CBKE
e-BIULETYN

09F911029D74E35BD84156C5635688C0 – niewiele znaczący ciąg znaków czy symbol rewolucji?

Rzecz o skutecznych technicznych zabezpieczeniach przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów.

Wiktor Kożuch

Absolwent wydziału Prawa i Administracji Uniwersytetu Śląskiego

Absolwent wydziału Organizacji i Zarządzania Politechniki Śląskiej (specjalizacja: Informatyka w Przedsiębiorstwie)

Prawnik w Kancelarii Radców Prawnych D. Malirz M. Wójtowicz i Wspólnicy w Katowicach.

Podczas gdy krajowa społeczność internetowa pochłonięta jest dyskusją na temat niedawnego zatrzymania tłumaczy-amatorów tłumaczących ścieżki dialogowe do filmów, na świecie w centrum zainteresowania znalazł się tytułowy ciąg znaków, a w raz z nim dyskusja o przyszłości zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów (przede wszystkim systemów typu DRM - Digital Rights Managment).

W niniejszym artykule postaram się przedstawić faktyczne i prawne aspekty stosowania zabezpieczeń typu DRM, w szczególności w kontekście dyrektywy 2001/29/WE Parlamentu Europejskiego w sprawie określonych aspektów prawa autorskiego i praw pokrewnych w społeczeństwie informacyjnym, obwiązującego polskiego prawa autorskiego, jak też w świetle planowanej jego nowelizacji w związku z planami implementacji wyżej wymienionej dyrektywy.

Ponadto spróbuję odnieść się do skutków ujawnienia sposobów przełamywania kolejnych zabezpieczeń tego typu.

Tajemniczy tytułowy ciąg znaków.

Na początek należy wyjaśnić czym jest *09F911029D74E35BD84156C5635688C0*. Ten niewiele znaczący ciąg liter i cyfr jest liczbą zapisaną w systemie szesnastkowym i odpowiada liczbie 13.256.278.887.989.457.651.018.865.901.401.704.640 (trzynaście sekstylionów) zapisanej w systemie dziesiętnym. Ciąg ten okazał się być kodem który otwiera dostęp do filmów (i nie tylko) zapisanych na płytach HD-DVD i Blu-Ray Disc (następna po CD i DVD generacja płyt) zabezpieczonych systemem Advanced Access Content System (AACS). Technologia ta została opracowana kosztem setek milionów dolarów (dokładne koszty opracowania tej technologii nie zostały ujawnione) przez konsorcjum złożone z m.in. z takich firm jak Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Brothers, IBM, Toshiba i Sony. W zamyśle twórców technologia ta miała być platformą pozwalającą „zarządzać" prawami autorskimi do utworów (przede wszystkim filmów) zapisanych na dyskach nowej generacji - HD-DVD i Blu-Ray Disc. Miała pozwolić ona na wprowadzenie ograniczeń m.in. w zakresie kopiowania zabezpieczonych płyt, typu stosowanego odtwarzacza, tzw. „regionów" czy minimalnych wymagań co jakości odtwarzanego utworu. Mimo, że prace nad tą technologią nadal trwają, pojawiające się na rynku amerykańskim pierwsze płyty HD-DVD i Blu-Ray Disc zostały nią już zabezpieczone. Oficjalne zatwierdzenie tego standardu i podpisanie umów licencyjnych przez uczestników konsorcjum było planowane na połowę roku 2007.

Krótka historia o złamaniu AACS czyli setki milionów dolarów wyrzucone w błoto.

Początek końca AACS rozpoczął się w grudniu 2006. Użytkownik forum Doom9 posługujący się pod nickiem muslix64 opowiedział swoją historię. Do konsoli do gier na początku grudnia dokupił odtwarzacz dysków HD-DVD. Wraz z odtwarzaczem otrzymał w ramach promocji dysk z filmem. Niestety dysk był zabezpieczony technologią AACS, a wprowadzone przez wydawcę restrykcje powodowały że do obejrzenia filmu wymagane było posiadanie wysokiej jakości telewizora lub monitora. Muslix64 takich nie posiadał, ale nadal chciał obejrzeć otrzymany

