CBKE
e-BIULETYN

Digital Rights Management – nowa era prawa autorskiego?

mgr Krzysztof Gienas

aplikant Prokuratury Rejonowej Szczecin-Zachód

1.0 Wprowadzenie.

Przepowiednie zakładające koniec dotychczasowego prawa autorskiego w konfrontacji z Internetem okazały się przesadzone[1]. Pomimo szeregu potencjalnych zagrożeń, jakie niesie dla twórców technologia informatyczna, staje się ona obecnie szeroko wykorzystywanym kanałem dystrybucji dóbr niematerialnych. Istotną rolę odgrywają przy tym sposoby redukowania skali naruszeń praw autorskich w środowisku elektronicznym. Na czoło w tym względzie wybija się przełożenie na praktykę znanego stwierdzenia, iż „odpowiedzią na technologię powinna być technologia"[2]. Obecnie do roli panaceum dla większości obaw środowisk twórczych pretendują rozwiązania określane zbiorczym mianem systemów Digital Rights Management (DRM). Przynoszą one ze sobą szereg zagadnień prawnych, jak dotychczas niezbyt dostrzeganych w rodzimej literaturze. Niemniej jednak o ich wadze świadczą chociażby działania Komisji Europejskiej odnoszące się do inicjowania dyskusji na temat DRM[3]. Zasadniczym celem niniejszego opracowania pozostaje nakreślenie siatki pojęciowej związanej z Digital Rights Management oraz przybliżenie regulacji odnoszących się do zagwarantowania nienaruszalności tego typu technologii w ujęciu prawnoporównawczym.

[1] Por. L. Jones, An artist`s entry into cyberspace : intellectual property on the Internet. EIPR 2/2000, s. 79.
[2] Ch. Clark, The answer to the machine is in the machine. [w:] B. Hugenholtz (red.), The future of Copyright in a Digital Environment, Kluver Law International 1996, s. 139.
[3] http://www.europa.eu.int/comm/internal_market/en/intprop/docs/com-2004-261_en.pdf.

2.0 Pojęcie Digital Rights Management.

Punktem wyjścia do dalszych rozważań pozostaje przybliżenie niektórych aspektów technicznych systemów DRM. Brak jest uniwersalnej definicji Digital Rights Management, choć samo tłumaczenie pojęcia wskazuje, iż punktem centralnym funkcjonowania owych rozwiązań jest zarządzanie prawami w środowisku elektronicznym. Jedna z najszerszych definicji DRM przyjmuje, iż pod tym terminem kryje się wszystko, co można zrobić, by zdefiniować, zarządzać prawami i śledzić treści w formie cyfrowej[4]. Prawidłowe funkcjonowanie systemu Digital Rights Management wymaga połączenia kilku komponentów. Po pierwsze dane o utworze, jego twórcy, podmiotach uprawnionych z tytułu majątkowych praw autorskich oraz zasady eksploatacji utworu powinny zostać zapisane w sposób pozwalający na odczytanie ich przez maszynę-komputer. Informacje te są z reguły umieszczane w tzw. metadanych porównywanych do katalogów bibliotecznych[5]. Z kolei definiowanie zakresu działań, które może podejmować użytkownik w stosunku do pracy, uzyskuje się dzięki zastosowaniu tzw. języków definiowania uprawnień. Obecnie dużą popularnością cieszy się język XrML. Istotną rolę w funkcjonowaniu komercyjnych systemów Digital Rights Management odgrywają środki technologiczne chroniące prace udostępniane w formie zdigitalizowanej. Generalnie w literaturze dzieli się zabezpieczenia techniczne utworów na te, które chronią dostęp do prac udostępnianych w formie cyfrowej oraz mechanizmy kontrolujące konkretne sposoby wykorzystywania dóbr niematerialnych[6]. Wśród nich można wyróżnić kontrolę dostępu opartą o hasła, szyfrowanie, elektroniczne znaki wodne. Potencjalnie kontrolą technologiczną może zostać objęty dostęp do utworu, możliwość zwielokrotniania go, ilość oraz czas „odtworzeń" pliku zawierającego chronioną prawem autorskim pracę.

Praktycznym zastosowaniem zabezpieczeń technicznych utworów jest *tzw. regionalizacja* odnosząca się do dystrybucji płyt DVD. System kodowania stosowany przy wprowadzaniu na rynek dóbr niematerialnych utrwalonych na tych nośnikach został podzielony na sześć międzynarodowych regionów. Urządzenia odtwarzające płyty DVD w danym regionie zostały zaprojektowane tak, by uniemożliwiać odtworzenie utworów nabytych w innym regionie. Nie ma przy tym znaczenia, iż nośnik jest w pełni oryginalny i znajduje się w posiadaniu uprawnionego użytkownika. Powodów wprowadzenia tego typu zróżnicowania należy upatrywać we względach natury ekonomicznej. Restrykcje odnoszące się do odtwarzania utworów pozwalają

[4] A. Arnab, Digital Rights Management – A current review, s. 5. Opracowanie dostępne pod adresem http://pubs.cs.uct.ac.za/archive/00000114/01/sota.pdf.
[5] M. Nahotko, Metadane. Elektroniczny Biuletyn Informacji Bibliotekarzy, 6/2000 http://ebib.oss.wroc.pl/arc/e014-02.html
[6] A. Matlak, Prawo autorskie w społeczeństwie informacyjnym. Zakamycze 2004, s. 126-127.

bowiem na dystrybucję dzieł filmowych na płytach DVD w jednym regionie, podczas gdy w innym będą one dopiero wyświetlane w kinach[7].

Wprowadzenie zabezpieczeń technicznych odnosi się zarówno do obecnych na rynku, jak i dopiero powstających utworów. Jednakże w pierwszym wypadku uzyskanie pozytywnych efektów w postaci redukcji naruszeń praw autorskich jest znacznie trudniejsze[8]. Przesądza o tym głównie fakt, iż część z kopii utworów, głównie w postaci analogowej, nie będzie opatrzona w zabezpieczenia, które będą chronić te same dzieła w formie zapisu cyfrowego. Nie sprawia przy tym trudności poddanie procesowi digitalizacji niezabezpieczonego utworu – przykładowo zeskanowanie książki.

Sukces komercyjnych rozwiązań DRM uzależniony pozostaje od zapewnienia kompatybilności pomiędzy różnymi metodami zabezpieczania prac[9]. W ten sposób umożliwiona pozostanie eksploatacja utworów przez uprawnionych użytkowników na poziomie porównywalnym z dotychczasowym korzystaniem z dzieł. Warto zasygnalizować, iż kontrola „konsumpcji" dóbr niematerialnych zapewniana przez systemy DRM odnosi się do czynności, które nie zostały tradycyjnie objęte zakresem przepisów prawa autorskiego[10]. Technologia pozwala bowiem na kontrolę, gdzie użytkownik decyduje się na korzystanie z utworu, jak często go eksploatuje, czy przekazuje go innych podmiotom.

