sprawiają, że sami pozbawiamy się prywatności oraz niezależności. Współczesna technologia doprowadziła do sytuacji, w której świat nie potrafiłby funkcjonować bez Internetu, natomiast Internet bez GAFAM, co oznacza brak jakiejkolwiek możliwości reakcji na tego typu proces inwigilacji[12].

Abstrahując już od inwigilacji danych przez GAFAM służącej do działań komercyjnych, warto przyjrzeć się bliżej polityce prywatności stosowanej przez ww. firmy. By najlepiej zobrazować ten proces, najlepszym przykładem będą portale społecznościowe, czyli Facebook. Jak wiadomo, na portalach społecznościowych przetwarzana jest masa informacji zarówno dotyczących danych osobowych użytkowników, jak i informacji wynikających z aktywności użytkownika (zdjęcia, prywatne wiadomości, dane kontaktowe, recenzje, opinie, komentarze). Wiąże się to z tym, iż użytkownicy chcą mieć kontrolę nad tym, jakie informacje są udostępniane co musi im zapewnić Facebook.

Po uchwaleniu RODO przez Komisję Europejską, zmienił się sposób polityki prywatności w wielu obszarach, a jednym z nich jest Facebook. By mógł on legalnie przetwarzać dane osobowe, muszą zostać spełnione pewne wymagania takie jak[13]:

- przetwarzane dane muszą być niezbędne do świadczenia usługi i sprecyzowane w treści umowy z osobą prywatną,
- wymagana jest dobrowolna, określona, świadoma i jednoznaczna zgoda w postaci wyraźnego potwierdzenia,
- użytkownik ma prawo do cofnięcia zgody, na co należy zwrócić mu uwagę,
- zgoda musi być wyrażona przez osobę, która jest w wieku wymaganym przez państwo członkowskie – w przeciwnym razie musi zostać udzielona przez rodzica lub opiekuna,

[12] K. Szymielewicz, *Władcy Danych/ Europa Kontra GAFA*, „polityka.pl", 10.03.2020.
[13] https://www.facebook.com/business/gdpr (dostęp: 08.05.2020 r.).

- w przypadku przetwarzania niektórych danych (np. określonych kategorii danych osobowych) wymagana jest wyraźna zgoda,
- jeżeli firma lub podmiot zewnętrzny ma prawnie uzasadnione interesy, w stosunku do których charakteru nadrzędnego nie mają prawa lub interesy osób prywatnych,
- przetwarzanie musi zostać wstrzymane, jeżeli sprzeciw zgłasza osoba prywatna.

Dodatkowo Facebook przedstawił 7 zasad prywatności, którymi się kieruje w działaniach dotyczących danych[14]:

- Facebook zapewnia kontrolę nad prywatnością.
- Portal pomaga ludziom zrozumieć, co dzieje się z ich danymi.
- Od samego początku tworzona jest prywatność produktów.
- Serwis dokłada wszelkich starań, aby dane były bezpieczne.
- Użytkownik jest właścicielem danych i może je usunąć.
- Poprawa jest stała.
- Facebook jest odpowiedzialny.

W ramach tych zasad zostały wprowadzone zmiany dotyczące ustawień prywatności, według których można wybierać, kto może zobaczyć nasze posty, w jaki sposób nasz profil może być wyszukany przez innych użytkowników, kto może wysyłać zaproszenia do znajomych oraz szereg innych ustawień dotyczących bezpieczeństwa danych. Nie oznacza to jednak, że użytkownicy mogą się czuć bezpieczni, gdyż na przestrzeni ostatnich lat doszło do poważnych wycieków danych z Facebooka.

W kwietniu 2018 r. wyciekły dane 87 mln użytkowników, w tym 57 tys. osób z Polski. Jak się później okazało, to firma Cambridge Analytica, która zajmowała się konsultingiem politycznym, pozyskała dane kilkudziesięciu milionów użytkowników Facebooka. Były one wykorzystywane do profilowania użytkowników pod kątem preferencji wyborczych i wpływania na ich polityczne decyzje. Następnie, we wrześniu 2018 r. doszło do kolejnego ataku hakerskiego, w którym hakerzy mogli wejść w posiadanie wrażliwych danych z kont 50 mln użytkowników poprzez lukę w zabezpieczeniu serwisu. Niedawno natomiast mass media szeroko komentowały informację o wycieku danych z 267 mln kont na Facebooku. Dane dotyczyły: adresu e-mail, imię i nazwisko, numeru telefonu, identyfikatora, informacje o ostatnim połączeniu wykonanym za pośrednictwem Messengera, status konta oraz datę urodzenia. Dane te zostały wystawione na sprzedaż przez hakerów na czarnym rynku za 623 euro, co świadczy o poziomie zagrożenia[15].

---

[14] M. Kuchta-Nykiel, *Facebook po raz pierwszy prezentuje zasady prywatności*, „socialpress.pl", 29.01.2018 r., https://socialpress.pl/2018/01/facebook-po-raz-pierwszy-prezentuje-zasady-prywatnosci (dostęp: 08.05.2020 r.).

[15] *Facebook pozwany w związku ze skandalem Cambridge Analytica*, „ businessindiser.com.pl", 2018, https://businessinsider.com.pl/media/internet/afera-cambridge-analytica-facebook-pozwany/edv34d2 (dostęp: 08.05.2020 r.); *Atak hakerski na Facebooka. 50 milionów użytkowników zagrożonych utratą danych,* "wirtualmedia.pl",2018, https://www.wirtualnemedia.pl/artykul/atak-

# Jak bronić się przed inwigilacją w sieci

Inwigilacja w sieci to stosunkowo nowe zjawisko, które jednak na przestrzeni ostatnich lat stanowi coraz większe zagrożenie dotyczące prawa do prywatności. Ustawy „inwigilacyjne" oraz zagrożenia wynikające z korzystania z różnych portali społecznościowych, komunikatorów czy innych serwisów, w których dane są masowo przetwarzane, sprawiają, że należy wiedzieć, jak się skutecznie bronić przed inwigilacją. Podstawą w tym zakresie jest przede wszystkim mądre korzystanie z komputera bądź telefonu.

Dotyczy to takich kwestii jak[16]:

- Nie należy otwierać niezapowiedzianych załączników i podejrzanych linków, zwłaszcza od mniej znanych osób.
- Nie należy instalować zbędnych aplikacji od niezaufanych producentów.
- Należy unikać używania pendrive'ów USB, a komputer i telefon trzeba wyposażyć w aktualne oprogramowanie antywirusowe.
- Nie należy używać tych samych haseł do różnych serwisów.

Dodatkowo warto wykonać kilka posunięć, które pozwolą nam zabezpieczyć się przed potencjalną inwigilacją. By skutecznie chronić dane na komputerze, warto je szyfrować. Na zwykłym komputerze z Windowsem można skorzystać z narzędzi do szyfrowania Microsoft BitLocker. Jeżeli komputer nie posiada takich narzędzi, to wystarczy zainstalować oprogramowanie open source typu TrueCrapt. Nie jest ono w 100% skuteczne, natomiast pozwoli zaszyfrować dane z dysku przed nieproszonymi gośćmi. W przypadku urządzeń mobilnych wystarczy włączyć szyfrowanie wchodząc w ustawienia zabezpieczeń. Warto również pomyśleć nad zmianą przeglądarki internetowej oraz poczty e-mail, która pozwoli zwiększyć bezpieczeństwo. Przeglądarka Tor Browser korzysta z trasowania cebulowego i zapobiega analizie ruchu sieciowego, a co za tym idzie – daje prawie anonimowy dostęp do zasobów Internetu. Jeżeli chodzi o pocztę e-mail, to wyróżniają się dwie usługi pocztowe: ProtonMail i Tutanota. Obie skrzynki pocztowe działają w oparciu o mocne zabezpieczenia i silne szyfrowanie danych[17].

Korzystając z portali społecznościowych oraz komunikatorów (Facebook, Messenger) również warto wdrożyć pewne działania. Przede wszystkim należy

---

hakerski-na-facebooka-50-milionow-uzytkownikow-zagrozonych-utrata-danych-dlaczego (dostęp: 08.05.2020 r.); *Hakerzy wystawili na sprzedaż dane 267 mln kont z Facebooka*, „cyberdefence24.pl", 2020, https://www.cyberdefence24.pl/hakerzy-wystawili-na-sprzedaz-dane-267-mln-kont-z-facebooka (dostęp: 08.05.2020 r.).

[16] D. Jemielniak, *Kilka porad jak uniknąć inwigilacji w sieci (po wprowadzeniu noweli policyjnej)*,"polityka.pl", 2016, https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1647758,1,kilka-porad-jak-uniknac-inwigilacji-w-sieci-po-wprowadzeniu-noweli-policyjnej.read (dostęp: 08.05. 2020 r.).

[17] M. Nowak, *Jak zabezpieczyć komputer, telefon, pocztę i komunikator przed rządową inwigilacją – poradnik dla początkujących*, „spidersweb.pl", 2016, https://www.spidersweb.pl/2016/01/ustawa-inwigilacyjna-szyfrowanie-danych-ochrona-prywatnosci-poradnik.html (dostęp: 08.05. 2020 r.).

przejrzeć dokładnie ustawienia zwracając szczególną uwagę na te związane z bezpieczeństwem, logowaniem, prywatnością, aplikacjami i reklamami oraz chronić dane z zakładki informacje. Dodatkowo warto ukryć dostępność na chacie, zaktualizować listę znajomych oraz wyłączyć wyszukiwanie profilu w przeglądarkach spoza Facebooka[18].

## Podsumowanie

Tematem rozważań było przedstawienie kwestii związanych z inwigilacją w sieci. Interpretacja polskich ustaw, które weszły w życie w ostatnich latach, potwierdziła słuszność tezy, iż można je nazwać ustawami „inwigilacyjnymi", budzącymi wiele wątpliwości co do słuszności oraz łamania prawa prywatności. Zaprezentowane przykłady ustaw to nie są jedyne ustawy dotyczące inwigilacji, lecz zdecydowanie najbardziej kontrowersyjne oraz szczegółowe. Również kontrowersyjna staje się kwestia inwigilacji ze strony światowych firm cyfrowych. Nie podlega wątpliwości fakt, iż koncerny cyfrowe wykorzystują dane miliardów ludzi, by wykorzystywać je do działań komercyjnych, doprowadzając do absurdalnych sytuacji, w których użytkownik jest atakowany z każdej strony reklamami ustawionymi pod jego potrzeby.

Jednym z tych koncernów jest największy portal społecznościowy Facebook. Pokazano w tekście politykę prywatności stosowaną przez Facebooka oraz bezradność ich systemu, który doprowadził do dramatycznych skutków w postaci wykradzionych milionów danych przez hakerów.