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

film. Dlatego postanowił go skopiować na dysk, tak aby móc później swobodnie obejrzeć go na zwykłym monitorze komputerowym. Jak chwali się muslix64 złamanie zabezpieczenia zajęło mu około dwa tygodnie, i pod koniec grudnia zeszłego roku na forum tym muslix64 najpierw opublikował dowód na złamanie zabezpieczenia dysku, a następnie opisał wykonaną procedurę, jednocześnie publikując narzędzie które średnio-zaawansowanemu użytkownikowi pozwalało samodzielnie załamać zabezpieczony tą technologią dysk. W kolejnych tygodniach mechanizm ten był udoskonalany przez społeczność internatów. Prawdziwy przełom nastąpił pod koniec kwietnia 2007 roku gdy, pewien użytkownik portalu społecznościowego Digg opublikował tytułowy kod usuwający wszelkie zabezpieczenia AACS. Temat ten podchwyciło kilku użytkowników portalu, i być może fakt ten nie odbył by się większym echem, gdyby nie fakt usunięcia, na żądanie konsorcjum któremu powierzono stworzenie AACS, przez administratorów Digg'a wszystkich wpisów zawierających ten kod. Dalsze wypadki zaskoczyły wszystkich. Internauci oburzeni cenzurą i próbą ograniczenia wolności słowa, nieraz nawet nie widząc czym jest tajemniczy ciąg znaków, zaczęli go masowo rozpowszechniać zarówno w samym Digg'u (którego administratorzy nie nadążali z kasowaniem kolejnych wpisów) jak i w całym Internecie (w klika dni na świecie powstało około 1,3 miliona stron na ten temat). Oczywiście konsorcjum odpowiedzialne za AACS zapowiedziało że kod zostanie zmieniony (wszystkie odtwarzacze HD-DVD i Bly-Ray Disk musiały przejść proces aktualizacji wewnętrznego oprogramowania). Jednak pod koniec maja został upubliczniony nowy kod (455FE10422CA29C4933F95052B792AB2), a pewna firma sprzedające oprogramowanie do odtwarzania filmów na komputerach zapowiedziała że posiada technologię która pozwala jej uzyskać każdy kolejny kod.

Jeszcze nieco historii czyli jak łamano inne zabezpieczenia.

Złamanie AACS nie było pierwszą spektakularną „wpadką" z systemami typu DRM. Już wcześniej podobnym systemem były zabezpieczane płyty DVD (dość szybko złamane dzięki czemu np. dziś niemal powszechne są odtwarzacze DVD multi-region), czy płyty CD z muzyką (dość nieudolnie zabezpieczane, do ich obejścia wystarczyło np. przytrzymanie klawisza Shift w momencie wkładania płyty do odtwarzacza komputerowego, czy zamalowania odpowiedniego fragmentu płyty czarnym mazakiem). Jedną z ciekawszych prób wprowadzenia systemu DRM na płytach CD z muzyką było dołączenie przez SONY do zabezpieczonych płyt niewielkiego

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

programu który instalował się w momencie próby odtworzenia płyt na komputerze stacjonarnym, praktycznie bez wiedzy użytkownika (jednocześnie w związku z błędami w kodzie tego programu stwarzał on ryzyko potencjalnego ataku hackerów na komputer z zainstalowanym tym programem). Po serii pozwów przed amerykańskie sądy SONY musiało się wycofać z tego pomysłu, a w ramach rekompensaty, niezadowolonym użytkownikom zaoferować darmowe płyty.

W tym miejscu należy jeszcze wspomnieć w kilku słowach o zabezpieczeniach stosowanych przez producentów gier i programów komputerowych. Tu też od lat próbuje zabezpieczać się nośniki przed kopiowaniem czy użytkiem wykraczającym poza przewidziane przez producenta ramy. Jak się łatwo domyśleć wszystkie te zabezpieczenia zostały przełamane. Jednak producenci gier i programów są w o tyle uprzywilejowanej sytuacji że w czasach powszechnego dostępu do Internetu mogą oprzeć swoje zabezpieczenia wprowadzając tzw. aktywację internetową. Rozwiązanie to mimo że o wiele skuteczniejsze niż wszystkie opisane dotychczas, to jednak i tu hackerzy potrafią przełamać większość zabezpieczeń opartych na tym mechanizmie. Ponadto, tego typu zabezpieczenia na razie nie są możliwe do zastosowania dla innych mediów, gdyż powszechny dostęp do Internetu przez inne niż komputer urządzenia (telewizor, kino domowe czy wieża HiFi) mimo iż jest od lat zapowiadany to nie został wprowadzony nawet w najbardziej rozwiniętych krajach świata.

Co na to prawo ?

Bój w wirtualnym świecie pomiędzy koncernami wdrażającymi coraz nowocześniejsze zabezpieczenia typu DRM a hackerami te zabezpieczenia przełamującymi to nie wszystko. Podobne spory toczą się na forum parlamentów wielu krajów oraz parlamentu europejskiego gdzie zgłaszane są kolejne propozycje aktów prawnych regulujących tę kwestię. Zdając sobie z tego sprawę że stworzenie doskonałego systemu DRM jest praktycznie niemożliwe koncerny niemal otwarcie lobbują za jak najszerszą ochroną swoich systemów dostępnymi środkami karnymi. Dotychczasowym największym zwycięstwem koncernów fonograficznych i audiowizualnych (chodzi tu przede wszystkim o tzw. wielką czwórkę: Universal, Sony BMG, Warner oraz EMI, które łącznie zarządzają np. prawami do około 70% światowej muzyki) jest uchwalenie w 1998 roku przez Senat USA ustawy „The Digital Millennium Copyright Act (DMCA)" (dostępna pod adresem:
http://thomas.loc.gov/cgi-bin/toGPO/http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf). Ustawa ta, uważana do dziś za jedno