3.0 Prawna ochrona nienaruszalności komponentów systemów Digital Rights Management.

Wykorzystanie zabezpieczeń technologicznych do ochrony utworów nie rozwiązuje całkowicie problemów dystrybucji dóbr niematerialnych w formie cyfrowej. Należy uwzględnić bowiem możliwość ich przełamania w drodze technik hackerskich. W literaturze niejednokrotnie podkreśla się, iż nie sposób opracować 100 % bezpiecznej technologii mającej zastosowanie komercyjne. Z kolei uzyskanie dostępu do niezabezpieczonych utworów, nawet przez niewielką część użytkowników, prowadzić będzie do ich niekontrolowanej dystrybucji za pośrednictwem elektronicznych środków komunikacji. Sprawia to, iż prawidłowe funkcjonowanie komponentów

[7] E. Dunt, J. Gans, S. King, The economic Consequences of DVD Restrictions, s. 4. http://www.mbs.edu/home/jgans/papers/dvd.pdf
[8] B. Turnbull, D. Marks, Technical protection measures : the intersection of technology, law and commercial licences. EIPR 5/2000, s. 200.
[9] Na temat przyszłości DRM w kontekście regulacji prawnych por. S. Bechtold, The Present and Future of Digital Rights Management - Musings on Emerging Legal Problems. [w:] E. Becker (red.), Digital Rights Management - Technological, Economic, Legal and Political Aspects. Springer Verlag, 2003, s. 597-654.
[10] A. Arnab, Digital Rights Management…, op. cit. , s. 7.

systemów Digital Rights Management uzależnione pozostaje od objęcia ich nienaruszalności specjalnym reżimem prawnym. Jedynie w ten sposób można zapewnić wysoki poziom ochrony dóbr niematerialnych eksploatowanych w postaci zapisu zero-jedynkowego. Założenie to jest realizowane poprzez wprowadzenie do przepisów prawa autorskiego regulacji zakazujących usuwania bądź obchodzenia zabezpieczeń technicznych stosowanych przy dystrybucji utworów.

3.1 Traktaty WIPO

Potrzeba wprowadzenia gwarancji prawnych wzmacniających ochronę oferowaną przez rozwiązania technologiczne znalazła odzwierciedlenie w przepisach Traktatów WIPO z 1996 roku : o prawie autorskim (art. 11 i 12) oraz o artystycznych wykonaniach i fonogramach (art. 18 i 19). Oba akty prawa międzynarodowego zakładają analogiczną ochronę środków technicznych oraz informacji służących zarządzaniu prawami autorskimi. Zgodnie z art. 11 traktatu WIPO o prawie autorskim, jego stronom nakazano wprowadzenie efektywnych środków prawnych przeciwdziałających obchodzeniu skutecznych środków technicznych, stosowanych przez autorów z związku z wykonywaniem ich uprawnień[11]. Ponadto wspomniane traktaty nakazują wprowadzenie prawnych środków przeciwdziałających usuwaniu lub zmianie, bez zezwolenia, informacji, które służą zarządzaniu prawami autorskimi (art. 12 traktatu o prawie autorskim oraz art. 19 traktatu o artystycznych wykonaniach i fonogramach).

Ramowy charakter kwestii poruszonych w traktatach WIPO sprawia, iż nie przynoszą one jednoznacznej odpowiedzi na szereg szczegółowych pytań. Po pierwsze nie przesądzają o rodzaju środków, które mają zostać podjęte przez ustawodawców krajowych, pozostawiając im w tym względzie wolną rękę. Może to doprowadzić do braku harmonizacji regulacji prawnych odnoszących się do tego zagadnienia. Poszczególne państwa za efektywny środek prawny mogą uznać regulacje karne, inne zaś poprzestać na oparciu się o przepisy prawa cywilnego. Nie mniej istotnym zagadnieniem pozostaje pominięcie milczeniem związków pomiędzy stosowaniem zabezpieczeń technicznych a korzystaniem z dozwolonych użytków przez użytkowników. Można bronić tezy, iż treść art. 11 traktatu o prawie autorskim pozwala na przyjęcie, iż usunięcie zabezpieczenia po to, by skorzystać z przywileju wynikającego z dozwolonego użytku, nie powinno być objęte zakazami prawnymi[12].

[11] Analogiczny zapis znalazł się w art 18 traktatu o artystycznych wykonaniach i fonogramach.
[12] T. Foged, Us v EU Anti Circumvention legislation : Preserving the public`s privileges in the digital age. EIPR 11/2000, s. 529.

Omawiane traktaty zakładają, iż zabezpieczenia powinny być stosowane przez autora. W chwili obecnej w większości przypadków twórcy nie będą samodzielnie stosować rozwiązań technologicznych. Czynności te zostaną podjęte przez inne podmioty, z reguły uprawnione z tytułu majątkowych praw autorskich. Nie ulega bowiem wątpliwości, iż dostrzegalna jest tendencja do coraz częstszego „rozdzielania" podmiotów autorskich praw osobistych oraz majątkowych. Na tle powyższych uwag można wyciągnąć wniosek o objęciu ochroną tylko tych zabezpieczeń technicznych, za którymi „stoi" twórca. W doktrynie jednakże odrzuca się tego typu interpretację, wskazując na potrzebę szerokiego rozumienia pojęcia „autor" użytego w art. 11 traktatu WIPO o prawie autorskim[13].

Z treści przepisów zawartych w traktatach WIPO nie można też jednoznacznie wywnioskować, czy zakazem powinny być objęte jedynie same czynności obchodzenia zabezpieczeń, czy także tzw. czynności przygotowawcze – odnoszące się do tworzenia i dystrybucji narzędzi służących do ich „deaktywacji"[14]. Na marginesie trzeba dodać, że samo pojęcie „czynności przygotowawcze" w tym kontekście jest dość sztuczną konstrukcją. Nie chodzi tu o przygotowanie, rozumiane chociażby przez pryzmat przepisów karnych i polegające na zbieraniu informacji, środków, opracowywaniu planu działania przez sprawcę późniejszego czynu zabronionego[15], a o tworzenie i oferowanie oprogramowania i usług ułatwiających obchodzenie komponentów systemów Digital Rights Management. Czynności te są wykonywane z reguły przez osoby, które nie dokonują samodzielnie obejścia zabezpieczeń. Analiza przepisów traktatów prowadzi jednak do wniosku, iż odnoszą się one jedynie do aktów obchodzenia rozwiązań technologicznych[16].