Podsumowując, warto zauważyć, iż postęp technologiczny, jaki nastąpił na przestrzeni ostatnich lat, doprowadził do sytuacji, w której takie zjawiska jak inwigilacja stają się jednym z głównych zagrożeń. Dlatego nie powinny być one bagatelizowane, a w interesie każdego z nas jest skuteczna ochrona przed nimi.

## Bibliografia

Klicki W., *Rok z ustawą inwigilacyjną*, Fundacja Panoptykon, Warszawa 2017.

Nyzio A., *Wokół „ustawy inwigilacyjnej". Geneza, przepisy i konsekwencje Ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*, „Jagielloński Przegląd Bezpieczeństwa" 2017, nr 1.

Szymielewicz K., *Władcy Danych/Europa Kontra GAFA*, „polityka.pl", 10.03.2020.

## Prawodawstwo

Powszechna Deklaracja Praw Człowieka ONZ z dnia 10 grudnia 1948 r. (rezolucja Zgromadzenia Ogólnego ONZ 217 A (III))

[18] *Jak zwiększyć swoją prywatność na Facebooku?*, „ideaforce.pl", 2018, https://www.ideoforce.pl/wiedza/jak-zwiekszyc-swoja-prywatnosc-na-facebooku,172.html (dostęp: 08.05.2020 r.).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. z 1997 r., nr 78, poz. 483 ze zm.).

Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. z 2016 r., poz. 147).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2016 r., poz. 904).

# Netografia

*Atak hakerski na Facebooka. 50 milionów użytkowników zagrożonych utratą danych,*"wirtualmedia.pl",2018, https://www.wirtualnemedia.pl/artykul/atak-hakerski-na-facebooka-50-milionow-uzytkownikow-zagrozonych-utrata-danych-dlaczego

*Facebook pozwany w związku ze skandalem Cambridge Analytica*, „businessindiser.com.pl", 2018, https://businessinsider.com.pl/media/internet/afera-cambridge-analytica-facebook-pozwany/edv34d2

*Hakerzy wystawili na sprzedaż dane 267 mln kont z Facebooka, „*cyberdefence24.pl", 2020, https://www.cyberdefence24.pl/hakerzy-wystawili-na-sprzedaz-dane-267-mln-kont-z-facebooka

https://en.wikipedia.org/wiki/Surveillance#cite_note-3

https://panoptykon.org/sites/default/files/prawo-do-prywatnosci_kliniki_prezentacja.pdf

https://www.facebook.com/business/gdpr.

*Jak zwiększyć swoją prywatność na Facebooku?,* „ideaforce.pl", 2018, https://www.ideoforce.pl/wiedza/jak-zwiekszyc-swoja-prywatnosc-na-facebooku,172.html.

Jemielniak D., *Kilka porad jak uniknąć inwgilacji w sieci ( po wprowadzeniu noweli policyjnej),*"polityka.pl", 2016, https://www.polityka.pl/tygodnikpolityka/ludzieistyle/1647758,1,kilka-porad-jak-uniknac-inwigilacji-w-sieci-po-wprowadzeniu-noweli-policyjnej.read

Klicki W., *Ustawa antyterrorystyczna wchodzi w życie – co się zmienia*, „panoptykon.org", 01.07.2016, https://panoptykon.org/wiadomosc/ustawa-antyterrorystyczna-wchodzi-w-zycie-co-sie-zmienia

Kuchta-Nykiel M., *Facebook po raz pierwszy prezentuje zasady prywatności*, „socialpress.pl", 29.01.2018 r., https://socialpress.pl/2018/01/facebook-po-raz-pierwszy-prezentuje-zasady-prywatnosci

Nowak M., *Jak zabezpieczyć komputer, telefon, pocztę i komunikator przed rządową inwigilacją – poradnik dla początkujących*, „spidersweb.pl", 2016, https://www.spidersweb.pl/2016/01/ustawa-inwigilacyjna-szyfrowanie-danych-ochrona-prywatnosci-poradnik.html

# BEZPIECZEŃSTWO W RUCHU POWIETRZNYM W KONTEKŚCIE ZMIAN PRAWNYCH DOTYCZĄCYCH BEZZAŁOGOWYCH STATKÓW POWIETRZNYCH

(*Dagmara Florek-Klęsk*)

## Wprowadzenie

Na przestrzeni ostatnich lat rośnie liczba firm produkujących bezzałogowe statki powietrzne, potocznie zwane dronami, jak i liczba ich użytkowników. Wraz z pojawieniem się dronów, pojawiły się nowe zagrożenia dla uczestników ruchu powietrznego, ze strony nieodpowiedzialnych użytkowników dronów. Z tego też względu ustawodawcy poszczególnych państw członkowskich Unii Europejskiej indywidualnie regulowali kwestię użytkowania dronów. Niemniej jednak, ze względu na globalny zasięg problemu, niezbędne stało się uregulowanie tej kwestii w sposób jednolity dla wszystkich krajów członkowskich Unii Europejskiej. Czerpiąc z doświadczeń i najlepszych praktyk z całego świata, wypracowano rozwiązania mające na celu poprawę bezpieczeństwa i otwarcie granic dla branży bezzałogowej w UE.

## Dron, czyli bezzałogowy statek powietrzny – definicja

Drony cieszą się globalną popularnością, a ich wszechstronne zastosowanie przysparza im coraz więcej amatorów. Z roku na rok, jak również w obliczu nieznanych dotychczas okoliczności, jak pandemia wirusa COVID-19, wzrastają możliwości uch zastosowania – począwszy od przenoszenia różnego rodzaju przedmiotów z miejsca na miejsce, poprzez wykorzystanie z tego urządzenia do tworzenia filmów, czy odnajdywania interesujących/poszukiwanych obiektów. Urządzenie to stało się nie tylko bardzo popularnym, ale i niezbędnym narzędziem pracy dla szczególnych grup zawodowych, jak np. Policji, straży pożarnej, wojska, ratowników, dziennikarzy, filmowców.

Fachowa nazwa dronów to bezzałogowe statki powietrzne (UAV). Niemniej jednak na chwilę obecną brak jest jednolitej definicji tego urządzenia, jak i jego nazwy, stąd też dokonując analizy słownikowej omawianego zagadnienia, należy zawęzić poszukiwania do hasła „dron", gdyż pod pojęciem „bezzałogowy statek powietrzny" możemy się natknąć na definicję np. balonu.

Termin „bezzałogowe statki powietrzne" zaczął się pojawiać w zagranicznej literaturze przedmiotu dopiero na początku lat 90. XX wieku. Jedne z pierwszych definicji opisywały bezzałogowe statki powietrzne jako „napędzane statki powietrzne, które nie mają na pokładzie człowieka operatora, wykorzystujące siłę nośną do utrzymania się w powietrzu, mogące samodzielnie latać według programu ustalonego przed startem lub być zdalnie sterowane, mogące być ponownie użyte oraz potrafiące przenosić uzbrojenie lub inne wyposażenie"[1]. Pomimo upływu czasu powyższa definicja, po dokonaniu niewielkich modyfikacji, jest nadal aktualna.

Literatura przedmiotu najczęściej odwołuje się natomiast do słownika terminów i definicji NATO AAP-6 z 2014 r., gdzie w miejsce dotychczas używanego terminu *drone* (rozumianego jako samodzielny pojazd bezzałogowy), wprowadzono nowy – *remotely piloted aircraft* (zdalnie sterowany statek powietrzny). Termin ten do dnia dzisiejszego nie został zmieniony i oznacza „bezzałogowy statek powietrzny kierowany ze stanowiska zdalnego sterowania przez operatora przeszkolonego i certyfikowanego według standardów ustalonych dla pilotów załogowych statków powietrznych"[2]. Od czasu wprowadzenia zmian definicja ta pozostała bez zmian.

W równie kompleksowy sposób do omawianego zagadnienia odnosi się dokument Joint Doctrine Note 2/11: the UK Approach to Unmanned Aircraft Systems[3] opublikowany przez Ministerstwo Obrony Narodowej Wielkiej Brytanii w marcu 2011 r. Zgodnie z tym dokumentem, przez „bezzałogowy statek powietrzny" (*unmanned aircraft*) rozumie on „statek powietrzny bez pilota na pokładzie, sterowany zdalnie za pomocą systemów o różnym stopniu automatyzacji, wielokrotnego użytku, mogącego przenosić śmiercionośne lub nieśmiercionośne ładunki". W obliczu problemów z uniwersalnym zastosowaniem powyższego terminu w niektórych sytuacjach wskazane jest użycie pojęcia „zdalnie sterowany statek powietrzny" (*remotely piloted aircraft*). Służy to podkreśleniu, że człowiek w każdym momencie kontroluje maszynę, w szczególności w przypadku misji bojowych, w których wykorzystywane są rakiety Hellfire lub inne środki rażenia[4].

Bezzałogowy statek powietrzny jest jedynie jednym z elementów większego systemu. Na prawidłowe bowiem funkcjonowanie drona składa się kilka czynników: urządzenie, umiejętności wykwalifikowanego operatora, oraz szereg podzespołów. W zależności od klasy urządzania oraz producenta, na taki system mogą

---

[1] M. Bucholc, *Bezzałogowe systemy powietrzne – wymiar współczesny i perspektywy* [w:] *Automatyzacja i robotyzacja pola walki wyzwaniem dla prawa międzynarodowego*, red. M. Szuniewicz, Gdynia 2015, s. 54.

[2] *Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO, AAP-6 (2017)*, s. 384, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf (dostęp: 11.10.2020 r.).

[3] *Joint Doctrine Note 2/11: the UK approach to unmanned aircraft systems (UAS)*, s. 46, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644084/20110505-JDN_2-11_UAS_archived-U.pdf (dostęp: 11.10.2020 r.).

[4] J. Chojnacki, D. Pasek, *Historia wykorzystania bezzałogowych statków powietrznych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, Vol. 11, nr 1, s. 176.

składać się różne składowe. I tak *Słownik terminów i definicji NATO AAP-6* zalicza do niego „bezzałogowy statek powietrzny, system wsparcia oraz całość personelu i wyposażenia niezbędnego do kierowania bezzałogowym statkiem powietrznym".

W tym miejscu warto też wskazać na słownikowe definicje. I tak dronem zgodnie z definicją *Słownika języka polskiego PWN* nazywamy „bezzałogowy statek latający, przeważnie niewielkich rozmiarów, sterowany zdalnie lub poruszający się zgodnie z zaprogramowaną trajektorią; wykorzystywany głównie w wojsku, coraz częściej także zastosowania cywilne"[5]. W *Słowniku Oxford University Press* znajdziemy zaś definicję, że dron to „zdalnie sterowany statek powietrzny lub pocisk"[6]. Zaś na stronach jednego z portali, których adresatami są operatorzy dronów można natrafić na definicję, iż dron to „bezzałogowy statek powietrzny, który może odbywać lot autonomiczny (samodzielnie, z użyciem autopilota lub innego systemu na pokładzie) lub zdalnie sterowany (kierowany przez operatora drona) poza zasięg wzroku"[7].