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

z najnowocześniejszych uregulowań prawa autorskiego w dobie technik cyfrowych, zawiera szczegółowe unormowania dotyczące ochrony systemów typu DRM, oraz penalizuje łamanie tego typu systemów. Ograniczona objętość niniejszego artykułu nie pozwala szerzej zająć się zawartymi w tym akcie prawnym regulacjami. Z Polskiego punktu widzenia, o wiele bardziej interesująca jest „europejska wersja" amerykańskiej DMCA. Za taką jest uważana 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 (polskojęzyczny tekst dostępny jest na stronie: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:01:PL:HTML, zwana dalej, od angielskiego Europeian Union Copyright Directive – EUCD). Dyrektywa ta w art. 6 ust. 1 zawiera kluczowy, z punktu widzenia niniejszego artykułu zapis mówiący: „*Państwa członkowskie przewidują stosowną ochronę prawną przed omijaniem skutecznych środków technicznych przez osobę, której znane jest lub w zależności od okoliczności, musi być znane, że zmierza ona w tym celu*.". Abstrahując od nieco niezrozumiałego brzmienia tego zapisu, to ten przepis w głównej mierze decyduje o prawnej ochronie systemów typu DRM. Kończąc ten fragment należy zauważyć że tylko dwa państwa (Czechy i Szwajcaria) wdrożyły tę dyrektywę w pełni, natomiast w znacznej części została wdrożoną przez Wielką Brytanię (2003), Finlandię (2005) oraz Francję (2006, ustawą zwaną DADVSI, co notabene odbiło się szerokim echem podczas prowadzonej w czasie uchwalania tej ustawy kampanii prezydenckiej). W Polsce jedynie w minimalnym zakresie implementowana tą dyrektywę ustawą z 1 kwietnia 2004 roku (w raz z innymi poprawkami do ustawy o prawie autorskim uchwalanymi przed wejściem Polski do UE). 25 kwietnia 2006 został przez Ministerstwo Kultury i Dziedzictwa Narodowego ogłoszony projekt ustawy implementującej tę dyrektywę niemal w pełni, jednak wobec jego powszechnej krytyki (o czym za chwilę), został on odłożony ad calendas graecas.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

Czym są z prawnego punktu widzenia „skuteczne techniczne zabezpieczenia”?

a) dyrektywa EUCD,

Dyrektywa ta jak już to zostało zauważone, nakazuje państwom członkowskim „*ochronę prawną przed obchodzeniem skutecznych środków technologicznych*”. Następująco definiuje ona zastosowane pojęcia:

a) "środki technologiczne" rozumie się wszystkie technologie, urządzenia lub części składowe, które przy normalnym funkcjonowaniu są przeznaczone do powstrzymania lub ograniczenia czynności w odniesieniu do utworów lub innych przedmiotów objętych ochroną, które nie otrzymały zezwolenia od podmiotu prawa autorskich lub prawa pokrewnego prawu autorskiemu przewidzianego przez prawo lub prawa sui generis przewidzianego w rozdziale III dyrektywy 96/9/WE.

b) *Środki technologiczne uważa się za "skuteczne", jeżeli korzystanie z chronionego utworu lub z innego przedmiotu objętego ochroną jest kontrolowane przez podmioty praw autorskich poprzez zastosowanie kodu dostępu lub mechanizmu zabezpieczenia, takiego jak szyfrowanie, zakłócanie lub każdej innej transformacji utworu lub przedmiotu objętego ochroną lub mechanizmu kontroli kopiowania, które spełniają cel ochronny.*

Odnoście definicji przedstawionej powyżej w punkcie a) wydaje się że jest ona na tyle szeroka aby objąć wszystkie kategorie stosowanych zabezpieczeń. W tym także programy komputerowe, gdyż w taką formę zabezpieczenia te mają najczęściej. Trafnie, moim zdaniem, chcąc osiągnąć zakładany cel prawodawca europejski posługuje się sformułowaniem „technologie” nie wskazując kategorii do której technologie te muszą należeć (w szczególności bez odwoływania się do techniki, co do której przynależność programów komputerowych jest dyskusyjna).