3.2 Digital Millenium Copyright Act

Dostosowanie amerykańskich przepisów do postanowień traktatów WIPO stanowią unormowania ustawy Digital Millenium Copyright Act (DMCA) z 1998 roku. Zawierają one kompleksową regulację problemu zabezpieczeń technologicznych, a nadto kreują sposób rozstrzygnięcia problemów na styku praktyki zastosowań systemów DRM i zachowań wchodzących w ramy dozwolonych użytków[17]. Już na wstępie należy zaznaczyć, że amerykańskie

[13] A. Matlak, Prawo autorskie…, op. cit. , s. 134.
[14] Zagadnienia odnoszące się tzw. czynności przygotowawczych zostaną poruszone szerzej w dalszej części opracowania.
[15] Por. treść art. 16 § 2 kodeksu karnego z dnia 6 czerwca 1997 roku.
[16] T. Foged, Us v EU..., op. cit. , s. 530.
[17] Szeroko na temat DMCA por. P. Samuelson, Intelectual Property and the Digital Economy : Why the Anti-circumvention regulations need to be revised, Berkley Technology Law Journal 1/1999; http://www.sims.berkeley.edu/~pam/papers/Samuelson.pdf

przepisy wychodzą ponad „próg minimum" zarysowany w traktatach WIPO z 1996 roku[18]. Wprowadzony przepisami DMCA do kodeksu USA § 1201 zakłada dychotomiczny podział zabezpieczeń technicznych na rozwiązania kontrolujące dostęp do dzieła oraz zapobiegające jego nieuprawnionemu kopiowaniu. Jednocześnie każdej z kategorii przyznano inny zakres ochrony prawnej przed obchodzeniem (circumvention). Samo pojęcie obchodzenia zabezpieczeń obejmuje szeroki katalog zachowań, włączając w to chociażby odszyfrowanie danych lub inne zachowania prowadzące do ich deaktywacji. W przypadku innowacji technologicznych realizujących założenie „odseparowania" osób nieuprawnionych od dzieł, zakazane pozostaje zarówno obchodzenie ich, jak i tworzenie lub sprzedaż narzędzi lub usług używanych do wspomnianych zachowań. Z kolei odnośnie zabezpieczeń kontrolujących kopiowanie dóbr niematerialnych chronionych przepisami prawa autorskiego, zakazem objęto jedynie tworzenie i „obrót" komponentami służącymi do ich obchodzenia. Ponadto § 1201 sprecyzował trzy warunki - okoliczności przesądzające o uznaniu, iż urządzenie lub usługa służy do obchodzenia zabezpieczeń technicznych, przy czym wystarczające jest wypełnienie jednego z nich. Po pierwsze – zostały one zaprojektowane lub wyprodukowane głównie w celu obchodzenia zabezpieczeń. Po drugie – wymieniony cel funkcjonowania lub możliwość ich wykorzystania do działań innych niż obchodzenie zabezpieczeń ma ograniczone znaczenie komercyjne. Ostatnia z okoliczności pozwalających na uznanie „narzędzi" lub usług za zabronione w świetle DMCA, to reklamowanie ich jako służące celom obchodzenia zabezpieczeń, które efektywnie kontrolują dostęp do dzieła. Nawiązując do drugiego z warunków, bez znaczenia pozostawać będzie fakt, czy narzędzie będzie wykorzystywane do celów, które nie naruszają uprawnień podmiotów uprawnionych z tytułu praw autorskich[19]. Zważyć należy, iż tego typu urządzenia lub usługi mogą być stosowane w celu zweryfikowania poziomu bezpieczeństwa zapewnianego przez aktualnie stosowane środki-zabezpieczenia techniczne. Zwraca się także uwagę na to, iż DMCA posługuje się zwrotem „cel". Literalna interpretacja § 1201 prowadzić może do przyjęcia, że tego typu narzędzie nie może spełniać żadnych dodatkowych celów bądź uboczne zastosowania rozwiązania informatycznego nie mogą być tak istotne, jak możliwość obchodzenia za jego pomocą zabezpieczeń technicznych. W przeciwnym wypadku urządzenie spełniające kilka równorzędnych funkcji nie będzie mogło być uznane za zakazane w świetle DMCA. Nie będzie bowiem ono zaprojektowane lub stworzone przede wszystkim w celu dokonywania aktów obchodzenia zabezpieczeń[20].

[18] J. Cunard, K. Hill, Ch. Barlas, Current developments in the field of digital rights management. Raport przygotowany dla potrzeb WIPO, s. 48. http://www.wipo.org/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf
[19] J. Cunard, K. Hill, Ch. Barlas, Current developments..., op. cit., s. 50-51.
[20] Ibidem.

Warunkiem współdziałania niektórych komponentów systemów DRM jest zapewnienie odpowiednich rozwiązań na poziomie urządzeń odtwarzających utwory. Pojawia się więc zagadnienie, czy producenci tego rodzaju sprzętu muszą wyposażać je w elementy co najmniej ułatwiające poprawne funkcjonowanie zabezpieczeń technicznych dzieł chronionych prawem autorskim. Założenie odzwierciedlone w treści DMCA przynosi negatywną odpowiedź na tak postawione pytanie. Zasada ta, określana mianem „*no mandate*", została wyraźnie wyrażona w przepisach ustawy[21].

DMCA wprowadza wyjątki od zakazu obchodzenia zabezpieczeń technicznych bądź tworzenia lub dystrybucji środków (urządzeń, usług) umożliwiających takie poczynania. Ustawa przewiduje siedem takich sytuacji odnoszących się do: działań podejmowanych przez biblioteki, archiwa, instytucje edukacyjne; czynności wykonywanych przez agencje rządowe; dekompilacji programu komputerowego; badań z zakresu kryptografii; ochrony małoletnich; ochrony prywatności; testowania zabezpieczeń systemów komputerowych. W doktrynie prezentowany jest pogląd, iż zakres tych wyłączeń jest bardzo wąski[22]. Ponadto w niektórych przypadkach wyjątkiem objęto jedynie samodzielne obchodzenie zabezpieczeń, pozostawiając zakaz odnoszący się do „czynności przygotowawczych" związanych z tworzeniem i dystrybucją umożliwiających to środków. W konsekwencji osoba, choć mogąca samodzielnie pozbawić pracę elektronicznej ochrony, nie zdoła tego uczynić z uwagi na brak dostępnych narzędzi informatycznych. Niewielu użytkowników posiada bowiem wiedzę pozwalającą na samodzielne obchodzenie komponentów systemów DRM w postaci zabezpieczeń technicznych.

Ponadto przepisy gwarantują ochronę informacji służących zarządzaniu prawami autorskimi (§ 1202). W praktyce do miana tego typu informacji pretendować będą informacje zawarte w metadanych, a dotyczące głównie identyfikacji pracy, podmiotów osobistych i majątkowych praw autorskich oraz zasad eksploatacji utworu. DMCA wprowadza zakaz nieuprawnionego usuwania informacji służących zarządzaniu prawami autorskimi oraz rozpowszechniania utworów z usuniętymi bądź zmienionymi metadanymi[23]. Zabronione jest również wprowadzanie fałszywych metadanych, jeśli zamiarem takiego działania jest umożliwienie, ułatwienie lub ukrycie naruszenia majątkowych praw autorskich[24].