Podsumowując powyższe rozważania, należy wskazać że brak jest na chwilę obecną jednolitej definicji bezzałogowego statku powietrznego, gdyż w zależności od źródła definicje te mogą się od siebie znacznie różnić. Na potrzeby niniejszego opracowania znaczenie terminu bezzałogowy statek powietrzny w znacznym stopniu ograniczono do jego znaczenia w rozumieniu *Słownika terminów i definicji NATO* z 2014 roku, zaś określenia dron, czy bezzałogowiec należy traktować jako jego synonimy.

## Drony – regulacje prawne

Bezzałogowe statki powietrzne (drony) to szybko rozwijający się sektor lotnictwa o olbrzymim potencjale zatrudnieniowym i prowzrostowym. Dlatego też niezbędne są regulacje prawne, które w sposób bezpieczny włączą zdalnie sterowane drony do przestrzeni powietrznej. Na potrzeby niniejszego artykułu regulacje prawne zostały ograniczone jedynie do tych, które mają zastosowanie do dronów cywilnych. I tak aktami prawnymi regulującymi szczegółowo kwestię korzystania z tych urządzeń są w szczególności:

1. Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 26 marca 2013 r. w sprawie wyłączenia zastosowania niektórych przepisów ustawy – Prawo lotnicze do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków (Dz.U. z 2013 r., poz. 440);
2. Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. z 2013 r., poz. 1393);
3. Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody (Dz.U. z 2013 r., poz. 627);

[5] *Słownik języka polskiego PWN*, https://encyklopedia.pwn.pl/haslo/dron;5572794.html (dostęp: 11.10.2020 r.).
[6] https://en.oxforddictionaries.com/definition/drone (dostęp: 11.10.2020 r.).
[7] http://www.swiatdronow.pl/slownik (dostęp: 11.10.2020 r.).

4. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2014 r., poz. 121);
5. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. nr 88, poz. 553);
6. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. nr 90, poz. 631)
7. Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 26 kwietnia 2013 r. w sprawie przepisów technicznych i eksploatacyjnych dotyczących statków powietrznych kategorii specjalnej, nieobjętych nadzorem EASA (Dz.U. z 2013 r., poz. 524);
8. Rozporządzenie Ministra Infrastruktury i Rozwoju z dnia 22 stycznia 2015 r. w sprawie przepisów ruchu lotniczego (Dz.U. z 2015 r., poz. 141).
9. Rozporządzenie Ministra Infrastruktury z dnia 11 czerwca 2010 r. w sprawie zakazów lub ograniczeń lotów na czas dłuższy niż 3 miesiące (Dz.U. z 2010 r.);
10. Rozporządzenie Ministra Infrastruktury z dnia 25 listopada 2008 r. w sprawie struktury polskiej przestrzeni powietrznej oraz szczegółowych warunków i sposobu korzystania z tej przestrzeni (Dz.U. z 2014 r., poz. 351);
11. Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 3 czerwca 2013 r. w sprawie świadectw kwalifikacji (Dz.U. z 2013 r., poz. 664).

Ten szybko rozwijający się sektor lotnictwa na zasięg globalny. Dlatego UE przyjęła rozporządzenia, których zadaniem jest bezpieczne włączenie zdalnie sterowanych dronów do europejskiej przestrzeni powietrznej. Potrzeba zmian wynikała z faktu, że Unia Europejska posiadała kompetencje regulacyjne jedynie w odniesieniu do dronów o masie powyżej 150 kg, pozostawiając w kompetencji krajów członkowskich regulacje dotyczące lżejszych dronów. Podlegały one zróżnicowanym, rozdrobnionym krajowym przepisom bezpieczeństwa, z tym że nie były one stosowane spójnie. Ponadto, zgodnie z szacunkami Komisji Europejskiej, ruch lotniczy ma się zwiększyć w ciągu najbliższych 20 lat o połowę, zaś do 2035 roku sektor dronów będzie bezpośrednio zatrudniał ponad 100 000 osób i będzie miał oddziaływanie ekonomiczne rzędu ponad 10 mld EUR rocznie, głównie w usługach[8]. Z tego też powodu dokonanie ujednolicenia przepisów „prawa dronów" stało się niezbędne.

Europejska Agencja Bezpieczeństwa Lotniczego ujednoliciła przepisy i procedury dla dronów we wszystkich państwach członkowskich Unii Europejskiej. Czerpiąc z doświadczeń i najlepszych praktyk z całego świata, wypracowano rozwiązania mające na celu poprawę bezpieczeństwa i otwarcie granic dla branży bezzałogowej w UE. W związku z powyższym, w dniu 11 czerwca 2019 zostały opublikowane dwa rozporządzenia unijne odnoszące się do dronów, których zadaniem jest dokonanie ujednolicenia regulacji prawnych dotyczących dronów na terenie Unii Europejskiej. Są nimi:

[8] *Drony: reforma unijnego bezpieczeństwa lotniczego*, https://www.consilium.europa.eu/pl/policies/drones/ (dostęp: 11.10.2020 r.).

1. Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich[9];
2. Rozporządzenie wykonawcze KOMISJI (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych[10];
3. Rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych[11];
4. Rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19[12];
5. Rozporządzenie wykonawcze Komisji (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do scenariuszy standardowych dla operacji wykonywanych w zasięgu widoczności wzrokowej lub poza zasięgiem widoczności wzrokowe[13].

Rozporządzenia weszły w życie z początkiem lipca 2019 roku, zaś państwa członkowskie miały rok na wdrożenie w życie nowych przepisów. Zgodnie z pierwotnym założeniem od dnia 1 lipca 2020 roku miały przestać obowiązywać krajowe przepisy i procedury państw członkowskich UE, dedykowane dla cywilnych użytkowników bezzałogowych statków powietrznych, jednakże ze względu na pandemię wirusa COVID-19 termin stosowania nowych przepisów europejskich dotyczących dronów został przesunięty przez Komisję Europejską na 1 stycznia 2021 r. Do czasu obowiązywania nowych przepisów operatorów dronów obowiązują przepisy krajowe.

## Nowe regulacje prawne dotyczące dronów

Rozporządzenia wprowadzają tyle zmian, że można zaryzykować stwierdzeniem, że tworzą one nowy system. Jest to system opierający się w dużej mierze na doświadczeniach wynikających ze stosowania przepisów krajowych państw członkowskich UE, ale jest on całkowicie inny od znanego nam polskiego systemu. Ze względu na obszerność zmian, w niniejszym opracowaniu omówiono te najważniejsze z punktu widzenia producenta, jak i operatora drona.

---

[9] Dz. Urz. UE. L 152/1.
[10] Dz. Urz. UE. L 152/45.
[11] Dz. Urz. UE. L 232/1.
[12] Dz. Urz. UE. L 176/13.
[13] Dz. Urz. UE. L 150/1.

***Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12.03.2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich (zwane dalej rozporządzeniem delegowanym)***

Rozporządzenie delegowane wprowadza ujednolicone dla państw członkowskich Unii Europejskiej, jak i państw członków EASA podstawowe wymogi techniczne, które mają zastosowanie do bezzałogowych statków powietrznych wykorzystywanych zgodnie z wytycznymi określonymi w rozporządzeniu wykonawczym Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (zwanym dalej rozporządzeniem wykonawczym).

Rozporządzenie delegowane reguluje takie kwestie jak: projektowanie, produkcję i wprowadzanie do wewnętrznego obrotu UE BSP[14] wykonujących operacje w kategorii otwartej. Wraz z wprowadzeniem wymogów technicznych, BSP w kategorii otwartej zostają objęte nadzorem, którego mechanizmy w Polsce reguluje m.in. ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (tekst jedn. Dz.U. z 2019 r., poz. 544) oraz z dnia 30 sierpnia 2002 r. o systemie oceny zgodności (tekst jedn. Dz.U. z 2018 r., poz. 155).

Rozporządzenie delegowane zawiera najważniejsze informacje o wymogach technicznych dla BSP oraz zasadach działania przyszłego nadzoru nad rynkiem BSP zarówno w UE, jak i w Polsce. Ponadto określa zasady wprowadzania na rynek wewnętrzny UE oraz swobodnego przepływu w UE bezzałogowców dopuszczonych do lotów w tzw. kategorii otwartej.

Jedną z największych zmian będzie brak podziału na loty o charakterze sportowym lub rekreacyjnym oraz na loty inne niż sportowe i rekreacyjne. Dotychczasowe komercyjne wykorzystanie BSP możliwe jedynie dla posiadaczy świadectwa kwalifikacji operatora bezzałogowego statku powietrznego UAVO[15] w większości przypadków stanie się ogólnodostępne. Z drugiej strony, na użytkowników , którzy latają całkowicie dla zabawy, spadną dodatkowe obowiązki, które do tej pory ich nie dotyczyły.

Pojawi się klasyfikacja wykonywanych lotów, podzielona na kategorie: otwartą, szczególną oraz certyfikowaną. Podział został dokonany w oparciu o stopień ryzyka wykonywanych operacji lotniczych.

**Kategoria otwarta** przeznaczona będzie dla lotów wykonywanych w warunkach VLOS[16], o najniższym stopniu ryzyka. Niskie ryzyko mają zapewnić jasno określone zasady, definiujące między innymi dopuszczalne masy startowe eksploatowanych BSP, ich wyposażenie, prędkości lotu, maksymalną energię kinetyczną uderzenia czy odległość od pojedynczych osób, jak i zgromadzeń osób.

---

[14] BSP – bezzałogowy statek powietrzny.

[15] UAVO – świadectwo kwalifikacji operatorów dronów, uprawniające do ich wykorzystywania w celach innych niż loty sportowe i rekreacyjne.

[16] VLOS – zasięg widoczności wzrokowej.

W kategorii otwartej każda osoba chcąca latać dronem o masie powyżej 250 g będzie musiała przejść proste szkolenie online oraz zaliczyć test online potwierdzający zdobycie wymaganej wiedzy teoretycznej. Urząd Lotnictwa Cywilnego planuje opracowanie i udostępnienie takich szkoleń na swojej stronie internetowej. W związku z powyższym będą one łatwo dostępne dla szerokiego grona odbiorców. Dla wszystkich użytkowników dronów o masie powyżej 250 g, stworzony zostanie również internetowy system obowiązkowej rejestracji[17].