O wiele bardziej wątpliwa jest definicja „skuteczności” przedstawiona powyżej w punkcie b). W szczególności uzasadnione wątpliwości budzi zwrot „korzystanie z chronionego utworu (...) jest kontrolowane przez podmioty praw autorskich”. W związku z tym powstaje pytanie kiedy następuje „utrata kontroli”? Czy jakiekolwiek przełamanie zabezpieczenia, nawet przez pojedynczą osobę, będzie utratą kontroli? Czy być może taką utratą kontroli (rozumianej jako kontrola

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

powszechna) będzie dopiero publicznie sposobów i narzędzi na tyle że staną się one powszechnie wykorzystywane? Czy wreszcie być może nawet zastosowanie zabezpieczeń powszechnie łamanych w prosty sposób będzie elementem kontroli który pozostanie nadal? Na pytania te doktryna dotychczas nie udzieliła żadnej odpowiedzi. Jedyne szerzej komentowane opinie pochodzą ze strony wydawców i dystrybutorów, którzy jednoznacznie stwierdzają iż prawidłowy jest pogląd mówiący o istnieniu kontroli nadal, pomimo powszechnego dostępu narzędzi do przełamywania zabezpieczeń. Pogląd ten mimo iż w pewnym zakresie można mu przyznać rację (bo czy zamykając mieszkanie, nawet zamkiem bardzo starego typu, który można otworzyć spinką do włosów, nie zachowujemy kontroli nad dostępem do mieszkania, a każda próba wejścia do mieszkania bez klucza nie będzie włamaniem ?), jako skrajnie stronniczy nie może być przedmiotem szerszych rozważań.

Należy w tym miejscu zwrócić uwagę na bezprecedensowe wydarzenie. Europejska społeczność internetowa dnia 25 maja 2007 roku z niepokojem oczekiwała na wyrok... Sądu Dystryktu Helsinki w Finlandii. Był to pierwszy wyrok sądu w kraju członkowskim UE który już choć w części implementował dyrektywę EUCD, dotyczący kwestii „skuteczności". Sąd ten orzekł że skuteczny, znaczy tyle co „spełniający cel jakiemu został stworzony". Tym samym system CSS (chroniący płyty DVD), bo jego złamania dotyczył rzeczony wyrok, przestał spełniać cel w jakim został stworzony (kontrolowanie korzystania z utworu przez podmiot uprawniony) w momencie gdy w 1999 roku norweski hacker przełamał to zabezpieczenie, a w Internecie pojawiły się powszechnie dostępne metody i programy do przełamywania tego typu zabezpieczeń. Jest to wyrok o tyle przełomowy co... przekreślający praktycznie całkowicie idee karania za przełamywanie skutecznych zabezpieczeń technicznych (przynajmniej w Finlandii). Zgodnie z jego tezą, można przyjąć że taki fakt jak „przełamie skutecznych technologicznych zabezpieczeń" praktycznie nigdy nie zaistnieje, ponieważ z momentem ich przełamania, stają się one nieskuteczne.

Oczywiście wyrok pojedynczego sądu w jednym z państw członkowskich UE nie daje jakichkolwiek podstaw do przejęcia zaproponowanej przez ten sąd interpretacji niejasnych pojęć dyrektywy. Jedyną wiążącą interpretację może wydać jedynie Europejski Trybunał Sprawiedliwości, który dotychczas nie zajmował się tego typu sprawą.

Jak w świetle dyrektywy zostałoby zakwalifikowane przełamanie AACS jest niezwykle trudno określić. Jeśli nawet początkowa procedura wykonana przez użytkownika Muslix64, jeśli tylko byłby obywatelem któregoś z państw członkowskich, mogłaby zostać potraktowana jako

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

„*obchodzenie skutecznych środków technologicznych*" zabezpieczających utwory (rozwiązanie przed grudniem 2006 uważano za skuteczne, a Musklix64 je przełamał, co udowodnił), to już ujawnienie kodu odblokowującego rodzi uzasadnione wątpliwości co do kwalifikacji takiego czynu. A to z kilku powodów: po pierwsze AACS już w grudniu 2006 przestało być zabezpieczeniem skutecznym, po drugie wcale nie jest pewne że użytkownik który kod ujawnił w Internecie sam skorzystał z niego przełamując zabezpieczenia, po trzecie kod ten jest oryginalnym kodem producenta zabezpieczenia i posłużenie się nim nie jest przełamaniem zabezpieczeń, tylko ich dezaktywacją zgodnie z przyjętą procedurą.

b) w świetle obowiązującego polskiego prawa autorskiego, oraz w związku z planowaną jego nowelizacją.

Nowelizacją prawa autorskiego z dnia 1 kwietnia 2004 roku (która weszła w życie 1 maja 2004 roku – w dniu wejścia polski do Unii), która w zamyśle ustawodawcy miała dostosowywać polskie do prawodawstwa Unijnego w tym dyrektywy EUCD, wprowadzono do ustawy o ochronie praw autorskich i prawach pokrewnych następujące definicje:

a) technicznymi zabezpieczeniami są wszelkie technologie, urządzenia lub ich elementy, których przeznaczeniem jest zapobieganie działaniom lub ograniczenie działań umożliwiających korzystanie z utworów lub artystycznych wykonań z naruszeniem prawa;

b) *skutecznymi technicznymi zabezpieczeniami są 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 kontroli zwielokrotniania, które spełniają cel ochronny;*

oraz następujący przepis karny (art. 118^1):

1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

urządzeniami lub ich komponentami, albo reklamuje je w celu sprzedaży lub najmu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Ta skromna regulacja, wobec niezwykle skomplikowanego problemu jakim są systemy DRM, jest z pewnością niewystarczająca. Ponadto regulacja ta świadczy o pewnym „braku spójnej koncepcji" ustawodawcy. Głównym zarzutem kierowanym przeciwko tej regulacji jest posłużenie się niewłaściwymi sformułowaniami.