Naruszenie omówionych zakazów skutkować może odpowiedzialnością zarówno cywilną, jak i karną.

---

[21] Por. M. Lejeune, Protection of Digital Content and Digital Rights Management Technologies under U.S. Copyright Law. [w:] E. Becker (red.), Digital Rights Management...., op. cit., s. 368.
[22] J. Cunard, K. Hill, Ch. Barlas, Current developments..., op. cit., s. 52.
[23] Na temat Por. A. Matlak, Prawo autorskie.., op. cit.,. s.161.
[24] Ibidem

3.3 Dyrektywa UE o harmonizacji niektórych aspektów prawa autorskiego w społeczeństwie informacyjnym z dnia 22 maja 2001 roku

Prawo wspólnotowe porusza kwestię ochrony komponentów aktualnie rozwijających się systemów DRM w treści kilku dyrektyw. Przepisy dyrektywy Rady Wspólnot Europejskich nr 91/250 z dnia 14 maja 1991 roku o ochronie prawnej programów komputerowych przewidują nakaz wprowadzenia regulacji zakazujących wprowadzanie do obrotu lub posiadanie w celach komercyjnych środków służących usuwaniu lub obchodzeniu zabezpieczeń chroniących programy komputerowe (art. 7 ustęp 1 punkt c dyrektywy). Pośrednio problematyki ochrony zabezpieczeń technicznych dotyczą również unormowania dyrektywy 98/94/WE Parlamentu Europejskiego i Rady z dnia 20 listopada 1998 roku w sprawie prawnej ochrony usług opartych na lub polegających na warunkowym dostępie. Choć nie odnosi się ona do ochrony zabezpieczeń technicznych utworów, to nakazuje wprowadzenie regulacji odnoszących się do usług, przy wykorzystaniu których jest obecnie dystrybuowana w Internecie większość prac.

Obecnie najistotniejsze, z punktu widzenia ochrony komponentów systemów Digital Rights Management, regulacje prawa wspólnotowego odnaleźć można w przepisach dyrektywy 2001/29/WE Parlamentu Europejskiego oraz Rady o harmonizacji niektórych aspektów prawa autorskiego w społeczeństwie informacyjnym z dnia 22 maja 2001 roku[25].

Przepisy definiują techniczne środki zabezpieczające jako wszelkie technologie, urządzenia lub komponenty, które przy normalnym trybie eksploatacji są przeznaczone do zapobiegania działaniom lub do ograniczania działań podejmowanych w odniesieniu do dzieł lub innych dóbr chronionych, na które nie zezwoliły osoby uprawnione z tytułu praw autorskich, praw pokrewnych lub praw *sui generis,* związanych z tzw. „nietwórczymi" bazami danych (art. 6 ustęp 3 dyrektywy).

Art. 6 ustęp 1 dyrektywy zakłada podjęcie przez Państwa Członkowskie działań zmierzających ku wprowadzeniu odpowiedniej ochrony prawnej przed usuwaniem skutecznych środków technicznych, w sytuacji gdy osoba podejmująca takie działanie wie lub ma uzasadnione podstawy, by wiedzieć, że realizuje taki cel. W rozumieniu przepisów dyrektywy skuteczny środek techniczny to taki, który prawidłowo spełnia swój cel, polegający na kontrolowaniu sposobów korzystania z dóbr niematerialnych – art. 6 ustęp 3 dyrektywy wskazuje na szyfrowanie, zniekształcenie lub inne sposoby transformacji utworów. Ponadto art. 6 ustęp 2 dyrektywy nakazuje

[25] Opubl. w O.J. L 167, 22 czerwca 2001 r.

wprowadzenie do porządków prawnych Państw Członkowskich zakazów odnoszących się do produkcji, szeroko pojętego obrotu i posiadania dla celów komercyjnych narzędzi pozwalających na ich obchodzenie. Wspomniany zakaz ma dotyczyć urządzeń, produktów lub komponentów (a także świadczenia usług) :

- promowanych, reklamowanych lub wprowadzanych na rynek w celu obejścia skutecznych technicznych środków zabezpieczających lub

- mających jedynie ograniczone znaczenie komercyjne lub przeznaczenie inne niż obchodzenie wspomnianych środków zabezpieczających lub

- zaprojektowanych, wyprodukowanych, przystosowanych lub wykonanych głównie w celu umożliwienia lub ułatwienia obchodzenia wspomnianych środków zabezpieczających

Dyrektywa przewiduje skomplikowaną konstrukcję rozwiązania konfliktów pomiędzy poszanowaniem interesów podmiotów praw autorskich a sytuacją prawną osób legalnie korzystających z utworów. Artykuł 6 ustęp 4 dyrektywy przyznaje w tym względzie pierwszeństwo dobrowolnym działaniom podejmowanym przez podmioty uprawnione z tytułu praw autorskich, włączając w to zawieranie umów. Ingerencja Państw Członkowskich w kwestie poszanowania korzystania z dóbr niematerialnych w ramach dozwolonych użytków jest możliwa dopiero przy braku takich działań.

Zgodnie z art. 6 ustęp 4 dyrektywy, jeżeli osoby uprawnione nie podejmą działań dobrowolnych, łącznie z zawarciem umów z innymi osobami, Państwa Członkowskie podejmą określone kroki zmierzające do zapewnienia, aby osoby uprawnione udostępniały podmiotom mogącym korzystać z użytków publicznych (wskazanych w art. 5 pkt 2a), c), d) i e oraz pkt 3a), b) lub e) dyrektywy) środki umożliwiające korzystanie z takich wyjątków w zakresie jaki jest niezbędny do korzystania z nich[26]. W przypadku dozwolonego użytku osobistego, Państwa Członkowskie mogą podjąć określone kroki przy zaistnieniu bezczynności po stronie podmiotów uprawnionych. Nie dotyczy to jednak wpływania na określenie ilości zwielokrotnień dokonywanych przez użytkowników. Dyrektywa nie precyzuje zarówno kroków, jakie mogą być podjęte przez Państwa Członkowskie, jak i podmioty uprawnione. Wskazanie na zawieranie umów jest jedynie przykładem. Z uwagą należy odnieść się do propozycji rozwiązania problemu dozwolonych użytków i zabezpieczeń technologicznych przez odpowiednie zarządzanie kluczami kryptograficznymi[27]. Ogólnikowość regulacji zawartych w art. 6 ustępie 4 dyrektywy skłania do uwagi, iż proponowane rozwiązanie może budzić poważne problemy w wewnętrznych porządkach

[26] Należy zwrócić uwagę, iż art. 6 nie odnosi się do wszystkich dozwolonych użytków wskazanych w dyrektywie. Państwa Członkowskie nie muszą bowiem podejmować działań wymaganych w świetle owego przepisu w odniesieniu do dozwolonych użytków uregulowanych w art. 5 ust. 3 lit. c), d) oraz f)-o) dyrektywy.