W samej kategorii otwartej zostanie dokonany dodatkowy podział na podkategorie A1, A2 i A3, gdzie między innymi zostaną wprowadzone zasady eksploatacji takie jak:

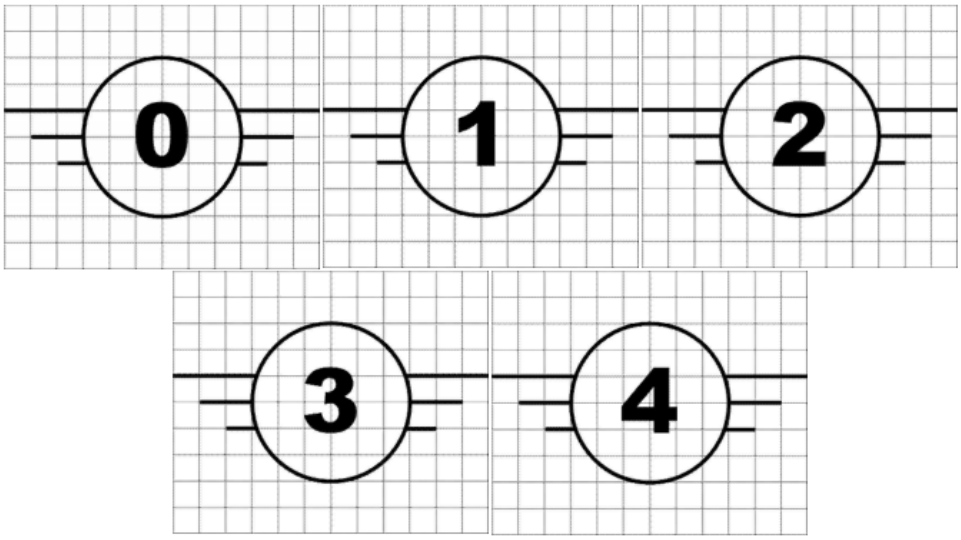
- limit wysokości wykonywanych lotów ustalony na 120 m;
- w przypadku BSP o masie startowej do 250 g (podkategoria A1) dopuszczane będą przeloty nad pojedynczymi osobami postronnymi, jednak nie nad zgromadzeniami osób;
- w przypadku BSP o masie startowej od 250 g do 900 g (podkategoria A1), nie będą dopuszczone loty nad zgromadzeniami osób, natomiast czas nieprzewidzianego przelotu nad pojedynczymi osobami postronnymi powinien być ograniczony w możliwie największym stopniu;
- bezzałogowce o masie startowej do 4 kg (podkategoria A2) będą wymagały od pilota uzyskania Certyfikatu Kompetencji Pilota BSP, będącego w pewnym zakresie odpowiednikiem obecnego świadectwa kwalifikacji UAVO. Aby otrzymać powyższy dokument będzie wymagane zaliczenie nadzorowanego egzaminu teoretycznego (aktualnie ULC jest na etapie ustalania z EASA[18], jak ma być realizowany taki egzamin), jak również oświadczenie o wystarczających umiejętnościach praktycznych. Podkategoria A2, dzięki powyższym wymaganiom umożliwi latanie w odległości poziomej 30 m od osób postronnych lub w odległości 5 metrów, jeżeli BSP posiada uruchomiony tryb niskiej prędkości, który będzie wymagany od BSP produkowanych w przyszłości;
- cięższe drony (podkategoria A3, od 4 do 25 kg) będą mogły być użytkowane jedynie w odległości minimum 150 m od ludzi i zabudowań.

Zgodnie z Częścią 1 Załącznika rozporządzenia delegowanego, dokonano podziału i opisu klas bezzałogowców. Zostały oznakowane kolejno: C0, C1, C2, C3, C4. A zatem nowe drony wprowadzane na unijny rynek sprzedaży będą musiały mieć oznakowanie zgodne z nowymi regulacjami. Będą to etykiety symbolizujące poszczególne klasy dronów i świadczące o ich zgodności z nowymi przepisami.

---

[17] Urząd Lotnictwa Cywilnego, dane za stroną https://www.ulc.gov.pl/pl/drony/wdrazanie-przepisow-ue/4718-informacje-ogolne (dostęp: 11.10.2020 r.).

[18] EASA – (ang. *European Aviation Safety Agency*) Europejska Agencja Bezpieczeństwa Lotniczego jest jednym z instytucjonalnych filarów europejskiego systemu bezpieczeństwa lotniczego obok Komisji Europejskiej, organizacji EUROCONTROL oraz krajowych władz lotniczych.




Rys. 1. Oznakowanie bezzałogowych statków powietrznych w ramach kategorii otwartej

Źródło: Część 1 Załącznika rozporządzenia delegowanego Komisji (UE) 2019/945.

Zgodnie z wymogami nowego prawa unijnego, klasy C0–C4 bezzałogowców powinny charakteryzować się następującymi specyfikacjami podanymi w tabeli 1.

Tabela 1. Specyfikacja bezzałogowych statków powietrznych w klasie otwartej

| | **C0** | **C1** | **C2** | **C3** | **C4** |
|---|---|---|---|---|---|
| **Waga** | < 250 g | < 900 g/ <80 J | < 4 kg | < 25 kg | < 25 kg |
| **Max prędkość** | < 19 m/s | < 19 m/s | - | - | - |
| **Max wysokość** | < 120 m | < 120 m | < 120 m | < 120 m | - |
| **Zasilanie** | < 24 V | < 24 V | < 48 V | < 48 V | - |
| **Zdalna identyfikacja** | NIE | TAK | TAK | TAK | - |
| **Świadomość przestrzenna** | NIE | TAK | TAK | TAK | - |
| **Oświetlenie** | NIE | TAK | TAK | TAK | - |
| **Ostrzeżenie o stanie baterii** | NIE | TAK | TAK | TAK | - |
| **Inne wymogi** | - | energia kinetyczna uderzenia < 80 J | wymagany tryb wolnego lotu < 3m/s | maksymalny typowy wymiar nie przekracza 3 m | brak trybów automatycznych, z wyjątkiem stabilizacji lotów |
| **Zastosowanie w kat. OPEN** | wszystkie podkategorie | wszystkie podkategorie | A2 i A3 | A3 | A3 |

Źródło: opracowanie własne na podstawie Części 1 Załącznika rozporządzenia delegowanego Komisji (UE) 2019/945.

Z kolei **kategoria szczególna** pozwoli na wykonywanie lotów niemieszczących się w wytycznych kategorii otwartej. Dopuszczone zostaną operacje zarówno w warunkach VLOS, jak i BVLOS[19]. Loty w kategorii szczególnej będą mogły odbywać się na podstawie:

1) oświadczenia o lotach według opublikowanego (przez EASA lub ULC) scenariusza standardowego lub
2) zgody wydanej przez Prezesa Urzędu Lotnictwa Cywilnego lub
3) uzyskanego certyfikatu LUC będącego Certyfikatem Operatora Lekkiego Bezzałogowego Systemu Powietrznego.

Scenariusze standardowe będą określać bardzo szczegółowo zasady wykonywanych lotów, wymagane parametry i wyposażenie BSP, jak również stopień wymaganego wyszkolenia personelu lotniczego. Operacje wykraczające poza dostępne scenariusze będą mogły być wykonane na podstawie jednorazowej zgody z ULC lub posiadanego certyfikatu LUC, który przeznaczony ma być dla podmiotów i świadczyć będzie o ich właściwym przygotowaniu do konkretnych operacji BSP.

**Kategoria certyfikowana** będzie oparta na certyfikacji w zakresie projektowania, produkcji i utrzymaniu zdatności do lotu bezzałogowych statków powietrznych (BSP o masie startowej powyżej 25 kg). Aktualnie oczekuje się na projekty odpowiednich regulacji.

Modelarze będą mogli latać na odrębnych zasadach, jednak w tym celu zrzeszeni w klubach lub stowarzyszeniach modelarstwa lotniczego będą musieli uzyskać zgodę i warunki od Urzędu Lotnictwa Cywilnego[20].

Rozporządzenie pierwotnie miało obowiązywać od 1 lipca 2020 roku, jednakże ze względu na pandemię COVID-19 przesunięto jego obowiązywanie i regulacje będą obowiązywać od 1 stycznia 2021 roku[21].

### *Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych*

Rozporządzenie to określa w dwóch artykułach 20 i 22 zasady przejściowe używania tzw. starych dronów. Zgodnie z art. 20 „Typy bezzałogowych systemów powietrznych w rozumieniu decyzji Parlamentu Europejskiego i Rady nr 768/2008/WE, które nie są zgodne z rozporządzeniem delegowanym (UE) 2019/945 i których nie skonstruowano do użytku prywatnego, mogą być nadal eksploatowane na następujących warunkach, jeżeli wprowadzono je do obrotu przed dniem 1 lipca 2022 r.:

---

[19] BVLOS – poza zasięgiem widoczności wzrokowej operatora.

[20] Urząd Lotnictwa Cywilnego, https://www.ulc.gov.pl/pl/drony/wdrazanie-przepisow-ue/4718-informacje-ogolne (dostęp: 11.10.2020 r.).

[21] Rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19.

a) w podkategorii A1 zdefiniowanej w części A załącznika, pod warunkiem że bezzałogowy statek powietrzny ma maksymalną masę startową wynoszącą mniej niż 250 g wraz z obciążeniem użytkowym;
b) w podkategorii A3 zdefiniowanej w części A załącznika, pod warunkiem, że bezzałogowy statek powietrzny ma maksymalną masę startową wynoszącą mniej niż 25 kg wraz z paliwem i obciążeniem użytkowym".

Art. 22 rozporządzenia stanowi zaś, że „Nie naruszając przepisów art. 20, użytkowanie w kategorii »otwartej« bezzałogowych systemów powietrznych, które nie spełniają wymogów określonych w częściach 1–5 załącznika do rozporządzenia delegowanego (UE) 2019/945, dopuszcza się w okresie przejściowym wynoszącym dwa lata, rozpoczynającym się rok po dacie wejścia w życie niniejszego rozporządzenia, z zastrzeżeniem następujących warunków:

a) bezzałogowy statek powietrzny o maksymalnej masie startowej mniejszej niż 500 g jest eksploatowany w graniach wymogów operacyjnych określonych w sekcji UAS.OPEN.020 pkt 1 w części A załącznika przez pilotów bezzałogowych statków powietrznych posiadających poziom kompetencji określony przez dane państwo członkowskie;
b) bezzałogowy statek powietrzny o maksymalnej masie startowej mniejszej niż 2 kg jest eksploatowany w taki sposób, że zachowywana jest minimalna odległość 50 metrów w poziomie od osób, a piloci bezzałogowych statków powietrznych posiadają poziom kompetencji co najmniej równorzędny poziomowi określonemu w sekcji UAS.OPEN.030 pkt 2 w części A załącznika;
c) bezzałogowy statek powietrzny o maksymalnej masie startowej większej niż 2 kg i mniejszej niż 25 kg jest eksploatowany w graniach wymagań operacyjnych określonych w sekcji UAS.OPEN.040 pkt 1 i 2, a piloci bezzałogowych statków powietrznych posiadają poziom kompetencji co najmniej równorzędny poziomowi określonemu w sekcji UAS.OPEN.020 pkt 4 lit. b) w części A załącznika".