Ustawa posługuje się pojęciem „zabezpieczenia techniczne". Mimo zdefiniowania tego pojęcia jako „wszelkie technologie" istnieje uzasadniona wątpliwość czy w pojęciu tym zawierają się także rozwiązania informatyczne (programy komputerowe) które stanowią większość ze stosowanych obecnie rozwiązań typu DRM. Wątpliwość powstała ta w szczególności wobec bardzo bogatego orzecznictwa i doktryny z zakresu prawa własności przemysłowej, które jednoznacznie wyłącza poza zakres techniki rozwiązania informatyczne (zaliczając je w zakres rozwiązań matematyczno-logicznych). Mimo iż poglądy te zostały wyrażone w związku z dyskusją o dopuszczalności patentowa programów komputerowych i dotyczą odrębnej gałęzi prawa, nie ma podstaw aby na gruncie prawa autorskiego technikę definiować w diametralnie różny.

Dostrzegając te i inne „niedociągnięcia" (m.in. brak uregulowania stosunku pomiędzy ochroną zabezpieczeń przed łamaniem, a dozwolonym użytkiem osobistym) pierwotnej implementacji dyrektywy EUCD, podjęto prace nad ponowną nowelizacją prawa autorskiego w tym zakresie. Efektem tego jest projekt ustawy o zmianie ustawy o prawie autorskim i prawach pokrewnych przygotowany przez Ministerstwo Kultury i Dziedzictwa Narodowego i datowany na dzień 25 kwietnia 2006 roku (dostępny na stronach Ministerstwa pod adresem: http://www.mkidn.gov.pl/website/document/?docId=419). Głównym założeniem tego projektu ma być właśnie uzupełnienie implementacji do prawa polskiego dyrektywy EUCD.

Ustawa ta, w zakresie tematyki niniejszego artykułu, zmienia ustawę o prawie autorskim w następujący sposób:
Przytoczone wyżej definicje kształtuje następująco:
a) technicznymi zabezpieczeniami są wszelkie technologie, urządzenia lub ich elementy, których przeznaczeniem jest zapobieganie działaniom lub ograniczenie działań umożliwiających korzystanie z utworów lub przedmiotów praw pokrewnych z naruszeniem prawa;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

b) skutecznymi technicznymi zabezpieczeniami są techniczne zabezpieczenia umożliwiające podmiotom uprawnionym kontrolę nad korzystaniem z chronionego utworu lub przedmiotu prawa pokrewnego poprzez zastosowanie kodu dostępu lub mechanizmu zabezpieczenia, w szczególności szyfrowania, zakłócania lub każdej innej transformacji utworu lub przedmiotu praw pokrewnych, lub mechanizmu kontroli zwielokrotniania, które spełniają cel ochronny;

Natomiast brzmienie przepisów karnych zmienia na następujące:

1. Kto wytwarza urządzenia, ich komponenty lub programy komputerowe przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami, ich komponentami lub programami komputerowymi albo reklamuje je w celu sprzedaży lub najmu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.
2. Kto posiada, przechowuje lub wykorzystuje urządzenia, ich komponenty lub programy komputerowe, o których mowa w ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Jak widać ten projekt nowelizacji w niekonwencjonalny sposób usuwa (a w zasadzie jedynie stara się usunąć) wątpliwości które postały na gruncie dotychczasowego brzmienia tych przepisów. Mianowicie zamiast odejść od sformułowania „środki techniczne" (w ramach którego nie mieści się kategoria programów komputerowych) Ministerstwo postanowiło zmodyfikować przepis karny w ten sposób że penalizuje m.in. wytwarzanie, posiadanie i wykorzystywanie programów komputerowych służących do obchodzenia skutecznych technicznych zabezpieczeń. Zabieg taki może sugerować iż, abstrahując od uznanego na gruncie prawa własności przemysłowej pojęcia techniki, zamiarem ustawodawcy było w tym konkretnym przypadku objęcie tym pojęciem także programów komputerowych. Jednak moim zdaniem, skuteczność tego zabiegu jest niewielka ponieważ to że zabezpieczenia techniczne mogą być łamane za pomocą programów komputerowych wcale nie determinuje tego iż zabezpieczenia te mogą być także programami komputerowymi. Jednak ostateczne rozstrzygnięcie tej kwestii leży w gestii doktryny i orzecznictwa, które ukształtuje się po ewentualnym wejściu w życie tych przepisów.