[27] L. Pallas-Loren, Technological protections In Copyright Law – Is more legal protection needed? – referat przedstawiony na konferencji BILETA 2001, http://www.bileta.ac.uk/01papers/loren.html

prawnych[28]. Należy ponadto podkreślić, iż art. 6 ustęp 4 dyrektywy nie ma zastosowania do usług na żądanie[29].

Przepisy nakazują wprowadzenie w porządkach krajowych ochrony informacji służących zarządzaniu prawami autorskimi, a udostępnianych w formie zapisu cyfrowego. Uznaje się za nie wszelkie informacje pozwalające na identyfikację dzieła, twórcy lub innej osoby uprawnionej, a nadto wskazujące na warunki korzystania z utworu oraz wszelkie oznaczenia numeryczne i kodowe przez które są one wyrażane[30]. Artykuł 7 dyrektywy obliguje do wprowadzenia ochrony prawnej przed świadomym i nieuprawnionym usuwaniem lub zmianą owych informacji oraz szeroko pojętym obrotem utworami, z których usunięto informacje służące zarządzaniu prawami autorskimi lub dokonano w nich zmian.

3.4 Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych.

W przepisach ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (dalej przytaczana jako :ustawa) można odnaleźć rozwiązania dostosowujące rodzime prawo do zobowiązań wynikających z dyrektywy UE o harmonizacji niektórych aspektów prawa autorskiego w społeczeństwie informacyjnym, z dnia 22 maja 2001 roku. Art. 6, w punktach 11 i 12, definiuje odpowiednio zabezpieczenia techniczne oraz skuteczne zabezpieczenia techniczne. Technicznymi zabezpieczeniami pozostają wszelkie technologie, urządzenia lub ich elementy, których przeznaczeniem jest zapobieganie działaniom lub ograniczenie działań umożliwiających korzystanie z utworów lub artystycznych wykonań z naruszeniem prawa. W świetle powyższej definicji na równi traktowane pozostają zabezpieczenia funkcjonujące w formie aplikacji dołączonej do pracy, jak i zaimplementowane na poziomie sprzętu komputerowego. Art. 6 punkt 11 za skuteczne zabezpieczenia techniczne uznaje „techniczne zabezpieczenia umożliwiające podmiotom uprawnionym kontrolę nad korzystaniem z chronionego utworu lub artystycznego wykonania poprzez zastosowanie kodu dostępu lub mechanizmu zabezpieczenia, w szczególności szyfrowania, zakłócania lub każdej innej transformacji utworu lub artystycznego wykonania lub mechanizmu zwielokrotniania, które spełniają ten cel". Efektywność narzędzia jest więc rozpatrywana przez pryzmat jego prawidłowego funkcjonowania i osiągania celu, jaki został

[28] Podkreśla się, że wzmocnienie potencjału tkwiącego w art. 6 ustęp 4 dyrektywy mogłoby nastąpić przez oznaczenie przez Państwa Członkowskie terminu, w którym mają być podjęte owe dobrowolne czynności.
Na ten temat por. S.. Stanisławska-Kloc, Autorskoprawna problematyka stosowania zabezpieczeń technicznych przed bezprawnym korzystaniem z utworów i przedmiotów praw pokrewnych, ZN UJ nr 80 z 2002 r., s. 213.

[29] Przesądza o tym treść art. 6 ustęp 4 dyrektywy wskazując iż nie ma on zastosowania do dzieł i innych chronionych dóbr udostępnionych publicznie na umownie uzgodnionych warunkach w taki sposób, że indywidualni odbiorcy (członkowie publiczności) mają do tych dzieł i dóbr dostęp z wybranego miejsca i w wybranym czasie.

[30] Przepisy dyrektywy odnoszą się również do informacji służących zarządzaniu prawami pokrewnymi oraz prawami sui generis do baz danych.

przed nim postawiony. Wypada w tym miejscu wskazać, iż praktyczna ocena skuteczności zabezpieczeń może rodzić pewne problemy, lecz zagadnienie to zostanie szerzej uwypuklone w dalszej części opracowania. Ochrona wspomnianych rozwiązań informatycznych została rozwiązana w sposób dwutorowy - uwzględniając zarówno ewentualną odpowiedzialność cywilną, jak i karną osoby dopuszczającej się ingerowania w prawidłowe funkcjonowanie zabezpieczeń technologicznych. Zgodnie z art. 79 ustęp 3 ustawy regulacje odnoszące się do roszczeń związanych z ochroną majątkowych praw autorskich (tj. art. 79 ustęp 1 i 2) należy stosować odpowiednio w przypadkach usuwania lub obchodzenia technicznych zabezpieczeń przed dostępem, zwielokrotnianiem lub rozpowszechnianiem utworu, jeżeli działania te mają na celu bezprawne korzystanie z utworu. Należy zwrócić uwagę, iż w art. 79 ustęp 3 ustawy zabrakło wskazania, że zakres ochrony obejmuje nie wszelkie zabezpieczenia techniczne, a jedynie te, które pozostają skuteczne.

Karnym aspektem ochrony zabezpieczeń technologicznych pozostaje art. 118^1 ustawy. Zakłada on karalność wytwarzania urządzeń lub ich komponentów przeznaczonych do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych. Jednocześnie za przestępstwo w świetle tego przepisu uznano obrót takimi urządzeniami lub ich komponentami, reklamowanie ich w celu sprzedaży lub najmu, a nadto ich posiadanie, przechowywanie lub wykorzystywanie.

Od chwili wprowadzenia tejże regulacji, art. 118^1 budził szereg wątpliwości wśród przedstawicieli doktryny[31]. Krytyka wynika głównie z wad konstrukcyjnych przepisu, które mogą powodować w praktyce jego stosowania negatywne konsekwencje. Jako przykład należy wskazać to, iż zakazy ujęte w art. 118^1 obejmują narzędzia lub komponenty „przeznaczone" do niedozwolonego usuwania lub obchodzenia zabezpieczeń technicznych. Nie jest to precyzyjne określenie, a więc pozostaje w sprzeczności z zobowiązaniami wynikającymi z art. 6 dyrektywy o harmonizacji niektórych aspektów prawa autorskiego w społeczeństwie informacyjnym. W świetle obowiązującego stanu prawnego wykładnia literalna nie pozwala na jednoznaczną ocenę, czy narzędzie musi być przeznaczone jedynie do ataków skierowanych przeciwko komponentom systemów DRM, czy też może spełniać także inne funkcje.