Reasumując, po wejściu w życie niniejszego rozporządzenia wykonawczego (2019/947) i przez okres przejściowy wynoszący 2 lata „stare" drony będą mogły latać na zasadach określonych w **art. 22** oraz **art. 20** (co jest istotne szczególnie dla wagi <250 g). Następnie po zakończeniu okresu przejściowego (dwóch lat), czyli od dnia 1 lipca 2022 r. „stare" drony będą mogły dalej latać, ale na zasadach określonych w **art. 20.**

Zgodnie z treścią ww. przepisów, drony wprowadzone do obrotu przed 1.07.2022 r. w dniu 1.07.2020 r. rozpoczynają „okres przejściowy" wynoszący dwa lata, w którym – w zależności od swojej wagi (w przedziałach: <250 g z art. 20 oraz <500 g, <2 kg i <25 kg z art. 22) – mogą latać w kategorii otwartej na zasad poszczególnych podkategorii (A1, A2, A3). Po dwóch latach – od dnia 1.07.2022 r. te same „stare" drony znów będą miały zmienione warunki lotów, ale tym razem podział jest prostszy: <250 g i powyżej 250 g do 25 kg. Drony najlżejsze będą mogły latać w podkategorii otwartej A1, a wszystko pozostałe zostaje

oddalone od ludzi i terenów mieszkaniowych, użytkowych, przemysłowych lub rekreacyjnych na minimum 150 m odległości w poziomie. Przepis z art. 20 nie obejmuje konstrukcji dronów, które zostały przez modelarzy zrobione na użytek prywatny (niewprowadzone do obiegu/sprzedaży, jedynie do wykorzystania do własnych celów prywatnych)[22].

***Rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych***

Rozporządzenie to zmienia rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych. Rozporządzenie to wprowadza wymagania techniczne dla dwóch nowych klas dronów C5 i C6, dedykowanych do scenariuszy standardowy STS-01 oraz STS-02 do lotów w kategorii szczególnej. Rozporządzenie to weszło w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej[23].

***Rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19***

Nadzwyczajna sytuacja spowodowana przez epidemię COVID-19 spowodowała, że na prośbę państw członkowskich, w tym Prezesa Urzędu Lotnictwa, Komisja Europejska zadecydowała o zmianie daty stosowania rozporządzenia wykonawczego Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych. Zgodnie ze zmieniającym rozporządzeniem wykonawczym termin obowiązywania nowych przepisów, które pierwotnie miały być stosowane od 1 lipca 2020 r., został przesunięty o 6 miesięcy, co oznacza, że zaczną one obowiązywać od 31 grudnia 2020 roku. Zatem do czasu obowiązywania nowych przepisów europejskich, operatorów bezzałogowych statków powietrznych obowiązują dotychczasowe przepisy krajowe.

***Rozporządzenie wykonawcze (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 z dnia 24 maja 2019 r.***

W dniu 13 maja 2020 r. opublikowano rozporządzenie wykonawcze (UE) 2020/639 zmieniające rozporządzenie wykonawcze (UE) 2019/947. W rozporządzeniu tym wprowadzono dwa standardowe scenariusze: STS-01 i STS-0. Zgodnie z omawianym rozporządzeniem:

---

[22] *Świat dronów*, http://www.swiatdronow.pl/wprowadzenie-do-przepisow-ue-czesc-2-przepisy-dla-starych-dronow (dostęp: 11.10.2020 r.).

[23] *Świat dronów*, http://www.swiatdronow.pl/zmiana-2020-1058-do-rozporzadzenia-delegowanego-ue-2019-945 (dostęp: 11.10.2020 r.).

a) scenariusz STS-01 obejmuje: operacje w zasięgu widoczności wzrokowej VLOS nad kontrolowanym obszarem naziemnym w środowisku zaludnionym,
b) scenariusz STS-02 obejmuje: operacje poza zasięgiem widoczności wzrokowej BVLOS z udziałem obserwatorów przestrzeni powietrznej nad kontrolowanym obszarem naziemnym w środowisku słabo zaludnionym

Scenariusze te będą stosowane w Kategorii Szczególnej lotów, do której będą dopuszczeni operatorzy z wyższymi uprawnieniami (m.in. z obecnymi świadectwami kwalifikacji UAVO), które będą dopuszczać do realizacji lotów wg scenariuszy standardowych).

## Podsumowanie

Głównym celem przyświecającym stworzeniu regulacji unijnych było zapewnienie stałego, wysokiego poziomu bezpieczeństwa w lotnictwie. Regulacje unijne wprowadzają bardzo dużo zmian w dotychczas obowiązujących przepisach i można śmiało zaryzykować stwierdzenie, że tworzą one nowy system. System, który z jednej strony bazuje na doświadczeniach wynikających ze stosowania przepisów krajów państw członkowskich UE, z drugiej jest zupełnie odmienny od znanego nam systemu polskiego. Nowe regulacje prawne są bardzo ważne z punktu widzenia każdego operatora bezzałogowego statku powietrznego (obecnego, a także przyszłego), gdyż w istotnym stopniu zmieniają dotychczasowe regulacje zawarte w polskim prawie. Nowy system będzie na pewno wyzwaniem dla całego środowiska lotniczego, ale również szansą na poprawę bezpieczeństwa w ruchu powietrznym, a także na znaczny rozwój branży. Ujednolicenie wymogów dla pilotów w całej Unii ułatwi prowadzenie działalności poza granicami Polski, umożliwi wykonywanie lotów transgranicznych i wprowadzi wzajemne uznawanie certyfikatów kompetencji pilota bezzałogowego statku powietrznego.

## Bibliografia

Bucholc M., *Bezzałogowe systemy powietrzne – wymiar współczesny i perspektywy* [w:] *Automatyzacja i robotyzacja pola walki wyzwaniem dla prawa międzynarodowe*go, red. M. Szuniewicz, Gdynia 2015.

Chojnacki J., Pasek D., *Historia wykorzystania bezzałogowych statków powietrznych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, Vol. 11, nr 1.

## Prawodawstwo

Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich.

Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.

Rozporządzenie delegowane Komisji (UE) 2020/1058 z dnia 27 kwietnia 2020 r. zmieniające rozporządzenie delegowane (UE) 2019/945 w odniesieniu do wprowadzenia dwóch nowych klas systemów bezzałogowych statków powietrznych.

Rozporządzenie wykonawcze (UE) 2020/639 z dnia 12 maja 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 z dnia 24 maja 2019 r.

Rozporządzenie wykonawcze Komisji (UE) 2020/746 z dnia 4 czerwca 2020 r. zmieniające rozporządzenie wykonawcze (UE) 2019/947 w odniesieniu do odroczenia dat rozpoczęcia stosowania niektórych środków w związku z pandemią COVID-19.

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (Dz.U. z 2013 r., poz. 1393).

Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody (Dz.U. z 2013 r., poz. 627).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2014 r., poz. 121).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. nr 88, poz. 553).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. nr 90, poz. 631).

Rozporządzenie Ministra Infrastruktury z dnia 25 listopada 2008 r. w sprawie struktury polskiej przestrzeni powietrznej oraz szczegółowych warunków i sposobu korzystania z tej przestrzeni (Dz.U. z 2014 r., poz. 351).

Rozporządzenie Ministra Infrastruktury z dnia 11 czerwca 2010 r. w sprawie zakazów lub ograniczeń lotów na czas dłuższy niż 3 miesiące (Dz.U. z 2010 r.).

Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 26 marca 2013 r. w sprawie wyłączenia zastosowania niektórych przepisów ustawy – Prawo lotnicze do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków (Dz.U. z 2013 r., poz. 440).

Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 26 kwietnia 2013 r. w sprawie przepisów technicznych i eksploatacyjnych dotyczących statków powietrznych kategorii specjalnej, nieobjętych nadzorem EASA (Dz.U. z 2013 r., poz. 524).

Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 3 czerwca 2013 r. w sprawie świadectw kwalifikacji (Dz.U. z 2013 r., poz. 664).

Rozporządzenie Ministra Infrastruktury i Rozwoju z dnia 22 stycznia 2015 r. w sprawie przepisów ruchu lotniczego (Dz.U. z 2015 r., poz. 141).

# Netografia

*Drony: reforma unijnego bezpieczeństwa lotniczego*, https://www.consilium.europa.eu/pl/policies/drones/

http://www.swiatdronow.pl/slownik

https://en.oxforddictionaries.com/definition/drone

https://www.ulc.gov.pl/pl/drony/wdrazanie-przepisow-ue/4718-informacje-ogolne

*Joint Doctrine Note 2/11: the UK approach to unmanned aircraft systems (UAS)*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644084/20110505-JDN_2-11_UAS_archived-U.pdf

*Słownik języka polskiego PWN*, https://encyklopedia.pwn.pl/haslo/dron;5572794.html
*Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO, AAP-6 (2017)*, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf
*Świat dronów*, http://www.swiatdronow.pl/wprowadzenie-do-przepisow-ue-czesc-2-przepisy-dla-starych-dronow
*Świat dronów*, http://www.swiatdronow.pl/zmiana-2020-1058-do-rozporzadzenia-delegowanego-ue-2019-945

# NOWE TECHNOLOGIE W ZARZĄDZANIU BEZPIECZEŃSTWEM SYSTEMÓW LOGISTYCZNYCH W ASPEKCIE UMACNIANIA BEZPIECZEŃSTWA NARODOWEGO

(*Renata Piętowska-Laska*)

## Wprowadzenie

Współcześnie innowacyjne technologie, wielki rozwój cyfryzacji, automatyzacji i szeroki dostęp do najnowszych trendów w danej dziedzinie kreują teraźniejszość i modelują przyszłość nowoczesnych przedsiębiorstw, łańcuchów dostaw a patrząc szerzej umacniają bezpieczeństwo narodowe Polski. Efektywność funkcjonowania bezpieczeństwa narodowego w dużej mierze zależy od logistyki, która powinna być nowoczesna, a nade wszystko odporna na wszelkie zakłócenia i zagrożenia.

Logistyka, która ściśle jest sprzężona z podmiotami i instytucjami zaangażowanymi w system bezpieczeństwa narodowego, w literaturze przedmiotu jest nazywana logistyką bezpieczeństwa[1]. Udział logistyki w bezpieczeństwie narodowym dotyczy przede wszystkim podmiotów z sektora transportowego, infrastruktury (magazynowej, krytycznej), a także ochrony środowiska naturalnego, żywnościowego oraz sektora militarnego, ratowniczego, socjalnego, prawnego i porządku publicznego.