Ciekawa kwestia wynikła także z proponowanego brzmienia art. 118^1, szczególnie w zakresie ustępu 2, gdzie zapisano sankcję karną do roku pozbawienia wolności już za samo

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

posiadanie programów komputerowych służących do usuwania skutecznych technicznych zabezpieczeń. Propozycja ta nie tylko wywołała uzasadnioną krytykę w środowisku prawników interesujących się prawem nowych technologii, ale także w pośród... zwykłych użytkowników komputerów! Bo oto, zgodnie z projektem, przestępcą mógł się stać każdy posiadacz nagrywarki komputerowej do której najczęściej załączany jest program służący do nagrywania ponieważ popularne oprogramowanie do nagrywania, także to dodawane nieodpłatnie do nagrywarek potrafi obejść praktycznie każde zabezpieczenie, a dodatkowo jest ono zazwyczaj sukcesywnie aktualizowanie, tak aby móc obchodzić także nowo tworzone zabezpieczenia. Krytyka ta była na tyle skuteczna (stosowne artykułu pojawiły się nawet w fachowej prasie informatycznej, nie publikującej dotychczas artykułów „prawniczych") że Ministerstwo zawiesiło tymczasowo prace nad tym kontrowersyjnym projektem ustawy, uznając że nie ma on charakteru pilnego, gdyż Polska implementowała już w pełni dyrektywę EUCD nowelizacją z 1 kwietnia 2004 roku (z czym, wobec argumentacji przedstawionej w poprzednim akapicie nie sposób się zgodzić).

Na marginesie należy zauważyć że nie byłby to jedyny (delikatnie mówiąc) nieprzemyślany przepis, penalizujący tak naprawdę już samo posiadanie zwykłego komputera (a w zasadzie wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom). Bo oto art. 269b k.k. w związku z art. 269a k.k. każe pozbawienia wolności podlega każdy kto „wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe służące do (...)" m.in. „(...) nieuprawnionego usunięcia danych teleinformatycznych". Jak łatwo się domyślić każdy komputer z zainstalowanym nawet najprostszym systemem operacyjnym posiada funkcję „Delete", która pozwala skasować dowolny plik z praktycznie dowolnego nośnika (dyskietki, dysku twardego, klipsa USB itp.). Jest więc przystosowany także do usuwania plików „cudzych", do których usuwania nie mamy uprawnień. Tak więc w momencie dokonywania zakupu (pozyskania) laptopa, na którym piszę niniejszy artykuł stałem się... przestępcą.

Wracając do tematyki niniejszego artykułu – systemów DRM – należy zauważyć że w Polsce o prawnych aspektach technicznych zabezpieczeń przed kopiowaniem (jak i zresztą także o innych związkach prawa z informatyką) dyskutuje się niewiele. Głównie dlatego że krajowi wydawcy niezwykle rzadko stosują systemy DRM. Jest to efektem co najmniej kilku czynników:

a) Licencje na nowoczesne systemy DRM są drogie, i wydawców nie stać jest na zabezpieczenia swoich wydawnictw tymi systemami.
b) W naszym kraju istnieje tzw. „przyzwolenie społeczne" na piractwo komputerowe (a w raz z nim też na łamania zabezpieczeń utworów). Także podejście organów ścigania do

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

tego typu przestępstw pozostaje nadal dalekie od oczekiwań (w ostatnich miesiącach nieco się to zmieniło czego dowodem są kolejne zatrzymania podejrzanych o „piractwo"). Najlepszym przykładem tego stanu rzeczy jest fakt, że w kronikach policyjnych, pośród coraz liczniejszych spraw prowadzonym przeciwko osobom łamiącym prawa autorskie, nie pojawiła się prawdopodobnie jeszcze żadna sprawa osoby której zarzucałoby popełnienie czynu określonego w art. 118^1 ustawy o prawie autorskim (przełamywanie skutecznych technicznych zabezpieczeń)

c) W Polsce istnieje szeroka definicja „dozwolonego użytku osobistego". Tymczasem stosowanie zabezpieczeń typu DRM uniemożliwia realizację niektórych ustawowych uprawnień użytkowników. Stosowanie zabezpieczeń typu DRM a realizacja uprawnień przewidzianych w ustawie o prawie autorskim wynikających z tzw. „dozwolonego użytku osobistego" jest tematem niezwykle interesującym, jednak na tyle szerokim, że mógłby być z powodzeniem przedmiotem odrębnego opracowania o zbliżonej objętości.

Jak chwali się wydawca (firma SP Records), jedną z pierwszych płyt CD krajowego wykonawcy, zabezpieczonych systemem DRM, jest wydana w... maju tego roku płyta zespołu Kazika Staszewskiego „El Dópa – Gra ?" (co nie jest do końca prawdą bo wcześniej zostały wydane zabezpieczone płyty m.in. Smolika, Myslovitz czy Budki Suflera, jednak zabezpieczenia te były stosowane dotychczas jedynie w limitowanych rozszerzonych edycjach kolekcjonerskich). Zastosowane dla tej płyty zabezpieczenie nie pozwala odtworzyć jej przy pomocy komputerowego odtwarzacza płyt CD. O niewielkiej skuteczności zastosowanego zabezpieczenia niech świadczy fakt że jest ono aktywne jedynie na komputerach z systemem operacyjnym Windows (korzystanie z jakiegokolwiek innego systemu operacyjnego, np. Linux, pozwala ponoć na odtwarzanie i kopiowanie tej płyty na komputerze bez jakikolwiek przeszkód).