Rodzimy ustawodawca wprowadził również ochronę informacji na temat zarządzania prawami autorskimi. Art. 6 ustęp 12 ustawy uznaje za nie informacje identyfikujące utwór, twórcę, podmiot praw autorskich lub dotyczące warunków eksploatacji utworu, o ile zostały one dołączone do egzemplarza utworu lub są przekazywane w związku z jego rozpowszechnianiem (w tym kody

[31] Por. J. Barta, R. Markiewicz,. Śluzy szeroko otwarte, Rzeczpospolita z 23 czerwca 2000 r.

identyfikacyjne). Zgodnie z art. 79 ustęp 4 ustawy, w przypadku nieuprawnionego usuwania, dokonywania zmian w zapisach wspomnianych elektronicznych informacji, a także świadomego rozpowszechniania utworu z usuniętymi lub zmienionymi informacjami, odpowiednio stosuje się art. 79 ustęp 1 i 2 (przewidujące roszczenia związane z ochroną majątkowych praw autorskich).

4.0 Konsekwencje wynikające z prawnej ochrony komponentów systemów DRM

Regulacje odnoszące się do ochrony komponentów systemów DRM muszą być precyzyjne, by mogły realizować stawiane przed nimi zadania. Na uwagę zwraca fakt, iż europejskie regulacje w tej mierze zakładają ochronę technologii blokujących lub ograniczających podejmowanie wobec utworów czynności, na które nie wyraziły zgody podmioty uprawnione z tytułu praw autorskich (lub praw sui generis do baz danych). Z kolei traktaty WIPO wyraźnie wskazywały na odnoszenie ochrony zabezpieczeń technologicznych jedynie do respektowania praw autorskich. Zdaniem autora niniejszego opracowania brak wyraźnej „relacji" pomiędzy stosowaniem zabezpieczeń, a ochroną praw autorskich w przepisach dyrektywy z dnia 22 maja 2001 roku o harmonizacji niektórych aspektów prawa autorskiego w społeczeństwie informacyjnym prowadzić może do pewnych praktycznych komplikacji. Brak zgody podmiotów uprawnionych, wyrażony poprzez zastosowanie odpowiednich środków technologicznych, może dotyczyć bowiem także czynności dopuszczalnych w świetle obowiązujących regulacji prawnych. Można bronić poglądu, iż taka wykładnia przepisów nie jest uzasadniona. Zamierzeniem ustawodawcy było bowiem objęcie ochroną jedynie tych rozwiązań technologicznych, które chronią utwory (ewentualnie bazy danych chronione na mocy prawa sui generis). Niemniej jednak uzasadnione pozostają obawy dotyczące objęcia zakresem zastosowań zabezpieczeń technologicznych prac, do których majątkowe prawa autorskie już wygasły bądź informacji, które nie podlegają ochronie na podstawie przepisów gwarantujących poszanowanie uprawnieniom twórców[32].

Nie wskazano przy tym, iż celem obchodzenia zabezpieczeń jest chęć naruszenia praw autorskich[33]. Ataki skierowane przeciwko komponentom systemów Digital Rights Management pozostają więc zakazane przez prawo w oderwaniu od mogących po nich nastąpić naruszeniach

[32] Przykładowo por. K. Koelman, The Public Domain Commodified : Technological Measures and Productive Information Usage, referat przedstawiony na seminarium "The Commodification of Information" Amsterdam 1 i 2 lipca 2004 roku, opracowanie dostępne pod adresem http://cli.vu/pubdirectory/179/manuscript.pdf
[33] T.C. Vinje,Copyright Imperiled?. EIPR 4/1999, s. 199.

majątkowych bądź osobistych praw autorskich. Do takiego wniosku dojść można nawet po pobieżnej analizie art. 6 dyrektywy UE z 2001 roku. Europejskie podstawy ochrony komponentów systemów DRM stawiają podmioty uprawnione w komfortowej pozycji w stosunku do konsumentów dóbr niematerialnych. Może okazać się przy tym, iż zapewnienia co do przyszłości dozwolonych użytków, wyrażone w art. 6 ust. 4 dyrektywy nie zrekompensują do końca obaw podmiotów powołujących się dotychczas w swoich działaniach na instytucje dozwolonych użytków.

Należy zwrócić uwagę, iż DMCA oraz analizowana dyrektywa UE odnoszą się zarówno do samego faktu obchodzenia zabezpieczeń technicznych jak i tzw. czynności przygotowawczych związanych z takimi działaniami. Traktaty WIPO w tej kwestii nie wskazywały wyraźnie na zakres czynności, które powinny zostać objęte zakazem w porządkach krajowych. W doktrynie wyprowadzano wniosek o odnoszeniu się przepisów jedynie do aktów obchodzenia zabezpieczeń[34]. Na marginesie trzeba ponownie zaznaczyć, iż amerykańskie przepisy w konfrontacji z poszczególnymi wyjątkami od zakazu nienaruszalności komponentów systemów DRM w różny sposób podchodzą do legalności produkcji i dystrybucji narzędzi pozwalających na obchodzenie zabezpieczeń.

Wyzwaniem stawianym przez regulacje odnoszące się do ochrony zabezpieczeń technicznych jest kwestia oceny efektywności konkretnego rozwiązania przez pryzmat gwarancji poszanowania praw autorskich. Dyrektywa w art. 6 ustęp 1 przewiduje bowiem ochronę jedynie skutecznych (efektywnych) rozwiązań technicznych. Ustawa DMCA z kolei wskazuje na „efektywną kontrolę" gwarantowaną przez komponenty systemów DRM[35]. Trudno w tej mierze wyprowadza jakieś generalne definicje, czy przesłanki odnoszące się do komponentów technologicznych. Rozwój informatyczny sprawia bowiem, iż skuteczność zabezpieczeń nie może być oceniana w oderwaniu od aktualnie dostępnych metod i środków pozwalających na zweryfikowanie ich bezpieczeństwa. Pomocne może okazać się porównywanie rozwiązania z poprzednio dostępnymi na rynku zabezpieczeniami, zakres jego komercyjnego wykorzystania[36], dostępność środków potencjalnie ułatwiających możliwość obchodzenia zabezpieczenia a także koszty, wysiłek i nakład czasu związany z podejmowaniem takich prób. Skuteczność zabezpieczenia można rozpatrywać również przez odwołanie się do stabilności, kompletności i pozbawienia błędów funkcjonalnych konkretnego zabezpieczenia. Praktyczne konsekwencje wprowadzenia skuteczności zabezpieczenia jako przesłanki przyznania mu ochrony sprowadzają się

[34] Por. T. Foged, Us v EU..., op. cit. , s. 530.
[35] J. Cunard, K. Hill, Ch. Barlas, Current developments..., op. cit., s. 49.
[36] Można zaryzykować tezę, iż im bardziej powszechne zastosowania komercyjne danego rozwiązania, tym większe narażenie go na próby przełamywania i obchodzenia przez użytkowników.

do realnego ograniczenia zakresu ochrony komponentów DRM. Przepisy nie będą chronić bowiem prymitywnych rozwiązań technologicznych, faktycznie nie zabezpieczających utworów..

Można tutaj – moim zdaniem – zastosować daleko idące porównanie z regulacjami rodzimego prawa karnego odnoszącymi się do karalności uzyskania nieuprawnionego dostępu do systemu komputerowego (art. 267 § 1 kodeksu karnego z dnia 6 czerwca 1997 roku)[37]. Rozważanie popełnienia przestępstwa hackingu jest możliwe, gdy osoba nieuprawniona uzyskała dostęp do informacji po uprzednim przełamaniu chroniących je zabezpieczeń. Komentatorzy wskazują na potrzebę utożsamiania w tym przypadku zabezpieczeń z środkami realnie chroniącymi informacje przed dostępem osób postronnych[38]. Z pewnością nie jest wystarczające tutaj odwołanie się jedynie do symbolicznych zabezpieczeń, odpowiadających gatunkowo standardowej informacji „nieuprawnionym wstęp wzbroniony" bez połączenia jej z mechanizmami egzekwującymi ów zakaz. Środki techniczne chroniące informacje (system komputerowy, w którym są one przechowywane) muszą być realne i funkcjonować poprawnie w chwili przełamywania ich przez hackera[39]. Podobnie w przypadku zabezpieczeń technologicznych, chronionych na podstawie przepisów prawa autorskiego, wymagane pozostaje spełnienie przez nich celu ograniczania lub wyłączania skuteczności konkretnych działań. Wyłącza to spod zakresu omawianych regulacji odnoszących się do prawidłowego funkcjonowania systemów DRM, rozwiązania prymitywne, skupiające się bardziej na ostrzeganiu użytkowników niż wprowadzaniu w życie ograniczeń. Wątpliwe pozostaje choćby uznanie za efektywną metodę kontroli korzystania z utworu poprzez stosowanie haseł w przypadku, gdy pominięcie wprowadzenia kodu nie wpływa na ograniczenie uprawnień użytkownika. Linia obrony zarówno osoby obchodzącej zabezpieczenia, jak i podmiotu udostępniającego w swojej ofercie niezbędne do tej czynności narzędzia, może sprowadzać się do wykazania braku efektywności rozwiązania technicznego poddanego „atakowi". Kontrowersyjne może okazać się jednak rozważanie zgodności z prawem czynności polegających na wykorzystaniu luki w zabezpieczenia – przykładowo poprzez zastosowanie odpowiedniej kombinacji klawiszy klawiatury.

Równie istotnym zagadnieniem pozostaje odpowiedź o klasyfikację konkretnego narzędzia jako odpowiadającego zakresowi przepisów zakazujących tzw. czynności przygotowawczych odnoszących się do zabezpieczeń technologicznych. Głównym celem urządzeń (lub usług) musi być bowiem obchodzenie wspomnianych komponentów informatycznych. Przemawiać ma za tym promowanie wspomnianych narzędzi jako użytecznych w przypadku

[37] Nie chodzi bynajmniej o zastosowanie analogii a jedynie wskazanie pewnego podobieństwa w traktowaniu z jednej strony zabezpieczeń technologicznych jako „efektywne" a z drugiej strony warunkom stawianym zabezpieczeniom chroniącym informacje, do których uzyskuje dostęp hacker.
[38] Por. A. Adamski, Prawo karne komputerowe. C.H. Beck 2000, s. 53-54.
[39] Ibidem

obchodzenia zabezpieczeń, bądź marginalne komercyjne znaczenie ich innych właściwości. Ustawodawca amerykański i europejski w tej kwestii posługuje się zbliżonymi kryteriami. W przypadku najistotniejszych właściwości urządzenia można posiłkować się celem towarzyszącym jego twórcy. Nie zawsze będzie to jednak prowadzić do prawidłowych wniosków[40]. Założenia przytaczanych regulacji prowadzą do przyjęcia, iż dystrybucja narzędzia o wielu właściwościach, w tym niektórych przydatnych w trakcie obchodzenia zabezpieczeń technicznych, uznana być powinna za zgodną z prawem. Wyjątkiem będzie sytuacja, w której funkcja urządzenia, z reguły programu komputerowego, będzie sprowadzać się przede wszystkim do obchodzenia zabezpieczeń. Jak to jednak ocenić? Odwołując się od szacunków procentowych? Wiele wskazuje, iż często pozostanie odwołanie się do opinii biegłych, rozważających właściwości i funkcjonalność narzędzi informatycznych wywołujących wątpliwości z punktu widzenia przepisów chroniących zabezpieczenia techniczne. Wskazane dylematy nie mają jedynie waloru teoretycznego. Wspomnianej ocenie mogą być poddane chociażby aplikacje pozwalające na „odzyskiwanie haseł". Przykładowo dokumenty tworzone w formacie .doc oraz .pdf mogą być chronione poprzez skorzystanie przez użytkownika z kodów dostępu. Zwłaszcza w przypadku plików odczytywanych przez Adobe Reader popularnością cieszy się blokowanie w ten sposób możliwości kopiowania części dokumentu, czy też modyfikowania go. Obecnie w Internecie dostępne są programy pozwalające na automatyczne „odgadnięcie" hasła i usunięcie nałożonych na dokument ograniczeń. Jak wynika z reklam i ofert znajdujących się na witrynach internetowych, mają one jednakże służyć uprawnionym użytkownikom, którzy zapomnieli wprowadzonego wcześniej kodu. Jeszcze większe trudności mogą wiązać się z oceną dopuszczalności oferowania aplikacji pozwalających na stworzenie kopii zapasowej (backup) oprogramowania chronionego przed zwielokrotnianiem za pomocą zabezpieczeń technicznych. W chwili obecnej trudno też odpowiedzieć na pytanie, czy dystrybucja kodu źródłowego programu służącego do obchodzenia zabezpieczeń technicznych w świetle rozwiązań unijnych jest zabroniona[41].

Duże wątpliwości wywołuje problem pogodzenia funkcjonowania systemów DRM z instytucjami tzw. dozwolonych użytków. Monopol autorski nie jest bowiem absolutny, a przepisy przewidują szereg sytuacji, w których doznaje on ograniczeń. Pomijając ich zróżnicowane uzasadnienie, należy podkreślić, iż stanowią one integralną część regulacji mających za przedmiot ochronę interesów podmiotów uprawnionych z tytułu praw autorskich. Rozwiązania technologiczne stanowią pewnego rodzaju novum w konfrontacji z dozwolonymi użytkami. Definiowanie

[40] Zbliżony nieco problem jawi się przy interpretacji znamion art. 269b kodeksu karnego, odnoszącego się do problemu tzw. „narzędzi hackerskich".
[41] Kod źródłowy pozostaje jedną z form wyrażenia utworu jakim jest program komputerowy. Szerzej na temat prawnych aspektów kodu źródłowego por. K. Gienas, Wypowiedź w kodzie. Computerworld 15/2004, s. 41.

uprawnień użytkowników korzystających z utworów zabezpieczanych w ten sposób musi być niezwykle precyzyjne. Tylko dzięki temu maszyna-komputer będzie w stanie je poprawnie przeanalizować i wprowadzić w życie. W środowisku elektronicznym brak jest miejsca na elastyczność, możliwość różnych efektów wykładni tych samych przepisów. Dochodzą do tego ograniczenia wynikające z wewnętrznej struktury języków definiowania uprawnień (REL), które zawierają słowniki dopuszczalnych pojęć, ich definicji oraz zwrotów, które mogą być wykorzystywane do opisu relacji - podmiot uprawniony z tytułu praw autorskich a użytkownik. Komputer nie jest w stanie „rozpoznać", czy generalnie zakazane działanie w konkretnej sytuacji powinno być uznane za dozwolone. Konsekwencją takiego stanu rzeczy pozostaje uniemożliwienie podjęcia przez użytkownika danej czynności. Implementacja w formie REL zakazu kopiowania będzie odnosić się do każdej próby zwielokrotnienia utworu. Z punktu widzenia systemu Digital Rights Management nie będzie miało tu znaczenia przykładowo to, iż kopiowanie mieści się w ramach dozwolonego użytku prywatnego. Prozaicznym przykładem konfrontacji między DRM a ograniczeniami praw autorskich pozostaje prawo cytatu. Maszyna w chwili obecnej nie jest w stanie ocenić, czy część utworu jest kopiowana w celu skorzystania z tego uprawnienia.

Przepisy amerykańskie przewidziały szereg wyjątków, ustanawiających po stronie użytkowników „right to hack", sprowadzające się do możliwości ingerowania w poprawne funkcjonowanie zabezpieczeń technicznych. Abstrahując od kierowanych pod adresem DMCA zarzutów, należy wskazać, iż jest to metoda prostsza niż standard wypracowany przez prawodawcę europejskiego. Brzmienie art. 6 ustęp 4 dyrektywy o harmonizacji niektórych aspektów prawa autorskiego w społeczeństwie informacyjnym nie pozwala na wyprowadzenie generalnej dopuszczalności prawa do usuwania zabezpieczeń technicznych utworów. Implementacja przepisów w wewnętrznych porządkach prawnych wskazuje, iż koncepcja wprowadzenia „right to hack" na gruncie europejskim nie znalazła uznania[42]. Na marginesie trzeba wspomnieć o wyprowadzaniu przez niektórych autorów uprawnienia do deaktywacji komponentów systemów DRM z uwagi na utożsamianie instytucji dozwolonych użytków z prawem podmiotowym służącym użytkownikom[43]. Analiza tej kwestii wykracza jednakże poza zakres rozważań poczynionych w niniejszym opracowaniu.

[42] Por. S. Lewinski, Rights Management Information and Technical Protection Measures as Implemented in EC Member States. International Review of Intellectual Property and Competition Law 7/2004, s. 844-849.
[43] J. Marcinkowska, Dozwolony użytek w prawie autorskim. Podstawowe zagadnienia. Zakamycze 2004, s. 283-287.

5.0 Uwagi końcowe.

Generalnie przepisy prawa autorskiego przewidują pewne ograniczenia w szeregu działań podejmowanych przez użytkowników w stosunku do utworów. Wypada wspomnieć chociażby o karalności sporządzania nieuprawnionych kopii utworów, potrzebie oznaczania w postanowieniach licencyjnych pól eksploatacji utworu. Pozwala to na przyjęcie pewnego poziomu kontroli nad korzystaniem z dóbr niematerialnych. Nie ma on jednakże charakteru absolutnego i doznaje znaczących ograniczeń w funkcjonowaniu instytucji prawnych określanych zbiorczym mianem dozwolonych użytków. Z kolei potencjalnie rzecz ujmując, dzięki zabezpieczeniom technicznym kontrola nad zdigitalizowanym utworem stała się niemal perfekcyjna. Rozwój systemów DRM pozwala bowiem na kontrolę szeregu czynności użytkownika, nie poprzestając jedynie na blokowaniu możliwości sporządzenia kopii utworu. Prowadzi to do uzasadnionych obaw, związanych przede wszystkim ze zbyt daleko idącą kontrolą dostępu do informacji. Z punktu widzenia podmiotów uprawnionych możliwość czerpania korzyści majątkowych z każdej formy eksploatacji utworów stanowi kuszącą perspektywę. Nic dziwnego więc, iż komponenty DRM używane są do analizy częstotliwości i czasu korzystania z utworu. Tego typu podejście do problemu eksploatacji dzieł w cyfrowej postaci prowadzi faktycznie do sytuacji, gdy twórcy (i podmioty majątkowych praw autorskich) korzystać mogą z szerszej gamy uprawnień, niż wynikająca z regulacji prawa autorskiego.

Można mieć więc uzasadnione obawy, czy prawna ochrona nienaruszalności systemów DRM nie jest w istocie swego rodzaju „koniem trojańskim", przynoszącym ze sobą szereg skomplikowanych problemów z punktu widzenia konsumentów. Zasadniczy cel, którym jest poszanowanie uprawnień podmiotów praw autorskich, wydaje się zagwarantowany poprzez stosowanie zabezpieczeń technologicznych. Technologiczna „samopomoc" kusi jednak możliwościami wprowadzania restrykcji, których prawo autorskie pierwotnie nie przewidywało. Tego typu redefinicja dotychczasowych uprawnień twórców jawi się jako zagrożenie dla interesów ogółu, a w szczególności dostępu do dóbr niematerialnych na zasadach wynikających z instytucji dozwolonych użytków.

W XIX wieku chińscy żeglarze jeszcze przed wpłynięciem do portu przekazywali istotne informacje swoim kontrahentom poprzez wywieszanie odpowiednich bander[44]. W XXI wieku podmioty uprawnione z tytułu majątkowych praw autorskich używając, a czasem nadużywając,

[44] K. Gienas, Kryptografia, prywatność, prawo, tekst opublikowany w październiku 2000 roku w serwisie internetowym http://www.vagla.pl

zabezpieczeń technicznych przekazują również istotną wiadomość. Być może nadchodzi nowa era prawa autorskiego. Czas, w którym to technika będzie wyznaczać relacje pomiędzy interesami majątkowymi, a oczekiwaniami odbiorców dóbr niemajątkowych. I z pewnością nie będą one wyważone. Można mieć jedynie nadzieję, iż wyrażona powyżej teza jest zbyt pesymistyczna, a odpowiednie stosowanie regulacji prawnych odnoszących się do nienaruszalności komponentów systemów Digital Rights Management zapobiegnie ewentualnym nadużyciom.