Wyniki ekonomiczne dowolnego podmiotu bezpieczeństwa zależą od wielu czynników, a zwłaszcza od wielopłaszczyznowych systemów informatyczno-technologicznych takich m.in. jak: najnowszej generacji programy informatyczne, urządzenia autonomiczne, systemy automatyczne, drony, technologia RFID (*Radio-Frequency Identification*), *Business Intelligence*, Logistyka 4.0, urządzenia Internetu rzeczy (IoT) oraz nowe technologie zwłaszcza w obszarze systemów logistyki produkcji (rodzina metod Pick-by) w przeważającej większości skoncentrowane na aspektach związanych z robotyzacją, rozszerzoną i wirtualną rzeczywistością.

[1] T. Jałowiec, *Logistyczne wymiary systemu bezpieczeństwa państwa*, „Logistyka" 2011, nr 2, s. 7.

## Zarządzanie bezpieczeństwem systemów logistycznych na potrzeby bezpieczeństwa narodowego

Zarządzanie bezpieczeństwem systemów logistycznych na potrzeby bezpieczeństwa narodowego to zestaw skoordynowanych działań, skierowanych na zbiór zasobów i łączących ich relacji, których celem jest przepływ zaplanowanego oraz zorganizowanego strumienia rzeczowego, a także usług logistycznych na korzyść podmiotów bezpieczeństwa. Sprowadza się ono między innymi do wdrożenia nowoczesnych rozwiązań ułatwiających zapobieganie, przygotowanie oraz reagowanie na zagrożenia procesów logistycznych realizowanych na rzecz podmiotów (instytucji) bezpieczeństwa. Tymi narzędziami są systemy informatyczne oparte o technologie internetowe. Pozwalają one prognozować i określać miejsce składowania zapasów, planować potrzeby materiałowe, dobierać transport, trasę przejazdu, obniżać koszty, zarządzać infrastrukturą i środkami trwałymi, co usprawnia realizację przedsięwzięć na rzecz podmiotów bezpieczeństwa zwłaszcza w sytuacji zagrożenia bezpieczeństwa narodowego[2]. Niezwykle pomocnym narzędziem w optymalizacji i skuteczności procesów logistycznych realizowanych na rzecz bezpieczeństwa narodowego jest automatyczna identyfikacja, która pozwala w trybie online śledzić wyroby, ich składowanie, zabezpieczać krytyczną infrastrukturę, w tym dostęp do budynków oraz systemów, w tworzeniu nowych poziomów bezpieczeństwa dla konsumentów w sektorze bankowym i zróżnicowanych usługach opartych na szybkim oraz skutecznym uwierzytelnianiu klienta w miejscu użytkowania. W obecnych czasach nie bez znaczenia dla bezpieczeństwa narodowego jest również: jakość, odporność na zakłócenia, użyteczność i terminowość informacji, które mogą zapewnić nowe technologie w obszarze logistyki zaopatrzenia, produkcji i dystrybucji.

## Najnowszej generacji programy informatyczne wspomagające procesy logistyczne

Determinantami bezpieczeństwa narodowego jest szeroko rozumiany postęp cywilizacyjny. Wiodącymi czynnikami tego postępu są technika i technologia, które to przyczyniają się do powstawania coraz to lepszych rozwiązań i nowych produktów. Niektóre z nich mogą być pomocne w zarządzaniu bezpieczeństwem systemów logistycznych działających na korzyść umacniania bezpieczeństwa narodowego kraju. Do nich w głównej mierze możemy zaliczyć programy informatyczne.

Programy te, wykorzystywane w systemach logistycznych, można podzielić na trzy kategorie: uniwersalne (moduł obsługujący konkretny proces logistyczny

[2] R. Jakubczak, J. Flis (red.), *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa 2011, s. 33.

lub systemy wielomodułowe dla określonych ogniw w relacji dostawca – odbiorca), specjalizowane (przeznaczone np. dla procesów integrujących łańcuch), pomocnicze (wspomagające pracę różnych działów firmy, a także zarządzające dokumentami, kontaktami z klientami, ułatwiające obliczanie kosztów logistycznych).

Programy informatyczne w logistyce nie tylko ułatwiają planowanie procesów, ale także dostarczają niezbędnych danych w trybie online, do podejmowania decyzji, w przypadku wystąpienia zakłóceń w przepływie strumienia rzeczowego.

W praktyce można spotkać typowe systemy informatyczne wspomagające procesy logistyczne. Możemy do nich zaliczyć systemy: efektywnej obsługi konsumenta (ECR – *Efficient Consumer Response*), zarządzania relacjami z klientem (CRM – *Consumer Relationship Management*), zarządzania łańcuchem dostaw (SCM – *Supply Chain Management*), planowania zasobów dystrybucji (DRP – *Distribution Resources Planning*), łączący funkcje kalendarzowe i bazy danych (CM – *Contact Management*), zarządzania magazynem (WMS – *Warehousing Management System*), zarządzania transportem (TMS – *Transport Management System*), planowania potrzeb logistycznych (LRP – *Logistics Requirements Planing*), zarządzania środkami trwałymi (EAM – *Enterprise Asset Management*). Natomiast do systemów wspomagających zarządzanie logistyczne można zaliczyć systemy i niektóre moduły takich rozwiązań, jak: planowania potrzeb materiałowych (MRP – *Materials Requirement Planning*), planowania zasobów produkcyjnych (MRP II – *Manufacturing Resources Planning*), zarządzania zasobami przedsiębiorstwa (ERP – *Enterprise Resource Planning*), pozwalające wykonywać złożone operacje planistyczne i symulacyjne wraz z optymalizacją (APS – *Advanced Planning System*)[3].

Pełne zgromadzenie danych niezbędnych do zarządzania elektronicznym przepływem w systemach logistycznych, tak ważne zwłaszcza w sytuacjach kryzysowych i zagrożenia bądź klęski żywiołowej, jest możliwe dzięki nowoczesnym narzędziom pozwalającym na zbieranie, analizowanie i przesyłanie danych wewnątrz każdej firmy i instytucji oraz w ich relacjach z otoczeniem bliższym i dalszym. W praktyce gospodarczej narzędziem tym jest automatyczne gromadzenie danych ADC (*Automatic Data Capture*), czyli bezpośrednie wprowadzanie danych do komputerowych systemów informatycznych lub innego sprzętu sterowanego mikroprocesorem za pomocą specjalnych urządzeń (bez użycia klawiatury). Urządzenia te w postaci czytników lub skanerów zapewniają szybkie i bezbłędne wprowadzenie danych do systemu. W praktyce, systemy ADC to m.in.[4]:

- świetlne sygnalizatory pobrań,
- OCR (*Optical Character Recognition*) – zestaw technik lub oprogramowanie służące do rozpoznawania znaków i całych tekstów w pliku graficznym

[3] A. Szymonik, *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne*, Wyd. Politechniki Łódzkiej, Łódź 2016, s. 152.

[4] Tamże, s. 169.

(zadaniem OCR jest zwykle rozpoznanie tekstu w zeskanowanym dokumencie),

- RFID (*Radio-Frequency Identification*) – technika, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu stanowiącego etykietę obiektu przez czytnik, w celu identyfikacji obiektu,
- systemy głosowe – użycie technologii głosowych zapewnia łatwy, dwukierunkowy sposób komunikacji między systemem informatycznym a jego użytkownikiem,
- czytniki kodów kreskowych – popularnie nazywane skanerami, są urządzeniami, które zamieniają światło odbite od kodu kreskowego na sygnał elektroniczny, zrozumiały dla kasy lub komputera (w zależności od rodzaju mechanizmu odczytu rozróżnia się czytniki kodów laserowe i diodowe/CCD),
- terminale RF – bezprzewodowa wymiana informacji drogą radiową online, terminale takie często są wyposażone w skaner kodów kreskowych,
- komputery montowane w pojazdach oraz przenośne komputery – mają przewagę nad urządzeniami podręcznymi (większy ekran, większa klawiatura), są wyposażone w przyjazny dla użytkownika interfejs.

Sprawnie funkcjonujący system bezpieczeństwa narodowego w kontekście logistyki nie jest możliwy bez zapewnienia informacyjnej ciągłości działania. Także funkcjonowanie bezpieczeństwa logistyki na korzyść podmiotu bezpieczeństwa jest w znacznym stopniu uzależnione od narastających i nabierających na sile zagrożeń dla procesów informacyjnych, dotyczących gromadzenia, analizowania, przechowywania i udostępniania danych.

## Nowe technologie w obszarze bezpieczeństwem systemów logistycznych i łańcuchów dostaw

Nowe technologie zwłaszcza w obszarze systemów logistyki produkcji w przeważającej większości skoncentrowane są na aspektach związanych z robotyzacją, Internetem rzeczy, rozszerzoną i wirtualną rzeczywistością. Jeśli chodzi o najnowsze metody kompletacji z rodziny metod Pick-by, to są one coraz częściej wykorzystywane w centrach logistycznych i magazynach, służąc sprawnemu, efektywnemu i bezpiecznemu zachowaniu ciągłości procesów logistycznych. W gronie rodziny metod Pick-by można wyróżnić[5]:

- Pick-by-Light – to sprawna kompletacja linii zamówieniowych przy pomocy sygnalizacji świetlnej,
- Pick-by-Voice – wykorzystanie technologii głosowej oraz magazynowego systemu IT do obsługi kompletacji zamówień,

[5] A. Szymonik, D. Chudzik, *Nowoczesna koncepcja logistyki produkcji*, Difin, Warszawa 2020, s. 147–157.

- Pick-by-Scan – korzystanie ze skanera lub ręcznego urządzenia do obsługi zleceń kompletacji,
- Pick-by-Point – budowa strefy kompletacji z wykorzystaniem systemu jednej lub wielu lamp,
- Pick-by-Radar – kontrola dostępu do schowków realizowana za pomocą lasera obrotowego,
- Pick-by-Frame – metoda oparta na multi-kompletacyjnym wózku, do którego dokuje się samonośną ramę wyposażoną w cyfrowe wyświetlacze ledowe, sprzężone radiowo z centralnym systemem IT,
- Pick-by-Vision – metoda komisjonowania z wykorzystaniem okularów z danymi, które mają na celu pomóc operatorowi w szybkim odnalezieniu miejsca przechowywania np. danego pojemnika i przeprowadzić go przez proces komisjonowania bez błędów,
- Pick-by-Watch – to wsparcie procesów sekwencyjnych oraz kompletacji za pośrednictwem smartwatchów, smartphonów oraz tabletów, zapewniające szybką i sprawną obsługę całego procesu.

Współcześnie najnowsze zdobycze technologiczne (nowoczesne cyfrowe modele biznesowe) umożliwiają świadczenie nowych usług, polepszają bezpieczeństwo relacji organizacyjnych oraz przyczyniają się do wzrostu konkurencyjności oraz do transformacji przemysłu do modelu cyfrowego 4.0. Nowe zasady, które napędzają nowoczesną, cyfrową produkcję, również wprowadzają erę Logistyki 4.0, która jest rozszerzeniem systemów cyberfizycznych i komunikacji między maszynami poza granice produkcji przemysłowej w całym łańcuchu dostaw. Obecne rozwiązania stosowane w Logistyce 4.0 wykorzystuje się już w praktyce, czego dowodem są następujące procesy[6]:

- śledzenie (monitoring) transportu i przesyłek (automatyczne generowanie wiadomości do klienta o ładunku, jego masie i szacowanym czasie przybycia),
- wspólne planowanie logistyki w obszarze dystrybucji, produkcji i zaopatrzenia w czasie rzeczywistym,
- automatyzacja i digitalizacja procesów,
- synchronizacja ładunków logistycznych z możliwością transportu (minimalizacja marnotrawstwa związanego z wykorzystaniem flot oraz krótsze czasy oczekiwania w punktach ładowania i rozładowania),
- szerokie wykorzystywanie chmur obliczeniowych w celu korzystania z baz danych on-line, oraz w przestrzeni wirtualnej, bez konieczności zakupu (instalacji) dodatkowych aplikacji (programów),
- cyfrowe odzwierciedlenie rzeczywistości w działaniach logistycznych w łańcuchach dostaw.

[6] Tamże, s. 14–15.

Nowe technologie determinują również dynamiczny rozwój branży logistycznej w obszarze Logistyki 4.0, czego przykładem mogą być[7]:

1) Autonomiczne pojazdy oraz środki transportu wewnętrznego – w 2018 roku firma Volvo Truck zaprezentowała w pełni autonomiczne ciągniki siodłowe. Autonomiczne ciężarówki w pierwszej kolejności mają być implementowane w obiektach zamkniętych, takich jak terminale portowe, czy też kopalnie.
2) Wykorzystanie dronów w logistyce ostatniej mili – w 2020 roku firma Amazon otrzymała certyfikat Federalnej Administracji Lotniczej (FAA), czyli zezwolenie na dostarczanie przesyłek dronami na terenie Stanów Zjednoczonych.
3) W 2020 roku prestiżową nagrodę IFOY Award dla wózka wysokiego składowania otrzymał Reach Truck Crown ESR1000 – maszyna wpisująca się w trend przemysłowego Internetu rzeczy, przetwarza i analizuje szereg danych w czasie rzeczywistym. Dzięki temu zarządzający magazynem ma szybki dostęp do informacji o stopniu wykorzystania floty, krytycznych sytuacji w obiekcie czy też możliwych awariach urządzenia.
4) Ciekawym rozwiązaniem technologicznym jest system automatycznego załadunku i rozładunku samochodów ciężarowych Q-Loader – wynalazek opracowany i skonstruowany przez inżynierów WDX umożliwia optymalizację strefy przeładunku w magazynach cechujących się znacznymi przepływami towarów.

Logistyka 4.0 zmierza w kierunku inteligentnych, samouczących się pojazdów oraz całych systemów intralogistycznych, gdzie technologia podejmuje autonomiczne decyzje, definiując swoje położenie m.in. z wykorzystaniem czujników optycznych, optymalizując trasy oraz poszczególne czynności w procesie. Jej celem jest zwiększenie wydajności, redukcja poziomu błędów oraz kosztów operacyjnych zwiększając tym samym widoczność, bezpieczeństwo oraz kontrolę ładunku w całym łańcuchu dostaw.

Kluczowymi czynnikami cyfrowej transformacji są obecnie technologie komunikacji Machine to Machine (M2M), wykorzystanie przemysłowego Internetu rzeczy oraz metody przetwarzania informacji. Internet rzeczy jest jednym z głównych czynników w nowych rozwiązaniach komunikacyjnych i interaktywnych. Obiekty fizyczne stają się tym samym „inteligentne", łączą się z Internetem za pomocą zastosowanych czujników (sensorów) i prowadzą do innowacyjnych zmian[8].

---

[7] *Logistyka 4.0 – przewodnik*. https://wdx.pl/2020/11/19/logistyka-4-0-przewodnik/#start (dostęp: 15.08.2020 r.).

[8] *A Fruitful Union: The Intersection of Industry 4.0 and Logistics 4.0*, www.blog.flexis.-com (dostęp: 15.08.2020 r.).

W skali makro według przedstawicieli amerykańskiego *Departamentu Transportu* z 2000 r., występują cztery zasadnicze odniesienia logistyczne do bezpieczeństwa narodowego, które można zawrzeć w następujących wyrażeniach[9]:

- potencjał transportu – zapewnienie bezpieczeństwa środkom przewozowym, infrastrukturze liniowej i punktowej, systemom informatycznym, szczególnie w odniesieniu do rozmieszczenia i dyslokacji wojsk na i poza terytorium kraju,
- gotowość transportu – utrzymanie zdolności przewozowych do niezawodnej realizacji zadań w sytuacjach nagłych,
- żywotność transportu – redukowanie wrażliwości środków przewozowych, infrastruktury liniowej i punktowej oraz użytkowników na niekorzystne uwarunkowania sytuacji kryzysowej,
- zagrożenia transportu – eliminowanie nielegalnego wykorzystania środków przewozowych (imigranci, narkotyki, broń itd.).

Wynika z powyższego, że logistyka, w tym wypadku rozpatrywana przez pryzmat transportu, odgrywa istotną rolę w zapewnieniu bezpieczeństwa narodowego. Decydującą rolę odgrywa w tej kwestii telematyka[10] bezpieczeństwa procesów transportowych, która jest utożsamiana z[11]:

- Inteligentnymi Systemami Transportowymi (ITS) – obejmują one szeroki zakres rozwiązań technologicznych mających na celu poprawę transportu poprzez zwiększenie mobilności i bezpieczeństwa w ruchu drogowym, a w jego skład wchodzą m.in.: centra zarzadzania ruchem, zintegrowane systemy zarządzania ruchem, systemy sterowania ruchem, systemy monitoringu wizyjnego (kamery przemysłowe, urządzenia rejestrujące obraz, monitory, obiektywy) CCTV (*Closed Circuit TeleVision*), systemy monitoringu wizyjnego do rozpoznawania i wyszukiwania pojazdów samochodowych identyfikowanych na podstawie numerów rejestracyjnych, systemy dynamicznego ważenia pojazdów, systemy informacji parkingowej,
- Inteligentnym Transportem (IT) – to współpracujące ze sobą dwa układy: inteligentna droga oraz inteligentny pojazd, wyposażony w urządzenia utrzymujące ciągłą, bezprzewodową wymianę informacji z urządzeniami zainstalowanymi nad/pod drogą lub jej poboczem.

Narzędziem wspomagającym proces podejmowania decyzji w sytuacjach kryzysowych jest *Business Intelligence* – BI (analityka biznesowa). BI można przedstawić jako proces przekształcania danych w informacje, a informacji w wiedzę, z pomocą szerokiego wachlarza aplikacji i technologii, która może być

---

[9] M. Skarżyński, *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej – aspekty logistyczne*, „Przegląd Politologiczny" 2015, nr 1, s. 150.

[10] Telematyka transportu to dział wiedzy o transporcie, integrujący informatykę i telekomunikację w zastosowaniach do potrzeb zarządzania i sterowania ruchem w systemach transportowych, stymulujący działalność techniczno-organizacyjną umożliwiającą podniesienie efektywności i bezpieczeństwa eksploatacji tych systemów. A. Szymonik, *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne…*, s. 91.

[11] Tamże, s. 92.

wykorzystana do zwiększenia sprawności oraz skuteczności określonych działań, w tym związanych z zapewnieniem bezpieczeństwa w sytuacjach kryzysowych.

Najważniejsze obszary związane z *Business Intelligence* to[12]:

- DW (*Data Warehouse*) – hurtownie danych – ładowanie, przetwarzanie ETL (*Extraction Transformation Load*),
- data mining – eksploracja danych, drążenie danych,
- czyszczenie danych i zarządzanie jakością danych, statystyka i techniczna analiza danych,
- OLAP (*Online Analytical Processing*) – analiza wielowymiarowa i wielowymiarowe struktury danych,
- MIS (*Management Information Systems*) – systemy informowania kierownictwa,
- raportowanie – wizualizacja informacji i panele informacyjne dla kierownictwa (*Dashboards*),
- CRM (*Customer Relationship Management*) – zarządzanie relacjami z klientami,
- SIS (*Spatial Information System*) – system informacji przestrzennej,
- DSS (*Decision Support Systems*) – systemy wspomagania decyzji.

Techniki prezentacyjne BI dobierane są odpowiednio do potrzeb użytkownika a wizualizacja stanu aktualnego realizowana jest w postaci obrazowej. Kokpit menedżerski (*management dashboard*) to atrakcyjny sposób prezentacji wyników – wizualizacja danych i raportów w postaci podobnej do pulpitów sterowniczych. Efektem zastosowania narzędzi BI w systemie bezpieczeństwa jest dostępność do szybkiej informacji, np. o[13]:

- terenie – rzeźbie i obiektach naturalnych, obiektach terenowych o istotnym znaczeniu dla planowania i prowadzenia działań ratowniczych, a także prognozowania i likwidacji skutków katastrof, klęsk żywiołowych i innych zagrożeń,
- siłach i środkach, które mogą być użyte w ratownictwie, np. dane o stanach osobowych jednostek organizacyjnych systemu,
- zapasowych dostawcach i ewentualnych rynkach zbytu, w przypadku nagłego załamania (np. na skutek tsunami) dotychczasowych rynków dostaw i konsumentów,
- zapasowej infrastrukturze logistycznej, np. magazynach, halach produkcyjnych, w sytuacjach kiedy wykorzystana uległa zniszczeniu,
- siłach i środkach, które potencjalnie mogą być użyte w ratownictwie oraz w eliminowaniu ich skutków (elementami tego zasobu mogą być dane o: stanach osobowych jednostek organizacyjnych systemu, ich wyposażeniu

[12] A. Szymonik, *Logistyka w bezpieczeństwie. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2011, s. 67.

[13] A. Szymonik, M. Bielecki, *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa 2015, s. 96; A. Szymonik, *Logistyka w bezpieczeństwie..*, s. 45.

technicznym, parametrach sprzętu, infrastrukturze obiektów własnych, a także dokumentacje jednostek, zakres obowiązków osób funkcyjnych, procedury postępowania w określonych sytuacjach, takich jak pożar, powódź itp.),

- aktualnym stanie zagrożeń bezpieczeństwa na obszarze odpowiedzialności – dane pochodzące z wszelkiego rodzaju urządzeń monitorujących zagrożenia oraz osób zgłaszających zajścia zdarzeń wymagających działań ratowniczych (na podstawie danych z monitoringu podsystem informacyjny, posługując się modelami matematycznymi oraz programowymi symulatorami opracowuje prognozy i scenariusze możliwego rozwoju zdarzeń).

Tabela 1. Nowoczesne technologie w systemach monitorowania bezpieczeństwa – obszary badawcze i związane z nimi priorytetowe technologie

| **Lp.** | **Obszar badawczy** | **Priorytetowe technologie** |
|---|---|---|
| 1 | Technologie informacyjne | Techniki łączenia danych, zbierania i klasyfikacji danych, technologie przetwarzania obrazu, technologie zarządzania informacjami i danymi. |
| 2 | Sztuczna inteligencja i wspieranie procesu decyzyjnego | Przeszukiwanie informacji i danych, zarządzanie wiedzą, modelowanie i symulacja, optymalizacja i technologie wspierania decyzji. |
| 3 | Urządzenia komunikacyjne | Komunikacja rekonfigurowana, bezpieczna komunikacja mobilna, zarządzanie sieciami komunikacyjnymi, szerokopasmowe łącza przesyłu danych. |
| 4 | Ochrona informacji | Technologie szyfrowania, przeszukiwanie danych, kontrola dostępu. |
| 5 | Technologie komputerowe | Techniki bezpiecznego przetwarzania, wysokowydajne przetwarzanie. |
| 6 | Systemy informatyczne | Infrastruktura wspierająca zarządzanie i rozpowszechnianie informacji, systemy optymalizacji i planowania procesu decyzyjnego. |
| 7 | Zintegrowane platformy | Platformy bezzałogowe (lądowe, morskie i lotnicze, satelity obserwacyjne i nawigacyjne). |
| 8 | Sprzęt oparty na czujnikach | Kamery, czujniki, w tym technologie wykrywania szczególnych zagrożeń chemicznych i biologicznych, urządzenia pasywne z czujnikami na podczerwień, przetwarzanie sygnałów wielowidmowych. |
| 9 | Nawigacja, prowadzenie, kontrola i śledzenie | Oznaczenia RFID (elektroniczne oznakowanie produktu), śledzenie, technologie GPS, radionawigacja, śledzenie oparte na kodach kreskowych. |
| 10 | Elektroniczne uwierzytelnienia | Systemy elektronicznego oznaczenia („etykiety"), „inteligentne karty" (*smart cards*). |

Źródło: opracowanie własne na podstawie: Z. Mierczyk, *Nowoczesne technologie w systemach monitorowania bezpieczeństwa* [w:] *Metodologia badań bezpieczeństwa narodowego. Bezpieczeństwo 2010*, t. II, AON, Warszawa 2011, s. 32–33.

Nowatorskie rozwiązania winny być rezultatem badań i priorytetowych technologii w obszarze systemów monitorowania bezpieczeństwa (tabela 1)[14].

Reasumując należy stwierdzić, że stan bezpieczeństwa narodowego nie zawsze jest stabilny, a we współczesnym świecie występują ciągłe jego zagrożenia. To wszystko powoduje, iż powinno się dążyć do doskonalenia funkcjonowania systemu bezpieczeństwa poprzez zastosowanie coraz to nowszych technologii i narzędzi wspomagających proces podejmowania decyzji zwłaszcza w sytuacjach kryzysowych, które przyczyniają się do poprawy jakości i skuteczności podejmowania decyzji w systemach związanych z zapewnieniem bezpieczeństwa narodowego.

## Zakończenie

Konstatując niniejsze rozważania na podkreślenie zasługuje fakt, że w trudnym dziele tworzenia bezpieczeństwa Polski i współtworzenia bezpieczeństwa Europy coraz częściej kluczowego znaczenia nabiera kształtowanie powszechnej świadomości o bezpieczeństwie narodowym jako koniecznym i niemożliwym do zastąpienia warunku włączenia całego społeczeństwa do współodpowiedzialności za tworzenie bezpieczeństwa narodowego. Aby szybko i sprawnie zachodziły te procesy należy niewątpliwie włączyć w tę działalność logistykę[15]. Pojawiające się zagrożenia i wyzwania współczesności wskazują jednoznacznie na rosnącą rolę technologii wspomagania zarządzania bezpieczeństwem systemów logistycznych, które mają wpływ na sprawność i skuteczność realizowanych procesów w systemie bezpieczeństwa narodowego. Zaprezentowane rozwiązania informatyczne to nie tylko nowoczesność, efektywność, wymierne korzyści organizacyjne, ekonomiczne, ale również bezpieczna logistyka z punktu widzenia umacniania bezpieczeństwa narodowego Polski.

## Bibliografia

Jakubczak R., Flis J. (red.), *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa 2011.

Jałowiec T., *Logistyczne wymiary systemu bezpieczeństwa państwa*, „Logistyka" 2011, nr 2.

Mierczyk Z., *Nowoczesne technologie w systemach monitorowania bezpieczeństwa* [w:] *Metodologia badań bezpieczeństwa narodowego, Bezpieczeństwo 2010*, t. II, AON, Warszawa 2011.

[14] A. Szymonik, *Inżynieria bezpieczeństwa systemów logistycznych*, Difin, Warszawa 2016, s. 43–45.

[15] R. Piętowska-Laska, *Logistyczne aspekty bezpieczeństwa narodowego – wybrane zagadnienia* [w:] *Zagrożenia ładu społecznego oraz bezpieczeństwa narodowego. Wybrane aspekty*, red. M. Gitling, I. Wojaczek, Wyd. Państwowa Wyższa Szkoła Wschodnioeuropejska w Przemyślu, Przemyśl 2017, s. 321.

Piętowska-Laska R., *Logistyczne aspekty bezpieczeństwa narodowego – wybrane zagadnienia* [w:] *Zagrożenia ładu społecznego oraz bezpieczeństwa narodowego. Wybrane aspekty*, red. M. Gitling, I. Wojaczek, Wyd. Państwowa Wyższa Szkoła Wschodnioeuropejska w Przemyślu, Przemyśl 2017.

Skarżyński M., *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej – aspekty logistyczne*, „Przegląd Politologiczny" 2015, nr 1.

Szymonik A., *Inżynieria bezpieczeństwa systemów logistycznych*, Difin, Warszawa 2016.

Szymonik A., *Logistyka w bezpieczeństwie. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2011.

Szymonik A., *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne*, Wyd. Politechniki Łódzkiej, Łódź 2016.

Szymonik A., Bielecki M., *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa 2015.

Szymonik A., Chudzik D., *Nowoczesna koncepcja logistyki produkcji*, Difin, Warszawa 2020.

## Netografia

*A Fruitful Union: The Intersection of Industry 4.0 and Logistics 4.0*, www.blog.flexis.-com (dostęp: 15.08.2020 r.).

*Logistyka 4.0 – przewodnik*. https://wdx.pl/2020/11/19/logistyka-4-0-przewodnik/#start (dostęp: 15.08.2020 r.).

# O AUTORACH

**Dagmara FLOREK-KLĘSK**, dr – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: dfk@prz.edu.pl. ORCID: 0000--0002-5069-2936.

**Paweł GIERŁACH** – student, bezpieczeństwo wewnętrzne II st., Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza.

**Wojciech GRYZIK** – student, bezpieczeństwo wewnętrzne II st., Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza.

**Andrzej KIEŁTYKA**, dr – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: kieltyka@prz.edu.pl. ORCID: 0000-0002--6069-3115.

**Elżbieta KOSIOR**, mgr – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: ekosior@prz.edu.pl. ORCID: 0000-0001--5572-8291.

**Elżbieta KURZĘPA**, dr – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: e_kurzepa@prz.edu.pl. ORCID: 0000-0003--0032-8607.

**Piotr ŁOSOWSKI** – student, bezpieczeństwo wewnętrzne II st., Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza.

**Adrian MARTINEZ** – student, bezpieczeństwo wewnętrzne II st., Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza.

**Marcin MERKWA**, dr – Zakład Nauk Historyczno i Teoretyczno Prawnych, Wydział Prawa i Administracji, Uniwersytet Rzeszowski; e-mail: mmerkwa@prz.edu.pl. ORCID: 0000-0001-7288-4552.

**Paweł MICHALAK** – student, bezpieczeństwo wewnętrzne II st., Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza.

**Anna MROCZKOWSKA** – studentka, bezpieczeństwo wewnętrzne II st., Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza.

**Krzysztof NOWAKOWSKI**, inż. – informatyka II st. Wydział Elektrotechniki i Informatyki, Politechnika Rzeszowska im. Ignacego Łukasiewicza.

**Renata PIĘTOWSKA-LASKA**, dr inż. – Katedra Systemów Zarządzania i Logistyki, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: rlaska@prz.edu.pl. ORCID: 0000-0001-5665-0377.

**Marta POMYKAŁA**, dr hab., prof. PRz – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: mpomykal@prz.edu.pl. ORCID: 0000-0002-2557-1876.

**Ewa PONDEL**, mgr – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: ewapondel@prz.edu.pl. ORCID: 0000-0001--8096-5897.

**Katarzyna PURC-KUROWICKA**, dr – Zakład Prawa i Administracji, Wydział Zarządzania, Politechnika Rzeszowska im. I. Łukasiewicza; e-mail: kasiapk@prz.edu.pl. ORCID: 0000-0003-1082-2772.

# New technologies – contemporary challenges in the area of law and security

## Summary

The publication entitled *New technologies – contemporary challenges in the area of law and security* is an attempt to show the ever-increasing impact of modern technologies on law and security. The increasingly common use of information technology in everyday life, the use of the Internet in professional and private activities, computerization of all procedures, building digital database systems in every field, or the emergence of new cyber threats make it necessary to look at the issues of compliance with the law and legal liability, as well as to protect security in cyberspace from a completely new perspective.

The impact of new technologies on changes in the field of law and security is undoubtedly huge. Due to the fact that the issues discussed is extensive, the selection of the subject of the publication had to be arbitrary and only contributed to a more in-depth study. The authors of the texts contained in this book are both experienced academics and students (mainly in the field of Internal Security at the Faculty of Management of the Rzeszów University of Technology). This is a great advantage of this publication as it allows one to show the problems of computerization from completely different perspectives.

The publication consists of three parts. In the first part an attempt has been made to outline the key challenges that technological progress creates in the area of law. Among others, the issues related to copyright, public procurement and constitutional law have been discussed. The attention has been also paid to the influence of new technologies on the concept of human rights. In the part devoted to security, the authors have tried to outline new types of threats to security and public order in the area of cybercrime. Subsequent considerations have discussed skimming, stalking, scams made via social networks, as well as surveillance. Separate considerations have also been devoted to the National Cybersecurity System and the comparison of the rules of criminal liability for cybercrimes in Poland, Great Britain and the United States.