Na koniec tej części rozważań krótka próba analizy przedstawianych na wstępie wydarzeń związanych z przełamaniem systemu AACD w świetle polskiego prawa. Tu wydają się aktualne wszystkie tezy przytoczone w analogicznym fragmencie dotyczącym interpretacji dyrektywy EUCD. Ewentualna odpowiedzialność kogokolwiek zależałaby od interpretacji pojęcia „skuteczne zabezpieczenia", w szczególności przez określenie momentu w którym podmiot uprawniony traci „kontrolę" nad korzystaniem z chronionego utworu. A w zakresie ujawnionego kodu, nawet przy szerokiej interpretacji „skuteczności" można by ewentualnie rozważyć odpowiedzialność osoby która wprowadziła sporny kod do urządzenia (komputera czy kina domowego) i dzięki temu

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

urządzenie to stało by się urządzeniem przeznaczonym do omijania zabezpieczeń. Natomiast samo uzyskanie, czy posiadanie w swoich zasobach spornego kodu, nie jest przestępstwem, gdyż kod ten (liczba), wobec braku technicznego charakteru, nie może być uznana za „komponent urządzenia".

Czyżby rodziło się nowe podejście do DRM ? Opinie o DRM po załamaniu AACS.

Na początek należy zauważyć że do dnia dzisiejszego na temat przyszłości zabezpieczeń typu DRM nie wypowiedzieli się najbardziej zainteresowani – tj. koncerny z tzw. „wielkiej czwórki". Jednakże, niejako w ich imieniu niezwykle ciekawe oświadczenie wydało konsorcjum odpowiedzialne za wdrożenie AACS. 25 maja 2007 roku organizacja AACS LA wydała oświadczenie w którym... zachęca członków organizacji do zmiany podejścia do modelu licencjonowania utworów tak aby zastosowane zabezpieczenia nie ograniczały ich „dozwolonego (uczciwego) użytku" w szczególności prawa do sporządzenia kopii na własne potrzeby (np. celem korzystania z nich w urządzeniach przenośnych typu MP3-player). Oczywiście co uważniejsi obserwatorzy rynku, dostrzegli w tej deklaracji, z jednej strony chęć przerzucenia odpowiedzialności za złamanie AACS na koncerny które swoją polityką bardzo restrykcyjnych ograniczeń „zmuszają" hackerów do łamania kolejnych systemów tego typu, a z drugiej strony chęcią pozyskania środków na kolejne badania nad systemem który umożliwiałby kopiowanie utworów w pewnym zakresie, natomiast w innym blokował taką możliwość. Pomijając motywację twórców AACS, warto zauważyć że głos ten pochodzi ze środowiska twórców zabezpieczeń. Wypowiadając się niejako przeciw „samym sobie" z pewnością nie robią tego bezpodstawnie. Ich głos powinien być moim zdaniem potraktowany jako swego rodzaju deklaracja iż, nie zależnie od nakładów finansowych, nie jest możliwe stworzenie naprawdę skutecznego zabezpieczenia typu DRM.

Kolejnym ciekawym głosem, jaki pojawił się po pierwszym przełamaniu systemu AACS jest list otwarty Steve'a Jobs'a z 6 lutego 2007 roku w sprawie DRM (list dostępny jest pod adresem: http://www.apple.com/hotnews/thoughtsonmusic/). Jobs jest współzałożycielem korporacji Apple, która jest właścicielem największego sklepu z utworami muzycznymi na świecie – iTunes. Apple zabezpiecza sprzedawane przez siebie utwory systemem DRM o nazwie FairPlay, który ogranicza kopiowanie i dystrybuowanie utworów. Steve Jobs w swoim liście wypowiada się stanowczo przeciwko systemom DRM. Uważa że stosowanie DRM służy jedynie „wojnie" pomiędzy

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

informatykami związanymi z wielkimi koncernami a hackearami przełamującymi kolejne zabezpieczenia.. Co do FairPlay stosowanego w iTunes, Jobs tłumaczy że jest on wymogiem narzuconym przez koncerny „wielkiej czwórki”, i mimo chęci nie może od niego odstąpić.

Także koncerny muzyczne, mimo że żaden z nich nie wydał w tej sprawie oficjalnego oświadczenia, także starają się wyciągnąć wnioski z ostatnich zdarzeń. Koncern EMI (dysponujący muzyką takich wykonawców jak: Kylie Minogue, Robbie Williams, The Beatles czy Norah Jones) w maju zaczął wprowadzanie do największych internetowych sklepów muzycznych plików wolnych od DRM. Już podpisał umowy na dystrybucję plików bez zabezpieczeń z sklepami: Amazon, eMusic oraz iTunes. Jest to na razie pierwszy krok, i jak się okazuje muzyka bez zabezpieczeń jest droższa od tej zabezpieczonej (dla sklepu iTunes jest to odpowiednio: 0,99$ za jeden utwór z DRM i 1,29$ za utwór bez DRM). Ponadto w plikach wolnych od zabezpieczeń dystrybuowanych przez iTunes odkryto zaszyfrowane informacje pozwalające identyfikować nabywcę konkretnego pliku (można przypuszczać że podobne informacje są ukryte w plikach EMI pozbawionych DRM sprzedawanych przez pozostałe sklepy). Myślę że nie trzeba dodawać że po zidentyfikowaniu w pliku takich danych, zgodnie z deklaracjami hackerów zamieszczonych na forach internetowych już zostały podjęte pierwsze próby opracowania prostego sposobu usuwania tych danych.

Co dalej z DRM ???

Jak to zostało wykazane powyżej, ochrona utworów za pomocą systemów typu DRM okazała się praktycznie całkowicie nieskuteczna. Na nic zdały się setki milionów dolarów wydane na coraz bardziej zaawansowane rozwiązania informatyczne. Zabezpieczenia były, są i będą łamane przez hackerów, którzy wydają się być zawsze o krok przed „specjalistami”. A w świecie „globalnej wioski” metody i narzędzia opracowane przez hackerów pozwalające w prosty sposób obejść każde zabezpieczenie stają się powszechne... tak naprawdę zanim metoda zabezpieczeń zacznie być naprawdę stosowana. Na nic także najbardziej restrykcyjne prawo (uchwalone, czego nie ukrywają koncerny, dzięki ich lobbingowi którego koszt jest szacowany również na setki milionów dolarów). Nawet najbardziej „nowoczesne” rozwiązania prawne, pozostają w tyle za niezwykle dynamicznie rozwijającym się światem informatycznym. Ponadto styk informatyki i prawa rodzi wiele problemów, których efektem jest taktowanie tego zagadnienia przez prawników oraz organa ścigania „po macoszemu” (jeśli są problemy ze zrozumieniem niektórych aspektów

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

prawa to lepiej go pominąć, szczególnie że wokół jest o wiele więcej „poważnych" tematów na badania naukowe, czy „prawdziwych" przestępców których trzeba ścigać).

Dla całości oglądu sprawy należy także przedstawić racje wydawców utworów, dla których systemy DRM są (a w zawadzie już chyba „były") pomysłem na obronę własnych, poniekąd słusznych, interesów.

Utwory (szczególnie muzyka i filmy komercyjne) już dawno przestały być „dobrami kultury", do których równy dostęp jest prawnie zagwarantowany. Stały się zwykłym, masowym, towarem. Dlatego trudno odbierać prawa koncernom do dowolnego decydowania o prawie do rozpowszechniania utworu zgodnie z włąsną wolą. Ograniczenia, nawet te wkraczające w zakres dozwolonego użytku osobistego (który notabene jest pojęciem nieco archaicznym, i wobec tak dynamicznego rozwoju technik komunikacji i dostępu do mediów, powinien moim zdaniem, szczególnie w Polsce, gdzie jest on niezwykle szeroki, zostać „zredukowany" i zbliżony do zakresu anglosaskiego „uczciwego użytku" – fair use) powinny, w związku z ogólną zasadą ochrony własności, także tej intelektualnej, być szanowane.

Podsumowując można z niemal z pewnością stwierdzić że los systemów typu DRM jest przesądzony. Wraz z rozwiązaniami prawnymi które miały je chronić, pozostaną jedynie epizodem rewolucji technologicznej jaką obecnie przeżywamy, wraz z przestrogą dla kolejnych pokoleń że olbrzymie pieniądze można kupić wiele (najnowszą technologię, a nawet prawo) ale nie można ograniczyć potęgi powszechnej komunikacji.

Jeśli nie zaawansowane technologie informatyczne, wzmocnione sankcjami karnymi to co?

Powyższe pytanie pozostawiam otwarte. Mam nadzieję że obecna ogólnoświatowa dyskusja na ten temat pozwoli wypracować nowe rozwiązania które z jednej strony zapewnią twórcom i wydawcom prawo do dowolnego kształtowania uprawnień odbiorców, a z drugiej strony nie ograniczą dostępu odbiorców do sztuki, także tej komercyjnej. Jedno jest pewne: ujawnienie metody na unieszkodliwienie systemu AACS, a w dalszej kolejności uniwersalnego kodu tego systemu, jeszcze przed jego powszechnym zastosowaniem z pewnością zmieni świat nowych technologii.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone