

平成 21 年度経済産業省委託調査

# コンテンツの技術的手段に係る 各国法制度調査研究報告書

平成 22 年 3 月  
西村あさひ法律事務所



## は し が き

明治大学特任教授、東京大学名誉教授

中山 信 弘

コンテンツ産業は、資源のないわが国としては、今後強化して行かねばならない分野であり、知的財産戦略計画でも夙に指摘されており、また政府として力を入れている。ところがわが国のコンテンツ産業の成長率は、世界の平均を遙かに下回っているのが現状である。そこで、海外諸国との比較において、法的・技術的観点から、わが国のコンテンツ産業の置かれている状況を正確に把握することがまず第一歩となろう。

コンテンツ産業の振興という観点からは、ビジネス・モデルの構築や、資本、技術等の問題が大きいであろうが、主として法的観点からの問題点を浮き上がらせることも重要である。違法複製物を減少させるためには、コンテンツの利用・流通の促進するシステムを構築する必要がある。このためには複製しにくい技術の開発をし、ネットにおける違法著作物の防止を図る一方で、正規著作物を安価・容易かつ安全な方法で入手できるようにもする必要がある。Kindleや iPad のように、世界的に新技術と新ビジネス・モデルが模索されており、わが国も遅れを取ってはならない。コンテンツを安価にするためには、権利処理に係るトランザクション・コストを減少させる必要もある。今回の権利者不明の場合の著作権法改正は若干の進歩ではあるが、デジタル時代には余りに不十分である。特に映像著作物の場合は、権利者が多数存在しており、難しい問題となっている。自由主義経済社会においては、自由な契約による処理が最も好ましいことは言うまでもないが、社会、文化、経済の諸側面での豊富化を実現するためにコンテンツの流通を促し、これを通じて新たなコンテンツの創作を活性化させる上で、何らかの法的な措置が必要となるかもしれない。いずれにせよ、権利者への還元の原資を豊富化させるとともに、コンテンツは無料であるという風潮を打破しなければならない。

これらの課題は、法律を改正するだけでは解決できないが、平成21年著作権法改正で、違法サイトからのダウンロードを、私的使用目的であっても違法としたことは、かかる風潮への歯止めとなる第一歩であると考えられる。今後俎上に登る問題としては、プロバイダーの責任、規制される行為の多様化（たとえば、製造・展示・輸出の違法化や規制強化）、アクセス・コントロール、三振制、罰則の新設、税関での輸入規制（ボーダーメジャー）等が考えられ、それらと並んで、フェアユース等の権利制限規定の見直しも必要となろう。中でもアクセス・コントロールは大きな議論となるであろうが、アクセス・コントロール技術は利用の仕方によっては過度の情報保護になったり、あるいは独占の助長

に繋がる面も有しており、その法的保護のあり方を考える上ではこのような側面に十分留意する必要があるばかりでなく、知的財産法と独禁法の関係についても、改めて認識する必要が出てこよう。

他方で、ネットの世界は自由であるべきであるという発想は極めて強く、世界的にみても規制を強めることには強い反対も予想される（局面は全く異なるがグーグルと中国政府の争いも、ネットは自由であるべきか否かという争いであろう）。しかしながら、規制の程度は違法状態の蔓延の状況との比較考量で決められるべきであろうと考えられる。そして、デジタル情報には事実上国境がないことを勘案すれば、この問題はわが国だけが孤立した政策を採ることはできず、模倣品・海賊版拡散防止条約（ACTA）に向けての動きに代表されるように、国際的な協調が極めて重要であるし、またわが国がリーダーシップを取るべきであろう。いずれにしても、この問題を検討するに当たっては、諸外国の状況を正確に把握する必要があり、日本を含め調査対象国として EU 諸国（イギリス、フランス、ドイツ）、米国、中国及び韓国の各国法制度を扱う本報告書が、今後の各種国際交渉や施策展開の基礎として活用され、我が国の今後の法制度のあり方についての考察を行う際の一助になることを期待している。

<<執筆担当者一覧>>

西村あさひ法律事務所

弁護士 川合 弘 造

弁護士 大向 尚 子

弁護士 藤井 康次郎

弁護士 濱野 敏彦

中国法弁護士 吳 亭 (中国報告書担当)

中国法アドバイザー 申 昌国(中国報告書担当)

韓国法弁護士 金 基泰(韓国報告書担当)

明治大学特任教授・東京大学名誉教授・弁護士 中山 信弘 (オブザーバ)

<海外協力事務所>

Cleary Gottlieb Steen & Hamilton LLP (EU 報告書及び米国報告書担当)

金・張法律事務所 (Kim & Chang) (韓国報告書担当)

金杜律師事務所 (KING & WOOD) (中国報告書につき協力)



## 目 次

### 第 1 編 技術的手段の保護に関する各国法制度比較

### 第 2 編 各国法制度調査報告書

#### I コンテンツの技術的手段に係る各国法制度調査研究(日本編)

1. コンテンツの技術的手段に関する国際ルール	7
(1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)	7
(2) 日本における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容	9
2. コンテンツの技術的手段に関する法令等	10
(1) 該当する法令等	10
(2) 法令等の規制内容	13
(3) 除外行為	20
(4) 救済措置	21
(5) いわゆる「無反応機器」規制	23
3. 裁判例、執行状況、被害状況等	24
(1) コンテンツの技術的手段に関する裁判例	24
(2) コンテンツの技術的手段に関する執行状況	26
(3) コンテンツの技術的手段に関する被害状況	26
4. 技術動向の調査	27
(1) コンテンツの技術的手段に関する技術動向(平成 11 年法改正当時から現在への比較)	27
(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術	28
(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況	28
5. 各国内の議論(規制に対する賛否・改正動向等)	29
(1) コンテンツの技術的手段に関する現行規制に対する議論	29
(2) コンテンツの技術的手段に関する規制に対する業界からの要望状況	31
(3) 法改正の動向・内容	31

(関連条文)

著作権法	33
不正競争防止法	39
民法	42
関税法	42
II コンテンツの技術的手段に係る各国法制度調査研究 (EU 編)	
1. コンテンツの技術的手段に関する国際ルール	43
(1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)	43
(2) EU における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容	43
2. コンテンツの技術的手段に関する法令等	43
(1) 該当する法令等	43
(2) 法令等の規制内容	45
(3) 除外行為	49
(4) 救済措置	54
(5) いわゆる「無反応機器」規制	57
3. 裁判例、執行状況、被害状況等	58
(1) コンテンツの技術的手段に関する裁判例	58
(2) コンテンツの技術的手段に関する執行状況	60
(3) コンテンツの技術的手段に関する被害状況	60
4. 技術動向の調査	60
(1) コンテンツの技術的手段に関する技術動向	60
(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術	62
(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況	62
5. 各国内の議論(規制に対する賛否・改正動向等)	63
(1) コンテンツの技術的手段に関する現行規制に対する議論	63
(2) コンテンツの技術的手段に関する規制に対する業界からの要望状況	63
(3) 法改正の動向・内容	64

(参考訳文(抄訳))



別紙 1 自由貿易協定・経済連携協定	66
別紙 2 フランス法	73
別紙 3 イギリス法	81
別紙 4 ドイツ法	89
Ⅲ コンテンツの技術的手段に係る各国法制度調査研究(米国編)	
1. コンテンツの技術的手段に関する国際ルール	95
(1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)	95
(2) 米国における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容	95
2. コンテンツの技術的手段に関する法令等	95
(1) 該当する法令等	95
(2) 法令等の規制内容	96
(3) 除外行為	97
(4) 救済措置	99
(5) いわゆる「無反応機器」規制	101
3. 裁判例、執行状況、被害状況等	101
(1) コンテンツの技術的手段に関する裁判例	101
(2) コンテンツの技術的手段に関する執行状況	103
(3) コンテンツの技術的手段に関する被害状況	104
4. 技術動向の調査	104
(1) コンテンツの技術的手段に関する技術動向	104
(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術	104
(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況	104
5. 各国内の議論(規制に対する賛否・改正動向等)	104
(1) コンテンツの技術的手段に関する現行規制に対する議論	104
(2) コンテンツの技術的手段に関する規制に対する業界からの要望状況	105
(3) 法改正の動向・内容	105

(参考訳文(抄訳))

別紙 1	106
オーストラリア 第 17 章	106
韓国 第 18 章	109
シンガポール 第 16 章	112
別紙 2 米国著作権法	115
IV コンテンツの技術的手段に係る各国法制度調査研究(韓国編)	
1. コンテンツの技術的手段に関する国際ルール	125
(1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)	125
(2) 韓国における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容	125
2. コンテンツの技術的手段に関する法令等	127
(1) 該当する法令等	127
(2) 法令等の規制内容	128
(3) 除外行為	131
(4) 救済措置	132
(5) いわゆる「無反応機器」規制	135
3. 裁判例、執行状況、被害状況等	135
(1) コンテンツの技術的手段に関する裁判例	135
(2) コンテンツの技術的手段に関する執行状況	135
(3) コンテンツの技術的手段に関する被害状況	135
4. 技術動向の調査	135
(1) コンテンツの技術的手段に関する技術動向	135
(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術	136
(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況	136
5. 各国内の議論(規制に対する賛否・改正動向等)	136
(1) コンテンツの技術的手段に関する現行規制に対する議論	136
(2) コンテンツの技術的手段に関する規制に対する業界からの要望状況	137
(3) 法改正の動向・内容	137

Exhibit 1	CHAPTER EIGHTEEN INTELLECTUAL PROPERTY RIGHTS	138
Exhibit 2	CHAPTER TEN INTELLECTUAL PROPERTY	141
Exhibit 3	著作権法関連条文 著作権法施行令関連条文	149
Exhibit 4	旧コンピュータプログラム保護法関連条文	150
Exhibit 5	オンラインデジタルコンテンツ産業発展法関連条文	154
Exhibit 6	ソニーモッドチップ判決	156
Exhibit 7	任天堂判決	158
V コンテンツの技術的手段に係る各国法制度調査研究(中国編)		
1.	コンテンツの技術的手段に関する国際ルール	160
	(1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)	160
	(2) 中国における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容	160
2.	コンテンツの技術的手段に関する法令等	160
	(1) 該当する法令等	160
	(2) 法令等の規制内容	165
	(3) 除外行為	171
	(4) 救済措置	172
	(5) いわゆる「無反応機器」規制	178
3.	裁判例、執行状況、被害状況等	178
	(1) コンテンツの技術的手段に関する裁判例	178
	(2) コンテンツの技術的手段に関する執行状況	182
	(3) コンテンツの技術的手段に関する被害状況	182
4.	技術動向の調査	182
	(1) コンテンツの技術的手段に関する技術動向	182
	(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術	183
	(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況	183
5.	各国内の議論(規制に対する賛否・改正動向等)	183
	(1) コンテンツの技術的手段に関する現行規制に対する議論	183

(2) コンテンツの技術的手段に関する規制に対する業界からの要望状況	185
(3) 法改正の動向・内容	185
(関連条文)	
著作権法	186
著作権法実施条例	187
コンピューター・ソフトウェア保護条例	188
ネットワーク伝播権保護条例	188
著作権集管理条例	192
2006年司法解釈	193
民法通則	193
民法通則意見	194
刑法	194
知的財産権税関保護条例	195
不正競争防止法	198
資料 A 現地報告書 (EU 編) (英文)	
資料 B 現地報告書 (米国編) (英文)	

## 第1編 技術的手段の保護に関する各国法制度比較



## 1. はじめに

本編では、本件調査対象国(日本、EU(加盟国であるフランス、イギリス及びドイツを含む)、米国、韓国及び中国)における技術的手段に関する条約、技術的手段に関する法令、保護対象技術、規制対象装置等、無反応機器、規制対象行為、刑事的制裁の有無、水際措置、例外規定等及び競争法との関係についての概要を記載する。詳細については、第2編の各国報告書をご参照いただきたい。

## 2. 技術的手段に関する条約

WIPO 著作権条約第 11 条及び WIPO 実演・レコード条約第 17 条において、各加盟国は、技術的手段の回避について適切な法的救済を定めるべきである旨規定されている。

技術的手段に関する規定を有する FTA 又は EPA として、日本が当事者となっているものとしては、日タイ EPA 及び日フィリピン EPA が存在する。米国が当事者となっているものとしては、米ヨルダン FTA、米チリ FTA、中米自由貿易協定(CAFTA)等多数の FTA が存在する。EU が当事者となっているものとしては、現時点で批准には至っていないものの、EU 韓 FTA が締結過程にある。韓国が当事者となっているものとしては、韓米 FTA 及び韓 EU FTA が存在する。中国については、技術的手段に関する規定を有する FTA 又は EPA は存在しない。

また、現在、米国、EU、日本等の先進国を中心に、模倣品・海賊版拡散防止条約(ACTA)が議論されているところ、そのアジェンダにおいて「第四節 デジタル環境における権利の執行」に関する項目の1つとして「技術的保護手段の回避(例外と制限の適用を含む)」の場合における救済措置の適用可能性が挙げられている<sup>1</sup>。

## 3. 技術的手段に関する法令

日本法においては、著作権法及び不正競争防止法において、技術的手段の保護が規定されている。

EU 指令においては、コンピュータ・プログラム以外の著作物等に関して著作権指令が、コンピュータ・プログラムに関してはコンピュータ・プログラム指令が、各々技術的手段についての規律を定めており、その国内実施にあたり、フランスでは知的財産法、イギリスでは著作権・意匠・特許法、ドイツでは著作権法において技術的手段の保護が規定されている。

米国においては、著作権法において技術的手段の保護が規定されている。

韓国においては、著作権法及びオンラインコンテンツ製作者を保護するために制定されたオンラインデジタルコンテンツ産業発展法において技術的手段の保護が規定さ

---

<sup>1</sup> <http://www.mofa.go.jp/mofaj/gaiko/ipr/atca09.html>  
[http://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/atca09\\_ja\\_ka.pdf](http://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/atca09_ja_ka.pdf)

れており、いずれの法律の規定にも該当する場合には、著作権法が優先的に適用される(オンラインデジタルコンテンツ産業発展法 21 条)。

中国では著作権法、著作権法に関する条例及び司法解釈において技術的手段の保護が規定されている。

本件調査対象国において、技術的手段の保護については、日本以外の国では著作権法を中心とする法律によって規定されている。

#### 4. 保護対象技術

日本法においては、著作権法及び不正競争防止法によりコンテンツの技術的手段に対する保護が図られている。著作権法における保護対象技術は、「技術的保護手段」(著作権法第 2 条第 1 項第 20 号)であり、著作権法はコピーコントロールのみを規制し、アクセスコントロールは規制していない。一方、不正競争防止法における保護対象は、「技術的制限手段」(不正競争防止法第 2 条第 7 項)であり、コピーコントロール及びアクセスコントロールを規制している。

EU 指令においては、コンピュータ・プログラム以外の著作物等及びコンピュータ・プログラムのいずれについても、保護対象技術は技術中立的に規定されており、コピーコントロール及びアクセスコントロールの両方を規制対象としている(著作権指令第 6 条第 3 項、コンピュータ・プログラム指令第 7 条第 1 項(c))。

米国法においても、保護対象技術は技術中立的に規定されており、コピーコントロール及びアクセスコントロールの両方を規制対象としている。

韓国法において、著作権法及びオンラインデジタルコンテンツ産業発展法における保護対象技術は、いずれも技術中立的であるが(著作権法第 2 条第 28 号及びオンラインデジタルコンテンツ産業発展法第 2 条 10 号)、コピーコントロールのみを規制するのか、それともコピーコントロール及びアクセスコントロールの両方を規制するのか明らかではない。

中国法においては、保護対象技術は技術中立的に規定されており、コピーコントロール及びアクセスコントロールの両方を規制している。

#### 5. 規制対象装置等

日本法においては、問題となる装置等の機能の観点から規制対象装置等を定めている。すなわち、著作権法における規制対象装置等は、「技術的手段の回避を行うことを専らその機能とする装置」等と規定されており、また、不正競争防止法における規制対象装置等は、「営業上用いられている技術的制限手段・・・により制限されている映像・・・を当該技術的制限手段の効果を妨げることにより可能とする機能のみを有する装置」等と規定されている。韓国法においても、「主な目的とする」との文言はあるが、機能面から規制対象装置等が定められているとみられる。すなわち、著作権法においては、技術的保護措置を除去・変更・迂回する等して無力化することを主



な目的とする技術・サービス・製品・装置またはその主要部品を規制対象としている(著作権法第124条第2項)。また、オンラインデジタルコンテンツ産業発展法においては、技術的保護措置の回避・除去または変更を主な目的とする技術・サービス・装置またはその主要部品を規制対象としている(オンラインデジタルコンテンツ産業発展法第18条第2項)。

これに対して、EU指令のうち著作権指令(コンピュータ・プログラム以外の著作物等)及び米国法においては、機能という観点からのみでなく、問題となる装置等の(1)販売状況、(2)マーケットからみた機能・用法及び(3)製造等の目的の3つの各観点から広く規制対象装置を捕捉している。すなわち、EU指令のうち著作権指令においては<sup>2</sup>、コンピュータ・プログラム以外の著作物等については、(i)効果的な技術的手段の回避を目的として宣伝され、広告され、もしくは市販されたもの、(ii)効果的な技術的手段の回避の他には、限られた商業上の重大な目的もしくは利用方法しか存在しないもの、(iii)専ら効果的な技術的手段の回避を可能にし、もしくは容易にする目的で設計、製造、適合もしくは実行されるもののいずれかに該当する装置等を規制している(著作権指令第6条第2項(a)乃至(c))。また、米国法においても、(i)技術的手段を回避することを主たる目的として、設計または製造されたもの、(ii)技術的手段を回避する以外には、限定された商業上の目的または用法しか有さないもの、(iii)技術的手段を回避するために使用することを知っている者またはこの者に協力する者によって販売されたもののいずれかに該当する装置等を規制対象としている(デジタルミレニアム著作権法第1201条(a)(2)(A)乃至(C)、同条(b)(1)(A)乃至(C))。

中国法においては、著作権法では行為のみを規制しており、規制対象装置等を定める規定は存在しない。

## 6. 無反応機器

日本法においては、いわゆる無反応機器については、著作権法及び不正競争防止法のいずれにおいても規制対象となっていない。

EU指令、フランス法、イギリス法、ドイツ法、韓国法及び中国法のいずれにおいても、無反応機器に対する特別な規定は存在しない(無反応機器が規制対象となるか否かは、上記各国法等の規制対象装置等の定義に該当するかによる)。

米国においては、特定のアナログ・ビデオカセットレコーダー及び一定のデジタル音声録音装置についてのみ若干無反応機器に関する規制がなされている(著作権法第10章及び著作権法第1201条(k))。

---

<sup>2</sup> なお、EU指令のうちコンピューター・プログラム指令においては、技術的手段を回避することを容易にすることを唯一の目的とするあらゆる手段のみを規制対象としている(コンピューター・プログラム指令第7条第1項)。

## 7. 規制対象行為

日本法においては、回避行為自体は著作権法及び不正競争防止法のいずれにおいても規制対象行為となっていない(但し、著作権法第30条第1項第2号により、「技術的保護手段の回避」により可能となり、又はその結果に障害が生じないようになった複製を、その事実を知らずに行う場合は規制対象となっている。)。韓国法においても、著作権法及びオンラインデジタルコンテンツ産業発展法のいずれにおいても、回避行為自体は規制対象行為となっていない。EU指令においては、コンピュータ・プログラム以外の著作物等については、一定の回避行為が規制対象行為になっているのに対して(著作権指令第6条第1項)、コンピュータ・プログラムについては、回避行為自体は規制対象行為とはなっていない。米国法においては、アクセスコントロールについては回避行為自体が規制対象行為となっているのに対して、コピーコントロールについては、規制対象行為となっていない。中国法においては、回避行為自体が規制対象行為となっている(著作権法第47条第6号)。

また、日本法においては、著作権法では一定の製造行為が規制対象行為となっているのに対して、不正競争防止法では規制対象行為となっていない。これに対して、EU指令のうち著作権指令、米国法、韓国法(著作権法及びオンラインデジタルコンテンツ産業発展法)及び中国法においては、いずれも一定の製造行為を規制対象行為としている。

そして、日本法においては、展示行為については、不正競争防止法では譲渡若しくは引き渡しのための展示行為が規制対象行為となっているのに対して、著作権法においては規制対象行為となっていない。また、広告行為については文言上の直接の記載はない。EU指令においては、コンピュータ・プログラム以外の著作物等について、「販売もしくは貸与目的の広告」が規制対象行為となっている<sup>3</sup>。米国法においては、展示行為や広告行為は、状況次第で「公衆提供」に該当し、禁止される余地がある。韓国法においては、著作権では展示行為を規制対象行為として明確には定められていないが、オンラインデジタルコンテンツ産業発展法では、譲渡・貸与のための展示行為が規制対象行為となっている。中国法においては、展示行為を規制対象行為として明確には定められていない。

日本法においては、輸出行為については、不正競争防止法では規制対象になっているのに対して、著作権法では規制対象になっていない。EU指令、米国法、韓国法(著作権法及びオンラインデジタルコンテンツ産業発展法)及び中国法のいずれにおいても、輸出行為を明示的に規制する規定は存在しない。ただし、米国においては、輸出行為が「その他の取引」に含まれることにより規制されると解される。また、中国に

---

<sup>3</sup> コンピューター・プログラムについては、迂回装置等を流通に置く全ての行為または商業目的で所持する行為が規制の対象であるとされており、展示行為や広告行為がこれに含まれるかは明確ではない。

においては、輸出行為が「公衆に提供する行為」に該当する可能性がある。

## 8. 刑事的制裁の有無

日本法においては、著作権法には刑事的制裁が定められているのに対して(著作権法第120条の2柱書)、不正競争防止法には刑事的制裁が定められていない。

EU指令において、コンピュータ・プログラム以外の著作物等については、加盟国は適切な制裁等を規定する旨等が規定されており(著作権指令第8条第1項)、フランス法、イギリス法及びドイツ法のいずれにおいても、コンピュータ・プログラム以外の著作物等については一定の刑事的制裁が定められている<sup>4</sup>。また、米国法及び韓国法(著作権法及びオンラインデジタルコンテンツ産業発展法)においても刑事的制裁が規定されている。中国法においては、刑事的制裁を明確に定める規定は存在しない。

## 9. 水際措置

日本法においては、技術的手段の回避装置等の輸出入にかかる水際措置は存在しない。

EU指令、フランス法、イギリス法、ドイツ法及び韓国法においても、技術的手段の回避装置等の輸出入にかかる水際措置の規定は存在しない。米国法においては、水際措置を定めた法規は存在しないものの、税関当局の内部で利用されているガイドラインにおいては、技術的手段の回避装置等が没収等の対象になるとの運用がなされている。中国法においては、知的財産権税関保護条例及び同実施規則において、著作権を侵害する物品のみならず、技術的手段の回避装置等に対しても輸出入にかかる水際措置がとられているように思われる。なお、韓国法においては、著作権法において行政機関による機器等の回収・廃棄措置・削除措置やオンラインサービス提供者に対する技術的保護措置無効かプログラムの掲載停止命令などの規定があるが、水際措置に関する明示規定はみられない。オンラインデジタルコンテンツ産業発展法にはいずれの規定もみられない。

## 10. 例外規定等

日本法においては、著作権法には技術的手段についての規制に対する例外規定等は存在しないが、不正競争防止法には「試験または研究」のために用いられる装置等に対する除外規定が存在する。

EU指令においては、コンピュータ・プログラム以外の著作物等については、一定の場合に、加盟国の国内法において規定されている著作権等の例外又は制限によりユー

---

<sup>4</sup> コンピュータ・プログラムについては、迂回装置等の製造・頒布について適切な救済措置を設けることがEU指令により要請されており、フランス、イギリス、ドイツにおいて民事的救済の規定はあるが、特別に刑事制裁を規定してはいない。

ザが本来受けられるはずの利益をユーザが受けられるように、権利者が一定の手段を提供するように適切な措置をとるべきことが定められている(著作権指令第 6 条第 4 項)<sup>5</sup>。

米国法においては、連邦議会図書館長による規則に基づくアクセス・コントロールの回避等の除外規定、互換性確保や暗号化研究のための回避行為・迂回装置等の製造頒布の除外規定等種々の例外が詳細に定められている(デジタルミレニアム著作権法第 1201 条(a) (1) (B) (C)、(d)～(j))。

韓国法においては、著作権法には現時点では除外規定等は存在しない。一方、オンラインデジタルコンテンツ産業発展法には、技術的保護措置の研究・開発のために技術的保護措置を無力化する装置または部品を製造する場合には、法律違反ではないものとする除外規定が存在する。

中国法においては、学校の授業又は科学研究の目的で著作物を提供する場合等についての除外規定が存在する(伝播権条例第 12 条各号)。

## 11. 競争法との関係

EU 及び米国においては、技術的手段に対する規制は、互換性を損ね、また、コンテンツ所有者が、反競争的な行為を行うことを容易にしているとの指摘もなされている。

実際にも EU においては、技術的手段により、域内における価格差が作り出されているとされ、競争当局により問題視されたケースもある。また、フランスにおいては、著作権指令を国内実施する際に、技術的手段により互換性が損なわれることのないように多くの規定が盛り込まれることとなった。

また、米国においては、問題となったアクセス・コントロールについて、裁判所により、アフターサービス市場やスペア・パーツ市場における支配力を強化する目的であると認定され、結論としてコンテンツ所有者の救済が否定された裁判例がある。

---

<sup>5</sup> ただし、私的使用のための複製についてはかかる措置を設けるかは加盟国の任意とされている。

また、コンピュータ・プログラムについては、コンピュータ・プログラム指令に技術的手段についての規制に対する除外規定等は存在しないものの、著作権指令前文 50 項に基づき、調査研究又は互換性を達成するとの目的に必要な装置等の製造・頒布については例外が認められると考えられている。

## 第 2 編 各国法制度調査報告書



## I コンテンツの技術的手段に係る各国法制度調査研究(日本編)





## I コンテンツの技術的手段に係る各国法制度調査研究の調査項目(日本編)

### 1. コンテンツの技術的手段に関する国際ルール

#### (1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)<sup>6</sup>

##### (a) 各条約における技術的手段に係る規定及びその義務の内容

WCT 第 11 条、WPPT 第 17 条では、「技術的手段の迂回に関する義務」として、各国は「著作権者(実演家又はレコード製作者)により許諾されておらず又は法によって許容されていない行為をその著作物(実演又はレコード)について制限する効果的な技術的手段」の回避について、適切な法的救済を定めるべき、としている。

### ア WIPO 著作権条約(WCT)

#### 〈条文〉

#### Article 11 Obligations concerning Technological Measures<sup>7</sup>

*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.*

#### 第 11 条 技術的手段に関する義務<sup>8</sup>

締約国は、著作権者によつて許諾されておらず、かつ、法令で許容されていない行為がその著作物について実行されることを抑制するための効果的な技術的手段であつて、この条約又はベルヌ条約に基づく権利の行使に関連して当該著作権者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。

技術的手段の保護に関する規定を盛り込んだ初めての条約である。

この規定が対象とする技術的手段については、条約で「著作権者によつて許諾されておらず、かつ、法令で許容されていない行為がその著作物について実行されることを抑制するための効果的な技術的手段であつて、この条約又はベルヌ条約に基づく権利

<sup>6</sup> 著作権に関する世界知的所有権機関条約 (WIPO Copyright Treaty) 、実演及びレコードに関する世界知的所有権機関条約 (WIPO Performance and Phonograms Treaty) 1996 年

<sup>7</sup> [http://www.wipo.int/treaties/en/ip/wct/trtdocs\\_wo033.html#P87\\_12240](http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html#P87_12240)

<sup>8</sup> [http://www.cric.or.jp/db/z/wch\\_index.html](http://www.cric.or.jp/db/z/wch_index.html)

の行使に関連して当該著作者が用いるもの」と規定されており、「許諾」が必要な著作物等について「技術的手段」の法的な保護及び救済について措置を講じることが求められているが、その内容については各国が判断することができる。したがって、少なくとも「著作権等の支分権」に関して「法的保護」することが条約上の要請を充たすものと解される、とされている<sup>9</sup>。すなわち、条約上権利行使の対象となる利用行為(複製等)に関するものであって、単なる視聴等を技術的に制限するアクセスコントロールは条約上の義務から除外されている、と解されている。ただし、「条約上の要請を充たした上で、「技術的保護手段」の範囲及びその規制の対象を拡大することは、条約上許容され、各国の判断に任されている」<sup>10</sup>として、実際、日本法においては、不正競争防止法において、アクセスコントロールに対する規制も行っている。

## イ WIPO 実演・レコード条約(WPPT)

### 〈条文〉

#### Article 18 Obligations concerning Technological Measures<sup>11</sup>

*Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.*

#### 第 18 条 技術的手段に関する義務<sup>12</sup>

締約国は、実演家又はレコード製作者によって許諾されておらず、かつ、法令で許容されていない行為がその実演又はレコードについて実行されることを抑制するための効果的な技術的手段であって、この条約に基づく権利の行使に関連して当該実演家又はレコード製作者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。

WIPO 著作権条約と同時に技術的手段の保護に関する規定を盛り込んでいる。WIPO

<sup>9</sup> 文化審議会著作権分科会「文化審議会著作権分科会報告書」73 頁(2006)参照<[http://www.bunka.go.jp/1tyosaku/pdf/singi\\_houkokusho\\_1801.pdf](http://www.bunka.go.jp/1tyosaku/pdf/singi_houkokusho_1801.pdf)>。

<sup>10</sup> 文化審議会著作権分科会「文化審議会著作権分科会報告書」73 頁(2006)参照<[http://www.bunka.go.jp/1tyosaku/pdf/singi\\_houkokusho\\_1801.pdf](http://www.bunka.go.jp/1tyosaku/pdf/singi_houkokusho_1801.pdf)>。

<sup>11</sup> [http://www.wipo.int/treaties/en/ip/wppt/trtdocs\\_wo034.html#P141\\_21174](http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html#P141_21174)

<sup>12</sup> [http://www.cric.or.jp/db/z/wjr\\_index.html](http://www.cric.or.jp/db/z/wjr_index.html)

実演等条約第 18 条の規定は、WIPO 著作権条約とほぼ同様である。

## (b) 各条約の締結状況

両条約とも締結している。

WIPO 著作権条約(2002 年 3 月 6 日に発効<sup>13)</sup>については、日本は発効前の 2000 年 6 月 6 日に加入し、2002 年 3 月 6 日に効力が生じている<sup>14</sup>。

WIPO 実演・レコード条約(2002 年 5 月 20 日に発効<sup>15)</sup>については、日本は 2002 年 7 月 9 日に加入し、2002 年 10 月 9 日に効力が生じている<sup>16</sup>。

## (2) 日本における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容

日タイ EPA<sup>17</sup>及び日フィリピン EPA<sup>18</sup>において技術的手段に関する規定が存在する。

<sup>13</sup> [http://www.wipo.int/pressroom/en/html.jsp?file=/redocs/prdocs/en/2001/wipo\\_pr\\_2001\\_300.html](http://www.wipo.int/pressroom/en/html.jsp?file=/redocs/prdocs/en/2001/wipo_pr_2001_300.html)

<sup>14</sup> WIPO 著作権条約は、30 国の批准・加入後 3 ヶ月経過することにより発効することとなっており(WIPO 著作権条約第 20 条)、2001 年 12 月 6 日にガボンが加入書を寄託したことにより、2002 年 3 月 6 日に発効した。

<sup>15</sup> [http://www.wipo.int/pressroom/en/html.jsp?file=/redocs/prdocs/en/2002/wipo\\_pr\\_2002\\_302.html](http://www.wipo.int/pressroom/en/html.jsp?file=/redocs/prdocs/en/2002/wipo_pr_2002_302.html)

<sup>16</sup> WIPO 実演・レコード条約は、30 国の批准・加入後 3 ヶ月経過することにより発効することとなっており(WIPO 実演・レコード条約第 29 条)、2002 年 2 月 20 日にホンジュラスが加入書を寄託したことにより、2002 年 5 月 20 日に発効した。

<sup>17</sup> 経済上の連携に関する日本国とタイ王国との間の協定第 133 条第 2 項

「各締約国は、著作者、実演家又はレコード製作者によって許諾されておらず、かつ、自国の法令で許容されていない行為がその著作物、実演又はレコードについて実行されることを抑制するための効果的な技術的手段であって、自国の法令に基づく権利の行使に関連して当該著作者、実演家又はレコード製作者が用いるものに関し、そのような技術的手段の回避を防ぐための十分な法的保護及び効果的な法的救済の措置を講ずるよう努める。」[http://www.mofa.go.jp/mofaj/gaiko/fta/j\\_asean/thailand/pdfs/mokuji.pdf](http://www.mofa.go.jp/mofaj/gaiko/fta/j_asean/thailand/pdfs/mokuji.pdf)

「Each Party shall endeavour to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors, performers or producers of phonograms in connection with the exercise of their rights under the laws and regulations of the Party and that restrict acts, in respect of their works, performances or phonograms, which are not authorised by the authors, performers or producers of phonograms concerned or permitted by the laws and regulations of the Party.」<http://www.mofa.go.jp/region/asia-paci/thailand/epa0704/agreement.pdf>

<sup>18</sup> 経済上の連携に関する日本国とフィリピン共和国との間の協定第 126 条第 2 項

「各締約国は、著作者、実演家又はレコード製作者によって許諾されておらず、かつ、自国の法令で許容されていない行為がその著作物、実演又はレコードについて実行されることを抑制するための効果的な技術的手段であって、自国の法令に基づく権利の行使に関連して当該著作者、実演家又はレコード製作者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。」[http://www.mofa.go.jp/mofaj/gaiko/fta/j\\_asean/philippines/pdfs/mokuji.pdf](http://www.mofa.go.jp/mofaj/gaiko/fta/j_asean/philippines/pdfs/mokuji.pdf)

「Each Party shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors,

日タイ EPA においては、「技術的手段の回避を防ぐための十分な法的保護及び効果的な法的救済の措置を講ずるよう努める。」(shall endeavour to provide)と規定されているのに対し、日フィリピン EPA では「技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。」(shall provide)と規定されている。

なお、現在、米国、EU、日本等の先進国を中心に、模倣品・海賊版拡散防止条約 (ACTA) が議論されているところ、そのアジェンダにおいて「第四節 デジタル環境における権利の執行」に関する項目の 1 つとして「技術的保護手段の回避(例外と制限の適用を含む)」の場合における救済措置の適用可能性」が挙げられている<sup>19</sup>。

## 2. コンテンツの技術的手段に関する法令等

### (1) 該当する法令等

#### ア 該当する法令等の概略及び類型の整理

日本法においては、コンテンツの技術的手段に対する保護を規定する法律として、著作権法及び不正競争防止法が存在する。

著作権法では、技術的保護手段(著作権法第 2 条第 1 項第 20 号)を回避した上での私的使用目的の複製を権利制限の適用除外とするとともに(著作権法第 30 条第 1 項第 2 号)、技術的保護手段の回避専用装置や回避専用プログラムの公衆への譲渡、譲渡目的の製造等について罰則(著作権法第 120 条の 2 第 1 号及び第 2 号)を設けて禁止している。「技術的保護手段」は、著作権法第 2 条第 1 項第 20 号において定義されている。

不正競争防止法では、技術的制限手段(不正競争防止法第 2 条第 7 項)の効果を妨げる機能のみを有する装置等を譲渡等する行為を不正競争に該当する行為類型として規定している(不正競争防止法第 2 条第 1 項第 10 号及び第 11 号)。「技術的制限手段」は、不正競争防止法第 2 条第 7 項において定義されている。

コンテンツの管理技術については、コンテンツのコピーを制限する「コピー管理技術(「コピーコントロール」)」とコンテンツのアクセスを制限する「アクセス管理技術(「アクセスコントロール」)」とに整理され、著作権法は、コピーコントロールのみを規制しているのに対し、不正競争防止法は、コピーコントロール及びアクセスコント

---

performers or producers of phonograms in connection with the exercise of their rights under the laws and regulations of the Party and that restrict acts, in respect of their works, performances or phonograms, which are not authorized by the authors, performers or producers of phonograms concerned or permitted by the laws and regulations of the Party. <<http://www.mofa.go.jp/region/asia-paci/philippine/epa0609/main.pdf>>

<sup>19</sup> <http://www.mofa.go.jp/mofaj/gaiko/ipr/atca09.html>  
[http://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/atca09\\_ja\\_ka.pdf](http://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/atca09_ja_ka.pdf)

ロールの両方を規制している<sup>20</sup>。

以下、条文に基づき、著作権法における 3 つの類型(著作権法第 30 条第 1 項第 2 号、著作権法第 120 条の 2 第 1 号及び同条第 2 号)、及び不正競争防止法における 2 つの類型(不正競争防止法第 2 条第 1 項第 10 号及び第 11 号)につき概要を記載する。

## イ 著作権法

### (ア) 類型Ⅰ： 回避装置の譲渡等した者に対する規制(著作権法第 120 条の 2 第 1 号)

類型Ⅰは、著作権法第 120 条の 2 第 1 号に規定されている規制であり<sup>21</sup>、「技術的保護手段の回避を行うことを専らその機能とする装置」又は「技術的保護手段の回避を行うことを専らその機能とするプログラムの複製物」を譲渡等する者に対する規制である。

### (イ) 類型Ⅱ： 回避サービス提供者に対する規制(著作権法第 120 条の 2 第 2 号)

類型Ⅱは、著作権法第 120 条の 2 第 2 号に規定されている規制であり、「業として公衆からの求めに応じて技術的保護手段の回避を行った者」に対する規制である。

### (ウ) 類型Ⅲ： 技術的保護手段を回避して私的利用による複製を行った者に対する規制(著作権法第 30 条第 1 項第 2 号)

類型Ⅲは、著作権法第 30 条第 1 項第 2 号に規定されている規制であり、複製行為が著作権法第 30 条第 1 項本文に該当する場合において、「技術的保護手段の回避」により可能となり、又はその結果に障害が生じなくなった複製を、その事実を知りながら行う者に対する規制である。

本来、著作物を複製すると複製権侵害(著作権法第 21 条)に該当するが、私的使用のための複製(著作権法第 30 条)に該当する場合には、著作権が制限されることにより、著作権侵害を構成しない。しかしながら、当該複製が「技術的保護手段の回避に

---

<sup>20</sup> なお、同じ技術がコピー管理目的にもアクセス管理目的にも使われ得ることに留意が必要である。具体例としては、マクロビジョン方式が挙げられる。マクロビジョン方式においては、マクロビジョンという信号が埋め込まれていて、あるバージョンではコピーを禁止することによりコピー管理をし、別のバージョンではコピーはできるものの再生画像等を乱れさせることによりアクセス管理をしている。また、いくつかの管理技術を組み合わせたコンテンツ流通も既に商用化されつつあり、コンテンツを提供する際にどの管理技術を採用するかは、本来コンテンツ提供事業者の創意工夫に基づき自由に選択することができるべきであり、アクセス管理技術及びコピー管理技術のいずれに分類されるかとは関係がない、という指摘もある。(小野昌延ほか『新・注解 不正競争防止法』(青林書院、新版、2007)550 頁〔小松〕参照)。

<sup>21</sup> 著作権法第 120 条の 2 第 1 号の文言のうち、「技術的保護手段」は著作権法第 2 条第 1 項第 20 号に、「(技術的保護手段の)回避」は著作権法第 30 条第 1 項第 2 号括弧書に、各々規定されている。

より可能となり、又はその結果に障害が生じなくなった複製を、その事実を知りながら行う場合」には、著作権が制限されず、複製権侵害となる。

## ウ 不正競争防止法

**(ア) 類型 A:** 他人が特定の者以外の者に映像等の視聴、プログラムの実行、映像等の記録をさせないために用いているもの以外の営業上用いられている技術的制限手段の効果を妨げる機能のみを有する機器等を譲渡等することに対する規制(不正競争防止法第2条第1項第10号<sup>22)</sup>)

類型 A は、不正競争防止法第2条第1項第10号に規定されている規制であり<sup>23)</sup>、他人が特定の者以外の者に映像等の視聴、プログラムの実行、映像等の記録をさせないために用いているもの以外の営業上用いられている技術的制限手段により制限されている映像等を、当該技術的制限手段の効果を妨げることにより可能とする機能のみを有する装置等を譲渡等する行為を規制している。

具体的には、映画ビデオにコンテンツとともに記録されている信号を用いて当該コンテンツの録画を制限するマクロビジョン方式や、所定の手続きを踏んで製造、販売等されている視聴機器以外の機器では解読できない形でコンテンツを暗号化している方式に対して、それらの技術の効果を妨げるキャンセラーを販売等する行為が該当する<sup>24)</sup>。

**(イ) 類型 B:** 他人が特定の者以外の者に映像等の視聴、プログラムの実行、映像等の記録をさせないために用いている技術的制限手段の効果を妨げる機能のみを有する機器等を譲渡等することに対する規制(不正競争防止法第2条第1項第11号)

類型 B は、不正競争防止法第2条第1項第11号に規定されている規制であり、他人が特定の者以外の者に映像等の視聴、プログラムの実行、映像等の記録をさせないために用いている技術的制限手段の効果を妨げる機能のみを有する機器等を譲渡等する行為を規制している。

具体的には、衛星放送あるいは有料ケーブルテレビジョン放送におけるペイパー

---

<sup>22)</sup> 不正競争防止法第2条第1項第10号と第11号の適用関係については、営業上用いられている技術的制限手段の態様にしたがって、客観的、形式的に切り分けられており、第10号において、第11号が適用される場合には第10号が適用されない旨の調整規定が設けられている。

<sup>23)</sup> 不正競争防止法第2条第1項第10号及び第11号の文言のうち、「技術的制限手段」は不正競争防止法第2条第7項に規定されている。

<sup>24)</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成18年改正版』(有斐閣、2007)72頁参照。

ビューサービス等契約者以外の者によってはスクランブルを解除できないように暗号が施されているものに対して、この技術の効果を妨げるスクランブル解除装置を販売等する行為が該当する<sup>25</sup>。

## (2) 法令等の規制内容

### (a) 規制対象技術(定義及び対象技術の具体例等)

#### ア 著作権法(類型Ⅰ・Ⅱ・Ⅲ共通)

##### (ア) 規制されている対象技術(保護対象技術)

「技術的保護手段」につき、著作権法第2条第1項第20号は、以下のとおり規定する。

#### 〈条文〉

#### 著作権法第2条第1項第20号

##### 技術的保護手段

電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法(次号において「電磁的方法」という。)により、第十七条第一項に規定する著作者人格権若しくは著作権又は第八十九条第一項に規定する実演家人格権若しくは同条第六項に規定する著作隣接権(以下この号において「著作権等」という。)を侵害する行為の防止又は抑止(著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。)をする手段(著作権等を有する者の意思に基づくことなく用いられているものを除く。)であつて、著作物、実演、レコード、放送又は有線放送(次号において「著作物等」という。)の利用(著作者又は実演家の同意を得ないで行つたとしたならば著作者人格権又は実演家人格権の侵害となるべき行為を含む。)に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、又は送信する方式によるものをいう。

定義にあたっては、以下の3つの要件を柱としている。

- ① 電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法(「電子的方法」)により、著作権、著作者人格権、著作隣接権(「著作権等」)を侵害する行為の防止又は抑止をする手段であること
- ② 著作権等を有する者の意思に基づくことなく用いられているものを除くこと
- ③ 著作物、実演、レコード放送又は有線放送(「著作物等」)の利用に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは

<sup>25</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成18年改正版』(有斐閣、2007)78頁参照。

有線放送に係る音若しくは影像とともに記録媒体に記録し、又は送信する方式によるものであること

規制対象は、コピーコントロールのみであり、アクセスコントロールは規制対象外である<sup>26</sup>。

具体的には、後掲(イ)のものが該当するとされている。

## (イ) 対象技術の具体例

- ・ SCMS (Serial Copy Management System)<sup>27</sup>
- ・ CGMS (Copy Generation Management System)<sup>28</sup>
- ・ 擬似シンクパルス方式(マクロビジョン方式)<sup>29</sup>

## イ 不正競争防止法

### (ア) 規制されている対象技術(保護対象技術)

「技術的制限手段」につき、不正競争防止法第 2 条第 7 項は、以下のとおり規定する。

#### 〈条文〉

#### 不正競争防止法第 2 条第 7 項

電磁的方法(電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。)により影像若しくは音の視聴若しくはプログラムの実行又は影

<sup>26</sup> 平成 10 年(1998 年)12 月の著作権審議会マルチメディア小委員会ワーキング・グループ(技術的保護・管理関係)報告においては、「技術的保護手段」の範囲について、著作物等の「使用」や「受信」といった著作権等の支分権の対象外の行為を技術的に制限する手段(アクセスコントロール)を技術的保護手段に含めることについては慎重な態度をとり、今後の検討課題であると整理した(半田正夫ほか『著作権法コンメンタール 1』(勁草書房、2009)〔吉田大輔〕291 頁以下参照。)

<sup>27</sup> SCMS は、録音媒体の特定の箇所に記録されたデジタル信号に、デジタル録音機器が対応することにより、無断複製の防止が行われる(著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁参照。)

<sup>28</sup> CGMS では、SCMS と同様に、録画媒体の特定の箇所に記録されたデジタル信号にデジタル録画機器が反応することにより、無断複製の防止(録画動作の停止)が行われる(著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁以下参照。)

<sup>29</sup> 擬似シンクパルス方式は、録画媒体に記録されたアナログ映像信号のうち、通常のテレビでは画面に映らない部分に特殊な信号を記録することにより(デジタル録画媒体やデジタル放送の場合には、記録、送信される特定のデジタル信号に基づき、再生・受信機器がアナログ映像信号を出力する際に特殊な信号を付加することにより)、アナログ録画機器の録画機能を正常に動作させないようにすることにより鑑賞に堪えない乱れた影像を録画させ、デジタル録画機器では録画動作を停止させて、無断複製を防ぐ。擬似シンクパルス方式については、上記信号を除去して正常な録画が行われるようにする専用装置がいくつも市販されている(著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁以下参照。)



像、音若しくはプログラムの記録を制限する手段であつて、視聴等機器(映像若しくは音の視聴若しくはプログラムの実行又は映像、音若しくはプログラムの記録のために用いられる機器をいう。以下同じ。)が特定の反応をする信号を映像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式又は視聴等機器が特定の変換を必要とするよう映像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式によるものをいう。

「技術的制限手段」とは、「電磁的方法(電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。)」により「映像若しくは音の視聴」や「プログラムの実行」(例えば、DVDの映画を見たり、ゲームソフトを使用したりすること)あるいは「映像、音、プログラムの記録」(例えば、DVDの映像をコピーすること)を「制限する手段」である。前者はアクセス管理技術であり、後者はコピー管理技術である<sup>30</sup>。

不正競争防止法第2条第1項第10号及び第11号は「営業上用いられている技術的制限手段」と規定しているため、「営業」とは関係しない、個人的な使用目的(個人のプライバシーを保護する目的)あるいは国家の防衛目的のための暗号等は本法での規制からはずれる<sup>31</sup>。「営業上用いられている技術的制限手段」のうち、「他人が特定の者以外の者に映像等の視聴、プログラムの実行、映像等の記録をさせないために用いているもの」は第2条第1項第11号の対象であり、それ以外が第10号の対象である。

### (イ) 対象技術の具体例<sup>32</sup>

不正競争防止法第2条第1項第10号につき

- ・ SCMS(Serial Copy Management System)
- ・ CGMS(Copy Generation Management System)
- ・ 擬似シンクパルス方式(マクロビジョン方式)
- ・ 無許諾記録物が視聴のための機器にセットされても、機器が動かないようにすることで、無許諾記録物による視聴を防ぐ技術

<sup>30</sup> 各文言の詳細については、小野昌延ほか『新・注解 不正競争防止法』(青林書院、新版、2007) [小松] 792頁以下参照。

<sup>31</sup> 小野昌延ほか『新・注解 不正競争防止法』(青林書院、新版、2007) [小松] 557頁は、「もっとも、著作権法、民法、刑法等で保護されうる。特に、著作権法第30条第1項第2号は、技術的保護手段を回避したコピー行為については、私的使用目的でも許されないとしている。」と指摘する。

<sup>32</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成18年改正版』(有斐閣、2007) 37頁参照。

- 不正競争防止法第2条第1項第11号につき  
・ 有料衛星放送のスクランブル

## (b) 規制対象製品及び対象プログラム等

### ア 著作権法

#### (ア) 類型Ⅰ(著作権法第120条の2第1号)

- (i) 「技術的保護手段の回避を行うことを専らその機能とする装置<sup>33</sup>(当該装置の部品一式であって容易に組み立てることができるものを含む。)<sup>34</sup>」
- (ii) 「技術的保護手段の回避を行うことを専らその機能とするプログラムの複製物」
- (iii) 「技術的保護手段の回避を行うことを専らその機能とするプログラム」

#### (イ) 類型Ⅱ(著作権法第120条の2第2号)

技術的保護手段の回避サービス

#### (ウ) 類型Ⅲ(著作権法第30条第1項第2号)

対象製品に対する限定はない。

すなわち、類型Ⅲにおいては行為自体が対象である。

### イ 不正競争防止法(類型A・B共通)

- (i) 「営業上用いられている技術的制限手段により制限されている映像・音の視聴、プログラムの実行、映像・音・プログラムの記録を当該技術的制限手段の効果を妨げることにより可能とする機能(以下、「当該機能」という。)のみを有する装置(当該装置を組み込んだ機器を含む)<sup>35</sup>」
- (ii) 「当該機能のみを有するプログラム(当該プログラムを他のプログラムと組み合わせ

<sup>33</sup> 「技術的保護手段の回避を行うことを専らその機能とする」装置・プログラムとはおおよそ技術的保護手段の回避以外に実用的な意味のある機能を持たない装置・プログラムという意味する(加戸守行『著作権法逐条講義』(著作権情報センター、2006)735頁参照。)

<sup>34</sup> 「当該装置の部品一式であって容易に組み立てることができるものを含む」は、完成した装置ではなく、装置を部品一式として容易に組み立てられる形式にしたものを指す(半田正夫ほか『著作権法コメント3』(勁草書房、2009)〔大家重夫〕593頁以下参照。)

<sup>35</sup> 「装置」とは一定の機能を有する機器の内蔵品という意味である。「当該機能のみを有する装置」としては、技術的制限手段を解除する機能を有するチップが典型例である。「機器」は上記の装置を内蔵するもの(一般に箱体)を指す。「機能のみを有する装置を組み込んだ機器」の例としては、マクロピジョンキャンセラー内蔵ビデオデッキがあげられる(小野昌延ほか『新・注解 不正競争防止法』(青林書院、新版、2007)〔小松〕561頁以下参照。)

せたものを含む)を記録した記録媒体もしくは記憶した機器」<sup>36</sup>

(iii)「当該機能のみを有するプログラム」

「機能のみ」との限定が付されているのは、これがないと映像や音の視聴、記録をするための装置やプログラムを提供する者が常に全ての技術的制限手段を「妨げる」機能を有するか否かを確認し、場合によっては取りやめたり、提供する装置等の他の機能を歪める程度まで設計を変更することが必要となり、これらの提供者の事業活動を過度に抑制することになるため、明確に「妨げる」機能のみを有することが認められる装置やプログラムを「不正競争」の対象とすることとしている<sup>37</sup>。

### (c) 規制対象行為

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

#### ア 著作権法

##### (ア) 類型 I (著作権法第 120 条の 2 第 1 号)

(i) 上記(b)ア(ア)(i)「技術的保護手段の回避を行うことを専らその機能とする装置(当該装置の部品一式であって容易に組み立てることができるものを含む。)」及び(ii)「技術的保護手段の回避を行うことを専らその機能とするプログラムの複製物」について

規制対象行為は、条文上、「公衆に譲渡し、若しくは貸し渡し、公衆への譲渡若しくは貸与の目的をもって製造し、輸入し、若しくは所持し、若しくは公衆の使用に供」する行為と規定されている。

したがって、①製造行為につき「(当該装置又はプログラムの複製物を)公衆への譲渡若しくは貸与の目的をもって製造する行為」、②提供行為につき「公衆に譲渡し、若しくは貸し渡す行為、公衆の使用に供する行為」、③輸出入行為につき「公衆への譲渡若しくは貸与の目的をもって輸入する行為」、④所持行為につき「公衆への譲渡又は貸与の目的をもって所持する行為」が規制対象となる。なお、⑤回避サービス提供行為について、「公衆の使用に供し」とは、「回避装置や回避プログラムの複製物を公衆の使用に供する行為で、公衆に店頭等で客に回避装置

<sup>36</sup> 「組み合わせられた」とは、当該プログラムがその機能を変更されることなく、単に別のプログラムが組み合わせられた状態を指すので、本来は他の機能を有するプログラムに外見上「技術的手段の効果を妨げる機能のみを有するプログラム」が含まれているようなものはここに含まれない(小野昌延ほか『新・注解 不正競争防止法』(青林書院、新版、2007)〔小松〕562頁参照。)

<sup>37</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成18年改正版』(有斐閣、2007)74頁参照。

や回避プログラムの複製物において使用させる行為をいう」<sup>38</sup>ことから、この態様については、本号により規制対象となる。

これに対して、③輸出入行為のうち輸出行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、については規制対象となっていない。

(ii)「技術的保護手段の回避を行うことを専らその機能とするプログラム」について

規制対象行為は、条文上、「技術的保護手段の回避を行うことを専らその機能とするプログラム・・・を公衆送信し、若しくは送信可能化」する行為と規定されている。回避プログラムを公衆送信又は送信可能化し、公衆へ伝播することで、回避手段が公衆に提供されることを意味する。

したがって、②提供行為につき「(当該プログラムを)公衆送信行為及び送信可能化行為」が規制対象となる。

これに対して、①製造行為、③輸出入行為<sup>39</sup>、④所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、については規制対象となっていない。

#### (イ) 類型Ⅱ(著作権法第120条の2第2号)

規制対象行為は、条文上、「業として公衆からの求めに応じて技術的保護手段の回避」する行為と規定されている。

したがって、⑤回避サービス提供行為につき、「業として公衆からの求めに応じて技術的保護手段の回避を提供する行為」が規制対象となる。

第1号は、技術的保護手段の回避を行うことを専らその機能とする装置等の公衆への譲渡等の禁止であるが、第2号は、人が技術的保護手段の回避を行い、第1号と同様な機能を果たすことを禁止するものである。

#### (ウ) 類型Ⅲ(著作権法第30条第1項第2号)

規制対象行為は、私的使用を目的とする場合の複製において、条文上「技術的保護手段の回避・・・により可能となり、又はその結果に障害が生じなくなった複製を、その事実を知りながら行う」と規定されている。

したがって、⑥回避行為(回避による複製)につき「私的使用目的の複製において、技術的手段の回避により可能となり、又はその結果に障害が生じなくなった複製を、

<sup>38</sup> 半田正夫ほか『著作権法コンメンタール3』(勁草書房、2009)〔大家重夫〕594頁参照。

<sup>39</sup> ただし、公衆送信行為が他国との間で行われる場合に輸出入行為に該当しうるかが問題となり得る。

その事実を知りながら行う複製行為」が規制対象となる。

## イ 不正競争防止法(類型 A・B 共通)

### (ア)「当該機能のみを有する装置(当該装置を組み込んだ機器を含む)」について

規制対象行為は、条文上、「譲渡し、引き渡し、譲渡若しくは引き渡しのために展示し、輸出し、若しくは輸入」する行為と規定されている。

したがって、②提供行為につき「(当該装置の)譲渡行為、引き渡し行為、及び、譲渡若しくは引き渡しのための展示行為」、③輸出入行為につき「輸出行為及び輸入行為」が規制対象となる。

これに対して、①製造行為、④所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、については規制対象となっていない<sup>40</sup>。

### (イ)「当該機能のみを有するプログラム(当該プログラムが他のプログラムと組み合わせたものを含む)を記録した記録媒体若しくは記憶した機器」について

規制対象行為は全て上記(ア)と同様である。

### (ウ)「当該機能のみを有するプログラム」について

規制対象行為は、条文上、「電気通信回線を通じて提供する」行為と規定されている。

したがって、②提供行為につき「(当該機能のみを有するプログラムを)電気通信回線を通じて提供する行為」が規制対象となる。

これに対して、①製造行為、③輸出入行為<sup>41</sup>、④所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、については規制対象となっていない。

---

<sup>40</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成 18 年改正版』(有斐閣、2007)77 頁において、以下のとおり説明されている。

「当該機器等を製造する行為はそれだけで直ちに公正競争を阻害することにつながらないため、対象としていない。」

「また、機器等の提供がそれぞれ多くの無効化行為を呼び起こしコンテンツ提供者に大きな被害をもたらす蓋然性が高いのに比べ、1 件 1 件の無効化行為自体は、互いに独立に行われその被害も限定的である。その一方で個々の無効化行為を 1 件ずつ補足し、民事訴訟の対象とすることは困難である。このため、コンテンツの取引秩序の維持のための不正競争防止法による規制においては、機器等の提供等を対象とし、無効化行為そのものは対象とされていない。無効化行為そのものについては、個々の事例に応じて民法上の違法性が評価されることになるものと考えられる。」

<sup>41</sup> ただし、公衆送信行為が他国との間で行われる場合に輸出入行為に該当しうるかが問題となり得る。

### (3) 除外行為

#### (a) コンテンツの技術的手段に関する規定の適用除外、例外、制限規定等の存否・内容

##### ア 著作権法(類型Ⅰ・Ⅱ・Ⅲ共通)

適用除外、例外、制限規定は存在しない。

##### イ 不正競争防止法(類型A・B共通)

「技術的制限手段の試験又は研究のため」に用いられる装置等の譲渡等については適用除外となっている(不正競争防止法第19条第1項第7号)。

#### (b) 著作権法にコンテンツの技術的手段に関する規定が存在する場合の技術的手段回避の禁止規定と権利制限規定との関係

著作権法において、技術的保護手段の回避の禁止と権利制限規定の関係についての明確な規定として、第30条第1項第2号が存在する。すなわち、本来、複製をすることは複製権侵害(著作権法第21条)に該当するが、私的使用のための複製(著作権法第30条)に該当する場合には、著作権が制限されることにより、著作権侵害を構成しない。しかしながら、当該複製が技術的保護手段の回避により可能となり、又はその結果に障害が生じないようになった複製を、その事実を知りながら行う場合には、著作権が制限されず、複製権侵害となる。

このように、私的使用のための複製(著作権法第30条)については、技術的保護手段の回避を禁止する第30条第1項第2号の例外規定が存在するのに対して、他の権利制限規定(図書館等における複製(第31条)等)については、このような例外規定は存在しない。そのため、私的使用のための複製(著作権法第30条)以外の権利制限規定に関しては、少なくとも文言上は、技術的保護手段の回避を伴う複製行為等を行ったとしても、複製権侵害等は成立しないものと思われる<sup>42</sup>。

<sup>42</sup> 第30条以外の権利制限規定において、第30条第1項第2号類似の例外を設けなかった理由は、私的使用のための複製以外の権利制限は、公益性、社会慣行、他の権利との調整といった趣旨から設けられているものであり、技術的保護手段の回避により可能となった複製等が行われたとしても、著作権者等の利益を不当に害するおそれがあるとまでは現状ではいえないことを考慮したからであるとされている(著作権法令研究会、通産省知的財産政策室『著作権法・不正競争防止法改正解説』(有斐閣、1999)95頁参照)。ただし、この点については、私的使用のための複製以外の制限規定には種々の存在理由があるが、それらとの比較衡量において何をもちて著作権者等の利益を不当に害する程度に達したと評価するのか、及び、私的使用目的の複製との差異は何であるのかについてより明解な検証が必要であるとの指摘がある(作花文雄「技術的保護手段等に関する法整備の概況と課題」コピーライト2003年7月号42頁参照。)

#### (4) 救済措置

##### (a) 救済措置の内容(民事的救済及び刑事的制裁)

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

以下は、全て上記①乃至⑦の各行為について共通

#### ア 著作権法

##### (ア) 類型Ⅰ・Ⅱ共通

###### (i) 民事的救済

民事的救済は著作権法上は規定がない。

ただし、不法行為に基づく損害賠償(民法第 709 条、第 719 条等)が適用され得る。

###### (ii) 刑事的制裁

3 年以下の懲役又は若しくは 300 万円以下の罰金、又はこれらの併科非親告罪である(著作権法第 123 条参照)。

##### (イ) 類型Ⅲ(著作権法第 30 条第 1 項第 2 号)

###### (i) 民事的救済

複製権侵害に基づき、差止請求(著作権法第 113 条)、損害賠償請求(民法第 709 条)等の民事的救済を得ることができる。

###### (ii) 刑事的制裁

なし(著作権法第 119 条第 1 項括弧書で、同法第 30 条第 1 項第 2 号による複製行為を除外している)

#### イ 不正競争防止法(類型 A・B 共通)

##### (ア) 民事的救済

複製権侵害に基づき、差止請求(不正競争防止法第 3 条)、損害賠償請求(不正競争防止法第 4 条)等の民事的救済を得ることができる。

##### (イ) 刑事的制裁

なし

**(b) (a)の救済措置の請求主体**

**ア 著作権法**

**(ア) 民事的救済(類型Ⅰ・Ⅱ・Ⅲ共通)**

著作権者等

**(イ) 刑事的制裁(類型Ⅰ・Ⅱ共通)<sup>43</sup>**

検察官

非親告罪である(著作権法第123条参照)。

**イ 不正競争防止法(類型A・B共通)**

**(ア) 民事的救済**

営業上の利益を侵害された者等(不正競争防止法第3条、第4条等)

**(イ) 刑事的制裁**

刑事的制裁が規定されていない。

**(c) 違反機器等の輸出入にかかる水際措置又は違反抑止のための行政措置の有無・内容**

**ア 著作権法**

下記の理由から、類型Ⅰ乃至Ⅲのいずれについても輸出入にかかる水際措置は存在しない。

**(ア) 類型Ⅰ(著作権法第120条の2第1号)**

著作権を侵害する物品については、輸出又は輸入してはならない貨物に規定されている(関税法第69条の2第1項第3号及び第69条の11第1項第9号)。しかし、類型Ⅰは、技術的保護手段を回避するための装置等が対象であり、これらは「著作権を侵害する物品」には該当しない。

よって、輸出入にかかる水際措置は存在しない。

**(イ) 類型Ⅱ(著作権法第120条の2第2号)**

類型Ⅱの対象行為は、技術的保護手段の回避サービスの提供であるため、「著作権を侵害する物品」として規制を受けることはない。

よって、輸出入にかかる水際措置は存在しない。

**(ウ) 類型Ⅲ(著作権法第30条第1項第2号)**

類型Ⅲは複製行為が著作権法第30条第1項本文に該当する場合において、技術的

<sup>43</sup> 類型Ⅲには、刑事的制裁がない(著作権法第119条第1号括弧書)。



保護手段の回避が行われていることを知りながら複製を行う者に対する規制であるため、「著作権を侵害する物品」として規制を受けることはない。

よって、輸出入にかかる水際措置は存在しない。

#### イ 不正競争防止法(類型 A・B 共通)

「不正競争防止法第 2 条第 1 項第 1 号から第 3 号までに掲げる行為を組成する物品」については輸出又は輸入してはならない貨物として規定されているため(関税法第 69 条の 2 第 1 項第 4 号及び第 69 条の 11 第 1 項第 10 号)、類型 A(不正競争防止法第 2 条第 1 項第 10 号)及び類型 B(不正競争防止法第 2 条第 1 項第 11 号)は規制対象外である。

よって、輸出入にかかる水際措置は存在しない。

### (5) いわゆる「無反応機器」規制

#### いわゆる「無反応機器」に対する法令、規則、指令等による規制の有無・内容

#### ア 著作権法(類型 I・II・III 共通)

結論 規制対象ではない。

理由 いわゆる無反応機器である場合、すなわち信号に反応する仕組みが録音、録画機器等に備わっていないために技術的保護手段が機能せずに録音・録画等が行われてしまうような場合には、信号の除去又は改変が行われているわけではないため、「(技術的保護手段の)回避」に該当しないからである。

#### イ 不正競争防止法(類型 A・B 共通)

結論 規制対象ではない。

理由 いわゆる無反応機器を規制すると記録、視聴等を制限するあらゆる信号に対応する措置を施すよう強制することとなるため、コンテンツ提供事業者の十分な自助努力を促す観点からも「不正競争」の対象としないことが適当である。いわゆる無反応機器の場合、技術的制限手段の効果を妨げる機能以外の機能を必ず有するため、「機能のみ」とすることにより対象から外れることになる<sup>44</sup>。

<sup>44</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成 18 年改正版』(有斐閣、2007)75 頁参照。

### 3. 裁判例、執行状況、被害状況等

#### (1) コンテンツの技術的手段に関する裁判例

・「マジコン」販売等差止請求事件(東京地判平成 21 年 2 月 27 日)<sup>45</sup>

#### ア 事案の概要

(ア) 原告が被告に対して、マジコン<sup>46</sup>の輸入・販売に対して不正競争防止法第 2 条第 1 項第 10 号を理由に差止請求を求めたのが本件事件である。

事実関係及び争点は以下のとおりである。

#### (イ) 事実関係

原告： ・ 任天堂

任天堂は、ゲーム機である「ニンテンドーDS」及び「ニンテンドーDS Lite」(以下、両者を合わせて「DS 本体」という。)並びに DS 本体用のゲームソフトを格納したゲーム・カード(以下「DS カード」という。)の販売等を業とする会社である。

・ ゲームソフトウェア制作会社

任天堂との間でライセンス契約を結んでいるゲームソフトウェア制作会社である。

被告： ・ 輸入、販売等業者

マジコンの輸入、販売等を行っている業者である。

#### 原告商品の仕組み：

DS 本体は、DS カードを挿入するスロットを有し、DS カードを挿入すると、DS カードに記録されている特定信号を受信した場合にのみ、それぞれの信号ごとに特定の反応をして、DS カードのプログラムを実行する仕組みになっている。

そのため、DS カードのゲームソフトを複製しても、DS カードに記録されている特定信号が単に複製されるだけであり、特定信号の機能を再現することができない。

以上のように、DS 本体と DS カードが組となって、特定信号を使用してプログラム

<sup>45</sup> 本事件の原告である任天堂は、本事件後、平成 21 年 10 月 5 日にいわゆるマジコンを輸入及び販売する業者 4 社に対して、不正競争防止法に基づき、輸入及び販売行為の差止、及び、合計約 4 億円の損害賠償を求めて提訴している (<http://www.nintendo.co.jp/corporate/release/2009/091005.html>、日経新聞 2009 年 10 月 6 日朝刊 12 面、参照。)。また、任天堂は、同年 11 月 10 にも、いわゆるマジコンと呼ばれる機器を輸入販売している業者 3 社に対して、不正競争防止法に基づき、輸入及び販売行為の差止、及び、合計 6 億円の損害賠償を求めて提訴している(毎日新聞 2009 年 11 月 12 日大阪朝刊 30 面参照、及び、<http://www.nintendo.co.jp/corporate/release/2009/091110.html> 参照。)。

<sup>46</sup> いわゆるマジコンとは、不正にコピーしたニンテンドーDS のソフトを使えるようにする機器のことをいう。インターネット通信販売、販売店等において、「R4」「DSTT」等の名称で販売されている事例が見られる。

の実行を制限することにより(以下、この仕組みを「原告仕組み」という。)、DSカードのゲームソフトのプログラムの複製物(以下、「本件吸い出しプログラム」という。)によるプログラムの実行を制限している。

被告装置：

被告装置は、マジコンと呼ばれる装置である。被告装置は microSD カードを挿入することができる。そして、本件吸い出しプログラム等を microSD カードに格納し、その microSD カードを被告装置に挿入し、その被告装置を DS 本体のスロットに挿入すると、DS 本体で本件吸出しプログラム等を実行することができる。

(ウ) 争点

本件事件の争点は以下の 3 点である。

- 争点① 原告仕組みが不正競争防止法 2 条 7 項の「技術的制限手段」に該当するか
- 争点② 被告製品が、技術的制限手段を無効化する機能「のみ」を有するか
- 争点③ 原告が被告の行為により営業上の利益を侵害されているか

## イ 判旨

(ア) 争点①について

不正競争防止法第 2 条第 7 項の技術的制限手段については、信号を検知した場合にプログラム等の実行を制限する方式(「検知→制限方式」)が技術的制限手段に該当することについては、当事者間で争いはなかった。

これに対して、信号を検知した場合にプログラム等の実行を可能とする方式(「検知→可能方式」)も技術的制限手段に該当するかが問題となった。

判旨は、当時の立法関連資料を詳細に検討した上で、検知→可能方式についても技術的制限手段に該当すると判示した。

(イ) 争点②について

裁判所は、「のみ」の要件について、以下のように判示した。「不正競争防止法第 2 条 1 項第 10 号の『のみ』は、必要最小限の規制という観点から規制対象となる機器等を、管理技術の無効化を専らその機能とするものとして提供されたものに限定し、別の目的で製造され提供されている装置等が偶然『妨げる機能』を有している場合を除外していると解釈することができ、これを具体的機器等で説明すると、MOD チップは『のみ』要件を満たし、パソコンのような汎用機器等及び無反応機器は『のみ』要件を満たさないと解釈することができる」。

そして、「数多くのインターネット上のサイトに極めて多数の本件吸い出しプログラムがアップロードされており、だれでも容易にダウンロードすることができるこ

と、被告装置の大部分が、そして大部分の場合に、本件吸い出しプログラムを使用するために用いられていることが認められるため、被告装置が「偶然『妨げる機能』を有しているにすぎないと認めることは到底できない」として、被告装置は「のみ」の要件を満たすと判示した。

(ウ) 争点③について

裁判所は、被告装置が輸入、販売されているために、原告は本来販売できたはずのDSカードを販売することができなくなっているため、現実には営業上の利益が侵害されていると判示した。

・東京地決平成17年1月31日(公刊物未登載)

本件は、ケーブルテレビ17社が、いわゆるスクランブル信号を解除することができるチューナーを輸入及び販売していた業者に対して、不正競争防止法違反を理由として販売の差止め等を求める仮処分を申し立てたという事案である。

これに対して裁判所は、当該チューナーの輸入及び販売の禁止、インターネットのサイトからの削除、及び、扱っている機器の廃棄を命じる仮処分決定をした<sup>47</sup>。

**(2) コンテンツの技術的手段に関する執行状況**

執行状況に関する統計的資料は見あたらない。但し、新聞報道等によれば、違法複製ゲームソフトとマジコンを販売していた者(ネットオークションへの出品事例を含む)に対する逮捕等摘発事例が複数存在する<sup>48</sup>。

**(3) コンテンツの技術的手段に関する被害状況**

統計情報等は見あたらない。

ニンテンドーDSのソフトの違法コピー、マジコン等の不正利用による被害額は全世界で3000億円以上との試算もあるとの報道がある<sup>49</sup>。

また、上記東京地決平成17年1月31日(公刊物未登載)を受けて記者会見をした日本ケーブル連盟は、「全国に出回っている違法チューナーはこれまでに20万台を超え、視聴料の被害は1ヶ月に六億円を上回っていると見られる」と述べている<sup>50</sup>。

<sup>47</sup> 「CATV視聴できる違法チューナー 東京地裁 販売差止めの仮処分を決定」NHKニュース2005年1月31日参照。

<sup>48</sup> <http://japan.cnet.com/news/tech/story/0,2000056025,20383677,00.htm>、大阪読売新聞2008年12月1日夕刊13面、<http://www.itmedia.co.jp/news/articles/0812/01/news072.html>、<http://japan.cnet.com/news/tech/story/0,2000056025,20384558,00.htm> 参照。

<sup>49</sup> 産経新聞2009年2月28日東京朝刊31面参照。

<sup>50</sup> 「CATV視聴できる違法チューナー 東京地裁 販売差止めの仮処分を決定」NHKニュース2005年1月31日参照。

## 4. 技術動向の調査

### (1) コンテンツの技術的手段に関する技術動向(平成 11 年法改正当時から現在への比較)

#### ア 著作権法

技術的保護手段に関する規定が導入された平成 11 年改正当時に技術的保護手段に該当する技術として想定されていた技術は、SCMS、CGMS、擬似シンクパルス方式(マクロビジョン方式)であった<sup>51</sup> <sup>52</sup>。現在もこれと概ね同様の技術が用いられているが、現在用いられている技術的保護手段については、「フラグ検出型」と「暗号技術利用型」とに大別することができる。

「フラグ検出型」は、基本的には暗号化されていない著作物等のコンテンツに複製制御フラグ(信号)を付し、複製機器がそのフラグを検出し、反応することで複製を制限する方法である。「フラグ検出型」においては、複製機器がフラグを検出・反応する場合しか複製制御ができないという短所がある。フラグ検出型の採用例として、MD レコーダ、オーディオ CD レコーダ、DVD レコーダ、D-VHS レコーダ等がある。例えば、音楽 CD から MD レコーダにコピーする場合にはコピーを一世代に限定する技術が用いられている(ただし、パソコン、携帯用オーディオプレーヤー等では機能しない)。また、映像関係では、録画機器を用いて複製・再生する場合、映像が乱れ、視聴に著しい障害を発生させる技術が用いられる場合もある。

「暗号技術利用型」は、コンテンツを暗号化し、複合鍵なしでは視聴できないようにした上で、複合鍵のライセンス契約に従い、利用者側の機器でコンテンツの再生、出力、複製等を行う際に一定の利用制限ができるようにする方法である。複合鍵のライセンス契約の内容に様々な条件を付すことが可能であり、例えば、相手方の機器が著作権保護技術に対応しているものであればデータを出力し、それ以外は出力不可にする等、複製制御以外にも様々な条件を付加してコンテンツの利用の制限をすることができるという長所がある。複製の制御の例としては、コピー世代の制限(例えば、コピー禁止、一世代のみコピー可、コピー制限なし等)やコピー個数の制限がある。転送・出力の制御の例としては、複製・転送が可能な機器の限定、出力先の限定、出力時及び出力先でのコンテンツの扱いの限定等がある。また、再生の制御の例としては、ライセンス契約上認められていない方法で作成された複製物を検知し、再生を禁止することが挙げられる。暗号技術利用型の例には、ソース側では、DVD ビデオ、DVD オーディオ、スーパーオーディオ CD、デジタル TV 放送、配信サービス等、また、利用機器側では、DVD レコーダ、著作権保護付小型メモリーカード(SD カード、メモリ

<sup>51</sup> 著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁参照。

<sup>52</sup> 文化庁・著作権審議会マルチメディア小委員会ワーキンググループ(技術的保護・管理関係)報告書(平成 10 年 12 月)16 頁参照。

スティック等)、配信サービス端末ソフトウェアや対応モバイル等がある<sup>53</sup>。

## イ 不正競争防止法

技術的制限手段に関する規定が導入された平成 11 年当時の技術的制限手段として想定されていた技術は、概ね現在用いられている技術と変わらない。すなわち、平成 11 年当時から現在に至るまで、音楽、映像等のコンテンツが記録部分に伝送されることを止める技術(SCMS、CGMS 等)、真正なデータを伝送せずに、雑音を入れることにより不完全な複製を作成させる技術(マクロビジョン方式等)、ゲームにおいて用いられる技術で、無許諾記録物が視聴のための機器にセットされても機器が動かないようにする技術、有料衛星放送にスクランブルをかける技術等が用いられている<sup>54 55 56</sup>。

### (2) 電子透かし等、コンテンツの技術的手段に関する新たな技術

電子透かしとは、デジタルコンテンツを不正利用から保護するために、著作権者を示すマーク(情報)を、気づかれないように画像や音等のデジタルコンテンツに忍ばせる技術である<sup>57 58</sup>。

電子透かしをコピーコントロールに用いる方法が検討されている。具体的には、CCI 信号(「コピー不可」、「1 回コピー可」、「複数回コピー可」というコピー可能レベルを示す信号)を用いるコピーコントロールにおいて、CCI 信号が除去、改変等される場合を考慮して、CCI 信号と同様の情報を、電子透かしによりコンテンツ自体に埋め込むという方法である<sup>59 60</sup>。

### (3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況

#### ア 現在使用されている技術について

上記の現在使用されている技術については、著作権法の技術的保護手段、及び、不正競争防止法の技術的制限手段のいずれも対応しているといえる。

ところで、最近の傾向として、コピーコントロールとアクセスコントロールを組み

<sup>53</sup> 半田正夫ほか『著作権法コンメンタール1』(勁草書房、2009)〔吉田大輔〕278頁以下参照。

<sup>54</sup> 著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)193頁以下参照。

<sup>55</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成18年改正版』(有斐閣、2007)37頁参照。

<sup>56</sup> 小野昌延ほか『新・注解 不正競争防止法』(青林書院、新版、2007)〔小松〕559頁参照。

<sup>57</sup> 小野東『電子透かしとコンテンツ保護』(オーム社、2001)2頁参照。

<sup>58</sup> 電子透かしについては、権利管理情報としての利用についても検討されている(加戸守行『著作権法逐条講義』(著作権情報センター、2006)62頁参照。)

<sup>59</sup> 小野東『電子透かしとコンテンツ保護』(オーム社、2001)39頁参照。

<sup>60</sup> 田中哲夫ほか「ホームデジタルコンテンツの保護技術」東芝レビュー57巻9号(2002)34頁参照。

合わせた技術が出てきている。このような技術に対しては、不正競争防止法においては、コピーコントロール及びアクセスコントロールを規制対象としているのであるから、当該技術にも対応していると思われる。また、コピーコントロールのみを規制対象としている著作権法においても、上記技術のうちのコピーコントロールの部分を規制対象とすることができると思われるため、当該技術に対応できていると思われる<sup>61 62</sup>。

## イ 電子透かし

電子透かしが、今後どのような形で利用されるかが明らかではないため、著作権法及び不正競争防止法が、電子透かしに対応できているかは明らかでない。

ところで、上記の CCI 信号と同様の情報を電子透かしによりコンテンツ自体に埋め込む方法に対しては、著作権法は対応できていると思われる。なぜなら、CCI 侵害の除去・改変についても、技術的保護手段の回避に該当すると考えられるため<sup>63</sup>、CCI 信号と同様の情報を電子透かしにより埋め込む場合も同様に考えることができると思われるからである。

また、不正競争防止法においても、CCI 信号の除去・改変が技術的制限手段の効果を妨げる行為であると思われるため、上記の CCI 信号と同様の情報を電子透かしによりコンテンツ自体に埋め込む方法に対応できているのではないかと思われる。

## 5. 各国内の議論(規制に対する賛否・改正動向等)

### (1) コンテンツの技術的手段に関する現行規制に対する議論

#### ア コピーコントロールとアクセスコントロールの区別について

著作権法の技術的保護手段が、コピーコントロールのみを規制対象としており、アクセスコントロールを規制対象としていない点については、物理的な信号の制御の在り方が複製の防止なのか、再生(音や影像の視聴、プログラムの使用)の防止なのかにより画一的に切り分けることについての批判<sup>64</sup>や、コピーコントロールとアクセスコントロールの区別は微妙であるためコピーコントロールのみを規制対象とするべきではないという批判<sup>65</sup>がある。

なお、不正競争防止法においてコピーコントロールとアクセスコントロールの両方

<sup>61</sup> 作花文雄「技術的保護手段等に関する法整備の概況と課題」コピーライト 2003 年 7 月号 34 頁参照。

<sup>62</sup> 半田正夫ほか『著作権法コンメンタール 1』(勁草書房、2009)〔吉田大輔〕292 頁参照。

<sup>63</sup> 加戸守行『著作権法逐条講義』(著作権情報センター、2006)230 頁参照。

<sup>64</sup> 作花文雄「技術的保護手段等に関する法整備の概況と課題」コピーライト 2003 年 7 月号 34 頁参照。

<sup>65</sup> 田村善之『著作権法概説』(有斐閣、第 2 版、2001)143 頁参照。

を規制対象としたのは、両者の区別が困難だからであるとされている<sup>66</sup>。

## イ いわゆる無反応機器について

無反応機器を規制すると、記録や視聴を制限するあらゆる信号に対応する措置を施すことを強制する結果となるため、コンテンツ提供事業者の十分な自助努力を促す観点から望ましくないとの見解がある<sup>67</sup>。

また、無反応機器を規制対象としないことに対しては賛成しつつも、無反応機器により迂回される保護手段に依存しなければならない状況が続くのであれば、権利者団体と複製機器製造業者との交渉が進展しなかったり、アウトサイダーが出現する場合に備えて、相当数の権利者や製造業者の意見を聴取しつつ適当な技術的保護手段を決定しうる公的な手続を用意するとともに、その手続を履践すれば無反応機器の提供をも取り締まることができるようにする等、何らかの法的な裏付け措置を導入する必要があるとの見解がある<sup>68 69</sup>。

## ウ アクセス権及び知る権利について

アクセス権(著作物を無断で知覚されない権利)については、文化審議会著作権分科会審議経過概要において、近年の情報技術の発達により、デジタル化されている著作物について知覚行為そのものをコントロールすることができるようになってきており、アクセス権の創設を含め、知覚行為を著作権の対象とすることの可否・必要性について検討する必要性が主張されている<sup>70</sup>。

これに対して、アクセス権の創設は人間が著作物に触れること自体を規制の対象とすることになるところ、著作物は万人に知覚されることを目指しているのだから、アクセス権の創設は妥当ではないとの見解がある<sup>71</sup>。

また、アクセス権に関しては、著作物の視聴等の「知覚行為」まで権利範囲を広げるかについては、「国民の知る権利」にも関わり、また、著作権の支分権の立て方全体に関わる根本的な問題であることから、慎重な議論が必要であるとの見解がある<sup>72</sup>。

---

<sup>66</sup> 著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88頁以下参照。

<sup>67</sup> 経済産業省知的財産政策室『逐条解説不正競争防止法 平成18年改正版』(有斐閣、2007)75頁参照。

<sup>68</sup> 田村善之『著作権法概説』(有斐閣、第2版、2001)147頁参照。

<sup>69</sup> 田村善之『不正競争防止法概説』(有斐閣、第2版、2003)389頁参照。

<sup>70</sup> [http://www.mext.go.jp/b\\_menu/shingi/bunka/toushin/011201.htm](http://www.mext.go.jp/b_menu/shingi/bunka/toushin/011201.htm)

<sup>71</sup> 財団法人デジタルコンテンツ協会「コンテンツ保護技術とその法的評価」(財団法人デジタルコンテンツ協会、2003)99頁。

<sup>72</sup> 半田正夫ほか『著作権法コンメンタール1』(勁草書房、2009)〔吉田大輔〕299頁参照。



## (2) コンテンツの技術的手段に関する規制に対する業界からの要望状況

コンテンツの技術的手段に関する規制に対する業界からの要望状況を示すものとして、平成 21 年 11 月 11 日から同年 12 月 11 日に実施された「インターネット上の著作権侵害コンテンツ対策に関する調査の結果について」<sup>73</sup>が参考になると思われる。

上記調査において、概ね規制強化に賛成する法人・団体が 17、概ね規制に慎重であるべきとする法人・団体が 7 であった。

また、上記調査において、アクセスコントロールの不正な回避を防止することに関して、デジタルコミック協議会等から、個人による回避行為自体を規制対象とすべきであるとの意見が、また、コンピュータエンターテイメント協会等から、関税法を改正して不正な回避装置等を輸入の差止め対象物とするとの意見が各々出されている。これに対して、電子情報技術産業協会等からは、研究開発等の企業活動を萎縮させる可能性があるため、規制には慎重であるべきであるとの意見が出されている。

そして、上記調査において、日本レコード協会等から、インターネットを介した被害については被害額の算定が困難であるから、法定賠償制度を創設すべきであるとの意見が出されている。これに対して、ヤフー株式会社等からは、現在の著作権法の適用により、個別の侵害実態に応じた柔軟な損害額の算定及び認定が行われているため、新たな制度は不要であるとの意見が出されている。

さらに、上記調査において、日本映像ソフト協会等から、著作権を侵害して行われるインターネット送信をするウェブサイトへ誘導するリンクをはる行為自体を著作権侵害行為とするべきであるとの意見が出されている。これに対して、日本知的財産協会等から、上記行為は現行法下でも違法とされる場合があるため、新たな規定の新設は不要であるとの意見が出されている。

ところで、いわゆる無反応機器については、著作権者の中には無反応機器を問題視する意見もある。しかし、その一方で、平成 16 年に文化庁へ提出された今後の法改正に関する意見の中で、著作物等の利用機器等を製造している業界は、利用機器等を提供する産業界に過大な負担を強いるという理由から規制に反対している<sup>74</sup>。

## (3) 法改正の動向・内容

法改正の動向は、現状見あたらない。ただし、現在、模倣品・海賊版拡散防止条約 (ACTA) が議論されているところ、そのアジェンダにおいて「第四節 デジタル環境における権利の執行」に関する項目の 1 つとして「技術的保護手段の回避(例外と制限の適用を含む)」の場合における救済措置の適用可能性が挙げられており<sup>75</sup>、ACTA の内容

<sup>73</sup> 知的財産戦略本部知的財産戦略推進事務局「インターネット上の著作権侵害コンテンツ対策に関する調査の結果について」<<http://www.kantei.go.jp/jp/singi/titeki2/chosaku/>>参照。

<sup>74</sup> 半田正夫ほか『著作権法コンメンタール 1』(勁草書房、2009)〔吉田大輔〕300 頁参照。

<sup>75</sup> <http://www.mofa.go.jp/mofaj/gaiko/ipr/atca09.html>  
[http://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/atca09\\_ja\\_ka.pdf](http://www.mofa.go.jp/mofaj/gaiko/ipr/pdfs/atca09_ja_ka.pdf)

によっては国内法の改正にも影響があるとみられている。

以 上

## **(関連条文)**

### **著作権法**

#### **(定義)**

#### **第2条第1項第20号**

#### **技術的保護手段**

電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法（次号において「電磁的方法」という。）により、第十七条第一項に規定する著作権若しくは著作権又は第八十九条第一項に規定する実演家人格権若しくは同条第六項に規定する著作隣接権（以下この号において「著作権等」という。）を侵害する行為の防止又は抑止（著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。）をする手段（著作権等を有する者の意思に基づくことなく用いられているものを除く。）であつて、著作物、実演、レコード、放送又は有線放送（次号において「著作物等」という。）の利用（著作者又は実演家の同意を得ないで行つたとしたならば著作権若しくは実演家人格権の侵害となるべき行為を含む。）に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは映像とともに記録媒体に記録し、又は送信する方式によるものをいう。

#### **(私的使用のための複製)**

#### **著作権法第30条第1項本文**

著作権の目的となつてゐる著作物（以下この款において単に「著作物」という。）は、個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること（以下「私的使用」という。）を目的とするときは、次に掲げる場合を除き、その使用する者が複製することができる。

#### **第30条第1項第2号**

技術的保護手段の回避（技術的保護手段に用いられている信号の除去又は改変（記録又は送信の方式の変換に伴う技術的な制約による除去又は改変を除く。）を行うことにより、当該技術的保護手段によつて防止される行為を可能とし、又は当該技術的保護手段によつて抑止される行為の結果に障害を生じないようにすることをいう。第二百十条の二第一号及び第二号において同じ。）により可能となり、又はその結果に障害が生じなくなつた複製を、その事実を知りながら行う場合

## (差止請求権)

### 第 112 条

著作者、著作権者、出版権者、実演家又は著作隣接権者は、その著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する者又は侵害するおそれがある者に対し、その侵害の停止又は予防を請求することができる。

- 2 著作者、著作権者、出版権者、実演家又は著作隣接権者は、前項の規定による請求をするに際し、侵害の行為を組成した物、侵害の行為によつて作成された物又は専ら侵害の行為に供された機械若しくは器具の廃棄その他の侵害の停止又は予防に必要な措置を請求することができる。

## (侵害とみなす行為)

### 第 113 条

次に掲げる行為は、当該著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する行為とみなす。

- 一 国内において頒布する目的をもつて、輸入の時に国内で作成したとしたならば著作者人格権、著作権、出版権、実演家人格権又は著作隣接権の侵害となるべき行為によつて作成された物を輸入する行為
- 二 著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する行為によつて作成された物（前号の輸入に係る物を含む。）を、情を知つて、頒布し、若しくは頒布の目的をもつて所持し、又は業として輸出し、若しくは業としての輸出の目的をもつて所持する行為
- 2 プログラムの著作物の著作権を侵害する行為によつて作成された複製物（当該複製物の所有者によつて第四十七条の二第一項の規定により作成された複製物並びに前項第一号の輸入に係るプログラムの著作物の複製物及び当該複製物の所有者によつて同条第一項の規定により作成された複製物を含む。）を業務上電子計算機において使用する行為は、これらの複製物を使用する権原を取得した時に情を知っていた場合に限り、当該著作権を侵害する行為とみなす。
- 3 次に掲げる行為は、当該権利管理情報に係る著作者人格権、著作権、実演家人格権又は著作隣接権を侵害する行為とみなす。
  - 一 権利管理情報として虚偽の情報を故意に付加する行為
  - 二 権利管理情報を故意に除去し、又は改変する行為（記録又は送信の方式の変換に伴う技術的な制約による場合その他の著作物又は実演等の利用の目的及び態様に照らしやむを得ないと認められる場合を除く。）
  - 三 前二号の行為が行われた著作物若しくは実演等の複製物を、情を知つて、頒布し、若しくは頒布の目的をもつて輸入し、若しくは所持し、又は当該著作物若しくは実演等を情を知つて公衆送信し、若しくは送信可能化する行為

- 4 第九十四条の二、第九十五条の三第三項若しくは第九十七条の三第三項に規定する報酬又は第九十五条第一項若しくは第九十七条第一項に規定する二次使用料を受ける権利は、前項の規定の適用については、著作隣接権とみなす。この場合において、前条中「著作隣接権者」とあるのは「著作隣接権者（次条第四項の規定により著作隣接権とみなされる権利を有する者を含む。）」と、同条第一項中「著作隣接権」とあるのは「著作隣接権（同項の規定により著作隣接権とみなされる権利を含む。）」とする。
- 5 国内において頒布することを目的とする商業用レコード（以下この項において「国内頒布目的商業用レコード」という。）を自ら発行し、又は他の者に発行させている著作権者又は著作隣接権者が、当該国内頒布目的商業用レコードと同一の商業用レコードであつて、専ら国外において頒布することを目的とするもの（以下この項において「国外頒布目的商業用レコード」という。）を国外において自ら発行し、又は他の者に発行させている場合において、情を知つて、当該国外頒布目的商業用レコードを国内において頒布する目的をもつて輸入する行為又は当該国外頒布目的商業用レコードを国内において頒布し、若しくは国内において頒布する目的をもつて所持する行為は、当該国外頒布目的商業用レコードが国内で頒布されることにより当該国内頒布目的商業用レコードの発行により当該著作権者又は著作隣接権者の得ることが見込まれる利益が不当に害されることとなる場合に限り、それらの著作権又は著作隣接権を侵害する行為とみなす。ただし、国内において最初に発行された日から起算して七年を超えない範囲内において政令で定める期間を経過した国内頒布目的商業用レコードと同一の国外頒布目的商業用レコードを輸入する行為又は当該国外頒布目的商業用レコードを国内において頒布し、若しくは国内において頒布する目的をもつて所持する行為については、この限りでない。
- 6 著作権者の名誉又は声望を害する方法によりその著作物を利用する行為は、その著作権者人格権を侵害する行為とみなす

#### **(損害額の推定等)**

#### **第114条**

著作権者、出版権者又は著作隣接権者（以下この項において「著作権者等」という。）が故意又は過失により自己の著作権、出版権又は著作隣接権を侵害した者に対しその侵害により自己が受けた損害の賠償を請求する場合において、その者がその侵害の行為によつて作成された物を譲渡し、又はその侵害の行為を組成する公衆送信（自動公衆送信の場合にあつては、送信可能化を含む。）を行つたときは、その譲渡した物の数量又はその公衆送信が公衆によつて受信されることにより作成された著作物若しくは実演等の複製物（以下この項において「受信複製物」という。）の数量（以下この項において「譲渡等数量」という。）に、著作権者等がその侵害の行為がなければ販売することができた物（受信複製物を含む。）の単位数当たりの利益の

額を乗じて得た額を、著作権者等の当該物に係る販売その他の行為を行う能力に応じた額を超えない限度において、著作権者等が受けた損害の額とすることができる。ただし、譲渡等数量の全部又は一部に相当する数量を著作権者等が販売することができないとする事情があるときは、当該事情に相当する数量に応じた額を控除するものとする。

- 2 著作権者、出版権者又は著作隣接権者が故意又は過失によりその著作権、出版権又は著作隣接権を侵害した者に対しその侵害により自己が受けた損害の賠償を請求する場合において、その者がその侵害の行為により利益を受けているときは、その利益の額は、当該著作権者、出版権者又は著作隣接権者が受けた損害の額と推定する。
- 3 著作権者又は著作隣接権者は、故意又は過失によりその著作権又は著作隣接権を侵害した者に対し、その著作権又は著作隣接権の行使につき受けるべき金銭の額に相当する額を自己が受けた損害の額として、その賠償を請求することができる。
- 4 前項の規定は、同項に規定する金額を超える損害の賠償の請求を妨げない。この場合において、著作権又は著作隣接権を侵害した者に故意又は重大な過失がなかつたときは、裁判所は、損害の賠償の額を定めるについて、これを参酌することができる。

### **(具体的態様の明示義務)**

#### **第 114 条の 2**

著作者人格権、著作権、出版権、実演家人格権又は著作隣接権の侵害に係る訴訟において、著作者、著作権者、出版権者、実演家又は著作隣接権者が侵害の行為を組成したもの又は侵害の行為によつて作成されたものとして主張する物の具体的態様を否認するときは、相手方は、自己の行為の具体的態様を明らかにしなければならない。ただし、相手方において明らかにすることができない相当の理由があるときは、この限りでない。

### **(書類の提出等)**

#### **第 114 条の 3**

裁判所は、著作者人格権、著作権、出版権、実演家人格権又は著作隣接権の侵害に係る訴訟においては、当事者の申立てにより、当事者に対し、当該侵害の行為について立証するため、又は当該侵害の行為による損害の計算をするため必要な書類の提出を命ずることができる。ただし、その書類の所持者においてその提出を拒むことについて正当な理由があるときは、この限りでない。

- 2 裁判所は、前項ただし書に規定する正当な理由があるかどうかの判断をするため必要があると認めるときは、書類の所持者にその提示をさせることができる。この場合においては、何人も、その提示された書類の開示を求められない。
- 3 裁判所は、前項の場合において、第一項ただし書に規定する正当な理由があるかどうかについて前項後段の書類を開示してその意見を聴くことが必要であると認めると

きは、当事者等（当事者（法人である場合にあつては、その代表者）又は当事者の代理人（訴訟代理人及び補佐人を除く。）、使用人その他の従業者をいう。第百十四条の六第一項において同じ。）、訴訟代理人又は補佐人に対し、当該書類を開示することができる。

- 4 前三項の規定は、著作者人格権、著作権、出版権、実演家人格権又は著作隣接権の侵害に係る訴訟における当該侵害の行為について立証するため必要な検証の目的の提示について準用する。

### **（鑑定人に対する当事者の説明義務）**

#### **第 114 条の 4**

著作権、出版権又は著作隣接権の侵害に係る訴訟において、当事者の申立てにより、裁判所が当該侵害の行為による損害の計算をするため必要な事項について鑑定を命じたときは、当事者は、鑑定人に対し、当該鑑定をするため必要な事項について説明しなければならない。

### **（相当な損害額の認定）**

#### **第 114 条の 5**

著作権、出版権又は著作隣接権の侵害に係る訴訟において、損害が生じたことが認められる場合において、損害額を立証するために必要な事実を立証することが当該事実の性質上極めて困難であるときは、裁判所は、口頭弁論の全趣旨及び証拠調べの結果に基づき、相当な損害額を認定することができる。

### **（名誉回復等の措置）**

#### **第 115 条**

著作者又は実演家は、故意又は過失によりその著作者人格権又は実演家人格権を侵害した者に対し、損害の賠償に代えて、又は損害の賠償とともに、著作者又は実演家であることを確保し、又は訂正その他著作者若しくは実演家の名誉若しくは声望を回復するために適当な措置を請求することができる。

### **（罰則）**

#### **第 120 条の 2 第 1 号**

次の各号のいずれかに該当する者は、三年以下の懲役若しくは三百万円以下の罰金に処し、又はこれを併科する。

技術的保護手段の回避を行うことを専らその機能とする装置（当該装置の部品一式であつて容易に組み立てることができるものを含む。）若しくは技術的保護手段の回避を行うことを専らその機能とするプログラムの複製物を公衆に譲渡し、若しくは貸与し、公衆への譲渡若しくは貸与の目的をもつて製造し、輸入し、若しくは所持し、

若しくは公衆の使用に供し、又は当該プログラムを公衆送信し、若しくは送信可能化した者

**第 120 条の 2 第 2 号**

業として公衆からの求めに応じて技術的保護手段の回避を行つた者

**(罰則)**

**第 121 条第 1 項**

第百十九条、第百二十条の二第三号及び第四号、第百二十一条の二並びに前条第一項の罪は、告訴がなければ公訴を提起することができない。



## 不正競争防止法

### (定義)

#### 第2条第1項第10号

営業上用いられている技術的制限手段（他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために用いているものを除く。）により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を当該技術的制限手段の効果を妨げることにより可能とする機能のみを有する装置（当該装置を組み込んだ機器を含む。）若しくは当該機能のみを有するプログラム（当該プログラムが他のプログラムと組み合わせられたものを含む。）を記録した記録媒体若しくは記憶した機器を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能のみを有するプログラムを電気通信回線を通じて提供する行為

#### 第2条第1項第11号

他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために営業上用いている技術的制限手段により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を当該技術的制限手段の効果を妨げることにより可能とする機能のみを有する装置（当該装置を組み込んだ機器を含む。）若しくは当該機能のみを有するプログラム（当該プログラムが他のプログラムと組み合わせられたものを含む。）を記録した記録媒体若しくは記憶した機器を当該特定の者以外の者に譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能のみを有するプログラムを電気通信回線を通じて提供する行為

#### 第2条第7項

電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。）により影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を制限する手段であつて、視聴等機器（影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録のために用いられる機器をいう。以下同じ。）が特定の反応をする信号を影像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式又は視聴等機器が特定の変換を必要とするよう影像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式によるものをいう。

## **(差止請求権)**

### **第3条**

不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、その営業上の利益を侵害する者又は侵害するおそれがある者に対し、その侵害の停止又は予防を請求することができる。

- 2 不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、前項の規定による請求をするに際し、侵害の行為を組成した物（侵害の行為により生じた物を含む。第五条第一項において同じ。）の廃棄、侵害の行為に供した設備の除却その他の侵害の停止又は予防に必要な行為を請求することができる。

## **(損害賠償)**

### **第4条**

故意又は過失により不正競争を行って他人の営業上の利益を侵害した者は、これによって生じた損害を賠償する責めに任ずる。ただし、第十五条の規定により同条に規定する権利が消滅した後にその営業秘密を使用する行為によって生じた損害については、この限りでない。

## **(損害の額の推定)**

### **第5条**

第二条第一項第一号から第九号まで又は第十五号に掲げる不正競争（同項第四号から第九号までに掲げるものにあつては、技術上の秘密（秘密として管理されている生産方法その他の事業活動に有用な技術上の情報であつて公然と知られていないものをいう。）に関するものに限る。）によって営業上の利益を侵害された者（以下この項において「被侵害者」という。）が故意又は過失により自己の営業上の利益を侵害した者に対しその侵害により自己が受けた損害の賠償を請求する場合において、その者がその侵害の行為を組成した物を譲渡したときは、その譲渡した物の数量（以下この項において「譲渡数量」という。）に、被侵害者がその侵害の行為がなければ販売することができた物の単位数量当たりの利益の額を乗じて得た額を、被侵害者の当該物に係る販売その他の行為を行う能力に応じた額を超えない限度において、被侵害者が受けた損害の額とすることができる。ただし、譲渡数量の全部又は一部に相当する数量を被侵害者が販売することができないとする事情があるときは、当該事情に相当する数量に応じた額を控除するものとする。

- 2 不正競争によって営業上の利益を侵害された者が故意又は過失により自己の営業上の利益を侵害した者に対しその侵害により自己が受けた損害の賠償を請求する場合において、その者がその侵害の行為により利益を受けているときは、その利益の額は、その営業上の利益を侵害された者が受けた損害の額と推定する。
- 3 第二条第一項第一号から第九号まで、第十二号又は第十五号に掲げる不正競争に

よって営業上の利益を侵害された者は、故意又は過失により自己の営業上の利益を侵害した者に対し、次の各号に掲げる不正競争の区分に応じて当該各号に定める行為に対し受けるべき金銭の額に相当する額の金銭を、自己が受けた損害の額としてその賠償を請求することができる。

- 一 第二条第一項第一号又は第二号に掲げる不正競争 当該侵害に係る商品等表示の使用
  - 二 第二条第一項第三号に掲げる不正競争 当該侵害に係る商品の形態の使用
  - 三 第二条第一項第四号から第九号までに掲げる不正競争 当該侵害に係る営業秘密の使用
  - 四 第二条第一項第十二号に掲げる不正競争 当該侵害に係るドメイン名の使用
  - 五 第二条第一項第十五号に掲げる不正競争 当該侵害に係る商標の使用
- 4 前項の規定は、同項に規定する金額を超える損害の賠償の請求を妨げない。この場合において、その営業上の利益を侵害した者に故意又は重大な過失がなかったときは、裁判所は、損害の賠償の額を定めるについて、これを参酌することができる。

#### **(信用回復の措置)**

##### **第 14 条**

故意又は過失により不正競争を行って他人の営業上の信用を害した者に対しては、裁判所は、その営業上の信用を害された者の請求により、損害の賠償に代え、又は損害の賠償とともに、その者の営業上の信用を回復するのに必要な措置を命ずることができる。

#### **(適用除外等)**

##### **第 19 条第 1 項**

第三条から第十五条まで、第二十一条（第二項第六号に係る部分を除く。）及び第二十二条の規定は、次の各号に掲げる不正競争の区分に応じて当該各号に定める行為については、適用しない。

##### **第 7 号**

第二条第一項第十号及び第十一号に掲げる不正競争 技術的制限手段の試験又は研究のために用いられる第二条第一項第十号及び第十一号に規定する装置若しくはこれらの号に規定するプログラムを記録した記録媒体若しくは記憶した機器を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該プログラムを電気通信回線を通じて提供する行為

## 民法

### (不法行為による損害賠償)

#### 民法第 709 条

故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。

### (共同不法行為者の責任)

#### 民法第 719 条

数人が共同の不法行為によって他人に損害を加えたときは、各自が連帯してその損害を賠償する責任を負う。共同行為者のうちいずれの者がその損害を加えたかを知ることができないときも、同様とする。

- 2 行為者を教唆した者及び幫助した者は、共同行為者とみなして、前項の規定を適用する。

## 関税法

### (輸出してはならない貨物)

#### 第 69 条の 2

次に掲げる貨物は、輸出してはならない。

- 三 特許権、実用新案権、意匠権、商標権、著作権、著作隣接権又は育成者権を侵害する物品
- 四 不正競争防止法（平成五年法律第四十七号）第二条第一項第一号から第三号まで（定義）に掲げる行為（これらの号に掲げる不正競争の区分に応じて同法第十九条第一項第一号から第五号まで（適用除外等）に定める行為を除く。）を組成する物品

### (輸入してはならない貨物)

#### 第 69 条の 11

次に掲げる貨物は、輸入してはならない。

- 九 特許権、実用新案権、意匠権、商標権、著作権、著作隣接権、回路配置利用権又は育成者権を侵害する物品
- 十 不正競争防止法第二条第一項第一号から第三号まで（定義）に掲げる行為（これらの号に掲げる不正競争の区分に応じて同法第十九条第一項第一号から第五号まで（適用除外等）に定める行為を除く。）を組成する物品

## Ⅱ コンテンツの技術的手段に係る各国法制度調査研究(EU 編)



## II コンテンツの技術的手段に係る各国法制度調査研究の調査項目 (EU 編)

### 1. コンテンツの技術的手段に関する国際ルール

#### (1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)

EU 及び仏、英、独はいずれも締結している。

#### (2) EU における自由貿易協定 (FTA) / 経済連携協定 (EPA) の技術的手段に関する規定の有無・内容

後述する各 EU 指令を除いて存在しない。

ただし、未だ批准には至っていないが、EU と韓国との FTA では、技術的手段に関する規定が存在する。

その内容は、後述する著作権指令第 6 条と同様である。ただし、以下の点において、著作権指令とは異なる。

まず、EU-韓国 FTA においては、データベースの sui generis right に関しての技術的手段については規制の対象外としている。次に、EU-韓国 FTA においては、著作権及び著作隣接権の例外によりユーザーが利益を享受できるように、権利者に対して自主的な手段をとるよう要請するとの規定を含んでいない。その代わりに、単に締約国は、各国法、WCT 条約、WPPT 条約に沿って、技術的手段についての規制の制限や例外を設けてもよいとされている。

### 2. コンテンツの技術的手段に関する法令等

#### (1) 該当する法令等

#### ア EU 指令

##### (ア) 著作権指令<sup>76</sup>

コンピューター・プログラム以外の著作権及び著作隣接権並びにデータベースについての sui generis right に関して、知りながら又は知ることのできる合理的な理由がありながら行う技術的手段の回避行為、及び、迂回装置の製造・頒布を防ぐために適当な措置を講ずることを加盟国に義務づけている(著作権指令第 6 条)。

<sup>76</sup> “Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society”(「著作権指令」)

## (イ) コンピューター・プログラム指令<sup>77</sup>

コンピューター・プログラムについて、迂回装置の製造・頒布を防ぐために適当な措置を講ずることを加盟国に義務づけている(コンピューター・プログラム指令第7条)。

※ その他、衛星放送等指令<sup>78</sup>においては、アクセス制限がなされている放送のアクセス制限を回避する迂回装置等の製造・頒布や広告を禁止することを加盟国に義務づけている<sup>79</sup>。また、データベース指令<sup>80</sup>には、技術的手段についての規定はない。

## イ フランス

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様、技術的手段の回避行為が禁止されるとともに、迂回装置等の製造・頒布が禁止される(知的財産法 L. 第 331 の 5 条～第 331 の 11 条、L. 第 342 の 3 条)。

コンピューター・プログラムについては、コンピューター・プログラム指令とは異なる規制となっており、迂回装置等を頒布する者に、ユーザーに対して、かかる迂回装置等を違法に利用した場合には、著作権侵害に基づく法的責任が生じることとなることを通知することを義務づけるに止まる(知的財産法 L. 第 122 の 6 の 2 条、R. 第 335 の 2 条)。

## ウ イギリス

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様、技術的手段の回避行為が禁止されるとともに、迂回装置等の製造・頒布が禁止される(著作権・意匠・特許法(「CDPA」)第 296ZA 条～第 296ZF 条)。

コンピューター・プログラムについては、基本的にコンピューター・プログラム指令と同様、迂回装置等の製造・頒布が禁止される(CDPA 第 296 条)。

---

<sup>77</sup> “Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (as amended and codified by Directive 2009/24/EC of 23 April 2009)”(「コンピューター・プログラム指令」)

<sup>78</sup> “Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access”(「衛星放送等指令」)

<sup>79</sup> 著作権指令と衛星放送等指令の重複適用はあり得るとされる(現地報告書(EU編)2頁)。

<sup>80</sup> “Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases”(「データベース指令」)



## エ ドイツ

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様、技術的手段の回避行為が禁止されるとともに、迂回装置等の製造・頒布が禁止される(著作権法第 95a 条～第 95d 条)。

コンピューター・プログラムについては、基本的にコンピューター・プログラム指令と同様、迂回装置等の製造・頒布が禁止される(著作権法第 69f 条)。

### (2) 法令等の規制内容

#### (a) 規制対象技術(定義及び対象技術の具体例等)

##### ア EU 指令

###### (ア) 著作権指令

「効果的な技術的手段」の回避行為及び迂回装置の製造・頒布が禁止される。ここで、「技術的手段」とは、その通常の過程において、著作権等の権利者の許諾のない行為を制限するように設計された技術、装置、部品である(著作権指令第 6 条第 3 項)。

また、「効果的」とは、権利者により、アクセスコントロールや保護過程(Protection process)、又は、コピーコントロールの適用を通じて、著作物等の使用がコントロールされ、保護の目的を達成する場合を意味する(著作権指令第 6 条第 3 項)。

ここで、アクセスコントロールや保護過程の例示として、暗号化、スクランブリング、その他の著作物の変形が挙げられているが、技術中立的に規定されている。コピーコントロールについては、例示はなく、技術中立的に規定されている。

###### (イ) コンピューター・プログラム指令

コンピューター・プログラムを保護するために適用されていると見做されるいかなる技術的手段(any technical device which may have been applied to protect a computer program)の除去、回避行為が禁止されている(コンピューター・プログラム指令第 7 条第 1 項(c))。

## イ フランス

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様である(知的財産法 L. 第 331 の 5 条)。

コンピューター・プログラムについては、端的にコンピューター・プログラムを保護する技術的手段とされているのみである(知的財産法 L. 第 122 の 6 の 2 条)。

## ウ イギリス

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様である(CDPA 第 296ZF 条)。

コンピューター・プログラムについては、コンピューター・プログラムの著作権者の許諾がなく、かつ、著作権法で制限されている行為を防止し、制限することを目的としたいかなる装置と規定されている(CDPA 第 296 条(6))。これは、コンピューター・プログラム指令よりも範囲が限定されているといえる<sup>81</sup>。

## エ ドイツ

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様である(著作権法第 95a 条(2))。

コンピューター・プログラムについては、基本的にコンピューター・プログラム指令と同様である(著作権法第 69f 条(2))。

### (b) 規制対象製品及び対象プログラム等

#### ア EU 指令

##### (ア) 著作権指令

迂回装置等については、技術中立的に規定されている。

迂回装置等は、以下の(i)～(iii)のいずれかに該当するものである。(著作権指令第 6 条第 2 項(a)～(c))

(i) 効果的な技術的手段の回避を目的として宣伝され、広告され、もしくは販売されたもの

(ii) 効果的な技術的手段の回避の他には、限られた商業上の重大な目的もしくは利用方法しか存在しないもの

(iii) 専ら効果的な技術的手段の回避を可能にし、もしくは容易にする目的で設計、製造、適合、もしくは実行されるもの

##### (イ) コンピューター・プログラム指令

迂回装置等については、技術中立的に規定されている。

迂回装置等は、技術的手段を回避することを容易にすることを唯一の目的とするあらゆる手段とされている(コンピューター・プログラム指令第 7 条第 1 項(c))。

## イ フランス

迂回装置等については、技術中立的に規定されている。

コンピューター・プログラム以外の著作物については、効果的な技術的手段の回避の目的のために設計され、又は、特に適合された手段とされる(知的財産法 L. 第 335

<sup>81</sup> 現地報告書(EU 編)14 頁。

の3の1条、R.第335の3条)。著作権指令第6条第2項(c)(上記ア・(ア)・(iii))に相当するものである。著作権指令第6条第2項(a)、(b)に対応する明示の規定はない<sup>82</sup>。

コンピューター・プログラムについては、コンピューター・プログラムを保護する技術的手段を除去又は回避する手段とだけ規定されており(知的財産法L.第122の6の2条)、コンピューター・プログラム指令とは異なり、目的による限定がなされていない。

## ウ イギリス

迂回装置等については、技術中立的に規定されている。

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様である(CDPA第296ZD条)。

コンピューター・プログラムについては、基本的にコンピューター・プログラム指令と同様である(CDPA第296条(1))。

## エ ドイツ

コンピューター・プログラム以外の著作物については、基本的に著作権指令と同様である(著作権法第95a条(3))。

コンピューター・プログラムについては、基本的にコンピューター・プログラム指令と同様である(著作権法第69f条(2))。

### (c) 規制対象行為

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

## ア EU 指令

### (ア) 著作権指令

知りながら又は知ることのできる合理的な理由がありながら行う技術的手段の回避行為(上記⑥)が規制の対象となっている(著作権指令第6条第1項)。また、回避サービスの提供(上記⑤)が規制の対象となっている(著作権指令第6条第2項)。

迂回装置等については、製造、輸入、頒布、販売、貸与、販売もしくは貸与目的の広告、商業目的の所持が規制の対象であるので(著作権指令第6条第2項)、上記①、②、③のうち輸入行為、④のうち商業目的の所持、⑦のうち販売と貸与目的の宣伝が規制の対象である。

<sup>82</sup> 現地報告書(EU編)12頁参照。

③のうち輸出行為については、規制の対象ではないとされる<sup>83</sup>。

#### **(イ) コンピューター・プログラム指令**

回避行為自体は規制の対象ではない。

迂回装置等(「技術的手段を回避することを容易にすることを唯一の目的としたあらゆる手段」)を流通に置く全ての行為または商業目的で所持する行為が規制の対象である(コンピューター・プログラム指令第7条第1項(c))。

### **イ フランス**

#### **(ア) コンピューター・プログラム以外の著作物**

回避行為(上記⑥)との関係では、迂回装置等を用いない回避行為(知的財産法 L. 第 335 の 3 の 1 条)、迂回装置等の利用(知的財産法 R. 第 335 の 3 条 I)、迂回サービスの利用(知的財産法 R. 第 335 の 3 条 II)が規制されている。

所持行為(上記④)との関係では、個人利用目的での迂回装置等の所持(知的財産法 R. 第 335 の 3 条 I)、商業目的での迂回装置等の所持(知的財産法 L. 第 335 の 3 の 1 条 II)の双方が規制されている。

迂回装置等については、製造、輸入、商業目的での提供、公衆への提供が規制されている(知的財産法 L. 第 335 の 3 の 1 条 II)。

また、回避サービスの提供行為が規制されている(知的財産法 L. 第 335 の 3 の 1 条 II)。そして、迂回装置等や回避サービスの宣伝行為も禁止されている(知的財産法 L. 第 335 の 3 の 1 条 II)。

#### **(イ) コンピューター・プログラム**

迂回装置等を頒布する者は、ユーザーに対して、かかる迂回装置等を違法に利用した場合には、著作権侵害に基づく法的責任が生じることとなる旨通知する義務を負うに止まる(知的財産法 L. 第 122 の 6 の 2 条、R. 第 335 の 2 条)。

ただし、裁判例からは、著作権侵害を可能にする回避装置の頒布もまた、著作権侵害にあたり得ることとなる<sup>84</sup>。

### **ウ イギリス**

#### **(ア) コンピューター・プログラム以外の著作物**

回避行為が規制されている(CDPA 第 296ZA 条(1))。

迂回装置等の製造、輸入、頒布、販売、貸与、販売もしくは貸与目的での提供・陳列、販売もしくは貸与目的での宣伝、商業目的での所持、回避サービスの提供が規制

---

<sup>83</sup> 現地報告書(EU 編)15 頁参照。

<sup>84</sup> 現地報告書(EU 編)17 頁。

されている(CDPA 第 296ZD 条(1) (b))。

なお、刑事罰の対象となる行為については、絞りがかけられており、商業目的を有することや、商業過程で行われること、又は、権利者に悪影響を及ぼすことが要件となっており、また、迂回装置等については、専ら効果的な技術的手段の回避を可能にし、もしくは容易にする目的で設計、製造、適合、もしくは実行されるものに限定される(CDPA 第 296ZB 条参照)。

### **(イ) コンピューター・プログラム**

迂回装置等の販売・貸与のための製造、輸入、頒布、販売・貸与、販売・貸与のための提供・陳列、販売・貸与のための宣伝、商業目的の所持が規制されている(CDPA 第 296 条(1) (b) (i))。

さらに、技術的手段の除去・回避を可能にし、または補助することを目的とした情報を公表する行為も規制の対象である(CDPA 第 296 条(1) (b) (ii))<sup>85</sup>。

## **エ ドイツ**

### **(ア) コンピューター・プログラム以外の著作物**

回避行為が規制されている(著作権法第 95a 条(1))。

迂回装置等については、製造、輸入、頒布、販売、貸与、販売・貸与目的の宣伝、商業目的の所持が規制されている(著作権法第 95a 条(3))。

また、回避サービスの提供が規制されている(著作権法第 95a 条(3))。

### **(イ) コンピューター・プログラム**

コンピューター・プログラムについては、著作権法第 95a 条～第 95d 条の適用がない。もっとも、著作権法第 69f 条(2)は、権利者は迂回装置等の破棄を求めることができることとされており、また、著作権法第 97 条に基づき迂回装置等の頒布について差止命令及び民事損害賠償を求めることができることとした裁判例、学説がある<sup>86</sup>。

## **(3) 除外行為**

### **(a) コンテンツの技術的手段に関する規定の適用除外、例外、制限規定等の存否・内容**

#### **ア EU 指令**

##### **(ア) コンピューター・プログラム以外の著作物等**

著作権指令第 6 条第 4 項は、技術的手段の保護と、著作権の例外、制限の行使とのバランスを配慮した規定である。

<sup>85</sup> この点については、コンピューター・プログラム指令よりも広範ともいい得るとされる(現地報告書(EU 編)19 頁)。

<sup>86</sup> 現地報告書(EU 編)20、39 頁。

#### a 著作権指令第6条第4項第1段落

出発点としては、権利者による任意的な解決がなされることが想定されている。任意的な解決としては、種々の方法が考えられ、例えば、技術的手段により保護されていない著作物の交付、技術的手段を解除するための暗号を解読する鍵の提供、適法な利用を可能とするように技術的手段を設計することなどがある<sup>87</sup>。

そして、権利者による任意的な解決がない場合には、加盟国は、権利者が、著作権指令第5条第2項(a)、同項(c)、同項(d)、同項(e)、同条第3項(a)、同項(b)もしくは同項(e)に従って国内法において規定される著作権等の例外または制限の受益者(ユーザー)に対して、かかる例外または制限から利益を得ることのできる方法を提供するように適切な措置をとらなければならないとしている(著作権指令第6条第4項第1段落)。

ここで引用されている著作権指令第5条に規定されている著作権等の例外は、同条第2項関係(複製権のみの例外)としては、コピー機による複製(アナログ複製)、図書館や博物館等の商業的利益を目的としない一定の機関による複製、放送機関による複製、病院・刑務所内での複製、同条第3項関係(著作権全ての例外)としては、教育・研究のための制限、障害者による利用のための制限、公共の安全、行政・立法・裁判手続のための制限である。

ただし、ユーザーが、こうした例外・制限から利益を得るための措置は、かかる著作権等の例外または制限から利益を得るために必要な限度でなされること、かつ受益者が関連する保護された著作物等に適法にアクセスできる場合に限るとされている(著作権指令第6条第4項第1段落)。

このように著作権指令は、権利者に対して措置をとることを要請するものであり、受益者(ユーザー)の側において回避行為を行うことを許容するものではない。また、著作権指令第6条第4項は、同指令第6条第1項のみの例外を規定するものなので、回避行為自体との関係でしか妥当しない。迂回装置等の頒布についての規制の例外は存在しない。

#### b 著作権指令第6条第4項第2段落(私的使用のための複製関係)

私的使用のための複製に関する例外との調整については、著作権指令第6条第4項第2段落で別途規定されている。ここでは、加盟国は、第5条第2項(b)に従って規定される私的使用のための例外または制限の受益者との関係においても、同項第1段落で定めるような措置をとることができるとされている。このよ

---

<sup>87</sup> 現地報告書(EU編)21頁。

うに、私的使用のための複製に関する例外との調整措置を規定するかどうかは、加盟国の義務ではなく、任意である。

また、権利者が、私的使用目的の複製のための手段をユーザーに提供する場合には、その複製物の数を限定することができるかとされている(著作権指令第 6 条第 4 項第 2 段落)。

## **c オン・デマンドサービスの取り扱い**

著作権指令第 6 条第 4 項第 5 段落は、いわゆるオン・デマンドサービスについては、同項第 1 段落及び第 2 段落の調整規定が適用されないとしている。これは、当事者間の契約自由を尊重する趣旨であるとされる<sup>88</sup>。

## **(イ) コンピューター・プログラム**

コンピューター・プログラムについての技術的手段の保護と著作権の例外との調整については、コンピューター・プログラム指令には規定が存在しない。もともと、かかる調整については、著作権指令において言及されており、コンピューター・プログラムについての技術的手段の保護は、コンピューター・プログラム指令の第 5 条第 3 項(調査・研究のための例外)及び第 6 条(互換性のための例外)の規定に従って行われる行為を可能にするために必要な技術的手段を回避する方法の開発または利用を抑制または防止すべきではないとされている(著作権指令前文第 50 項)。

したがって、コンピューター・プログラムについての技術的手段との関係においては、調査研究又は互換性を達成するとの目的に必要な迂回装置等の頒布について<sup>89</sup>、禁止されていないと解することができるかもしれない<sup>90</sup>。

## **イ フランス**

### **(ア) コンピューター・プログラム以外の著作物等**

教育と研究の例外、障害者のための例外、図書館・博物館の例外、公共の安全、行政・立法・裁判手続のための例外、私的利用のための例外が規定されている(知的財産法 L. 第 331 の 31 条)。

ただし、これらの例外については、コピーコントロールについてのみ認められ、アクセスコントロールについては認められない。また、著作物等の通常の使用を妨げず、権利者の正当な利益を不公正に損なうことのない場合にのみ認められる。(知的

---

<sup>88</sup> 現地報告書(EU 編)24 頁。

<sup>89</sup> 先述したように、コンピューター・プログラムについての技術的手段との関係では回避行為自体はそもそも規制されていない。

<sup>90</sup> かかる調整規定は、指令本体の条項ではなく前文に規定されているのみであるが、著作権指令前文第 50 項は、コンピューター・プログラムについての技術的手段の保護の例外を創設したと一般的に認められているとされる(現地報告書(EU 編)26 頁)。

財産法 L. 第 331 の 7 条第 2 段落)

さらに、互換性のための例外が特別に規定されている(知的財産法 L. 第 331 の 5 条第 4 段落、L. 第 331 の 31 条、L. 第 331 の 32 条)。

### (イ) コンピューター・プログラム

(参考として、コンピューター・プログラムの保護との関係での例外として、)誤謬を修正するための例外(知的財産法 L. 第 122 の 6 の 1 条 I)、バックアップのための例外(知的財産法 L. 第 122 の 6 の 1 条 II)、調査・研究のための例外(知的財産法 L. 第 122 の 6 の 1 条 III)、互換性のための例外(知的財産法 L. 第 122 の 6 の 1 条 IV)が規定されている<sup>91</sup>。

### (ウ) 例外の実施

著作権指令に規定されるように、まずは、権利者の自主的な対応に委ねられている(知的財産法 L. 第 331 の 7 条参照)。

権利者とユーザーとの間の自主的解決が達成できない場合には、ユーザーは、フランスにおいて技術的手段について規制を行う HADOPI に解決を要請することができる(知的財産法 L. 第 331 の 33 条)。HADOPI はかかる要請を受けて、例外の行使のための条件等を定めた上で、権利者に例外行使のために行動すべきことを命令することができる。

さらに、コンピューターセキュリティ又は暗号化研究のためであれば、権利者に損害を生じさせない限りにおいて、権利者の承諾なく回避行為を行うことについては刑事責任が生じないとされている(知的財産法 R. 第 335 の 3 条、R. 第 335 の 4 条)。

## ウ イギリス

### (ア) コンピューター・プログラム以外の著作物等

コンピューター・プログラム以外の著作物等については、CDPA 第 296ZE 条が、CDPA 別表 5A を引用する形で例外を規定している。別表 5A には、研究や私的調査、視覚障害者のための例外、教育的放送機関による例外、議会・司法手続のための例外、法定権限に基づく行為による例外等が規定されている。もともと、かかる例外事由は、CDPA に定められる著作権の例外事由に比し狭く、例えば、一時的複製の例外(CDPA 第

<sup>91</sup> 現地報告書(EU 編)27 頁にはコンピューター・プログラムに関する例外として記載されているが、これはコンピューター・プログラムの保護の例外との趣旨であると思われる。そもそもフランスにおいては、先述のとおり、法律の条文としては、コンピューター・プログラムについては、迂回装置等の製造・頒布は直接禁止されてはならず、一定の表示義務を課されているに止まる。そこで、法律の条文としては、技術的手段についての例外・除外はそもそも問題とならないと思われる。



28 条 A)、批評、報道の例外(CDPA 第 30 条)、教育目的のためのアンソロジーの例外(CDPA 第 33 条)、教育機関における記録、上映等の例外(CDPA 第 34 条)等については含まれていない<sup>92</sup>。また、私的使用のための複製も例外とされていない<sup>93</sup>。

他に、暗号化研究のための例外(CDPA 第 296ZA 条(2))、国家安全保障、犯罪抑止や捜査目的における法執行機関、情報機関の活動の例外(CDPA 第 296ZB 条(3))が規定されている。

#### (イ) コンピューター・プログラム

コンピューター・プログラムについては、特別に例外を定めた規定はない<sup>94</sup>。

#### (ウ) 例外の実施

コンピューター・プログラム以外の著作物等について、ユーザーは、担当国務長官に解決を要請することができる。国務長官は、権利者とユーザーとの間の自主的解決の存在の有無を調査の上、自主的解決が達成できない場合には、例外の行使のための条件等を定めた上で、権利者に例外行使のために行動すべきことを命令をすることができる。(CDPA 第 296ZE 条)

### エ ドイツ

#### (ア) コンピューター・プログラム以外の著作物等

コンピューター・プログラム以外の著作物等については、著作権法第 95b 条が規定しており、公共の安全・司法執行のための例外、障害者のための例外、学校利用・教育目的の編集のための例外、学校教育利用の放送のための例外、調査及び私的研究のための例外が規定されている。その他には、公共の安全、犯罪対策の目的の公権力機関による職務については、規制の対象とならない(著作権法第 95a 条(4))。

ただし、私的利用のための複製については、私的な研究目的における写真的複製(アナログ複製)等が例外とされるのみであり、私的利用目的のためのデジタル複製は例外となされていない<sup>95</sup>。

#### (イ) コンピューター・プログラム

コンピューター・プログラムについては、特別に例外を定めた規定は不見当である。

---

<sup>92</sup> 現地報告書(EU 編)29 頁参照。

<sup>93</sup> 現地報告書(EU 編)24 頁参照。

<sup>94</sup> 現地報告書(EU 編)29～31 頁参照。もっとも、先述したとおり、コンピューター・プログラムについては、回避行為自体は禁止されていない。

<sup>95</sup> 現地報告書(EU 編)31～32 頁参照。

#### (ウ) 例外の実施

権利者は、例外の受益者(ユーザー)に対して例外を行使する手段を提供しなければならないとされる(著作権法第 95b 条(1))。かかる義務の違反については、ユーザーは手段の提供を訴訟において請求できる(著作権法第 95b 条(2) 参照)。

#### (b) 著作権法にコンテンツの技術的手段に関する規定が存在する場合の技術的手段回避の禁止規定と権利制限規定との関係

上述(3)(a)の記述を参照。

#### (4) 救済措置

##### (a) 救済措置の内容(民事的救済及び刑事的制裁)

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

#### ア EU 指令

##### (ア) 著作権指令

加盟国は、適切な制裁及び救済を規定するものとし、かかる制裁及び救済が確実に適用されるために必要な全ての措置をとるものとする。そして、このようにして規定される制裁は、有効であり、比例的であり、かつ抑止力を有するものとする(著作権指令第 8 条第 1 項)

さらに、加盟国は、自国の領土内で行われた侵害行為により利益が害された権利者が、損害賠償を求めて訴訟を起こし、差し止めを求め、さらに適切である場合には、迂回装置等の没収を求めることができるようにするために必要な措置をとるものとする(著作権指令第 8 条第 2 項)。

##### (イ) コンピューター・プログラム指令

加盟国は、禁止行為に対して適切な救済を定めることとされる(コンピューター・プログラム指令第 7 条第 1 項)。

さらに、加盟国は、迂回装置等についての没収について定めることができるとされる(コンピューター・プログラム指令第 7 条第 3 項)。

#### イ フランス

##### (ア) 民事救済<sup>96</sup>

知的財産法に違反する行為であり、権利者に損害が生じた場合には、不法行為に基

<sup>96</sup> 現地報告書(EU 編)33~34 頁参照。

づく民事損害賠償請求、差止請求をすることができる。

コンピューター・プログラム以外の著作物等については、証拠の差し押さえや暫定措置を求めることができる (decree no. 2006-1763 により導入された。L. 第 332 の 1 条参照)。

もし、回避行為ないし迂回装置等の頒布がインターネットを通じて行われている場合には、権利者は、インターネット・サービス・プロバイダ(「ISP」)に対して、これらの行為を停止するための適切な措置をとるように求めることができる (2004 年 6 月 21 日法 6. I. 8)。

## (イ) 刑事制裁

コンピューター・プログラム以外の著作物等については、以下の三類型に分けられる。①迂回装置等の頒布等や回避サービスの提供について、6 ヶ月以下の自由刑及び 30000 ユーロ以下の罰金が科される (知的財産法 L. 第 335 の 3 の 1 条 II、L. 第 335 の 4 の 1 条 II 等)。②迂回装置等を用いない回避行為について、3750 ユーロ以下の罰金が科される (知的財産法 L. 第 335 の 3 の 1 条 I、L. 第 335 の 4 の 1 条 I 等)。③個人利用目的での迂回装置等の所持、迂回装置等の利用、迂回サービスの利用について、750 ユーロ以下の罰金が科される (知的財産法 R. 第 335 の 3 条等)。

コンピューター・プログラムについては、裁判例において、迂回装置等の提供は、知的財産法 L. 第 122 の 6 条、L. 第 335 の 3 条によって規制されるどころの一般の著作権を侵害する行為とされ得る。その場合には、著作権侵害について規定されている刑事責任が生じることとなる。

また、コンピューター・プログラムについて、迂回装置等の頒布につき、法で規定する通知をユーザーに怠った場合には、450 ユーロ以下の罰金が科される (知的財産法 L. 第 122 の 6 の 2 条、L. 第 335 の 2 条)。

## ウ イギリス

### (ア) 民事救済<sup>97</sup>

CDPA に違反する行為であり、権利者に損害が生じた場合には、不法行為に基づく民事損害賠償請求 (被告が知らなかった場合、また、知ることのできる合理的な理由がない場合は除く)、差止請求 (暫定措置も可能) をすることができる。

また、迂回装置等の没収を求めることができる (CDPA 第 296 条 (4)、第 296ZD 条)。

特定の条文はないが、一般法理で、被告に対して侵害の経路等についての情報提供を求めることができる。

<sup>97</sup> 現地報告書 (EU 編) 35～37 頁参照。

## (イ) 刑事制裁

CDPA 第 296ZB 条(コンピューター・プログラム以外の著作物等についての迂回装置等の頒布のうち悪質なもの<sup>98</sup>)に違反する場合には、刑事罰の対象となる。

略式起訴手続の場合には、3 ヶ月以下の自由刑又は法令上の上限を超えない額の罰金、又はこれらの併科である。正式起訴手続の場合には、2 年以下の自由刑又罰金、又はこれらの併科である。没収についても規定されている(CDPA296ZC 条)。

## エ ドイツ

### (ア) 民事救済<sup>99</sup>

技術的手段に関する規制の違反に対しては、著作権法第 97 条に基づき差止請求(迂回装置等の頒布に関して)、損害賠償請求(商業的な違反の場合)をすることができるとする裁判例、学説がある。また、不法行為の法理に基づく差止請求、損害賠償請求もし得る。また、侵害者や第三者(ISP 等)に対して侵害の経路等について情報の提供を求めることができる(商業的な違反の場合。著作権法第 101 条)。

## (イ) 刑事制裁

コンピューター・プログラム以外の著作物等については、技術的手段についての規制の違反は刑事制裁(1 年以下の自由刑又は罰金)の対象となる(回避行為について著作権法第 108b 条(1)、迂回装置等の製造・頒布について同条(2))。

コンピューター・プログラムについては、技術的手段に関して特に刑事罰は設けられていない。

<b>(b) (a) の救済措置の請求主体</b>
---------------------------

## ア フランス<sup>100</sup>

### (ア) 民事救済

違反行為により影響(損害等)を被る者が、損害賠償を求めることができる。技術的手段そのものが知的財産権として保護されていない場合には、技術的手段の開発者等は損害賠償請求をすることができない。

## (イ) 刑事制裁

検察官である。ただし、違反行為により影響を被る者も訴追することができる。

<sup>98</sup> 詳細は、本報告第 2・2・(2)・(c)・ウを参照。

<sup>99</sup> 現地報告書(EU 編)38~39 頁参照。

<sup>100</sup> 現地報告書(EU 編)40 頁参照。

## イ イギリス<sup>101</sup>

### (ア) 民事救済

CDPA 第 296 条(コンピューター・プログラムについての迂回装置等の頒布)及び CDPA 第 296ZD 条(コンピューター・プログラム以外の著作物等についての迂回装置等の頒布)は、以下の 3 類型の者について民事救済を得る権利を認めている。①公衆に技術的手段により保護されている著作物等を発行・発信している者、②①の者と異なる場合には、著作権者又は当該権利について排他的ライセンスを受けた者、③技術的手段についての知的財産権を有する者又は当該権利について排他的ライセンスを受けた者。

CDPA 第 296ZA 条(回避行為の禁止)については、上記の 3 類型の者のうち、①と②についてのみ民事救済を得る権利を認めている。

### (イ) 刑事制裁

検察官である。

## ウ ドイツ<sup>102</sup>

### (ア) 民事救済

違反行為により影響(損害等)を被る者である。

### (イ) 刑事制裁

検察官である。ただし、検察官による訴追がなされない場合には、違反行為により影響を被る者も訴追することができる。

### (c) 違反機器等の輸出入にかかる水際措置又は違反抑止のための行政措置の有無・内容

EU 指令、フランス法、イギリス法、ドイツ法においては、迂回装置等についての水際措置は特に規定されていない。

### (5) いわゆる「無反応機器」規制

#### いわゆる「無反応機器」に対する法令、規則、指令等による規制の有無・内容

著作権指令もコンピューター・プログラム指令も、いわゆる無反応機器を特に規制の対象とはしていない。

もともと、著作権指令との関係では、いわゆる無反応機器が、(i)効果的な技術的手段の回避を目的として宣伝され、広告され、もしくは市販されたもの、(ii)効果的な技術的手段の回避の他には、限られた商業上の重大な目的もしくは利用方法しか存

<sup>101</sup> 現地報告書(EU 編)40~41 頁参照。

<sup>102</sup> 現地報告書(EU 編)41 頁参照。

在しないもの、(iii)専ら効果的な技術的手段の回避を可能にし、もしくは容易にする目的で設計、製造、適合、もしくは実行されるものに該当する場合には規制の対象となる<sup>103</sup>。著作権指令前文第 48 項においても、通常の電子機器の運用及び技術開発を妨害してはならないこと、禁止されるものとの関係を除けば、特定の装置、製品、部品またはサービスを設計しなくてはならないという義務を課すものではないことが述べられている。

同様に、コンピューター・プログラム指令との関係でも、いわゆる無反応機器が、技術的手段を回避することを容易にすることを唯一の目的としたあらゆる手段に該当する場合は規制的対象となる<sup>104</sup>。

EU 指令と同様に、フランス法、イギリス法、ドイツ法においても特に無反応機器についての規制はなされていない(それぞれの国内法に定める迂回装置等の定義に該当しない限り、規制の対象とはならない)。

### 3. 裁判例、執行状況、被害状況等

#### (1) コンテンツの技術的手段に関する裁判例<sup>105</sup>

##### ア フランス

先例の蓄積としては、消費者が、著作権の制限による利益の享受を企図して行う訴訟が中心である。フランスが、著作権指令を国内で実施をして以降は、こうした訴えは法廷でなく、HADOPI に提起しなければならなくなった(かかる立場は、フランスの最高裁判所に相当する Cour de Cassation でも確認されている<sup>106</sup>)。もっとも、消費者はかかる判断を迂回する観点から、製品の品質の暗黙の保証を理由として通常裁判において争ったり、消費者法を基に通常裁判において争う例も見られる。

技術的手段の回避行為や迂回装置等の頒布が問題になったケースものとして以下の 2 件がある。

まず、1989 年には、コンピューター・プログラムを保護する技術的手段の回避行為は当然には違法とならないとされた<sup>107</sup>。この判決は、コンピューター・プログラム指令以前のものであるが、現在でも引き続き妥当するとされる。

<sup>103</sup> 著作権指令第 6 条第 2 項参照。現地報告書(EU 編)42 頁。現実的には、(i)効果的な技術的手段の回避を目的として宣伝され、広告され、もしくは市販されたものに該当し得るかもしれない。

<sup>104</sup> コンピューター・プログラム指令第 7 条第 1 項(c)。現地報告書(EU 編)43 頁。現実的には、いわゆる無反応機器がこれに該当することは考えにくいものと思われる。

<sup>105</sup> 現地報告書(EU 編)44~48 頁参照。

<sup>106</sup> Cour de Cassation, 19 June 2008.

<sup>107</sup> Paris Court of Appeals, 13e ch., 2 March 1989.

次に、2005年に、刑事訴訟において、コンピューター・プログラムを保護する技術的手段につき迂回装置等を開発、頒布する行為について、著作権侵害となる(知的財産法L.第335の3条)との判決が下された<sup>108</sup>。

## イ イギリス

先例は非常に少ない。

民事訴訟としては、Sony 対 Owen 事件<sup>109</sup>及び Sony 対 Ball 事件<sup>110</sup>において、プレイステーション 2 のゲームソフト及びコンソールに付加された、地域制限のための技術的手段(regional control code and devices)を回避することを可能とする迂回装置等を輸入し、イギリスにおいて販売したことが CDPA 第 296 条に違反するとされた。

また、最近、ゲームソフトやコンソールに付加されている技術的手段を回避し、海賊版のゲームソフトを利用することができるようにするモッドチップを商業的に提供、販売、保持、頒布していたことについて、CDPA 第 296ZB 条に違反するものとして、刑事訴追がなされた<sup>111</sup>。

## ウ ドイツ

技術的手段を回避するソフトウェアを ebay にて提供する行為について違法とされた例がある<sup>112</sup>。

技術的手段を回避するソフトウェアがリンク先のウェブサイトで提供されていることを知りながら、当該ウェブサイトへのハイパーリンクを自らの開設するウェブサイトに設けることが著作権法第 95a 条(3)に違反するとされた例がある<sup>113</sup>。

また、著作権法第 95a 条(3)に規定される「広告」について、商業的な活動に限定されず、問題となる製品の販売を促進するいかなる種類の言明も含まれるとして、ebay において 1 回だけ販売のために提供した行為もこれに該当するとした例がある<sup>114</sup>。

技術的手段の回避についての記事を発行すること自体は、著作権法第 95a(3)に規定

---

<sup>108</sup> Paris Court of Appeals, 13e ch., 17 June 2005.

フランスがコンピューター・プログラム指令第 7 条(1)を完全には実施していないことを踏まえた救済的判断との評価も可能である(現地報告書(EU 編)44 頁)。

<sup>109</sup> Sony Computer Entertainment v Owen & Ors [2002] EWHC 45 Ch.

<sup>110</sup> Kabushiki Kaisha Sony Computer Entertainment Inc v Ball & Ors [2004] EWHC 1738 Ch.

<sup>111</sup> Higgs 対 R 事件及び R 対 Gilham 事件。R 対 Gilham 事件においては、CDPA 第 296ZB 条の基で刑事訴追をする場合の要件事実を詳細に裁判所が判断した。また、Higgs 対 R 事件については、訴追側において、海賊版 DVD ソフトを利用することが、著作物の全体ないし重要部分の複製を伴うことについての立証をしなかったため被告人が勝訴している。詳細は、現地報告書(EU 編)46 頁参照。

<sup>112</sup> LG München, 13.6.2007, 21 S 2042/06 及び LG Köln, 23.11.2005, 28 S 6/05.

<sup>113</sup> LG München, 14.11.2007, 21 O 6742/07; LG München 11.10.2006, 21 O 2004/06.

<sup>114</sup> BGH, 17.7.2008, I ZR 219/05.

される「広告」に該当せず、また、技術的手段を回避することの一般的なガイダンスを含む記事を発行すること自体は、回避サービスの提供には該当しないとした例がある<sup>115</sup>。

## (2) コンテンツの技術的手段に関する執行状況

執行状況についての統計的資料は入手できなかった。

## (3) コンテンツの技術的手段に関する被害状況

被害状況についての統計的資料は入手できなかった。

## 4. 技術動向の調査

### (1) コンテンツの技術的手段に関する技術動向

#### ア 映画・ビデオ

DVD Forum<sup>116</sup>は、1996年から、発売される全てのDVDについてCSS(コンテンツ・スクランブル・システム)<sup>117</sup>を利用することを推奨しており、現在も改良版のCSSが利用されている。

AACS Licensing Administrator LLC<sup>118</sup>は、HD DVD、Blue-Ray ディスク等の次世代ビデオメディアのためのフォーマットとして、Advanced Access Content System(“AACS”)<sup>119</sup>を2005年に発表した。

Digital Video Broadcasting(DVB)<sup>120</sup>の合同技術委員会は、DVB-CPCM<sup>121</sup>を開発し、2007年及び2008年初めに実装された。

マイクロソフトのOSであるウィンドウズ・ビスタは、ビデオに関して、Protected Video Path(PVP)<sup>122</sup>を利用している。

<sup>115</sup> OLG München, 28. 7. 2005, 29 U 2887/05.

もっとも、問題となったオンラインの記事においては、迂回装置等(ソフトウェア)が提供されているウェブサイトへのハイパーリンクが貼られており、さらに当該迂回装置等の使用方法を説明していたので、最終的には違法とされた(現地報告書(EU編)48頁)。

<sup>116</sup> ハードウェアメーカ、コンピュータプログラム会社、コンテンツ・プロバイダーその他のDVD及びHD DVDの利用者の主要な業界代表者。

<sup>117</sup> CSSについては、現地報告書(EU編)50頁。

<sup>118</sup> AACS Licensing Administrator LLCは、主要なコンテンツ・プロバイダー(ディズニー、IBM、インテル、マイクロソフト、パナソニック、ソニー、東芝及びワーナーブラザーズ)によるジョイント・ベンチャーである。

<sup>119</sup> AACSについては、現地報告書(EU編)50頁。

<sup>120</sup> DVBについては、現地報告書(EU編)50頁。

<sup>121</sup> DVB-CPCMについては、現地報告書(EU編)50頁。

<sup>122</sup> PVPについては、現地報告書(EU編)51頁。



## イ 音楽

大手音楽会社は、アクセスコントロール及びコピーコントロールを用いた技術的手段から、電子透かしを用いる方法に切り替える動きにある。また、2007年には、大手は、インターネットによる音楽のダウンロード販売において、デジタル著作権管理技術を用いずに、クリップラップライセンス、又は、クリックスルーライセンスを用いることを発表した。一方、2009年1月21日、マイクロソフトは、MSN Mobile Music サービスをデジタル著作権管理技術で行うことを発表した<sup>123</sup>。

## ウ コンピューター・ゲーム

コンピューター・ゲームにはデジタル著作権管理技術が用いられている。例えば、違法に複製をすると、当初はゲームをすることができるものの、次第にゲームができなくなるFADEシステム<sup>124</sup>というデジタル著作権管理技術が存在する。

また、SecuROM システムというコピープロテクト技術が存在するが、このシステムは2008年にアメリカの消費者からSporeというゲームソフトをインストールすることができる回数を制限していたことを理由にクラスアクションによる訴訟を提起された。

## エ コンピューター・プログラム

コンピューター・プログラムは、以下の5つの方法により保護されている。

まず、暗号鍵を用いる方法である。この方法は、暗号技術を用いてコピーされることを防ぐ方法である。

次に、バス暗号化及び暗号化されたコードを用いる方法がある。この方法は非常に高いセキュリティが求められる場合に用いられる方法である。

そして、反海賊版用の外付けハードウェアを用いる方法がある。この方法は、反海賊用の外付けハードウェアを用いて、各コンピューター・プログラムにシリアルナンバーを持たせる方法である<sup>125</sup>。

さらに、エンド・ユーザーが利用する前に、正規のエンド・ユーザーであることを確認する方法が用いられている。

最後に、コードにスクランブルをかけ、または、コードを難読化することにより、デジタル著作権管理技術に準拠した装置のみにより複製等を可能とする方法が用いられている。

---

<sup>123</sup> 具体的な著作権管理技術の内容については、現地報告書(EU編)51頁。

<sup>124</sup> FADEシステムについては、現地報告書(EU編)52頁。

<sup>125</sup> この方法ではハードウェアを製造するには費用がかかるため、一般的には、貴重な、また、専門的なコンピューター・プログラムに対してのみ用いられる。

## オ 電子書籍

電子書籍については、デジタル著作権管理技術により、ダウンロード回数、コピー、印刷を制限するのが一般的である。

### (2) 電子透かし等、コンテンツの技術的手段に関する新たな技術

#### ア 映画・ビデオ

近年、デジタルからアナログに変換された後に、再びデジタルに変換することを阻止する技術が出てきている。この技術により、いわゆるアナログホール問題は、徐々に解決されてきている。

#### イ 音楽

上記映画・ビデオと同様、アナログ変換された後に、再びデジタルに変換することを阻止する技術が出てきている。

また、Spotify は、2009 年 10 月に、近いうちに定期的な音楽ダウンロードサービスを提供すると発表した。そして、同社のスポークスパーソンによれば、ダウンロードした音楽データは、そのダウンロードを行った装置でのみ再生することができるということである。

#### ウ 電子書籍

ドイツでは、電子書籍の出版社は、電子透かしを用いる傾向にある。電子透かしを用いることにより、著者情報はデジタル製品に直接結びつき、これと同時に、権限を与えられたユーザーは文書に登録される。また、Adobe は、絵の中に電子透かしを入れる技術を提案している。

### (3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況

EU 各国では、現在使用されているか否かにかかわらず、技術中立的に回避技術を規制対象としている。そして、実際、技術的手段に対する法的保護については、一般的には著作権者は満足しているようである。しかしながら、コンテンツの保護が成功するか否かは、法律的なコンテンツの保護の強さよりも、技術的なコンテンツの法的保護の強さによるとの見解が広まってきている。また、著作権者の力が拡大し過ぎることを懸念する声も聞かれる。

アナログホールの問題に対しては、EU では立法による対処はなされていない。なぜなら、アナログホールの問題については、法律よりも技術によって対処した方がよいと一般的に考えられているからである。その具体例が電子透かしであり、電子透かしを利用すれば、コンテンツがアナログコピーされた後であってもモニタリングが可能である。

## 5. 各国内の議論<sup>126</sup>(規制に対する賛否・改正動向等)

### (1) コンテンツの技術的手段に関する現行規制に対する議論

#### ア フランス

フランスでは、技術的手段が互換性を妨げるのではないかという点について、大きな問題提起がなされている。そうした背景もあり、著作権指令を国内実施する際には、技術的手段により互換性が損なわれることのないように多くの規定が盛り込まれることとなった。

#### イ イギリス

技術的手段についての規制が、コンテンツ権利者の保護に傾き過ぎているとの指摘が消費者から出されている。

また、消費者団体から、技術的手段についての規制が、互換性を妨げており、消費者の利益を損なうとともに、イノベーションを妨げているとの指摘がなされている。さらに、言論界においては、技術的手段についての規制が、反競争的行為を助長しているとの指摘も存在する<sup>127</sup>。

図書館の代表者からは、技術的手段についての規制により、図書館に認められた広範な著作権の制限の行使が妨げられていると述べている。

#### ウ ドイツ

ドイツ海賊党(the German Pirate Party)は、技術的手段は、芸術へのアクセスが人為的に制限しており、また、著作物の正当な利用を妨げていると述べている。

### (2) コンテンツの技術的手段に関する規制に対する業界からの要望状況

#### ア フランス

2007年の「Olivennes 合意」に基づき、音楽業界は、互換性を妨げている技術的手段の利用を止める方向にある。最終的には、2009年1月にアップル社も互換性のないファイルの使用を止めた。ただし、ARMTは、技術的手段について全面的に放棄されるべきではなく、もっと効率的で、互換性があり、透明で柔軟なデジタル権利の保護の方法への発展途上にあると述べている。

映画界は、音楽界とは異なり、互換性については大きな問題となっていないことも

<sup>126</sup> 現地報告書(EU編)55～67頁。

<sup>127</sup> 当初、アップル社のダウンロード音源は、EUの他の地域に比して10%程度高く、地域制限をする技術的手段によってこれが維持されていたところ、2004年にイギリス競争当局から問題を指摘された。2008年1月には、EC委員会により、アップル社は、イギリスにおける値段を下げることとなるとの発表がなされた。(現地報告書(EU編)57頁)

あり、現状の技術的手段を支持する姿勢を崩していない。ただし、複数の事業者によるオン・デマンドサービスが提供なされるに至って、互換性の問題が浮上している。

出版業界は、Eブックの頒布にあたり、著作権侵害を恐れて技術的手段を利用しているが、サービスの提供者間の対話が十分ではなく、互換性の問題が生じている。この問題については政府の関係機関にも報告がなされ、現在ワーキンググループがこの問題についての検討を進めている。

テレビゲーム業界は、長く技術的手段を利用している。ハードコピーについてはコピー・コントロールを利用し、オンラインゲームについてはアクセスコントロールを利用している。このことを、大半の消費者は仕方がないこととして受け入れているように思われる。

## イ イギリス

産業界は、技術的手段を非常に支持している。しかしながら、技術的手段の利用について、批判が強まるにつれ、互換性を損なわず、ユーザーの適正な利用を妨げない、より洗練された技術が必要なのではないかとの認識が広まりつつある。

音楽業界においては、サービスの提供者は、ユーザーにコピーを許容する方が、ビジネス上得策であるとの考えを持つようになっている。

映画業界は、技術的手段の利用を続けることが、非常に重要であるとの考えを変えていない。

なお、消費者について、あまりに著作権法に疎く、何を買っているのかについての認識をもっと有するべきである(著作権侵害についてきちんと認識をすべきである)との問題提起がなされており、消費者の認識を向上させる観点から、製品に適当なラベリングをすることについて検討が進められている。

## ウ ドイツ

ドイツの業界団体の代表は、著作権侵害に対しては、警告のメールを送付することで対応すべきであり、また、著作権に関する国際機関が海外における違法ダウンロードの問題に対してより適切に行動をすべきであるとの考えを示した。

### (3) 法改正の動向・内容

#### ア フランス

法改正の動向は、現状見あたらない。

## イ イギリス

「Digital Britain レポート(2009 年版)」においては、ファイル共有や P2P といった違法な経路でデジタルコンテンツにアクセスするユーザーを大幅に減らすことが掲げられた。これを受ける形で、2010 年 4 月の施行を目指して、Digital Economy 法案が提出された。当該法案では、①権利者が継続的に著作権を侵害する者の IP アドレスを把握し、これを ISP に伝え、ISP から当該侵害者に警告を送付すること、②もし、警告が無視された場合には、権利者は、法的措置をとるために裁判所の命令により侵害者のリストを ISP から入手できること等が提案されている。

そして、かかる法律が施行されてから 12 ヶ月以内に、違法なファイルの共有行為を 70%以上減らすことができない場合には、侵害者がインターネットに接続できないようにする技術的手段の導入が新たに規定されることとなる可能性がある。

当該法案は、2010 年の選挙の前に十分に審議されることとなるかにつき疑問はあるが、野党である保守党も一般論として当該法案を支持している。

## ウ ドイツ

法改正の動向は、現状見あたらない。

以 上

(参考訳文(抄訳))

別紙 1

自由貿易協定・経済連携協定

I. ヨーロッパ指令の関連条項

A. コンピュータ・プログラム指令

第 5 条 制限行為の例外

1. ～2. (略)
3. コンピュータ・プログラムのコピーを使用する権利を有する者は、この者が権利を有するプログラムのローディング、表示、稼働、送信または保存するという行為のいずれかを行っている間は、権利者の許諾なく、プログラムのいずれかの要素の基礎となっているアイデアと原理を知るためにプログラムの機能を観察、研究または試験する権利を有する。

第 6 条 逆コンパイル

1. 第 4 条(1)の第(a)および(b)号で意味する範囲内でのコードの複製およびその形態の変換が、独立して創られたコンピュータ・プログラムと他のプログラムとの互換性を達成するために必要な情報を取得するために必要不可欠な場合には、権利者の許諾を必要としてはならない。ただし、次の条件を満たすことを条件とする。
  - (a) これらの行為がライセンシーもしくはプログラムのコピーを使用する権利を有する他の者またはこれらの者の代わりにそうすることを許諾された者によって実行されること。
  - (b) 互換性を達成するために必要な情報が、第(a)号に定める者にとって今まで容易に入手できるものではないこと。
  - (c) これらの行為が互換性を達成するために必要な元のプログラムの部分に限定して行われること。
2. ～3. (略)

## 第7条 保護の特別手段

1. 第4、5および6条の規定を害することなく、加盟国は、その国内法に従い、次のいずれかの行為を行う者に対する適切な救済措置について定める。

(a)～(b) (略)

(c) コンピュータ・プログラムを保護するために適用されている技術的手段を許諾なく除去することまたは回避することを容易にすることを唯一の目的としたあらゆる手段を、流通に置くすべての行為または商業目的で所持する行為。

2. (略)

3. 加盟国は、第1項第(c)号に定めるすべての手段の差押えについて定めることができる。

**B. データベース指令 (略)**

**C. 条件付きアクセス指令 (略)**

**D. 著作権指令**

前文

(47)

技術の発展は、著作権、著作権に関連する権利またはデータベースの独自の (sui generis) 権利の権利保有者が許諾していない行為を防止しまたは制限するために意図された技術的手段を、権利者が使用できるようにするだろう。しかし、これらの手段によってもたらされる技術的保護の回避を可能にし、または容易にするために違法な活動が行われる危険が存在する。域内市場が機能することを潜在的に妨げることのある断片的な法的アプローチを避けるためには、効果のある技術的手段の回避およびそのような趣旨の装置、生産品またはサービスの提供に対する調和のとれた法的保護を規定する必要がある。

(48)

そのような法的保護は、電器装置の通常の働きおよびその技術的発展を妨げることなく、著作権、著作権に関連する権利またはデータベースの sui generis 権の権利保有者が許諾していない行為を効果的に制限する技術的手段に関して規定されるべきである。そのような法的保護は、装置、生産品、構成品またはサービスが第6条の禁止に該当しない限り、そのような装置、生産品、構成品またはサービスを技術的手段に対応するように設計する義務を意味しない。そのような法的保護は、均衡を尊重し、技術的保護を回避するため以外の商業的に重要な目的または用途を持つ装置または活

動を禁じてはならない。特に、この保護は、暗号化の研究を妨げてはならない。

(50)

そのような調和のとれた法的保護は、指令 91/250/EEC が規定する保護の特定の条項に影響を及ぼさない。特に、それは同指令が専属的に対象としているコンピューター・プログラムに関して用いられる技術的手段の保護に適用してはならない。それは、指令 91/250/EEC 第 5 条第 3 項または第 6 条の条件に従って行われる行為を可能とするために必要な技術的手段を回避するいかなる方法の開発または使用を抑止しまたは禁止するものであってはならない。同指令第 5 条および第 6 条は、もっぱらコンピューター・プログラムに適用される排他的権利の例外を定めている。

(例外および制限)

#### 第 5 条

- 1 過渡的または付随的で、技術的プロセスの不可欠で主要な部分であり、かつ、著作物その他の目的物に行われる以下のことを可能にすることを唯一の目的とする第 2 条に掲げる一時的複製行為で、独自の経済的重要性を持たないものは、第 2 条に規定する複製権から免除されるものとする。
  - (a) 仲介者による第三者間のネットワークにおける送信、または、
  - (b) 適法な使用
- 2 加盟国は、次の場合に、第 2 条に規定する複製権に、例外または制限を規定することができる。
  - (a) なんらかの種類の写真技術の使用またはその他の類似の効果をもつ行程により行われる紙または同様の媒体への複製に関する場合。ただし、シートミュージックは例外とし、権利者が正当な対価を受けることを条件とする。
  - (b) 第 6 条に掲げる著作物その他の対象に対する技術的手段の適用または不適用を勘案して権利者が公正な補償を受けることを条件として、私的使用のために、および直接にも間接にも商業的でない目的のために、自然人により行われるいずれかの媒体への複製に関する場合
  - (c) 公衆がアクセスできる図書館、教育的施設もしくは博物館により、または記録保存所により行われ、直接にも間接にも経済的または商業的利益のためでない、特定の複製行為に関する場合
  - (d) 放送機関が自己の施設により、自己の放送のために行う著作物の一時的記録に関する場合。これらの記録物の公的記録保存所における保存は、その記録が資料として特別の性質を有することを理由として認められる。
  - (e) 権利者が公正な補償を受けることを条件として、病院または刑務所のような非商業目的で営む社会施設により行われる放送の複製に関する場合
- 3 加盟国は、次の場合に、第 2 条および第 3 条に規定する権利に、例外または制限を



規定することができる。

- (a) 不可能であることが明らかでない限り著作者の氏名を含む出所が明示されることを条件として、かつ非商業的目的を達成することにより正当化される範囲において、もっぱら授業または学術研究のための説明を目的とする利用。
- (b) 特定の障害により要求される限度において、直接障害に関係し、かつ、非商業的性質を持つ障害者の利益のための利用
- (c) 利用が明示的に留保されておらず、著作者の氏名を含む出所が明示される限り、時事の経済、政治または宗教の話題に関する発行された記事または同様の性質の放送された著作物その他の対象の報道機関による複製、公衆への伝達または利用可能化、および報道目的により正当化される範囲において、かつ、不可能であることが明らかでない限り著作者の氏名を含む出所が明示されることを条件として、時事の事件の報道に関する著作物その他の対象の利用
- (d) 批評または論評等のための引用。ただし、すでに適法に公衆に利用可能にされている著作物その他の対象に関するものであり、また、不可能であることが明らかでない限り著作者の氏名を含む出所が明示され、およびその利用が公正な慣行に合致し、かつ特定の目的により要求される範囲であることを条件とする。
- (e) 公共の安全のための、または行政、立法もしくは司法手続の適当な行為もしくは報告を保証するための利用
- (f) 報道目的により正当化される範囲において、かつ、不可能であることが明らかでない限り著作者の氏名を含む出所が明示されることを条件として、政治的演説の、および公の講演または同様の著作物もしくは対象の抜粋の利用
- (g) 公共機関が開催する宗教儀式または公的祝典の間の利用
- (h) 公の場所に恒常的に設置するために作成された建築または彫刻の著作物の利用
- (i) 著作物その他の対象が付随的に他の素材へ包含される場合
- (j) 芸術作品の一般公開または販売を広告する目的で利用される場合。ただし、そのイベントを宣伝するために必要とされる限度においてなされることとし、他の商業的利用を除く。
- (k) カリカチュア、パロディまたはパスティシュのための利用
- (l) 設備の実演または修繕に係る利用
- (m) 建築物を再建築するための建築物の形式の美術の著作物または図面もしくは設計図の利用
- (n) 第 2 項 (c) に掲げる施設の構内に設置された端末により、研究または私的学習のために個々の公衆のそれぞれに、施設の収集物に含まれる購入または許諾の条件の対象でない著作物その他の対象を伝達または利用可能化する利用
- (o) 重要でない一定のその他の例外または制限がすでに国内法に存在する場合の利用。ただし、この条に包含される他の例外または制限を害することなく、それらがアナログの利用のみに関係し、また、域内市場における商品およびサービスの

自由な流通に影響を及ぼさないことを条件とする。

- 4 加盟国が第 2 項および第 3 項に従って複製権の例外または制限を規定する場合には、権限を与えられた複製行為のために正当化される範囲で、同様に第 4 条に掲げる頒布権の例外または制限を規定することができる。
- 5 第 1 項、第 2 項、第 3 項および第 4 項に規定する例外または制限は、著作物その他の対象の通常の利用を妨げず、かつ権利者の正当な利益を不当に害しない特定の特別な場合にのみ適用されなければならない。

(技術的手段に関する義務)

#### 第 6 条

- 1 加盟国は、関係する者が、その目的のためであることを知り、または知るべき合理的な理由を有しながら行う、効果的な技術的手段の回避に対して、適切な法的保護を与えるものとする。
- 2 加盟国は、次のものの製造、輸入、頒布、販売、貸与、販売もしくは貸与のための宣伝、または装置、製品もしくは部品の商業目的の所持に対して、適切な法的保護を与えるものとする。
  - (a) 効果的な技術的手段の回避を目的として宣伝され、広告され、もしくは市販されたもの
  - (b) 効果的な技術的手段の回避の他には、限られた商業上の重大な目的もしくは利用方法しか存在しないもの
  - (c) 専ら効果的な技術的手段の回避を可能にし、もしくは容易にする目的で設計、製造、適合、もしくは実行されるもの
- 3 本指令の適用上、「技術的手段」とは、法律に規定された著作権もしくは著作権に関連する権利、または指令 96/9/EC 第 3 章に規定された sui generis 権の権利者により権限を与えられていない、著作物その他の対象に関する行為を、その通常のプロセスにおいて防止または禁止するよう意図されたいずれかの技術、装置または部品を意味する。技術的手段は、アクセス・コントロールや暗号化、スクランブル掛けその他の保護の目的を達成する著作物その他の対象の変形といった保護過程またはコピー・コントロールの適用によって、保護のある著作物その他の対象の利用が権利者により制御される場合は、「効果がある」とみなされる。
- 4 第 1 項に規定する法的保護にかかわらず、権利者とその他の関係者との間の合意を含む、権利者がとる任意の手段がないときは、加盟国は、第 5 条第 2 項 (a)、第 2 項 (c)、第 2 項 (d)、第 2 項 (e)、第 3 項 (a)、第 3 項 (b) または第 3 項 (e) に従い国内法に規定される例外または制限の受益者に、その例外または制限から利益を受けるのに必要な範囲で、かつ、その受益者が保護のある著作物その他の対象に適法にアクセスできる場合に、その例外または制限から利益を受ける方法を権利者が提供することを保証する適当な手段をとらなければならない。

加盟国はまた、私的使用のための複製がすでに権利者により可能にされていない場合は、関係する例外または制限から利益を受けるのに必要な範囲で、かつ、第 5 条第 2 項 (b) および第 5 項の規定に従って、権利者がこれらの条項に従い複製の数に関する適正な手段を採用することを妨げることなく、第 5 条第 2 項 (b) に従い規定される例外または制限の受益者に関して、そのような手段をとることができる。

任意の合意の実施において適用されるものを含む、権利者により任意に適用される技術的手段、および加盟国によりとられる手段の実施に際して適用される技術的手段は、第 1 項に規定する法的保護を享有するものとする。

第 1 段および第 2 段の規定は、公衆のそれぞれが個別的に選択する場所および時期においてアクセスできるように合意された契約条件に基づき、公衆に利用可能にされる著作物その他の対象には適用されない。

この条が指令 92/100/EEC および 96/9/EC の関係で適用されるときは、この項を準用するものとする。

(制裁および救済)

#### 第 8 条

- 1 加盟国は、本指令に定める権利の侵害および義務の違反に関して、適当な制裁および救済を規定し、それらの制裁および救済が適用されることを保証するために必要なあらゆる手段をとるものとする。このように規定される制裁は、有効であり、比例的であり、かつ抑止力のあるものでなければならない。
- 2 各加盟国は、その領土において行われる侵害行為によって利益が害される権利者が、損害賠償もしくは差止めまたはその双方、ならびに適当な場合は、侵害物品および第 6 条第 2 項に掲げる装置、製品または部品の差押えを求める訴訟を提起できることを保証するために必要な手段をとるものとする。
- 3 加盟国は、そのサービスが第三者により著作権または著作権に関連する権利を侵害する形で利用される仲介者に対して、権利者が差止めを求める地位にあることを保証しなければならない。

## II. EU—韓国間の審理中の FTA 関連条項

注：以下は、交渉完了後のテキストを記載するものであり、国際法上の問題として拘束力を有するものではない。正式なテキストは、必要な承認手続きが完了次第、EU 官報に掲載される予定である。

#### 第 10.12 条 技術的手段の保護

1. 各締約国は、関係するものが、その目的のためであることを知り、または知るべき正当な理由を有する者により行われる、効果的な技術的手段の回避に対し、適切な法的保護を規定するものとする。
2. 各締約国は、以下の装置、製品または部品の、製造、輸入、頒布、販売、貸与、販売もしくは貸与目的の広告、商業目的の所持、あるいはそのようなサービスの提供行為に対する適切な法的保護を規定するものとする。

効果的な技術的手段につき、

- (a) [効果的な技術的手段の]回避を目的として宣伝され、広告され、もしくは市販されるもの、または
  - (b) [効果的な技術的手段の]回避のほか、限られた商業的に重大な目的もしくは利用方法しか存在しないもの、または
  - (c) 主として[効果的な技術的手段の]回避を可能にし、もしくは容易にする目的で設計され、製造され、適合され、もしくは実行されるもの。
3. 本協定の解釈上、技術的手段とは、その通常の使用過程において、著作物もしくは他の対象に関して、各締約国の立法により規定された著作権もしくは著作権に関連する権利の権利者により許諾されていない行為を防止し、または制限するよう設計された技術、装置もしくは部品を意味する。技術的手段は、保護された著作物もしくは他の目的物が、暗号化、スクランブルその他著作物もしくは他の目的物の変換といったアクセス・コントロールもしくはプロテクション・プロセス、または、保護の目的を達成するコピー・コントロール・メカニズムの適用を通じて、権利者により管理される場合に「効果的」とであるとみなされるものとする。
  4. 各締約国は、自国の立法および第 10.5 条に規定される関連する国際協定に従って、第 1 項および第 2 項を実施する措置に対する例外および制限を規定することができる。

#### 第 10.13 条 権利管理情報の保護 (略)

## 別紙 2 フランス法

注：以下は、2010年1月1日現在で施行されているフランス知的所有権法典の関連規定を定めるものである。

### Ⅲ 一般規定

#### A 技術的手段

##### L 第 331 の 5 条

- 1 コンピュータ・プログラム以外の著作物の著作権者、もしくは実演、レコード、ビデオプログラムまたは番組の著作権に関連する権利者により許諾されていない利用を防止し、または制限するために設計された効果的な技術的手段は、本法典の規定に従って保護される。
- 2 第 1 項に規定される技術的手段とは、意図されたとおりに利用される場合に本項に規定される機能を果たす技術、装置または部品をいう。これら技術的手段は、同項に基づく利用が、かかる保護目的を達成する、アクセス・コードの適用、暗号化、スクランブルその他保護対象の変換といった保護過程の適用により、または、コピー・コントロール・メカニズムにより権利者によって管理される場合に、効果的であるとみなされる。
- 3 プロトコル、フォーマットまたは暗号化、スクランブルもしくは変換の方式は、それ自体としては、本条に規定される技術的手段を構成しない。
- 4 技術的手段は、著作権を尊重しつつも、互換性の効果的な実施を妨げてはならない。技術的手段の提供者は、L 第 331 の 31 条および L 第 331 の 32 条の規定に従って、互換性に不可欠な情報へのアクセスを提供する。
- 5 本節の規定は、伝達の自由に関する 1986 年 9 月 30 日の法律第 86-1067 号第 79 の 1 条から第 79 の 6 条および第 95 条に規定される法的保護を害するものではない。
- 6 技術的手段は、本法典に規定され、また権利者により与えられる権利の限度内における著作物または保護対象の適法な利用を妨げることはできない。

7 本条の規定は、本法典L第122の6の1条の規定を害することなく、適用される。

#### L第331の6条

私的複製のための例外およびL第331の31条2項において規定される例外の特権は、L第331の7条からL第331の10条、L第331の33条からL第331の35条およびL第331の37条の規定により保証される。

#### L第331の7条

- 1 L第331の5条に定められる技術的手段を利用する権利者は、複製物の部数を制限するためにそれらを利用することができる。ただし、かかる権利者は、それらの手段の利用が、L第331の31条2項に規定される例外の受益者からそれらの例外を有効に行使する権利を奪わないよう有用な措置をとる。かかる権利者は、消費者の公認団体および他の利害関係者とともに、こうした手段を決定するため最善の努力を払うものとする。
- 2 本条の規定は、技術がそれを可能とする限度において、これら例外の効果的な利益を著作物、レコード、ビデオグラムまたは番組への適法なアクセスに従わせることができ、かつ、その通常の利用を害し、または著作物もしくは保護対象の権利者の適法な利益に不当な損害を与えないことを保証することができる。

#### L第331の8条

著作物または著作権に関連する権利による他の保護対象が、当事者間で合意される契約条項に従って、各人が選択する場所から、および各人が選択する時にアクセスすることができるように公衆の利用に供される場合には、権利者は、L第331の7条の規定を採用する義務を負わない。

#### L第331の10条

著作物、ビデオグラム、番組またはレコードの読取りへのアクセス条件、および技術的保護手段の実行によってL第122の5条2項およびL第211の3条2項に規定される私的複製のための例外に加えられうる制限は、利用者に知らされなければならない。

**B 権利管理情報(略)**

**C データベース(略)**

**D コンピュータ・プログラム**

L 第 122 の 6 の 2 条

コンピュータ・プログラムを保護する技術的装置を除去もしくは回避する手段に関する広告または使用説明書には、かかる手段の違法利用には侵害の場合について規定されている制裁が課される旨を記載するものとする。

R 第 335 の 2 条

コンピュータ・プログラムを保護する技術的装置を除去もしくは回避する手段に関する広告または使用説明書に、かかる手段の違法利用には侵害の場合について規定されている制裁が課される旨の表示が明示的に付されていない場合、第 3 級の軽罪について規定されている制裁を課すものとする。

**IV 回避に関する規定**

**A コンピュータ・プログラム以外の著作物について**

L 第 335 の 3 の 1 条

- I コード解読、暗号解読、その他プロテクションもしくはコントロールのメカニズムを回避し、無効にし、または除去することを目的とする個人的介入によって著作物の保護を改変するために、L 第 331 の 5 条に定められる効果的な技術的手段に対して、研究以外の目的で、それと知りながら損ねる行為は、II に規定される既存の技術応用、装置または部品の利用以外の手段によって実現される場合には、3,750 ユーロの罰金に処せられる。
- II 以下に掲げる方法のいずれかにより効果的な技術的手段を回避する目的で設計され、もしくは特別に適合された手段を、他の者に対し、直接もしくは間接に、それと知りながら提供し、または提案する行為は、6 ヶ月の禁固および 30,000 ユーロの罰金に処せられる。
- (1) 技術応用、装置もしくは部品を、研究以外の目的で、製造し、または輸入すること。
  - (2) 技術応用、装置もしくは部品を、販売、貸与もしくは賃貸のために保持し、それと同

一の目的のために提供し、またはなんらかの形式で公衆に提供すること。

- (3) この目的のために役務を提供すること。
- (4) 前記に掲げる方式のいずれかの利用を誘引し、またはそのための宣伝を委託し、構想し、組織し、複製し、頒布し、もしくは普及すること。

Ⅲ これらの規定は、本法典に規定される権利の限度内において、コンピュータ・セキュリティの目的のために実行される行為については適用されない。

#### R 第 335 の 3 条

1. 以下に掲げる行為には、第 4 級の軽罪について規定されている罰金が課される。
  - (1) 著作物、実演、レコード、ビデオグラム、番組もしくはデータベースを保護する本法典 L 第 331 の 5 条にいう効果的な技術的手段を損ねる目的で設計され、もしくは特別に適合された技術応用、装置もしくは部品の個人利用目的の保持または利用
  - (2) 前号にいう効果的な技術的手段に損害を与える目的で設計され、または特に適合された役務の利用
- 2 これらの規定は、権利者に損害を与える行為およびコンピュータ・セキュリティーまたは暗号化の科学的研究の目的で実行される行為については適用されない。

#### **B コンピュータ・プログラムについて**

前記 L 第 122 の 6 の 2 条を参照のこと。

#### **V 技術的手段の適用制限規定**

#### **A HADOPI に関する規定ならびに/または著作権および著作権に関連する権利の例外規定**

#### L 第 331 の 13 条

1. 最高機関は、以下の責任を負う。
  - (1)～(2) (略)
  - (3) 著作権または著作権に関連する権利により保護される著作物および保護対象の技術的保護手段および識別の分野を規制し、監視する任務



## L 第 331 の 31 条

- 1 著作権または著作権に関連する権利により保護される著作物および保護対象の技術的保護手段および識別の分野を規制し、監視する任務に関連して、最高機関は、以下の職務を執行する。
  - (1) 同機関は、L 第 331 の 5 条に規定される技術的手段が、相互の不適合または互換性の不能により、コンピュータ・プログラム以外の著作物の著作権者または実演、レコード、ビデオグラムまたは番組の著作権に関連する権利者により明示的に許可された制限とは別に、著作物の利用に対して追加的および独立的な制限を課す結果とならないことを保証する。
- 2 同機関は、技術的保護手段の実施が、以下において定められる例外の利益を受益者から奪う結果とならないことを保証する。
  - (1) 本法典 L 第 122 の 5 条 2 項、3 項(e)、7 項および 8 項(2009 年 1 月 1 日現在)
  - (2) 本法典 L 第 211 の 3 条 2 項、3 項最終号、6 項および 7 項(2009 年 1 月 1 日現在)
  - (3) 本法典 L 第 342 の 3 条 3 項および 4 項(2009 年 1 月 1 日現在)
  - (4) 本法典 L 第 331 の 4 条(2009 年 1 月 1 日現在)
- 3 同機関は、技術的保護手段の実施が、文化遺産法典 L 第 132 の 4 条 2 項、L 第 132 の 5 条および L 第 132 の 6 条に規定される収集、保全および現地協議を目的とする複製の例外の利益を受益者から奪う結果とならないことを保証する。
- 4 (略)

## L 第 331 の 33 条

L 第 331 の 31 条 2 項に規定される例外の受益者またはかかる個人を代表する認可法人は、最高機関に対して、L 第 331 の 8 条に定められる技術的手段により生じるかかる例外の実行についての制限に関する紛争についての請求を申し立てることができる。

## **B 互換性および/または他のコンピュータ・プログラムにのみ適用される例外に関する規定**

### L 第 331 の 32 条

- 1 コンピュータ・プログラムの発行者、技術的システムの製作者およびサービス・オペレーターは、互換性に不可欠な情報へのアクセスが拒否された場合、最高機関に対し、当事者の権利を尊重しつつ、既存のシステムおよびサービスの互換性を保証する

こと、ならびに互換性に不可欠な情報を技術的手段に関する権利者から受領することを要求することができる。同機関は、この申立から 2 ヶ月の期間内にその決定を行う。

2～3 (略)

4 同機関は、当事者が提案する約束であって、互換性に反する慣行を終らせることができる性質のものを受諾することができる。当事者間に合意がない場合には、同機関は、利害関係者がその意見を述べるようにした後に、請求の却下の理由を付した決定を行い、または請求者が互換性に不可欠な情報にアクセスすることができる条件、技術的手段の効率性および完全性を保証するために請求者が尊重しなければならない約束、ならびにアクセスおよび保護内容の利用の条件を、必要の場合には制裁を課すことも併せて、規定する差止命令を発する。同機関が言い渡した処罰は、同機関によって確定される。

5 同機関は、その差止命令の不履行の場合、または同機関が受諾した約束の不履行の場合に、金銭的制裁を命じる権限を有する。各金銭的制裁は、利害関係者が被った損害の重大性、金銭的制裁を受ける団体または企業の状況、および互換性に反する慣行の反復に比例する。各制裁は、個別に、かつ理由を付して決定される。その最高額は、法人の場合には互換性に反する慣行が実施されていた会計年度の前年度に生じた最高の税外世界売上げ額の 5% とし、その他の場合には 1,500,000 ユーロとする。

6～7 (略)

## **VI 救済手段に関する規定**

### **A 証拠手段**

#### L 第 332 の 1 条

1 警視および警視がない場合には簡易裁判所判事は、本法第 1 編によって保護される著作権のある著作物の著作者、権利者、権利譲受人または権利承継人の求めに応じて、その著作物の違法な複製を構成する複製物または L 第 331 の 5 条および L 第 331 の 11 条のそれぞれに規定される技術的手段および情報を損ねる複製物、製品、器具、装置、部品もしくは手段を差し押さえる義務を負う。

2 差押えが、進行中のまたはすでに告知されている上演・演奏もしくは公の実演を延期させ、または中止させる結果となるような場合には、求めに応じて発せられる命令によって、第一審裁判所裁判長から特別の許諾を得なければならない。第一審裁判所裁判長は、また、同一の方法で、以下に掲げることを命じることができる。

- (1) 著作物を違法に複製し、またはL第331の5条およびL第331の11条のそれぞれに規定される技術的手段および情報を損ねるような進行中の製造を一時中止すること。
- (2) 著作物の違法な複製を構成する複製物であってすでに製造されたものもしくは製造中のもの、またはL第331の5条およびL第331の11条のそれぞれに規定される技術的手段および情報を損ねる製造され、もしくは製造中の複製物、製品、器具、装置、部品もしくは手段、生じた収益ならびに違法複製物を、日時を問わず差し押さえること。同裁判所は、また、関連文書と同様、著作物を製造し、または違法に頒布するために利用された用具および道具の実際の差押えを命じることができる。
- (3) 著作権を侵害するあらゆる手段により行われる創作性のある著作物の複製、上演・演奏または放送により生じ、またはL第331の5条およびL第331の11条のそれぞれに規定される技術的手段および情報を損ねることにより生じる収益を差し押さえること。
- (4)～(5) (略)

3 第一審裁判所裁判長は、同一の方法により、本法典第2編に定められる著作権に関連する権利者の求めに応じて、前記(1)から(5)までに規定される措置を命じることができる。

4 第一審裁判所裁判長は、前記の命令において、差押人があらかじめ保証を設定することを命じることができる。

## **B 刑事規定**

### **1. 一般規定**

L第335の3条 (略)

### **2. コンピュータ・プログラム以外の著作物**

L第335の3の1条 (前出参照)

L第335の4の1条

- I コード解読、暗号解読、その他プロテクションもしくはコントロールのメカニズムを回避し、無効にし、もしくは削除することを目的とする個人的介入により実演、レコード、ビデオグラムまたは番組の保護を改変するため、L第331の5条に規定される効果的な技術的手段に対し、研究以外の目的で、それと知りながら損ねる行為は、

下記Ⅱにいう既存の技術応用、装置または部品の利用以外の手段によって行われる場合には、3,750ユーロの罰金に処せられる。

- Ⅱ L 第 331 の 5 条に規定される効果的な技術的手段に対して損害を与えるために設計され、もしくは特別に適合された手段を、以下に掲げる方式のいずれかによって、直接的もしくは間接的に、それと知りながら他人に提供し、または提案する行為は、6 ヶ月の禁固および 30,000 ユーロの罰金に処せられる。
- (1) 技術応用、装置もしくは部品を、研究以外の目的で、製造し、または輸入すること。
  - (2) 技術応用、装置もしくは部品を、販売、貸与もしくは賃貸のために保持し、それと同一の目的のために提供し、またはなんらかの形式で公衆に提供すること。
  - (3) この目的のために役務を提供すること。
  - (4) 前記に掲げる方式のいずれかの利用を誘引し、またはそのための宣伝を委託し、構想し、組織し、複製し、頒布し、または普及させること。
- Ⅲ これらの規定は、本法典に規定される権利の限度内において、コンピュータ・セキュリティの目的のために実行される行為については、適用されない。

### 3. データベース

#### L 第 342 の 3 の 1 条

- 1 L 第 331 の 5 条に規定される効果的な技術的手段であって、L 第 342 の 1 条の適用を受けて製作者が許諾しなかったデータベースの利用を防止し、または制限するのに適しているものは、L 第 335 の 4 の 1 条に規定される保護を受ける。
- 2 第 1 項に規定される技術的保護手段を利用するデータベース製作者は、L 第 331 の 31 条 2 項、L 第 331 の 7 条から L 第 331 の 10 条、L 第 331 の 33 条から L 第 331 の 35 条および L 第 331 の 37 条に規定される条件に従って、それらの実行により L 第 342 の 3 条に定められる例外の受益者から有効な利益が奪われないよう適切な措置をとらなければならない。
- 3 L 第 342 の 3 条に定められる例外の利益を受ける能力に関する紛争であって、本条第 1 項に規定される技術的手段に関わるものは、L 第 331 の 12 条に規定される著作物の放送およびインターネット上の権利の保護のための最高機関に付託される。

### 別紙 3 イギリス法

#### 著作権、意匠および特許法 (CDPA)

#### 第 296 条：コンピュータ・プログラムに適用される技術的装置の回避<sup>151</sup>

- 1 本条は以下の場合に適用される。
  - (a) 技術的装置がコンピュータ・プログラムに適用され、かつ
  - (b) 侵害複製物を作成するために利用されることを知り、または知るべき理由を有する者 (A) が、
    - (i) 専ら技術的装置の無許諾の除去または回避を容易にすることを目的とする方法について、販売もしくは貸与のための製造、輸入、頒布、販売または貸与、販売もしくは貸与のための提供または陳列、販売もしくは貸与のための宣伝、または商業目的の所持を行う場合、または
    - (ii) 技術的装置の除去もしくは回避を可能にし、または補助することを目的とした情報を公表する場合。
- 2 著作権侵害について、以下の者は、A に対し著作権者と同様の権利を有する。
  - (a) 技術的装置が適用されているコンピュータ・プログラムについて、
    - (i) その複製物を公に発行する者、または
    - (ii) 公衆に伝達する者
  - (b) 著作権者またはその排他的被許諾者が (a) で規定されている者に当たらない場合は、その者
  - (c) コンピュータ・プログラムに適用された技術的装置の知的財産権者またはその排他的被許諾者
- 3 (略)
- 4 さらに、第 2 項に規定される者は、著作権者が侵害複製物に関して有するのと同様、コンピュータ・プログラムに適用されている技術的装置の無許諾の除去または回避を容易にするために利用する意図をもってある者が所有し、保管し、または管理する第 1 項に規定するいずれかの手段に関し、第 99 条または第 100 条（特定の物品の引渡しおよび押収）に基づく権利を有する。

<sup>151</sup> 規則 2003 年第 2498 号 (SI 2003/2498) 規則第 3 条、第 24 条 (1) により置換。施行日：2003 年 10 月 31 日。規則 2003 年第 2498 号 (SI 2003/2498) 規則第 1 条参照。保留規定および暫定規定については同規則第 30 条から第 40 条参照。

5 (略)

6 本条におけるコンピュータ・プログラムに関する技術的装置についての言及は、そのコンピュータ・プログラムの著作権者により許諾されていない行為かつ著作権により制限されている行為を防止し、または制限することを目的とする装置についてのものである。

7～8 (略)

#### 第 296ZA 条：技術的手段の回避

1 本条は以下の場合に適用される。

- (a) 効果的な技術的手段がコンピュータ・プログラム以外の著作物に適用され、かつ
- (b) ある者(B)が、自らがその目的を達成しようとしていることを知りながら、または知るべき合理的な理由を有しながら、かかる手段を回避する行為を行う場合。

2 本条は、ある者が暗号化研究目的で効果的な技術的手段を回避する行為を行う場合は適用されない。ただし、回避行為を行う場合に、またはその研究から得られた情報を公表する場合に、その者が著作権者の権利に不利益な影響を与える場合は、この限りではない。

3 著作権侵害について、以下の者は、B に対し著作権者と同様の権利を有する。

- (a) 効果的な技術的手段が適用されている著作物について、
  - (i) その複製物を公に発行する者、または
  - (ii) 公衆に伝達する者
- (b) 著作権者またはその排他的被許諾者が(a)で規定されている者に当たらない場合は、その者

4～5 (略)

6 第 1 項から第 4 項、第 5 項(b)およびこれら項の目的のために効力を有する本法の他の規定は、必要な適合の上、興行権、出版権およびデータベース権に適用される。

7 (略)

#### 第 296ZB 条：技術的手段の回避のために設計された装置および役務<sup>152</sup>

1 ある者が以下の行為を行った場合は罪となる。専ら効果的な技術的手段の回避を可能にし、もしくは容易にする目的で設計され、製造され、もしくは適合された装置、製品または部品を、

- (a) 販売または貸与目的で製造し、
  - (b) 私的または家庭内での利用以外の目的で輸入し、
  - (c) 商業の過程で、
    - (i) 販売または貸与し、
    - (ii) 販売または貸与の目的で提供または陳列し、
    - (iii) 販売または貸与の目的で宣伝し、
    - (iv) 所持し、
    - (v) 頒布し、または、
  - (d) 商業以外の過程において、著作権者に不利益な影響を与える程度に頒布する行為。
- 2 ある者が以下の行為を行った場合は罪となる。効果的な技術的手段の回避を可能にし、または容易にすることを目的とするサービスについて、
- (a) 商業の過程で、または
  - (b) 商業以外の過程において、著作権者に不利益な影響を与えるほど、提供、促進、宣伝、または販売する行為。
- 3 第1項および第2項は、以下の目的のため、法執行機関もしくは情報機関により、またはそれらに代わってなされる行為を違法とはしない。
- (a) 国家安全保障の利益のため、または
  - (b) 犯罪の防止もしくは発見、犯罪捜査、または訴追の実行のため
- また、本項における「情報機関」とは、2000年調査権限規制法第81条において定められる意味を有する。
- 4 第1項および第2項に規定される罪につき有罪である者は、以下の罰を課される。
- (a) 略式手続きによる3ヶ月を超えない期間の禁固もしくは法定の最大金額を超えない額の罰金またはその両方
  - (b) 起訴による有罪判決による罰金もしくは2年を超えない期間の禁固またはその両方
- 5 被告人が以下の事実を知らなかった、または知るべき合理的な理由を有しなかったことを証明する場合は、本項に規定される罪の訴追に対する抗弁となる。
- (a) 装置、製品もしくは部品、または
  - (b) 役務が、
- 効果的な技術的手段の回避を可能にし、または容易にしたこと。

第 296ZC 条：技術的手段の回避のために設計された装置および役務：捜査令状および没収

- 1 第 297B 条(捜査令状)、第 297C 条(無許諾のデコーダーの没収：イングランドおよび

ウェールズまたは北アイルランド)および第 297D 条(無許諾のデコーダーの没収：スコットランド)の規定は、以下の修正の上、第 296ZB 条に規定される罪に適用される。

- 2 第 297B 条における第 297A 条 1 項に規定される罪についての言及は、第 296ZB 条 1 項または 2 項に規定される罪についての言及であると解釈されるものとする。
- 3 第 297C 条 2 項(a)および第 297D 条 15 項における第 297A 条 1 項に規定される罪についての言及は、第 296ZB 条 1 項に規定される罪についての言及であると解釈されるものとする。
- 4 第 297C 条および第 297D 条における無許諾のデコーダーについての言及は、効果的な技術的手段の回避を目的とする装置、製品もしくは部品についての言及であると解釈されるものとする。

#### 第 296ZD 条：技術的手段の回避のために設計された装置および役務に関する権利および救済

- 1 本条は以下の場合に適用される。
  - (a) 効果的な技術的手段がコンピュータ・プログラム以外の著作物に適用され、かつ、
  - (b) ある者(C)が、そうした手段の
    - (i) 回避のために宣伝、広告、または販売され、
    - (ii) 回避以外には限定的な商業上の重要な目的または利用方法のみを有し、または、
    - (iii) 専ら回避を可能にし、もしくは容易にする目的で設計、製造、適合または実行された装置、製品または部品を製造し、輸入し、頒布し、販売し、貸与し、販売もしくは貸与目的で提供または陳列し、販売もしくは貸与目的で宣伝し、商業目的で所持し、またはそのような役務を提供する場合。
- 2 著作権侵害について、以下の者は、C に対し著作権者と同様の権利を有する。
  - (a) 効果的な技術的手段が適用される著作物について、
    - (i) その複製物を公に発行する者、または
    - (ii) 公衆に伝達する者
  - (b) 著作権者またはその排他的被許諾者が(a)で規定されている者に当たらない場合は、その者
  - (c) 著作物に適用された効果的な技術的手段の知的財産権者またはその排他的被許諾者



3 (略)

4 さらに、第 2 項に規定される者は、著作権者が侵害複製物に関して有するのと同様、技術的手段を回避するために利用する意図をもってある者が所有し、保管し、または管理する装置、製品または部品に関し、第 99 条または第 100 条（特定の物品の引渡しおよび押収）に基づく権利を有する。

5～6 (略)

7 本条により付与された権利の侵害についての手続きに適用されるのと同様に、第 97 条 1 項(善意による著作権侵害)において、著作物に著作権が存在することを知らない、または知るべき理由を有しなかった被告への言及は、その者の行為が著作権侵害を可能にし、もしくは容易にしたことを知らない、または知るべき理由を有しなかったことへの言及であると解釈されるものとする。

8 第 1 項から第 5 項、第 6 項(b)、第 7 項およびこれら項の目的のために効力を有する本法の他の規定は、必要な適合の上、興行権、出版権およびデータベース権に適用される。

9 (略)

#### 第 296ZE 条：効果的な技術的手段が許される行為を妨げている場合の救済

1 本条において、「許される行為」とは、別表 5A の第 1 部に掲げられる本法の規定に基づいて著作物についてなされる著作権の本質に反しない行為を意味し、「自主的な手段または合意」とは、それによって、ある者の許される行為の実行を可能にする効果を有する以下のことを意味する。

- (a) コンピュータ・プログラム以外の著作物に関して、著作権者、その排他的被許諾者、複製物を発行する者または著作物を公衆に伝達する者によって採用される自主的な手段、または
- (b) コンピュータ・プログラム以外の著作物に関して、著作権者、その排他的被許諾者、複製物を発行する者または著作物を公衆に伝達する者と他の当事者との間でなされる合意

2 コンピュータ・プログラム以外の著作物に適用された効果的な技術的手段により、ある者が当該著作物に関する許される行為を実行することが妨げられている場合、その者または許される行為の実行が妨げられている者らの代表者は、国務長官に対して申立ての通知を提出することができる。

- 3 申立ての通知を受領した場合、国務大臣は当該著作物の著作権者またはその排他的許諾者に対し、以下に掲げる目的の達成に不可欠または適切だと認める指示を出すことができる。
  - (a) 当該申立ての原因が存在する著作物に関して、自主的な手段または合意が存在するかどうかの確認、または
  - (b) (自主的な手段または合意が存在しないと認められた場合)当該申立ての申立人が許される行為を実行するのに必要な手段が、当該許される行為による利益を享受するのに必要な範囲で、当該著作物の著作権者またはその排他的被許諾者によって、提供されることの保証
- 4 (略)
- 5 指示を実行することは、第 3 項(a)および(b)に基づいて当該指示が与えられた者の責務であるとする。
- 6～8 (略)
- 9 本条は、合意された契約条件に従い、公衆の各人が個別に選択する場所から、および各人が個別に選択する時に著作物にアクセスできるような方法で、公衆の利用に供されている著作物には適用されない。
- 10 申立ての申立人が保護された著作物に適法にアクセスできる場合、または申立ての申立人が集合体の代表者である場合には当該集合体がかかる著作物に適法にアクセスできる場合にのみ、本条は適用される。
- 11 第 1 項から第 10 項は、必要な適合の上、以下について適用される。
  - (a) 興行権、またこの文脈における「許される行為」という表現は、別表 5A の第 2 部に掲げられる本法の規定に基づいてなされる行為を指す。
  - (b) データベース権、またこの文脈における「許される行為」という表現は、別表 5A の第 3 部に掲げられる本法の規定に基づいてなされる行為を指す。
  - (c) 出版権

#### 第 296ZF 条：第 296ZA 条から第 296ZE 条の解釈

- 1 第 296ZA 条から第 296ZE 条において、「技術的手段」とは、その通常の動作の過程において、コンピュータ・プログラム以外の著作物を保護するために設計された技術、装置または部品をいう。
- 2 著作物の利用が意図した保護を達成するための以下の行為を通じて著作権者によりコ

ントロールされている場合、当該手段は「効果的」である。

- (a) アクセスコントロールまたは暗号化、スクランブルその他著作物の変換といった保護過程
- (b) コピーコントロールメカニズム

3 本条において、

- (a) 著作物の保護とは、著作権者により許諾されず、著作権により制限されている行為の防止または制限をいい、
- (b) 著作物の利用は、著作権により制限される行為の範囲外の著作物の利用に拡大されない。

4 本法第1部の目的のために定義された第296ZA条から第296ZE条において使用される表現は、当該章と同様の意味を有する。

## 別表 5A : 第 296ZE 条が適用される許される行為

### 第1部：著作権の例外

第29条(研究及び私的調査)

第31A条(私的使用目的で作成する利用可能な複製物)

第31B条(視覚障害者のための複数の複製物)

第31C条(中間的複製物および録音物)

第32条(1)、(2)および(3)(授業または試験を目的として行われること)

第35条(教育放送機関による録音・録画)

第36条(発行された著作物からの文章の教育機関による複写複製)

第38条(司書による複製：定期刊行物の記事)

第39条(司書による複製：発行された著作物の部分)

第41条(司書による複製：他の図書館への複製物の提供)

第42条(司書または文書保管人による複製：著作物の代替複製物)

第43条(司書または文書保管人による複製：ある種の未発行著作物)

第44条(輸出の条件として作成を必要とされる著作物の複製物)

第45条(議会手続および司法手続)

第46条(王立委員会および法定調査)

第47条(公衆の閲覧に供される、または公的登録簿に載っている資料)

第48条(公務の過程で国王に伝達される資料)

第49条(公的記録)

第50条(法定の権限に基づいて行われる行為)

- 第 61 条(民謡の録音物)
- 第 68 条(放送を目的とする付随的録音・録画)
- 第 69 条(放送の監督および管理を目的とする録音・録画)
- 第 70 条(タイム・シフトを目的とする録音・録画)
- 第 71 条(放送の写真)
- 第 74 条(放送の字幕入り複製物の提供)
- 第 75 条(記録保存を目的とする録音・録画)

## 第 2 部：興行権の例外

- 別表 2 第 4 項(授業または試験を目的として行われること)
- 別表 2 第 6 項(教育機関による放送の録音・録画)
- 別表 2 第 7 項(輸出の条件として作成を必要とされる著作物の複製物)
- 別表 2 第 8 項(議会手続および司法手続)
- 別表 2 第 9 項(王立委員会および法定調査)
- 別表 2 第 10 項(公的記録)
- 別表 2 第 11 項(法定の権限に基づいて行われる行為)
- 別表 2 第 14 項(民謡の録音物)
- 別表 2 第 16 項(放送を目的とする付随的録音・録画)
- 別表 2 第 17 項(放送の監督および管理を目的とする録音・録画)
- 別表 2 第 17A 項(タイム・シフトを目的とする録音・録画)
- 別表 2 第 17B 項(放送の写真)
- 別表 2 第 20 項(放送の字幕入り複製物の提供)
- 別表 2 第 21 項(記録保存を目的とする放送の録音・録画)

## 第 3 部：データベース権の例外

1997 年データベースにおける著作権その他の諸権利に関する規則(規則 1997 年第 3032 号)  
規則第 20 条および別表 1

## 別紙 4 ドイツ法

### I. 総則

#### ドイツ著作権法第 53 条

- (1) 自然人が、私的使用のために、あらゆる媒体を使用して著作物を 1 部複製することは、この複製が、直接または間接的に営利を目的としない限りにおいて、許される。ただし、明らかに違法に製作されまたは公衆によるアクセスが可能とされたな原本を、複製のために使用しないものとする。当該複製の作成を許された者が、無償であることを条件として、または写真製版法もしくはその他類似の効果を有する方法で紙もしくは類似の媒体に複製する場合、この者は、これらの複製を他の者に作成させることもできる。
- (2) 次の場合は、複製を 1 部作成しまたは他の者に複製を 1 部作成させることが許される。
  1. 個人的な学術的使用のためであり、その限りにおいて行われ、かつ商業目的によらない場合。
  2. 個人の保存文書に収録するためであり、その限りにおいて行われ、かつ著作物の個人的な複製物を、複製のための原本として使用した場合。
  3. 時事問題に関する情報を自己のために収集するためであり、ラジオで放送された著作物である場合。
  4. その他次のものを、個人的に使用するため。
    - (a) 新聞もしくは雑誌に掲載された出版著作物または個別の寄稿作品の少量。
    - (b) 少なくとも 2 年前から絶版になっている著作物。

第 2 号の場合にあつては、さらに下記のいずれかに該当する場合にのみ、適用する。

1. 写真製版法もしくはその他類似の効果を有する方法を使って、紙または類似の媒体に複製が行われる場合。
2. 専らアナログ的に使用される場合。
3. その保存文書が、公益目的で運営され、かつ直接にも間接的にも経済または商業目的を追求するものでない場合。

第 3 号および第 4 号の場合にあつては、第 1 号または第 2 号のいずれかの条件を満たす場合にのみ許される。

(3) 新聞、雑誌または公衆にアクセス可能となった、出版著作物もしくは個別の寄稿作品の少量を、私的使用のために複製し、複製させることは、次の目的のために複製が必要であり、かつ必要とする限りにおいて、許される。

1. 学校、訓練および教育を行う非営利的機関ならびに職業教育機関における、説明を用いた指導の目的をもって、これらに参加する者のため必要な部数について行うこと。
2. 国家試験および、学校、大学、訓練および教育を行う非営利的機関ならびに職業教育機関における試験のために、これらに参加する者のため必要な部数について行うこと。

学校における指導目的のために著作物を複製することは、著作権者の許諾を得た場合に限り、常に許される。

(4)～(7) (略)

#### ドイツ著作権法第 69f 条

- (1) 権利者は、非合法的に製造もしくは頒布されたすべての複製物または非合法的な頒布目的を有するすべての複製物を廃棄するよう、その所有者または占有者に求めることができる。第 98 条第 2 項および第 3 項は、これに準用する。
- (2) 第 1 項は、コンピュータ・プログラムを保護するために適用されているといい得る技術的装置の許諾なき除去または回避を容易にすることを唯一の目的とするあらゆる手段に準用する。

#### ドイツ著作権法第 95a 条

- (1) この法律で保護する著作物またはその他この法律で保護する対象物の保護に効果的な技術的手段は、回避行為が、当該著作物もしくは対象物へのアクセスまたはそれらの利用を可能にするために行われることを、行為者が知りまたは知り得べき場合には、権利者の許諾なく回避してはならない。
- (2) この法律において、技術的手段とは、技術、装置および部品であつて、保護著作物またはその他この法律で保護する対象に関する権利者の許諾のない行為を、その通常の動作において禁止または制限するよう設計されたものをいう。技術的手段が効果的であるとは、保護著作物またはその他この法律で保護する対象物の使用が、アクセス・コントロール、暗号化、スクランブリングもしくはその他の変形といった保護過程またはコピー・コントロール・メカニズムなどの、保護目標を達成する保護

の方法の適用を通じて、権利者にコントロールされている場合をいう。

- (3) 次の各号のいずれかに該当する装置、製品または部品の製造、輸入、頒布、販売、賃貸、販売もしくは賃貸の広告および商業目的の所持ならびにサービスの提供は、禁止する。
  1. 効果的な技術的手段の回避を目的として、宣伝、広告または市販されたもの。
  2. 効果的な技術的手段の回避を除き、限られた商業的に重要な目的または利用方法しか有しないもの。
  3. 効果的な技術的手段の回避を可能または容易にすることを主たる目的として、設計、製造、適合または実行されるもの。
- (4) 第1項および第3項の禁止は、公共の安全の保護または刑事手続における政府機関の職務および権限に影響を及ぼさない。

#### ドイツ著作権法第95b条

- (1) 権利者がこの法律に従い技術的手段を用いる場合、当該権利者は、次の制限規定の受益者が、保護著作物または保護された対象物に合法的にアクセスできるときには、次の制限規定に定める著作物の利用を可能にするため必要な手段を、この受益者に講じる義務を負う。当該義務を除外する契約上の合意は、無効とする。
  1. 第45条(司法および公共の安全)
  2. 第45a条(障害者)
  3. 第46条(宗教、学校または教育の用に供する編集物)ただし、宗教的意義を有する使用は除く。
  4. 第47条(学校放送)
  5. 第52a条(教育および研究のための公衆提供)
  6. 第53条(私的およびその他自己使用のための複製)
    - (a) 第1項。ただし、紙または類似媒体への写真技法もしくはその他類似的効果のある処理による複製に限る。
    - (b) 第2項第1文第1号
    - (c) 第2項第1文第2号であって、同項第2文第1号(紙への写真複写)または第3号に関連するもの。
    - (d) 第2項第1文第3号および第4号であって、いずれの場合においても第2文第1号および第3文に関連するもの。
    - (e) 第3項
  7. 第55条(放送機関による複製)

- (2) 第 1 項の義務に違反する者について、先のいずれかの制限規定の受益者は、当該規定に定める各権利の実現に必要な手段を講じるよう求めることができる。提供した手段が、権利者団体と先の制限規定の受益者団体との間の合意に合致する場合には、その手段は、当該権利を実現するに足りるものと推定する。
- (3) 著作物およびその他関連する対象物が、合意した契約上の条件に基づき、かつ公衆の構成員が個別に選択した場所および時刻においてアクセス出来る方法で公衆の利用に供された場合、第 1 項および第 2 項は適用しない。
- (4) 第 1 項の義務を履行するために適応される技術的手段(自発的合意の実施に適応されるものを含む)は、第 95a 条に基づく法的保護を受ける。

#### ドイツ著作権法第 95c 条 (略)

#### ドイツ著作権法第 95d 条

- (1) 技術的手段で保護する著作物およびその他技術的手段で保護する対象物には、明確に視認できる方法で、適用された技術的手段のプロパティ情報を含んだラベルが付されなければならない。
- (2) 著作物またはその他保護された対象物に技術的手段を適用する者は、第 95b 条第 2 項第 1 文に基づく主張を可能とするために、自己の氏名またはサービスを行う企業名および住所を提供しなければならない。これは、第 95b 条第 3 項の場合には、適用しない。

## II. 救済措置に関する規定

#### ドイツ著作権法第 97 条

- (1) 著作権またはその他この法律で保護する権利に対する侵害行為が繰り返されるおそれがある場合、損害を被った者は、その権利を侵害する者に対し、その侵害停止を求める差止めの訴えを提起できる。差止めの訴えは、侵害行為が初めて繰り返されたときにおいても、提起することができる。
- (2) 故意または過失により侵害行為を行う者は、損害賠償の責めを負う。損害を被った者は、損害賠償の代わりに、侵害した者がその侵害から得た利益の引渡しを請求できる。損害賠償は、その侵害から得た利益を基礎として算定することもできる。学



術的出版物の著者(第 70 条)、写真家(第 72 条)および実演家(第 73 条)は、侵害が故意または過失による場合には、金銭的損害がないときであっても、正義の実現に必要な限りにおいて、被った損害の金銭的補償を求めることができる。

#### ドイツ著作権法第 97a 条 (略)

#### ドイツ著作権法第 98 条

- (1) 損害を被った者は、製造され、違法に頒布されまたは非合法的な頒布目的を有する複製物であって、侵害者が占有または所有するものすべてを廃棄するよう求めることができる。第 1 文は、侵害者が、主に複製物を製作することを意図して所有する装置にも、同じく適用できる。
- (2) 著作権またはその他この法律で保護する権利を侵害する者は、違法に製造または頒布された当該複製物を回収または破棄するよう請求できる。
- (3) 損害を被った者は、第 1 項に定める措置に代えて、侵害した者が所有するすべての複製物を、その製造費用を超えない公正な報酬と引き換えに自己へ引渡すよう、請求できる。
- (4)～(5) (略)

#### ドイツ著作権法第 101 条

- (1) 著作権またはその他この法律で保護する権利を商業目的をもって侵害する者は、当該複製物の出所および頒布経路に関する情報を、損害を被った者に遅滞なく提供しなければならない。商業目的は、侵害行為の回数およびその重大性から認定することができる。
- (2) 明白な侵害行為の場合または侵害された者が侵害する者に対して訴えを提起した場合、その申立は、第 1 項の規定にかかわらず、その業務において下記のいずれかに該当する第三者を相手として提起することもできる。
  1. 侵害している複製物を占有した者
  2. 侵害しているサービスを利用した者
  3. 侵害行為に利用されたサービスを提供した者
  4. 第 1 号、第 2 号または第 3 号を犯した者と協力し、かつ製造または頒布についてその者を助けた者ただし、当該第三者が、侵害する者に対し、ドイツ民事訴訟法第 383 条ないし第

385 条において証拠の提出を拒否する権利を有することとなる場合を除く。前段本文に基づく申立において、裁判所は、請求された情報が提供されるまで、侵害者に対する法的手続を中断できる。情報の提供義務を負う者は、侵害された者に必要経費の補償を求めることができる。

(3)～(10) (略)

#### ドイツ著作権法第 108b 条

- (1) 下記の者が、故意および許諾なく第 2 項に定める行為をし、よって著作物またはその他関連する防御的な権利を少なくとも軽過失の限度で侵害、侵害を容易、可能または隠蔽したときには、その行為が、専ら加害者または加害者と個人的な関係のある者の私的な利用のために実行された場合または当該利用に関連する場合でない限り、その者を、最大 1 年の自由刑または罰金刑に処することができる。
  1. 権利者の同意なく、効果的な技術的手段を回避することによって、この法律で保護する著作物またはその他この法律で保護する保護対象にアクセスもしくは第三者がアクセスできるようまたはそのような利用を容易にすることを意図する者。
  2. (略)
- (2) 第 95a 条第 3 項に反して、装置、製品もしくはその一部を、商業目的をもって製造、紹介、頒布、販売または賃借する者もまた罰する。
- (3) 第 1 項に定める場合において、商業目的をもって行為した加害者は、最大 3 年の自由刑または罰金に処する。

### Ⅲ コンテンツの技術的手段に係る各国法制度調査研究(米国編)



### Ⅲ コンテンツの技術的手段に係る各国法制度調査研究の調査項目(米国編)

#### 1. コンテンツの技術的手段に関する国際ルール

##### (1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)

いずれも締結している。

##### (2) 米国における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容

存在する。

NAFTA とイスラエルとの FTA については、WIPO 著作権条約等の成立以前に締結しているので、技術的手段に関する規定は存在しない。

その後に締結された、ヨルダンとの FTA では、ごく簡潔に、技術的手段を回避するための機器等のトラフィックを禁止し、違反に対しては、民事、刑事制裁を設けることを規定された。

さらに、その後の FTA<sup>128</sup>においては、基本的に、後述する DMCA の技術的手段についての規制に類似する規定を備えている。例えば、適用除外等については、DMCA と同様の規定がある。

ただし、チリとの FTA については、DMCA とは異なり、主観的要件により限定を加えており、悪意ないし知ることのできる合理的な理由がある場合における、アクセス・コントロールの回避行為及び技術的手段を回避するための機器等のトラフィックを禁止している。シンガポール、オーストラリア、韓国<sup>129</sup>、との FTA も同様に主観的要件による限定がある。

一方で、モロッコ、バーレーン、CAFTA(中米自由貿易協定)<sup>130</sup>、オマーン、ペルー、パナマ、コロンビアとの間の FTA においては、DMCA と同様に、主観的要件による限定は加えられていない。

#### 2. コンテンツの技術的手段に関する法令等

##### (1) 該当する法令等

1998 年に制定されたデジタルミレニアム著作権法(「DMCA」)により、著作権法が改正

<sup>128</sup> ただし、2010 年 1 月現在において、コロンビア、韓国、パナマとの FTA についてはまだ発効していない。

<sup>129</sup> 現地報告書(米国編)2 頁においては、米韓 FTA については主観的要件による限定がないと解説されているものの、米韓 FTA の関連条文を参照するに主観的要件による限定がなされているものと思われる。

<sup>130</sup> 米国とコスタリカ、ドミニカ共和国、エルサルバドル、グアテマラ、ホンジュラス、ニカラグアとの間の FTA である。

され、コンテンツの技術的手段に対する保護についての規定が設けられた(著作権法第1201条)。

その類型は以下のとおりである。

著作権法により保護される著作物へのアクセスを制限する「アクセス管理技術(「アクセスコントロール」)」を回避する行為が禁止される。(著作権法第1201条(a)(1)(A))

アクセスコントロール又はコンテンツの著作権者の権利を保護するための措置(「権利保護措置」)を回避するための装置等(サービスを含む。以下、「迂回装置等」)<sup>131</sup>について、製造、輸入、公衆提供、供給又はその他の取引を行うこと(「トラフィッキング」)が禁止される。(著作権法第1201条(a)(2)、同条(b)(1))

このとおり、アクセスコントロールについては回避行為自体が禁止されているが、権利保護措置については回避行為自体は禁止されていない。

ここで、技術的手段の回避とは、技術的手段を回避、迂回、除去、無効化又は損壊することを意味する。(著作権法第1201条(a)(3)(A)、同条(b)(2)(A))

## (2) 法令等の規制内容

### (a) 規制対象技術(定義及び対象技術の具体例等)

アクセスコントロールについては回避行為及び迂回装置等のトラフィッキングが禁止されている。ここで、アクセスコントロールとは、技術中立的に規定されており、その通常の操作過程において、著作物へアクセスするためには、著作権者の許諾を得て、情報を入力すること、手続もしくは処理を行うことを必要とするものを意味する(著作権法第1201条(a)(3)(B)参照)。

権利保護措置については迂回装置等のトラフィッキングが禁止されている。ここで、権利保護措置とは、技術中立的に規定されており、その通常の操作過程において、著作権者に認められた著作権の行使を妨害、限定又は制限するものを意味する(著作権法第1201条(b)(2)(B)参照)。

### (b) 規制対象製品及び対象プログラム等

トラフィッキングが禁止される迂回装置等については、技術中立的に規定されている。

トラフィッキングが禁止される迂回装置等は、以下の(i)-(iii)のいずれかに該当するものである。(著作権法第1201条(a)(2)(A)-(C)、同条(b)(1)(A)-(C))

(i) 技術的手段を回避することを主たる目的として、設計又は製造されたもの

<sup>131</sup> 内容は後述2(2)(b)にて詳述する。

(ii) 技術的手段を回避する以外には、限定された商業上の目的又は用法しか有さないもの

(iii) 技術的手段を回避するために使用することを知っている者又はこの者に協力する者によってマーケティング(販売)されたもの

### **(c) 規制対象行為**

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

アクセスコントロールについては、回避行為自体が禁止されるので、⑥は禁止される。

権利保護措置については、回避行為自体は禁止されないため、⑥は含まれない。なお、回避行為の後に複製等をする場合には、それが著作権侵害となる場合には、禁止される。

また、アクセスコントロール及び権利保護措置ともに、先述したとおり、迂回装置等(サービスを含むことに注意)の製造、輸入、公衆提供、供給又はその他の取引を行うことが禁止される。

そこで、上記のうち、①、②、③のうち輸入行為、⑤については禁止されることは明らかである。③のうち輸出行為については、明示されていないが、「公衆提供、供給又はその他の取引」に含まれ、禁止されると解釈され得るとされる<sup>132</sup>。

単なる迂回装置等の所持行為は禁止されていないので、④は禁止されない。

⑦宣伝・情報の流布行為については、状況次第では、「公衆提供」に該当することになり、禁止される<sup>133</sup>。

### **(3) 除外行為**

#### **(a) コンテンツの技術的手段に関する規定の適用除外、例外、制限規定等の存否・内容**

以下の除外が存在する。

ア 連邦議会図書館長による規則に基づくアクセス・コントロールの回避(著作権法第

<sup>132</sup> 現地報告書(米国編)10頁に示された現地弁護士の見解による。この点については、DMCAの保護法益との関係をどのように考えるのか、当職らにより質問をしたものの、詳細は定かではないものと思われ現地報告書にはこの点についての説明は入っていない。

<sup>133</sup> 裁判例によれば、迂回装置を入手することのできるウェブサイトへのリンクを貼ることは、トラフィックを構成すると判断されている。単なる回避方法についての情報の開示が、トラフィックを構成するかについての裁判例は不詳である。(現地報告書(米国編)10頁を参照。)

1201 条(a) (1) (B) (C))<sup>134</sup>

- イ 著作物のコピーを入手するかを決定するための非営利図書館等によるアクセス・コントロールの回避(著作権法第 1201 条(d))
- ウ 連邦政府又は州政府による適法な捜査、情報活動のためのアクセス・コントロールの回避及びアクセス・コントロールと権利保護措置に係る技術的手段の迂回装置等の製造・頒布(著作権法第 1201 条(e))
- エ 独自に創作したコンピューター・プログラムと他のプログラムとの互換性を確保することを目的としたリバース・エンジニアリングのためのアクセス・コントロールの回避及びアクセス・コントロールと権利保護措置に係る技術的手段の迂回装置等の開発・利用(著作権法第 1201 条(f))<sup>135</sup>

<sup>134</sup> 連邦議会図書館長が著作権局の建議に基づき、アクセス・コントロールの回避行為禁止の対象から除外されるべき著作物を規則において定めることとされており、かかる著作物の使用者については、アクセス・コントロールの回避行為の禁止により、著作権を侵害しない形での当該著作物を使用するにあたり、不利益を受ける又は不利益を受ける可能性がある場合には、アクセス・コントロールの回避行為の禁止は適用されない。かかる除外を定める規則については、3 年ごとに更新されることとされている。(著作権法第 1201 条(a) (1) (B) (C))

現在、2006 年に制定された規則がいまだ効力を有している。2006 年規則は、2009 年 10 月 27 日をもって失効するとされていたが、著作権局が新規則についての建議を行わなかったため、著作権局は無期限に 2006 年規則が延長される旨の暫定的な規則を出している。現地報告書(米国編) 11 頁参照。

現在有効な規則においては、以下の 6 種類の著作物が指定されており、これらはアクセス・コントロールの回避行為の禁止について適用除外となっている。①大学の映画又はメディア研究部門の教育図書館に収録されている視覚著作物で、メディアの研究又は映画の教授が教室において教育使用の目的でこれらの作品の一部を使って編集物を作成するために回避がなされる場合、②アクセスするために、もはや廃用となったメディア又はハードウェアを必要とするコンピューター・プログラム及びビデオゲームで、図書館又は記録保管所がこれらの作品を保存する目的で複製のために回避がなされる場合、③ソフトウェアの違法コピーを防止するための特殊な機器である dongle により保護されているコンピューター・プログラムで、dongle が故障又は破損しているために著作物にアクセスすることができず、かつ、dongle がすでに廃用されている場合、④e-book のフォーマットで頒布される言語著作物で、当該著作物の既存の e-book のフォーマットで頒布されているすべてについて、e-book の音読機能やスクリーン・リーダーがテキストを特定の形式に変換することを防止するアクセス・コントロールを含むもの、⑤無線電話の端末を無線電話通信網に接続することができるファームウェア方式のコンピューター・プログラムで、無線電話通信網に適法に接続するために回避が行われる場合、⑥コンパクト・ディスク形式で頒布され、かつ、適法に購入した作品へのアクセスをコントロールし、かつ、パーソナル・コンピューターの安全性を危うくするような安全性の欠陥や脆弱を作り出すような技術的手段によって保護されているサウンド・レコーディング及びそれに関連する視聴覚作品で、そのような安全性の欠陥や脆弱を誠実に検査し、調査、修正するために回避が行われる場合。

<sup>135</sup> 他のコンピューター・プログラムとの互換性を確保するのに必要な特定や解析を行うという目的の場合に限り、著作権侵害とならない範囲で、技術的手段を回避すること、又は、回避のための技術的手段を開発することは禁止されない。また、これらにより得た情報や方法について、著作権侵害とならない範囲で、コンピューター・プログラムとの互換性を達成する目的において、他者に提供することは、禁止されない。



- オ 暗号化研究のためのアクセス・コントロールの回避及びアクセスコントロールに係る技術的手段の迂回装置等の開発・利用(著作権法第 1201 条(g))
- カ 未成年者保護のためのアクセス・コントロールの場合、裁判所は違法性の判断の際に、アクセス・コントロールの必要性を考慮することができる(著作権法第 1201 条(h))
- キ アクセス・コントロールが著作物にアクセスする個人の識別情報を収集又は流布する機能を持つ場合、当該行為を妨害するために行われるアクセス・コントロールの回避(著作権法第 1201 条(i))
- ク コンピューター又はコンピューター・システムのセキュリティ検査のためのアクセス・コントロールの回避及びアクセスコントロールに係る迂回装置等の開発・製造・頒布・利用(著作権法第 1201 条(j))

**(b) 著作権法にコンテンツの技術的手段に関する規定が存在する場合の技術的手段回避の禁止規定と権利制限規定との関係**

DMCA により著作権法に加えられた技術的手段に係る規定は、著作権法の下で従来認められてきた権利、救済措置、権利の制限、フェア・ユースを含む著作権侵害に対する抗弁に影響を与えない(著作権法第 1201 条(c))。

**(4) 救済措置**

**(a) 救済措置の内容(民事的救済及び刑事的制裁)**

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

すべての技術的手段についての規定への違反につき、民事救済及び刑事制裁の双方が存在する。

**ア 民事救済**

(ア) 暫定的及び終局的な差止命令(著作権法第 1203 条(b)(1))

(イ) 差押命令(著作権法第 1203 条(b)(2))

#### (ウ) 損害賠償(著作権法第 1203 条(b) (2)、1203 条(c))

- 現実的損害賠償(著作権法第 1203 条(c) (2))  
被害者に生じた実損害及び当該実損害の算定には含まれない違反者の利得について損害賠償請求をすることができる。
- 法定損害賠償(著作権法第 1203 条(c) (3))  
違反行為一つにつき、200 米ドル以上、2,500 米ドル以下の損害賠償請求をすることができる。
- 三倍賠償(著作権法第 1203 条(c) (4))  
裁判所は、繰り返しの違反者に対しては、損害賠償の額を三倍まで加重することができる。

#### イ 刑事制裁(著作権法第 1204 条)

悪意、かつ、商業目的又は利得目的の違反者に対しては刑事制裁が課される(著作権法第 1204 条(a))。

初犯の場合には、法定刑は、5 年以下の懲役又は若しくは 500,000 米ドル以下の罰金、又はこれらの併科である(著作権法第 1204 条(a) (1))。

累犯の場合には、法定刑は、10 年以下の懲役又は若しくは 1,000,000 米ドル以下の罰金、又はこれらの併科である(著作権法第 1204 条(a) (2))。

### (b) (a) の救済措置の請求主体

#### ア 民事救済

損害を被った者<sup>136</sup>(著作権法第 1203 条(a))

#### イ 刑事制裁

検察官

非親告罪とされる<sup>137</sup>。

### (c) 違反機器等の輸出入にかかる水際措置又は違反抑止のための行政措置の有無・内容

違反機器等の輸出入にかかる特定の水際措置は存在しない。

ただし、税関当局の内部で利用されているガイドラインには、著作権法に違反する物品を没収等することのできる税関当局の一般的権限に基づき、DMCA に係る規定に違

<sup>136</sup> “Any person injured by a violation” と規定されている。

<sup>137</sup> 現地報告書(米国編)16 頁。

反する物品についても没収等の対象となるとされている<sup>138</sup>。

#### **(5) いわゆる「無反応機器」規制**

##### **いわゆる「無反応機器」に対する法令、規則、指令等による規制の有無・内容**

いわゆる無反応危機は、一般的には、規制対象となっていない。

もっとも、いわゆる無反応危機が、(i)技術的手段を回避することを主たる目的として、設計又は製造されたもの、(ii)技術的手段を回避する以外には、限定された商業上の目的又は用法しか有さないもの、(iii)技術的手段を回避するために使用することを知っている者又はこの者に協力する者がマーケティングしたものに該当する場合には、規制の対象となる<sup>139</sup>。

また、特定のアナログ・ビデオカセットレコーダーについて、自動制御コピー・コントロール技術に適合しないものを製造、輸入、公衆提供、供給又はその他の取引を行うことが禁止される(著作権法第1201条(k))<sup>140</sup>。

さらに、1992年音声家庭録音法(Audio Home Recording Act)により著作権法第10章が設けられ、一定のデジタル音声録音装置について、SCMS(Serial Copy Management System)が導入されていないものの製造・頒布等が禁止されている<sup>141</sup>。

### **3. 裁判例、執行状況、被害状況等**

#### **(1) コンテンツの技術的手段に関する裁判例**

技術的手段に関する規制内容の内実については、裁判所の判断において幾分具体化がなされている<sup>142</sup>。

まず、著作権により保護されているケーブルテレビ放送や衛星放送等に無権限者がアクセスできるようにする装置については、多くの件で、裁判所により著作権法第1201条違反と判断されている<sup>143</sup>。

また、テレビ・ゲームの利用者が、地域制限のアクセス・コントロール(region

<sup>138</sup> 現地報告書(米国編)17頁。

<sup>139</sup> 現地報告書(米国編)17頁。現実的には、(iii)技術的手段を回避するために使用することを知っている者又はこの者に協力する者がマーケティングしたものに該当し得るかもしれない。

<sup>140</sup> これはいわゆるアナログ・ホールの問題に対応するためであるとされる(現地報告書(米国編)17頁)。

<sup>141</sup> もっとも、パソコンのハードドライブは、一定のデジタル音声録音装置には含まれず、もはやこの規定は時代遅れとなっているとされる(現地報告書(米国編)18頁)。

<sup>142</sup> 詳細は、現地報告書(米国編)6～9、18～23頁を参照。

<sup>143</sup> 例えば、U.S. v. Whitehead 532 F.3d 991 (9<sup>th</sup> Cir. 2008), DirecTV v. Borrow, 2005 US Dist LEXIS 1328 (N.D. Ill. 2005); Comcast of Ill. v. Hightech Electronics, 2004 US Dist LEXIS 14619 (N.D. Ill. 2004); DirecTV v. Ferguson, 328 F.Supp2d 904 (N.D. Ind. 2004)等。

encoded)を改変することのできる「ゲーム・エンハンサー(game enhancer)」<sup>144</sup>や海賊版のゲームの利用を妨げる技術的手段を回避する「モッドチップ(modification chips)」<sup>145</sup>については、裁判所により著作権法第 1201 条違反とされている。

さらに、最も注目を集めた事件として、DVD を保護する技術的手段を回避するソフトウェア・プログラム(CSS を解読することのできるソフトウェア・プログラム)について、裁判所により著作権法第 1201 条に違反するものと判断されている<sup>146</sup>。加えて、ユーザーが、コピー・プロテクション・コントロールを取り除き、保護されたフォーマットのストリーミング・メディアを捕らえ、これを保護がされていないフォーマットにコピーすることのできるソフトウェア・プログラムについても、裁判所により著作権法第 1201 条に違反するものと判断されている<sup>147</sup>。

テレビ・ゲームの製造者の認証プロトコルを回避し、これによりユーザーが海賊版のゲームを利用できるようにするサービスを提供したことについても、裁判所により著作権法第 1201 条に違反するものと判断されている<sup>148</sup>。

音楽や映画等、伝統的に保護の対象と考えられてきたコンテンツを超えて、DMCA の技術手段についての規制に違反するともされ得る。裁判所は、ウェブ上においてチケット販売する会社の、チケットを販売するウェブサイトのアクセスコントロールを回避し、当該チケット販売会社の方針に反して、ユーザーが同時に複数枚のチケットを購入できるようにしたことが DMCA の規制に違反する可能性が非常に高いとした<sup>149</sup>。

一方で、DMCA の規制の射程の限界を画する判断をした裁判例もある。これらの裁判例においては、アクセス・コントロールについて、アフターサービス市場やスペア・パーツ市場における支配力を強化するものであるとされた。

具体的には、裁判所は、コンピューター用のプリンターの大手メーカー(原告)のプリンターのトナー・カートリッジに埋め込まれたプログラムは純粹に機能的であり、保護される表現に該当せず、むしろ、トナー・カートリッジのアフターサービス市場において競合相手の製品を単に締め出すことを目的としたものであるとし、当該ソフ

---

<sup>144</sup> Sony Computer Entertainment America, Inc. v. Gamemasters 87 F.Supp.2d 976 (N.D. Cal. 1999)

<sup>145</sup> Sony Computer Entertainment America, Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 81 U.S.P.Q.2d 1045 (N.D. Cal. 2006)

<sup>146</sup> RealNetworks, Inc v. DVD Copy Control Assoc., Inc. 2009 WL 2475338 (N.D. Cal.), 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004)、Universal City Studios, Inc. v. Corley 273 F.3d 429 (2<sup>nd</sup> Cir. 2001)等。

<sup>147</sup> RealNetworks, Inc. v. Streambox, 2000 WL 127311 (W.D. Wash. 2000)

<sup>148</sup> MDY Industries, LLC v. Blizzard Entertainment, Inc., 616 F. Supp. 2d 958 (D. Ariz. 2009), subsequent determination, 2009 WL 649719 (D. Ariz. 2009). Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005)

<sup>149</sup> Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007)

トウェアへのアクセス・コントロールを回避する行為は違法とはならないとした<sup>150</sup>。

もう一つの事例においては、裁判所は、ガレージ・ドアの開閉装置を製造・販売している会社(原告)の携帯用のガレージ・ドア開閉機に内蔵されているソフトウェアについて著作権の保護の対象となししつつも、当該ソフトウェアへのアクセス・コントロールの目的は、著作権侵害の防止ではなく原告のスペア・パーツ市場における支配力の強化であるとし、DMCAの規制違反を認めなかった<sup>151</sup>。

## (2) コンテンツの技術的手段に関する執行状況

執行状況に関する統計的資料は入手できなかった。

Westlawによれば、DMCAの技術的手段についての規定に触れる裁判例は100以上存在する。

刑事制裁の規定はあるものの、注目された刑事事件の実例は極めて少ない。その中では、U.S. v. Elcom Ltd. 事件<sup>152</sup>においては、ロシア人のコンピューター科学者が逮捕され、3週間留置され、e-bookの技術的手段を解読するプログラムを取引したとの訴因により起訴された。雇用者であるElcomに対する訴追に協力することとの引き換えに当該科学者に対する訴追は取り下げられた。もっとも、Elcomは最終的には陪審員より無罪とされた。また、U.S. v. Whitehead 事件<sup>153</sup>においては、被告人は、DirecTVのアクセスカードをプログラムするために必要なソフトウェアを購入し、販売し、頒布したとして訴追され、1,000時間のコミュニティーサービス、50,000ドルの被害弁償等を命じられた。U.S. v. Mynaf 事件<sup>154</sup>においては、被告人は、4,500以上の海賊版のビデオカセットが被告人が借りていた施設から発見されたところ、著作物へのアクセスコントロールを回避する装置を利用し、アクセスコントロールを回避したことを認め、著作権法第1201条違反により、24ヶ月の懲役、200,000ドルの罰金を命じられた。

<sup>150</sup> Lexmark International v. Static Control Components, 253 F. Supp. 2d 943, 66 U.S.P.Q.2d (BNA) 1405 (E.D. Ky. 2003)

<sup>151</sup> Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 72 U.S.P.Q.2d (BNA) 1225 (Fed. Cir. 2004), cert. denied, 2005 WL 218463 (U.S. 2005)

ただし、立法過程からは、著作権者に対してアクセス・コントロールそのものに対する保護を与えることを議会は意図していたことが窺われ、著作権を保護する目的のアクセス・コントロールだけを保護対象とする本判決は、かかる議会の意図とは整合しないとの指摘がなされている(現地報告書(米国編)9頁)。

<sup>152</sup> 203 F. Supp. 2d 1111 (N.D. Cal. 2002)

<sup>153</sup> 532 F.3d 991 (9<sup>th</sup> Cir. 2008)

<sup>154</sup> (E.D. Cal.)

### **(3) コンテンツの技術的手段に関する被害状況**

被害状況についての統計的資料は入手できなかった。

## **4. 技術動向の調査**

### **(1) コンテンツの技術的手段に関する技術動向**

報告書 EU 編を参照。

### **(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術**

デジタル放送において broadcast flag が導入されかけている。broadcast flag は、デジタル放送のデータに組み込まれる情報であり、消費者が当該デジタル放送を録画する能力、録画したデータを再生する能力に制限を加えるものである。

2005 年には、連邦通信委員会(FCC)が、HDTV の製造業者に対し、broadcast flag へ備えるように命じる規則を発したが、American Library Association v. FCC 事件<sup>155</sup>において、裁判所は FCC がかかる規則を公布したことにつき、FCC の権限を超えたものであるとの判断を下した。それ以来、同様の規則は出されていないが、放送業者は引き続きかかる規則の導入についてロビー活動を行っている。

### **(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況**

アクセス・コントロール、権利保護措置、トラフィッキングが禁止される迂回装置等については技術中立的に規定されているため、新たな技術にも対応できるようになっている。

技術的手段についての規制により、海賊版が大幅に減ったとはいえないかもしれないが、技術的手段についての規制は、少なくとも、大企業が著作権法第 1201 条違反とされる迂回装置等を頒布することに対する抑止力とはなっている。

また、技術的手段についての規制は、大きなコンテンツ所有者が新たなビジネスモデルや流通方式を試行することを可能としている。

## **5. 各国内の議論(規制に対する賛否・改正動向等)**

### **(1) コンテンツの技術的手段に関する現行規制に対する議論**

技術的手段に対する規制については、以下の 3 点から疑問が提起されている。

#### **ア フェア・ユース**

DMCA の技術的手段に対する規制は、著作権を侵害するかどうかを問わず、その主要な目的が技術的手段の回避である装置等のトラフィッキングを違法とした。これにより、ユーザーによるフェア・ユースの機会が事実上奪われている。

<sup>155</sup> 406 F.3d 689 (D.C. Cir. 2005)

## イ ファースト・セール(消尽)

消尽理論からすると、著作物の複製の購入者においては、本来いつでも、何度でも当該複製を利用すること、さらには知人に貸与することも可能である。DMCA の技術的手段に対する規制は、消尽理論により本来可能であるはずの購入者の利用形態を制約するものである(たとえば、地域制限(region encoding)を付すことにより、購入者の利用を制約している)。

## ウ 反競争的行為

DMCA の技術的手段に対する規制は、コンテンツ所有者が、反競争的な行為を行うことを容易にしているとの指摘がある。例えば、アップル社のオンライン音楽プレーヤー市場とオンライン音楽販売市場における強大さは、アップル社のフォーマット以外の音楽ではハードウェアでの再生が困難であり、また、アップル社のフォーマット以外のハードウェアでは音楽の再生が困難であることによる。2004 年には、Real Networks 社は、自社のフォーマットの音楽でもアップル社の iPod で再生が可能となるように試みたが、アップル社による著作権法第 1201 条違反に問うとの警告によりこれを断念した。

### (2) コンテンツの技術的手段に関する規制に対する業界からの要望状況

映画業界(MPAA)や音楽業界(RIAA)は、DMCA の技術的手段についての規制を支持している。MPAA は州レベルでも同様の規制を導入することをロビーしており、RIAA は個人に対しても訴訟を提起することを喧伝している。

ただし、音楽業界は、近時、技術的手段を取り除く方向に向かっている。CD から DRM 保護が取り除かれ、また、アップル社の iTunes や Real Networks 社の Rhapsody も保護がなされていない音楽ファイルを多く販売している。

一般的には、学界、図書館、市民の自由権を標榜する NPO は、DMCA の技術的手段についての規制にもともと反対であり、また、著作権者がこれをエンフォースすることにも反対である。

### (3) 法改正の動向・内容

大きな法改正の動向は、現状見あたらない。

以 上

(参考訳文(抄訳))

別紙 1

オーストラリア

第 17 章

第 17.4.7 条

(a) 各締約国は、著作者、実演家およびレコードの製作者がその権利の行使に関連して使用するもので、かつ、これらの者の著作物、実演およびレコードについて許諾のない行為を制限する、効果的な技術的手段を回避することに対して、適切な法的保護および効果的な法的救済を提供するため、下記のいずれかにあたる者が、第 17.11.13 条に定める救済の責を負いかつそれに従う旨を定める。

(i) 保護された著作物、実演、レコードまたはその他の対象に対するアクセスをコントロールする効果的な技術的手段を、それと知りまたは知り得る相当の理由がありながら、許諾なく回避する者。

(ii) 次のいずれかにあたる装置、製品、部品を、製造、輸入、頒布、公衆に提供、供給または取引する者、あるいはサービスを公衆に提供、供給する者。

(A) 効果的な技術的手段を回避する目的をもって宣伝、広告または市販されるもの。

(B) 効果的な技術的手段を回避すること以外に、限られた商業上重要な目的または利用方法しか有しないもの。

(C) 効果的な技術的手段の回避を可能または容易にすることを主たる目的として、設計、製造または実行されるもの。

各締約国は、ある者が、故意に、かつ商業的利益または金銭的利得を得る目的をもって、上記のいずれかの行為に従事したと認められる場合に適用する刑事手続および刑罰を定める。各締約国は、当該刑事手続および刑罰が、非営利の図書館、文書資料館、教育機関または公的な非商業的放送機関に対して適用されないことを定めることができる。

(b) 効果的な技術的手段とは、その通常の動作過程において、保護された著作物、実演、レコードもしくはその他保護された対象に対するアクセスをコントロールする、または、著作権を保護する、技術、装置または部品をいう。



(c) 前記第(a)項の規定を実施するあらゆる国内法に違反しない限り、締約国のいずれも、第(a)項を実施するにあたり、当該製品が、家庭用電化製品、通信機器もしくはコンピュータ関連製品の設計またはこれらの部分および部品の設計ならびに選択が、特定の技術的手段に対応しなければならないとする義務を負わない。

(d) 各締約国は、本条を実施する国内法の違反が、その締約国の著作権法のもとで発生し得るいかなる侵害とも別個の民事上または刑事上の行為であって独立である旨を定める。

(e) 各締約国は、第(a)項を実施するあらゆる国内法における例外を、以下のすべての行為に限定し、この例外は、第(f)項に従い、関連する国内法に適用する。

(i) 合法的に取得したコンピュータ・プログラムの複製に関する非侵害リバーズ・エンジニアリング行為であって、独立して作成されたコンピュータ・プログラムとその他のプログラムとの互換性を達成することを唯一の目的として、当該行為に従事する者が容易に入手できるものでないコンピュータ・プログラムの特定要素について、善意で行ったもの。

(ii) 善意による非侵害行為であって、著作物、実演またはレコードの、複製、固定されていない実演または展示を、合法的に取得し、かつ、当該行為の許諾を得るために誠実に努力した、相当の資格を有する研究者が、情報のスクランブリングおよび非スクランブリングのための技術の欠陥および脆弱性の特定および分析を唯一の目的に必要な限度で行ったもの。

(iii) 未成年者の不適切なオンライン上のコンテンツへのアクセスを防止することを唯一の目的として、部品または部分を、それ自体は第(a)(ii)項を実施する国内法で禁止されない、技術、製品、サービスまたは装置に組み込むこと。

(iv) 善意による非侵害行為であって、コンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークの所有者により、それらの試験、調査またはセキュリティの修正を唯一の目的として、許諾されるもの。

(v) 非侵害行為であって、自然人のオンライン上の行為を反映した個人識別情報を秘密裏に収集または流布する機能を、自然人の著作物へのアクセス能力に全く影響を与えない方法で、特定および無効にすることを唯一の目的としたもの。

(vi) 適法に許諾を受けた行為であって、政府職員、政府系機関または政府の契約者

が、法の執行、諜報、安全保障または類似の行政目的のために行ったもの。

(vii) 非営利の図書館、文書資料館または教育機関が行う、著作物、実演またはレコードへのアクセスであって、他にそれらを手に入れる方法がない場合に、それらを取得するための決定を行うことを唯一の目的としたもの。

(viii) 特定の種類の著作物、実演またはレコード上の著作物、実演またはレコードの非侵害的利用に対して、実際に生じまたは生じ得る悪影響が、立法または行政の審査若しくは手続において十分に立証された場合の、当該非侵害的利用。ただし、かかる審査又は手続は、当該審査又は手続が終結した日から少なくとも4年ごとに行われるものとする。

(f) 第(a)項を実施するあらゆる国内法の例外は、第(e)項で定める行為について、次のすべての場合に限り、かつ、効果的な技術的手段の回避に対する法的保護の適切性または法的救済の有効性を損ねることのない限度に限り、適用することができる。

(i) 第(a)(i)項を実施する国内法は、第(e)項に定める各行為について、例外の対象とすることができる。

(ii) 第(a)(ii)項を実施する国内法は、著作物、実演またはレコードへのアクセスをコントロールする効果的な技術的手段に適用するにあたり、第(e)(i)項、同(ii)項、同(iii)項、同(iv)項および同(vi)項に定める行為について、例外の対象とすることができる。

(iii) 第(a)(ii)項を実施する国内法は、それを著作権を保護する効果的な技術的手段に適用するにあたり、第(e)(i)項および同(vi)項に定める行為について、例外の対象とすることができる。

#### **第 17.4.8 条 (略)**

**韓国**  
**第 18 章**

**第 18.4.7 条**<sup>156</sup>

(a) 各締約国は、著作者、実演家およびレコードの製作者がその権利の行使に関連して使用するもので、かつ、これらの者の著作物、実演およびレコードについて許諾のない行為を制限する、効果的な技術的手段を回避することに対して、適切な法的保護および効果的な法的救済を提供するため、下記のいずれかにあたる者が、第 18.10.13 条に定める救済の責を負いかつそれに従う旨を定める。

(i) 保護された著作物、実演、レコードまたはその他の対象に対するアクセスをコントロールする効果的な技術的手段を、それと知りまたは知り得る相当の理由がありながら、許諾なく回避する者。

(ii) 次のいずれかにあたる装置、製品、部品を、製造、輸入、頒布、公衆に提供、供給または取引する者、あるいはサービスを公衆に提供、供給する者。

(A) 上記のいずれかに該当する者により、またはその者が、効果的な技術的手段を回避する目的で宣伝、広告または市販することを知りながら、これと共同して行為する他の者により、効果的な技術的手段を回避する目的をもって宣伝、広告または市販されるもの。

(B) 効果的な技術的手段を回避すること以外に、限られた商業上重要な目的または利用方法しか有しないもの。

(C) 効果的な技術的手段の回避を可能または容易にすることを主たる目的として、設計、製造または実行されるもの。

各締約国は、非営利の図書館、文書資料館、教育機関または公的な非商業的放送機関以外の者が、故意に、かつ商業的利益または私的な金銭的利得を得る目的をもって、上記のいずれかの行為に従事したと認められる場合に適用する刑事手続および刑罰を定める。当該刑事手続および刑罰には、侵害に対する適用と同様、第 18.10.27 条の第(a)項、第(b)項および第(e)項に列記する救済および関係当局の行為に対する適用を、必要な変更の上、

---

<sup>156</sup> 訳者注：現地報告書原文では「7」とのみ記載あるが、FTA 原文では「18.4.7」に該当するため「第 18.4.7 条」と記載。

含める。

(b) 前記第(a)項の規定を実施するあらゆる国内法に違反しない限り、締約国のいずれも、第(a)項を実施するにあたり、当該製品が、家庭用電化製品、通信機器もしくはコンピュータ関連製品の設計またはこれらの部分および部品の設計ならびに選択が、特定の技術的手段に対応しなければならないとする義務を負わない。

(c) 各締約国は、本条を実施する国内法の違反が、その締約国の著作権および著作権に関連する権利に関する法のもとで発生し得るいかなる侵害とも別個独立の訴訟原因である旨を定める。

(d) 各締約国は、第(a)項を実施するあらゆる国内法における例外および制限を、以下のすべての行為に限定し、この例外は、第(e)項に従い、関連する国内法に適用する。

(i) 合法的に取得したコンピュータ・プログラムの複製に関する非侵害リバーズ・エンジニアリング行為であって、独立して作成されたコンピュータ・プログラムとその他のプログラムとの互換性を達成することを唯一の目的として、当該行為に従事する者が容易に入手できるものでないそのコンピュータ・プログラムの特定要素について、善意で行ったもの。

(ii) 善意による非侵害行為であって、著作物、実演もしくはレコードの、複製、固定されていない実演または展示を、合法的に取得し、かつ当該行為の許諾を得るために誠実に努力した、相当の資格を有する研究者が、情報のスクランブリングおよび非スクランブリングのための技術の欠陥および脆弱性の特定および分析からなる研究を唯一の目的に必要な限度で行ったもの。

(iii) 未成年者の不適切なオンライン上のコンテンツへのアクセスを防止することを唯一の目的として、部品または部分を、それ自体は第(a)(ii)項を実施する国内法で禁止されない、技術、製品、サービスまたは装置に組み込むこと。

(iv) 善意による非侵害行為であって、コンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークの所有者により、それらの試験、調査またはセキュリティの修正を唯一の目的として、許諾されるもの。

(v) 非侵害行為であって、自然人のオンライン上の行為を反映した個人識別情報を秘密裏に収集または流布する機能を、自然人の著作物へのアクセス能力に全く影響を与えない方法で、特定および無効にすることを唯一の目的としたもの。

(vi) 適法に許諾を受けた行為であって、政府職員、政府系機関または政府の契約者が、法の執行、諜報、安全保障目的または類似の行政目的のために行ったもの。

(vii) 非営利の図書館、文書資料館または教育機関が行う、著作物、実演またはレコードへのアクセスであって、この他にそれら入手する方法がない場合に、それらを取得するための決定を行うことを唯一の目的としたもの。

(viii) 特定の種類の著作物、実演またはレコード上の著作物、実演またはレコードの非侵害的利用に対して、実際に生じまたは生じ得る悪影響が、立法または行政の手續において実質的証拠によって立証された場合の、当該非侵害的利用。ただし、本号に従い採択された制限または例外は、手續が終結した日から 3 年を超えない更新可能な期間、効力を有するものとする。

(e) 第(a)項を実施するあらゆる国内法の例外および制限は、第(d)項で定める行為について、次のすべての場合に限り、かつ、効果的な技術的手段の回避に対する法的保護の適切性または法的救済の有効性を損ねることのない限度に限り、適用することができる。

(i) 第(a)(i)項を実施する国内法は、第(d)項に定める各行為について、例外および制限の対象とすることができる。

(ii) 第(a)(ii)項を実施する国内法は、それを著作物、実演またはレコードへのアクセスをコントロールする効果的な技術的手段に適用するにあたり、第(d)(i)項、同(ii)項、同(iii)項、同(iv)項および同(vi)項に定める行為について、例外および制限の対象とすることができる。

(iii) 第(a)(ii)項を実施する国内法は、それを著作権または著作権に関連する権利を保護する効果的な技術的手段に適用するにあたり、第(d)(i)項および同(vi)項に定める行為について、例外および制限の対象とすることができる。

(f) 効果的な技術的手段とは、その通常の動作過程において、保護された著作物、実演、レコードもしくはその他保護された対象に対するアクセスをコントロールする、または、著作権もしくは著作権に関連する権利を保護する、技術、装置または部品をいう。

#### **第 18.4.8 条 (略)**

## シンガポール

### 第 16 章

#### 第 16.4.7 条<sup>157</sup>

(a) 各締約国は、著作者、実演家、レコードの製作者およびこれらの承継人がその権利の行使に関連して使用するものであり、かつ、これらの者の著作物、実演およびレコードについて許諾のない行為を制限する、効果的な技術的手段を回避することに対して、適切な法的保護および効果的な法的救済を提供するため、下記のいずれかにあたる者が、第 16.9.5 条に定める救済の責を負いかつそれに従う旨を定める。

(i) 保護された著作物、実演、レコードまたはその他の対象に対するアクセスをコントロールする効果的な技術的手段を、それと知りまたは知り得る相当の理由がありながら、許諾なく回避する者。

(ii) 次のいずれかにあたる装置、製品、部品を、製造、輸入、頒布、公衆に提供、供給または取引する者、あるいはサービスを公衆に提供、供給する者。

(A) 効果的な技術的手段を回避する目的をもって宣伝、広告または市販されるものの。

(B) 効果的な技術的手段を回避すること以外に、限られた商業上重要な目的または利用方法しか有しないもの。

(C) 効果的な技術的手段の回避を可能または容易にすることを主たる目的として、設計、製造または実行されるもの。

各締約国は、非営利の図書館、文書資料館、教育機関または公的な非商業的放送機関以外の者が、故意に、かつ商業的利益または私的な金銭的利得を得る目的をもって、かかるいずれかの行為に従事したと認められる場合、犯罪行為により有罪となることを定める。

(b) 本条において、効果的な技術的手段とは、その通常の動作過程において、保護された著作物、実演、レコードもしくはその他保護された対象に対するアクセスをコントロールする、または、著作権もしくは著作権に関連する権利を保護する、技術、装置または部品

---

<sup>157</sup> 訳者注：英文報告原文では「7」とのみ記載あるが、FTA 原文では「16.4.7」に該当するため「第 16.4.7 条」と記載。

をいう。

(c) 第 7(a)条は、効果的な技術的手段の回避を禁止することを各締約国に義務づけるが、家庭用電化製品、通信機器もしくはコンピュータ関連製品の設計またはこれらの部分および部品的设计ならびに選択が、特定の技術的手段に対応しなければならないことを、締約国に義務づけない。これらの設計及び選択が、特定の技術的手段に積極的に対応すべき旨の要件の欠如は、第 7(a)条の規定を実施するその締約国の国内法の違反との主張に対する抗弁とはならない。

(d) 各締約国は、本条を実施する法の違反が、その締約国の著作権および著作権に関連する権利に関する法のもとで発生し得るいかなる侵害からも独立したものである旨を定める。

(e) 各締約国は、第 7(a)(ii)条で禁止された、アクセスをコントロールするもので、かつ、下記第(i)号にあっては、保護された著作物における著作権もしくは著作権に関連する権利のあらゆる排他的権利を保護する効果的な技術的手段を回避する技術、製品、サービス、装置の例外を、次のすべての行為に限定する。ただし、これらの例外が、締約国が定める効果的技術的手段の回避に対する法的保護の適切性または法的救済の有効性を損ねるものではないことを条件とするものとする。

(i) 合法的に取得したコンピュータ・プログラムの複製に関する非侵害リバーズ・エンジニアリング行為であって、独立して作成されたコンピュータ・プログラムとその他のプログラムとの互換性を達成することを唯一の目的として、当該行為に従事する者が容易に入手できるものでないそのコンピュータ・プログラムの特定要素について、善意で行ったもの。

(ii) 善意による非侵害行為であって、著作物の複製、実演または展示を、合法的に取得し、かつ当該行為の許諾を得るために誠実に努力した、相当の資格を有する研究者が、情報のスクランプリングおよび非スクランプリングのための技術の欠陥および脆弱性の特定しおよび分析することを唯一の目的に必要な限度で行ったもの。

(iii) 未成年者の不適切なオンライン上のコンテンツへのアクセスを防止することを唯一の目的として、部品または部分を、技術、製品、サービスまたは装置に組み込むこと。ただし、当該技術、製品、サービスまたは装置それ自体が、第 7(a)(ii)条[を]実

施する国内法で禁止されていないことを条件とするもの]<sup>158</sup>とする。

(iv) 善意による非侵害行為であって、コンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークの所有者により、それらの試験、調査またはセキュリティの修正を唯一の目的として、許諾されるもの。

(f) 各締約国は、第 7(a)(i)条でいう禁止行為の例外を、第 7(e)条で列記する行為および次の行為に限定する。ただし、当該例外は、締約国が定める効果的な技術的手段の回避に対する法的保護の適切性または法的救済の有効性を損ねることのないものとする。

(i) 非営利の図書館、文書資料館または教育機関が行う、著作物へのアクセスであって、この他にそれを入手する方法がない場合に、それを取得するための決定を行うことを唯一の目的としたもの。

(ii) 非侵害行為であって、自然人のオンライン上の行為を反映した個人識別情報を秘密裏に収集または流布する機能を、自然人の著作物へのアクセス能力に全く影響を与えない方法で、特定および無効にすることを唯一の目的としたもの。

(iii) 特定の種類の著作物の非侵害的利用に対して、実際に生じまたは生じ得る悪影響が、立法または行政の手續において確実に立証された場合の、かかる特定の種類の著作物についての当該非侵害的利用。ただし、本号に従い採択された例外は、かかる手續が終結した日から 4 年を超えない期間、効力を有するものとする。

(g) 各締約国は、適法に許諾された行為であって、政府職員、政府系機関または政府の契約者が、法の執行、諜報、国防、安全保障または類似の行政目的のために行ったものについて、第 7(a)条で定める禁止行為の例外を定めることもできる。

#### 第 16.4.8 条 (略)

---

<sup>158</sup> 訳者注：英文報告原文では記載がないが、米国商務省国際通商局の([http://tcc.export.gov/static/text\\_final.pdf](http://tcc.export.gov/static/text_final.pdf))では、「provided that such technology, product, service or device itself is not prohibited under the measures implementing paragraph 7(a)(ii); and」とあるため、訳を補充。



(参考訳文(抄訳))

別紙 2

米国著作権法 技術的手段関連条文  
(抄訳)

第 12 章  
著作権保護および管理システム

- \* 1201. 著作権保護システムの回避
- \* 1202. 著作権管理情報の同一性
- \* 1203. 民事上の救済
- \* 1204. 刑事犯罪および刑罰
- \* 1205. 除外規定

第 1201 条 著作権保護システムの回避

- (a) 技術的手段の回避に関する違反
- (1)
- (A) 何人も、本編に基づき保護する著作物へのアクセスを効果的にコントロールする技術的手段を回避してはならない。前段に定める禁止は、本章の制定日から起算した 2 年間の終了時に施行する。
- (B) 第(C)号に基づく決定として、特定の種類の属する著作権のある著作物の使用者が、第(A)号に定める禁止によって、本編に基づく特定の種類の著作物をその著作権を侵害することなく使用できることについて不備に基づき不利益を受け、または続く 3 年間に不利益を受けるおそれがある場合、当該禁止は、当該使用者に適用しない。
- (C) 連邦議会図書館長は、第(A)号に定める 2 年間およびそれに続く各 3 年毎に、著作権局長が商務省情報通信担当長官補と協議しその見解について報告説明した上で行う勧告に基づき、第(B)号における特定の種類の属する著作権のある著作物の使用者が、第(A)号に定める禁止によって本編に基づき特定の種類の著作物をその著作権を侵害することなく使用できることについて、不利益を受けまたは続く 3 年間に不利益を受けるおそれがあるかにつき、規則制定手続において定める。当該規則制定を行うにあたり、当該図書館長は、次のすべてを審査する。
- (i) 著作権のある著作物の利用可能性。
  - (ii) 非営利の文書保管、保全および教育目的のための著作物の利用可能性。
  - (iii) 著作権のある著作物に使用される技術的手段の回避に対する禁止が、批評、解説、ニュース報道、学習指導、学術または研究に及ぼす影響。
  - (iv) 技術的手段の回避が、著作権のある著作物の市場または価値に及ぼす効果。
  - (v) その他連邦議会図書館長が、適切と思料する要素。

- (D) 連邦議会図書館長は、著作権のある著作物の種類のうち、連邦議会図書館長が第(C)号に基づき行う規則制定手続において、著作権のある著作物の使用者が侵害なくこれを利用するにつき不利益を受けまたは受ける可能性があり、第(A)号に含まれる禁止が当該使用者に対して当該種類の著作物については続く3年間は適用されるべきでないとして決定したものを、公表する。
  - (E) 第(B)号に基づく第(A)号で定める禁止の適用についての例外および第(C)号に基づき行われた規則制定手続における決定は、本項以外の本編の規定を執行するいかなる訴訟においても、抗弁とすることはできない。
- (2) 何人も、以下のいずれかに該当するあらゆる技術、製品、サービス、装置、部品もしくはそれらの一部を、製造、輸入、公衆に提供、供給またはその他の取引をしてはならない。
- (A) 本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避することを主たる目的として、設計または製造されるもの。
  - (B) 本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避する以外には、商業的に限られた重要な目的または用法しか有さないもの。
  - (C) 本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避するために使用することを知っている者またはこの者に協力する者によって販売されたもの。
- (3) 本節において、次の各用語は、それぞれ次の意味を有する。
- (A) 「技術的手段を回避する」とは、著作権者の許諾なく、スクランブルのかかっている著作物のスクランブルを解除し、暗号化された著作物の暗号を解除しまたはその他技術的手段を回避、迂回、除去、無効もしくは損壊することを意味する。
  - (B) 技術的手段が「著作物へのアクセスを効果的にコントロールする」とは、当該手段が、その通常の動作過程において、著作物へアクセスするために、著作権者の許諾を得て情報の入力、手続もしくは処理を必要とする場合を意味する。
- (b) 違反行為(追加的)
- (1) 何人も、以下のいずれかに該当するあらゆる技術、製品、サービス、装置、部品またはそれらの一部を製造、輸入、公衆に提供、供給またはその他の取引をしてはならない。
- (A) 著作物もしくはその一部に関する本編に基づく著作権者の権利を、効果的に保護する技術的手段が施す保護の回避を主たる目的として、設計または製造されるもの。
  - (B) 著作物またはその一部に関する本編に基づく著作権者の権利を、効果的に保護する技術的手段が施す保護を回避すること以外には、商業的に限られた重要な目的または用法しか有さないもの。

- (C) 著作物またはその一部に関する本編に基づく著作権者の権利を、効果的に保護する技術的手段が施す保護を回避するために使用することを、知っている者またはこの者に協力する者によって販売されたもの。
- (2) 本節において、次の各用語は、それぞれ次の意味を有する。
  - (A) 「技術的手段が施す保護を回避する」は、技術的手段を回避、迂回、除去、無効化または損壊することを意味する。
  - (B) 技術的手段が「本編に基づく著作権者の権利を効果的に保護する」とは、当該手段が、その通常の動作過程において、本編に基づく著作権者の権利の行使を防止、限定または制限する場合を意味する。
- (c) その他の権利等(影響を受けない)
  - (1) 本条のいかなる規定も、本編に基づく権利、救済、制限またはフェア・ユースを含む著作権侵害に対する抗弁に影響を及ぼさない。
  - (2) 本条のいかなる規定も、技術、製品、サービス、装置、部品もしくはそれらの一部に関する著作権侵害に対する代位もしくは寄与責任を拡大または縮小しない。
  - (3) 本条のいかなる規定も、家庭用電化製品、通信機器またはコンピュータ製品の一部もしくは部品または当該一部もしくは部品の組み込まれた製品が、第(a)節(2)または第(b)節(1)の禁止に該当しない限り、これらの設計もしくはこれらの一部および部品の設計ならびに選択が、特定の技術的手段に対応することを要請しない。
  - (4) 本条のいかなる規定も、家庭用電化製品、通信機器またはコンピュータ製品を使用した活動による言論もしくは報道の自由の権利を拡大または縮小しない。
- (d) 非営利の図書館、文書資料館および教育機関の例外
  - (1) 非営利の図書館、文書資料館または教育機関が、本編に基づき認められる行為に従事することを唯一の目的として、著作権のある著作物のコピーを取得するか否かを誠実に決定するためにのみ、商業的利用に供されている著作権のある著作物にアクセスすることは、第(A)節(1)(a)に違反しない。本項に基づきアクセスした著作物のコピーは、次のすべての制限を受ける。
    - (A) かかる誠実な決定を下すために必要な期間を超えて、保管してはならない。
    - (B) その他のいかなる目的にも使用してはならない。
  - (2)～(5) (略)
- (e) 法の執行、情報活動およびその他の政府活動

本条は、合衆国、州もしくは州の分権体の公務員、エージェントもしくは従業員または合衆国、州もしくは州の分権体との契約に基づき行為する者の、適法な権限に基づく調査、

保護、情報保全または情報活動を禁止するものではない。本節において、「情報保全」は、政府のコンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークの弱点を特定し対処するために行われる活動を意味する。

(f) リバース・エンジニアリング

- (1) 第(a)節(1)(A)の規定にかかわらず、コンピュータ・プログラムのコピーを使用する権利を適法に取得した者は、単独で作成されたコンピュータ・プログラムと他のプログラムとの互換性を達成するために必要であり、かつ回避に従事する者が従来容易に利用できなかったプログラムの要素を特定および分析することを唯一の目的として、当該特定行為および分析行為が、本編に基づく侵害にあたらない限りにおいて、当該取得したプログラムの特定の部分へのアクセスを効果的にコントロールする技術的手段を、回避することができる。
- (2) 第(a)節(2)および第(b)節の規定にかかわらず、第(1)項に基づく特定行為および分析行為を可能にするため、または、単独で作成されたコンピュータ・プログラムと他のプログラムとの互換性を可能にするために、本編に基づく侵害にあたらない限りにおいて、技術的手段を回避するためのまたは技術的手段が施す保護を回避するための技術的方法を、開発および利用することができる。

(3)(4) (略)

(g) 暗号化研究

(1) 定義

本節において、次の各用語は、それぞれ次の意味を有する。

- (A) 「暗号化研究」とは、暗号化技術の分野における知識を前進させるため、または、暗号化製品の開発を支援するため、著作権のある著作物に適用する暗号化技術の欠点および弱点の特定ならびに分析に必要な活動を意味する。
- (B) 「暗号化技術」とは、数式またはアルゴリズムを用いて、情報にスクランブルをかけることおよびスクランブルを解析することを意味する。

(2) 暗号化研究において許容される行為

第(a)節(1)(A)の規定にかかわらず、誠実な暗号化研究活動の過程において、発行著作物のコピー、レコード、実演または展示に適用された技術的手段を回避することは、次のすべてを満たす場合には、当該規定に違反しない。

- (A) 行為者が、当該発行著作物の暗号化されたコピー、レコード、実演または展示を適法に取得したこと。
- (B) 当該行為が、暗号化研究を行うために必要であること。
- (C) 行為者が、回避する前に、許諾を得るため誠実に努力をしたこと。
- (D) 当該行為が、本編に基づく侵害にあたらないまたは本条以外の適用法(第 18 編第

1030 条および 1986 年コンピュータ詐欺及び不正利用防止法によって修正された第 18 編の規定を含む)に違反しないこと。

(3) (略)

(4) 研究活動のための技術的方法の利用

第(a)節(2)の規定にかかわらず、次の行為は当該規定に違反しない。

(A) 第(2)項に定める誠実な暗号化研究活動をすることを唯一の目的として、技術的手段を回避するための技術的方法を開発および利用すること。

(B) 第(2)項に定める誠実な暗号化研究活動をする目的または他の者に第(2)項に定める誠実な暗号化研究活動を認証させる目的で、自己と協力して作業を行う他の者に技術的方法を提供すること。

(5) (略)

(h) 未成年者に関する例外

第(a)節を部品または一部分に適用するにあたり、裁判所は、下記のすべてに該当する技術、製品、サービスまたは装置への意図された組み込みおよび実際の組み込みが必要であるか否かを考慮することができる。

(1) それ自体は、本編の規定に違反しないこと。

(2) インターネット上の素材への未成年者によるアクセスを防止することを、唯一の目的とすること。

(i) 個人識別情報の保護

(1) 回避の許容

第(a)節(1)(A)の規定にかかわらず、次のすべての条件をみたす場合には、本編に基づき保護する著作物へのアクセスを効果的にコントロールする技術的手段を回避しても、当該規定に違反しない。

(A) 技術的手段またはその保護する著作物に、その保護する著作物にアクセスしようとする自然人のオンライン上の活動を反映した個人識別情報を、収集または流布する機能があること。

(B) 技術的手段またはその保護する著作物の通常動作の過程において、これらにアクセスしようとする者の個人識別情報が収集または流布されることをこの者に明示的に通知せず、かつこの者に当該収集もしくは流布を防止または制限する能力を提供せずに、当該自然人の個人識別情報が収集または流布されること。

(C) 回避行為が、第(A)号に掲げる機能を特定しおよび解除する効果のみを有し、かつ、著作物にアクセスしようとする者の権能に何ら効果を及ぼさないこと。

- (D) 回避行為が、保護著作物へアクセスしようとする自然人の個人識別情報の収集または流布を防止することを唯一の目的として行われ、かつその他のいかなる法にも反しないこと。

- (j) セキュリティ検査

- (1) 定義

本節において、「セキュリティ検査」は、コンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークの所有者または運営者の許諾を得て、セキュリティ上の欠点または弱点を誠実に検査、調査または補正することを唯一の目的として、当該コンピュータ、コンピュータ・システムまたはコンピュータ・ネットワークにアクセスすることを意味する。

- (2) セキュリティ検査における許容行為

第(a)節(1)(A)の規定にかかわらず、セキュリティ検査行為に従事することが、本編に基づく侵害または本条以外の適用法(第 18 編第 1030 条および 1986 年コンピュータ詐欺及び不正利用防止法によって修正された第 18 編の規定を含む)の違反にあたらない場合、この行為は、第(a)節(1)(A)の規定に違反しない。

- (3) (略)

- (4) セキュリティ検査のための技術的方法の利用

第(a)節(2)の規定にかかわらず、第(2)項で定めるセキュリティ検査行為を行うことを唯一の目的として技術的方法を開発、製造、頒布または利用することは、当該規定に違反しない。ただし、当該技術的方法が、他には何ら第(a)項(2)に違反しない場合に限る。

- (k) 特定のアナログ装置および特定の技術的手段

- (1) 特定のアナログ装置

- (A) 本章の制定日後 18 ヶ月を経過したときから、何人も、次のいずれかに該当するものについて製造、輸入、公衆に提供、供給またはその他の取引をしてはならない。

- (i) 自動制御コピー・コントロール技術に適合するものを除く、VHS 方式アナログ・ビデオ・カセット・レコーダー。

- (ii) 自動制御コピー・コントロール技術に適合するものを除く、8 ミリ方式アナログ・ビデオ・カセット・カムコーダー。

- (iii) 自動制御コピー・コントロール技術に適合するものを除く、ベータ方式アナログ・ビデオ・カセット・レコーダー。ただし、本要件は、本章の制定日後のいずれかの 1 暦年に 1,000 台の上記レコーダーが合衆国内で販売されるまで適用しないものとする。

- (iv) 自動制御コピー・コントロール技術に適合するものを除く、8ミリ方式アナログ・ビデオ・カセット・レコーダー(アナログ・ビデオ・カセット・カムコーダーを除く)。ただし、本要件は、本章の制定日後のいずれかの1暦年に20,000台の上記レコーダーが合衆国内で販売されるまで適用しないものとする。
  - (v) 自動制御コピー・コントロール技術に適合するものを除く、NTSC方式ビデオ入力を用いて収録するアナログ・ビデオ・カセット・レコーダーであつて、かつ第(i)段ないし第(iv)段に含まれないもの。
- (B) 本章の制定日を効力発生日として、何人も、下記のいずれかに該当するものについて製造、輸入、公衆に提供、供給またはその他の取引をしてはならない。
- (i) 従来自動制御コピー・コントロール技術に適合してきたものを、適合しないものとするため、当該制定日後に設計が変更された、VHS方式アナログ・ビデオ・カセット・レコーダーまたは8ミリ方式アナログ・ビデオ・カセット・レコーダー。
  - (ii) 従来フォーライン・カラーストライプ・コピー・コントロール技術に適合していたものを、適合しないものとするため、上記制定日後に設計が変更された、VHS方式アナログ・ビデオ・カセット・レコーダーまたは8ミリ方式アナログ・ビデオ・カセット・レコーダー(8ミリ方式アナログ・ビデオ・カセット・カムコーダーでないもの)。

VHS方式アナログ・ビデオ・カセット・レコーダーまたは8ミリ方式アナログ・ビデオ・カセット・レコーダーを従来製造または販売してこなかった製造業者は、本章の制定日後に製造するレコーダーの初期設計を、フォーライン・カラー・ストライプ・コピー・コントロール技術に適合させ、かつ以後継続してフォーライン・カラーストライプ・コピー・コントロール技術に適合させなければならない。本号において、アナログ・カセット・レコーダーの通常再生モードを用いて参照用のディスプレイ機器に表示したときに、その画面の一部分に画面を見えなくするような可視の線を用いた表示を示す信号を記録した場合は、当該レコーダーが、フォーライン・カラーストライプ・コピー・コントロール技術に「適合する」ものとする。

(2)～(4) (略)

(5) 違反

本節第(1)項の違反は、本条第(b)節(1)の違反として扱う。本節第(2)項の違反は、本章第1203条(c)(3)(A)における「回避行為」とみなす。

## 第1202 著作権管理情報の同一性 (略)

### 第1203条 民事上の救済

(a) 民事訴訟

第1201条または第1202条の違反によって損害を被った者は、当該違反についての適切な

連邦地方裁判所に民事訴訟を提起することができる。

(b) 裁判所の権限

第(a)節に基づき提起された訴訟において、裁判所は、以下を行うことができる。

- (1) 違反を防止または抑制するために合理的と判断する条件において、暫定的および終局的差止命令を発することができる。ただし、いかなる場合においても、憲法修正第1条が保障する言論の自由または報道の自由に対する事前抑制を行ってはならないものとする。
- (2) 違反者として嫌疑がかけられている者が占有もしくは支配下に置く装置または製品であって、違反行為に関連したと信じる相当の理由があるものにつき、合理的と判断した条件において、訴訟係属中いつでも差押えを命じることができる。
- (3) 第(c)節に基づく損害賠償を、付与することができる。
- (4) その裁量によって、合衆国もしくはその公務員以外の当事者によるまたはこの当事者に対する費用の回復を、認めることができる。
- (5) その裁量によって、相当な弁護士費用を、勝訴当事者に付与することができる。
- (6) 違反を認定する終局判決または審判の一部として、違反行為に関連した装置もしくは製品であって、違反者が占有もしくは支配下に置きまたは第(2)項に基づき差し押さえを受けたものにつき、治癒的改変または破壊することを命じることができる。

(c) 損害賠償の付与

(1) 総則

本編に別段の定めがある場合を除き、第1201条または第1202条に違反した者は、以下のいずれかの責を負う。

(A) 第(2)項に定める、現実的損害賠償および違反者の追加的利益。

(B) 第(3)項に定める、法定損害賠償。

(2) 現実的損害賠償

裁判所は、訴えを提起した当事者が、違反の結果として自ら被った現実的損害および違反者が受けた利益であって、違反に起因し、かつ現実的損害に算入されていないものにつき、当該当事者が終局判決前のいずれかの時点において選択した場合、これらを、訴えを提起した当事者に付与する。

(3) 法定損害賠償

(A) 訴えを提起した当事者は、終局判決前はいつでも、第1201条違反における回避行為、装置、製品、部品、提供またはサービスの提供ごとにつき、合計で200ド



ル以上または 2,500 ドル以下であって、裁判所が正当と判断した額の法定損害賠償を選択できる。

- (B) 訴えを提起した当事者は、終局判決前はいつでも、各第 1202 条違反について合計で 2,500 ドル以上または 25,000 ドル以下の、法定損害賠償を選択することができる。

(4) 再度の違反行為

別の第 1201 条または第 1202 条の違反についての終局判決後 3 年以内に同一の行為者が同条に違反したことについて、損害を被った当事者が立証責任を果たし、裁判所がこれを認定した場合、裁判所が正当と判断する額の限りにおいて、損害賠償の額を 3 倍まで加重することができる。

(5) 善意の違反行為

(A) 総則

違反者が、自己の行為が違反にあたることを知らず、かつ違反であると信じる理由がなかったことについて、違反者が立証責任を果たし、裁判所がこれを認定した場合、裁判所は、その裁量において、損害賠償の額を減額または免除することができる。

(B) 非営利の図書館、文書資料館、教育機関または公共放送事業者

(i) 定義

本号において、「公共放送事業者」は、第 118 条(g)において付与する意味を有する。

(ii) 総則

非営利の図書館、文書資料館、教育機関または公共放送事業者の場合において、当該図書館、文書資料館、教育機関または公共放送事業者が、自己の行為が違反行為にあたることを知らず、かつ違反であると信じる理由がなかったことにつき、当該図書館、文書資料館、教育機関または公共放送事業者が立証責任を果たし、裁判所がこれを認定した場合、裁判所は、損害賠償を免除する。

## 第 1204 条 刑事犯罪および刑罰

(a) 総則

故意かつ商業的利益または私的な経済的利得を目的として、第 1201 条または第 1202 条に違反する者は、次のとおりに処する。

- (1) 初犯については、500,000 ドル以下の罰金もしくは 5 年以下の禁固またはその双方。
- (2) 再犯については、1,000,000 ドル以下の罰金もしくは 10 年以下の禁固またはその

双方。

(b) 非営利の図書館、文書資料館、教育機関または公共放送事業者に係る制限

第(a)節は、非営利の図書館、文書資料館、教育機関または公共放送事業者(第 118 条(g)の定義に従う)には適用しない。

(c) 出訴期限

本条に基づく刑事手続は、訴訟原因の発生後 5 年以内にこれを開始しない限り、行うことはできない。

**第 1205 条 除外規定 (略)**

#### IV コンテンツの技術的手段に係る各国法制度調査研究(韓国編)



KIM & CHANG  
金・張 法律事務所

(110-720) ソウル特別市鐘路区内資洞223世洋ビル  
Website: www.kimchang.com E-mail: lawkim@kimchang.com  
Tel: +82-2-3703-1114 Fax: +82-2-737-9091-3

2010年1月15日

西村あさひ法律事務所  
弁護士 川合 弘造 先生  
弁護士 大向 尚子 先生

金・張法律事務所  
弁護士 韓相郁

題目：技術的保護措置制度の調査の件

貴所の調査依頼に対し、調査・検討した結果を以下のとおりご報告申し上げます。

－記－

**1. コンテンツの技術的手段に関する国際ルール**

**(1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)**

いずれも締結されています。WIPO 著作権条約は2004年6月24日に発効され、WIPO 実演・レコード条約は2009年3月18日に発効されました。

**(2) 韓国における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容**

- (i) 韓-チリ FTA、韓-シンガポール FTA、韓-EFTA FTA、韓-ASEAN FTA が発効中ですが、これら FTA には技術的手段に関する規定が存在しません。
- (ii) 韓-米 FTA、韓-インド CEPA、韓-EU FTA が署名・交渉妥結され、これら FTA のうち、韓-米 FTA、韓-EU FTA に技術的手段に関する規定が存在します。韓-米 FTA 協定文の知的財産権に関する部分は Exhibit1、韓-EU FTA 協定文の知的財産権に関する部分は Exhibit2 をご参考下さい。

● 技術的保護措置に関連する韓-米FTAの特徴

- 技術的保護措置に利用統制措置 (Copy Control Measures or Use Control Measures) 及びアクセス統制措置 (Access Control Measures) がいずれも含まれていません<sup>159</sup>。
- 著作者、実演者及び音盤製作者が自身の権利行使に関連して使用しているその著作物、実演及び音盤に関連した許諾を受けていない行為を制限する効果的な技術措置を迂回する行為を規制します(韓-米 FTA Article 18.4.7. (f))。
- 規制される行為は、(1) 効果的なアクセス統制型技術措置を、知っていながら、または知るだけの合理的な根拠をもって、許諾なしに迂回する場合 (Article 18.4.7. (a) (i))、(2) 効果的な技術措置の迂回を主目的として考案された装置、商品または部品を製造、輸入、配布、公衆に提議、提供または密売したり、これに関連したサービスを公衆に提議したり提供する行為です (Article 18.4.7. (a) (ii))。
- アクセス統制関連の技術措置迂回行為自体も違反行為の一つとして規定します。しかし、利用統制措置の迂回行為自体は適用対象に含めていません (Article 18.4.7. (a) (i), (ii) 参照)<sup>160</sup>。
- 技術措置迂回行為などの違反行為が著作権などの侵害とは別個の訴訟原因であることを規定されております。(Article 18.4.7. (c))
- 違反行為に対しては、民事責任及び刑事責任が問われ、民事的救済には差押さえを含む暫定措置、法定損害賠償制度、訴訟費用支払い命令、廃棄命令などが含まれており (Article 18.10.13.)、刑事責任に関しては、違反行為が重大な故意または、故意にそして商業的利益または私的な金銭的利益を得る目的で行われた場合は刑事処罰をするようにしています (Article 18.4.7. (a))。
- 技術的保護措置違反にならない特定の例外事由を設けています。(1) コンピュータプログラムの互換性のためのリバースエンジニアリング、(2) 暗号化技術の欠陥または脆弱性を調査、研究するための行為、(3) 未成年者保護のために有害物へのアクセスを遮断するための行為、(4) コンピュータシステムの保安状態を点検、調査、補完するための行為、(5) オンライン上の個人活動に関する情報を収集、流布する機能を確認して防止するための行為、(6) 法執行、情報収集、安全保障のための公務員の合法的行為、(7) 非営利図書館、記録保存所、教育機関などが購入を決定するために該当資料にアクセスする行為など (Article 18.4.7. (d) (i)-(vii))。これに加えて、非

<sup>159</sup> 韓-米 FTA 上の技術的保護措置は下記の Article 18.4.7. (f) の強調部分の解釈上、利用統制型技術措置 (利用統制措置) 及びアクセス統制型技術措置 (アクセス統制措置) に分けてみる事ができます。以下、本報告書では主に利用統制措置、アクセス統制措置などと簡略に称します。

[Effective technological measure means any technology, device, or component that, in the normal course of its operation, controls access to a protected work, performance, phonogram, or other protected subject matter, or protects any copyright or any rights related to copyright]

<sup>160</sup> アメリカの Digital Millennium Copyright Act の規定内容と類似したものと理解されます。

侵害利用を実質的証拠によって確認できる場合、行政的、立法的手続を通じて3年を周期に例外事項を追加導入できるようにしています(Article 18.4.7.(d)(viii))。

● **技術的保護措置に関連する韓-EU FTAの特徴**

- 技術的保護措置に利用統制措置及びアクセス統制措置がいずれも含まれています(Article 10.12.3.)。
- 技術措置迂回行為に対して十分な法的保護を提供するよう規定しております(Article 10.12.1.)。
- 技術措置迂回行為のための装置などを製造、輸入、配布、販売、貸与、販売や貸与のための広告、営利目的のための所持等をするを違反行為として規定しております(Article 10.12.2.)。
- 韓-EU FTA 上、技術的保護措置に対する民事的救済、刑事的制裁と関連しては韓-米 FTA とは異なり著作権と別途の救済手段を予定せず、知的財産権一般の救済手段が技術的保護措置にも与えられると解釈されます。民事的救済手段では差し迫った侵害を防止するための予防措置(Article 10.46.)、知的財産権を侵害する物品の廃棄などの是正措置(Article 10.47.)、禁止命令(Article 10.48.)、損害賠償(Article 10.50.)、刑事的制裁手段では商業的規模の故意的な侵害の場合に懲役刑及び/又は罰金刑言渡を含む罰則を設けることを規定しており(Article 10.59.)、著作権侵害に使われた道具の没収なども合わせて規定しております(Article 10.60.)。
- 国内規範とローマ条約、ベルヌ条約、WIPO 著作権条約、WIPO 実演・音盤条約などの国際条約の実体規定に符合する限度内で技術的保護措置に対する制限と例外を設定できるようにしています(Article 10.12.4.)。

(iii) その他、韓-カナダ FTA、韓-メキシコ FTA、韓-GCC FTA、韓-オーストラリア FTA、韓-ニュージーランド FTA、韓-ペルー FTA は交渉が進行中であり、韓-日本 FTA、韓-中国 FTA、韓-MERCOSUR FTA、韓-トルコ FTA、韓-ロシア BEPA、韓-コロンビア FTA、韓-イスラエル FTA、韓-SACU FTA は交渉準備、共同研究が進行中です。

**2. コンテンツの技術的手段に関する法令等**

**(1) 該当する法令等**

**(i) 著作権法、Exhibit3**

**(ii) 旧コンピュータプログラム保護法、Exhibit4**

ただし、同法は2009年7月23日付で廃止され、その後コンピュータプログラムも著作権法の改正(2009年4月23日改正、2009年7月23日施行)によって著作権法によって保護されることになりました。

### (iii) オンラインデジタルコンテンツ産業発展法、Exhibit5

ご参考までに、オンラインコンテンツ製作者を保護するために制定された本法上、オンラインデジタルコンテンツ製作とは「情報通信網で使用するためにデジタル形態の原情報を加工したりデジタル形態以外の原情報をデジタル方式に転換又は加工すること」をいい、アナログ資料をデジタル化したりデジタル資料を他の形態に加工する者に適用される法であり、アナログ形態の原資料をデジタル化した者には著作権法上の保護が与えられませんが、本法による保護を考慮して考えることができます。オンラインコンテンツ製作者が著作権法による保護を受ける場合には著作権法が本法に優先し保護を適用されるため(第 21 条)、補充的な法律であると言えます。

## (2) 法令等の規制内容

### (a) 規制対象技術(定義及び対象技術の具体例等)

#### (i) 著作権法

著作権その他この法によって保護される権利に対する侵害行為を効果的に防止または抑制するためにその権利者や権利者の同意を得た者が適用する技術的措置を技術的保護措置と定義しています(法第 2 条第 28 号)<sup>161</sup>。

Copy Control のみを対象とするのか、Access Control も対象とするのか、法の規定のみでは明確ではありません。現行の著作権法の解釈上、Access Control は規制対象

<sup>161</sup> その他、著作権法上技術的保護措置に関する規定又はこれと類似したり隣接した規定には次のようなものがある。最近新設された条項である著作権法第 104 条は、「他者の間でコンピュータなどを利用して著作物などを伝送させることを主な目的とするオンラインサービス提供者(「特殊な類型のオンラインサービス提供者」)は、権利者の要請がある場合、当該著作物などの不法な伝送を遮断する技術的な措置など必要な措置をとらなければならない」と規定しています。上記法条の「技術的な措置」が著作権法上の技術的保護措置に該当するのか混乱をもたらす面がありますが、著作権法上の技術的保護措置は、権利者またはその委任を受けた者が著作物に適用する技術である反面、第 104 条の技術的な措置は、権利者の要請がある場合に著作物流通の媒介者(特殊な類型の OSP)によって施行されるという点で区別されると考えられます。第 104 条の技術的な措置には、フィルタリング、ウォーターマーキング、特徴点基盤コンテンツ識別技術などが上げられています。文化体育観光部は告示第 2007-24 号を通して著作権法第 104 条の適用を受ける特殊な類型の OSP を 1)個人又は法人のコンピュータなどに保存された著作物などを公衆が利用できるようアップロードした者に商業的利益又は利用便宜を提供する OSP、2)個人又は法人のコンピュータなどに保存された著作物などを公衆がダウンロードできるよう機能を提供しダウンロードする者が費用を支払う形態で事業をする OSP、3)P2P 技術を基盤に個人又は法人のコンピュータなどに保存された著作物などをアップロードしたりダウンロードできる機能を提供して商業的利益を得る OSP、4)個人又は法人のコンピュータ等に著作物などを検索して伝送できるプログラムの提供を主な目的とする OSP などと告示したところがあります。特殊な類型の OSP が著作権法第 104 条による必要な措置をしない場合、文化体育観光部長官は当該 OSP に 3 千万ウォン以下の過怠金を賦課することができます(著作権法第 142 条第 1 項)。



ではないという学説が提示されています<sup>162</sup>。

技術的保護措置標準化に関する事項は、文化体育観光部長官が告示するものとなっていますが(法第2条の2)、現在まで告示された内容はありません。

## (ii) 旧コンピュータプログラム保護法

「技術的保護措置」とは、プログラムに関する識別番号・固有番号の入力、暗号化その他、本法による権利を効果的に保護する核心技術または装置などを通じてプログラム著作権を保護する措置をいうと定義しています(旧法第2条第9号)。

Copy Control のみを対象とするのか、Access Control も対象とするのか、法の規定のみでは明確ではありません。関連判例は存在しますが、Access Control が明示的に規制されるのかに対する明確な判断はありませんでした(3.(1)(i)で後述)。

## (iii) オンラインデジタルコンテンツ産業発展法

「技術的保護措置」とは、オンラインデジタルコンテンツ製作者が本法によって保護される利益の侵害を効果的に防止するために適用する技術または装置をいうと定義しています(法第2条第10号)。

# (b) 規制対象製品及び対象プログラム等

## (i) 著作権法

技術的保護措置を除去・変更・迂回するなど無力化することを主な目的とする技術・サービス・製品・装置またはその主要部品が規制の対象です(法第124条第2項)。

## (ii) 旧コンピュータプログラム保護法

技術的保護措置を相当に無力化する機器・装置・部品など及び技術的保護措置を無力化するプログラム及び技術的保護措置を無力化する技術が規制の対象です(旧法第30条第2項)。

## (iii) オンラインデジタルコンテンツ産業発展法

技術的保護措置の回避・除去または変更(以下「無力化」という)を主な目的とする技術・サービス・装置またはその主要部品が規制の対象です(法第18条第2項)。

<sup>162</sup> アクセス統制措置に対しては、回避行為自体もまた規制する一部外国の立法例とは異なり、技術的保護措置の無力化行為自体については言及がないので、利用統制措置のみを規律するものとみられるという点を最も大きな理由としてあげている。丁相朝編、「著作権法註解」(博英社、2007)、p. 1170、林源善(元文化観光部著作権課長)執筆部分

(c) 規制対象行為

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

(i) 著作権法

①、②、③(輸出行為を除く)、⑤の行為が規制対象(法第 124 条第 2 項)。残りの行為は規制対象から除外(特に⑥の回避行為は規制対象でないことにご留意下さい。このような立法をとる理由については、技術的保護措置を回避して著作物を不法複製、伝送などに利用すれば、ただちに著作権侵害として擬律できるためという説明があります。)

(ii) 旧コンピュータプログラム保護法

⑥の回避行為自体を規制対象として定めています<sup>163</sup>。機器・装置・部品などに対しては①、③(輸出行為を除く)及び公衆に譲渡・貸与または流通する行為が規制対象です。技術的保護措置を無力化するプログラムに対しては、伝送、配布する行為が規制対象です。技術的保護措置を無力化する技術に対しては、提供する行為が規制対象です(以上、旧法第 30 条第 2 項)。

(iii) オンラインデジタルコンテンツ産業発展法

①、②、③(輸出行為を除く)及び譲渡・貸与または伝送したり、譲渡・貸与のために展示する行為が規制対象です。残りの行為は規制対象ではありません(法第 18 条第 2 項)。

<sup>163</sup> 利用統制型の技術的保護措置を回避する行為自体は、技術的保護措置を回避して著作物を不法に利用する場合、ただちに著作権侵害として擬律することが可能であるため、著作権法とは異なり迂回行為自体を規制する旧コンピュータプログラム保護法では、利用統制措置だけでなくアクセス統制措置もまた規制の対象とするとみることができるという見解が提示されています。

### (3) 除外行為

#### (a) コンテンツの技術的手段に関する規定の適用除外、例外、制限規定等の存否・内容

##### (i) 著作権法

適用除外、例外、制限規定などに対する規定は特別に存在しません<sup>164</sup>。

ただし、著作権法施行令で、文化体育観光部長官が技術的保護措置の無効化禁止に対する例外事由に関する施策を樹立・施行するものとなっていますが、現在までに告示された内容はありませぬ(施行令第1条の2第2項第4号)。

##### (ii) 旧コンピュータプログラム保護法

下記(1)～(6)に該当する時には、技術的保護措置の無力化行為自体が禁止されないものと例外が設定されています(旧法第30条第1項但書)。(1)旧法第10条の規定によるプログラムの同一性を変更する場合、(2)旧法第12条の各号の1に該当して複製・使用する場合、(3)旧法第14条の規定によるプログラムの使用者が必要な範囲内で当該複製物を複製する場合、(4)正当な権原によって使用する者が他のプログラムとの互換性を維持するために必要な場合、(5)正当な権原による最終使用者からプログラムの修正、補完の要請を受けた場合、(6)正当な権原によって使用する者が研究、教育などの目的でプログラムと関連した暗号化分析をするために必要な場合

##### (iii) オンラインデジタルコンテンツ産業発展法

技術的保護措置の研究・開発のために技術的保護措置を無力化する装置または部品を製造する場合には、法律違反ではないものと規定(法第18条第2項但書)。

#### (b) 著作権法にコンテンツの技術的手段に関する規定が存在する場合の技術的手段回避の禁止規定と権利制限規定との関係

##### (i) 著作権法

明確な規定は存在しません。ただし、技術的保護措置自体が著作権法によって保護される権利に対する侵害行為を効果的に防止または抑制するために適用する措置として定義されており、技術措置の迂回行為自体を著作権法で禁止せず、技術的保護措置の制限と例外を著作権と別途に設定していない立法態度は、技術措置の迂回行為の目

<sup>164</sup> 著作権法上、技術的保護措置の規定に特に別途の制限と例外に対する規定がないことは、著作権に対する制限と例外に該当する場合、技術的保護措置にも法的保護の例外を認めることであるという趣旨で解釈する見解が存在します。林源善(元文化観光部著作権課長)、「実務者のための著作権法」(韓国著作権委員会、2009)、377頁。これに比べて技術的保護措置関連行為禁止に対する例外を著作権侵害に対する例外と別途に規定した旧コンピュータプログラム保護法は著作権法で認める著作権と技術的保護措置の牽連性を完全に否定する立法態度を取ったものと評価しております。「著作物に対する使用権及び接近権の問題に関する研究」(文化観光部、2003)、p. 46. [韓国著作権法学会(ホ・フィソン会長)研究用役報告書]。

の上、著作権に対する例外と制限が適用されるものなので、著作権侵害につながらない場合、このような目的の迂回行為は許容することにするという解釈によって、著作権によって保護されない範囲では技術的保護措置を回避する行為も法に違反すると解釈されない可能性が高いです。

#### (ii) 旧コンピュータプログラム保護法

上記(3)(a)(ii)でみたように、法律に列挙された一定の場合、技術的保護措置の無力化行為自体は違法でないと明示的に規定しています(旧法第 30 条第 1 項但書参照)。

#### (iii) オンラインデジタルコンテンツ産業発展法

明確な規定は存在しません。ただし、技術的保護措置自体がオンラインデジタルコンテンツ産業発展法によって保護される権利を保護するための措置として定義されているため(法第 2 条第 10 号)、同法によって保護されない範囲では技術的保護措置を回避する行為も法に違反すると解釈されない可能性が高いです。

#### (4) 救済措置

##### (a) 救済措置の内容(民事的救済及び刑事的制裁)

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

##### (i) 著作権法

**民事的救済:** 技術的保護措置に反する行為に対する救済のための特別な規定は存在せず、従って違反行為別に救済手段が規定されてもいません。

技術的保護措置の無力化技術の提供などは、著作権侵害見なし行為として(法第 124 条第 2 項)、著作権侵害行為に対する救済手段一般規定が適用されます。侵害者に対し侵害の停止請求が可能です。侵害のおそれがある者に対し侵害の予防または損害賠償の担保請求が可能です(法第 123 条第 1 項)。上記請求と共に侵害行為により作られた物品の廃棄またはそれ以外の必要な措置を請求することが可能です(法第 123 条第 2 項)。権利侵害に対する損害賠償請求が可能です(法第 125 条)。

技術的保護措置の無力化を主な目的とする技術、サービス、製品、装置、部品などを提供した者は、技術的保護措置の無力化技術の提供などを直接原因とした責任以外にも、その技術、サービスなどの提供を受けて著作権を侵害した者と著作権侵害に対する共同不法行為者としての責任を負う可能性があります。

**刑事的制裁:**違反行為別に処罰を異にしていません。業としてまたは営利を目的に侵害見なし行為をした者に対して 3 年以下の懲役または 3 千万ウォン以下の罰金を科したり、これを併科することができます(法第 136 条第 2 項第 5 号)。

## (ii) 旧コンピュータプログラム保護法

**民事的救済:**民事的救済手段に対する規定が存在せず、著作権法とは異なり、権利侵害見なし行為としてもみないので、著作権侵害行為に対する民事的救済手段を活用することができるか疑問があります<sup>165</sup>。

**刑事的制裁:**違反行為別に処罰を異にしていません。業や営利目的を要件とせず、単純に旧コンピュータプログラム保護法第 30 条に違反すれば、5 年以下の懲役または 5 千万ウォン以下の罰金に処すか、これを併科することができるように定めています(旧法第 46 条第 1 項第 3 号)。

## (iii) オンラインデジタルコンテンツ産業発展法

**民事的救済:**違反行為別に救済手段が規定されてはいません。技術的保護措置侵害行為の中止や予防及びその違反行為による損害賠償を請求することができる規定しています。技術的保護措置の無力化技術などの提供者がオンラインコンテンツ侵害行為者と共同不法行為者としての責任を負う可能性があります。

**刑事的制裁:**違反行為別に処罰を異にしていません。業や営利目的を要求せず、単純にオンラインデジタルコンテンツ産業発展法第 18 条第 2 項本文の規定に違反した者は、1 年以下の懲役または 2 千万ウォン以下の罰金に処すようにしています(第 22 条第 1 項)。

## (b) (a)の救済措置の請求主体

### (i) 著作権法

**民事的救済:**著作権または著作権法によって保護される権利を有している者が請求可能。

**刑事的制裁:**親告罪としていません(法第 140 条第 2 号)。

### (ii) 旧コンピュータプログラム保護法

**刑事的制裁:**技術的保護措置の無力化行為自体(旧法第 30 条第 1 項)に対しては親告罪

<sup>165</sup> 一部の見解は、この点を理由に旧コンピュータプログラム保護法上の技術的保護措置関連の規定は著作権の保護と直接的な牽連関係のない独自の制度であるとみている。

としており、無力化サービスの提供等(旧法第 30 条第 2 項)に対しては親告罪として  
いません(旧法第 48 条)。

### (iii) オンラインデジタルコンテンツ産業発展法

**民事的救済:** 技術的保護措置侵害行為によって自身の営業に関する利益が侵害され  
た、または侵害されるおそれがある者。

**刑事的制裁:** 親告罪(法第 22 条第 2 項)。

## (c) 違反機器等の輸出入にかかる水際措置又は違反抑止のための行政措置の有無・内容

### (i) 著作権法

文化体育観光部長官、特別市長、広域市長、道知事、特別自治道知事、市長、郡  
守、区庁長などは、関係公務員に著作物などの技術的保護措置を無力化するために製  
作された機器、装置、情報及びプログラムに対する回収、廃棄または削除措置をさせ  
ることができるように規定しています(法第 133 条第 1 項)。

オンラインサービス提供者により技術的保護措置を無力化するプログラムまたは情  
報が伝送される場合、文化体育観光部長官がオンラインサービス提供者に対して技術  
的保護措置無力化プログラムの複製・伝送者に対する警告やこれの削除または伝送中  
断を命じることができるようにしています。この警告を 3 回以上受けた複製・伝送者  
が技術的保護措置無力化プログラムを伝送し続けた場合、オンラインサービス提供者  
に該当複製・伝送者のアカウントを 6 ヶ月以内の期間を定めて停止することを命じる  
ことができ、技術的保護措置無力化プログラムの削除または伝送中断命令が 3 回以上  
下された掲示板に対しては、文化体育観光部長官がオンラインサービス提供者に 6 ヶ  
月以内の期間に該当掲示板サービスの全部または一部の停止を命じることができます  
(法第 133 条の 2)。

### (ii) 旧コンピュータプログラム保護法

文化体育観光部長官は、技術的保護措置を無力化させるために製作された機器、装  
置、部品、プログラムなどを発見したときには、関係公務員をしてこれを回収、削  
除、廃棄させることができます(旧法第 34 条第 1 項)。

### (iii) オンラインデジタルコンテンツ産業発展法

特別な規定はありません。



**(5) いわゆる「無反応機器」規制**

**いわゆる「無反応機器」に対する法令、規則、指令等による規制の有無・内容**

韓国では特に「無反応機器」という法的概念を使用していない結果、これに対する特別な法の規制も存在しないため、そのような特定事案が問題になる場合、技術的保護措置の無力化規制一般論に照らして評価されるものと思料されます。

**3. 裁判例、執行状況、被害状況等**

**(1) コンテンツの技術的手段に関する裁判例**

**(i) 刑事判決**

**-ソニーモッドチップ判決(具体的な内容は Exhibit6)**

旧コンピュータプログラム保護法を適用した大法院判決であるソニー判決では、SONY Play Station2 に適用された Access Control がゲームプログラムの物理的複製を防ぐことはできませんが、通常の装置やプログラムではアクセスコードの複製が不可能であり、仮に不法にゲームプログラムを複製したとしても、PS2 を通じたプログラムの実行が不可能であるだけに、アクセスコードはゲームプログラムの物理的複製を防ぐのと同様な効果をもつ技術的保護措置に該当し、これを回避する機器であるモッドチップを装着することによってアクセスコードのないゲーム CD の実行を可能にしたことは、コンピュータプログラム保護法上、技術的保護措置の無力化に該当すると判断。

**-任天堂判決(具体的な内容は Exhibit7)**

旧コンピュータプログラム保護法を適用した下級審である任天堂判決では、ソニーモッドチップ事件と同様に、R4 カートリッジが任天堂社が採択した技術的保護措置を無力化する機器に該当すると認めて、被告人に実刑を宣告。

**(ii) 民事判決**

事例はありません。

**(2) コンテンツの技術的手段に関する執行状況**

上記判決以外に知られている執行状況はありません。

**(3) コンテンツの技術的手段に関する被害状況**

統計が集計されたものではありません。

**4. 技術動向の調査**

**(1) コンテンツの技術的手段に関する技術動向**

アクセス統制措置として放送信号などの暗号化、プログラムに対する識別番号・固

有番号の入力などが使用されており、利用統制措置として DVD に適用される Contents Scrambling System などが使用されています。

## (2) 電子透かし等、コンテンツの技術的手段に関する新たな技術

特別に浮彫りにされたり、論議されている新しい技術は見つけることが難しいです。

## (3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況

韓国の政策当局は技術的保護措置の無力化への対応に非常に積極的なので、新技術に対する法的対応も遅れなくなされるものと思料されます。

## 5. 各国内の議論(規制に対する賛否・改正動向等)

### (1) コンテンツの技術的手段に関する現行規制に対する議論

ソニーモッドチップ判決(Exhibit6)及び任天堂判決(Exhibit7)参照。ソニーモッドチップ事件では技術的保護措置関連の規定がプログラムの複製物を正当な権原によって所持、使用する者がプログラムの滅失などに備えて複製するなど、個人的にプログラム著作物を利用する行為まで制限することで、憲法上の権利侵害であるという被告人の主張がありましたが、正当な権原を持った利用者が滅失などに備えて、プログラムを複製する目的で技術的保護措置を回避することは、旧プログラム保護法で明示的に許容される明示的な例外事由に該当するため、複製物の滅失や毀損に備えた複製だけをした場合、旧プログラム保護法の規定によっても直ちに許容されることであり、モッドチップの場合、著作権侵害という主な目的以外の上記のような副次的な機能だけを強調する抗弁は受け入れ難いという理由で被告人の主張を排斥しました<sup>166</sup>。任天堂事件では、R4 などの無力化機器が音楽、映画などのデータを使用するのに必要だという面で不法ではないという主張がありましたが、著作権を侵害する不法プログラムを使用できるようにすることがその無力化機器の主な目的かどうかの基準によって、被告人の主張を排斥しました。一角では、韓-米 FTA の批准などで将来導入される可能性のあるアクセス統制措置に対しては、著作権法が権利として付与しない行為を統制するための技術が含まれる可能性があり、そのようなアクセス統制措置が保護される場合、著作権制限制度の趣旨が没却し得るという点で、その導入に疑問を提起する見解が提示されています。

<sup>166</sup> 旧法第 14 条第 1 項は「プログラムの複製物を正当な権原により所持、使用する者はその複製物の滅失、毀損又は変質などに備えるために必要な範囲内で当該複製物を複製できる」と規定しているところ、上記の規定により使用者が必要な範囲内で複製する場合、技術的保護措置の無力化禁止例外規定に該当するというものです(旧コンピュータプログラム保護法第 30 条第 3 号)。



## (2) コンテンツの技術的手段に関する規制に対する業界からの要望状況

権利者側の業界からの要望としては、技術的保護措置に関する法的保護を強化することを期待しているものと把握されます。ただし、政府は技術的保護措置が採択されたコンテンツを正当に保有する消費者の互換性確保などの側面で、技術的保護措置の標準化を追求していますが、一部業界では技術的保護措置の標準化は経済主体の自律性を損ない得るという点で反対する雰囲気があります。

## (3) 法改正の動向・内容

韓-米 FTA が批准されこれが履行されることになれば、次のような改正が伴われると期待されます。(1)アクセス統制措置に対する事項を明示的に著作権法で規定し、アクセス統制措置に対しては直接的な迂回行為自体を禁止する、(2)刑事責任の範囲に関して、現行の著作権法は業としてまたは営利を目的とする場合に刑事処罰の対象にしていますが、韓-米 FTA では刑事処罰は重大な故意または、故意にそして商業的利益または私的な金銭的利益を得る目的としているので、この規定内容に従う、(3)現行の著作権法は技術的保護措置の場合にも著作権に対する一般的な例外規定がそのまま適用されるという解釈論があるが、韓-米 FTA では技術措置保護の例外事由を別途に定めているため、相当な制度の変化が予想されます。

以 上

Exhibit 1

CHAPTER EIGHTEEN  
INTELLECTUAL PROPERTY RIGHTS

**ARTICLE 18.4: COPYRIGHT AND RELATED RIGHTS**

7. (a) In order to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that authors, performers, and producers of phonograms use in connection with the exercise of their rights and that restrict unauthorized acts in respect of their works, performances, and phonograms, each Party shall provide that any person who:

- (i) knowingly, or having reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, phonogram, or other subject matter; or
- (ii) manufactures, imports, distributes, offers to the public, provides, or otherwise traffics in devices, products, or components, or offers to the public or provides services, that:
  - (A) are promoted, advertised, or marketed by that person, or by another person acting in concert with, and with the knowledge of, that person, for the purpose of circumvention of any effective technological measure;
  - (B) have only a limited commercially significant purpose or use other than to circumvent any effective technological measure; or
  - (C) are primarily designed, produced, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure,

shall be liable and subject to the remedies set out in Article 18.10.13.<sup>167</sup> Each Party shall provide for criminal procedures and penalties to be applied when any person, other than a nonprofit library, archive, educational institution, or public noncommercial broadcasting entity, is found to have engaged willfully and for purposes of commercial advantage or private financial gain in any of the foregoing activities. Such criminal procedures and penalties shall include the application to such activities of the remedies and authorities listed in subparagraphs (a), (b), and (e) of Article 18.10.27 as applicable to infringements, *mutatis mutandis*.

- (b) In implementing subparagraph (a), neither Party shall be obligated to require that the design of, or the design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as the product

---

<sup>167</sup> In addition, each Party shall provide that any person who, unknowingly and without reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, phonogram, or other subject matter shall be liable and subject at least to the remedies set out in subparagraphs (a), (c), and (d) of Article 18.10.13.

does not otherwise violate any measures implementing subparagraph (a).

- (c) Each Party shall provide that a violation of a measure implementing this paragraph is a separate cause of action, independent of any infringement that might occur under the Party's law on copyright and related rights.
- (d) Each Party shall confine exceptions and limitations to measures implementing subparagraph (a) to the following activities, which shall be applied to relevant measures in accordance with subparagraph (e):<sup>168</sup>
  - (i) noninfringing reverse engineering activities with regard to a lawfully obtained copy of a computer program, carried out in good faith with respect to particular elements of that computer program that have not been readily available to the person engaged in those activities, for the sole purpose of achieving interoperability of an independently created computer program with other programs;
  - (ii) noninfringing good faith activities, carried out by an appropriately qualified researcher who has lawfully obtained a copy, unfixed performance, or display of a work, performance, or phonogram and who has made a good faith effort to obtain authorization for such activities, to the extent necessary for the sole purpose of research consisting of identifying and analyzing flaws and vulnerabilities of technologies for scrambling and descrambling of information;
  - (iii) the inclusion of a component or part for the sole purpose of preventing the access of minors to inappropriate online content in a technology, product, service, or device that itself is not prohibited under the measures implementing subparagraph (a)(ii);
  - (iv) noninfringing good faith activities that are authorized by the owner of a computer, computer system, or computer network for the sole purpose of testing, investigating, or correcting the security of that computer, computer system, or computer network;
  - (v) noninfringing activities for the sole purpose of identifying and disabling a capability to carry out undisclosed collection or dissemination of personally identifying information reflecting the online activities of a natural person in a way that has no other effect on the ability of any person to gain access to any work;
  - (vi) lawfully authorized activities carried out by government employees, agents, or contractors for the purpose of law enforcement, intelligence, essential security, or similar governmental purposes;
  - (vii) access by a nonprofit library, archive, or educational institution to a work, performance, or phonogram not otherwise available to it, for the sole purpose of making acquisition decisions; and
  - (viii) noninfringing uses of a work, performance, or phonogram in a particular class of works, performances, or phonograms when an actual or likely

---

<sup>168</sup> Either Party may request consultations with the other Party to consider how to address, under subparagraph (d), activities of a similar nature that a Party identifies after the date this Agreement enters into force.

adverse impact on those noninfringing uses is demonstrated in a legislative or administrative proceeding by substantial evidence, provided that any limitation or exception adopted in reliance on this clause shall have effect for a renewable period of not more than three years from the date the proceeding concludes.

- (e) The exceptions and limitations to measures implementing subparagraph (a) for the activities set forth in subparagraph (d) may only be applied as follows, and only to the extent that they do not impair the adequacy of legal protection or the effectiveness of legal remedies against the circumvention of effective technological measures:
  - (i) Measures implementing subparagraph (a)(i) may be subject to exceptions and limitations with respect to each activity set forth in subparagraph (d).
  - (ii) Measures implementing subparagraph (a)(ii), as they apply to effective technological measures that control access to a work, performance, or phonogram, may be subject to exceptions and limitations with respect to activities set forth in subparagraph (d)(i), (ii), (iii), (iv), and (vi).
  - (iii) Measures implementing subparagraph (a)(ii), as they apply to effective technological measures that protect any copyright or any rights related to copyright, may be subject to exceptions and limitations with respect to activities set forth in subparagraph (d)(i) and (vi).
- (f) **Effective technological measure** means any technology, device, or component that, in the normal course of its operation, controls access to a protected work, performance, phonogram, or other protected subject matter, or protects any copyright or any rights related to copyright.

#### **ARTICLE 18.10: ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS**

13. In civil judicial proceedings concerning the acts described in paragraphs 7 and 8 of Article 18.4, each Party shall provide that its judicial authorities shall, at the least, have the authority to:

- (a) impose provisional measures, including seizure of devices and products suspected of being involved in the prohibited activity;
- (b) provide an opportunity for the right holder to elect award of either actual damages it suffered or pre-established damages;
- (c) order payment to the prevailing right holder at the conclusion of civil judicial proceedings of court costs and fees, and reasonable attorney's fees, by the party engaged in the prohibited conduct; and
- (d) order the destruction of devices and products found to be involved in the prohibited activity.

Neither Party may make damages available under this paragraph against a nonprofit library, archives, educational institution, or public noncommercial broadcasting entity that sustains the burden of proving that it was not aware and had no reason to believe that its acts constituted a prohibited activity.

Exhibit 2

CHAPTER TEN  
INTELLECTUAL PROPERTY

**ARTICLE 10.12: PROTECTION OF TECHNOLOGICAL MEASURES**

1. Each Party shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that such person is pursuing that objective.

2. Each Party shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purpose, of devices, products or components, or the provision of services which:

- (a) are promoted, advertised or marketed for the purpose of circumvention of;
- (b) have only a limited commercially significant purpose or use other than to circumvent; or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating of,

any effective technological measures.

3 For the purposes of this Agreement, technological measure means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorized by the right holder of any copyright or any right related to copyright as provided for by each Party's legislation. Technological measures shall be deemed effective where the use of a protected work or other subject matter is controlled by the right holders through the application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject matter, or a copy control mechanism, which achieves the objective of protection.

4. Each Party may provide for exceptions and limitations to measures implementing paragraphs 1 and 2 in accordance with its legislation and the relevant international agreements referred to in Article 10.5.

**ARTICLE 10.46: PROVISIONAL AND PRECAUTIONARY MEASURES**

1. Each Party shall ensure that the judicial authorities may, at the request of the applicant, issue an interlocutory injunction intended to prevent any imminent infringement of an intellectual property right, to forbid, on a provisional basis and subject, where appropriate, to a recurring penalty payment where provided for by its legislation, the continuation of the alleged infringements of that right, or to make such continuation subject to the lodging of guarantees intended to ensure the compensation of the right holder. An interlocutory injunction may also be

issued against an intermediary<sup>169</sup> whose services are being used by a third party to infringe copyright, related rights, trademarks or geographical indications.

2. An interlocutory injunction may also be issued to order the seizure of the goods suspected of infringing an intellectual property right so as to prevent their entry into or movement within the channels of commerce.

3. In the case of an infringement committed on a commercial scale, each Party shall ensure that, if the applicant demonstrates circumstances likely to endanger the recovery of damages, the judicial authorities may order the precautionary seizure of the movable and immovable property of the alleged infringer, including the blocking of bank accounts and other assets.

#### **ARTICLE 10.47: CORRECTIVE MEASURES**

1. Each Party shall ensure that the competent judicial authorities may order, at the request of applicant and without prejudice to any damages to the right holder by reason of the infringement, and without compensation of any sort, destruction of goods that they have found to be infringing an intellectual property right or any other measures to definitely remove those goods from the channels of commerce. If appropriate, the competent judicial authorities may also order destruction of materials and implements principally used in the creation or manufacture of those goods.

2. The judicial authorities shall order that those measures be carried out at the expense of the infringer, unless particular reasons are invoked for not doing so.

3. In considering a request for corrective measures, the need for proportionality between the seriousness of the infringement and the remedies ordered as well as the interests of third parties shall be taken into account.

#### **ARTICLE 10.48: INJUNCTIONS**

1. Each Party shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement.

2. Where provided for by law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Each Party shall also ensure that right holders are in a position to apply for an injunction against intermediaries<sup>170</sup> whose services are being used by a third party to infringe copyright, related rights, trademarks or geographical indications.

---

<sup>169</sup> For the purposes of this paragraph, the scope of intermediary is determined in each Party's legislation, but shall include those who deliver or distribute infringing goods, and also where appropriate, include online service providers.

<sup>170</sup> For the purposes of this paragraph, the scope of intermediary is determined in each Party's legislation, but shall include those who deliver or distribute infringing goods, and also where appropriate, include online service providers.

#### **ARTICLE 10.50: DAMAGES**

1. Each Party shall ensure that when the judicial authorities set damages:
  - (a) they shall take into account all appropriate aspects, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the right holder by the infringement; or
  - (b) as an alternative to subparagraph (a), they may, in appropriate cases, set the damages as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorization to use the intellectual property right in question.
2. Where the infringer did not knowingly, or with reasonable ground to know, engage in infringing activity, the Parties may provide that the judicial authorities may order the recovery of profits or the payment of damages which may be pre-established.
3. In civil judicial proceedings, each Party, at least with respect to works, phonograms, and performances protected by copyright or related rights, and in cases of trademark counterfeiting, may establish or maintain pre-established damages, which shall be available on the election of the right holder.

#### **ARTICLE 10.54: SCOPE OF CRIMINAL ENFORCEMENT**

Each Party shall provide for criminal procedures and penalties to be applied at least in cases of willful trademark counterfeiting and copyright and related rights<sup>171</sup> piracy on a commercial scale.

#### **ARTICLE 10.59: PENALTIES**

For the offences referred to in Article 10.54, each Party shall provide for penalties that include sentences of imprisonment and/or monetary fines that are effective, proportionate and dissuasive.

#### **ARTICLE 10.60: CONFISCATION**

1. For the offences referred to in Article 10.54, each Party shall provide that its competent authorities shall have the authority to order confiscation and/or destruction of all counterfeit trademark goods or pirated copyright goods, materials and implements predominantly used in the creation of counterfeit trademark goods or pirated copyright goods and the assets derived from, or obtained directly or indirectly, through the infringing activity.

---

<sup>171</sup> The term “related rights” is defined by each Party in accordance with its international obligations.

2. Each Party shall ensure that the counterfeit trademark goods and pirated copyright goods that have been confiscated under this Article shall, if not destroyed, be disposed outside the channels of commerce, under the condition that the goods are not dangerous for the health and security of persons.
3. Each Party shall further ensure that confiscation and destruction under this Article shall occur without compensation of any kind of the defendant.
4. Each Party may provide that its judicial authorities have the authority to order the confiscation of assets the value of which corresponds to that of such assets derived from or obtained directly or indirectly through the infringing activity.



Exhibit 3

[改正 2009 年 4 月 22 日、施行 2009 年 7 月 23 日  
改正 2009 年 3 月 25 日、施行 2009 年 9 月 26 日<sup>172)</sup>

著作権法<sup>173)</sup> 関連条文

第 1 条(目的)

この法は著作者の権利とこれに隣接する権利を保護し著作物の公正な利用を図ることにより文化及び関連産業の向上発展に尽くすことを目的とする。

第 2 条(定義)

この法で使用する用語の意味は次の通りである。

10. 「伝送」とは、公衆送信のうち公衆の構成員が個別的に選択した時間と場所にて接近できるように著作物等を利用に提供することをいい、それに伴い行われる送信を含む。
22. 「複製」とは、印刷・写真撮影・複写・録音・録画その他の方法によって有形物に固定したり、有形物としてさらに制作することをいい、建築物の場合には、その建築のための模型または設計図書によってこれを施工することを含む。
28. 「技術的保護措置」とは著作権その他この法によって保護される権利に対する侵害行為を効果的に防止または抑制するためにその権利者や権利者の同意を得た者が適用する技術的措置をいう。
32. 「公衆」とは、不特定多数人(特定他数人を含む)をいう。

第 2 条の 2(著作権保護に関する施策の樹立等)

第 1 項： 文化体育観光部長官は、この法の目的を達成するために、次の各号の施策を樹立・施行することができる。

1. 著作権の保護及び著作物の公正な利用環境作りのための基本政策に関する事項
2. 著作権の認識拡散のための教育及び広報に関する事項
3. 著作物等の権利管理情報及び技術的保護措置の政策に関する事項

第 2 項： 第 1 項による施策の樹立・施行に必要な事項は、大統領令で定める。

<sup>172)</sup> 二回の法改正により改正日と施行日の前後が入れ替わっているが、本調査項目とは特に関連がない。

<sup>173)</sup> 法律の韓国語テキストは以下のサイトで確認できる。  
[http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK\\_TYPE=LAW\\_BON&LAW\\_ID=A0715&PROM\\_NO=09785&PROM\\_DT=20090731&](http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK_TYPE=LAW_BON&LAW_ID=A0715&PROM_NO=09785&PROM_DT=20090731&)

#### 第 104 条(特殊な類型のオンラインサービス提供者の義務等)

第 1 項： 他者の間でコンピュータを利用して著作物等を伝送させることを主な目的とするオンラインサービス提供者（以下「特殊な類型のオンラインサービス提供者」という）は、権利者の要請がある場合、該当著作物等の不法な伝送を遮断する技術的な措置など必要な措置をとらなければならない。この場合、権利者の要請及び必要な措置に関する事項は大統領令で定める。

第 2 項： 文化体育観光部長官は、第 1 項の規定による特殊な類型のオンラインサービス提供者の範囲を定めて告示することができる。

#### 第 123 条(侵害の停止など請求)

第 1 項： 著作権その他この法によって保護される権利(第 25 条・第 31 条・第 75 条・第 76 条・第 82 条及び第 83 条の規定による補償を受ける権利を除く。以下この条で同様)を有する者は、その権利を侵害する者に対して侵害の停止を請求することができる、その権利を侵害するおそれがある者に対して侵害の予防または損害賠償の担保を請求することができる。

第 2 項： 著作権その他この法によって保護される権利を有する者は、第 1 項の規定による請求をする場合に、侵害行為によって作られた物品の廃棄やその他の必要な措置を請求することができる。

第 3 項： 第 1 項及び第 2 項の場合またはこの法による刑事の起訴があるときには、裁判所は原告または告訴人の申請によって担保を提供させて、または提供させずして、臨時に侵害行為の停止または侵害行為によって作られた物品の差押えその他の必要な措置を命じることができる。

第 4 項： 第 3 項の場合に、著作権その他この法によって保護される権利の侵害がないという趣旨の判決が確定したときには、申請者はその申請によって発生した損害を賠償しなければならない。

#### 第 124 条(侵害と見なす行為)

第 2 項： 正当な権利なしに著作権その他この法によって保護される権利の技術的保護措置を除去・変更・迂回するなど無力化することを主な目的とする技術・サービス・製品・装置またはその主要部品を提供・製造・輸入・譲渡・貸与または伝送する行為は、著作権その他この法によって保護される権利の侵害と見なす。

#### 第 125 条(損害賠償の請求)

第 1 項： 著作財産権その他この法によって保護される権利(著作人格権及び実演者の人格権を除く)を有する者(以下「著作財産権者等」という)が、故意または過失によって権利を侵害した者に対してその侵害行為によって自己が被った損害の賠償を請求する場合に、その権利を侵害した者がその侵害行為によって利益を得たときには、その利

益の額を著作財産権者等が被った損害の額と推定する。

第 2 項： 著作財産権者等が故意または過失によってその権利を侵害した者に対してその侵害行為によって自己が被った損害の賠償を請求する場合に、その権利の行使によって通常得ることのできる金額に相当する額を著作財産権者等が被った損害の額としてその損害賠償を請求することができる。

第 3 項： 第 2 項の規定にかかわらず、著作財産権者等が被った損害の額が第 2 項の規定による金額を超える場合には、その超過額に対しても損害賠償を請求することができる。

第 4 項： 登録されている著作権・出版権・プログラム排他的発行権・著作隣接権またはデータベース製作者の権利を侵害した者は、その侵害行為に過失があるものと推定する。

### 第 133 条 (不法複製物の回収・廃棄及び削除)

第 1 項： 文化体育観光部長官、特別市長・広域市長・道知事・特別自治道知事または市長・郡守・区庁長(自治区の区庁長をいう)は、著作権その他この法によって保護される権利を侵害する複製物(情報通信網を通じて伝送される複製物は除く)または著作物等の技術的保護措置を無力化するために製作された機器・装置・情報及びプログラムを発見したときには、大統領令で定めた手続及び方法によって関係公務員をしてこれを回収・廃棄または削除させることができる。

### 第 133 条の 2 (情報通信網を通じた不法複製物等の削除命令等)

第 1 項： 文化体育観光部長官は、情報通信網を通じて著作権やその他この法によって保護される権利を侵害する複製物または情報、技術的保護措置を無力化するプログラムまたは情報(以下「不法複製物等」という)が伝送される場合に、韓国著作権委員会(以下「委員会」という)の審議を経て大統領令で定めるところによってオンラインサービス提供者に次の各号の措置をとるよう命じることができる。

1. 不法複製物等の複製・伝送者に対する警告
2. 不法複製物等の削除または伝送の中断

第 2 項： 文化体育観光部長官は、第 1 項第 1 号による警告を 3 回以上受けた複製・伝送者が不法複製物等を伝送した場合、委員会の審議を経て大統領令で定めるところによってオンラインサービス提供者に 6 ヶ月以内の期間を定めて該当複製・伝送者のアカウント[オンラインサービス提供者が利用者を識別・管理するために使用する利用権限アカウント(E-Mail 専用アカウントは除く)をいい、該当オンラインサービス提供者が付与した他のアカウントを含む]を停止するよう命じることができる。

第 4 項： 文化体育観光部長官は、オンラインサービス提供者の情報通信網に開設された掲示板(「情報通信網利用促進及び情報保護等に関する法律」第 2 条第 1 項第 9 号の掲示板のうち商業的利益または利用の便宜を提供する掲示板をいう。以下同様)のう

ち、第1項第2号による命令が3回以上下された掲示板で、該当掲示板の形態、掲示される複製物の量や性格などに照らして該当掲示板が著作権などの利用秩序を深刻に毀損すると判断される場合には、委員会の審議を経て大統領令で定めるところによってオンラインサービス提供者に6ヶ月以内の期間を定めて該当掲示板サービスの全部または一部の停止を命じることができる。

### 第133条の3(是正勧告等)

第1項： 委員会はオンラインサービス提供者の情報通信網を調査して不法複製物等が伝送された事実を発見した場合には、これを審議してオンラインサービス提供者に対して次の各号に該当する是正措置を勧告することができる。

1. 不法複製物等の複製・伝送者に対する警告
2. 不法複製物等の削除または伝送の中断
3. 反復的に不法複製物等を伝送した複製・伝送者のアカウントの停止

第3項： 委員会はオンラインサービス提供者が第1項による勧告に従わない場合には、文化体育観光部長官に第133条の2第1項及び第2項による命令をするよう要請することができる。

### 第136条(権利の侵害罪)

第2項： 次の各号のいずれか一つに該当する者は、3年以下の懲役または3千万ウォン以下の罰金に処したり、これを併科することができる。

5. 業としてまたは営利を目的に第124条第2項の規定によって侵害行為と見なす行為を行った者

### 第140条(告訴)

この章の罪に対する公訴のためには、告訴がなければならない。ただし、次の各号のいずれかに該当する場合には、この限りでない。

1. 営利のために常習的に第136条第1項及び第136条第2項第3号に該当する行為を行った場合
2. 第136条第2項第2号・第5号及び第6号、第137条第1号ないし第4号、第6号及び第7号と第138条第5号の場合
3. 営利を目的に第136条第2項第4号の行為を行った場合(第124条第1項第3号の場合には、被害者の明示的意思に反して処罰することができない)

### 第142条(過料)

第2項： 次の各号のいずれか一つに該当する者には1千万ウォン以下の過料を課す。

3. 第133条の2第1項・第2項及び第4項による文化体育観光部長官の命令を履行しない者

[改正 2009 年 8 月 6 日、施行 2009 年 8 月 7 日]

### 著作権法施行令<sup>174</sup>関連条文

#### 第 1 条の 2

第 2 項： 法第 2 条の 2 第 1 項第 3 号によって文化体育観光部長官が樹立・施行する著作物、実演・音盤・放送またはデータベース(以下「著作物等」という)の権利管理情報及び技術的保護措置に関する施策には、次の各号の事項が含まれなければならない。

1. 権利管理情報の統合的管理のための標準体系開発に関する事項
2. 権利管理情報の除去・変更などの禁止に対する例外事由に関する事項
3. 技術的保護措置の標準化に関する事項
4. 技術的保護措置の無力化禁止に対する例外事由に関する事項
5. その他著作物等の権利管理情報及び技術的保護のために文化体育観光部長官が必要と認める事項

---

<sup>174</sup> 施行令の韓国語テキストは以下のサイトで確認できる。

[http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK\\_TYPE=LAW\\_BON&LAW\\_ID=B2534&PROM\\_NO=21676&PROM\\_DT=20090806&](http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK_TYPE=LAW_BON&LAW_ID=B2534&PROM_NO=21676&PROM_DT=20090806&)

Exhibit 4

[2009年4月22日に改正、2009年7月23日に施行された著作権法によって廃止]

旧コンピュータプログラム保護法<sup>175</sup>関連条文

第1条(目的)

この法はコンピュータプログラム著作物の作者の権利、その他にコンピュータプログラム著作物と関連した権利を保護し、その公正な利用を図って当該関連産業と技術を振興することにより国民経済の健全な発展に尽くすことを目的とする。

第2条(定義)

この法で使用する用語の定義は次の通りである。

5. 「公表」とは、プログラムを発行したり、これを公衆に提示する行為をいう。
- 5の2. 「配布」とは、原プログラムまたはその複製物を公衆に対価をもらってまたはもらわずに譲渡または貸与する行為をいう。
6. 「発行」とは、公衆の需要に応じるためにプログラムを複製・配布する行為をいう。
7. 「伝送」とは、公衆が受信したり利用できるようにするために情報通信の方法によってプログラムを送信したり利用に提供する行為をいう。
9. 「技術的保護措置」とは、プログラムに関する識別番号・固有番号の入力、暗号化その他この方法による権利を効果的に保護する核心技術または装置等を通じてプログラム著作権を保護する措置をいう。

第10条(同一性維持権)

プログラム作者は、次の各号の1に該当する場合を除いては、そのプログラムの題号・内容及び形式の同一性を維持する権利を持つ。

1. 特定のコンピュータ以外には使用できないプログラムを他のコンピュータに使用できるようにするために必要な範囲内での変更
2. プログラムを特定のコンピュータにより効果的に使用できるようにするために必要な範囲内での変更
3. プログラムの性質またはその使用目的に照らしてやむを得ないと認められる範囲内での変更

<sup>175</sup> 法律の韓国語テキストは以下のサイトで確認できる。  
[http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK\\_TYPE=LAW\\_BON&LAW\\_ID=A0714&PROM\\_NO=08852&PROM\\_DT=20080229](http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK_TYPE=LAW_BON&LAW_ID=A0714&PROM_NO=08852&PROM_DT=20080229)



## 第 12 条(プログラム著作権の制限)

次の各号の 1 に該当する倍には、その目的上必要な範囲内で公表されたプログラムを複製または配布することができる。ただし、プログラムの種類・用途、プログラムのうち複製された部分が占める比重及び複製の部数等に照らしてプログラム著作権者の利益を不当に害する場合には、この限りでない。

1. 裁判または捜査のために複製する場合
2. 「初・中等教育法」、「高等教育法」による学校及び他の法律の規定により設立された教育機関(上級学校入学のための学力が認められたり、学位を授与する教育機関に限る)にて教育を担当する者が授業過程に提供する目的で複製または配布する場合
3. 「初・中等教育法」による学校及びこれに準ずる学校の教育目的のための教科用図書に掲載するために複製する場合
4. 家庭などの限定された場所で個人的な目的(営利を目的とする場合を除く)で複製する場合
5. 「初・中等教育法」、「高等教育法」による学校及びこれに準ずる学校の 入学試験その他の学識及び技能に関する試験または検定の目的(営利を目的とする場合を除く)で複製または配布する場合
6. プログラムの基礎をなすアイデア及び原理を確認するためにプログラムの機能を調査・研究・試験する目的で複製する場合(正当な権原によってプログラムを使用する者が当該プログラムを使用中の場合に限る)

## 第 14 条(プログラム使用者による複製等)

第 1 項： プログラムの複製物を正当な権原によって所持・使用する者は、その複製物の滅失・毀損または変質等に備えるために必要な範囲内で当該複製物を複製することができる。

第 2 項： プログラムの複製物を所持・使用する者は、当該プログラムの複製物を所持・使用する権利を喪失したときには、そのプログラム著作権者の特別な意思表示がない限り、第 1 項の規定により複製したものを廃棄しなければならない。ただし、プログラムの複製物を所持・使用する権利を当該複製物が滅失することにより喪失した場合にはこの限りでない。

## 第 30 条(技術的保護措置の侵害などの禁止)

第 1 項： 誰であれ正当な権原なしに技術的保護措置を回避、除去、損壊などの方法で無力化(以下「技術的保護措置の無力化」という)してはならない。ただし、次の各号の 1 に該当する場合にはこの限りでない。

1. 第 10 条の規定によるプログラムの同一性を変更する場合

2. 第 12 条各号の 1 に該当して複製使用する場合
3. 第 14 条の規定によるプログラム使用者が必要な範囲内で複製する場合
4. 正当な権原によって使用する者が他のプログラムとの互換性を維持するために必要な場合
5. 正当な権原による最終使用者からプログラムの修正・補完の要請を受けた場合
6. 正当な権原によって使用する者が研究・教育などの目的でプログラムに関連した暗号化分析をするために必要な場合

第 2 項： 誰であれ相当に技術的保護措置を無力化する機器・装置・部品などを製造・輸入したり公衆に譲渡・貸与または流通してはならず、技術的保護措置を無力化するプログラムを送送・配布したり技術的保護措置を無力化する技術を提供してはならない。

### 第 34 条 (不正複製物等の回収措置等)

第 1 項： 文化体育観光部長官は次の各号のいずれか一つに該当するプログラム、情報または機器などを発見したときには、関係公務員をしてこれを回収・削除・廃棄させることができる。

1. 正当な権原を持たない者が流通または使用提供など営利を目的に複製したプログラム
2. 削除
3. プログラム著作権を侵害する方法で製作されたプログラムをその事情を知りつつ取得した者が業務上使用するプログラム
4. 削除
5. 技術的保護措置の無力化を行うために製作された機器、装置、部品、プログラム等

第 2 項： 第 1 項の規定によって関係公務員が当該プログラムまたは機器などを回収したときには、その所有者または占有者に回収証を交付しなければならない。

第 3 項： 文化体育観光部長官は第 1 項の規定により関係公務員が回収などをするにあたり技術的諮問及びこれに準ずる支援が必要なときには、第 35 条の規定によるコンピュータプログラム保護委員会またはプログラム著作権保護に関連した協会等の団体に協力を要請することができる。

第 4 項： 第 1 項及び第 2 項の規定によって回収などの処分をする関係公務員は、その権限を表示する証票を携帯し、これを関係人に提示しなければならない。

### 第 34 条の 2 (情報通信網を通じた不正複製物等に対する是正命令)

第 1 項： 文化体育観光部長官は次の各号のプログラムまたは情報が情報通信網を通じて伝送された場合に、第 35 条の規定によるコンピュータプログラム保護委員会の審議を経て、オンラインサービス提供者をして大統領で定めるところによってその取扱の



拒否・停止または制限など(以下「拒否等」という)をするように命じることができる。  
ただし、第 34 条の 3 第 3 項の規定によってコンピュータプログラム保護委員会が是正命令を要請する場合には、コンピュータプログラム保護委員会の審議を省略することができる。

1. 正当な権原を持たない者が伝送したプログラム
2. プログラム著作権を侵害する情報
3. 技術的保護措置を無力化するプログラム及び情報

第 2 項： 文化体育観光部長官は第 1 項の規定による命令の対象となるオンラインサービス提供者に事前に意見提出の機会を与えなければならない。

第 3 項： 「行政手続法」第 22 条第 4 項ないし第 6 項及び第 27 条の規定は、第 2 項の意見提出に関してこれを準用する。

#### **第 46 条(罰則)**

第 1 項： 次の各号のいずれか一つに該当する者は、5 年以下の懲役または 5 千万ウォン以下の罰金に処すか、これを併科することができる。

1. 第 29 条第 1 項の規定に違反した者
2. 第 29 条第 4 項第 1 号または第 2 号の規定に該当する行為をした者
3. 第 30 条の規定に違反した者

#### **第 48 条(告訴)**

第 46 条第 1 項(第 3 号の場合のうち第 30 条第 2 項の規定に違反した場合を除く)及び同条第 3 項第 2 号第 4 号の罪は、プログラム著作権者またはプログラム排他的発行者等の告訴があつてはじめて公訴を提起することができる。

Exhibit 5

[改正 2009 年 5 月 22 日、施行 2009 年 8 月 23 日]

オンラインデジタルコンテンツ産業発展法<sup>176</sup> 関連条文

**第 1 条(目的)**

この法はオンラインデジタルコンテンツ産業の発展に必要な事項を定めることにより、オンラインデジタルコンテンツ産業の基盤を造成し、その競争力を強化して国民生活の向上と国民経済の健全な発展に尽くすことを目的とする。

**第 2 条(定義)**

この法で用いる用語の定義は次の通りである。

1. 「デジタルコンテンツ」とは、符号・文字・音声・音響・イメージまたは映像等で表現された資料または情報で、その保存及び利用において効用を高められるよう電子の形態で製作または処理されたものをいう。
2. 「オンラインデジタルコンテンツ」とは、情報通信網利用促進及び情報保護等に関する法律第 2 条第 1 項第 1 号の規定による情報通信網(以下「情報通信網」という)で使用されるデジタルコンテンツをいう。
7. 「複製」とは、オンラインデジタルコンテンツを電子的媒体など有形物に固定したり、有形物としてさらに製作することをいう。
8. 「伝送」とは、情報通信網を通じて利用者が個別に選択した時間と場所で受信したり利用できるようにオンラインデジタルコンテンツを送信したり利用に供することをいう。
10. 「技術的保護措置」とは、オンラインデジタルコンテンツ製作者がこの法によって保護される利益の侵害を効果的に防止するために適用する技術または装置をいう。

**第 18 条(禁止行為等)**

第 1 項: 誰であれ正当な権限なく、他人が相当な努力をもって製作して表示したオンラインコンテンツの全部または相当な部分を複製または伝送する方法で競争事業者の営業に関する利益を侵害してはならない。ただし、オンラインコンテンツを最初に製作して表示した日から 5 年が経過した時にはこの限りでない。

<sup>176</sup> 法律の韓国語テキストは以下のサイトで確認できる。

[http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK\\_TYPE=LAW\\_BON&LAW\\_ID=A1748&PROM\\_NO=09708&PROM\\_DT=20090522&](http://likms.assembly.go.kr/law/jsp/Law.jsp?WORK_TYPE=LAW_BON&LAW_ID=A1748&PROM_NO=09708&PROM_DT=20090522&)

第 2 項： 誰であれ正当な権限なく、第 1 項本文の行為を効果的に防止するためにオンラインコンテンツ製作者やそれから許諾を受けた者がデジタルコンテンツに適用した技術的保護措置の回避・除去または変更(以下「無力化」という)を主な目的とする技術・サービス・装置またはその主要部品を提供・輸入・製造・譲渡・貸与または伝送したり譲渡・貸与のために展示する行為をしてはならない。ただし、技術的保護措置の研究・開発のために技術的保護措置を無力化する装置または部品を製造する場合にはこの限りでない。

#### **第 19 条 (損害賠償請求等)**

第 1 項： 第 18 条第 1 項本文及び第 2 項本文の規定に違反する行為(以下「違反行為」という)によって自身の営業に関する利益が侵害された、または侵害されるおそれがある者は、その違反行為の中止や予防及びその違反行為による損害の賠償を裁判所に請求することができる。

第 2 項： 裁判所は、損害の発生は認められるが損害額を算定するのが困難な場合には、弁論の全趣旨及び証拠調査結果を参酌して相当な損害額を認めることができる。

#### **第 21 条 (他の法律との関係)**

オンラインコンテンツ製作者が「著作権法」の保護を受ける場合には「著作権法」がこの法に優先して適用される。

#### **第 22 条 (オンラインコンテンツの複製等の罪)**

第 1 項： 第 18 条第 1 項本文の規定に違反してオンラインコンテンツ製作者の営業に関する利益を顕著に侵害した者または同条第 2 項本文の規定に違反した者は、1 年以下の懲役または 2 千万ウォン以下の罰金に処す。

第 2 項： 第 1 項の罪は、第 19 条の規定による損害賠償請求等を行える者の告訴があつてはじめて公訴を提起することができる。

Exhibit 6

ソニーモッドチップ判決

大法院 2006 年 2 月 24 日言渡 2004 ド 2743 判決

被告人：イム〇〇

関連条文：コンピュータプログラム保護法第 2 条第 9 号、第 30 条、第 46 条第 1 項第 3 号

[判断内容の一部]

1. コンピュータプログラム保護法第 2 条第 9 号、第 7 条を総合すれば、上記「技術的保護措置」とは、プログラムに関する識別番号・固有番号の入力、暗号化及びその他法による権利を保護する核心技術または装置などを通じてプログラム著作者に付与された公表権、氏名表示権、同一性維持権とプログラムを複製、改作、翻訳、配布、発行及び伝送する権利など、プログラム著作権に対する侵害を効果的に防止する措置を意味するとみるのが相当である。
2. ソニー・エンタテインメント社の Play Station2 機器で実行されるゲームプログラム CD には、ゲームプログラムのほかに access code が収録、格納されており、PS2 には boot ROM が内蔵されていて、PS2 に挿入されるゲーム CD に access code があるかどうかを検索し、access code がなくゲームプログラムだけが内蔵された CD は、プログラムが実行できないように設計されているが、被告人が PS2 に装着したモッドチップは、access code の役割を代行するもので、access code なしにゲームプログラムだけが複製、格納された CD が PS2 に挿入された場合でも、PS2 の boot ROM をして access code が収録されている正規 CD であると認識させることで、不法に複製されたゲーム CD もプログラムの実行を可能にした装置であるとみる。
3. Access code や boot ROM だけで本件ゲームプログラムの物理的な複製自体は防ぐことができないが、通常の装置やプログラムのみでは access code の複製が不可能であり、仮に不法にゲームプログラムを複製したとしても、PS2 を通じたプログラムの実行は不可能であるだけに、access code はゲームプログラムの物理的な複製を防ぐのと同様な効果を持つ技術的保護措置に該当するといえ、従って被告人がモッドチップを装着することによって access code のない複製 CD も実行が可能にしたことは、コンピュータプログラム保護法第 30 条第 2 項所定の技術的保護措置を無力化する行為に該当すると判断。
4. 一方、法第 30 条第 2 項が憲法に違反するかどうかも審理されたが、上記法条はプ

プログラムの複製物を正当な権原によって所持・使用する者が個人的にプログラム著作物を利用する行為を制限するためのものではなく、多数の人がプログラム著作物を不法に利用できるよう技術的保護措置の無力化装置を伝搬する行為などを制限しようとするものであり、特定のプログラム著作物を正当に購入した者がそのプログラム著作物の原本を保護する目的で技術的保護措置を無力化し複製物を生成することは、法第30条第1項第3号、第14条によって許容されるものであるため、法第30条第2項がプログラム著作物の適法な取得者の原本保護のための複製行為を不当に制限するものであるという被告人の主張を排斥。

### **[判決に対する評価]**

上記判決の原審判決(釜山地方法院 2004 年 4 月 22 日言渡し 2004 ノ 307 判決)を参照すれば、法院は被告人が不特定多数人に Play Station2 のコンソールを分解し、モッドチップを装着した行為が旧コンピュータプログラム保護法第 30 条第 2 項所定の「相当に技術的保護措置を無力化する機器・装置・部品などを流通させる行為」に該当すると見ました。ご参考までに、この判決では取り扱われませんでした。モッドチップが装着された Play Station2 を使用した利用者の場合「誰でも正当な権原なしに技術的保護措置を回避、除去、損壊などの方法で無力化してはならない」という規定を違反したものと判断され得ると思われ。この判決は、旧コンピュータプログラム保護法が Access Control までを規律するものなのかどうか規定上明確でない中で、アクセス統制措置の回避が実質的に Copy Control の回避と同じ効果を持つならば、Access Control の回避も禁止されると前向きに判断して著作権保護に万全を期することにしたところにその意味がある。

Exhibit 7

**任天堂判決**

(2009年6月8日に言い渡されたソウル南部地方法院の判決。コンピュータプログラム保護法違反認定。被告人が控訴したが棄却され、さらに被告人が上告して2009年11月12日に上告棄却により有罪判決が確定。)

ソウル南部地方法院2009年6月8日言渡2008ゴ単2104判決

被告人：キム〇〇

関連条文：コンピュータプログラム保護法第46条第1項第3号、第30条

**[判決理由のうち犯罪事実の部分]**

「被告人は〇〇貿易を実質的に運営している。

被害者任天堂株式会社では、不法複製されたゲーム用ソフトウェアの使用を防止するために任天堂 DS ゲーム機及び正規品カートリッジ(ゲーム用ソフトウェアはカートリッジに格納されており、カートリッジを任天堂 DS ゲーム機本体に挿入してゲームソフトウェアを駆動する)に次のような技術的保護措置をした。

任天堂正規品カートリッジ用 ROM にはノーマルモード(Normal Mode)、セキュアモード(Secure Mode)及びゲームモード(Game Mode)の3つのモードがあり、任天堂 DS ゲーム機は、ノーマルモードで正規品カートリッジに格納されている ROM 内登録データを読み出して、Nintendo ロゴデータの CRC、ROM 内登録データの CRC が所定の値になっているかをチェックする手順を行い、セキュアモードで暗号化された命令を送って正規品カートリッジが暗号化された命令を正常に解釈して正常にデータをスクランブルして任天堂 DS ゲーム機本体に供給することができるかをチェックし、ゲームモードで正規品カートリッジの Nintendo ロゴデータをチェックするように作られており、任天堂 DS ゲーム機は上記チェックの各段階を全部正常に通過した場合のみゲームを実行し、上記各段階のうちどこか一部分でも通過できない場合には、ゲームカードのゲームが実行不能または停止するように作られている。

そして、セキュリティチェックのためのハードウェア的装置として、任天堂正規品ゲームカートリッジの回路の中には、セキュリティ回路(Security Circuit)が含まれているが、セキュリティ回路はゲームモードで乱数を生成して命令をデスクランブルし、セキュアモード及びゲームモードでデータをスクランブルするスクランブル回路(Scramble Circuit)、セキュアモードで暗号化した命令を復号化するためのデクリプト回路(Decrypt Circuit)、一連の命令を処理するコマンドシーケンサー(Command Sequencer)で構成されている。

被告人は不法複製された任天堂用ゲームソフトウェアをゲーム機本体に使用できる装置である R4 及び DSTT カートリッジを国内に輸入・販売すれば多くの収益をあげることができると判断して、中国と香港からこれを輸入してオンライン上で販売しようと考えた。この R4 及び DSTT は各カートリッジの ROM メモリマップに位置する Boot Segment 領域に Nintendo ロゴデータが格納されていて、そのほかに任天堂 DS ゲーム機の全てのセキュリティ手続を通過することができるセキュリティ回路を含んでおり、上記のような被害者会社の技術的保護措置を無力化している。

被告人は 2007 年 12 月 13 日頃、ソウル江西区空港洞にある金浦空港より、〇〇貿易を輸入者として R4 カートリッジ 1,000 個を国内に搬入したことをはじめとし、別紙犯罪一覧表記載のとおり R4 を 27,620 個、DSTT を 800 個輸入した。

これにより被告人は、上記のような方法で被害者会社の技術的保護措置を無力化する機器を輸入した。」<sup>177</sup>

### [判決に対する評価]

被告人が輸入した R4 カートリッジは、インターネット等からダウンロードしたゲームソフトを任天堂 DS ゲーム機で実行できるようにする機器で、任天堂 DS の正規のゲームカードと同一のサイズ、外観及び端子を備えており、これを DS ゲーム機に装着すれば、DS ゲーム機の全ての段階の技術的保護措置を通過できる回路が作動し、不法ゲームソフトを自由に使用することができるようになる。結局、ソニーコンピュータエンタテインメントが Play Station2 ゲーム機で採択した技術的保護措置を回避するように設計されたモッドチップ(Mod Chip)が問題となった事件(大法院 2006. 2. 24. 言渡 2004 ド 2743 判決)でその違法性を認めたのと同じ理由で R4 の違法性を認めたものと理解される。R4 は不法に複製されたプログラムを駆動する目的以外の目的にも使用することができるが、その機器の主な目的が技術的保護措置を回避して、不法に複製されたプログラムを駆動することにあるかどうかであると評価したものと考えられる。

---

<sup>177</sup> 被告人は不法に複製された R4 及び DSTT を輸入・販売したことに對し違法性の認識がなく、R4 のような装置なしでは映画や動画などのデータを任天堂 DS ゲーム機で読み出すことが不可能なので、これを無条件に不法であるとするのは、公正な利用を図るという著作権法の基本原則も考慮していないものであると主張したが、裁判所は R4 カートリッジが不法に複製されたゲームソフトを使用することが主な目的の機器であるという点を認めて、このような被告人の主張を受け入れなかった。





## V コンテンツの技術的手段に係る各国法制度調査研究(中国編)



## V コンテンツの技術的手段に係る各国法制度調査研究の調査項目(中国編)

### 1. コンテンツの技術的手段に関する国際ルール

#### (1) WIPO 著作権条約(「WCT」)、WIPO 実演・レコード条約(「WPPT」)

いずれも締結している。

WIPO 著作権条約については、中国は 2007 年 3 月 9 日に加入し、2007 年 6 月 9 日に発効している<sup>178</sup>。

WIPO 実演・レコード条約については、中国は 2007 年 3 月 9 日に加入し、2007 年 6 月 9 日に効力が生じている<sup>179</sup>。

#### (2) 中国における自由貿易協定(FTA)/経済連携協定(EPA)の技術的手段に関する規定の有無・内容

見当たらない。

### 2. コンテンツの技術的手段に関する法令等

#### (1) 該当する法令等

##### ア 類型の整理

中国法においては、コンテンツの技術措置<sup>180</sup>に対する保護を規定する法令として、「著作権法」<sup>181</sup>、「コンピューター・ソフトウェア保護条例」<sup>182</sup>(以下、「ソフトウェア条例」という)、「情報ネットワーク伝播権保護条例」<sup>183</sup>(以下、「伝播権条例」という)及び「インターネット上の著作権に関わる紛争事件の審理における法律適用の若干問題に

<sup>178</sup> WIPO 著作権条約は、30 国の批准・加入により発効することとなり( WIPO 著作権条約第 20 条)、2001 年 12 月 6 日にガボンが加入書を寄託したことにより、2002 年 3 月 6 日に発効した。中国政府は、本条約加入の際、差しあたり香港及びマカオには適用しないという声明を出している。

<sup>179</sup> WIPO 実演・レコード条約は、30 国の批准・加入により発効することとなり( WIPO 実演・レコード条約第 29 条)、2002 年 2 月 20 日にホンジュラスが加入書を寄託したことにより、2002 年 5 月 20 日に発効した。中国政府は、本条約加入の際、差しあたり香港及びマカオには適用しないという声明を出している。

<sup>180</sup> 「技術措置」とは、「権利者の承諾を得ずに著作物、実演、録音・録画製品を閲覧、観賞すること、又は情報ネットワークを通じて公衆に著作物、実演、録音・録画製品を提供することを防止、制限するために用いる有効な技術、装置又は部品」をいうとされており(ネットワーク伝播権保護条例第 26 条第 2 項)、中国法制下においては、下記著作権法等において、「技術措置」と規定されているものが日本法における「技術的手段」に該当すると思われる。そこで、以下、「技術措置」を本報告における技術的手段に該当するものとして記載する。

<sup>181</sup> 法律(狭義の法律)、1990 年 9 月 7 日公布、翌年 6 月 1 日施行、2001 年 10 月 27 日改正。

<sup>182</sup> 行政法規(日本の政令に相当する。)、2001 年 12 月 20 日公布、翌年 1 月 1 日施行。

<sup>183</sup> 2006 年 5 月 18 日公布、同年 7 月 1 日施行。

関する解釈」(法積[2006]11号<sup>184</sup>) (以下、「2006年司法解釈<sup>185</sup>」という)が存在する<sup>186</sup>。

中国法においては、日本法のようにコンテンツの管理技術について、コンテンツのコピーを制限する「コピー管理技術(「コピーコントロール」)」とコンテンツのアクセスを制限する「アクセス管理技術(「アクセスコントロール」)」とに分けられておらず、コピーコントロール及びアクセスコントロールをいずれも「技術措置」として規制している。

そして、技術措置に対する保護については、大きく4つの類型(類型I乃至IV)に分けることができる。類型Iは著作権法、ソフトウェア条例及び伝播権条例により、類型II・IIIは伝播権条例により<sup>187</sup>、類型IV<sup>188</sup>は2006年司法解釈により、各々規定されている。

そこで、以下においては、各類型毎に検討する。

---

<sup>184</sup> 司法解釈、最高人民法院審判委員會2000年12月19日公布、同年12月21日施行、2003年12月23日第一次改正、2006年11月20日第二次改正、同年12月8日施行。

<sup>185</sup> 司法解釈は、最高人民法院及び最高人民檢察院が法令の具体的な適用問題について行う解釈で、法的効力を有する規範である(法發[2007]第12号第5条、高檢發研字[1996]第7号第2条)。その中で最高人民法院の公布する司法解釈は、「解釈」、「規定」、「批復」及び「決定」という四つの形式に分かれ、法律(広義)の適用又はある種類の案件若しくは問題の法律(広義)適用問題について解釈を行う場合、「解釈」の形式を採る(法發[2007]第12号第6条第1項、第2項)。日本の最高裁判所が個別の事件とは別に法律の解釈を示すことはないのに対して、中国の最高人民法院は、屢々ある法律問題について条文形式で司法解釈を制定・公布する。実際、司法解釈は法令同様の機能を果たしており、実務的に非常に重要な位置を占めている。

<sup>186</sup> 中国における法令の優劣関係は、大要、「憲法、法律、行政法規、部門規章(國務院の構成部門である部や委員會が制定する法規範)」となる。法律は、全国人民代表大會とその常務委員會が制定する法規範であり、行政法規は、中央政府である國務院が制定する法規範であり、一般に条例と呼ばれるものが多いが、「規定」や「弁法」と称されるものも存在する。なお、司法解釈と法令との優劣関係に関する明確な規定は存在せず、明らかではない。ただ、裁判文書(判決、裁定等)に複数の法令等を引用する場合は、法律及び法律(立法)解釈、行政法規、地方性法規、自治条例又は単行条例、司法解釈の順に引用することになっている(最高裁の司法解釈(法積[2009]第14号)第2条)。また、民事裁判文書において、法律、法律(立法)解釈又は司法解釈は必ず引用しなければならないが、適用される行政法規、地方性法規又は自治条例と単行条例については、直接引用することができる(同解釈第4条)。

<sup>187</sup> 不正競争防止法(1993年9月2日公布、同年12月1日施行)には、技術措置に関し明記した規定は存在しない。しかし、經營者が類型I・IIの行為を行い、他の經營者の合法的な權益を侵害し、社会經濟秩序を乱す場合は、不正競争行為と認められ規制される可能性がある(不正競争防止法第2条)。

<sup>188</sup> 司法解釈第6条(2003年第一次改正時に追加された新規定)は、法律条文(著作権法第47条第6号)そのものに対する解釈というよりも、最高人民法院の長年の裁判経験に基づき、ある種の案件の法律適用問題についてその解決策を定めたものである。そのため、いわば「立法的な解釈」と言えるため、1つの独立した類型として整理している。

## イ 類型 I : 技術措置の回避又は破壊を行う者に対する規制(著作権法第 47 条第 6 号、ソフトウェア条例第 24 条第 1 項第 3 号、伝播権条例第 4 条第 2 項及び第 18 条第 2 号)

類型 I は、著作権法、ソフトウェア条例及び伝播権条例に規定されている規制であり、技術措置の回避又は破壊を行う者に対する規制である。

これらの 3 つの法令は、各々適用範囲が異なる。すなわち、著作権法は、全ての著作権に適用されるのに対して、ソフトウェア条例はソフトウェア著作権のみに対して適用され、また、伝播権条例は情報ネットワーク伝播権<sup>189</sup>のみに対して適用される。

また、これらの 3 つの法令は、規定内容は実質的に同じである<sup>190</sup>。

従って、これらの 3 つの法令の適用範囲が重なる部分については、重ねて規定されているといえる<sup>191</sup>。

### (ア) 著作権法(第 47 条第 6 号)

著作権者又は著作隣接権者<sup>192</sup>(以下、「著作権者等」という)の承諾を得ずに、著作権者等が著作権<sup>193</sup>及び著作隣接権<sup>194</sup>(以下、「著作権等」という)を保護するために、その著作物、録音・録画製品等(以下、「著作物等」という)に施した技術措置を故意<sup>195</sup>に

<sup>189</sup> 情報ネットワーク伝播権とは、有線又は無線方式で公衆に著作物を提供し、公衆が自分で選んだ日時と場所で著作物を得ることができるようにする権利のことをいう(著作権法第 10 条第 1 項第 12 号)。

<sup>190</sup> 規定文言自体には若干の相違がある。例えば、著作権法第 47 条第 6 号及びソフトウェア条例第 24 条第 1 項第 3 号においては、「回避又は破壊」行為の主体を限定していないのに対して、伝播権条例第 4 条第 2 項及び第 18 条第 2 項においては、「いかなる組織又は個人」と規定されている。

<sup>191</sup> 中国の立法においては、上位の法令で定めた規定と同じ規定を、下位の法令において重ねて規定するのが一般的である。

<sup>192</sup> 原文は「著作権に関連する権利者」となっているが、学説上「著作隣接権者」と解されている(中国司法試験指導用書 2008 年版 223 頁)。そこで、以下「著作隣接権者」と称する。

<sup>193</sup> 中国法で言う著作権には著作財産権と著作者人格権が含まれる(著作権法第 10 条)。

<sup>194</sup> 原文の直訳は「著作権に関連する権利(権益)」である、出版社、実演家、録音・録画制作者及びラジオ局・テレビ局の権利を指し(著作権実施条例第 26 条)、学説上「著作隣接権」と解されている(中国司法試験指導用書 2008 年版 223 頁)。そこで、以下「著作隣接権」と称する。

<sup>195</sup> 著作権法、ソフトウェア条例及び伝播権条例によると、技術措置の回避又は破壊行為の法的責任を追及する場合、「故意」の要件を満たさなければならない。従って、過失により回避又は破壊行為を行った場合、上記法令により法的責任を追及することはできない。しかし、回避又は破壊により取得した著作物等を他人が著作権者等の承諾を得ずに使用することを知り又は知るべきであった場合は、最高人民法院審判委員会が 1988 年 4 月 2 日公布した司法解釈「民法通則の全面的執行過程における若干の問題に関する意見(試行)」(法弁發[1988]6 号)(以下「民法通則意見」と言う)第 148 条第 1 項により、違法使用者との共同不法行為が成立する可能性がある(張耕「略論版權的技術保護措置(On the Technologically Protective Measures of Copyright)」現代法学 2004 年 4 月第 26 卷第 2 期 123 頁)。

回避又は破壊する行為を行う者に対する規制である<sup>196</sup>。

#### (イ) ソフトウェア<sup>197</sup>条例(第 24 条第 1 項第 3 号)

ソフトウェア著作権者の承諾を得ずに、ソフトウェア著作権者がそのソフトウェア著作権を保護するために施した技術措置を故意に回避又は破壊する行為を行う者に対する規制である<sup>198</sup>。

#### (ウ) 伝播権条例(第 4 条第 2 項及び第 18 条第 2 号)

著作権者、実演家及び録音・録画制作者(以下、「権利者」という)がその情報ネットワーク伝播権<sup>199</sup>(以下、「伝播権」という)を保護するために著作物等に施した「技術措置」<sup>200</sup>を故意に回避又は破壊する行為を行う者に対する規制である。

### ウ 類型Ⅱ：技術措置を回避又は破壊するための装置等の製造、輸入又は提供、及び、他人が技術措置を回避又は破壊するための技術的サービスの提供に対する規制(伝播権条例第 4 条第 2 項及び第 19 条第 1 号)

類型Ⅱは、伝播権条例第 4 条第 2 項及び第 19 条第 1 号に規定されている規制であり、主に技術措置の回避又は破壊に用いる装置又は部品を故意に製造、輸入又は提供する行為、及び、故意に他人が技術措置を回避し又は破壊するために技術的サービス

---

<sup>196</sup> 本号における「技術措置」及び「技術措置の回避又は破壊」について、著作権法及び著作権法実施条例はいずれも定義を定めていない。これに対して伝播権条例には、「技術措置」についての定義が規定されている(第 26 条第 2 項)。従って、伝播権条例における「技術措置」の定義は著作権法における技術措置の解釈の参考にはなるものと思われる。

<sup>197</sup> 著作権法における「著作物」には、「コンピューター・ソフトウェア」(同条第 8 号)及び著作物のデジタル型式(法積[2006]第 11 号(2006 年 12 月 8 日公布、施行)第 2 条)が含まれる。

<sup>198</sup> 本号における「技術措置」及び「技術措置の回避又は破壊」のいずれについても、ソフトウェア条例は定義を定めていない。

<sup>199</sup> ネットワーク伝播権は、有線又は無線の方式により公衆に著作物、実演又は録音・録画製品を提供し、公衆にその個人的に選択した時間及び場所において著作物、実演又は録音・録画製品を獲得される権利をいう(伝播権条例第 26 条第 1 項)。著作権法においてもネットワーク伝播権について定義されており、著作権法上の伝播権の対象が「作品」に限られることに対して、伝播権条例における伝播権の対象は、「作品」のみならず、「実演製品」及び「録音・録画製品」も含まれる点が異なり、その他は同じである。なお、伝播権条例及び著作権法のいずれのネットワーク伝播権の定義においても、「公衆」に対するものであるため、特定の個人に対して伝播する行為(例えば、P2P)はネットワーク伝播権の範囲外であると思われる。

<sup>200</sup> 伝播権条例第 26 条第 2 項に「技術措置」の定義が置かれている。上記のように著作権法、伝播権条例及びソフトウェア条例においては各々適用範囲が異なるため、伝播権条例第 26 条第 2 項の「技術措置」の定義規定(伝播権条例第 26 条第 2 項)が、そのまま著作権法及びソフトウェア条例の「技術措置」と同じ意義を有すると解することはできない。ただし、伝播権条例第 26 条第 2 項の「技術措置」の定義が、著作権法及びソフトウェア条例の「技術措置」の解釈において参考になるものと思われる。

を提供する行為に対する規制である。

第4条第2項に違反する行為に対する責任の内容について第19条に「著作権行政管理部门は警告を与え、違法所得を没収し、主に技術措置の回避、破壊に用いる装置又は部品を没収することができる。情状が重い場合は、主にネットワークサービスの提供に用いるコンピュータ等の設備を没収し、かつ10万円以下の過料に処することができる。犯罪を構成する場合は、刑事責任を追及する。」と記載されている<sup>201</sup>。

#### **エ 類型Ⅲ：伝播権条例第7条乃至第9条に基づき著作者の許諾を得ずに著作物を提供する場合において、本来必要とされる技術措置を講じないことに対する規制(伝播権条例第10条第4号、第11条及び第18条第5号)**

類型Ⅲは、伝播権条例第10条第4号、第11条及び第18条第5号に規定されている規制である。

著作権者は情報ネットワーク伝達権を享有する(伝播権条例第2条)。

しかし、伝播権条例において、第三者が一定の条件の下、図書館等の収蔵物を図書館等のサービスを受ける者に対して提供する場合(伝播権条例第7条)、義務教育等を実施するために教育ソフトを学生に対して提供する場合(伝播権条例第8条)、及び、貧困救済のために著作物を農村地区の公衆に対して提供する場合(伝播権条例第9条)には、著作権者の許諾を得ずに、情報ネットワークを通じて著作物等の提供をすることが認められている。

ただし、伝播権条例第7条に基づいて著作物を提供する場合には、サービスを受ける者以外の者が著作物を取得すること及び著作物の複製により著作権者に実質的な損害をもたらすことを防止するために、伝播権条例第8条及び第9条に基づいて著作物を提供する場合には、サービスを受ける者以外の者が著作物を取得することを防止するために、技術措置を講じることを求める規制が置かれており(伝播権条例第10条第4号)、これが類型Ⅲの規制である。

#### **オ 類型Ⅳ：他人の技術措置を回避又は破壊するための方法、設備又は材料の掲載、伝播又は提供する者に対する規制(2006年司法解釈第6条)**

類型Ⅳは、他人の技術措置を故意に回避又は破壊するための方法、設備又は材料として使用されることを明らかに知りながら、掲載、伝播又は提供を行ったインターネットサービス提供者に対する規制である。

<sup>201</sup> 「提供」行為については、第4条第2項においては、「公衆に提供」と規定されているのに対し、第19条第1号では、「他人に提供する」と規定されており、第19条第1号に規定する提供行為は第4条第2項に規定されている提供行為よりも広い。そして、第19条第1号に該当し、かつ、第4条第2項に該当しない提供行為に対して第19条柱書の責任を問われるかは明らかでない。

## (2) 法令等の規制内容

### (a) 規制対象技術(定義及び対象技術の具体例等)

#### ア 類型 I

##### (ア) 著作権法(第 47 条第 6 号)

###### (i) 規制されている対象技術(保護対象技術)

「技術措置」である。ただし、「技術措置」に対する定義規定はない。

###### (ii) 対象技術の具体例

- ・ SCMS(Serial Copy Management System)<sup>202</sup>
- ・ CGMS(Copy Generation Management System)<sup>203</sup>
- ・ 擬似シンクパルス方式(マクロビジョン方式)<sup>204</sup>
- ・ 電子ファイル指示ソフト
- ・ 電子署名
- ・ 電子透かし

##### (イ) ソフトウェア条例(第 24 条第 1 項第 3 号)

###### (i) 規制されている対象技術(保護対象技術)

「技術措置」である。ただし、「技術措置」に対する定義規定はない。

###### (ii) 対象技術の具体例

上記(ア)(ii)と同様である。

<sup>202</sup> SCMS は、録音媒体の特定の箇所に記録されたデジタル信号に、デジタル録音機器が対応することにより、無断複製の防止が行われる(著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁参照。)

<sup>203</sup> CGMS では、SCMS と同様に、録画媒体の特定の箇所に記録されたデジタル信号にデジタル録画機器が反応することにより、無断複製の防止(録画動作の停止)が行われる。信号には、「コピー不可」、「コピー1 世代」、「コピー自由」の 3 種類があるが、現在市販されている DVD の多くには、「コピー不可」の信号が録音されており、ダビングできないようになっている(著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁以下参照。)

<sup>204</sup> 擬似シンクパルス方式は、録画媒体に記録されたアナログ映像信号のうち、通常のテレビでは画面に映らない部分に特殊な信号を記録することにより(デジタル録画媒体やデジタル放送の場合には、記録、送信される特定のデジタル信号に基づき、再生・受信機器がアナログ映像信号を出力する際に特殊な信号を付加することにより)、アナログ録画機器の録画機能を正常に動作させないようにすることにより鑑賞に堪えない乱れた映像を録画させ、デジタル録画機器では録画動作を停止させて、無断複製を防ぐ。擬似シンクパルス方式については、上記信号を除去して正常な録画が行われるようにする専用装置がいくつも市販されている(著作権法令研究会・通商産業省知的財産政策室『著作権法・不正競争防止法改正解説 デジタルコンテンツの法的保護』(有斐閣、1999)88 頁以下参照。)



**(ウ) 伝播権条例(第 4 条第 2 項及び第 18 条第 2 号)**

**(i) 規制されている対象技術(保護対象技術)**

「技術措置」(伝播権条例第 26 条第 2 項)である。

技術措置とは、権利者の許諾を得ずに著作物、実演、録音・録画製品を閲覧、鑑賞すること、又は情報ネットワークを通じて公衆に著作物、実演、録音・録画製品を提供することを防止、制限するために用いる有効な技術、装置又は部品をいう。

コピーコントロール及びアクセスコントロールの両方を規制対象としている。

**(ii) 対象技術の具体例**

上記(ア)(ii)と同様である。

**イ 類型Ⅱ(伝播権条例第 4 条第 2 項及び第 19 条第 1 号)**

**(i) 規制されている対象技術(保護対象技術)**

「技術措置」(伝播権条例第 26 条第 2 項)である。

コピーコントロール及びアクセスコントロールの両方を規制対象としている。

**(ii) 対象技術の具体例**

上記ア(ア)(ii)と同様である。

**ウ 類型Ⅲ(伝播権条例第 10 条第 4 号、第 11 条及び第 18 条第 5 号)**

**(i) 規制されている対象技術(保護対象技術)**

「技術措置」(伝播権条例第 26 条第 2 項)である。

コピーコントロール及びアクセスコントロールの両方を規制対象としている。

伝播権条例第 7 条に基づいて著作物を提供する場合には、サービスを受ける者以外の者が著作物を取得すること及び著作物の複製により著作権者に実質的な損害をもたらすことを防止するための技術措置が対象である。

また、伝播権条例第 8 条及び第 9 条に基づいて著作物を提供する場合には、サービスを受ける者以外の者が著作物を取得することを防止するための技術措置が対象である。

**(ii) 対象技術の具体例**

上記ア(ア)(ii)と同様である。

## エ 類型Ⅳ(2006年司法解釈第6条)

### (i) 規制されている対象技術(保護対象技術)

「技術措置」である。ただし、「技術措置」に対する定義規定がない<sup>205</sup>。

### (ii) 対象技術の具体例

上記ア(ア)(ii)と同様である。

## (b) 規制対象製品及び対象プログラム等

### ア 類型Ⅰ

#### (ア) 著作権法(第47条第6号)

対象製品又は対象プログラムに対する限定はない。

すなわち、行為自体が対象である。

#### (イ) ソフトウェア条例(第24条第1項第3号)

対象製品又は対象プログラムに対する限定はない。

すなわち、行為自体が対象である。

#### (ウ) 伝播権条例(伝播権条例第4条第2項及び第18条第2号)

対象製品又は対象プログラムに対する限定はない。

すなわち、行為自体が対象である。

### (エ) 小括

以上の次第で、類型Ⅰにおいては、いずれの場合も行為自体が対象であり、対象製品又は対象プログラムに対する限定はない。

## イ 類型Ⅱ(伝播権条例第4条第2項及び第19条第1号)

(ア) 主に技術措置の回避又は破壊に用いる装置又は部品

(イ) 技術措置を回避又は破壊するための技術的サービス

## ウ 類型Ⅲ(伝播権条例第10条第4号、第11条及び第18条第5号)

対象製品又は対象プログラムに対する限定はない。

<sup>205</sup> 著作権法、伝播権条例及びソフトウェア条例においては各々適用範囲が異なるため、伝播権条例第26条第2項の「技術措置」の定義規定(伝播権条例第26条第2項)が、そのまま著作権法及びソフトウェア条例の「技術措置」と同じ意義を有すると解することはできない。ただし、伝播権条例第26条第2項の「技術措置」の定義が、著作権法及びソフトウェア条例の「技術措置」の解釈において参考になるものと思われる。2006年司法解釈第6条は2003年改正時追加された規定である。2006年司法解釈第6条の「技術措置」について直接定義する規定は存在しないものの、伝播権条例第26条第2項の定義が参考になるとと思われる。

すなわち、類型Ⅲにおいては、講じるべき技術措置を講じないという不作為が対象である。

## エ 類型Ⅳ(2006年司法解釈第6条)

もっぱら技術措置の回避又は破壊に用いる方法、設備及び材料

### (c) 規制対象行為

一特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

## ア 類型Ⅰ

### (ア) 著作権法(第47条第6号)

#### ・ 規制対象行為

著作権又は著作権に関連する権利を保護する技術措置を故意に回避又は破壊する行為

①機器等(プログラムを含む)製造行為、②機器等(プログラムを含む)提供行為、③機器等(プログラムを含む)輸出入行為、④機器等(プログラムを含む)所持行為、⑤回避サービス提供行為、⑦宣伝・情報の流布行為

→規制対象外。ただし、他人が技術措置の回避又は破壊に使用することを知り又は知るべきであったにも関わらず、上記行為を行った場合は、民法通則意見第148条第1項により、回避又は破壊行為者との共同不法行為が成立する可能性がある。

⑥回避行為(回避による複製)

→規制対象

そのほか、技術措置の「破壊行為」も規制対象である。

### (イ) ソフトウェア条例(第24条第1項第3号)

#### ・ 規制対象行為

著作権者がそのソフトウェア著作権を守るために施した技術措置を故意に避け、又は破壊する行為

規制対象行為は全て上記(ア)と同じ。

**(ウ) 伝播権条例(第4条第2項及び第18条第2号)**

・ **規制対象行為**

故意に技術措置を回避し又は破壊する行為

規制対象行為は全て上記(ア)と同じ。

**イ 類型Ⅱ(伝播権条例第4条第2項及び第19条第1号)**

**(ア)「主に技術措置の回避又は破壊に用いる装置又は部品」について**

・ **規制対象行為**

故意に製造、輸入又は公衆に提供する行為

①機器等(プログラムを含む)製造行為

→規制対象である。

②機器等(プログラムを含む)提供行為

→公衆に提供する行為が規制対象<sup>206</sup>

③機器等(プログラムを含む)輸出入行為

→輸入行為が規制対象。輸出行為については、公衆に提供する行為に該当する可能性があるが、明らかではない。

④機器等(プログラムを含む)所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為

→規制対象外

**(イ)「技術措置を回避又は破壊するための技術的サービス」について**

・ **規制対象行為**

サービスを提供する行為

①機器等(プログラムを含む)製造行為、②機器等(プログラムを含む)提供行為、③機器等(プログラムを含む)輸出入行為、④機器等(プログラムを含む)所持行為

→規制対象外

---

<sup>206</sup> 伝播権条例第4条第2項には、「公衆に提供」と規定されているが、伝播権条例第19条第1号には、「他人に提供」と規定されている。

⑤回避サービス提供行為

→規制対象である。また、破壊のための技術的サービスの提供も規制対象である。

⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為

→規制対象外

## エ 類型Ⅲ(伝播権条例第10条第4号、第11条及び第18条第5号)

### ・ 規制対象行為

技術措置を講じないという不作為

①機器等(プログラムを含む)製造行為、②機器等(プログラムを含む)提供行為、③機器等(プログラムを含む)輸出入行為、④機器等(プログラムを含む)所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為

→規制対象外

## オ 類型Ⅳ(2006年司法解釈第6条)

### ・ 規制対象行為

他人の技術措置を故意に回避又は破壊するための方法、設備又は材料として使用されることを明らかに知りながら、掲載、伝播又は提供を行う行為。

①機器等(プログラムを含む)製造行為

→規制対象外

②機器等(プログラムを含む)提供行為

→他人の技術措置を故意に回避又は破壊するための方法、設備又は材料として使用されることを明らかに知りながら、提供する行為が規制対象である。

③機器等(プログラムを含む)輸出入行為

→輸出行為については、提供する行為に該当する可能性があるが、明らかではない。

④機器等(プログラムを含む)所持行為⑤回避サービス提供行為、⑥回避行為(回避による複製)

→規制対象外

⑦宣伝・情報の流布行為

→他人の技術措置を故意に回避又は破壊するための方法、設備又は材料として使用さ

れることを明らかに知りながら、伝播する<sup>207</sup>行為が規制対象である。

そのほか、技術措置を回避又は破壊に用いる方法、設備又は材料の「ネット掲載行為」も規制対象である。

### (3) 除外行為

#### (a) コンテンツの技術的手段に関する規定の適用除外、例外、制限規定等の存否・内容

##### ア 類型 I

###### (ア) 著作権法(第 47 条第 6 号)

第 47 条第 6 号に「法律、行政法規に別段の定めがある場合を除く」と記載されているが、下記伝播権条例 12 条を除き、適用除外、例外、制限規定等は見当たらない。

###### (イ) ソフトウェア条例(第 24 条第 1 項第 3 号)

第 24 条柱書に「著作権法、本条例又はその他の法律、行政法規に別段の定めがある場合を除き」と記載されているが、下記伝播権条例第 12 条以外に適用除外、例外、制限規定等は見当たらない。

###### (ウ) 伝播権条例(第 4 条第 2 項及び第 18 条第 2 号)

回避についてのみ、例外規定(伝播権条例第 12 条)が存在する。

次の場合は、技術措置の回避が許される。

##### ・ 伝播権条例第 12 条各号

- (1) 学校の授業又は科学研究のために、情報ネットワークを通じて少数の教育、科学研究職員のためにすでに公表された著作物、実演、録音・録画製品を提供する場合で、当該著作物、実演、録音・録画製品が情報ネットワークによってのみしか取得できないとき
- (2) 営利を目的とせず、情報ネットワークを通じて視覚障害者が感知できる独特な方法によりすでに公表された文字作品を視覚障害者に提供する場合で、当該著作物が情報ネットワークによってのみしか取得できないとき
- (3) 国家機関が行政、司法の手續に従い公務を執行する場合
- (4) 情報ネットワーク上でコンピュータ及びそのシステム又はネットワークに対して安全性能をテストする場合

##### イ 類型 II・III 共通(伝播権条例第 4 条第 2 項、第 10 条第 4 号、第 11 条、第 18 条第 5 号)

<sup>207</sup> 本報告における「伝播する」とは、「広く伝える」という意味である。法令上は「伝播」の意義について明確に定めていないが、日本でいう「公衆送信」とほぼ同義と考えて良いと思われる。

## 及び第 19 条第 1 号)

適用除外、例外、制限規定等は存在しない。

## ウ 類型Ⅳ (2006 年司法解釈第 6 条)

適用除外、例外、制限規定等は存在しない。

### (b) 著作権法にコンテンツの技術的手段に関する規定が存在する場合の技術的手段回避の禁止規定と権利制限規定との関係

コンテンツの技術措置についての規定として、著作権法第 47 条第 6 号が規定されている。また、権利制限規定として、著作権法第 22 条(著作物の自由利用)及び第 23 条(教科書への掲載)が規定されている。

しかし、著作権法第 47 条第 6 号と著作権法第 22 条及び第 23 条の例外規定の適用関係については明らかではない。

ただし、学説では、著作権に対する例外又は制限規定である著作権法第 22 条は、第 47 条第 6 号の行為に適用されないという見解が多数を占める<sup>208</sup>。

## (4) 救済措置

### (a) 救済措置の内容(民事的救済及び刑事的制裁)

—特に、①機器等(プログラムを含む)製造行為、②機器等提供行為、③機器等輸出入行為、④機器等所持行為、⑤回避サービス提供行為、⑥回避行為(回避による複製)、⑦宣伝・情報の流布行為、の各行為について

以下は、全て上記①乃至⑦の各行為について共通

## ア 類型Ⅰ

### (ア) 著作権法(第 47 条第 6 号)

#### (i) 民事的救済

侵害行為の停止、影響の除去、謝罪、損害賠償等(著作権法第 47 条柱書、民法

<sup>208</sup> 李楊「技術措置権及其反思(On Right to Technical Measures)」ネットワーク法律評論 2002 年第 2 卷 9 頁、王遷「対技術措置立法保護的比較研究」知識産権 2003 年第 13 卷 74 期 3 頁、張耕「略論版權の技術保護措置(On the Technologically Protective Measures of Copyright)」現代法学 2004 年 4 月第 26 卷第 2 期 123 頁、朱理「版權技術措置法律保護の三個等級(Technological Measure, Copyright, Limitations and Exceptions)」ネットワーク法律評論 2005 年第 6 卷第 1 期 34 頁、羅莉「数字私人複製所引起の利益平衡問題(Interests Balancing of Private Digital Copying)」法学 2008 年第 318 期 88 頁、梁志文「版權人的自力救済及其限度(Copyright Holder's Private Remedy and Its Limits: Black Screen Incident of Microsoft)」法学 2008 年第 325 期 120 頁、熊琦「論接觸權(Also Concerning the Defects of Classification of Property Right of Copyright and Its Overcoming)」法律科学 2008 年第 169 期 93 頁。

通則<sup>209</sup>第 134 条第 1 項)並びに妨害の排除、危険の除去、財産の返還、原状の回復、修理、再制作及び交換、違約金の支払い及び名誉の回復等(民法通則第 134 条第 1 項)。

なお、人民法院は、民事事件の審理において、前項の規定を適用する他、訓戒又は始末書提出を命じ、不法活動による財物及び不法所得を没収することができる、かつ法律の規定に基づき過料又は拘留<sup>210</sup>に処することができる(民法通則第 134 条第 3 項)。

## (ii) 行政処分

公共の利益を損ねた場合は、侵害行為の停止命令、違法所得の没収、権利侵害複製品の没収、処分、かつ不法経営額<sup>211</sup>の 3 倍以下又は 10 万人民币以下の過料に処することができる。情状が重い場合は、さらに主に権利侵害複製品の制作に使われた材料、道具、設備等を没収することができる(著作権法第 47 条柱書、著作権法实施条例<sup>212</sup>第 36 条)。

## (iii) 刑事的制裁

明確な刑事的制裁規定は存在しない(刑事上の救済について、著作権法第 47 条柱書に規定が置かれており、「犯罪に該当するときは、法によって刑事責任を追及する」と規定されている。しかし、著作権法第 47 条第 6 号に該当する行為であ

<sup>209</sup> 法律、1986 年 4 月 12 日公布、翌年 1 月 1 日施行。日本でいう民法総則及び債権総論(不法行為等も含む)に相当する基本法律である。中国には日本のような統一民法典がなく、民法通則、物権法、担保法、契約法、婚姻法及び相続法という個別の法律に分かれている。不法行為法(中文は「侵權責任法」)については、2009 年 12 月 26 日に公布されており、2010 年 7 月 1 日より施行する予定である。

<sup>210</sup> 司法機関である裁判所が課すものであって、行政罰と区別するために、学説上「司法過料」、「司法拘留」と称するのが一般的である。司法過料又は司法拘留は、行政罰に類似する中国独特の民事的制裁形式である。これは、人民法院が民事訴訟において係争事件と関連する民事法律違反行為を発見し、それについて制裁する必要があると認めた場合に、違法行為者に対して行う制裁措置である(民法通則意見第 163 条第 1 項)。ただし、法律により行政機関が過料又は拘留に処すると定めた場合はその限りではない(民法通則第 134 条第 3 項に関する最高人民法院 1993 年 11 月 4 日司法解釈)。また、法律により没収、過料、拘留の制裁措置をとる場合は人民法院長の承認を得て、別途民事制裁決定書を作成しなければならず、被制裁者は、制裁決定に不服がある場合、制裁決定書を受領した翌日から 10 日以内に一級上の人民法院に不服審査を一度申し立てることができる(民法通則意見第 163 条)。しかし、不服審査結果についてなお不服がある場合、訴訟を提起することができるか否かについては必ずしも明らかではない。実務上、訴訟当事者司法過料又は司法拘留等の制裁を課すことについて、躊躇を示す人民法院が多いようである(汪有生「民事制裁縁何適用難」<[http://www.sdcour.gov.cn/art/2006/08/24/art\\_8770.html](http://www.sdcour.gov.cn/art/2006/08/24/art_8770.html)>)。

<sup>211</sup> この不法経営額の意義に関する明文規定は見当たらないが、中国国家工商行政管理総局の商標権侵害における不法経営額の算定基準(商標字[1990]第 7 号)によると、不法経営額とは、権利侵害商品の売上総額と在庫商品の仕入総額の和である。著作権侵害における不法経営額の算定にも参考になると思われる。

<sup>212</sup> 2002 年 8 月 2 日公布、同年 9 月 15 日施行。



る、「技術措置を故意に回避又は破壊する行為」については、刑法の規定がない。そのため、著作権法第 47 条第 6 号に違反しても刑事責任を追及されることはない。もっとも、「技術措置を故意に回避又は破壊する行為」が、他人の刑法第 217 条(著作権侵害に関する罪)又は第 218 条(権利侵害複製品販売罪)該当行為を幫助等する行為に該当する場合には、知的財産権侵害刑事事件に関する最高人民法院＝最高人民検察院の司法解釈(法釈[2004]第 19 号)<sup>213</sup>に基づき、共犯として訴追される可能性はある<sup>214</sup>。この場合、非親告罪である。)

## (イ) ソフトウェア条例(第 24 条第 1 項第 3 号)

### (i) 民事的救済

救済措置については上記(ア)(i)と同様。ただし、根拠条文は著作権法第 47 条柱書、民法通則第 134 条第 1 項、第 3 項及びソフトウェア条例第 24 条第 1 項柱書。

### (ii) 行政処分

社会公共の利益を損なった場合は、著作権行政管理部門が侵害行為の停止を命じ、違法所得を没収し、権利侵害複製品を没収、廃棄し、かつ不法経営額の 3 倍(不法経営額が不明の場合は 10 万人民币元)又は 5 万人民币元の過料に処することができる。情状が重大である場合、著作権行政管理部門は、さらに主に権利侵害複製品の制作に用いられた材料、道具、設備等を没収することができる(著作権法第 47 条柱書、著作権法实施条例第 36 条、ソフトウェア条例第 24 条第 1 項柱書及び第 2 項)。

### (iii) 刑事的制裁

明確な刑事的制裁規定は存在しない。ただし、営利目的で、著作権者の許可を得ず、ソフトウェアの著作権者が施した技術措置である暗号を複合化し、当該ソフトウェアのプラグインソフトを制作及び販売した者に対して、不法経営罪(刑法第 225 条第 4 号)の成立を認めた裁判例がある<sup>215</sup>。

---

<sup>213</sup> 「知的財産権侵害刑事事件の処理における具体的な法律適用の若干問題に関する解釈」(2004 年 12 月 8 日公布、同月 22 日施行)第 16 条。

<sup>214</sup> 任軍民「法国信息网络刑事保護对我国有关立法啓示(Enlightenment on China's Legislation view on Criminal Protection of France's Information Network)」知識産権 2006 年第 16 卷第 95 期 85 頁。

<sup>215</sup> 「QQ 幻想」事件((2006)深南法刑初字第 803 号)。

## **(ウ) 伝播権条例(第 4 条第 2 項及び第 18 条第 2 号)**

### **(i) 民事的救済**

救済措置は上記(ア)(i)と同様。ただし、根拠条文は著作権法第 47 条柱書、民法通則第 134 条第 1 項、第 3 項及び伝播権条例第 18 条柱書。

### **(ii) 行政処分**

公共の利益を損ねた場合は、著作権行政管理部門が権利侵害行為の停止を命じ、違法所得を没収し、かつ不法経営額 3 倍以下又は 10 万元以下の過料に処することができる。情状が重い場合は、著作権行政管理部門は、ネットワークサービスの提供に主に使用するコンピュータ等の設備を没収することができる(著作権法第 47 条柱書、著作権実施条例第 36 条及び伝播権条例第 18 条柱書)。

### **(iii) 刑事的制裁**

明確な刑事的制裁規定は存在しない(伝播権条例第 18 条柱書に「犯罪を構成する場合は、法により刑事責任を追及する」と規定されているが、共犯の場合を除き、実際には刑事責任を追及することができない。なお、共犯として訴追される場合は、非親告罪である。)

## **イ 類型Ⅱ(伝播権条例第 4 条第 2 項及び第 19 条第 1 号)**

### **(i) 民事的救済**

救済措置は上記ア(ア)(i)と同様。ただし、根拠条文は民法通則第 134 条第 1 項及び第 3 項<sup>216</sup>。

### **(ii) 行政処分**

公共の利益を損ねた場合は、著作権行政管理部門が権利侵害行為の停止を命じ、違法所得を没収し、かつ 10 万元以下の過料に処することができる。情状が重い場合は、著作権行政管理部門は、ネットワークサービスの提供に主に使用するコンピュータ等の設備を没収することができる(伝播権条例第 19 条柱書)。

### **(iii) 刑事的制裁**

明確な刑事的制裁規定は存在しない(伝播権条例第 19 条柱書に「犯罪を構成する場合は、法により刑事責任を追及する」と規定されているが、共犯の場合を除き、実際には刑事責任を追及することができない。なお、共犯として訴追される

<sup>216</sup> 伝播権条例第 19 条柱書に民事的救済措置の規定が存在しない。しかし、脚注 44 の記載のように、類型Ⅱの行為が著作権侵等侵害行為とみなされる可能性もあるので、その場合は、著作権法第 46 条第 11 号に基づき、差止、損害賠償等の民事責任を追及することができる。

場合、非親告罪である。)

## ウ 類型Ⅲ(伝播権条例第 10 条第 4 号、第 11 条及び第 18 条第 5 号)

### (i) 民事的救済

救済措置は上記ア(ア)(i)と同様。ただし、根拠条文は民法通則第 134 条第 1 項、第 3 項及び伝播権条例第 18 条柱書。

### (ii) 行政処分

公共の利益を損ねた場合は、著作権行政管理部門が権利侵害行為の停止を命じ、違法所得を没収し、かつ 10 万元以下の過料に処することができる。情状が重い場合は、著作権行政管理部門は、ネットワークサービスの提供に主に使用するコンピュータ等の設備を没収することができる(伝播権条例第 18 条柱書)。

### (iii) 刑事的制裁

明確な刑事的制裁規定は存在しない(伝播権条例第 18 条柱書に「犯罪を構成する場合は、法により刑事責任を追及する」と規定されているが、共犯の場合を除き、実際には刑事責任を追及することができない。なお、共犯として訴追される場合、非親告罪である。)

## エ 類型Ⅳ(2006 年司法解釈第 6 条)

### (i) 民事的救済

ア(ア)(i)と同様。

### (ii) 行政処分

なし<sup>217</sup>

### (iii) 刑事的制裁

なし

<b>(b) (a)の救済措置の請求主体</b>
--------------------------

## ア 類型Ⅰ・Ⅱ・Ⅲ共通

### (ア) 民事的救済

著作権者等権利を侵害された者

<sup>217</sup> 2006 年司法解釈第 6 条は、「著作権法第 47 条第 6 号の規定に従い、不法行為責任を追及することができる」となっている。

### (イ) 行政処分

行政罰であるため、誰でも告発することができる。

### (ウ) 刑事的制裁

共犯の場合を除き、刑事的制裁自体が存在しないため、刑事責任を追及することができない。他の著作権侵害行為との共犯として提訴する場合は、原則検察官、一定の場合は著作権者等が請求主体となる<sup>218</sup>。この場合は、非親告罪である。

## イ 類型Ⅳ

### (ア) 民事的救済

著作権者等

### (イ) 行政処分

行政処分が規定されていない。

### (ウ) 刑事的制裁

刑事的制裁が規定されていない。

### (c) 違反機器等の輸出入にかかる水際措置又は違反抑止のための行政措置の有無・内容

知的財産権税関保護条例<sup>219</sup>及びその実施規則<sup>220</sup>に水際措置又は違反抑止のための行政措置が存在する。

知的財産権を侵害する物品については、輸出又は輸入してはならない(知的財産権税関保護条例第3条)。厳密に言えば、もっぱら技術措置の回避又は破壊に用いる装置、部品(伝播権条例第18条第2号)及び設備又は材料(2006年司法解釈第6条)は、著作権侵害物品に該当しない。しかし、中国の著作権関連法令、学説及び実務上は、

<sup>218</sup> 被害者自ら刑事訴訟を提起することを中国法では「自訴」という。(1)告訴を待って処理する事件(親告罪)、(2)被害者が証拠によって証明することができる軽微な刑事事件及び(3)被害者が証拠を提出して、被害者の身体又は財産上の権利に対する被告人の侵害行為に対して法に基づき刑事責任を追及すべきであることを証明することができるが、公安機関又は人民検察院が被告人の刑事責任を追及しない事件については、被害者自ら刑事訴訟を提起することができる(刑事訴訟法第170条)。

<sup>219</sup> 行政法規、2003年12月2日公布、翌年3月1日施行。

<sup>220</sup> 部委規章(日本の省令に相当)、2004年5月25日公布、同年7月1日施行。

回避又は破壊行為をも著作権侵害行為とみなして規制しているように思われる<sup>221</sup>。

よって、違反機器等は、知的財産権税関保護条例及びその実施細則により規制されうると考えられる。なお、著作権法第 47 条、ソフトウェア条例第 24 条、伝播権条例第 18 条及び第 19 条の「著作権行政管理機関」には税関が含まれると解される。

#### (5) いわゆる「無反応機器」規制

##### いわゆる「無反応機器」に対する法令、規則、指令等による規制の有無・内容

無反応機器規制に関する明確な法令、規則、指令等は見当たらず、著作権法等により規制されるかについては明らかではない<sup>222</sup>。

### 3. 裁判例、執行状況、被害状況等

#### (1) コンテンツの技術的手段に関する裁判例

##### 〈民事事件〉

- ・ 北京精彫 Vs 上海奈凱 ソフトウェア著作権侵害紛争事件(上海市高级人民法院[2006]沪高民三(知)終字第 110 号<sup>223</sup>(差止請求、公開謝罪請求及び損害賠償請求事件))

#### ア 事案の概要

上訴人(1 審原告)である北京精彫科技有限公司は、小型切削具の高速彫刻機械の研究開発及び製造を行う会社である。

被上訴人である上海奈凱電子科技有限公司は、主にデジタル彫刻システムの製造・販売業を営む会社である。

上訴人は、上訴人が独自に開発した精彫 CNC 彫刻システム(以下、「CNC システム」と

<sup>221</sup> 「2008 年度国家司法試験指導用書」(法律出版社、2008 年)第 3 巻 225 頁は、著作権法における著作権侵害行為を民事責任を負う著作権侵害行為(第 46 条)と総合的責任を負う著作権侵害行為(第 47 条)の二種に分けている。また、後述「北京精彫 Vs 上海奈凱」ケースに対する判例評釈(中国最高人民法院公報掲載)及び「済南白兔 Vs 北京索邦等」においても、「ソフトウェア条例第 24 条第 1 項第 3 号の規定に基づき、著作権者がそのソフトウェア著作権を守るために施した技術措置を故意に避け、又は破壊する行為は、ソフトウェア著作権侵害行為である」と明言している。

<sup>222</sup> なお、法文は「回避又は破壊に用いる装置」等と規定しているため、単に技術的制限等に反応しない機器を販売しても規制対象ではない、ということになりうる。ただ、条文上、「回避」の定義規定がないため、「反応しない」ことが実質には回避に該当すると解釈される可能性が全くないとも限らず、このように解釈される場合には、無反応機器は規制対象となると思われる。また、ネットワーク伝播権保護条例では「主に技術措置の回避又は破壊に用いる装置又は部品を」と規定されている。この「主に」との文言によって、当該機器が技術措置を回避する機能を有していたとしても、技術措置の回避が主な目的でない場合は、規制対象とならないということになりうる。なお、2006 年司法解釈では『主に(中文『主要』)』ではなく『もっぱら(中文『専門』)』を使用している。中文『専門』の意義については、『他のことにかかわらないで、そのことだけをするさま』又は『それを主とするさま』という二通り(又はそれ以上)の解釈があり得るため、解釈の仕方によっては『主要』より狭く解釈される可能性がある。

<sup>223</sup> 原審事件番号：2006 年沪一中民五(知)初第 134 号

いう)を販売していた。CNC システムは、ソフトウェアである JDPaint と本体<sup>224</sup>から成る商品である。JDPaint は、上訴人の独自定義ファイルである Eng 形式のファイル(以下、「Eng ファイル」という。)を生成する仕組みになっていたため、通常のソフトウェアでは Eng ファイルを読み取ることができなかった。また、上訴人はこの Eng ファイルに暗号化を施していた。

ところが、被上訴人が、暗号化が施された Eng ファイルを読み取ることができる Ncstudio という商品を販売し始めたため、CNC システムの売り上げが減少した。

そこで上訴人は、Ncstudio による、暗号化が施された Eng ファイルを Ncstudio によって読み取る行為は、ソフトウェア著作権を保護するために施した技術措置の回避又は破壊行為に該当するとして、ソフトウェア条例第 24 条第 1 項第 3 号に基づき、被告の装置の開発及び販売の差止、公開謝罪及び損害賠償を求めた。しかし、原裁判所が上訴人の請求を退けたため、上訴人が上訴した。

争点は、①暗号化された Eng ファイルが、JDPaint に対して施された技術措置といえるか、②上訴人が JDPaint により生成されるファイルとして Eng ファイルを選択したことが、ソフトウェア条例第 24 条第 1 項第 3 号の「ソフトウェア著作権を保護するために」施した措置であるといえるか、の 2 点であった。

## イ 判旨(結論：差止請求、公開謝罪請求及び損害賠償請求のいずれについても請求棄却)

### (ア) 争点①について

まず、上訴人の独自定義ファイルである Eng ファイル自体は、JDPaint に対する技術措置には該当しない。なぜなら、Eng ファイルの基本的機能はデータ交換であり、JDPaint を暗号化により保護することを基本的機能とするものではないからである。また、Eng ファイル自体を分析等することにより JDPaint が複製されるという関係にはないからである。

また、Eng ファイルに施された暗号化も、JDPaint に対する技術措置には該当しない。なぜなら、Eng ファイルは JDPaint により作成されるものの、Eng ファイルに対して施された暗号化は、あくまでも Eng ファイルのみに対する暗号化であり、JDPaint に対するものとはいえないからである。

### (イ) 争点②について

上訴人が、JDPaint により作成されるファイルとして、上訴人の独自定義ファイルである Eng ファイルを採用したのは、JDPaint を CNC システムにおいてのみ使用できるようにして、JDPaint と本体の抱き合わせ販売を強固にするためである。上訴人による Eng ファイルの採用は、JDPaint を合法的に取得した者が、他のシステムにより JDPaint を使用する機会を排除する行為であり、ソフトウェア著作権に対して本来与

<sup>224</sup> 本体とは、精彫デジタルコントロールシステム及び機械のことである。

えられるべき保護範囲を超えているものである。従って、Eng ファイルは JDPaint を「保護するために」施した技術措置には該当しない。

- ・ **中国学術出版社 Vs 北京天地 データベース著作権紛争事件(北京市第一中級人民法院 [2006]一中民初字第 5890 号)(差止請求及び損害賠償請求事件)**

## **ア 事案の概要**

原告である「中国学術期刊(CD 版)」電子雑誌社は、「中国学術期刊(CD 版)」の編集、出版等を目的とする国有企業である。

被告である網聯天地(北京)科技有限公司は、コンピュータ関連サービス、ソフトウェアの開発、販売等を行う中小企業である。

原告は、「中国知網」というウェブサイトにおいて CNKI データベースの有料サービスを提供しており、ユーザーは予め取得した ID とパスワードを該当欄に入力してログインし、必要なデータ(論文等)を閲覧及びダウンロードすることができる仕組みになっていた。

これに対して、被告は、自らが情報を提供するウェブサイト(<http://www.sippo.com/>)を通じて、原告が CNKI データベースのために施した技術措置を回避する方法により<sup>225</sup>直接原告のデータベースにリンクをはり、ログインしたユーザーに有償で関連データを提供していた。

そこで原告が被告に対し、被告が無断で原告のデータベースにリンクをはり、ID とパスワードを他人に提供する等の法法により、原告のデータベースを他人に有償で提供した行為に対して、差止及び損害賠償を求めた。

## **イ 判旨(結論：差止請求及び損害賠償請求の一部につき請求認容)**

被告はネットワークサービスの経営者であるから、ネットワークにおける ID とパスワードの特性について知っていることは明らかである。被告は、営利目的の下に、原告の技術措置を回避して、原告が編集著作権を有するデータベースを他人に提供した。

被告の上記行為は、ネットワーク伝播権侵害及び故意に技術措置を回避する行為に該当する。

---

<sup>225</sup> 実際に被告がどのような方法を用いたのかについては、必ずしも明らかではない。

## 〈刑事事件〉

- ・ 「QQ 幻想」事件（(2006) 深南法刑初字第 803 号）（著作権侵害罪・不法経営罪被告事件）

### ア 事案の概要

X は「QQ 幻想」というインターネットゲームソフトを開発した。被告人 Y1 は、X の許可を得ずに「QQ 幻想」の暗号を復号化し、「QQ 幻想助理」というプラグインソフトを作成した。Y2 は、Y1 から「QQ 幻想助理」のソースコードを教えてもらい、Y3 乃至 Y5 とともに、「QQ 幻想助理」を販売して、総額約 31 万人民币元の利益を得た。

争点は、被告人らが、営利の目的で、著作権者の許可を得ず、著作権者が施した技術措置を破壊し、プラグインソフトを作成及び販売する行為が、①刑法第 217 条の著作権侵害罪に該当するか、②刑法第 225 条第 4 号の不法経営罪に該当するか、の 2 点である。

### イ 判旨（結論：著作権侵害罪につき否定、不法経営罪につき肯定<sup>226</sup>）

#### （ア）争点①について

被告人らが著作権者が施した技術措置を故意に破壊する行為は、刑法第 217 条で定める著作権侵害罪のいずれの規定にも該当しない。従って、刑法の「罪刑法定主義」の原則から、被告人の行為が著作権侵害罪に当たるものとするのは妥当ではない。

#### （イ）争点②について

被告人らが、国家主管部門の批准を得ずに、「QQ 幻想助理」を販売する経営行為は、インターネットの出版市場に関する国家の管理制度に違反し、インターネットゲーム市場の秩序を混乱させる行為であるため、刑法及び最高人民法院の「非法出版物刑事案件的法律適用に関する若干問題の解釈」に基づき、Y1 乃至 Y5 の 5 人に対して不法経営罪が成立する。

なお、Y1 は直接「QQ 幻想助理」の販売を行っていないものの、「QQ 幻想助理」の作成者であり、「QQ 幻想助理」を Y2 に提供すれば Y2 が「QQ 幻想助理」を販売するであろうことを知った上で Y2 に提供しており、かつ、「QQ 幻想助理」の売り上げの一部から報酬を得ていたのであるから、共同犯罪の意思伝達を行ったといえる。よって、Y1 にも

<sup>226</sup> 裁判所は、検察院の起訴罪名である著作権侵害罪については否定したものの、起訴罪名とされていなかった不法経営罪の成立を認めた。中国においては、刑事訴訟法の執行における若干問題に関する解釈（法積[1998]第 23 号）第 176 条第 2 号において「起訴事実が明確で、証拠が確実で且つ充分であり、起訴罪名と人民法院が審理・認定する罪名と異なる場合は、有罪判決を下さなければならぬ。」と規定されているため、裁判所は検察院の起訴罪名と異なる罪名により有罪判決を下すことができると解される。実際、中国の裁判実務においては、裁判所が検察院の起訴罪名と異なる罪名により有罪判決を下す例が少なくない。中国最高裁判所が公表している 1997 年 10 月から 2005 年 9 月までの 3077 事案の中で、罪名が変更された事案が約 12%を占めている（王満生＝揚節輝「法官可以変更指控罪名：德国的啓示」（政治与法律、2007 年第 5 期）脚注 1 参照）。



不法経営罪が成立する。

## (2) コンテンツの技術的手段に関する執行状況

コンテンツの技術措置の執行状況に関する資料は見当たらない。ただし、上記の判例等から、「技術措置」の合法性に関する判断基準として、大要、以下の 5 つを挙げることができる<sup>227</sup>。

- (i) 世界で一般的に使用され、かつ認められている技術措置(本報告書(2)の(a)項目のア(ア)(ii)以下ご参照)の合法性を肯定すべきであること
- (ii) 技術措置で保護する対象は、著作権法により保護される特定の著作物であり、制限する対象は、著作権者の授権又は著作権法に基づく合理的使用以外の著作権侵害行為であること
- (iii) 技術措置は攻撃性を持たないものでなければならないこと(例えば、ウィルスをもたらすような措置は、「技術措置」には該当しない。)
- (iv) 技術措置は著作権侵害行為(海賊版の製造活動)を制限するためのものであるが、権利侵害を阻止する限度を超えてはならないこと<sup>228</sup>
- (v) 技術措置は公的利益を害してはならないこと<sup>229</sup>

## (3) コンテンツの技術的手段に関する被害状況

見当たらない。

## 4. 技術動向の調査

### (1) コンテンツの技術的手段に関する技術動向

アクセス統制措置として暗号化技術が使用されており、コピーを制限する措置として SCMS がある。上記のほか、電子透かし、電子署名、電子指紋(Digital

<sup>227</sup> 中国著作権保護センター・新聞出版総署人事司編集《著作権判例評析》上海辞書出版社 2009 年 6 月第 1 版、判例 69 以下。最高人民法院民三庭庭長 蔣志培「インターネットにおける著作権の司法保護—インターネット著作権紛争案件に関する最高人民法院の司法解釈の理解と適用」(<http://www.shdf.gov.cn/newshtml?id=9530&category=27>)。

<sup>228</sup> 1997 年の江民事件において、江民というウィルスソフトウェアの開発、製造、販売等を行う会社は、自社製品にロジックロックという機能を採用していた。そのロジックロック機能は、江民社製のウィルスソフトウェアの海賊版を製造・提供している者にほとんど被害を与えていないにもかかわらず、海賊版を買った消費者(特に海賊版と知らない善意の第三者)の PC システムをロックし、システムの安全性を脅かすほどの被害を与えた。結果、北京市公安局は、江民社の行為は、自社製品の海賊版を抑制するために「ロジックロック」機能を搭載したとはいえ、「中華人民共和国コンピュータ情報システム安全保護条例」に違反するものとして、3000 人民元の過料処分を下した。江民事件に関する報道については、[http://www.etiri.com.cn/publishi/chanquan\\_show.php?id=~1059240](http://www.etiri.com.cn/publishi/chanquan_show.php?id=~1059240) 参照。

<sup>229</sup> 著作権法で認められる合理使用を制限するのは公的利益を害するとされるものとして、「技術措置がインターネットの権利侵害を攻撃する利器となる」(中国知識産権報 2006 年 7 月 6 日)参照。

Fingerprinting)等も使用されているとのことである<sup>230</sup>。ただし、これらが技術措置として利用されているのかは明らかではなく、権利管理情報として利用されている可能性もある。

## **(2) 電子透かし等、コンテンツの技術的手段に関する新たな技術**

北京華旗資訊デジタル・テクノロジー有限公司は 2002 年から中国の新華社と連携し、電子透かし技術を新華社の記者が撮影した写真に応用したとの報道がある。また、同社は、この技術をデジタルカメラに応用し、世界初の著作権保護機能を有するデジタルカメラを製造したとの報道もある<sup>231</sup>。ただし、この「著作権保護機能」が、技術措置が施されているという意味であるのかは明らかではなく、権利管理情報として利用されている可能性もある。

## **(3) 現在使用されている技術、及び、新たな技術に対する法律の対応状況**

2006 年より、国家版權局は WIPO と毎年 1 回中国において「国際版權シンポジウム」を共催し、著作権関連産業の発展及び保護を主題とし、先進国からインターネットに関連する産業界及び著作権に関する学界の代表を招いて、産業の新しい発展及び法律の対応について意見交換を行っている。中国政府は、コンテンツの技術措置及びそれを破壊・回避する手段への規制は国家の情報ネットワークの安全にかかわるものと認識されているため、法的対応は遅滞なくなされると思料される。

## **5. 各国内の議論(規制に対する賛否・改正動向等)**

### **(1) コンテンツの技術的手段に関する現行規制に対する議論**

#### **ア 技術措置の回避又は破壊禁止規定と権利制限規定との関係について**

技術措置の回避又は破壊禁止について、著作権法第 47 条第 6 号、ソフトウェア条例第 24 条第 1 項第 3 号、伝播権条例第 4 条第 2 項及び第 18 条第 2 号第 24 条が規定されている。しかし、その例外については、伝播権条例第 12 条に回避禁止に関する例外が規定されているだけで、他の規定は見当たらない。なお、権利制限規定として、著作権法第 22 条及び第 23 条が規定されている。

しかし、上記回避又は破壊禁止規定と著作権法第 22 条及び第 23 条の関係については明らかではなく、学説上激しい議論が繰り返されている。ただし、学説では、著作権法第 22 条及び第 23 条は、回避又は破壊行為に適用されないという見解が多数を占

<sup>230</sup> 「技術措置がインターネットの権利侵害を攻撃する利器となる」中国知識産権報 2006 年 7 月 6 日参照。

<sup>231</sup> <http://www.video.com.cn/tech/drm/200610/1161055931496.html> 参照。

める<sup>232</sup>。また、著作権法第47条第6号により、技術措置権という新たな権利が設けられたという見解も見られる<sup>233</sup>。

## イ 回避等行為に対する刑事責任の追及可否について

回避等行為に対する刑事責任について、著作権法第47条柱書、ソフトウェア条例第24条第1項柱書及び伝播権条例第18条柱書にいずれも規定が置かれており、例えば著作権法第47条柱書には「犯罪に該当するときは、法によって刑事責任を追及する」と規定されている。しかし、著作権法第47条第6号に該当する行為である、「技術措置を故意に回避又は破壊する行為」については、刑法の規定がない。そのため、著作権法第47条第6号に違反しても刑事責任を追及されることはない。もっとも、「技術措置を故意に回避又は破壊する行為」が、他人の刑法第217条(著作権侵害に関する罪)又は第218条(権利侵害複製品販売罪)該当行為を幫助等する行為に該当する場合には、知的財産権侵害刑事事件に関する最高人民法院＝最高人民検察院の司法解釈(法積[2004]第19号)<sup>234</sup>に基づき、共犯として訴追される可能性はある<sup>235</sup>。

## ウ 著作権集管理機構が技術措置を講じることができるか否か

著作権集管理機構とは、著作権者等の利益のために法に従い設立され、著作権者等の授権に基づき、著作権者等の著作権等に対して集管理を行う社会団体である(著作権集管理条例<sup>236</sup>第3条第1項)。

しかし、著作権集管理機構が著作権者等に与えられた技術措置を自ら講じることができるか否かについては必ずしも明らかではないが、著作権集管理機構は、著作

<sup>232</sup> 李楊「技術措置権及其反思(On Right to Technical Measures)」ネットワーク法律評論2002年第2巻9頁、王遷「対技術措置立法保護的比較研究」知識産権2003年第13巻74期3頁、張耕「略論版権的技術保護措置(On the Technologically Protective Measures of Copyright)」現代法学2004年4月第26巻第2期123頁、朱理「版権技術措置法律保護的三個等級(Technological Measure, Copyright, Limitations and Exceptions)」ネットワーク法律評論2005年第6巻第1期34頁、羅莉「数字私人複製所引起的利益平衡問題(Interests Balancing of Private Digital Copying)」法学2008年第318期88頁、梁志文「版権人的自力救済及其限度(Copyright Holder's Private Remedy and Its Limits: Black Screen Incident of Microsoft)」法学2008年第325期120頁、熊琦「論接触権(Also Concerning the Defects of Classification of Property Right of Copyright and Its Overcoming)」法律科学2008年第169期93頁。

<sup>233</sup> 李楊「技術措置権及其反思(On Right to Technical Measures)」ネットワーク法律評論2002年第2巻9頁。ただし、これに反対する見解としては、張耕「略論版権的技術保護措置(On the Technologically Protective Measures of Copyright)」現代法学2004年4月第26巻第2期123頁等がある。

<sup>234</sup> 「知的財産権侵害刑事事件の処理における具体的な法律適用の若干問題に関する解釈」(2004年12月8日公布、同月22日施行)第16条。

<sup>235</sup> 任軍民「法国信息网络刑事保護对我国有关立法啓示(Enlightenment on China's Legislation view on Criminal Protection of France's Information Network)」知識産権2006年第16巻第95期85頁。

<sup>236</sup> 行政法規、2004年12月28日公布、翌年3月1日施行。

権者等の授権により、自己の名義で著作権等使用許諾契約の締結、利用料の徴収及び単独で著作権等に関する訴訟及び仲裁に参加することができるのみならず、「著作権者等に関する権利を行使」することができるため(同条例第 2 条)、自ら技術措置を施すことができるという見解が存在する<sup>237</sup>。

## **(2) コンテンツの技術的手段に関する規制に対する業界からの要望状況**

コンテンツ産業界は、技術措置に関する規制及び法律執行の強化を期待している。また、ハイテック企業は、技術措置の採用が新しいビジネス・新しい市場としてとらえられているため、技術措置に関する規制の強化を擁護している。

## **(3) 法改正の動向・内容**

著作権関連業界及び学界では、著作権法の第二回の改正の要望が強いため、2007 年より、国家版權局は著作権法の第二回改正に関する研究・論証作業を進めている。2009 年 4 月頃、国家版權局副局長閻曉宏は記者会見で、「わが国の著作権法は 20 世紀 90 年代に制定・公布されたもので、2001 年に一回目の改正がなされた。一回目の改正は WTO 加盟に伴い、著作権法を国際ルールに適応させるための改正である。2001 年から現在まで、すでに 8 年が過ぎた。この間、技術の進歩、国内外の環境の変化、著作権関連産業の発展は著しく、著作権法はそれに相応する改正を行う必要がある。」と、著作権の改正作業を加速させる意思を表明した<sup>238</sup>。ただ、今年是中国商標法及び不正競争防止法の改正作業が迫っているため、著作権法の改正成立まで少なくとも二、三年かかるのではないかと予想される。

以 上

<sup>237</sup> 張耕「略論版權的技術保護措置(On the Technologically Protective Measures of Copyright)」現代法学 2004 年 4 月第 26 卷第 2 期 124 頁。

<sup>238</sup> 「国家版權局：著作権法が再度改正、インターネット関連内容を追加予定」(2009 年 4 月 22 日北京晨报)。「専門家検討：著作権法の第 2 次改正」(2009 年 6 月 30 日中国芸術報)。

## (関連条文)

### 著作権法<sup>239</sup>

#### (著作物の自由利用)

#### 第 22 条

次の各号に掲げる著作物利用の場合には、著作権者の許諾を受けず、著作権者に報酬を支払わなくてもよい。但し、著作者の氏名、著作物の名称を明示しなければならず、かつ著作権者が本法によって享有するその他の権利を侵害してはならない。

- (1) 個人的な学習、研究又は鑑賞のために、他人の公表された著作物を利用する場合
- (2) ある著作物を紹介し、批評し、又はある問題を説明するため、著作物の中で他人の公表された著作物を適当に引用する場合
- (3) 時事ニュースの報道のために、新聞、雑誌、放送局、テレビ局等のメディアで、すでに公表された著作物を不可避免的に再現し又は引用する場合
- (4) 新聞、雑誌、ラジオ局、テレビ局等のメディアが、他の新聞、雑誌、ラジオ局、テレビ局等のメディアによってすでに公表された、政治、経済、宗教問題に関する時事的な文章を掲載し又は放送する場合。但し著作者が掲載、放送を禁じる旨の声明をした場合を除く。
- (5) 新聞、雑誌、ラジオ局、テレビ局等のメディアが公衆の集会で行われた演説を掲載し又は放送する場合。但し、著作者が掲載、放送を禁ずる旨の声明をした場合を除く。
- (6) 学校の授業又は科学研究のために、すでに公表された著作物を翻訳し又は少量複製して、教育又は科学研究者の使用に供する場合。但し、出版、発行してはならない。
- (7) 国家機関が公務遂行のために、合理的な範囲内ですでに公表された著作物を利用する場合
- (8) 図書館、公文書館、記念館、博物館、美術館等が陳列又は原物保存の必要のために、当該館に収蔵されている著作物を複製する場合
- (9) すでに公表された著作物を無料で実演し、当該実演が公衆から料金を受けとらず、実演者にも報酬を支払っていない場合
- (10) 屋外の公共の場所に設置又は陳列された芸術著作物について、模写、写生、撮影、録画を行う場合
- (11) 中国の公民、法人又はその他の組織がすでに公表した、漢民族の言語・文字で創作された著作物を少数民族の言語・文字に翻訳して国内で出版、発行する場合

<sup>239</sup> 本法の中国語テキストは以下のサイトで確認できる。  
<[http://www.npc.gov.cn/wxzl/gongbao/2001-10/29/content\\_5277072.htm](http://www.npc.gov.cn/wxzl/gongbao/2001-10/29/content_5277072.htm)>

(12) 公表された著作物を点字に改めて出版する場合

前項の規定は出版者、実演家、録音・録画制作者、ラジオ局、テレビ局の権利の制限にも適用する。

### **(教科書への掲載)**

#### **第 23 条**

九年制義務教育及び国の教育計画を実施する為に編集、出版される教科書については、著作者が事前に利用を禁じる旨の声明をした場合を除き、著作権者の許諾を受けないで、その中にすでに公表された著作物の一部又は短編の文字著作物、音楽著作物又は単独の美術著作物、写真著作物を取り入れることができる。但し、規定に従って報酬を支払い、著作者の氏名、著作物の名称を明示しなければならず、かつ著作権者が本法によって享有するその他の権利を侵害してはならない。

前項の規定は出版社、実演家、録音・録画製作者、ラジオ局、テレビ局の権利の制限にも適用する。

### **(技術措置を回避又は破壊した者の責任)**

#### **第 47 条第 6 号**

次の各号に掲げる不法行為を行った場合には、情状に応じて侵害の停止、影響の除去、謝罪、損害賠償等の民事責任を負わなければならない。同時に公共の利益を損なった場合には、著作権行政管理部門が不法行為停止を命じ、違法所得を没収し、権利侵害複製品を没収、廃棄し、また、過料に処することができる。情状が重大である場合には、著作権行政管理部門はさらに、主に権利侵害複製品の製作に使われた材料、道具、設備等を没収することができる。犯罪に該当する場合は、法によって刑事責任を追及する。

(6) 著作権者又は著作権に関連する権利者の承諾を得ずに、権利者がその著作物、録音・録画製品等のために施した著作権又は著作権に関連する権利を保護する技術措置を故意に回避又は破壊すること。但し、法律、行政法規に別段の定めがある場合を除く。

### **著作権法实施条例<sup>240</sup>**

#### **(行政処罰)**

#### **第 36 条**

著作権法第 47 条に掲げる不法行為があり、同時に社会公共の利益を侵害した場

<sup>240</sup> 本条例の中国語テキストは以下のサイトで確認できる。  
<[http://www.gov.cn/gongbao/content/2002/content\\_61712.htm](http://www.gov.cn/gongbao/content/2002/content_61712.htm)>

合、著作権行政管理部門は、不法経営額の 3 倍以下の過料に処することができる。不法経営額を計算することが難しい場合は、10 万元以下の過料に処することができる。

## コンピューター・ソフトウェア保護条例<sup>241</sup>

### (技術措置を回避又は破壊した者の責任)

#### 第 24 条第 1 項柱書及び第 3 号

「中華人民共和国著作権法」、本条例又はその他の法律、行政法規に別途規定している場合を除き、ソフトウェア著作権者の許諾を得ずに、次の各号に掲げる不法行為があった場合、情状に応じて侵害の停止、影響の除去、謝罪、損害賠償等の民事責任を負わなければならない。同時に社会公共の利益を損なった場合は、著作権行政管理部門が不法行為の停止を命じ、違法所得を没収し、権利侵害複製品を没収、廃棄し、かつ過料に処することができる。情状が重大である場合は、著作権行政管理部門は、さらに主に権利侵害複製品の製作に用いられた材料、道具、設備等を没収することができる。刑法に触れる場合、著作権侵害罪、権利侵害複製品販売罪に関する刑法の規定に照らし、法により刑事責任を追及する。

- (3) 著作権者がそのソフトウェア著作権を守るために施した技術措置を故意に避け、又は破壊した場合

### (過料)

#### 第 24 条第 2 項

前項第 1 号又は第 2 号の行為があった場合、1 件につき 100 人民元又は製品価値の 5 倍以下の過料に処することができる。前項第 3 号、第 4 号又は第 5 号の行為があった場合、5 万人民元以下の過料に処することができる。

## ネットワーク伝播権保護条例<sup>242</sup>

### (情報ネットワーク伝播権の保護)

#### 第 2 条

権利者が享有する情報ネットワーク伝播権は、著作権法及び本条例の保護を受ける。法律、行政法規に別途規定がある場合を除き、いかなる組織又は個人も、他人の著作物、実演、録音・録画製品を情報ネットワークを通じて公衆に提供する場合は、

<sup>241</sup> 本条例の中国語テキストは以下のサイトで確認できる。  
<[http://www.gov.cn/gongbao/content/2002/content\\_61861.htm](http://www.gov.cn/gongbao/content/2002/content_61861.htm)>

<sup>242</sup> 本条例の中国語テキストは以下のサイトで確認できる。  
<[http://www.gov.cn/gongbao/content/2006/content\\_327751.htm](http://www.gov.cn/gongbao/content/2006/content_327751.htm)>

権利者の許諾を取得し、かつ報酬を支払わなければならない。

### **(技術措置の回避・破壊)**

#### **第4条**

情報ネットワーク伝達権を保護するため、権利者は技術措置を講じることができる。

いかなる組織又は個人も技術措置を故意に回避し又は破壊してはならず、主に技術措置の回避又は破壊に用いる装置又は部品を故意に製造、輸入又は公衆に提供してはならず、また他人が技術措置を回避し又は破壊するための技術的サービスを故意に提供してはならない。但し、法律、行政法規に回避できると定められている場合を除く。

### **(図書館等の収蔵物のデジタル化著作物)**

#### **第7条**

図書館、公文書館、記念館、博物館、美術館等は、著作権者の許諾を得ずに、情報ネットワークを通じて、当該館内のサービス対象に当該館内に収蔵されている合法的に出版されたデジタル著作物及び法に従い陳列又は原物保存の必要のためにデジタル化形式で複製された著作物を提供することができ、これに対し報酬を支払わないものとするが、直接又は間接に経済的利益を獲得してはならない。当事者に別途約定のある場合を除く。

前項に定める陳列又は原物保存のためにデジタル化形式で複製する必要がある著作物は、すでに破損し若しくは破損、紛失若しくは盗難の危機にあるもの、又はその保存様式がすでに旧式化してしまった場合で、かつ市場で購入できない若しくは表示価格を遥かに上回る価格でしか購入できない著作物でなければならない。

### **(教育ソフトの制作・提供)**

#### **第8条**

情報ネットワークを通じて九年制義務教育又は国の教育計画を実施する場合は、著作権者の許諾を得ずに、そのすでに公表された著作物の一部又は短編の文字著作物、音楽著作物又は一幅の美術著作物、写真著作物を利用して教育ソフトを制作することができ、教育ソフトを制作した又は法に従い教育ソフトを取得した遠隔教育機構が情報ネットワークを通じて登録している学生に提供することができる。但し、著作権者に報酬を支払わなければならない。

### **(農村地区の公衆への著作物の提供)**

#### **第9条**

貧困救済のため、情報ネットワークを通じて農村地区の公衆に、中国公民、法人又



はその他の組織がすでに公表した栽培・養殖、病気の予防治療、防災減災等の貧困救済に関連する著作物及び基本的な文化的需要に適応した著作物を無料で提供する場合、ネットワークサービス提供者は、提供する前に、提供しようとする著作物及びその著作者並びに支払予定の報酬基準を公告しなければならない。公告した日から 30 日以内に、著作権者が提供に同意しない場合は、ネットワークサービス提供者はその著作物を提供してはならない。公告の日から 30 日以内に著作権者に異議のない場合は、ネットワークサービス提供者はその著作物を提供することができ、かつ公告した基準に従い著作権者に報酬を支払う。ネットワークサービス提供者が著作権者の著作物を提供した後に、著作権者が提供に同意しなかった場合は、ネットワークサービス提供者は直ちに著作権者の著作物を削除し、かつ公告した基準に従い著作権者に著作物を提供した期間の報酬を支払わなければならない。

前項の規定に従い著作物を提供する場合、直接又は間接に経済的利益を獲得してはならない。

#### **(情報ネットワーク伝播権制限の場合の遵守条件)**

##### **第 10 条柱書及び第 4 号**

本条例の規定に従い著作権者の許諾を得ずに情報ネットワークを通じて公衆にその著作物を提供する場合は、さらに次の各号に掲げる規定を遵守しなければならない。

- (4) 技術措置を講じて、本条例第 7 条、第 8 条、第 9 条に定めるサービス対象以外のその他の者が著作権者の著作物を取得することを防止し、かつ本条例第 7 条に定めるサービス対象の複製行為が著作権者の利益に実質的な損害をもたらすことを防止する。

#### **(情報ネットワークを通じた実演及び録音・録画製品の提供)**

##### **第 11 条**

情報ネットワークを通じて他人に実演、録音・録画製品を提供する場合は、本条例第 6 条から第 10 条までの規定を遵守しなければならない。

#### **(技術措置の回避が許される場合)**

##### **第 12 条**

次の各号の事由に該当する場合は、技術措置を回避することができる。但し、他人に技術措置を回避する技術、装置又は部品を提供してはならず、権利者が法に従い享有するその他の権利を侵害してはならない。

- (1) 学校の授業又は科学研究のために、情報ネットワークを通じて少数の教育、科学研究者のためにすでに公表された著作物、実演、録音・録画製品を提供する場合で、当該著作物、実演、録音・録画製品が情報ネットワークによってのみしか取得できないとき

- (2) 営利を目的とせず、情報ネットワークを通じて視覚障害者が感知できる独特な方法によりすでに公表された文字作品を視覚障害者に提供する場合で、当該著作物が情報ネットワークによってのみしか取得できないとき
- (3) 国家機関が行政、司法の手續に従い公務を執行する場合
- (4) 情報ネットワーク上でコンピュータ及びそのシステム又はネットワークに対して安全性能をテストする場合

#### **(技術措置を回避又は破壊した者の責任)**

##### **第 18 条第 2 号**

本条例の規定に違反し、次の各号に掲げられる不法行為のいずれかがある場合は、状況に応じて権利侵害の停止、影響の除去、謝罪、損害賠償等の民事責任を負わなければならない。同時に公共の利益を損ねた場合は、著作権行政管理部門が不法行為の停止を命じ、違法所得を没収し、かつ 10 万元以下の過料に処することができる。情状が重い場合は、著作権行政管理部門は、主にネットワークサービスの提供に使用するコンピュータ等の設備を没収することができる。犯罪を構成する場合は、法に従い刑事責任を追及することができる。

- (2) 故意に技術措置を回避し又は破壊した場合

#### **(情報ネットワークを通じて無断で著作物を公衆に提供等した者の責任)**

##### **同条第 5 号**

- (5) 情報ネットワークを通じて提供する他人の著作物、実演、録音・録画製品に、著作物、実演、録音・録画製品の名称又は著作者、実演者、録音・録画製作者の氏名(名称)を明示していない場合、或いは報酬を支払っていない場合、或いは本条例の規定に従い技術措置を講じてサービス対象以外にその他の者が他人の著作物、実演、録音・録画製品を取得することを阻止しなかった場合、或いはサービス対象の複製行為が権利者の利益に対し実質的損害をもたらすことを阻止しなかった場合

#### **(技術措置の回避・破壊に用いる装置を製造等した者の責任)**

##### **第 19 条第 1 号**

本条例の規定に違反し、次の各号に掲げるいずれかの行為がある場合、著作権行政管理部門は警告を与え、違法所得を没収し、主に技術措置の回避、破壊に用いる装置又は部品を没収することができる。情状が重い場合は、主にネットワークサービスの提供に用いるコンピュータ等の設備を没収し、かつ 10 万元以下の過料に処することができる。犯罪を構成する場合は、刑事責任を追及する。

- (1) 主に技術措置の回避、破壊に持する装置又は部品を故意に製造し、輸入し又は他人に提供し、或いは他人が技術措置を回避し又は破壊するために技術的サービス

を故意に提供した場合

### (用語の定義)

#### 第26条第1項、第2項

本条例における用語の定義は以下の通りである。

情報ネットワーク伝達権とは、有線又は無線の方式により公衆に著作物、実演、又は録音・録画製品を提供し、公衆にその個人的に選択した時間及び場所において著作物、実演又は録音・録画製品を獲得させる権利をいう。

技術措置とは、権利者の許諾を得ずに著作物、実演、録音・録画製品を閲覧、鑑賞すること、又は情報ネットワークを通じて公衆に著作物、実演、録音・録画製品を提供することを防止、制限するために用いる有効な技術、装置又は部品をいう。

### 著作権集管理條例<sup>243</sup>

#### (著作権集管理の定義)

##### 第2条

本条例にいう著作権集管理とは、著作権集管理組織が権利者の授権を経て、集中的に権利者の関連する権利を行使し、かつ自己の名義をもって次の各号に掲げる活動を行うこうをいう。

- (1) 使用者と著作権又は著作権に関連する権利の使用許諾契約(以下「使用許諾契約」という)を締結する。
- (2) 使用者から使用料を徴収する。
- (3) 権利者の使用料を支払う。
- (4) 著作権又は著作権に関連する権利にかかる訴訟、仲裁等を行う。

#### (著作権集管理組織の定義)

##### 第3条

本条例に言う著作権集管理機構とは、権利者の利益のために法により設立され、権利者の授権に基づき権利者の著作権又は著作権に関連する権利に対して集管理を行う社会団体をいう。

著作権集管理機構は、社会団体登記管理に関する行政法規及び本条の規定に従い登記を行い活動を展開しなければならない。

---

<sup>243</sup> 本条例の中国語テキストは以下のサイトで確認できる。  
<[http://www.gov.cn/gongbao/content/2005/content\\_63330.htm](http://www.gov.cn/gongbao/content/2005/content_63330.htm)>

**(方法等の提供等行為)**

**第 6 条**

もっぱら他人の技術措置を故意に回避又は破壊するための方法、設備又は材料として使用されることを明らかに知りながら、掲載、伝播又は提供を行ったネットワークサービス提供者について、人民法院は当事者の訴求及び詳細な情状に基づき、著作権法第 47 条第 6 号の規定に従い、不法行為責任を追及することができる。

**民法通則<sup>245</sup>**

**(共同不法行為)**

**第 130 条**

2 人以上の者が共同不法行為により他人に損害を与えた場合には連帯責任を負わなければならない。

**(民事責任の負担方式)**

**第 134 条**

民事責任の負担方式には、主として次のものがある。

- (1) 侵害の停止
- (2) 妨害の排除
- (3) 危険の除去
- (4) 財産の返還
- (5) 原状の回復
- (6) 修理、再製作及び交換
- (7) 損害の賠償
- (8) 違約金の支払
- (9) 影響の除去及び名誉の回復
- (10) 謝罪

前項の民事責任の負担方式は、単独で用いることができ、併用することもできる。

人民法院は、民事事件の審理において、前項の規定を適用するほか、訓戒又は始末書提出を命じ、不法活動に用いられる財物及び不法所得を没収することができ、かつ

---

<sup>244</sup> 本司法解釈の中国語テキストは以下のサイトで確認できる。  
<[http://www.court.gov.cn/sfjs/show.php?file\\_id=114658&key=%B7%A8%CA%CD](http://www.court.gov.cn/sfjs/show.php?file_id=114658&key=%B7%A8%CA%CD)>

<sup>245</sup> 本法の中国語テキストは以下のサイトで確認できる。  
<[http://www.npc.gov.cn/wxz1/wxz1/2000-12/06/content\\_4470.htm](http://www.npc.gov.cn/wxz1/wxz1/2000-12/06/content_4470.htm)>

法律の規定に基づき過料又は拘留に処することができる。

## 民法通則意見<sup>246</sup>

### (共同不法行為)

#### 第 148 条第 1 項

他人を教唆及び幫助して不法行為を行わせた者は、共同の不法行為者であり、連帯した民事責任を負わなければならない。

## 刑法<sup>247</sup>

### (著作権侵害罪)

#### 第 217 条

営利を目的とし、次の各号に掲げる著作権侵害事由のいずれかに該当し、違法所得金額が比較的大きく又はその他の重い情状のある場合は、3 年以下の有期懲役若しくは拘留に処し、罰金を併科し、又は罰金を単科する。違法所得金額が巨額であり又はその他の特に重い情状のある場合には、3 年以上 7 年以下の有期懲役に処し、罰金を併科する。

- (1) 著作権者の許諾を経ずに、その文字作品、音楽、映画、テレビ、録画作品、コンピュータソフトウェア及びその他の作品を複製・発行したとき。
- (2) 他人の専有出版権を有する図書を出版したとき。
- (3) 録音録画製作者の許諾を経ずに、当該製作者が製作した録音録画を複製・発行したとき。
- (4) 他人の署名を冒用した美術作品を製作し、販売したとき。

### (権利侵害複製品販売罪)

#### 第 218 条

営利を目的とし、本法第 217 条に定める権利侵害複製品であることを明らかに知りながらこれを販売し、違法所得金額が巨額である者は、3 年以下の有期懲役若しくは拘留に処し、罰金を併科し、又は罰金を単科する。

---

<sup>246</sup> 本司法解釈の中国テキストは以下のサイトで確認できる。  
<[http://www.court.gov.cn/sfjs/show.php?file\\_id=7385&key=%B7%A8%CA%CD](http://www.court.gov.cn/sfjs/show.php?file_id=7385&key=%B7%A8%CA%CD)>

<sup>247</sup> 本法の中国語テキストは以下のサイトで確認できる。  
<[http://www.npc.gov.cn/wxzl/gongbao/2000-12/17/content\\_5004680.htm](http://www.npc.gov.cn/wxzl/gongbao/2000-12/17/content_5004680.htm)>

## (不法経営罪)

### 第 225 条第 4 号

国の規定に違反し、次の各号に掲げる不法経営行為のいずれかをして、市場秩序を攪乱し、情状が重い者は、5 年以下の有期懲役若しくは拘留に処し、違法所得と同額以上 5 倍以下の罰金を併科し、又は罰金を単科する。情状が特に重い場合には、5 年以上の有期懲役に処し、違法所得と同額以上 5 倍以下の罰金又は財産没収を併科する。

(4) <sup>248</sup>市場秩序を重大に攪乱するその他の不法経営行為

法釈[2004]第 19 号 <sup>249</sup>

## (共犯)

### 第 16 条

他人が知的財産権侵害犯罪を実施することを明らかに知りながら、その者のために貸付、資金、口座、領収書、証明、許可証、又は生産、経営場所、若しくは運輸、貯蔵、輸出入代理等の便宜、幫助を提供した場合は、知的財産権犯罪の共犯者として処罰を決定する。

知的財産権税関保護条例 <sup>250</sup>

## (荷受人・荷送人の知的財産権状況についての申告義務)

### 第 5 条

輸入貨物の荷受人又はその代理人及び輸出貨物の荷送人及びその代理人は、国の規定に従い、税関に対し、輸出入貨物と関連のある知的財産権の状況を事実通りに申告し、かつ関連証明文書を提出しなければならない。

## (知的財産権の税関総署における登録)

### 第 7 条

知的財産権者は、本条例の規定に基づき、その知的財産権について税関総署に登録

<sup>248</sup> 本号の番号は、1999 年 12 月 25 日に公布された刑法修正案 8 条 (<[http://www.npc.gov.cn/wxzl/wxzl/2000-12/05/content\\_4760.htm](http://www.npc.gov.cn/wxzl/wxzl/2000-12/05/content_4760.htm)>)により、第 3 号より第 4 号に変更された。ただ、上記脚注 9 に引用されたサイトには第 3 号のままになっている。

<sup>249</sup> 本司法解釈の中国語テキストは以下のサイトで確認できる。  
<[http://www.court.gov.cn/sfjs/show.php?file\\_id=98384&key=%B7%A8%CA%CD](http://www.court.gov.cn/sfjs/show.php?file_id=98384&key=%B7%A8%CA%CD)> 又は  
<<http://www.spp.gov.cn/site2006/2006-02-28/000934936.html>>

<sup>250</sup> 本条例の中国語テキストは以下のサイトで確認できる。  
<[http://www.gov.cn/gongbao/content/2004/content\\_63078.htm](http://www.gov.cn/gongbao/content/2004/content_63078.htm)>

を申請することができる。登録を申請する場合、申請書を提出しなければならない。申請書には、次の各号の内容を記載するものとする。

- (1) 知的財産権者の名称又は氏名、登録地又は国籍等
- (2) 知的財産権の名称、内容及びその関連情報
- (3) 知的財産権の使用許諾状況
- (4) 知的財産権者が知的財産権を合法的に使用する貨物の名称、産地、出入国地の税関、輸出入業者、主な特徴、価格等
- (5) 知的財産権を侵害する既知の貨物の製造者、輸出入業者、出入国地の税関、主な特徴、価格等

前項に定める申請書の内容について証明書がある場合、知的財産権者は、証明文書を添付しなければならない。

### **(貨物の差押えの申請)**

#### **第 12 条**

知的財産権者は、権利侵害の疑いのある貨物が輸出入されようとしているのを発見したときは、貨物出入国地の税関に、権利侵害の疑いのある貨物の差押を申請することができる。

### **(税関が知的財産権侵害疑いに気づいた場合に、知的財産権者に書面通知する義務)**

#### **第 16 条**

税関が輸出入貨物に登録された知的財産権を侵害する疑いがあることに気づいた場合、直ちに書面で知的財産権者に通知しなければならない。知的財産権者が通知送達日から 3 執務日以内に本条例第 13 条の規定に従い申請を提出し、かつ本条例第 14 条の規定に従い担保を提供したときは、税関は、権利侵害の疑いのある貨物を差押え、書面で知的財産権者に通知し、かつ税関差押証明書を荷受人又は荷送人に送達しなければならない。知的財産権者が期間内に申請を提出しない、又は担保を提供しないときは、税関は貨物を差押えてはならない。

### **(貨物の点検)**

#### **第 17 条**

税関の同意を得て、知的財産権者及び荷受人又は荷送人は、関連貨物を点検することができる。

### **(税関と知的財産権主管部門の協力義務)**

#### **第 21 条**

税関が差し押さえた権利侵害の疑いのある貨物について調査を行うにあたり、知的財産権主管部門に協力を求める場合、関連知的財産権主管部門は、協力しなければならない。

らない。

知的財産権主管部門が輸出入貨物に関わる権利侵害事件の処理にあたり、税関に協力を求める場合、税関は、協力しなければならない。

### **(訴訟提起前の不法行為の差し止め及び財産保全)**

#### **第 23 条**

知的財産権者は、税関に保護措置の実施を申請した後、「中華人民共和国商標法」、「中華人民共和国著作権法」又は「中華人民共和国専利法」の規定に基づき、訴えを提起する前に、差し押さえられた権利侵害の疑いのある貨物について、人民法院に対し、不法行為差止命令又は財産保全措置の実施を申請することができる。

税関は、人民法院の不法行為差止命令又は財産保全に関する執行協力通知を受領した場合、協力しなければならない。

### **(犯罪の疑いのある事件を公安機関へ移送)**

#### **第 26 条**

税関は、知的財産権保護の実施にあたり、犯罪の疑いのある事件を発見したときは、事件を公安機関に移送して処理させなければならない。

### **(侵権貨物の没収及び処分)**

#### **第 27 条**

差し押さえた権利侵害の疑いのある貨物が税関の調査を経て知的財産権を侵害すると認定された場合、税関が没収する。

税関は、知的財産権を侵害する貨物を没収した後、知的財産権を侵害する貨物の関連状況を書面で知的財産権者に通知しなければならない。

没収された知的財産権を侵害する貨物を社会公益事業に用いることができる場合は、税関は、関連公益機関に引渡して社会公益事業に用いさせなければならない。知的財産権者に買取の意思がある場合は、税関は、有償で知的財産権者に譲渡することができる。没収された知的財産権を侵害する貨物を社会公益事業に用いることができず、かつ知的財産権者に買取の意思がない場合は、税関は、権利侵害の特徴を取り除いた後、法に従い競売することができる。権利侵害の特徴を取り除くことができないときは、税関は、これを廃棄しなければならない。



## 不正競争防止法<sup>251</sup>

### (不正競争及び事業者の定義)

#### 第2条

事業者は市場取引において、自由意思、平等、公正、誠実信用の原則に従い、みんなに認められる商業道德を遵守しなければならない。

本法にいう不正競争とは、事業者が本法の定めに違反し、他の事業者の合法的な権益に損害を与え、社会の経済秩序を乱す行為をいう。

本法にいう事業者とは、商品経営又は営利性サービス(以下「商品」にはサービスを含む)に従事する法人、その他の経済組織及び個人をいう。

---

<sup>251</sup> 本法の中国語テキストは以下のサイトで確認できる。  
<[http://www.npc.gov.cn/wxzl/gongbao/2000-12/05/content\\_5004600.htm](http://www.npc.gov.cn/wxzl/gongbao/2000-12/05/content_5004600.htm)>



資料 A

現地報告書 (EU 編)

(英文)



Research Issues for Research and Study of Each Country's Legal Framework  
Concerning Technological Measures to Protect Contents

**European Union**

**Part One Recital**

The firm is to research and assemble information on the following research issues (inquiry items) and to report to Nishimura & Asahi in writing in English.

**Part Two Research Issues (Inquiry Items)**

**1. International Rules**

- (1) Whether the research subject country is a party to any treaties that have provisions concerning technological measures to protect contents (e.g., WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty).

The European Community as well as individual Member States of the European Union such as France, the United Kingdom and Germany, are parties to the WIPO Copyright Treaty (the "WCT") and the WIPO Performances and Phonograms Treaty (the "WPPT") adopted on 20 December 1996.

Article 11 of the WCT and Article 18 of the WPPT ("Obligations concerning Technological Measures") provide that: "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

Article 12 of the WCT and Article 19 of the WPPT ("Obligations concerning Rights Management Information") provide that:

"(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use

of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.”

---

- (2) Whether the FTAs/EPAs to which the research subject country is a party include any provisions concerning technological measures to protect contents. If they are included, the substance thereof.

More than four years after the WCT and the WPPT were signed (but before they entered into effect<sup>1</sup>), the European Union adopted rules concerning technological measures in Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (the “Information Society Directive”).<sup>2</sup>

---

<sup>1</sup> Although they were adopted on 20 December 1996, the WCT only entered into force on March 6, 2002 and the WPPT on 20 May 2002 (after ratification by 30 Contracting Parties).

<sup>2</sup> Before the Information Society Directive was enacted, the problem of safeguarding conditional access systems and devices first arose in Europe with a recommendation issued by the Council of Europe in 1991. The Council of Europe passed a Recommendation of the Committee of Ministers to Member States (No. R(91)14) on legal protection of encrypted television services, later completed by Recommendation No. R(95)1 on Measures against Sound and Audiovisual Piracy. In 1996 the European Commission addressed the piracy problem in a Green Paper on the legal protection of encrypted services in the internal market. Following a survey conducted in 1995, the Green Paper noted that there was a substantial difference in the level of protection in the Member States’ national legislations in relation to encrypted services. Hence, the Commission saw a need to legislate on anti-piracy legal protection, more precisely to harmonise national legislations protecting electronic remunerated services using conditional access systems. Following the recognition of a need for Community action, the European Union had adopted Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access (the “Conditional Access Directive”), aiming to protect access to and remuneration for various kinds of services delivered electronically (e.g., television and radio broadcasting, whether by wire or over the air including by satellite, as well as “information society services”) and through means of conditional access (i.e., “any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior individual authorization” of the service provider). Examples are pay-per-view and encrypted television and Internet websites which charge for access. The legal protection afforded to such services by the Conditional Access Directive consists of requiring Member States to take measures against illicit devices which give unauthorised access to protected services that are remunerated. Indeed the Conditional Access Directive provides that Member States are required to prohibit activities relating to the manufacturing, trading, possession, installation of (in every instance for commercial purposes) and use of commercial communications to promote any equipment or computer program designed or adapted to give access to a protected service in an intelligible form without the prior authorization of the service provider (in practice, hardware devices such decoders, but also functional smart cards and computer programs to bypass protection). It is targeted at ensuring that the service provider is remunerated, rather than at protecting the content of the service itself. As regards the relationship between the Conditional Access Directive and the Information Society Directive, it is possible that the protections granted by the Information Society Directive against the circumvention of technological measures (such as copy control and access control mechanisms) overlap in certain cases with the provisions of the Conditional Access Directive, so that certain technological measures could be protected on both

The Information Society Directive was adopted after several years of enquiry and discussions at the European Commission. In 1995, the Commission published a Green Paper on Copyright and Related Rights in the Information Society and on 10 December 1997 it introduced its first Proposal for the Information Society Directive, followed by an amended proposal on 21 May 1999. When the initial Proposal for the Information Society Directive was drafted, EU law on the subject matter was essentially limited to Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (as amended and codified by Directive 2009/24/EC of 23 April 2009, the “Computer Programs Directive”)<sup>3</sup> and Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (the “Database Directive”)<sup>4</sup>. As it was necessary to adapt and supplement these Directives to respond to new economic realities, a “Common Position” was adopted on 28 September 2000 and the Information Society Directive was adopted 8 months later.

The Information Society Directive recognizes that “there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect” (recital 47), without, however, “preventing the normal operation of electronic equipment and its technological development” (recital 48).

According to Article 6 of the Information Society Directive entitled “Obligations as to technological measures,” Member States are required to provide “adequate legal protection against the circumvention of any effective technological measures”. Mimicking the structure adopted in the WCT and the WPPT, rights-management information are treated separately in Article 7 of the Information Society Directive, which provides for legal protection against the removal or alteration of electronic rights-management information. Sanctions regarding the violation of the Information Society Directive are essentially left to the discretion of the Member States (see question 2(4)).

The Information Society Directive provides legal protection in respect of technological measures that effectively restrict acts not authorized by the rightholders of any copyright, rights related to copyright<sup>5</sup> or the sui generis

---

grounds. However, the Information Society Directive makes no mention of remuneration requirement and the core difference between the Conditional Access Directive and the Information Society Directive is that the former protects access to a service while the latter protects the content itself. We thus considered that a detailed analysis was not warranted in this report, which focuses on technological measures to protect content.

<sup>3</sup> One of the main goals of the Computer Programs Directive was to clarify the legal protection of computer programs and harmonise it under copyright law. The first Proposal of the European Commission was introduced on 12 April 1989.

<sup>4</sup> The Database Directive was adopted in order to harmonise the legal protection of databases offered by the legislation of the Member States which was until then protected differently (if at all) in the various countries of the European Community, under copyright laws or a form of sui generis database rights. The first Proposal for the Database Directive was introduced on 23 June 1992 and a Common Position was adopted on 10 July 1995.

<sup>5</sup> Related rights, also sometimes called “neighbouring rights”, include the rights of performers, phonogram and film producers and broadcasting organizations.

right in databases<sup>6</sup>. It does not however apply to computer programs, which are protected pursuant to the Computer Programs Directive. According to Article 7(1)(c) of the Computer Programs Directive, Member States are required to provide appropriate remedies against persons putting into circulation, or possessing for commercial purposes, “any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.” While the Computer Programs Directive is limited to prohibiting the business of trafficking in illicit devices, the Information Society Directive prohibits both the business of trafficking in illicit devices or circumventing services, as well as the act of circumvention of technological measures (see question 2(2)(b) and (c)). As a result, while this distinction is not made by the WCT, EU law comprises two different legal regimes applicable to technological measures: one applicable to computer programs, on the one hand, and one applicable to copyrighted works of authorship other than computer programs, rights related to copyright and the sui generis right in databases, on the other hand.

In order to come into effect at the national level, the Computer Programs Directive and the Information Society Directive had to be transposed by the various Member States of the European Union, each of them having to enact its own implementing laws or decrees. Even though implementation of the Information Society Directive was supposed to be completed by all the Member States by 22 December 2002, most countries (with the exception of Greece and Denmark) failed to meet that deadline, some of them such as France and Spain taking more than five years after the Information Society Directive was adopted.

---

<sup>6</sup> According to the Database Directive, a person (national or domiciliary of a Member State, or a corporation formed according to the laws of a Member State and has its registered office or principal place of business within the European Union) having made substantial investment in the creation of a database (i.e., “a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means”) enjoys certain exclusive rights in such database, regardless of whether it is also protected under copyright law, for fifteen years from the end of the year that the database was made available to the public, or from the end of the year of completion for private databases. Any substantial change that could be considered to be a substantial new investment will lead to a new term of database rights.



To our knowledge, even though other FTAs and EPAs involving France, the UK, Germany or the European Union may contain certain provisions relating to the protection of intellectual property, those that are currently in force do not specifically address the issue of technological measures to protect contents.

However, an EPA between the EU and the Republic of Korea, which has been initialled in Brussels on October 15, 2009, includes certain provisions on technological measures to protect contents (see [Annex 1](#)). This EPA has not yet been ratified. The provisions of the EPA concerning technological measures are, for the most part, identical to Articles 6 and 7 of the Information Society Directive, except for the following:

- in the pending EPA, the protection afforded to technological measures and right management information does not seek to protect the sui generis right in databases;
- regarding the protection of technological measures, there is no requirement that rightholders take “voluntary measures” to ensure that certain users have the means of benefiting from exceptions on copyright and related rights (see question 2(3)). The relevant provision of the pending EPA sets out only that each Party may provide for exceptions and limitations to effective technological measures in accordance with its legislation and the WCT and the WPPT.

---

## **2. Laws of the Research Subject Country Concerning Technological Measures to Protect Contents**

### (1) Laws concerning technological measures to protect contents

Whether there are any provisions of laws, rules, orders or the like that concern technological measures to protect contents in the research subject country. If so, the specific substance of the provisions of such laws, rules, orders or the like. If the originals thereof are not written in English, they should be translated into English.

The following sets out the substance of the relevant provisions of the European Directives (a) as well as of the national laws of France (b), England (c) and Germany (d) that were generally adopted to implement the European Directives.

#### (a) European Directives

##### *(i) Information Society Directive*

Articles 6 and 7 of the Information Society Directive provide that:

“Article 6 - Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,

any effective technological measures.

3. For the purposes of this Directive, the expression “technological measures” means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis [database] right (...). Technological measures shall be deemed “effective” where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

4. (...) <sup>7</sup>”

“Article 7 - Obligations concerning rights-management information

1. Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:

(a) the removal or alteration of any electronic rights-management information;

(b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under [the sui generis database right] (...) from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis [database] right (...).

2. For the purposes of this Directive, the expression “rights-management information” means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or

---

<sup>7</sup> Please see question 2(3) under which paragraph 4 is reproduced in full.

covered by the sui generis [database] right (...), the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject matter referred to in this Directive or covered by the sui generis [database] right (...).”

*(ii) Computer Programs Directive*

Article 7 (Special measures of protection) of the Computer Programs Directive provides that: “Member States shall provide, in accordance with their national legislation, appropriate remedies against a person committing any of the following acts: (...) (c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.”

(b) French law

French laws concerning technological measures result primarily from the implementation of the two European Directives. The Computer Program Directive was implemented in May 1994 by law no.94-361 and the Information Society Directive was implemented in August 2006 by law no.2006-961. Both those laws have been codified in the French Intellectual Property Code (the “IPC”).

Rules concerning technological measures applied to works protected by copyright and related rights (other than computer programs) are mainly provided under Articles L. 331-5 to L. 331-11 of the IPC. Provisions concerning rights management information are set forth in Article L. 331-11 of the IPC. Rules concerning technological measures applied to protected databases are set out in Article L. 342-3 of the IPC. Those Articles implement in large part the relevant provisions of the Information Society Directive.

The law and decree implementing the Computer Programs Directive did not fully transpose the provisions Article 7(1)(c). Instead, Articles L. 122-6-2 and R. 335-2 of the IPC essentially created an obligation for those distributing means of circumvention to notify users that an unlawful use of such means could be liable to sanctions applicable for cases of infringement of intellectual property rights.

The provisions of the IPC pertaining to the protection of technological measures are set forth in Annex 2.

(c) UK law

The Copyright, Designs and Patents Act 1988, as amended (the “CDPA”), is the primary source of national legislation in the UK relating to digital rights management and is designed to implement the requirements of international

and European legislation in that regard.<sup>8</sup> The most relevant provisions of the CDPA are contained in Sections 296 to 296ZG CDPA and may be considered to fall into three categories:<sup>9</sup>

- (I) Section 296 relates to the circumvention of technical devices applied to copyright computer programs only (this section was in the original 1988 legislation but has been updated twice, initially by statutory instrument in 1992 to implement Article 7(1)(c) of the Computer Programs Directive and latterly in 2003 by the CRRR 2003);
- (II) Sections 296ZA-ZF relate to the circumvention of effective technological measures applied to copyright works other than computer programs (implementing Article 6 of the Information Society Directive); and
- (III) Section 296ZG relates to the removal of rights management information from works and the subsequent circulation of works or copies of works from which rights management information has been removed (implementing Article 7 of the Information Society Directive).<sup>10</sup>

The provisions of UK law pertaining to the protection of technological measures are set forth in Annex 3.

(d) German law

Article 95a to 95d of the German Copyright Act, as amended in 2003, contain specific provisions for the protection of content using technological measures.

Article 95a of the German Copyright Act provides, as a general rule, that the circumvention of any technological measure for content protection is prohibited. The prohibition includes production, import, distribution, sale, lease and marketing of products or services for the circumvention of such technological measures. Even though § 69a Sect. 5 of the German Copyright Act expressly states that Articles 95a et seq. do not apply to computer programs, Article 69f of the German Copyright Act contains very

---

<sup>8</sup> The provisions of Section 296 CDPA were amended in 2003 by the Copyright and Related Rights Regulations (“CRRR 2003”) SI 2003/2498, which also created Sections 296ZA-ZG CDPA to implement the Information Society Directive.

<sup>9</sup> Sections 297-299 relate to the unauthorized reception of transmissions and unauthorized decoders used in such reception (implementing the Conditional Access Directive). As discussed at the European level (see footnote 2 above), these Sections fall outside the remit of this report.

<sup>10</sup> Note that, unlike Section 296, Sections 296ZA-G also apply, *mutatis mutandis*, where such technological measures have been applied to the subject-matter of rights in performances, the rights of broadcasting organisations, publication rights and the *sui generis* database rights.

similar provisions prohibiting the circumvention of technological measures to protect computer programs.<sup>11</sup>

Article 95b of the German Copyright Act is an exception to Article 95a of the German Copyright Act and implements Article 6(4) of the Information Society Directive. It obligates rightholders to provide necessary means and information of the circumvention of technological protection measures if that is necessary for the use in due course by certain public and private institutions.

Article 95c deals with the protection of technological protection measures on rights-management information. It provides, as a general rule, that rights-management information have to be protected and should not be removed or changed without permission of the rightholder.

In addition to the European Directive requirements, Article 95d provides, out of concern for consumer protection, that rightholders must sufficiently and clearly label products to which technological protection measures have been applied.

The provisions of German law pertaining to the protection of technological measures are set forth in Annex 4.

---

(2) Substance of restrictions provided for in such laws

- (a) What are the technologies restricted by the laws? (Definitions and specific examples or the like of the restricted technologies should be described.)

In order to encompass the full spectrum of the rapidly evolving circumvention techniques, the Information Society Directive is generally phrased in technology-neutral terms in that it does not specifically define or provide examples of restricted circumventing technologies. As a result, under Article 6(2) of the Information Society Directive, any “devices, products or components or the provision of services” may be restricted if they fall within the scope of the prohibition provided therein. Likewise, Article 7(1) of the Computer Programs Directive targets all “means” which “sole intended purpose” is to facilitate the unauthorized removal or circumvention of technological measures.

---

<sup>11</sup> Art. 69f Sect. 2 is *lex specialis* to and therefore overrides Art. 95a – 95d (Grützmacher in: Wandtke/Bullinger, *UrhR*, § 69a, Rn. 81). Pursuant to Art. 69f Sect. 2 of the German Copyright Act, the rightholder may require the destruction of any means which is solely intended to facilitate the unauthorized removal or circumvention of a technical device protecting a computer program. In addition, the rightholder may claim injunctive relief and damages pursuant to Article 97 of the German Copyright Act. Injunctive relief and damages may also be claimed under general tort law (Articles 823 and 826 of the German Civil Code). Civil remedies for the circumvention or removal of any technical device protecting computer programs are hence very similar to the civil remedies provided under Articles 95a to 95d of the German Copyright Act.

The broad “catch all” approach adopted by the relevant European Directives is reflected in French, English and German law, which purpose is generally not to restrict circumventing technologies but to restrict the acts involved in circumvention, however achieved, even encompassing circumvention technologies that are not yet existing.

---

(b) What are the products and programs or the like that are restricted by the laws?

(i) European Directives

1. *Information Society Directive*

As a complement to Article 6(1) of the Information Society Directive, which provides for protection against acts of circumvention of technological measures *per se*, Article 6(2) prohibits the supply of certain circumvention devices, products or components. However, not every device, product or component enabling or facilitating the circumvention of technological measures is prohibited under Article 6(2). First, only those that would enable the circumvention of “*effective* technological measures”<sup>12</sup> are concerned by the prohibition. Second, devices, products or components are prohibited only insofar as they:

“(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.”

---

<sup>12</sup> According to Article 6(3) of the Information Society Directive, “technological measures shall be deemed “effective” where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.” Essentially, to be considered effective, technological measures must meet their protection objective. Presumably, technological measures that do not reliably restrict unauthorized acts should thus be considered ineffective and thus not protected. However, the European Court of Justice did not yet have the opportunity to shed light on this issue. Furthermore, two types of technological measures are envisaged in Article 6(3): those which control access to a work (e.g., by way of encryption techniques) and copy control mechanisms. In spite of this distinction, both types of technological measures follow the same legal regime, except that in certain circumstances, rightholders will have an obligation to facilitate the circumvention of copy control mechanisms but not access control mechanisms pursuant to Article 6(4) of the Information Society Directive (see question 2(3)(a)).

Recital 48<sup>13</sup> of the Information Society Directive reaffirms that the legal protection afforded to technological measures is not intended to prevent “the normal operation of electronic equipment and its technological development” and “implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection.” According to the Explanatory Memorandum to the 1997 Proposal for the Information Society Directive, this solution would “ensure that general-purpose electronic equipment and services are not outlawed merely because they may also be used in breaking copy protection or similar measures.”<sup>14</sup>

However, paragraphs (a) to (c) of the provision make no distinction between circumvention devices that facilitate infringement of copyrights, related rights or sui generis rights in databases, and those that do not. In addition, paragraph (b) does not require a “circumvention purpose” on the part of the manufacturer or distributor of the devices. As noted in the Study on the Implementation of the Information Society Directive, “the provision casts a cloud on technology with ‘dual-purpose’ capabilities, which might inhibit technological innovation<sup>15</sup>.”

## *2. Computer Programs Directive*

Under Article 7(1) of the Computer Programs Directive, only “means” (which presumably includes any type of equipment or computer program) of which the sole intended purpose is to facilitate the circumvention of technological measures protecting computer programs have to be prohibited. This criterion is harder to fulfil than the criteria for distinguishing illegal circumvention devices from lawful multi-purpose equipment used in Article 6(2) of the Information Society Directive.

## *3. Technological measures applied to complex works*

As a result of the vagueness of the “computer programs” concept (which is not defined in the Computer Programs Directive), it may sometimes be difficult to determine in which category certain works should fall, e.g., content stored as digital files. In addition, certain “complex” works composed of both a computer program and another protected element that is not a computer program (e.g., videogames) include technological measures

---

<sup>13</sup> Recitals are intended to state the reasons on which EU legal acts are based, a requirement provided for by Article 296 of the Treaty on the Functioning of the European Union. Recitals are necessary for the European Court of Justice to exercise its supervision on the legal basis of the Directive. They do not have the independent legal value of a Directive provision, but often give courts a ground to expand the scope of a provision that leaves room to interpretation.

<sup>14</sup> European Commission, Explanatory Memorandum to the Proposal for a European Parliament And Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, 10 December 1997, COM(97) 628 final, p. 41.

<sup>15</sup> Institute for Information Law, University of Amsterdam, Study on the Implementation and Effect in Member States’ Laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the Information Society, February 2007, p. 80.

protecting both the underlying software code and other copyrighted elements (images, etc.), and will thus require the application of the two legal regimes. This may result in contradictory findings since the applicable rules will differ (e.g., the finding that a given circumvention technique should be prohibited in respect of a technological measure used to protect non-software items but authorized when it is used to access or copy computer programs).

(ii) French law

1. *Works other than computer programs*

Articles L. 335-3-1-II and R. 335-3 of the IPC prohibit the supply of “means” (which include devices and products) that are “designed or specially adapted for the purpose of undermining an effective technological measure”. This provision echoes Article 6.2(c) of the Information Society Directive restricting dealings in products or devices that are “primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention”. As a result, general-purpose devices are immune from the prohibition because they are, by definition, not “designed or specially adapted” for the purpose of circumventing technological measures. It should also be noted that there is no provision in French law implementing the case provided for in Articles 6.2(a) and 6.2(b) of the Information Society Directive, which respectively prohibit dealings in products or devices that “are promoted, advertised or marketed for the purpose of circumvention of” any effective technological measures,<sup>16</sup> and have a “limited commercially significant purpose or use other than to circumvent” any effective technological measures.

2. *Computer programs*

Article 7(1)(c) of the Computer Program Directive, which refers to “means the sole intended purpose of which is to facilitate the circumvention,” was not fully implemented into French law. Rather, Article L. 122-6-2 of the IPC does not distinguish between “means” according to their “intended purpose”. As a result, general-purpose devices could, in theory, be considered as means capable of circumventing technical devices protecting computer programs.

3. *Complex works*

As explained in paragraph (i) above, in the case of complex works, such as videogames, each copyrighted element of the work requires the application of the corresponding rules regarding technological measures. When each element is protected by its own distinct technological measure, technical devices protecting the computer program element will be governed by one set of rules (i.e., stemming from the incomplete implementation of the Computer

---

<sup>16</sup> It appears that the French legislator chose not to penalize dealings in products and devices simply because they are promoted or advertised as circumventing (and could potentially also have non-negligible uses other than circumvention) but, rather, opted to prohibit the act of advertising products and devices that fall in the scope of the prohibition established by Articles L. 335-3-1-II and R. 335-3 of the IPC, i.e., those that are “designed or specially adapted for the purpose of undermining an effective technological measure”. See question 2(2)(c)(ii).



Programs into French law) while the technological measures protecting the copyrighted elements other than the computer program will follow the other set of rules (stemming from the implementation of the Information Society Directive into French law).<sup>17</sup> However, if only one technological measure is used to protect both the computer program and non-software elements of the complex work, no solution is provided for by the law: courts could decide to apply the regime stemming from either the Computer Programs Directive or the Information Society Directive, or even both cumulatively. This gives rise to legal uncertainty and we are not aware of any case law addressing this issue.

(iii) UK law

The CDPA has largely reproduced *verbatim* the provisions of the relevant European Directives. Please refer to the answer in paragraph (i) above for further information.

In relation to copyrighted works other than computer programs, the CDPA restricts the supply of certain circumvention devices, products or components. Section 296ZA CDPA implements Article 6(1) of the Information Society Directive and merely prohibits acts of circumvention *per se*. Section 296ZD CDPA implements Article 6(2) of the Information Society Directive. Firstly, Section 296ZD is only concerned with the circumvention of “effective technological measures” (as defined in Section 296ZF).<sup>18</sup> Secondly, “devices, products or components” are restricted only insofar as they fulfil the qualification criteria listed in Article 6(2) of the Information Society Directive.

Section 296ZB CDPA creates a criminal offence to further bolster the UK’s implementation of Article 6(2) of the Information Society Directive.<sup>19</sup> Firstly,

---

<sup>17</sup> Thierry Maillard, “Mesures techniques de protection, logiciels et acquis communautaire : Interfaces et interférences des directives 91/250/CEE et 2001/29/CE”, RLDI 2005/5, no.154.

<sup>18</sup> Section 296ZF(1) mirrors the Information Society Directive and defines “technological measures” to mean “any technology, device or component which is designed, in the normal course of its operation, to protect a copyright work other than a computer program.” Again, this broad drafting was clearly intended to keep track of developments in the “technology” involved in technological measures; it appears likely that all technological measures applied to copyright works other than computer programs will be caught by this definition. It is therefore not necessary that the protection of the work is the sole or primary purpose of the relevant technology; all that is required is that the technology must be designed to protect that work in “the normal course of its operation.” Pursuant to Section 296ZF(2), measures are only “effective” if they actually permit the “use of the work” to be controlled by the copyright holder through an access control or protection process or a copy control mechanism. Such “use” only means the acts restricted by copyright for the purposes of this section; the phrase (and hence the scope of “effective”) will not extend to uses of the work that are outside the scope of the acts restricted by copyright. As a result, technological measures under the Sections of the CDPA implementing the Information Society Directive must be effective in actually controlling at least one or more acts that would be an infringement of copyright.

<sup>19</sup> The WIPO has stated that it believes criminal offences “may also be needed since the manufacture, importation and distribution of illicit circumvention devices is a kind of piratical activity” (WIPO discussion of digital rights management (2007), available on [http://www.wipo.ch/edocs/mdocs/copyright/en/wipo\\_ip\\_cm\\_07/wipo\\_ip\\_cm\\_07\\_www\\_825](http://www.wipo.ch/edocs/mdocs/copyright/en/wipo_ip_cm_07/wipo_ip_cm_07_www_825))

Section 296ZB is again concerned only with the circumvention of “effective technological measures.” Secondly, Section 296ZB is concerned with a narrower range of devices, products or components than Section 296ZD. The criminal sanctions of the CDPA only prohibit devices, products or components that are “primarily designed, produced or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures.”

In relation to copyrighted computer programs, Section 296(1) CDPA restricts “any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of the technical device” applied to a computer program. Section 296(6) defines a “technical device” as “any device intended to prevent or restrict acts that are not authorised by the copyright owner of that computer program and are restricted by copyright.” This definition of “technical device” is narrower than that contained in the Computer Programs Directive, which simply defines a “technical device” as “any technical device which may have been applied to protect a computer program.”

In relation to rights management information,<sup>20</sup> Section 296ZG CDPA is concerned with the removal or alteration of such information where such information has been applied to a copyright work. As a result, any device or technology that facilitates such action would be caught, irrespective of its nature.

*(iv) German law*

Article 95a Sec. 3 of the German Copyright Act faithfully implements Article 6(2) of the Information Society Directive and protects rightholders against dealings in products or parts of products, and the provision of services, which are promoted advertised or marketed for the purpose of circumvention, or which have no significant commercial purpose or use other than to circumvent, or which have been predominantly designed to, manufactured, adapted or offered to facilitate the circumvention of effective technological measures.

---

80.doc, accessed on 18 October 2009. Accordingly, Section 296ZB CDPA creates a criminal offence in relation to the circumvention of effective technological measures applied to protect a copyright work other than a computer program.

<sup>20</sup> This term is defined by Section 296ZG(7)(b). Under UK law, “Rights management information” is information: (i) that is provided by the copyright owner or the holder of any right under copyright (this part of the definition represents an attempt to incorporate the term “rightholders” from the Information Society Directive but it is unclear in its scope; presumably it includes the copyright owner and his exclusive licensee but it may also include non-exclusive licensees as well); (ii) that identifies the work, the copyright owner or the holder of any intellectual property rights, or information about the terms and conditions of use of the work; and (iii) the definition includes any numbers or codes that represent such information.

- (c) What are the actions that are restricted by the laws? (All restricted actions should be described.) Specifically, explicit descriptions should be given as to whether the following are restricted actions:
- (i) manufacture of circumvention devices or the like (including programs);
  - (ii) provision of circumvention devices or the like (including programs);
  - (iii) export and import of circumvention devices or the like (including programs);
  - (iv) possession of circumvention devices or the like (including programs);
  - (v) provision of circumvention services;
  - (vi) circumvention (reproduction by circumvention); and
  - (vii) dissemination of advertisements/information regarding circumvention devices or the like (including programs) or circumvention services or circumvention method.

(i) European Directives

1. *Information Society Directive*

Article 6(1) of the Information Society Directive requires that EU Member States prohibit acts of circumvention of effective technological measures by any person who knows or has reasonable grounds to know that he is committing an act of circumvention.

In addition, Article 6(2) of the Information Society Directive requires that EU Member States prohibit the provision of circumventing services as well as acts facilitating or preparatory to actual circumvention, which comprise the following actions in relation to circumventing devices, products or components (provided that they fall in the categories described under question 2(b)(i)):

- manufacture,
- import,
- distribution,
- sale,
- rental,
- advertisement<sup>21</sup> for sale or rental, and
- possession for commercial purposes.

“Export” is not included in the prohibition and does not fall under “distribution”. However, EU Member States are required to prohibit the import of circumventing devices pursuant to Article 6(2) of the Information Society Directive (provided that they fall in the categories described under question 2(b)(i)).

2. *Computer Programs Directive*

---

<sup>21</sup> Although we did not find any commentary on the Information Society Directive on this point, we believe that the terms of Article 6(2) would imply that a commercial purpose is necessary. Therefore our understanding is that “advertisement for sale and rental” do not include the mere publication and disclosure for non-commercial purposes.

Article 7(1) of the Computer Programs Directive does not prohibit the act of circumventing technological measures protecting computer programs. It only requires Member States to prohibit the trafficking<sup>22</sup> in circumvention devices for such technological measures.

(ii) *French law*

1. *Works other than computer programs*

The implementation into French law of the prohibition of acts of circumvention provided under Article 6(1) of the Information Society Directive was split between two Articles of the IPC: on the one hand, Article L. 335-3-1-I of the IPC, which prohibits the act of circumvention without a circumventing device, and, on the other hand, Article R. 335-3 of the IPC, which prohibits the possession for personal use or use of a circumvention device, as well as resorting to a service designed or specially adapted for the purpose of circumventing a technological measure.<sup>23</sup>

In addition, Article L. 335-3-1-I of the IPC prohibits the act of knowingly undermining an effective technological measure for a purpose other than research. The French Constitutional Court recently handed down a decision restricting the scope of the exception to research in cryptography.<sup>24</sup>

Article 6(2) of the Information Society Directive has been implemented by Article L. 335-3-1-II of the IPC. In substance, this provision prohibits the

---

<sup>22</sup> This term is generally used in this context to cover “any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program” (Article 7(1)(c) of the Computer Programs Directive).

<sup>23</sup> There was no rationale for this distinction and the split between the two Articles. The French legislator unwillingly omitted a portion of the new legal regime stemming from the Information Society Directive when the latter was implemented in France. This omission was later corrected in Article R. 335-3 of the IPC.

<sup>24</sup> *Conseil constitutionnel*, 27 July 2006, decision no.2006-540 DC. In this decision, the Constitutional Court was asked to examine the compliance of law no. 2006-961 implementing the Information Society Directive with the French Constitution. The Court held that because the term “interoperability” was not clearly defined, it would be unconstitutional to impose criminal sentences based on legal provisions using that expression. That term was therefore deleted from sections of the IPC dealing with criminal sentences. This deletion did not however affect other Articles of the IPC using the term interoperability, particularly those relating to the interoperability exception. In that decision the Constitutional Court also clarified the meaning of the term “research” in the research exception to the protection of technological measures. According to the Court, “research” should be construed restrictively as “research in cryptography”, in accordance with the preparatory works of the French Parliament that led to the adoption of law no. 2006-961 implementing the Information Society Directive. As a result of the decision of the Constitutional Court, the draft of Article R. 335-3 of the IPC was modified and the version that was eventually enacted by the French legislator provides as follows: “These provisions do not apply to acts that cause damages to rightholders and that are performed for the purposes of computer security or scientific research in cryptography.” English law did not suffer from the same lack of precision, as Section 296ZA CDPA expressly refers to “research in cryptography”.

fact of knowingly providing or proposing to a third party, directly or indirectly, means designed or specially adapted for the purpose of circumventing an effective technological measure by carrying out one of the following practices:

- 1° manufacturing or importing, for purposes other than research, a technological application, a device or a component;
- 2° possessing for sale, lending or renting, offering to the same ends or offering to the public in any manner a technological application, device or component;
- 3° offering a service to this end;
- 4° inducing the use of, or commissioning, conceiving, organizing, reproducing, distributing or disseminating an advertisement for, one of the practices mentioned in paragraphs 1° to 3° above.

## *2. Computer programs*

As previously explained, Article 7(1)(c) of the Computer Programs Directive was only partially implemented into French law. Article L. 122-6-2 of the IPC only prohibits the advertisement or publication of user's handbook concerning circumvention devices without the express mention that the unlawful use of such devices is liable to penalties applicable to copyright infringement.

Dealings in circumvention devices is not prohibited under Article L. 122-6-2 of the IPC. However, under French case law, the distribution of circumvention devices that enable the infringement of copyright also amounts to copyright infringement. Infringement can relate to copyright in the computer program which the technical device seeks to protect or to copyright in the technical device, if the technical device itself consists of a copyrighted computer program. Therefore, if a computer program is protected by a technical device which is also a copyrighted computer program, commercial dealings in devices enabling the circumvention of the technical device could be prohibited if the circumvention would result in performing one of the actions prohibited under the copyright infringement statute<sup>25</sup> in relation to either the technical device or the underlying computer program.

By underlining the fact that circumvention devices can be used unlawfully, Article L. 122-6-2 of the IPC also suggests that there can be lawful uses of such devices. In the case of a technical device consisting of a computer

---

<sup>25</sup> According to Article L. 122-6 of the IPC, infringement of copyright relating to computer programs occurs when a person other than the rightholder carries out, without being authorized to do so, one of the following actions:

- “1° the permanent or temporary reproduction of a computer program, partially or as a whole by any means and in any form. Insofar as loading, displaying, running, transmission or storage of this computer program require such reproduction, these acts shall be performed only with the authorization of the author;
- 2° the translation, adaptation, arrangement or any other alteration of a computer program and the reproduction of the computer program thereof;
- 3° the offer for sale or for free, including rental, of the copy or copies of the computer program by any process (...)”

program, it has been recognised that circumvention that does not result in copying or executing the technical device was not prohibited per se.<sup>26</sup>

(iii) *UK law*

The relevant UK legislation has largely reproduced *verbatim* the provisions of the relevant European Directives.

1. *Works other than computer programs*

Sections 296ZA and 296ZD CDPA implement Articles 6(1) and 6(2) of the Information Society Directive respectively. Section 296ZA(1) CDPA applies where (a) effective technological measures have been applied to a copyright work other than a computer program and (b) a person does anything which circumvents those measures. Section 296ZD(1)(b) CDPA restricts a person who “manufactures, imports, distributes, sells or lets for hire, offers or exposes for sale or hire, advertises for sale or hire, or has in his possession for commercial purposes any device, product or component, or provides services which” fulfil the qualification criteria of Article 6(2) of the Information Society Directive.<sup>27</sup>

Section 296ZB CDPA creates a criminal offence; it mirrors Article 6(2) of the Information Society Directive but narrows the scope of that Article by introducing certain modifications (*italicized* below). Pursuant to Section 296ZB(1), a person commits an offence if he:

- “(a) manufactures *for sale or hire*, or
- (b) imports *otherwise than for his private and domestic use*, or
- (c) *in the course of a business*—
  - (i) sells or lets for hire, or
  - (ii) offers or exposes for sale or hire, or
  - (iii) advertises for sale or hire, or
  - (iv) possesses, or
  - (v) distributes, or
- (d) *distributes otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner*, any device, product or component which is *primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures.*”

---

<sup>26</sup> Paris Court of Appeals, 13e ch., 2 March 1989.

<sup>27</sup> The breadth of drafting here is significant. Whilst Section 296ZA renders the act of circumvention tortious, Section 296ZD is concerned with restricting the commercial trade of, and the commercial provision of services in relation to, circumvention techniques. The scope of the restricted actions includes all those actions that this research report asked us to consider. It is notable that even some non-commercial actions such as distribution or importation will incur liability. Whilst the act of exporting devices, products or components is not specifically restricted by the CDPA and only infringing activities within the UK will be subject to UK jurisdiction, it is likely that an exporter operating within the UK would fall within the restrictions provided under Section 296ZB CDPA on other grounds (as exporters generally also manufacture, possess or distribute infringing devices in addition to exporting them). Furthermore, the jurisdiction into which the goods were subsequently imported may restrict such import (as in the case of EU Member States).

Pursuant to Section 296ZB(2), a person also commits an offence if he “provides, promotes, advertises or markets—  
(a) *in the course of a business, or*  
(b) *otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner,*  
a service the purpose of which is to enable or facilitate the circumvention of effective technological measures.”<sup>28</sup>

## 2. *Computer programs*

Section 296 CDPA restricts two categories of action:

(a) manufacturing for sale or for hire, importing, distributing, selling or letting for hire, offering or exposing to sale or hire, advertising for sale or hire or possessing for commercial purposes any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of the technical device; or

(b) publishing information intended to enable or assist persons to remove or circumvent the technical device.<sup>29</sup>

There is therefore no liability for the actual act of circumventing technological measures in relation to computer programs *per se*.

## 3. *Rights management information*

Subject to the knowledge of the person infringing copyright, Section 296ZG CDPA restricts the removal and tampering with rights management information and the distribution, importation or communication to the public of copies of a copyrighted work where such rights management information have been removed or tampered with.<sup>30</sup>

---

<sup>28</sup> In the UK, therefore, actions relating to devices, products or components with only a limited commercial purpose or which are not primarily designed with the circumvention of technological measures in mind will therefore only attract civil liability. Similarly, the provision of services with a limited commercial purpose will only attract civil liability. Criminal liability has been reserved for clear instances where a dedicated circumvention product or service has been marketed and distributed pursuant to a business, or distributed or provided to a commercially significant extent otherwise than in the course of a business. The provisions of the UK law therefore implement the UK’s obligations under not only the Information Society Directive but also the WCT and the WPPT, in restricting private actions that are of such extent as to prejudice a rightholder’s interest. In considering the requirements of the WCT and WPPT, the UK has therefore taken the policy decision that criminal penalties are required to provide an effective deterrent and to protect rightholders (cf. footnote 17 above).

<sup>29</sup> In construing the broad requirement of the relevant Directive to restrict “trafficking” in circumvention devices, the UK legislature took a policy decision to restrict the publication of information intended to enable or assist persons in removing or circumventing the device. The UK legislation therefore may go beyond the scope of restrictions required for implementation of the Directive.

<sup>30</sup> Section 296ZG CDPA restricts two types of action. First, pursuant to Section 296ZG(1), civil rights and remedies arise against a person who, knowingly and without authority, removes or alters electronic rights management information which – (i) is associated with a copy of a copyright work, or (ii) appears in connection with the communication to the public of a copyright work, and where he knows, or has reason to believe, that by so doing he is

(iv) German law

1. *Works other than computer programs*

Article 95a Sec 3 of the German Copyright Act explicitly prohibits the manufacture, import, distribution (which includes both physical and intangible dissemination), sale, rental, advertisement for sale or rental and possession for commercial purposes as well as the provision of services. The use of circumvention technologies is prohibited by Article 95a Sec. 1 of the German Copyright Act.

2. *Computer programs*

Articles 95a to 95d of the German Copyright Act do not apply to computer programs. Article 69f Sect. 2 of the German Copyright Act provides that rightholders may obtain the destruction of any means the sole intended purpose of which is to facilitate the removal or circumvention of a technical device protecting a computer program. Additionally, rightholders may be granted injunctive relief under Article 97 of the German Copyright Act.<sup>31</sup>

- 
- (3) Are any exclusions of application, exceptions, restrictive provisions or the like provided for in the provisions concerning technological measures to protect contents? If they are provided for, what is the specific substance thereof? Please explain the exclusions in relation to the rights restriction provisions of copyright.

**Presentation of the scheme**

Article 6(4) of the Information Society Directive attempts to reconcile the protection of technological measures with the exercise of limitations on copyright and related rights provided for in Article 5 of the Information Society Directive.<sup>32</sup> It provides that rightholders should take “voluntary

---

inducing, enabling, facilitating or concealing an infringement of the copyright. Second, pursuant to Section 296ZG(2), such rights and remedies also arise against a person who, knowingly and without authority, distributes, imports for distribution or communicates to the public copies of a copyright work from which electronic rights management information – (a) associated with the copies, or (b) appearing in connection with the communication to the public of the work, has been removed or altered without authority and where he knows, or has reason to believe, that by so doing he is inducing, enabling, facilitating or concealing an infringement of copyright. Liability under Section 296ZG only arises in respect of acts occurring after 31 October 2003. Furthermore, no act done after 31 October 2003 pursuant to an agreement made before 22 December 2002 will incur liability under this Section.

<sup>31</sup> Grützmacher in: Wandtke/Bullinger, UrhR, 3. Aufl. 2009, § 69 f., Rn. 5.

<sup>32</sup> The full text of Article 6(4) reads as follows:

“4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate



measures,” including agreements between them and other parties concerned, to ensure that certain users have the means of benefiting from those exceptions on copyright and related rights referred to in Article 5 of the Information Society Directive that have been implemented in national law.

Since the Directive does not describe what types of voluntary measures are required, it is primarily up to the rightholders to decide how they want to fulfil this legal obligation.<sup>33</sup> In the absence of voluntary measures from rightholders, Member States must take “appropriate measures” for that purpose.

Article 6(4) of the Information Society Directive is phrased as an exception to Article 6(1) only so that the obligation to provide the means to exercise a limitation applies only to the circumventing act itself, and not to the supply of circumventing devices or services prohibited under article 6(2). In addition, Article 6(4) creates an obligation to provide the means to exercise a limitation on rightholders but does not give users any authority to perform

---

measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply *mutatis mutandis*.”

<sup>33</sup> Voluntary measures can take on many forms, including the supply of a non-protected version of the work, or of an encryption key, either directly to the end user or deposited with a third party. Another possible solution is to design the technological measures so that certain lawful uses are possible. Article 6(4) also encourages the negotiation of agreements between rights owners and parties concerned. According to the Study on the Implementation of the Information Society Directive (p. 107): “This voluntary path is actually being pursued in various Member States. For example, the Motion Pictures Association has entered into negotiations with the British Film Institute (BFI) regarding the right to make archival copies of films. In January 2005, the German National Library has reached an agreement with the German Federation of the Phonographic Industry and the German Booksellers and Publishers Association on the circumvention of technological protection measures (TPM) such as access and copy controls on CDs, CD-ROMs, and e-books.”

acts of circumvention themselves.<sup>34</sup> Furthermore, rightholders do not have an obligation to grant access to their work in order for a user to benefit from a limitation contained in the list of Article 6(4) first paragraph, but rather, to facilitate the exercise of a limitation once a user has been granted lawful access to a work. As a result, this provision only obligates rightholders to facilitate the circumvention of copy control mechanisms (i.e., technological measures design to restrict acts within the rightholder's prerogatives such as the act of reproduction or making the work available)<sup>35</sup>, not access control mechanisms.

In light of the discretion given to Member States by Article 6(4) of the Information Society Directive, this provision has been implemented in various ways at the national level. According to a recent comparative study<sup>36</sup>, eleven Member States, mostly Western European countries, “joined the EU legislation in wishing that stakeholders would take ‘voluntary measures’ (...) to grant access and use to beneficiaries of exceptions” while the others obligate rightholders to make available copyright works to beneficiaries of copyright exceptions (most often, however, without specifying how this has to be done), or do not provide for any remedy. Also, according to that study, “the provision of remedies in case rightholders refuse to comply spontaneously with the law is rather diverse” from Member State to Member State, and ranges from ignoring the issue altogether, to having the matters settled by mediation boards and arbitrators or leaving those cases to ordinary courts. The next section summarizes the solutions adopted in France (a), the UK (b) and Germany (c) in that regard.

#### **General limitations under the Information Society Directive: Article 6(4), first paragraph**

The limitations to copyright that Article 6(4), first paragraph, of the Information Society Directive seeks to protect are not all limitations appearing in the list of Article 5 of the Information Society Directive, but rather, only certain public policy exceptions included in Articles 5(2) and 5(3). These limitations are:

- acts of reproduction by means of reprographic equipment (Article 5(2)a));
- acts of reproduction by publicly accessible libraries, educational establishments or museums, or by archives (Article 5(2)c));

---

<sup>34</sup> According to one scholar: “Consequently, to benefit from exceptions, the beneficiary does not have to circumvent [technological measures], but each Member State must act as a guarantor of the exceptions. This solution has an advantage and a drawback. The advantage is that one does not have to be a hacker in order to enjoy copyright exceptions; the disadvantage is that Member States' intervention goes to the detriment of freedom of contract between the rightholder and the beneficiary and harmonization of EU exceptions.” (Alvise Maria Casellati, *The Evolution of Article 6.4 of the European Information Society Copyright Directive*, 24 Colum. – VLA J.L. & Arts 369, p. 6).

<sup>35</sup> For instance, the Serial Copy Management System (SCMS), which enables the making of copies from the original but not from another copy.

<sup>36</sup> Marcella Favale, *Technological Protection Measures and Copyright Exception in EU 27: Towards the Harmonization* DePaul College of Law, p. 14 et seq.

- ephemeral recordings of works made by broadcasting organizations (Article 5(2)d));
- reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons (Article 5(2)e));
- use for the sole purpose of illustration for teaching or scientific research (Article 5(3)a));
- uses for the benefit of people with a disability (Article 5(3)b)); and
- use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings (Article 5(3)e)).

Rightholders are therefore entitled to override the copyright limitations not mentioned above by using technological measures, including the mandatory limitation provided in Article 5(1) of the Information Society Directive on transient and incidental acts of reproduction (such as cookies, or cache files),<sup>37</sup> as well as the exceptions for quotation and news reporting, which are traditional testimonials of the freedom of information.<sup>38</sup> Moreover, since certain copyright limitations set forth above have not been implemented by all the Member States (e.g., the limitation on reproductions of broadcasts made by social institutions), this list may be even shorter in certain countries.<sup>39</sup>

#### **The private copying exception: Article 6(4), second paragraph**

The private copying exception is treated separately under the second paragraph of Article 6(4) of the Information Society Directive. Member States may, but are under no obligation to, take action in respect to the private copying exception, “unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned (...).” Moreover, rightholders may in any case use technological to control the number of reproductions. As regards the rationale for making this exception voluntary, it appears to be the result of the influence of European lobbying groups<sup>40</sup>. As some

---

<sup>37</sup> Of all the limitations and exceptions to copyright listed in Article 5 of the Information Society Directive, the possibility to carry out temporary acts of reproductions which are “transient or incidental [and] an integral and essential part of a technological process” set out in Article 5(1) is the only one that is compulsory and must be implemented in all the Member States; all the others are optional and can be implemented at the discretion of each Member State.

<sup>38</sup> According to the Study on the Implementation of the Information Society Directive (p. 110): “By omitting a number of other key limitations in this provision, the European legislator has failed to take account of the possible impact that the prohibition on the circumvention of technological measures applied to copyrighted works may have on activities such as criticism, comment, news reporting, parody, scholarship, or research.”

<sup>39</sup> According to a comparative study, while some countries like the UK impose on rightholders an obligation to comply with all the limitations listed in the first paragraph of Article 6(2), others selected only a few exceptions from that list, while the rest, especially Eastern European countries, did not envisage any compliance for the rightholders. Marcella Favale, p. 22.

<sup>40</sup> Marcella Favale, p.12.

commentators noted, “Article 6.4 is a highly unusual and unclear provision and very much the creature of political compromise.”<sup>41</sup>

Thus, France, UK and Germany had a choice to make with respect to the implementation of this provision. In France, if private regulation is unsuccessful, the beneficiary of the private use exception may obtain satisfaction by filing a claim with an administrative agency called the “Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet” (High authority for work broadcast and protection of the rights on the Internet or “HADOPI”). However, Article L. 331-7 paragraph 2 of the IPC, codifying settled case law on that topic, restricts the private copying exception, which may be effectively exercised only if it satisfies a three-step test aiming at ensuring that it does not undermine the normal use of the work or cause an unfair damage to the legitimate interests of the rightholder.

The UK and Germany adopted a different approach. In Germany, there are no provisions with regard to measures in respect of a beneficiary of the private use exception. Therefore, the circumvention of technological measures may not be justified by the private copying exception. In the UK, Section 296ZE CDPA offers a process for complaints to be made to the Secretary of State where technological measures restrict permitted acts. The permitted acts, as enumerated in Schedule 5A CDPA, include the Section 29 right to research and private study. The Secretary of State may make an order for relief of a beneficiary of, inter alia, the private study exemption where he is satisfied that no voluntary measures or agreements exist that have the effect of enabling a person using the work to carry out the permitted act. However, the private copying exception is not protected by the scope of Section 296ZE.

### **Carve-out of “on-demand” services**

Pursuant to the fourth paragraph of Article 6(4) of the Information Society Directive, technological measure limitations relating to both the public policy exceptions referred to in the first paragraph of Article 6(4) and the private copying exception treated under the second paragraph of that Article do not apply to “on-demand” services, i.e., works “made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.”

For some commentators, the “on-demand” services exception should apply only to online services for which the contracting parties have negotiated the terms of use. As noted in the Study on the Implementation of the Information Society Directive, “such an interpretation of the exception in the fourth paragraph of Article 6(4) of the Directive would be in line with the presumed intention of the European legislator, since it would preserve the respective parties’ freedom of contract while protecting the licensee from an unbridled use of standard form contracts. In light of the above, the reasons behind the legislator’s decision to relieve rightholders from the obligation to provide users with the means to exercise a limitation with respect to works that are made available pursuant to contractual terms of use are, for some

---

<sup>41</sup> Michael Hart, “The Copyright in the Information Society Directive: an Overview”, EIPR 2002, No2, p.63

commentators, just as obscure as the legislator's choice of limitations included in the first paragraph<sup>42</sup>."

### **Limitations on the protection of technological measures applied to computer programs**

The relationship between technological measures applied to computer programs and copyright exceptions is not addressed in the Computer Programs Directive but in the Information Society Directive, which was adopted about a decade later. Recital 50 of the Information Society Directive provides that the protection of technological measures that hinder the usage of computer programs should "neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the [exceptions] of Article 5(3) [which permits research as to the ideas and principles which underlie a computer program]<sup>43</sup> or Article 6 [which permits decompilation necessary to achieve the interoperability of an independently created computer program with other programs]<sup>44</sup> of [the Computer Programs Directive]."

---

<sup>42</sup> Study on the Implementation of the Information Society Directive, p. 112

<sup>43</sup> Article 5(3) of the Computer Programs Directive provides as follows: "The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do."

<sup>44</sup> Article 6 of the Computer Programs Directive provides as follows:

"1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of points (a) and (b) of Article 4(1) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

(a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to do so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and

(c) those acts are confined to the parts of the original program which are necessary to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with a normal exploitation of the computer program."

As a result, the distribution of circumvention devices that are necessary to perform acts of decompilation authorized under Article 6 of the Computer Programs Directive or research as to the principles underlying a computer program (reverse engineering) may not be restricted by the protection of technological measures.<sup>45</sup> Thus, it appears that, for example, devices or computer programs that enable to decrypt an encrypted software product may lawfully be produced and distributed if they fall within the above-described exceptions. One undecided issue is whether the distribution of a device capable of decrypting computer programs for any purpose, and therefore also for the purpose of studying the ideas underlying the program, should be prohibited.

(a) French law

(i) Scope of exceptions

1. Works other than computer programs

According to Article L.331-5 paragraph 6 of the IPC, technological measures cannot prevent the lawful use of the work within the limits of the rights provided for by the IPC and granted by the rightholders. The IPC provides for several exceptions limiting the application of technological measures.

Pursuant to Article L. 331-31 of the IPC, the following five exceptions to copyright are to be balanced with the interest of rightholders in implementing technological measures:

- the exception with respect to teaching and research;
- the exception in favour of handicapped persons;
- the exception with respect to the libraries, museums and archives;
- the exception necessary for the accomplishment of a parliamentary procedure of control, jurisdictional or administrative, provided for by the law, or started up for a public security purpose: this is a new exception, added by the law no.2009-1311 of 28 October 2009; and
- the private copying exception.

The exercise of those five exceptions limiting the application of technological measures are restricted by Article L. 331-7 paragraph 2 of the IPC in two ways. Firstly, this provision only obligates rightholders to facilitate the circumvention of copy control mechanisms, not access control mechanisms. Secondly, those exceptions may be effectively exercised only if they satisfy a three-step test aiming at ensuring that they do not undermine the normal use of the work or cause an unfair damage to the legitimate interests of the rightholder.

---

<sup>45</sup> It is generally admitted that recital 50 of the Information Society Directive creates an exception to the prohibition of circumvention of technological measures in the context of the legal protection of computer programs (Alvise Maria Casellati, *The Evolution of Article 6.4 of the European Information Society Copyright Directive*, 24 Colum. – VLA J.L. & Arts 369, p. 14). In the absence of any authority to the contrary, scholars do not seem to question the legal force of this exception on the ground that it stems from a recital and not an actual directive provision.

In addition, Article L. 331-5, paragraph 4 of the IPC provides a sixth exception with respect to relations between the rightholder and technical operators, pursuant to which technological measures should not be used to prevent interoperability. In accordance with the European Directives, professionals are encouraged to determine the conditions to exercise the interoperability exception by themselves, through the negotiation of agreement whereby the rightholders would accept to communicate information necessary to achieve interoperability (Article L. 331-32 of the IPC). In addition, under the so-called “decompilation exception” (Articles L. 331-5, paragraph 7 and L. 122-6-1 IV of the IPC) decompilation of a computer program may be carried out without the rightholder’s consent if it is necessary to achieve interoperability. French law also goes further than the European Union Directives by providing that any computer program publisher, manufacturer of technological system and any service operator may ask the HADOPI to guarantee interoperability (Article L. 331-32 of the IPC). However, a claim may be filed with the HADOPI in that regard by professionals only, so that the interoperability exception has a restricted scope of application that does not include consumers.

## 2. Computer programs

According to L. 122-6-1 IV of the IPC, the interoperability exception also applies to computer programs.

In addition, other exceptions limiting the application of technological measures apply only to computer programs, as they are necessary for the use of the computer programs by the person entitled to use it in accordance with its intended purpose. Those exceptions include (i) the right to correct errors (Article L. 122-6-1 I of the IPC), (ii) the right to make a back-up copy (Article L. 122-6-1 II of the IPC), (iii) the right to observe, study or test the functioning of the computer programs in order to determine the ideas and principles which underlie any elements of the computer programs (Article L. 122-6-1 III of the IPC).

French law therefore fully implemented the provisions of recital 50 of the Information Society Directive (see paragraph (i) above).

### (ii) Implementation of the exceptions

Like the Information Society Directive, French law encourages private regulation, and provides that the conciliation between the right to implement technological measures and exceptions to copyright and related rights should first be dealt with by the rightholders themselves. In this respect, article L. 331-7 of the IPC provides that the rightholders have to ensure that the implementation of technological measures does not deprive the beneficiaries of certain copyright and related right exceptions of their effective exercise (those exceptions are listed in articles L. 331-31 and L.331-5, paragraph 4, of the IPC and further examined under question 3(b) below). In principle, rightholders are to determine such voluntary measures together with interested parties, such as consumers’ associations.

If private regulation is unsuccessful and the negotiations between the rightholders and users do not lead to an agreement, the only way for a beneficiary of an exception to obtain satisfaction is by filing a claim with the

HADOPI. Indeed, the beneficiaries of copyright and related right exceptions are not granted a general right to circumvent technological measures in order to exert copyright exceptions but are only entitled to seek remedies from the HADOPI (as explained below). However, circumvention is allowed in two specific cases: Articles R. 335-3 and R. 335-4 of the IPC provide that a person is not criminally liable for acts that do not cause damages to rightholders and which are committed either (i) for computer security reasons, or (ii) for scientific research in cryptography. Therefore, in those two situations, the beneficiary of an exception may use devices or services in order to circumvent a technological measure that deprives him of the effective exercise of the exception.

In any other situation<sup>46</sup>, a claim must be filed with the HADOPI. The HADOPI is a new public independent authority created by law no.2009-669 of June 12, 2009 and which replaces the Autorité de Régulation des Mesures Techniques (Authority for the Regulation of Technological Measures or “ARMT”) that was, until then, competent for matters relating to technological measures. According to Article L. 331-13 of the IPC, the HADOPI’s role is to regulate and monitor the field of technological measures. Article L. 331-31 of the IPC specifies that the HADOPI has to ensure that the implementation of technological measures does not deprive the beneficiaries of the above-mentioned exceptions to copyright and related rights. The HADOPI is also in charge of determining the conditions of the exercise of those exceptions and, in particular, the minimum number of protected copies authorized within the framework of the private copying exception, based on the type of work or the protected subject, the various means of public communication and the possibilities offered by the available protection technologies.

Pursuant to Article L. 331-33 of the IPC, a claim may be filed with the HADOPI by any persons who are beneficiaries of those exceptions listed in Articles L. 331-31 and L. 331-5, paragraph 4, of the IPC, or any other approved legal entity representing such persons (e.g., consumer associations).

If the claim cannot be resolved by way of conciliation, the HADOPI has two months from the filing of the claim to render a decision. It may issue injunctions, subject to penalty if necessary, and impose financial sanctions in the event of non-compliance with its injunctions or with the conditions set forth in its decision (e.g., commitments that must be respected by users of the work to preserve the efficiency and the integrity of the technological measures concerned, as well as the terms of access and use of the protected content).<sup>47</sup>

---

<sup>46</sup> Except when technological measures protect works broadcasted on television, in which case the Conseil supérieur de l’audiovisuel (“CSA”) would be competent. Indeed, works broadcasted on television are subject to a special regime with respect to the application of technological measures, due to the private copying exception. According to Article L. 331-9 of the IPC, editors and distributors of television services cannot use technological measures that would deprive the public of the benefit of the private copying exception, including on a digital medium. The Conseil supérieur de l’audiovisuel (CSA) is competent to regulate technological measures matters in that regard, instead of the HADOPI.

<sup>47</sup> Financial sanctions are to be proportional and take into account the importance of the damage caused to the interested parties, the situation of the sanctioned person or entity and whether such entity committed similar acts several times. The financial sanctions



(b) UK law

Unlike other provisions of the CDPA relating to the general law on copyright, there is no provision which directly allows a user of a copyrighted work to circumvent technological measures to facilitate a permitted use (as defined by the CDPA). The liability created by the CDPA for the act of circumventing, or otherwise dealing in devices relating to the circumvention of, technological measures is therefore relatively strict. There is little protection for a user who circumvents technological measures applied to a copyright work to enable them to enjoy what would otherwise be a permitted use of that work.

Protection of Permitted Acts: Section 296ZE CDPA implements Article 6(4) of the Information Society Directive in the UK, establishing the protection of “permitted acts” in the provisions of the CDPA. A complainant, or representative of a class, who has “lawful access to the protected copyright work” may send a complaint notice to the Secretary of State who will investigate the matter further. If a “permitted” act is being prevented by an effective technological measure, the Secretary of State may require the owner of the copyright or his exclusive licensee to ensure that the person making the complaint can carry out the permitted act. Failure to comply with such direction from the Secretary of State is an actionable breach of a statutory duty.

Section 296ZE is limited in scope. It does not apply to technical devices protecting computer programs. Section 296ZE only protects permitted acts as defined by Part 1 of Schedule 5A to the CDPA – it does not protect the “fair dealing” exemptions et al. which were created elsewhere in the CDPA.<sup>48</sup> It should be noted that the “permitted use[s]” enumerated in Schedule 5A which, if prevented, may provide grounds for a complaint under Section 296ZE are narrower than the “permitted acts” normally enjoyed by the user of a copyright work under the CDPA generally.<sup>49</sup>

Upon the receipt of a notice of complaint, the Secretary of State may make such directions as appear to him to be expedient to investigate whether, initially, any “voluntary agreement” subsists which is relevant to the copyright work the subject of the complaint.<sup>50</sup> A “voluntary agreement” is a measure or agreement between a copyright owner, his exclusive licensee or a person issuing copies, or communicating to the public, a work other than a

---

cannot exceed (i) in the case of a company, 5 % of the highest global turnover excluding taxes generated over the course of fiscal year preceding the sanctioned practices or (ii) in other cases, EUR 1.5 million.

<sup>48</sup> Cf. APiG Digital Rights Management Report, p. 9.

<sup>49</sup> The scope of the “permitted acts” provided for by Schedule 5A, and which can therefore be grounds for an application under Section 296ZE, is narrower than the scope of acts generally permitted by copyright law. For example, Schedule 5A does not provide for the following acts generally permitted by the relevant Sections of the CDPA: the right to make temporary copies (Section 28A); criticism, review and news reporting (Section 30); anthologies for educational use (Section 33); and recording, playing or showing works in the course of activities of an educational establishment (Section 34).

<sup>50</sup> Section 296ZE(3)(a).

computer program, the effect of which is to enable a person to carry out a permitted act.<sup>51</sup> If no such agreement or measure exists, the Secretary of State may give directions to ensure that the owner or exclusive licensee of the copyright work makes available to the complainant the means of carrying out the permitted act to the extent necessary to benefit from such act.<sup>52</sup> It is generally assumed that a decision of the Secretary of State with regard to a complaint under Section 296ZE will be amenable to judicial review.<sup>53</sup>

“Authorisation”: The language of the CDPA implies that authorisation by a rights-holder of an infringing act will operate as a defence to liability in respect of that rights-holder. This defence is relevant to all the Sections of the CDPA under consideration in this report.

The CDPA uses the language of “unauthorised” or “without authority” in relation to the various infringing acts or goods but does not define these terms.<sup>54</sup> Section 296ZF(3)(a) is most explicit, mentioning acts that are “not authorised by the copyright owner of that work and are restricted by copyright”. The effect of this wording is not clear; however, it is arguable that authorisation of infringing acts by the owner of the underlying copyright will operate as a general defence to liability under the CDPA for those acts.<sup>55</sup> Furthermore, authorisation by a person who would otherwise enjoy rights under the CDPA would provide a defence to a claim by him in respect of the acts that he authorises but such authorisation would not alter liability in respect of any other rightholders.

“Knowledge” exemptions: The CDPA incorporates “knowledge” exemptions, most of which derive from the relevant European Directives:

- A person liable under Section 296 (“Circumvention of technical devices applied to computer programs”) will only be so liable if he “knows or has reason to believe” that the means in which he deals or the information he publishes “will be used to make infringing copies.”
- A person liable under Section 296ZA (“Circumvention of technological measures”) will only be so liable if he “knows or has reasonable grounds to know” that he is “pursuing that objective” when he is circumventing the measures in question.<sup>56</sup>

---

<sup>51</sup> Section 296ZE(1).

<sup>52</sup> Section 296ZE(3)(b).

<sup>53</sup> Cf. Copinger and Skone James on Copyright, p. 884.

<sup>54</sup> The phrase “without authority” derives from the WCT and WPPT (and is reproduced in the Information Society Directive) but is undefined by those treaties (and that Directive).

<sup>55</sup> It remains unclear whether such authorisation must be express or may be implied. It should also be noted that the question of “authority” or “authorisation” for the purposes of the statutory language will presumably be without prejudice to the operation of the general English law on waiver and forbearance (and related equitable shields against a claim, such as promissory estoppel), which may provide a defendant with relief from a claim.

<sup>56</sup> The judge in *Sony v Ball* noted that the liability here is stricter than that under Section 296; all that is required is for the defendant to have knowledge that he is circumventing the measures applied to the work. He does not need to know that copyright subsists in that work as is required for liability under Section 296.

- A person liable under Section 296ZB will benefit from the higher standard of proof required by the English criminal law. It is a defence for the defendant to prove that he did not know and had no reasonable ground for believing that the device, product, component or service in question enabled or facilitated the circumvention of effective technological measures.
- Liability under Section 296ZD (“Rights and remedies in respect of devices and services designed to circumvent technological measures”) is strict and is not subject to a “knowledge” exemption.
- A person liable under Section 296ZG (“Electronic rights management information”) will only be liable where (i) he knows that he is acting in relation to a public work from which rights management information has been removed without authority and (ii) he “knows or has reason to believe” that such action will induce, facilitate or conceal an infringement of copyright.

“Innocent Infringement”: Under Section 97(1) CDPA, a person with rights will not be entitled to an award of damages if the infringing person did not know and had no reason to believe that copyright subsisted in the work to which his action related. This defence is a general provision of the UK law with regard to remedies for infringement of copyright but only applies to awards of damages and is without prejudice to the availability of injunctive relief.

Other exemptions: There is a further exception to Section 296ZA CDPA under Section 296ZA(2) which provides for research into cryptography unless the extent of circumvention “affects prejudicially the rights of the copyright owner.” Section 296ZB does not make unlawful anything done by, or on behalf of, law enforcement agencies or any of the intelligence services in the interests of national security or for the purposes of the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

Furthermore, Section 296 CDPA (“*Circumvention of technical devices applied to computer programs*”) does not prohibit the act of circumvention itself in relation to such works; therefore, a person wishing to research, or otherwise privately use, that work will not infringe that Section merely by the circumvention of any technical devices applied to that work. Section 296 CDPA is therefore narrower in scope than Sections 296ZA and 296ZD CDPA implementing the Information Society Directive in that Section 296 CDPA is drafted so as to restrict only possession for commercial purposes of, and activities involved in trading in, means which are solely intended to facilitate circumvention and/or the wider publication of circumvention techniques. Conversely, in respect of technological measures applied to works other than computer programs, Section 296ZA restricts the act of circumvention itself.

(c) German law

Article 95b of the German Copyright Act provides for exceptions to Article 95a and imposes on copyright holders an obligation to supply certain beneficiaries with the means necessary to exercise certain copyright

limitations, provided that the beneficiaries have lawful access to the works in the first place. This obligation was extended to producers of protected databases (although no express provision exists in that regard, it is considered that Article 95b applies by way of analogy).

Article 6(4) of the Information Society Directive has been implemented in a restricted manner in Germany. The copyright exceptions in respect of which the rightholders have an obligation are limited to (i) public security and judicial administration, (ii) limitations for the benefit of disabled persons, (iii) collections for use in schools and for teaching illustration, (iv) broadcasts made for specific educational purposes in schools, and (v) making works available for purposes of research and private study.

The rightholders' obligation in respect of the private copying exception covers reprographic copying on paper or similar media, copies for one's own research purposes, copies made for archiving purposes, copies from newspapers for individual information on daily news, but not other private copying for personal domestic uses. Therefore, the circumvention of technological measures may not be justified by the private copying exception<sup>57</sup>. The German Copyright Act was amended in 2007. The issue of private digital copying was discussed controversially during the legislative process. Positions ranged from a prohibition of digital copying of works protected with technical measures to a right to private digital copying even if the works are protected with technical measures. Consumers mainly advanced the latter position while rightholders mainly took the position to prohibit any private digital copying. Allowing the following was also debated: (i) digital copying only after a certain period of time after first publication, (ii) private digital copies only from works owned, or (iii) private digital copying only for certain purposes such as artistic use<sup>58</sup>. The German Copyright Act as amended in 2007 contains only a limited right of private copying that basically covers reprographic copying on paper or similar media for certain privileged purposes as outlined above. Digital copying is not covered by the private copying exception.

In addition, public authorities enjoy a general self help right to circumvent technological measures for purposes of public administration and the judiciary. The rightholder is furthermore obligated to make circumvention tools available should self help prove impossible.

---

(4) Remedial measures

- (a) What are the civil and criminal remedies? (All remedial measures should be considered.) Specifically, consider focusing on whether any measures that respond to the following actions are provided for, and if they are provided for, describe the specific measures.
- (i) manufacture of circumvention devices or the like (including programs);

---

<sup>57</sup> BGH, 17.07.2008, I ZR 219/05

<sup>58</sup> <http://www.urheberrecht.org/topic/Korb-2/bmj/707.pdf>

- (ii) provision of circumvention devices or the like (including programs);
- (iii) export and import of circumvention devices or the like (including programs);
- (iv) possession of circumvention devices or the like (including programs);
- (v) provision of circumvention services;
- (vi) circumvention (reproduction by circumvention); and
- (vii) dissemination of advertisements/information regarding circumvention devices or the like (including programs), circumvention services or circumvention method.

By way of introduction, Article 8(1) of the Information Society Directive only obliges Member States to “provide appropriate sanctions and remedies” and to “take all the measures necessary to ensure that those sanctions and remedies are applied.” The sanctions have to be “effective, proportionate and dissuasive.” Article 8(2) sets out the obligation for Member States to create mechanisms to enable rightholders to seek damages, injunctions and the seizure of infringing material and components referred to in Article 6(2). As a result of the discretion left to Member States in implementing sanctions, remedial measures are largely a question of national laws, which may differ in terms of both, the persons able to exercise rights when a technological measure is circumvented, and the scope of available remedies. According to a comparative study, “most Western European countries provided for criminal sentences against the circumvention of technological protection measures” (ranging from imprisonment to a fine) while “most Eastern European countries provided only for civil remedies against circumvention of [technological protection measures].”<sup>59</sup>

Article 7 of the Computer Programs Directive also requires Member States to provide “appropriate remedies” against persons committing a prohibited act. Article 7(3) further specifies that Member States may, but are not obligated to, provide for the seizure of any circumvention “means” referred to in Article 7(1)(c). Member States thus also enjoy great leeway in the implementation of remedial measures under the Computer Programs Directive.

(i) *French law*

1. *Civil remedies*

A rightholder may bring a civil suit against persons having circumvented a technological measure based on the following grounds:

- Contractual grounds, if the circumvention was prohibited under an agreement entered into between the rightholder and the person having circumvented. As an example, agreements between editors of music websites and Internet users downloading musical works commonly include anti-circumvention clauses.

---

<sup>59</sup> Marcella Favale, p. 14.

- Tort grounds, if the rightholder can demonstrate that the circumvention violated the relevant provisions of the IPC (as set forth under question 2(2)(c)) and that such violation caused damages to the rightholder.<sup>60</sup>

With regard to works other than computer programs, decree no.2006-1763 of 23 December 2006 makes certain evidentiary steps and provisional remedies that are applicable in cases of copyright infringement (such as evidentiary seizures of suspected circumvention devices pursuant to Article L. 332-1 of the IPC) also available in cases of circumvention of technological measures.

If the circumvention or the distribution of circumvention devices is carried out via the Internet, the rightholder will have the right to file a petition (even *ex parte* if it is justified) to have the concerned Internet service provider or hosting service provider implement the necessary measures to stop such circumvention or distribution of circumvention devices (Article 6.I.8 of the law of 21 June 2004).

## *2. Criminal remedies*

### (a) Works or databases other than computer programs

With regard to circumvention of technological measures used to protect works or databases other than computer programs, three levels of criminal liability may be distinguished depending on the type of act that has been committed: (i) trafficking in unlawful circumvention devices, or providing circumvention services, (ii) circumvention without use of a circumvention device or service (i.e., hacking), or (iii) personal possession or use of circumvention device. First, knowingly dealings in devices specially adapted for the purpose of circumventing an effective technological measure, or providing circumvention services (please see question 2(2)(c) for a precise description of prohibited actions) is punished by imprisonment for up to 6 months and a fine of up to €30,000.<sup>61</sup> Second, the act of knowingly circumventing effective technological measures by means other than those

---

<sup>60</sup> Other tort theories that have been used by rightholders before the implementation of the Information Society Directive into French law, including unfair competition. In a decision rendered on 20 October 1988 by the Paris Court of Appeals, damages were awarded to a rightholder on the ground of unfair competition and parasitism. The court's rationale was that circumvention resulted in disorganization within the company and caused a loss of income to the rightholder. However, the ground of unfair competition may only be used in cases where there is a commercial competition between the parties in terms of clients and products.

<sup>61</sup> Articles L. 335-3-1 II and L. 335-3-2 II of the IPC with regard to copyrighted content, Articles L. 335-4-1 II and L. 335-4-2 II of the IPC with regard to content protected by related rights, and Articles L. 342-3-1 and L. 342-3-2 of the IPC with regard to databases. Criminal sanctions may be doubled if the person committing the infringement had entered into an agreement with the victim of the infringement. Additional criminal remedies are provided for in Articles L. 335-5 and L. 335-6 of the IPC, including the seizure of the turnover resulting from the offence or the destruction of infringing devices. According to Article L. 335-8 of the IPC, companies also incur the following sanctions: be prohibited from carrying, directly or indirectly, professional activities for up to 5 years, be placed under legal supervision for up to 5 years; be constrained to close down establishments; be delisted from regulated stock markets or unable to participate in public offerings; be prohibited from drawing checks or using credit cards for up to 5 years.

designed or specially adapted for the purpose of circumvention, is punished by a fine up to €3,750.<sup>62</sup> Third, possessing for personal use or using technical applications, devices, components or services designed or specially adapted for the purpose of circumventing an effective technological measure is punished by a €750 fine.<sup>63</sup>

#### (b) Computer programs

As explained under question 2(2)(c), the Computer Programs Directive was not fully implemented into French law. However, under French case law, the provision of circumvention devices used to undermine technical measures protecting computer programs can be sanctioned based on the general law of copyright infringement pursuant to Articles L. 122-6 and L. 335-3 of the IPC. As a result, criminal remedies available in cases of copyright infringement would also be applicable in this case.

Also, pursuant to Articles L. 122-6-2 and R. 335-2 of the IPC, the advertisement or publication of user's handbook concerning circumvention devices without the express mention that the unlawful use of such devices is liable to penalties applicable to copyright infringement can be sanctioned by a €450 fine.

#### (ii) UK law

Civil remedies: Persons with rights under Sections 296 (*"Circumvention of technical devices applied to computer programs"*), 296ZA (*"Circumvention of technological measures"*), 296ZD (*"Rights and remedies in respect of devices and services designed to circumvent technological measures"*) and 296ZG CDPA (*"Electronic rights management information"*) are entitled to civil remedies.

The civil rights and remedies conferred by the CDPA are expressed to be the same "as a copyright owner has in respect of an infringement of copyright."<sup>64</sup> The principal remedies for infringement of copyright are: (i) either "accounts of profit" or damages; (ii) injunctive relief; and (iii) in relation to rights under Sections 296 and 296ZD only, seizure or delivery up/forfeiture of the infringing goods.<sup>65</sup>

In relation to (i) above, it is for the claimant to elect for any reward to be made to him on the basis of an "account of profit" or damages.

---

<sup>62</sup> Articles L. 335-3-1 I and L. 335-3-2 I of the IPC with regard to copyrighted content, Articles L. 335-4-1 I and L. 335-4-2 I of the IPC with regard to content protected by related rights, and Articles L. 342-3-1 and L. 342-3-2 IPC with regard to databases.

<sup>63</sup> Articles R. 335-3 and R. 335-4 of the IPC.

<sup>64</sup> Rights and remedies available in the UK are therefore concurrent with other rights under the CDPA and the UK law on copyright.

<sup>65</sup> Accounts of profit and injunctive relief are equitable remedies (and subject to equitable defences and bars – for example: a claimant must himself have behaved equitably; delay will bar an equitable claim etc).

An account of profit generally will seek to take from the wrongdoer all the profit that has accrued to him as a result of his piracy. Such relief will generally be granted in cases where there has been a deliberate and knowing infringement, especially where such infringement has been commercially motivated.

Damages are intended to return the person with rights to the position he would have occupied, had the infringement not occurred. Claimants will typically elect for damages. Damages may be awarded for lost profits and for foreseeable consequential losses. Alternatively, a royalty payment may be imposed. Very exceptionally, exemplary damages may be awarded to deter future infringement.

Pursuant to Section 97(1) CDPA, damages will not be an available remedy where the infringement is innocent (i.e., the defendant did not know and had no reason to believe that copyright subsisted in the work to which his action related); the only remedies in such situations will therefore be accounts of profit or injunctive relief.

Alternatively, pursuant to Section 97(2) CDPA, additional damages may be available. The court has the discretionary power, having regard to all the circumstances but with particular regard being paid to both the flagrancy of the infringement and also any benefit accruing to the defendant by his infringement, to award additional damages. The extent of such discretionary additional damages is whatever the court deems the justice of the case to require. However, additional damages cannot be awarded where a claimant has elected for an account of profits.

Injunctive relief is a court order requiring a person or persons to take, or refrain from taking, certain actions; injunctions may take many forms. The court has a wide-ranging power to impose (a) interim injunctions prior to trial and (b) final injunctions at trial. When considering whether to grant an interim injunction, a court will have regard to the guidance established in *American Cyanamid Co v Ethicon Co*.<sup>66</sup> Final injunctions will be granted where the court considers them necessary to adequately compensate a successful claimant (i.e., where damages, or an account of profit, alone are inadequate).

In relation to (iii) above, a person with rights under Section 296 has the right in respect of infringing copies to seize without court order, or to obtain an order for delivery up of, any “means” mentioned by Section 296(1).<sup>67</sup> The

---

<sup>66</sup> *American Cyanamid Co v Ethicon Co* [1975] AC 396. Firstly, it must be established that the claimant has a serious case to be tried; if this is not established, an injunction will not be considered further. Secondly, if a permanent injunction at trial together with damages for any interim loss would compensate the claimant adequately an interim injunction will be unnecessary; typically, damages will not be adequate as the loss in a case of copyright infringement is difficult to quantify. Thirdly, the court must be satisfied that, if the defendant were to succeed at trial, a cross undertaking in damages from the claimant would compensate the defendant adequately for being unjustly restrained during the interim period. If the second and third issues (above) appear unclear to the court, a decision must be made on the basis of the least unjust outcome, having regard to the actual or potential rights and liabilities of the parties concerned.

<sup>67</sup> Sections 100 and 196 CDPA provide for the due process of seizure. A person wishing to seize infringing copies must demonstrate that (i) the copy is exposed, or immediately available, for sale or hire; and (ii) the copy is one in respect of which an order for delivery up



right arises against a person who has those means in his possession, custody or control with the intention that they “should be used to facilitate the unauthorised removal or circumvention of any technical device which has been applied to a computer program”.<sup>68</sup> A similar right of delivery up or seizure is conferred by Section 296ZD in relation to any “device, product or component which a person has in his possession, custody or control with the intention that it should be used to circumvent effective technological measures”.

The CDPA does not contain any specific provisions in regard to the circumvention of technological measures which provide for the rights of rightholders to request information on distribution channels, including information on customers and suppliers. However, it is a general provision of English law that a claimant may apply for a court order requiring a defendant to make an affidavit giving the names and details of, inter alia, suppliers and purchasers of infringing materials and articles known to him.<sup>69</sup> Precedent cases suggest that such orders may be made in respect of physical distribution channels or the Internet.<sup>70</sup>

Criminal penalties: Penalties may be imposed upon persons made criminally liable under Section 296ZB CDPA (“*Devices and services designed to circumvent technological measures*”).

A person guilty of an offence (howsoever committed) under Section 296ZB is liable: (i) on summary conviction to imprisonment for a term not exceeding three months or to a fine not exceeding the statutory maximum, or both; or (ii) on conviction on indictment to a fine or imprisonment for a term not exceeding two years, or both.<sup>71</sup> Section 296ZC(1) applies other sections of

---

under Section 99 or 195 CDPA could be obtained. This means the person from whom the object is seized must have had it in his possession, custody or control in the course of a business and it must have been made less than six years prior to the seizure. In order to exercise the right: (i) notice of the time and place of the proposed seizure must be served at a police station; (ii) nothing in the possession, custody or control of a person at a permanent or regular place of business may be seized; (iii) no force may be used during seizure; (iv) a notice must be left at the place of seizure containing particulars of the person on whose authority the seizure was made; and (v) the exercise of this right is subject to later court orders in relation to the seized goods. Because of these considerations, the right is seldom used; improper use of the right may result in an action against the person exercising the right in the tort of unlawful interference with goods (which may give rise to an award of aggravated or exemplary damages).

<sup>68</sup> Section 296(4). Cf. Sections 99 and 100. Once subject to an order for delivery up, the court may make an order for forfeiture (Section 114).

<sup>69</sup> *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133.

<sup>70</sup> *Polydor Ltd v Woodhouse* [2005] EWHC 3191 (Ch); *Grant v Google* [2006] All ER (D)(MAY).

<sup>71</sup> These penalties are relatively minor, being less severe than those created for other offences by the CDPA. This is because, in passing the European Communities Act 1972, the UK Government limited the penalties for criminal offences created by subordinate legislation made under that 1972 Act to a maximum permitted level: European Communities Act 1972, section 2(2) and Schedule 2 paragraph 1(1)(d). As the offence created by Section 296ZB was created by statutory instrument (the CRRR 2003) to implement the Information Society Directive, the penalties for that Section are capped at the statutory maximum.

the CDPA (providing for the authorisation of search warrants and forfeiture remedies) apply with modification to offences under Section 296ZB.<sup>72</sup>

Where a Justice of the Peace (and, in Scotland, a sheriff) is satisfied by information given on oath by a police officer of the requisite rank that there are reasonable grounds for believing an offence under Section 296ZB has been or is about to be committed in any premises and that evidence related to such offence is in those premises, he may issue a search warrant. Such warrant authorises a constable and any persons accompanying him – within a period of 28 days from its issue – to enter and search the premises, using such reasonable force as is necessary.<sup>73</sup>

Where devices, products or components for the purpose of circumventing effective technological measures come into the possession of any person in connection with the investigation or prosecution of an offence under Section 296ZB(1), that person may apply to court for an order for the forfeiture of such devices, products or components.<sup>74</sup> Where an order is granted, the court may order that the forfeited items be destroyed.<sup>75</sup>

*(iii) German law*

The German Copyright Act provides for both civil and criminal remedies for any illegal circumvention of technological protection measures.

Rightholders may file for injunctive relief against any person who manufactures, imports, distributes, sales, rents, markets or possesses for commercial purposes devices, including computer programs, for the circumvention of technological protection measures. Rightholders may also claim damages, in cases of commercial copyright infringements<sup>76</sup> and request information on distribution channels, including information on customers and suppliers pursuant to Section 101 of the German Copyright

---

<sup>72</sup> Section 296ZC in effect borrows and modifies wording from existing sections of the CDPA providing for offences in relation to broadcasting: from Section 297B, which provides for the authorisation of search warrants in relation to investigations into the use of unauthorised decoders; and from Sections 297C and 297D, which provide for the forfeiture of such unauthorised decoders (in England, Wales or Northern Ireland and in Scotland, respectively).

<sup>73</sup> Section 297B, modified by Sections 296ZC(1) and (2).

<sup>74</sup> Section 297C(1), modified by Sections 296ZB(1), (3) and (4). The court may only grant such order if it is satisfied, inter alia, that a relevant offence under Section 296ZB(1) has been committed in relation to those devices, products or components (Sections 297C(2)-(5), modified by Sections 296ZB(1), (3) and (4)). Such order may be appealed (Section 297C(6), modified by Sections 296ZB(1), (3) and (4)).

<sup>75</sup> Alternatively, Section 297B provides for persons with rights and remedies under Section 298 to apply to the court to order that the items be forfeited to them rather than be destroyed. Similar provisions apply to Scotland (Section 297D, modified by Sections 296ZB(1),(3) and (4)).

<sup>76</sup> Pursuant to Section 101a copyright infringement may also be deemed commercial if the infringement is severe or if a great amount of infringements occurred. The scope of the provision is unclear. The use of so-called Peer-to-Peer Networks was considered a commercial activity (even if no profit is sought) because of the undefined amount of users that could access files provided for download.

Act. If such devices are distributed via the Internet, rightholders may request information from third parties, including Internet service providers, to identify infringers pursuant to Section 101 of the German Copyright Act. All illegal copies have to be either delivered to the rightholder or destroyed.

The rightholder may claim injunctive relief and damages pursuant to Article 97 of the German Copyright Act. The Regional Court of Cologne found that the remedies provided under Article 97 may be claimed against the seller of computer programs intended to circumvent technological measures to protect content.<sup>77</sup> While the sale of such computer programs did not, in and of itself, amount to infringement of copyright or other rights under the German Copyright Act, such trafficking was considered a sufficiently precise threat to copyright to trigger the application of injunctive relief. Most commentators agree that, although not clearly stated in the decision, the Court applied Article 97 of the German Copyright Act by way of analogy even if the case did not directly involve the infringement of a copyrights or other rights protected by the German Copyright Act. This decision therefore seems to extend the availability of injunctive and damage reliefs provided for in this provision to cases of trafficking in circumvention devices which pose a sufficiently precise threat to copyright. It is not certain that the same reasoning will be followed by other German (including Federal) courts, which may, for instance, choose to grant similar relief under general tort law rather than Article 97 of the German Copyright Act.

Violation of the provisions for the circumvention of technological protection measures is considered a criminal offence pursuant to Article 108b of the German Copyright Act. Article 108b Sect. 1 provides for criminal penalties for the act of circumvention of technological measures to protect content while Article 108b Sect. 2 sanctions the trafficking of means intended to circumvent technological measures for a commercial purpose.

The same civil remedies apply in respect of circumvention of technological measures protecting computer programs and other copyrighted material. However, computer programs do not fall in the scope of Article 108b of the German Copyright Act so the circumvention of a device protecting a computer programs is, per se, not sanctioned criminally. Nevertheless, under German law, computer programs receive the protection afforded to all works of authorship so that the general criminal remedies available for copyright infringement would be applicable if the circumvention gave rise to infringement of the copyright in a computer program.

Please see [Annex 4](#) (II), which sets forth the applicable provisions under German law.

---

<sup>77</sup> LG Köln, MMR 2006, 412, 414.

- (b) Who is capable of requesting the remedial measures set forth in (a) above?

(i) French law

1. *Civil remedies*

Any person affected by the violation of the rules set forth under question 2(2) may bring an action for damages against the perpetrator. The claimant can therefore be the rightholder, his successors and assigns, or any person whose interests have been directly damaged by the circumvention. However, except if the technological measure is itself protected by intellectual property (e.g., a copyrighted computer program the circumvention of which amounts to copyright infringement), the developer of the technological measures is usually not entitled to claim damages since the technological measures' sole purpose is to protect a content covered by intellectual property rights.

2. *Criminal remedies*

Criminal prosecution for the imposition of criminal penalties generally falls upon the Procureur de la République (i.e., the attorney general), although prosecution may also be initiated by the injured party<sup>77</sup>, as defined above.

(ii) UK law

Sections 296 (“*Circumvention of technical devices applied to computer programs*”) and 296ZD (“*Rights and remedies in respect of devices and services designed to circumvent technological measures*”) confer rights (which are the same as a copyright owner has in respect of an infringement of copyright) on the following persons:

- (i) a person issuing to the public copies of, or communicating to the public, the work to which the technological measure has been applied;
- (ii) the copyright owner or his exclusive licensee, if not the same person as (i) above; and
- (iii) the owner or exclusive licensee of any intellectual property right (this will presumably include rights other than copyright as well – i.e. patents et al.) in the relevant technological measure itself.<sup>78</sup>

---

<sup>77</sup> In the absence of an indictment by the attorney general, an injured party may file a criminal suit against the perpetrator of a criminal offence. However, even before a criminal court, the injured party is not granted the power to indict but only to seek damages. If the perpetrator is found liable, the plaintiff would likely collect damages, but it will still be up to the attorney general to make a recommendation as to what criminal sanctions should be incurred, and for the court to decide whether criminal sanctions are warranted. In addition, the injured party having filed a criminal suit must bring forward evidence it has collected privately and is not granted special investigative powers for that purpose.

<sup>78</sup> “Issuing” and “communicating” are defined by the CDPA. “Issuing to the public” is defined as the act of putting into circulation in the EEA copies of a work not previously so circulated in the EEA by or with the consent of the copyright holder (or the act of putting into circulation outside the EEA copies not previously so circulated in the EEA or elsewhere). “Communicating to the public” is defined as communicating to the public by electronic transmission, including by “on demand” service.

Conversely, Sections 296ZA (“*Circumvention of technological measures*”) and 296ZG (“*Electronic rights management information*”) only confer rights on the persons enumerated at (i) and (ii), but not (iii). An owner of rights inhering in technological measure or rights management information (as appropriate) therefore does not have rights conferred upon him by Sections 296ZA and 296ZG.

Criminal offences under Section 296ZB (“*Devices and services designed to circumvent technological measures*”) will be investigated and prosecuted by the UK police together with the Crown Prosecution Service.

(iii) German law

1. *Civil remedies*

An injured rightholder is always entitled to request the application of the remedial measures set forth under question 3(a) above. The Federal Court of Justice decided that an exclusive licensee whose rights of use have been affected may also bring an action for injunctive relief.<sup>79</sup>

2. *Criminal remedies*

Criminal prosecution for the imposition of criminal penalties generally falls upon the attorney general. However, in the absence of prosecution by the attorney general, the injured party may file a criminal suit against the perpetrator (“*Privatklage*”).<sup>80</sup>

- 
- (c) Are there any border measures pertaining to export and/or import of violational devices or the like, or any administrative measures to deter violation provided for? If they are provided for, what is the specific substance of the measures?

(i) French law

Article L. 335-10 of the IPC relating to customs measures only provides for border measures in respect of products infringing copyrights but does not directly cover circumvention devices.

(ii) UK law

As discussed, UK law restricts importation of certain circumvention devices, as defined by the relevant sections of the CDPA:

---

<sup>79</sup> BGH, 20 December 1994, X ZR 56/93.

<sup>80</sup> The attorney general is obliged to prosecute all criminal offences. However, in cases of minor public interest in criminal prosecution, the attorney general may decide to close proceedings. In the context of this study, a typical situation would be illegal file sharing on so-called peer-to-peer networks. Attorney generals usually identify file sharers but close proceedings afterwards. The injured party may file a criminal suit against the perpetrator. However, fines imposed on the perpetrator in such proceedings will be paid to the state. Therefore, the injured party will usually claim civil rather than criminal remedies.

- Section 296 prohibits importing for commercial purposes any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of a technical device applied to a copyright computer program.
- Section 296ZB prohibits importation, otherwise than for private and domestic use, of circumvention devices relating to effective technological measures applied to copyright works other than computer programs.
- Section 296ZD prohibits importing for commercial purposes any circumvention devices relating to effective technological measures applied to copyright works other than computer programs.<sup>81</sup>

No specific border measures are provided for under UK law for circumvention devices.<sup>82</sup>

(iii) *German law*

No such border measures are provided for under German law for circumvention devices.

---

(5) Restrictions on so-called “non-reacting devices”

Whether there are any restrictions provided for by way of laws, rules, orders, or the like against so-called “non-reacting devices,” which are devices that do not detect protective technological measures (i.e., copy protect signals and access protect signals) attached to contents, and allow copying of contents and replaying of unlawful reproductions as a result. If so, the specific restriction clauses. Describe the substance of any such restrictions.

The Information Society Directive and the Computer Programs Directive do not address the issue of “non-reacting devices.” They should be treated like all circumvention devices under the European Directives.

As a result, if non-reacting devices fall within the scope of the Information Society Directive (i.e., they enable the circumvention of technological measures protecting works other than computer programs), the test to determine whether their production, distribution and possession should be prohibited or not will be to apply the criteria provided in Article 6(2), and will essentially depend on whether they have a commercially significant purpose

---

<sup>81</sup> See Part 2(2) above for the specific criteria involved in determining circumvention devices.

<sup>82</sup> Infringing copies may be confiscated in the UK by Her Majesty’s Revenue & Customs, together with the UK Border Agency, in accordance with general law. EU Council Regulation 1383/2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights [2003] OJ L196/7 provides for counterfeit or pirated goods (including infringing copies) on the initiative of customs authorities or at the successful application of a rightholder.

or use other than to circumvent technological measures (see question 2(2)(b)). As explained in recital 48 of the Information Society Directive, there is “no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6.” For instance, a regular PC that can be used to decrypt a file but also as a word processor should not fall under the criteria.

If non-reacting devices fall within the scope of the Computer Programs Directive (i.e., they enable the circumvention of technological measures protecting computer programs), their distribution will be prohibited only if their sole purpose is to facilitate the circumvention of technological measures (see question 2(2)(b)).

Likewise, under UK law, it is the fact of circumvention, rather than the manner in which circumvention is achieved, that is restricted by the law. “Non-reacting devices” are therefore also subject to the restrictions of the CDPA described above.

By way of example in the UK, the case of *Sony v Ball* concerned the Messiah 2 chip for the Playstation 2, which was a non-reactive device. It essentially enabled a Playstation 2 modified with the chip to read a greater range of discs, including those subject to regional-control technology. This device was held by the court to infringe both Sections 296 and 296ZA.<sup>83</sup> Similarly, two recent criminal cases under Section 296ZB CDPA involved ‘modchips’ designed to bypass regional-control technology and thereby enable consoles to read unlawful reproductions. Such devices were held clearly to facilitate the circumvention of technological measures.<sup>84</sup> Strictly, the devices restricted in UK case law were products which made reacting devices (i.e. the copy-protected hardware) non-reacting; however, the act of circumvention was the key issue at stake.

Similarly, German and French laws do not explicitly address the issue of “non-reacting devices”, which are to be treated like all circumvention devices. It should however be noted that, in respect of technical devices protecting computer programs, since French law did not fully implement article 7(1)(c) of the Computer Programs Directive, no reference to the “intended purpose” of the device is made in Article L. 122-6-2 of the IPC so that any publication or user’s handbook concerning non-reacting devices would have to state that the unlawful use of such means is liable to the penalties laid down for cases of infringement regardless of whether the device has a non-circumvention purpose.

---

<sup>83</sup> *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball & Ors* [2004] EWHC 1738 Ch. The case is discussed in more details under question 3(1).

<sup>84</sup> *Higgs v R* [2008] EWCA Crim 1324; *Gilham v R* [2009] EWCA Crim 2293. However, these cases have established that it is not sufficient to show that the measures simply discourage the making of infringing copies; rather it must be demonstrated that the act of playing the infringing copy is a restricted use of the work to which measures have been applied; this is because in the definition of “effective technological measure”, “protection” should only be construed to be protection against unauthorised acts that are restricted by copyright (cf. Section 296ZF(3)(a) CDPA).

### 3. Data Regarding Precedents, Enforcement Status, Damage Status, Etc.

#### (1) Precedents relating to technological measures to protect contents

##### *(a) France*

Most precedents relating to technological measures concern final users trying to take advantage of exceptions to copyright. The leading case in this regard is the so-called “Mulholland Drive case”<sup>85</sup>, which involved a consumer who had purchased a DVD of the film Mulholland Drive but was prevented from making an analogue copy by a copy-control mechanism embedded in the DVD. With the help of a consumers' association, he filed a claim against the concerned rightholder and distributor of the DVD. In a decision handed down on 28 February 2006, the *Cour de Cassation* (the French highest court for civil and criminal law matters) reversed the decision of the Paris Court of Appeals of 22 April 2005, which had ordered the rightholder to put the consumer in a position to exercise the private copying exception to copyright. For the *Cour de Cassation*, the rightholder's interest in the normal exploitation of the work and implementation of technological measures to that end prevailed over that of the consumer's in exercising the private copying exception (which the *Cour de Cassation* was careful not to characterize as a right granted to users of copyrighted works but as a mere defence to infringement actions).

It should be noted that this decision was rendered before France adopted the law implementing the Information Society Directive in 2006. Today, a consumer wishing to file a claim against a rightholder in order to exercise one of the copyright exceptions recognized under French law as a limitation to technological measures would have to do so not with a tribunal but with the HADOPI (formerly, ARMT). The *Cour de Cassation* has confirmed this position in a decision dated 19 June 2008.<sup>86</sup> As a result, while consumers may use the private copying exception as a defence in an infringement suit brought by a rightholder, they will have to petition the HADOPI in order to enforce that exception. However, with various degrees of success, consumers sometimes attempt to circumvent this rule by grounding their

---

<sup>85</sup> UFC Que Choisir v. Alain Sarde Film and Studio Canal.

<sup>86</sup> The HADOPI has exclusively jurisdiction to arbitrate on claims brought by the beneficiaries of exceptions to copyright against rightholders implementing technological measures that would prevent the exercise of those exceptions (see question 2(3)(a)). However, although it was created on April 6, 2007, the ARMT never rendered any decision. This may be explained in part by the fact that the music industry decided to stop using technological measures around that period. A second reason is that the complexity of the procedure and financial risks associated therewith might have persuaded consumers not to file claims with the ARMT. Indeed, the claimant is liable for costs if the claim is dismissed. Furthermore, even if the ARMT (now the HADOPI) rules in favour of the claimant, he would still bear the financial risks related to an uncertain and costly judicial procedure since the respondent would have the right to appeal. In this respect, the recently created Article L. 331-36 of the IPC establishing the possibility for the HADOPI to give non-binding opinions could encourage consumers to increasingly resort to the HADOPI in its regulatory capacity.



claims not on copyright exceptions but on the implied warranty against hidden defects<sup>87</sup> or on consumer protection laws.<sup>88</sup>

We are aware of only two cases relating to the circumvention of technological measures that were tried in the past twenty years. In the first case, which was handed down in 1989 (i.e., before the Computer Programs Directive was adopted), the Paris Court of Appeal recognized that circumvention (the court uses the term “neutralization”) of a technical device protecting a computer program was not per se unlawful.<sup>89</sup> This seems to still be the case under the Computer Programs Directive. In the second case, the Paris Court of Appeals ruled that the act of developing or making available to the public a computer program circumventing a technical device protecting a computer program amounted to copyright infringement under Article L. 335-3 of the IPC.<sup>90</sup> This case was considered as an attempt to remedy the fact that French law only partially transposed Article 7(1)(c) of the Computer Programs Directive and still lacks specific remedies applicable to trafficking in means which sole purpose is to circumvent technical devices applied to protect computer programs.

*(b) The UK*

The English courts have produced very few precedent cases. The reported cases in this area are the cases of *Sony Computer Entertainment v Paul Owen & others* [2002]; *Sony Computer Entertainment v Gaynor David Ball & others* [2004]; *Higgs v R* [2008] EWCA Crim 1324; and *Gilham v R* [2009] EWCA Crim 2293.<sup>91</sup>

The civil cases of *Sony v Owen* and *Sony v Ball* concerned the sale in the UK of chips designed to enable the circumvention of regional control code and devices applied to Playstation 2 games and the Playstation 2 console. Certain individuals were importing and selling (and in some cases installing) chips which circumvented technological measure and which were used to create

---

<sup>87</sup> Even though such suits were sometimes successful (e.g., *Tribunal de Grande Instance* of Nanterre, 2 September 2003), an action involving a consumer arguing that works protected by anti-copying measures violated the implied warranty against hidden defects was recently dismissed by the Paris Court of Appeals (Paris Court of Appeals, 4e ch., 20 June 2007).

<sup>88</sup> The *Tribunal de Grande Instance* (civil first instance tribunal) of Nanterre ruled in favour of consumers in several cases including in the *UFC Que Choisir v. Sony France* case of 15 December 2006, involving the sale of non-interoperable products (CDs) without proper warning. Other similar judgments were handed down by the *Tribunal de Grande Instance* of Nanterre on 2 September 2003, and 31 May 2007.

<sup>89</sup> Paris Court of Appeals, 13e ch., 2 March 1989.

<sup>90</sup> Paris Court of Appeals, 13e ch., 17 June 2005. The Court sentenced the concerned individual to 7 months imprisonment (with reprieve). It should be emphasized that the ruling was based on copyright infringement, which calls for more severe sanctions than those applicable to circumvention.

<sup>91</sup> *Sony Computer Entertainment v Owen & Ors* [2002] EWHC 45 Ch; *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball & Ors* [2004] EWHC 1738 Ch. Note that the claim in *Sony v Ball* was framed to allege breach of Section 296 and 296ZA, in the alternative. This case indicates that as a litigation strategy, it may be desirable in the UK to be able to show that technological measures have been applied to hardware and other copyrighted works other than computer programs, since the scope of 296ZA is more favourable to a claimant.

“infringing copies” for the purposes of Section 296 CDPA (“Circumvention of technical devices applied to computer programs”). It was held that these devices infringed UK law and the individuals were liable to Sony for damages and costs.

The ruling in *Sony v Ball* in particular suggests that any device that achieves circumvention will be caught by the broad drafting of UK law – even the transient transmission of data from game disc to RAM chip required for a Playstation 2 console, fitted with a “Messiah 2” pirate chip, to “read” that game was held to constitute copying which infringed the underlying copyright. The fact that the RAM chip only constituted an “infringing article” for a fractional moment of time did not enable the defendant in that case to escape the language of Section 296 CDPA.

The recent reported criminal cases of *Higgs v R* and *R v Gilham* concerned the commercial offer, sale, possession and distribution of similar “modchips” designed to enable persons to circumvent copy-protection code embedded in various consoles and games and thereby play pirated copies of games (from which the DRM had been stripped in copying). The modchips made the consoles “non-reactive”, preventing the console hardware from detecting the absence of regional copy-protect codes. The devices therefore fell within the definition in Section 296ZB CDPA of devices, products or components “primarily designed, produced or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures”.

In *R v Gilham*, the judge summarised the various elements of an offence under Section 296ZB which the prosecution had to prove:

- “(1) That the game is or includes copyright works within the meaning of Section 1 [CDPA].
- (2) That the playing of a counterfeit DVD on a game console involves the copying of a copyright work.
- (3) That such copying is of the whole or a substantial part of a copyright work: Section 16(3) [CDPA];
- (4) That the game consoles and/or genuine DVDs (i.e. copies of the copyright work or works created by or with the licence of the owner of the copyright) include effective technological measures within the meaning of Section 296ZF [CDPA] designed to protect those copyright works.
- (5) That in the course of a business the defendant sold or let for hire a device, product or component which was primarily designed, produced or adapted for the purpose of enabling or facilitating the circumvention of those technological measures. It is to be noted that this issue does not depend on the intention of a defendant who is not responsible for the design, production or adaptation of the device, product or component; his intention is irrelevant.”

In *Higgs*, the prosecution did not seek to prove at trial that the playing of the counterfeit DVD involved the copying of a whole or substantial part of a copyright work and the defendant’s appeal succeeded on this technicality (the prosecution failed to prove all elements of the offence).

Therefore, the successful appeal by the defendant in *Higgs* highlighted a key aspect of the definition of “effective technological measures”. A copy-control

technological measure is only “effective” (Section 296ZF(2)&(3) CDPA) if it “achieves the intended protection”. In *Higgs* and *Gilham*, it was therefore necessary to show that, once the device had been circumvented, it was indeed possible to make infringing copies – i.e. the momentary copies of the copyrighted information in the RAM chip of the console or the copyrighted images (designs and artwork) on the screen.

The judge in *Gilham* reminded the court of the fact that “in appropriate cases, the Court will grant injunctive relief, and a breach of an injunction will lead to punishment for contempt of court” and that where an offender “has substantially profited from criminal conduct, proceedings for the civil recovery of the proceeds of his crimes may be brought under Part 5 of the Proceeds of Crime Act 2002”.

(c) Germany

(i) The District Court of Munich decided in 2007 that offering software for the circumvention of technological protection measures on ebay is illegal and issued an injunctive relief.<sup>92</sup> The defendant has argued that he did not offer the incriminated software and that it cannot be excluded that family members had used his ebay account. The court held that the owner of an ebay account is liable for all infringements committed on that account in civil proceedings.

(ii) The District Court of Munich decided in 2006 and in 2007 that the owner of a webpage setting a hyperlink to another webpage is liable under Article 95a Sec. 3 No.1 of the German Copyright Act if he is aware of the fact that software for the circumvention of technological measures is offered on that webpage.<sup>93</sup>

(iii) The Federal Court of Justice ruled in 2008 that advertising for the purpose of Article 95 a Sec. 3 of the German Copyright Act can consist of every kind of statement aiming to promote the concerned product.<sup>94</sup> It is not restricted to commercial actions and covers private and one-time offers for sale.

The defendant offered software on ebay that could copy works even if they were protected by technological measures. The claimant stopped the Internet auction without having sold any software. The defendant signed a cease-and-desist letter but refused to pay the claimant’s legal fees. The Federal Court of Justice decided that the claimant was entitled to cease-and-desist fees pursuant to Article 97 Sec. 1 of the German Copyright Act. This is only the case if an interested average user can understand the technological measures without the help of any further information.

(iv) The Higher Regional Court of Munich decided in 2005 that publishing an article about circumvention of effective technological measures does not amount to advertising for the purpose of Article 95a Sec. 3 of the German

---

<sup>92</sup> LG München, 13.6.2007, 21 S 2042/06.

<sup>93</sup> LG München, 14.11.2007, 21 O 6742/07; LG München 11.10.2006, 21 O 2004/06.

<sup>94</sup> BGH, 17.7.2008, I ZR 219/05.

Copyright Act.<sup>95</sup> Also, publishing an article containing general instructions about circumventing technological measures does not amount to the provision of circumvention services. However, in the case at hand, the publisher of an online article had placed a hyperlink to a webpage offering circumvention software for downloading and described the use of such software, which was held to constitute an infringement.

(v) The Regional Court of Cologne ruled in 2005 that offering software on ebay for the circumvention of technological measures is illegal. Pursuant to Article 97 of the German Copyright Act rightholders are entitled to damages and injunctive relief.<sup>96</sup> Accordingly, the court granted an injunctive relief and ordered the infringer to pay all legal costs, including attorney fees for a cease-and-desist letter.

---

(2) Enforcement status relating to technological measures to protect contents

(a) France

The few French court decisions on the topic of enforcement status relating to technological measures are described under question 3(1). There are no statistical data available with regard to criminal or civil enforcement status.

(b) The UK

It is apparent from the facts in *Sony v Owen* that an interim injunction had previously been granted to prevent one defendant from retailing the circumvention devices. This was therefore one example of an interim or interlocutory order that an English court might make to protect the persons upon whom rights are conferred by the CDPA.

The “Digital Britain” Report published by the UK Government in 2009 suggest that a civil action to enforce rights under the CDPA would have a minimum cost between £6,000-£10,000.<sup>97</sup> Given this cost, many rights-holders would be unwilling to pursue an infringement to court unless the infringement in question were as extensive and easily prosecuted as in *Owen* and *Ball*.

No statistical data was available in that regard.

---

<sup>95</sup> OLG München, 28.7.2005, 29 U 2887/05.

<sup>96</sup> LG Köln, 23.11.2005, 28 S 6/05.

<sup>97</sup> UK BIS Department, “What Role for a Digital Rights Agency?”, p. 20; accessed at <http://www.ipso.gov.uk/digitalbritain.pdf>.

*(c) Germany*

An effective system to protect contents by civil proceedings has been established. Injunctive relief is generally granted on short notice by the courts based on interim injunctions. No statistical data was available in that regard.

---

- (3) Damage status relating to technological measures to protect contents (Include statistical data if any. Hearings or the like should be conducted in the research as appropriate.)

*(a) France*

Due to the very limited number of relevant cases, no statistical data is available with regard to damages awarded in cases involving the circumvention of technological measures in France.

*(b) The UK*

In *Sony v Owen*, damages were awarded for Sony's loss of profit; additional damages were awarded as a result of the defendant continuing to sell circumvention devices in breach of an injunction restraining him from so doing. Section 97 of the CDPA allows a court to award additional damages where the infringement of copyright is flagrant, to have a deterrent effect in instances where the infringement of IPR is sustained and obvious. The precise extent of damages in *Sony v Owen* was unreported.

Similarly, in *Sony v Ball* the extent and nature of damages was unreported; it is to be presumed that damages were awarded for loss of profit.

No statistical data was available in that regard.

*(c) Germany*

No statistical data was available with regard to the damage status relating to technological measures to protect contents.

---

#### **4. Research on Technological Trends**

- (1) Technologies that are currently used pertaining to technological measures to protect contents. (Information should be assembled according to category.)

*(a) Film and video*

Beginning in 1996, the DVD Forum<sup>98</sup> recommended the application of a Content Scrambling System<sup>99</sup> (“CSS”) to all DVD releases. Despite being the subject of several successful attempts at circumvention by hackers, CSS is still used in an updated form today. In 2005, the AACS Licensing Administrator LLC<sup>100</sup> announced a specification standard for next-generation video media formats, such as HD DVD and Blu-Ray Disc (“BRD”). The Advanced Access Content System (“AACS”)<sup>101</sup> appeared in hardware and other devices from 2006 onwards.

Since 2005, the Digital Video Broadcasting (“DVB”)<sup>102</sup> Joint Technical Committee has been developing its DVB Content Protection & Copy Management system (“DVB-CPCM”). The DVB-CPCM is a digital right management standard intended to regulate and protect digital television broadcasting in Europe.<sup>103</sup> The development of the scheme appeared to have become stalled as of late 2007 and early 2008, when negotiations over the technical specification submitted to European regulators broke down.

---

<sup>98</sup> The leading industry representative for hardware manufacturers, computer programs firms, content providers and other users of DVD and HD DVD.

<sup>99</sup> The initial form of CSS utilised basic algorithms to encrypt DVD recordings; hardware manufacturers were required to sign licence agreements restricting the inclusion of features which would facilitate copying of encryption-free content on their DVD players.

<sup>100</sup> A joint venture between leading content providers including Disney, IBM, Intel, Microsoft, Panasonic, Sony, Toshiba and Warner Brothers.

<sup>101</sup> AACS uses advanced cryptography techniques together with rights management information to identify technology and to track attempts at circumvention. Compared to CSS, the nearest standard, the system displays several differences. All players of a certain type are equipped with the same decryption key. Content is encrypted on a title-specific basis and then encrypted under each model’s decryption key. Each disc therefore contains decryption keys for each individual player type. Each small section of content is further encrypted using different keys. Digital watermarks are applied to each disc version to enable the administrators to track which sections of media are made subject to successful hacks. Similarly, if a player is compromised, the theory is that it could be “revoked” – i.e. not included as a supported system in future disc releases. However, this would clearly be a controversial step and involve costs in regard to consumers who use that platform. In addition, the AACS has been designed to enable next-generation technological measures designed to close the so-called “analogue hole” (see question 4(2)).

<sup>102</sup> The DVB is an industry-led consortium of over 270 broadcasters, operators, manufacturers and regulatory bodies involved in digital television in over 35 countries.

<sup>103</sup> Some industry commentators view the DVB-CPCM as the European version of a “Broadcast Flag” idea that was unsuccessfully launched in the USA by Fox in 2005 and made subject to legal challenges. However, there are many technical differences between the two digital right management technologies. The DVB-CPCM adds metadata to digital content which, when played through a CPCM-enabled device, enable a broadcaster to set detailed parameters on the use of that content. For example, the content could be made to expire after a time limit, be unable to be played on more than one device, be unable to be copied etc. Furthermore, the technology can be used to establish ‘user domains’, limited by the physical location of the compliant device(s) – for example, an in-car television or a home entertainment system – or simply by geographic area.

Microsoft's Windows Vista operating system utilises a digital right management system in relation to video, the Protected Video Path<sup>104</sup> ("PVP"), as part of its Protected Media Path technology.

*(b) Music and audio*

Since late 2007 and early 2008, the four "major" record labels – namely EMI, Sony, Universal and Warner – have ceased to include digital right management technology on their audio CDs. In particular, major record labels have generally stopped using access control and copy control technological measures and switch to digital watermarking in the hope of increasing their sales volumes (see question 4(2) below).<sup>105</sup> It is now unusual to encounter audio CDs that are subject to digital right management technology.

In relation to music downloads via the Internet, the "big four" music labels announced in 2007 that they would be moving away from the use of digital right management<sup>106</sup> in relation to their online content. The distribution of digital right management-free music has coincided with the use of other legal protection methods, such as "clickwrap" or "clickthrough" licensing agreements that alert consumers to the relevant copyright law, set the contractual terms of distribution and discourage infringement. However, on 21 January 2009 Microsoft announced that its new MSN Mobile Music service would be returning to digital right management-protected downloads.<sup>107</sup>

---

<sup>104</sup> The concept uses Microsoft's "signed content" verification signatures; it seeks to prevent unsigned applications from running at the same time as digital right management-protected video content is playing. This prevents users from using computer programs that are not compliant with the digital right management to copy protected content, since Microsoft controls verification signatures via licence. Data is encrypted en route to the graphics card, for example, to prevent copying. The PVP also controls video outputs via the PVP Output Protection Management scheme ("PVP-OPM"). This system, inter alia, prevents output from being displayed on monitors which are not equipped to display high density copy right content ("HDCP"). This digital right management therefore is not interoperable with older monitors.

<sup>105</sup> See for instance, in Germany: <http://www.heise.de/ct/meldung/Musik-Downloadportale-verkaufen-wieder-mehr-Alben-748961.html>.

<sup>106</sup> The online music sector has traditionally been dominated by two digital right management systems: Microsoft's Windows Media Digital Rights Management system and Apple's "Fair Play" system. The main other digital right management systems included Microsoft's "PlaysForSure" technology, Sony's OpenMG "Connect" digital right management technology, "iTunes Plus" and Rhapsody's own proprietary digital right management encryption system called "Helix".

<sup>107</sup> The protection technology employed would mean that the songs downloaded would be locked to the device used to download them. Microsoft also accepted that the digital right management technology would mean that whenever a user upgraded their handset or device, the music locked to it would be lost. (Source: PC Pro.co.uk, "Q&A: Microsoft defends return to DRM", accessed on 18 October 2009 at <http://www.pcpro.co.uk/news/245859/q-a-microsoft-defends-return-to-drm>.)

*(c) Computer games*

Computer games are subject to extensive digital right management protection; indeed, many of the earliest and most primitive technological measures were applied to computer games. The FADE system<sup>108</sup> was developed by Macrovision and employed an innovative new approach to content protection. The SecuROM system<sup>109</sup> was a prominent copy protection technology which received negative publicity in 2008 when consumers in the US filed a class action against Electronic Arts for restricting the number of installs possible with the game *Spore*.

*(d) Computer programs*

Computer programs have been protected by:

- encryption keys – such keys may require the manual entry of a code or serial number to verify the copy or, as is increasingly common, be invisible to the end-user but use cryptography techniques to prevent copying of the computer program;
- bus encryption and encrypted code (for use in highly secure processes which do not need to produce intelligible contents for end-users);
- external anti-piracy hardware (colloquially known as ‘dongles’) which contain dedicated serial numbers for each copy of the computer program (given the cost of producing such hardware, this technology has generally only been used for expensive, specialist computer program);
- Internet/phone product activation, which require end-users to verify their copy of a program prior to use (once registered, a copy will often refuse to install or run on another machine); or
- code-scrambling or obfuscation, whereby contents can only be copied or read (usually within a device) where the device is compliant with the DRM attached to the copy.

*(e) E-books*

Digital right management techniques are used extensively in relation to E-books. Digital right management usually restrict the number of devices on which a download will play and also prevent copying or printing. Microsoft Reader contains digital right management technology, with varying levels of protection.<sup>110</sup> Adobe Acrobat is equipped with digital right management

---

<sup>108</sup> Game discs would be issued with barely perceptible fake ‘scratches’ on the disc image. When copied by conventional means, the copier would detect and correct these scratches. The game files would then detect a copied disc as a pirated copy. If a pirate copy was detected, the FADE system would slowly degrade features of the game and render the game unplayable. This was intended to result in an extremely frustrating experience for an infringing user, since the pirated copy would initially appear to be fully playable.

<sup>109</sup> The SecuROM TPM was designed to prevent both casual and commercial copying and reverse engineering and in particular required extensive online or phone activation to enable users to play games protected by the technology.

<sup>110</sup> Some books are unable to be modified. Microsoft Reader also “inscribes” some books with rights management information identifying the original legal purchaser of the book –



encryption which enables publishers and distributors of E-Book content to set different security levels for that content.

*(f) Corporate and library documents*

Electronic digital right management technology, in particular rights management information, are applied to corporate and library documents to enable the tracking and control of those documents.

- 
- (2) Whether there are any new technologies pertaining to technological measures to protect contents, such as digital watermarking. If any, the nature thereof. (Information should be assembled according to category.)

*(a) Film and video*

Some modern copying technologies<sup>111</sup>, which are likely to be applied to video, are capable of distinguishing signals that are present in the analogue signal and then refusing to copy those signals; modern technology may slowly be closing the so-called “analogue hole”. It has been suggested during recent industry and governmental reviews of the state of digital right management technology that there could be more industry standards using technological measures which discourage analogue copying in the near future (our research suggested such technologies, for example in relation to the AAC3 system, may emerge at the consumer level from 2010-12 onwards).<sup>112</sup>

*(b) Music and audio*

The new technology described above in (a) can also be applied to audio media. A leading example of such digital “watermarking” in relation to audio media is Verance’s Audio Watermark Technology, which is available for licensing by BRD and HD DVD manufacturers.<sup>113</sup>

In October 2009, Spotify announced that it will soon offer a subscription service for music downloads. It was not stated explicitly whether digital right management will be applied to the downloads; however, a spokesperson for Spotify said that the tracks would not be able to play on devices other than the device used to download them. Also, if the subscription is not

---

copies will therefore bear that person’s details. Premium content is linked to Reader itself, which can only be activated via the same Microsoft Live ID for a limited number of times. The E-Book will therefore only play on the device used to download it where that device is equipped with Reader.

<sup>111</sup> New digital right management technologies are capable of producing an encrypted signal in outputs over analogue connections. This signal will be in the form of variation to the waveform of the analogue output to such a subtle degree as to be imperceptible to the end-user. Copy devices and related technologies that are compliant with the industry standard will then refuse to copy the analogue output back into digital form.

<sup>112</sup> APIG Digital Rights Management Report, p. 5.

<sup>113</sup> Source: BNET UK Business Wire: accessed on 19/10/09 at [http://findarticles.com/p/articles/mi\\_m0EIN/is\\_2007\\_July\\_2/ai\\_n19330330/](http://findarticles.com/p/articles/mi_m0EIN/is_2007_July_2/ai_n19330330/).

renewed, the option to play songs offline will cease to exist.<sup>114</sup> However, Virgin Media had already announced in June 2009 that it would be offering the world's first subscription service without digital right management or download limits.

*(c) Digital books*

In Germany, publishers of digital books tend to use watermarking<sup>115</sup>. Thereby the information about the author can be directly connected with the digital product. At the same time the authorized user is registered in the document.

Adobe offers with its new invention "Lightroom 3" the possibility to put watermarking in pictures that can be saved and organized in Lightroom 3.<sup>116</sup>

- 
- (3) Whether laws are succeeding in covering the technologies pertaining to technological measures to protect contents that are currently used and to new technologies.

As explained under question 2(a) above, European jurisdictions have generally adopted a broad "catch all" approach encompassing all types of circumvention technologies whether in existence or not yet existing. In practice the legal protection of technological measures appears to be satisfactory to the rightholders since, apart from most rightholders of music and audio contents, the rightholders of other types of contents continue to resort to them. For instance in the UK, despite the small number of reported precedent cases, governmental inquiries indicate that industry representatives are generally satisfied that the CDPA provides adequate protection for digital right management technologies.<sup>117</sup>

However, many commentators feel that the law is increasingly irrelevant in relation to technological measures in particular; the success of the technologies is dependent upon the strength of their technical, rather than the legal, protection of content. Conversely, many consumer respondents to Governmental inquiries have suggested that Section 296ZE CDPA ("Protection of Permitted Acts") is inadequate. The UK process has been criticized as slow and "without teeth"<sup>118</sup> and the provisions of this Section have reportedly never been used. This suggests that the legal protection of technological measures is stronger than some UK consumers would like; the protection of the CDPA may favour rightholders over consumers.

---

<sup>114</sup> Source: BBC News, accessed on 18 October 2009 at <http://news.bbc.co.uk/1/hi/technology/8285252.stm>.

<sup>115</sup> Source: <http://www.stern.de/digital/homeentertainment/illegale-tauschboersen-angriff-der-buchpiraten-1514330.html>; <http://www.heise.de/ct/meldung/E-Book-Reader-Cybook-Opus-bei-Libreka-755565.html>.

<sup>116</sup> Source: <http://www.heise.de/ct/meldung/Betaphase-von-Lightroom-3-startet-836153.html>.

<sup>117</sup> APIG Digital Rights Management Report, p. 10.

<sup>118</sup> APIG Digital Rights Management Report, p. 11.

Some commentators also think that the legal protection of technological measures, as stated by the two European Directives, is not fully consistent with international norms, lacks a real harmonization between Member States (due to the vagueness of the provisions of Article 6 of the Information Society Directive in particular), comprises provisions that lack legal certainty and is imbalanced to the benefit of content providers and technology developers, and to the detriment of the users.<sup>119</sup> Those authors are particularly concerned the broadening of the rightholders' powers, because the protection of technological measures is not expressly linked to the actual infringement of copyright law.

Finally, the "analogue hole" problem has not been tackled directly by legislation in the EU, as this issue is generally considered to be better addressed by technology than by laws. For instance, one answer to this problem is the development of watermarking technologies that remain visible in analogue signals (as explained under question 2(a)) and that enable the monitoring of the protected content even after an analogue copy has been made. Certain countries such as France encourage the development of a national repertory of analogue copies of existing protected works that could be used to develop new technologies or devices able to detect and trace contents even in their analogue form.<sup>120</sup>

---

## 5. Controversy within the Country

- (1) Arguments against restrictions concerning technological measures to protect contents made within the country. Additionally, what arguments have been made in relation to information access rights and the right to know?

To our knowledge, the main controversies and reaction in respect to technological measures have appeared at the national level rather than at the EU-level.

### *(a) France*

In France the controversy surrounding technological measures focused on the need to ensure interoperability. Prior to 2009, most distributors of musical content were selling music protected by technological measures preventing customers from playing the music files they legally purchased on different devices, while unlawfully downloaded content was often fully interoperable. For example music bought on Apple's iTunes Store could only be read using an Apple device. This prompted strong reactions from consumer groups, which claimed that technological measures in fact encouraged unlawful downloading. As a result, the 2006 law implementing the Information Society Directive into French law included numerous

---

<sup>119</sup> Study on the Implementation of the Information Society Directive, pp. 95-101; Marcella Favale, pp. 4 -6.

<sup>120</sup> "Plan France Numérique 2012", in ARMT, *Rapport Annuel 2008*

provisions ensuring that interoperability would not be hampered by technological measures.

*(b) The UK*

The use of, and rationale for, digital right management have both been heavily contested and criticized in the UK.

Legislation and regulation:

Consumer respondents to the UK APIG Digital Rights Management inquiry felt that UK legislation and policy was developed by bureaucrats with little understanding of the issues involved and biased towards the concerns of businesses. They felt that legislation in this area originated with trade-related Directives that made inadequate provision for consumer interests. The APIG called for a UK Stakeholders' Group to consult on these issues – possibly to be headed by the British Library – to obtain wider-ranging views.<sup>121</sup> Lord Carter's "Digital Britain" report of 2009 recently suggested a similar function for the UK "Rights Agency".<sup>122</sup>

The relevant UK legislation has also been criticised for protecting technological measures that not only stop copyright infringement, but also restrict legitimate activities (for example, scientific research) and impede competition. Critics noted that, whilst it discussed many issues surrounding the use of digital right management, the recent "Digital Britain" Report was out-of-date and biased and failed to take proper account of consumers' points of view.<sup>123</sup>

Interoperability and competition:

The UK National Consumer Council has expressed the view that interoperability issues with digital right management are so severe (and that they are so poorly understood by consumers) that they risk infringing the provisions of general law on consumer rights and information requirements.<sup>124</sup> Other consumer groups claim that, in making content unavailable through non-proprietary programs and devices, technological measures restrict third-party program access, devalue the material for consumers and stifle innovation.<sup>125</sup> Respondents were divided over the

---

<sup>121</sup> APIG Digital Rights Management Report, pp. 20-21.

<sup>122</sup> APIG Digital Rights Management Report, p. 21. BIS et al. "Copyright in a Digital World: What Role for a Digital Rights Agency?", p. 5. It now appears that Ofcom will fulfil the functions envisaged for the "Digital Rights Agency".

<sup>123</sup> Cf. C. Doctorow, "Digital Britain report: Why Lord Carter should get real", The Guardian (10 February 2009); accessed at <http://www.guardian.co.uk>.

<sup>124</sup> For example. the UK Trade Descriptions Act 1968 prohibits traders from putting misleading information on their goods. It has been suggested by consumer rights agencies in the UK that consumers should be informed of the restrictions which digital rights management technology apply to digital media through the use of labeling.

<sup>125</sup> House of Commons Culture, Media and Sport Committee review, "New Media and the Creative Industries" (fifth report of 2006-7 session), pp. 56-7.

question of the effectiveness of Government intervention; the APIG was generally fearful of over-regulation.<sup>126</sup>

Some UK commentators argue that digital right management are being used in a “turf war” between major industry players to prevent interoperability with competitors’ products and to maintain restrictive business models and market control rather than to prevent copyright infringement.<sup>127</sup> The APIG noted a potential competition issue in relation to regional variations in pricing on iTunes, which it considered to be at odds with the single market.<sup>128</sup> UK prices were around 10% higher than in the rest of the Eurozone. Regional-control and copy-control technological measures and regional licensing agreements restricting the use of downloaded content prevented arbitrage or consumer substitution and the UK consumer protection organisation Which? filed a formal complaint. In January 2008, the European Commission announced that Apple would be reducing prices in the UK following a reference by the UK competition authorities in 2004. Competition Commissioner Neelie Kroes described the pricing as incompatible with “a truly Single Market for music downloads”.<sup>129</sup>

#### UK consumer interest groups:

Libraries and archives within the UK use rights management information to track their catalogues, to watermark electronic deliveries of their materials and to assist them in meeting their obligations to both publishers and consumers. However, library representatives have stated that technological measures can cause issues and often prevent libraries from benefiting from the broad statutory exemptions available to them. The British Library has advocated a “Digital is not different” approach among digital right management designers to address the many concerns raised by libraries.

Some technological measures restrict access to materials used by library visitors with disabilities, particularly among those with audio and visual impairments. Representatives of consumer groups for the disabled note the insufficient recognition among technological measures designers of the fact that protected content (especially E-books) would be unable to interact with specialist hardware and software used by many disabled consumers to convert content into a format accessible to them.<sup>130</sup> The APIG called for “much wider-ranging exemption[s]” for genuine academic research, for people with audio or visual disabilities and for libraries.<sup>131</sup>

---

<sup>126</sup> APIG Digital Rights Management Report, pp. 9 and 18.

<sup>127</sup> Cf. T. Anderson, “How Apple is Changing DRM”, *The Guardian* (15 May 2008), accessed on 18 October 2009 at <http://www.guardian.co.uk/technology/2008/may/15/drm.apple>.

<sup>128</sup> APIG Digital Rights Management Report, pp. 18-19.

<sup>129</sup> “European Commission welcomes Apple’s announcement to equalise prices for music downloads from iTunes in Europe”, Press Release IP/08/22 of 1/9/08; accessed at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/22&type=HTML&aged=0&language=EN&guiLanguage=en> on 20 October 2009.

<sup>130</sup> APIG Digital Rights Management Report, pp. 12-14.

<sup>131</sup> APIG Digital Rights Management Report, pp. 10-11.

Other controversy:

The UK Government rejected an online petition in February 2007, which was signed by 1,414 people and hosted on the UK Government's e-petition website, calling for digital right management to be banned in the UK. The Open Rights Group "(a consumer rights organization) commented that the petition indicated a growing awareness among UK consumers of digital right management and associated issues.<sup>132</sup>

The proposal for a national ID card has also prompted discussion of technological measures, especially among the UK press. There is concern that insufficient protection might enable criminal persons to alter, falsify or "steal" privileged and highly confidential information.

*(c) Germany*

The German Pirate Party was founded on September 10<sup>th</sup>, 2006 in Germany. The party opposes the dismantlement of civil rights in telephony and on the Internet, in particular the European data retention policies and Germany's new Internet law entitled "Access Impediment Act".<sup>133</sup> The party opposes copy protection measures since they would shorten the availability of artistic works in an artificial way. Furthermore they would also interfere with the legitimate use of the works and cause an uncontrollability and surveillance of its users. The party promotes the general availability and use of digital works in order to improve information, knowledge and culture because they would form an essential basement for our modern society. They claim that the current restrictions on circumvention of technological measures to protect contents would criminalize a whole generation since children and teenagers would usually only use technological measures in a natural way without any criminal intent.

- 
- (2) Status of request from industries against restrictions concerning technological measures to protect contents. (Are they satisfied with the current provisions mentioned above or would they prefer more or less restrictive provisions? This may vary depending on the industry. Can be analyzed according to each industry area.)

*(a) France*

*(i) Music industry*

In 2006 during the preparation of the law implementing the Information Society Directive, Apple announced that they were considering leaving the French market because the proposed new provisions concerning interoperability and technological measures would hinder or even kill online

---

<sup>132</sup> Source: CNET News.com, accessed on 18 October 2009 at [http://news.cnet.com/2100-1028\\_3-6160760.html](http://news.cnet.com/2100-1028_3-6160760.html).

<sup>133</sup> Source: <http://www.piratenpartei.de/>.

music distribution.<sup>134</sup> Eventually, Apple softened its position because the law created an administrative agency (formerly known as the “ARMT” now the HADOPI) which mission was to assess the balance between work protection and lawful use, in particular with regard to interoperability.

Contrary to Apple, several players and commentators in the field (including the ARMT) considered that non-interoperable files constituted the most serious obstacle to the development of a lawful offer capable of competing with peer-to-peer networks. Music industry majors eventually rallied this position and stopped using technological measures hindering interoperability, starting with EMI in 2007, followed by Warner Music in March 2008, and Universal Music and Sony BMG in September 2008. Apple finally renounced using non-interoperable files in January 2009. These decisions are in compliance with the “Olivennes Agreements” signed in November 2007 by most players in the music industry in France, whereby they agreed to remove technological measures preventing interoperability from their French online music catalogue. Article 25 of the law of 12 June 2009 creating the HADOPI enshrined this obligation.

The music industry was said to have realized that technological measures were not an efficient solution to fight piracy since they only penalized lawful consumers. However, after conducting several hearings on this issue, the ARMT moderated this view, considering that technological measures should not be abandoned altogether, but in a phase of evolution toward a more efficient, interoperable, transparent and flexible digital right management.<sup>135</sup>

#### *(ii) Film industry*

The situation is sharply different in the film industry, particularly because the DVD standard included, since its inception, a technological measure and was broadly used, therefore limiting the risks of incompatibility. The development of an online and “on demand” film offer by several industry players could nevertheless raise interoperability issues.

Technological measures and rights management information also help ensure that the period of time to be observed between a film being shown in movie theatres for the first time and its exploitation on various media (rules on the so-called “chronology of media”) is respected, as those techniques are used to secure the distribution of movies in hard copies and digital “on demand” format.

#### *(iii) Book industry*

Digital books (E-books) have become more widespread starting in 2008. The threat of copyright infringement has lead distributors to resort to technological measures. Due to a lack of dialogue among actors in the industry, several interoperability issues were raised. A report on digital books was delivered to the Ministry of Culture and Communication,

---

<sup>134</sup> Apple’s French spokesperson even asserted that the French law implementing the Information Society Directive in fact sponsored piracy.

<sup>135</sup> ARMT report 2008, p.24.

emphasizing this lack of collaboration between the different actors. A working group is actually in charge of this issue.

*(iv) Videogame industry*

Videogame distributors have been using technological measures for a long time. They primarily use copy control mechanisms for hard copies and access control mechanisms for online games. Even if these technological measures are often restrictive and hinder interoperability, most consumers seem to have accepted them as necessary.

*(b) The UK*

There are many UK industry forums, lobbying groups, organisations and consultancies that regularly contribute to discussion in the UK, including:<sup>136</sup>

- The UK Alliance Against IP Theft, a major forum and representative of many trade and enforcement organizations, many of whom also lobby independently on specific issues;<sup>137</sup>
- British Music Rights, which represents the UK commercial music industry;
- The Producers Alliance for Cinema and Television (PACT), which represents the independent UK visual media industry; and
- The UK Film Council, which is a non-departmental public body concerned with the regulation and support of the British film industry.

UK industry representatives and lobbying groups have been extremely supportive of digital right management technologies. However, mounting criticism, especially in the audio and music sector, has led to a growing awareness among industry commentators of the need to use more sophisticated digital right management techniques that do not reduce user-convenience and interoperability.

APIG Digital Rights Management Report (June 2006)

The All Parliamentary Internet Group invited submissions from stakeholders on a range of issues relating to digital right management:<sup>138</sup>

---

<sup>136</sup> An extensive list appears in the preamble to the APIG Digital Rights Management Report, p. 2.

<sup>137</sup> The Alliance's members include: Anti-Copying in Design (ACID), the Anti-Counterfeiting Group (ACG), the Authors Licensing and Collecting Society (ALCS), the British Brands Group, the British Recorded Music Industry Limited (BPI), the British Video Association (BVA), the British Software Alliance (BSA), the Cinema Exhibitors Association (CEA), the Design and Artists Copyright Society (DACS), the Entertainment and Leisure Software Publishers Association (ELSPA), the Entertainment Retailers Association, the Federation Against Copyright Theft (FACT) and the Federation Against Software Theft (FAST), the Film Distributors Association (FDA), the Motion Picture Association (which is the international voice of the US film industry), the Premier League, the Publishers Licensing Society (PLS) and the Video Standards Council (VSC).



- Industry submissions recognised that a strong legal framework was required; the CDPA was acknowledged as providing extensive and adequate protection. However, industry submissions indicate that small-scale civil infringements will seldom be pursued, despite the fact that the aggregate cost to the industry each year is relatively high.<sup>139</sup>
- Rightscom, a European consultancy specializing in IP issues, suggested that technological measures prevent consumers from committing illegal act and support legal boundaries without really inhibiting “permitted uses” of material. Consumer respondents did not share this view. The Report indicated that technological measures are increasingly common in the distribution of media by intermediary parties (i.e., not just the rightholder).<sup>140</sup>
- In the music industry, many record companies using technological measures were starting in 2006 to allow some copies to be made (for “fair use”) but there was concern that this was a marketing device and did not represent genuine change among digital right management-users.<sup>141</sup> Many “independent” content providers in the UK have taken the view that allowing copying assists their business. Some independent music labels and distributors stated that their own technological measures were restricted by the dominance of certain digital right management systems. The Association for Independent Music (“AIM”) stated their belief that the “loss of some measure of copyright control” is a prerequisite “factor in reaching new and enthusiastic music markets around the world”. AIM (and the APIG) noted that the commercial success enjoyed by the Arctic Monkeys in the UK owed a great deal to the development of their media profile via file-sharing and non-restricted websites.<sup>142</sup> Since the APIG report, the music industry has increasingly moved away from applying digital right management to downloadable music.
- The British film and visual media industry indicated that they see technological measures as continuing to play a vital role in the protection and monetisation of rights in visual media. PACT have stated that they see technological measures as essential to the distribution and marketing of legal content on the Internet. Other representatives of the UK visual media industry also suggested that effective use of technological

---

<sup>138</sup> The APIG is a “discussion group between new media industries and Parliamentarians”. Issues on which APIG invited submissions included: the so-called “copyright trade off”; the extent to which the law should protect digital right management systems and new forms of content sharing licences; the problems faced by libraries, the disabled and consumers (with focus on interoperability and competition issues); the consequences of digital right management systems on functionality; and the role of the UK Parliament generally. A summary of the report’s findings and recommendations appears on page 22 of the report.

<sup>139</sup> APIG Digital Rights Management Report, p. 6.

<sup>140</sup> APIG Digital Rights Management Report, pp. 7-9.

<sup>141</sup> For example, in 2004 an Apple “upgrade” for iTunes actually reduced the number of permitted copies from 10 to 7. APIG Digital Rights Management Report, p. 14.

<sup>142</sup> APIG Digital Rights Management Report, p. 6.

measures might signal the end of the staggered “time-window” effect in distribution.<sup>143</sup>

- Consumers in the UK were stated to be extremely ignorant of the actual application of copyright law. EMI and Intel stated that consumers “should be aware” of what they are buying. The APIG report concludes that there is a need for effective labelling on products to inform consumers and made a recommendation to the Office of Fair Trading (“OFT”) in this regard.<sup>144</sup>

#### The Gowers Review of Intellectual Property (December 2006)

The Gowers Review observed three major issues with the current state of digital right management:

- technological measures can enable content providers to go beyond protecting content and legal rights and to protect business models which may be anti-competitive or otherwise illegal;
- digital right management can prevent uses permitted under fair dealing exceptions and digital right management do not necessarily expire when copyright expires; and
- digital right management can damage users’ computers or cause operability issues.

Furthermore, the Review made two recommendations for future policy-making:

- It should be made easier for users to file notice of a complaint under Section 296ZE (“Protection of Permitted Acts”); and
- UK regulators should investigate the possibility of introducing consumer labelling to provide more guidance to consumers without imposing unnecessary regulatory burdens.<sup>145</sup>

#### “New Media and the Creative Industries” Report, UK Culture, Media and Sport Committee (2007)<sup>146</sup>

The Review indicated that industry representatives were supportive of digital right management.<sup>147</sup> The Review recognised the extensive findings of the APIG Report and made several criticisms of digital right management usage:

---

<sup>143</sup> APIG Digital Rights Management Report, pp. 6-7.

<sup>144</sup> APIG Digital Rights Management Report, pp. 15-16.

<sup>145</sup> The Gowers Review, pp. 72-74.

<sup>146</sup> Fifth Report of the 2006-7 Session of the UK House of Commons’ Culture, Media and Sport Committee: “New Media and the Creative Industries” (2007)

<sup>147</sup> The British Screen Advisory Council advised that it saw technological measures, and copy control in particular, as integral to the British film industry. The Business Software Alliance predicted that if digital right management tools were more effectively used to prevent P2P file sharing, the value of the online music market would increase from £46.8

- digital right management have damaged consumer trust and “have sometimes provided a very poor deal for consumers”; and
- digital right management should not be allowed to operate in defiance of exemptions for unlicensed copying enshrined in UK copyright law.

However, the Review concluded that:

- Regulation is premature as technology is still in development;
- Many record companies were voluntarily making digital right management-free content available to consumers;
- digital right management systems have value in fighting piracy and assist in the protection of creative content;
- It should be left to companies to decide the extent to which they wish to impose restrictions on the use of their products; and
- digital right management should be applied carefully to avoid dissuading consumers from accessing and supporting legitimate markets.

#### Industry support for legislation

On 27<sup>th</sup> October 2009, Jean-Bernard Levy, the CEO of Vivendi (which owns Universal Music and one of France’s largest ISPs) announced at the UK Creativity and Business International Network Conference that the UK Government must implement a “three-strikes” policy to cut off persistent Internet infringers. Levy argued that ISPs should support legislation to curb illegal use of bandwidth, to increase creativity and monetization.<sup>148</sup>

#### *(c) Germany*

The CEO of the “Börsenverein des Deutschen Buchhandels”, an association of German publishers, recently criticized the actions of the German Attorney General regarding criminal proceedings initiated against copyright infringements<sup>149</sup>. He supports the idea of e-mails with a warning sent to users that commit copyright infringements. Furthermore he is of the opinion that an international copyright organization has to put more and quicker effort into taking actions against illegal downloading abroad. However, he spoke in favour of the newly created right of disclosure according to Article 101 of the German Copyright Act. Nevertheless he also pointed out that filing such a suit is very expensive. Furthermore it would not support a company’s image to pursue a claim against their own

---

million in 2005 to £134.6 million in 2007 and £194.5 million in 2008. Other industry respondents were similarly supportive.

<sup>148</sup> M. Sweney, “Vivendi head calls for ‘three-strikes’ rule to tackle UK filesharers”, The Guardian (27 October 2009); accessed at <http://www.guardian.co.uk/media/2009/oct/27.htm>.

<sup>149</sup> Source: <http://www.heise.de/ct/meldung/Buchhandel-wirft-Politikern-Versagen-beim-Urheberrechtsschutz-vor-215227.html>.

customers. He believes that digital watermarking would be a good way in order to track people who have violated against copyright preventions.

He has a skeptical view towards a “culture flatrate”, which was suggested by the Green Party. They wanted to set up a flat rate for copy-protected works. He argues that there would be a large number of people who were not interested in downloading music or books but preferred to buy them in stores. Also, this would eliminate business concepts like iTunes.

- 
- (3) Whether there are trends in amendments to laws. If so, what are the trends?

*(a) France*

France has promulgated new legislation entitled “Law concerning dissemination of works and the protection of rights on Internet” (also known as the “HADOPI laws”) in June and October 2009. Therefore no trends in amendments are yet to be noted. The HADOPI laws were drafted to encompass future technological evolutions. For instance, it introduced Article L. 331-26 in the IPC, which provides for the publication of an up-to-date list of relevant functional specifications regarding securization methods and a list of labelled means of securization. Similarly, it created Article L. 331-23 of the IPC, pursuant to which the HADOPI will indicate, in its annual report, the main evolutions regarding technological measure and rights management information, and provide an evaluation of the efficiency of such measures. Furthermore, the new Article L331-13 of the IPC will enable the HADOPI to recommend amendments to the law.

However some commentators have emphasized the weakness of the new laws in light of the evolution of consumer’s behaviour. Those authors point out that HADOPI will focus its activity on illegal downloading of contents; however, recent studies seems to show that peer-to-peer is declining while streaming is increasingly used. This development will de-emphasize rights to control copies of a work and accentuate the importance of rights of access. Nevertheless, the HADOPI laws tend to be centred on copy control, to the detriment of access control. This technological change has not yet been reflected in French copyright law.

*(b) The UK*

In the APIG Digital Rights Management Report 2006:

- None of the industry representative groups invited to make submissions to the felt that the provisions of UK law were in any way inadequate.
- Conversely, consumer respondents to the APIG inquiry suggested that the provisions on exemptions (especially the complaints procedure pursuant to Section 296ZE (“Protection of Permitted Acts”)) are inadequate. The UK process has been criticised as slow compared to other countries. Complaints to the Secretary of State have been described as “without

teeth” and criticised as expensive and time-consuming. The APIG noted that the procedure has yet to be used in the UK.

- Many participants felt that legislation would become increasingly irrelevant, as technological measures become more sophisticated and harder to overcome and public policy is less required to take account of the inevitability of widespread circumvention. Industry commentators noted the cost and length of time involved in successfully enforcing rights or prosecuting individuals. APIG’s report suggested that further legislation on the issue of digital right management might not play a significant role.<sup>150</sup>

The “Digital Britain” Report of 2009, however, called for legislation to reduce the significant proportion of users who access digital content through unlawful channels, via file-sharing and P2P:<sup>151</sup>

- The major policy target of the Report was the reduction of unlawful file-sharing by UK users by 70-80%.<sup>152</sup>
- The Report did not directly address the issue of digital right management. However, the UK Government is supportive of industry perspectives and views technological measures to protect contents as valuable tools in restricting infringement of copyright protection. The chief concern of the Report was to promote standardisation and interoperability in digital right management. The Report called for “Digital Test Beds” to be used to test new technologies, including digital right management technologies, alongside developers.<sup>153</sup>
- The Report envisaged a “Digital Rights Agency” in the UK to encourage consumers to prefer “free, easy and legal” content to unlawful content. The Agency would: increase public awareness of copyright law, digital right management and digital technology issues; resolve disputes and address consumer complaint; and regulate a Code of Practice among industry players (and particularly ISPs) regarding infringement.<sup>154</sup>
- Finally, the Report initiated legislative measures (involving Ofcom or a “Digital Rights Agency”) by which ISPs would co-operate in the warning

---

<sup>150</sup> APIG Digital Rights Management Report, pp. 6, 10-11.

<sup>151</sup> The report estimated that P2P file-sharing cost the UK music industry £180 million in 2008 and that the cost for the UK TV and film industry was £152 million in 2007. The report did not cite accurate figures for other industries but it noted that every industry sector was reporting significant losses.

<sup>152</sup> “Digital Britain” Final Report (2009), p. 110. However, it was emphasised that the biggest users of unlawful material are also the biggest users of paid-for content.

<sup>153</sup> “Digital Britain” Final Report (2009), p. 124 ff.

<sup>154</sup> Cf. BIS et al., “What Role for a Digital Rights Agency?”, p. 5; accessed at <http://www.ipso.gov.uk/digitalbritain.pdf>.

and investigation of repeat infringers of copyright or publishers of circumvention technology or circumvented content.<sup>155</sup>

In a speech of 28 October 2009, the UK Business Secretary (Lord Mandelson) stated that the legislation is intended to come into force in April 2010.<sup>156</sup> Under the proposed Digital Economy Bill:

- Ofcom will draw up a Code of Practice to implement the process and also set up a body to hear legal Appeals;
- Rightholders will “phish” to identify the IP addresses of persistent infringers and notify the relevant ISP;
- A notified ISP will send a First Warning to the alleged infringer explaining that further infringement may result in legal action;
- If subsequent Warnings are ignored, the rights-holder may obtain a court order to review the list of offenders and to enable it to take legal action.

If a 70% reduction in illegal file sharing is not achieved within 12 months, then “technical measures” (i.e., restricting Internet connections) may be implemented under a Revised Code of Practice, again regulated by Ofcom. Under the “technical measures” regime:

- Repeat infringement would lead to inclusion on a Serious Infringer List and result in technical measures (the ISP would be obliged to implement such measures);
- The alleged infringer would have 20 working days to appeal, during which time technical measures would be suspended;
- Further appeal will be possible to a Tribunal within 30 working days of an unsuccessful appeal, during which time technical measures would remain suspended; and
- After appeals, technical measures would remain in place or be withdrawn.

The Digital Economy Bill had its first reading in the House of Lords on 19 November 2009. The Bill implements many aspects of the Digital Britain report which require primary legislation, although it is doubtful whether there will be sufficient legislative time for it to be passed before the general election due next year. However, the Conservative Party has confirmed its general support for the proposals. The Bill is unusual in that it proposes measures relating to online infringement of copyright, public-service broadcasting and content, network infrastructure and digital safety in one piece of legislation. While many copyright owners will welcome the

---

<sup>155</sup> “Digital Britain” Final Report (2009), pp. 113-4. The Report also discussed proposals to introduce levied fees to be integrated into the cost of copying technology, to charge consumers for the privilege of being able to copy and “re-use” content.

<sup>156</sup> M. Sweney, “Lord Mandelson sets date for blocking filesharers’ internet connections”, *The Guardian* (28th October 2009); accessed at <http://www.guardian.co.uk>. It appears that ISPs and rights-holders will pay a flat fee to bear the costs of the “Digital Britain” legislation and strategy.

obligations to be imposed on ISPs aimed at reducing illegal file-sharing, such as the potential suspension of an infringer's internet connection, there has been criticism that the sanctions available to rights-owners are draconian and loosely drafted. There is also concern at the power reserved to the Secretary of State to amend copyright law by secondary legislation with minimal parliamentary scrutiny.

In an open letter to the UK Secretary of State for Business, Innovation and Skills, Facebook, Google, Yahoo! and eBay have recommended the removal of clause 17 from the draft "Digital Economy" Bill. Clause 17 gives the Secretary of State the authority to amend the CDPA for the purpose of preventing or reducing online copyright infringement, if it is appropriate to do so because of technological developments. These Internet companies believe that the provision is too broad and would give the Secretary of State unprecedented powers, which might put legitimate use of current technology at risk and discourage future innovation. The Bill had its second reading in the House of Lords on 2nd December 2009 and is due to enter the committee stage on 6th January 2010.

More generally, a UK Copyright Strategy Review commenced in 2008. In 2009, the UK Intellectual Property Office ("UK IPO") and the Department for Business, Innovation & Skills ("BIS") published a joint position report summarizing the progress of the Review. The report indicates that the UK Government supports legislation at the EU and national level to modernize the general law on copyright; however, this report did not consider digital right management specifically.

The UK IPO was also awarded an Excellence Award by the British Recorded Music Industry (BPI) on 21 October 2009 for its continued assistance via the IPO Intelligence Hub in battling music piracy. The Hub has assisted the BPI and enforcement agencies in over 130 investigations in 2009. 2009 has apparently seen an increase in the number of arrests, including of an organised group of pirates operating in the North-West of England.<sup>157</sup> This trend suggests that the extent of scrutiny and prosecution of infringers and circumvention by UK regulatory bodies may be increasing.

*(c) Germany*

In Germany the "Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums" came into effect on 1 September 2008 in order to implement the European Directive 2004/48/EG (so-called Enforcement Directive) into national law.

End

---

<sup>157</sup> Source: UK IPO, accessed on 21 October 2009 at <http://www.ipo.gov.uk/press-release-20091021>.

Annex 1  
FTAs/EPAs

I. Relevant provisions of the European Directives

A. Computer Programs Directive<sup>158</sup>

Article 5 - Exceptions to the restricted acts

1. In the absence of specific contractual provisions, the acts referred to in points (a) and (b) of Article 4(1) shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.
2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract in so far as it is necessary for that use.
3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

Article 6 – Decompilation

1. The authorisation of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of points (a) and (b) of Article 4(1) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:
  - (a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so;
  - (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and
  - (c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.
2. The provisions of paragraph 1 shall not permit the information obtained through its application:
  - (a) to be used for goals other than to achieve the interoperability of the independently created computer program;
  - (b) to be given to others, except when necessary for the interoperability of the independently created computer program; or
  - (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which

---

<sup>158</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:01:EN:HTML>



infringes copyright.

3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with a normal exploitation of the computer program.

1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

- (a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to do so;
- (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with a normal exploitation of the computer program.

#### Article 7- Special measures of protection

1. Without prejudice to the provisions of Articles 4, 5 and 6, Member States shall provide, in accordance with their national legislation, appropriate remedies against a person committing any of the following acts:

- (a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
- (b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
- (c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

2. Any infringing copy of a computer program shall be liable to seizure in accordance with the legislation of the Member State concerned.
3. Member States may provide for the seizure of any means referred to in point (c) of paragraph 1.
  - o Database Directive<sup>159</sup>

#### Article 1 - Scope

1. This Directive concerns the legal protection of databases in any form.
2. For the purposes of this Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
3. Protection under this Directive shall not apply to computer programs used in the making or operation of databases accessible by electronic means.

#### Article 7 - Object of protection

1. Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.
2. For the purposes of this Chapter:
  - (a) "extraction" shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;
  - (b) "re-utilization" shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community;

Public lending is not an act of extraction or re-utilization.

3. The right referred to in paragraph 1 may be transferred, assigned or granted under contractual licence.
4. The right provided for in paragraph 1 shall apply irrespective of the eligibility of that database for protection by copyright or by other rights. Moreover, it shall apply irrespective of eligibility of the contents of that database for protection by copyright or by other rights. Protection of databases under the right provided for in paragraph 1 shall be without prejudice to rights existing in respect of their contents.
5. The repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal

---

<sup>159</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML>

exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted.

#### Article 10 - Term of protection

1. The right provided for in Article 7 shall run from the date of completion of the making of the database. It shall expire fifteen years from the first of January of the year following the date of completion.

2. In the case of a database which is made available to the public in whatever manner before expiry of the period provided for in paragraph 1, the term of protection by that right shall expire fifteen years from the first of January of the year following the date when the database was first made available to the public.

3. Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection.

- o Conditional Access Directive<sup>160</sup>

#### Article 2 - Definitions

For the purposes of this Directive:

- (a) protected service shall mean any of the following services, where provided against remuneration and on the basis of conditional access:
  - television broadcasting, as defined in Article 1(a) of Directive 89/552/EEC,
  - radio broadcasting, meaning any transmission by wire or over the air, including by satellite, of radio programmes intended for reception by the public,
  - information society services within the meaning of Article 1(2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services (7),or the provision of conditional access to the above services considered as a service in its own right;
- (b) conditional access shall mean any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior individual authorisation;
- (c) conditional access device shall mean any equipment or software designed or adapted to give access to a protected service in an intelligible form;

---

<sup>160</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0084:EN:HTML>

- (d) associated service shall mean the installation, maintenance or replacement of conditional access devices, as well as the provision of commercial communication services in relation to them or to protected services;
- (e) illicit device shall mean any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorisation of the service provider;
- (f) field coordinated by this Directive shall mean any provision relating to the infringing activities specified in Article 4.

#### Article 3 - Internal market principles

1. Each Member State shall take the measures necessary to prohibit on its territory the activities listed in Article 4, and to provide for the sanctions and remedies laid down in Article 5.
2. Without prejudice to paragraph 1, Member States may not:
  - (a) restrict the provision of protected services, or associated services, which originate in another Member State; or
  - (b) restrict the free movement of conditional access devices;

for reasons falling within the field coordinated by this Directive.

#### Article 4 - Infringing activities

Member States shall prohibit on their territory all of the following activities:

- (a) the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices;
- (b) the installation, maintenance or replacement for commercial purposes of an illicit device;
- (c) the use of commercial communications to promote illicit devices.

- o Information Society Directive<sup>161</sup>

#### Recital 47

Technological development will allow rightholders to make use of technological measures designed to prevent or restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases. The danger, however, exists that illegal activities might be carried out in order to enable or facilitate the circumvention of the technical protection provided by these measures. In order to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, there is a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.

---

<sup>161</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML>

#### Recital 48

Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightholders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development. Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography.

#### Recital 50

Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs.

#### Article 5 - Exceptions and limitations

1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:

- (a) a transmission in a network between third parties by an intermediary, or
- (b) a lawful use

of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

- (a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation;
- (b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;

- (c) in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage;
- (d) in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the grounds of their exceptional documentary character, be permitted;
- (e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.

3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:

- (a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;
- (b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;
- (c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source, including the author's name, is indicated, unless this turns out to be impossible;
- (d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;
- (e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;
- (f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this turns out to be impossible;
- (g) use during religious celebrations or official celebrations organised by a public authority;
- (h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;
- (i) incidental inclusion of a work or other subject-matter in other material;

- (j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;
- (k) for the purpose of caricature, parody or pastiche;
- (l) use in connection with the demonstration or repair of equipment;
- (m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;
- (n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;
- (o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

4. Where the Member States may provide for an exception or limitation to the right of reproduction pursuant to paragraphs 2 and 3, they may provide similarly for an exception or limitation to the right of distribution as referred to in Article 4 to the extent justified by the purpose of the authorised act of reproduction.

5. The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.

#### Article 6 - Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

- (a) are promoted, advertised or marketed for the purpose of circumvention of, or
- (b) have only a limited commercially significant purpose or use other than to circumvent, or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,

any effective technological measures.

3. For the purposes of this Directive, the expression “technological measures” means any technology, device or component that, in the normal course of its

operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed “effective” where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply *mutatis mutandis*.

#### Article 7 - Obligations concerning rights-management information

1. Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts:

- (a) the removal or alteration of any electronic rights-management information;
- (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority,

if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or



any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive 96/9/EC.

2. For the purposes of this Directive, the expression “rights-management information” means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC.

#### Article 8 - Sanctions and remedies

1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

– Relevant provisions of the pending EC-Korea EPA<sup>162</sup>

Note: the following sets forth the text after the completion of negotiations and is not binding as a matter of international law. The authentic text will be published in the Official Journal of the European Union upon the completion of the necessary ratification procedures.

#### Article 10.12 - Protection of technological measures

1. Each Party shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that such person is pursuing that objective.

2. Each Party shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes, of devices, products or components, or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of;

---

<sup>162</sup> [http://trade.ec.europa.eu/doclib/docs/2009/october/tradoc\\_145180.pdf](http://trade.ec.europa.eu/doclib/docs/2009/october/tradoc_145180.pdf)

- (b) have only a limited commercially significant purpose or use other than to circumvent; or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of,

any effective technological measures.

3. For the purposes of this Agreement, **technological measure** means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by each Party's legislation. Technological measures shall be deemed effective where the use of a protected work or other subject matter is controlled by the right holders through the application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject matter, or a copy control mechanism, which achieves the objective of protection.

4. Each Party may provide for exceptions and limitations to measures implementing paragraphs 1 and 2 in accordance with its legislation and the relevant international agreements referred to in Article 10.5.

#### Article 10.13 - Protection of rights management information

1. Each Party shall provide adequate legal protection against any person knowingly performing without authority any of the following acts:

- (a) the removal or alteration of any electronic rights management information; or
- (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject matter protected under this Agreement from which electronic rights management information has been removed or altered without authority,

if such person knows, or has reasonable grounds to know, that by doing so it is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by the law of the relevant Party.

2. For the purposes of this Agreement, rights management information means any information provided by right holders which identifies the work or other subject matter referred to in this Agreement, the author or any other right holder, or information about the terms and conditions of use of the work or other subject matter, and any numbers or codes that represent such information.

3. Paragraph 2 shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject matter referred to in this Agreement.

## Annex 2 French Law

Note: the following sets forth the relevant provisions of the French Intellectual Property Code (“IPC”) as will be in force as of 1 January 2010.

- General provisions
- Technological measures

### Article L. 331-5 of the IPC<sup>163</sup>

The effective technological measures designed to prevent or limit uses not authorized by the rightholder of any copyright or any related right, in respect of a work, other than a computer program, a performance, a sound recording, a video recording or a broadcast, are protected as provided herein.

Technological measure within the meaning of the first paragraph refers to any technology, device or component that, when used as intended, achieves the function provided for in this paragraph. These technological measures are deemed to be effective when a use under the same paragraph is controlled by the rightholders through the application of an access code, a protection process such as encryption, scrambling or any other transformation of the protected subject or by a copy control mechanism that achieves such protection goal.

A protocol, a format, or an encryption, scrambling or transformation method do not in and of themselves constitute a technological measure within the meaning of this article.

Technological measures should not prevent the effective implementation of interoperability, while respecting copyright. The suppliers of technological measures provide access to information that is essential to interoperability in accordance with the provisions of 1° of article L. 331-31 and of L. 331-32.

The provisions of this chapter do not undermine the legal protection provided by articles 79-1 to 79-6 and article 95 of law no. 86-1067 of September 30, 1986 relative to the freedom of communication.

Technological measures cannot prevent the lawful use of the work or the protected subject within the limits of the rights provided for by this code, as well as those granted by the rightholders.

The provisions of this article apply without prejudice to the provisions of article L.122-6-1 of this code.

---

<sup>163</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212283&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=1338322279&oldAction=rechCodeArticle>

Article L. 331-6 of the IPC<sup>164</sup>

The benefit of the private copying exception and the exceptions mentioned in 2° of article L. 331-31 is guaranteed by the provisions of articles L. 331-7 to L. 331-10, L. 331-33 to L. 331-35 and L. 331-37.

Article L. 331-7 of the IPC<sup>165</sup>

The rightholders who use the technological measures defined in article L. 331-5 may use them to limit the number of copies. However they shall take all useful measures to ensure that their implementation does not compromise the rights of the beneficiaries of the exceptions mentioned in 2° of article L. 331-31 of their effective exercise. They shall use their best efforts to determine these measures together with the certified consumers' associations and the other interested parties.

The provisions of this article may, to the extent allowed by the technology, subordinate the effective benefit of these exceptions to lawful access to a work or a sound recording, a video recording or a broadcast and ensure that they do not undermine its normal use nor cause any unfair damage to the legitimate interests of the rightholders with respect to the work or the protected subject.

Article L. 331-8 of the IPC<sup>166</sup>

The rightholders are not, however, required to use the provisions of L. 331-7 when the work or another subject protected by a related right is made available to the public in accordance with the contractual provisions agreed to among the parties, so that each may have access to it from the location and at the time that they choose.

Article L. 331-9 of the IPC<sup>167</sup>

The editors and distributors of television services cannot use technological measures that would deprive the public of the benefit of the private copying exception, including on a digital medium and format, as provided in 2° of article L.122-5 and 2° of article L.211-3.

The *Conseil Supérieur de l'Audiovisuel* [the "High council for audiovisual matters"] ensures compliance with the obligations of the first paragraph as provided in articles 42 and 48-1 of law no. 86-1067 of September 30, 1986 relating to the freedom of communication.

---

<sup>164</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000021212278&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000021212278&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

<sup>165</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000021212290&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000021212290&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

<sup>166</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000020740181&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000020740181&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

<sup>167</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000020740176&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000020740176&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

Article L. 331-10 of the IPC<sup>168</sup>

The terms of access to the reading of a work, a video recording, a broadcast or a sound recording and the limitations likely to be made to the private copying exception mentioned in 2° of article L.122-5 and in 2° of article L. 211-3 by the implementation of a technological protection measure must be brought to the attention of the user.

o Rights management information

Article L. 331-11 of the IPC<sup>169</sup>

Information in electronic format concerning the regime of rights relating to a work, other than a computer program, a performance, a sound recording, a video recording or a broadcast, are protected as provided herein, when one of the items of information, numbers or codes is attached to the reproduction or appears in relation to the communication to the public of the work, the performance, the sound recording, the video recording or the broadcast to which it relates.

Electronic information refers to any information provided by a rightholder that allows the identification of a work, a performance, a sound recording, a video recording, a broadcast, or a rightholder, any information regarding the conditions and rules governing the utilization of a work, a performance, a sound recording, a video recording or a broadcast, as well as any number or code representing all or part of this information.

o Databases

Article L. 342-3 of the IPC<sup>170</sup>

When a database is made available to the public by the rightholder, he may not prohibit:

- 1 The extraction or the reuse of an insubstantial part, evaluated qualitatively or quantitatively, of the contents of the database, by a person having lawful access;
- 2 The extraction for private purposes of a qualitatively or quantitatively substantial part of the contents of a non-electronic database, subject to compliance with the copyrights or related rights with respect to the works or materials incorporated into the database.
- 3 The extraction and reuse of database as provided in the first two paragraphs of 7° of article L. 122-5;
- 4 The extraction and reuse of a substantial part, evaluated qualitatively or quantitatively, of the contents of the database, subject to the databases created for

---

<sup>168</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000020740171&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000020740171&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

<sup>169</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740168&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=1563574560&oldAction=rechCodeArticle>

<sup>170</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006279252&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=235369580&oldAction=rechCodeArticle>

teaching purposes and the databases created for a digital edition of written works, and created exclusively for the illustration within the framework of teaching and research, to the exclusion of any entertaining or recreational activity, when the public for whom this extraction and this reuse is intended is comprised mainly of pupils, students, teachers or researchers concerned directly, that the source is indicated, that the use of this extraction and this reuse does not give rise to any commercial exploitation and that it is compensated by payment negotiated on a lump-sum basis.

Any provision contrary to 1° above shall be void.

The exceptions mentioned in this article may not undermine the normal use of the database nor cause any unjustified damage to the legitimate interests of the database producer.

- Computer programs

Article L. 122-6-2 of the IPC<sup>171</sup>

Any advertisement or user's handbook concerning means of removing or circumventing any technical device protecting a computer program shall state that the unlawful use of such means is liable to the penalties laid down for cases of infringement.

Article R. 335-2 of the IPC<sup>172</sup>

Any advertisement or user's handbook concerning means of removing or circumventing any technical device protecting a computer program, which does not bear a notice in clear characters that the unlawful use of such means is liable to the penalties laid down for cases of infringement, shall incur the penalties laid down for petty offences of the 3<sup>rd</sup> class.

- Provisions relating to circumvention

- With respect to works other than computer programs

Article L. 335-3-1 of the IPC<sup>173</sup>

I. The fact of knowingly undermining, for purposes other than research, an effective technological measure as defined in article L. 331-5, in order to alter the protection of a work by decoding it, decrypting it or, by any other individual intervention, with the aim of circumventing, defeating or removing a mechanism of protection or of control, when this undermining is realized by means other than the use of an existing technological application, device or component mentioned in II, is punishable by a fine of €3,750.

---

<sup>171</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006278921&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

<sup>172</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006280049&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

<sup>173</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000006279236&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000006279236&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

II. The fact of knowingly providing or proposing to a another person, directly or indirectly, means designed or specifically adapted for the purpose of circumventing an effective technological measure by one of the following ways, is punishable by 6-month imprisonment and a fine of €30,000:

- manufacturing or importing, for purposes other than research, a technological application, a device or a component;
- possessing for sale, lending or rental, offering to the same ends or offering to the public in any manner a technological application, device or component;
- offering a service to this end;
- inducing the use or commissioning, conceiving, organizing, reproducing, distributing or disseminating an advertisement for one of the abovementioned processes.

III. These provisions do not apply to acts performed for computer security purposes, within the limits of the rights provided for by this code.

Article R. 335-3 of the IPC<sup>174</sup>

Is punished by a fine as provided for 4<sup>th</sup> class petty offences the fact of:

1 Possessing for personal use or using a technological application, device or component designed or specifically adapted for the purpose of undermining an effective technological measure referred to in article L. 331-5 of this code protecting a work, a performance, a sound recording, a video recording, a broadcast or a database;

2 Resorting to a service designed or specifically adapted for the purpose of undermining an effective technological measure referred to in the previous paragraph.

These provisions do not apply to acts that cause damages to rightholders and that are performed for the purposes of computer security or scientific research in cryptography.

- o With respect to computer programs

Please see above: Article L. 122-6-2 of the IPC.

---

<sup>174</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006280050&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

- Provisions limiting the application of technological measures
- Provisions with respect to the HADOPI and/or exceptions to copyright and related Rights

Article L. 331-13 of the IPC<sup>175</sup>

The High Authority is in charge of:

- 1 A mission to encourage the development of lawful offering and to observe the licit and illicit use of the works and the subjects to which is attached a copyright or a related right within the electronic communication networks used to provide online communication services to the public;
- 2 A mission to protect these works and subjects against infringement committed within the electronic communication networks used to provide online communication services to the public;
- 3 A mission to regulate and monitor the field of technological protection measures and identification of works and subjects protected by a copyright or by a related right.

For the purposes of these missions, the High Authority may recommend any legislative or regulatory modification. The Government may consult with it regarding any proposed law or decree affecting the protection of literary and artistic property rights. The Government or the parliamentary commissions may also consult with it concerning any question under its jurisdiction.

Article L. 331-23 of the IPC<sup>176</sup>

In connection with its mission to encourage the development of lawful offering, whether commercial or not, and to observe the use, whether licit or not, of works and subjects protected by any copyright or by any related right within electronic communication networks, the High Authority publishes indicators each year, the list of which is determined by decree. It summarizes the development of lawful offering in the report mentioned in article L. 331-14.

Pursuant to the terms established by a decree of the *Conseil d'Etat* [the “Council of State”], the High Authority attributes to the offers proposed by persons whose business is to offer online communication services to the public a label allowing users of this service to clearly identify the lawful nature of these offers. This labelling is periodically revised.

The High Authority ensures the implementation, the enhancement and the updating of a referencing portal for these same offers.

It evaluates, in addition, the experiments conducted in the field of content identification and filtering technologies by the creators of such technologies, the rightholders with respect to the works and protected subjects and the persons who

---

<sup>175</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740259&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=1850928299&oldAction=rechCodeArticle>

<sup>176</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740330&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=693515139&oldAction=rechCodeArticle>



provide an online public communication service. It summarizes the main changes observed in the area, in particular with regards to the efficiency of such technologies, in its annual report provided for by article L. 331-14.

It identifies and studies the technological methods allowing the illicit use of works and subjects protected by any copyright or by any related right within electronic communication networks. In the report provided for in article L. 331-14, it proposes, if applicable, remedial solutions.

#### Article L. 331-26 of the IPC<sup>177</sup>

After consulting with the creators of means of securization intended to prevent the illicit use of access to an online public communication service, persons whose business is to offer access to such a service as well as companies governed by title II of this book and the duly formed professional defence organisms, the High Authority publishes the relevant functional specifications that these methods should present.

At the end of the certified evaluation procedure taking into account their conformity with the specifications mentioned in the first paragraph and their efficiency, the High Authority prepares a list of labelled means of securization. This labelling is periodically revised.

A decree of the *Conseil d'Etat* specifies the evaluation and labelling procedure for these means of securization.

#### Article L. 331-31 of the IPC<sup>178</sup>

In connection with its mission to regulate and monitor the field of technological protection measures and identification of works and protected subjects by copyright or by related rights, the High Authority exercises the following functions:

[1°] It ensures that the technological measures mentioned in article L. 331-5 do not result, due to their mutual incompatibility or their incapacity to interoperate, in additional and independent limitations to the use of a work from those expressly granted by the rightholder of any copyright or a in respect of a work other than a computer program, or of any related right in respect of a performance, a sound recording, a video recording or a broadcast;

The High Authority ensures that the implementation of technological measures of protection do not result in depriving the beneficiaries of the exceptions defined in:

- 2°, e of 3° as of January 1, 2009, 7° and 8° of article L. 122-5;
- 2°, last paragraph of 3° as of January 1, 2009, 6° and 7° of article L. 211-3;
- 3° and, as of January 1, 2009, 4° of article L. 342-3;
- and of article L. 331-4.

---

<sup>177</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212240&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=1354243225&oldAction=rechCodeArticle>

<sup>178</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212222&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

It also ensures that the implementation of technological protection measures do not result in depriving the beneficiaries of the copying exception for the purposes of collection, conservation and onsite consultation mentioned in 2° of article L. 132-4 and in articles L. 132-5 and L. 132-6 of the *Code du patrimoine* [National Heritage Code];

Subject to articles L. 331-7 to L. 331-10, L. 331-33 to L. 331-35 and L. 331-37 of this code, the High Authority determines the rules governing the exercise of the above-mentioned exceptions and determines in particular the minimum number of authorized copies within the framework of the private copying exception, based on the type of work or the protected subject, the various means of public communication and the possibilities offered by the available protection technologies.

#### Article L. 331-33 of the IPC<sup>179</sup>

Any beneficiary of the exceptions set forth in 2° of article L- 331-31 or any approved legal entity which represents such person may file a claim with the High Authority on any dispute relating to the restrictions that technological measures defined in article L. 331-8 create in the exercise of those exceptions.

#### Article L. 331-36 of the IPC<sup>180</sup>

The High Authority may be asked for a non-binding opinion by one of the persons mentioned in article L. 331-32 on any issue relating to the interoperability of technological measures.

It may also be asked for a non-binding opinion, by a person that is the beneficiary of one of the exceptions mentioned in 2° of article L. 331-31 or by the legal entity that represents it, on any issue relating to the effective implementation of this exception.

#### Article R. 335-4 of the IPC<sup>181</sup>

Is punished by a fine as provided for 4<sup>th</sup> class petty offences the act of:

1 Possessing for personal use or using a technological application, device or component designed or specifically adapted to remove or modify a piece of information referred to in article L. 331-22 and for the purposes of infringing any copyright, any related right or a database producer's right, concealing or facilitating such an infringement.

2 Resorting to a service designed or specifically adapted for the purpose of infringing the rights referred to in the previous paragraph, under the same conditions.

---

<sup>179</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212204&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

<sup>180</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212182&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

<sup>181</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006280051&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

These provisions do not apply to acts that do not cause damages to rightholders and that are performed for the purposes of computer security or scientific research in cryptography.

- o Provisions with respect to interoperability and/or to other exceptions applying only to computer programs

Article L. 331-32 of the IPC<sup>182</sup>

Any publisher of a computer program, manufacturer of a technical system and any service operator may, in the event of a refusal to be granted access to information essential to interoperability, ask the High Authority to guarantee the interoperability of the existing systems and services, in respect of the rights of the parties, and to receive from the rightholder with respect to the technological measures, the information essential to interoperability. The High Authority has two months from the filing of this request to render a decision.

Information that is essential to interoperability includes technical documentation and the programming interfaces required for a technological device to access, including in an open standard within the meaning of article 4 of law no. 2004-575 of 21 June 2004 for confidence in the digital economy, a work or a subject protected by a technological measure and attached electronic information, in respect of the terms of use of the work or the protected subject that were initially defined.

The rightholder of the rights with respect to a technological measure may not require the beneficiary to waive the publication of the source code and the technical documentation of its independent and interoperating computer program unless it proves that doing so would seriously undermine the security and the efficiency of such technological measures.

The High Authority may accept the commitments proposed by the parties and likely to end the practices contrary to interoperability. Unless an agreement is reached among the parties and after having allowed the interested parties to present their observations, it renders its motivated decision of dismissing the request or issues an injunction laying down, if needed subject to penalty, the conditions under which the requesting party may be granted access to the information essential to interoperability and the commitments that he must respect to guarantee the efficiency and the integrity of the technological measure, as well as the conditions of access and use of the protected content. The penalty ordered by the High Authority is calculated and enforced by the latter.

The High Authority has the power to order a financial sanction in the event of non-compliance with its injunctions, or in the event of the non-compliance with the commitments that it accepted. Each financial sanction is proportional to the importance of the damage caused to the interested parties, to the situation of the sanctioned organism or company and if applicable, the reiteration of practices contrary to interoperability. It is determined individually and on a motivated basis. The maximum amounts to 5 % of the highest global turnover excluding taxes generated over the course of ended fiscal years preceding the one in which the practices contrary to interoperability were implemented in the case of a company and to €1.5 million in other cases.

---

<sup>182</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212211&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

The decisions of the High Authority are rendered public while respecting the secrets protected by law. They are notified to the parties who may submit an appeal before the Paris Court of Appeals. The appeal results in a suspension of the decision.

The president of the High Authority reports to the Competition Authority any abuses of a dominant position or any practices preventing free competition that it may be aware of in the sector of technological measures. This filing may be submitted within the framework of an urgent proceeding, as provided in article L. 464-1 of the Commercial Code. The president of the High Authority may also submit a request, for a non-binding opinion, regarding any question under its jurisdiction. The Competition Authority transmits to the High Authority any filing entering within the scope of jurisdiction of the latter and requests its non-binding opinion concerning the practices that have been reported to it in the sector of technological measures mentioned in article L. 331-5 of this code.

Article L. 122-6-1 of the IPC<sup>183</sup>

I. The acts referred to in 1° and 2° of article L. 122-6 shall not require authorization by the author when they are necessary for the use of the computer program by the person entitled to use it in accordance with its intended purpose, including for error correction.

However, an author may by contract reserve the right to correct errors and stipulate any particular rules governing the acts referred to in 1° and 2° of article L. 122-6, necessary for the use of the computer program by the person entitled to use it in accordance with its intended purpose.

II. A person entitled to use the computer program may make a back-up copy when doing so is necessary to ensure the use of the computer program.

III. A person entitled to use the computer program shall be entitled, without the authorization of the author, to observe, study or test the functioning of this computer program in order to determine the ideas and principles which underlie any element of the computer program when performing any of the acts of loading, displaying, running, transmitting or storing the computer program which he is entitled to do.

IV. Reproducing the code of the computer program or translating the form of that code shall not require the authorization of the author if reproducing or translating within the meaning of 1° or 2° of article L. 122-6 is indispensable for obtaining the information necessary to achieve the interoperability of an independently created computer program with other computer programs, providing that the following conditions are met:

1 these acts are performed by a person entitled to use a copy of the computer program or on his behalf by a person authorized to do so;

2 the information necessary to achieve interoperability has not previously been readily and quickly available to the persons referred to in 1° above;

3 and these acts are limited to the parts of the original computer program which are necessary to achieve interoperability.

---

<sup>183</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006278920&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

The information thus obtained may not:

- 1 be used for goals other than to achieve interoperability of the independently created computer program;
- 2 be communicated to third parties, except if it is necessary for the interoperability of the independently created computer program;
- 3 nor be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

V. This article may not be interpreted in such a way as to undermine the normal exploitation of the computer program or to cause any unreasonable damage to the legitimate interests of the author.

Any stipulation contrary to the provisions of paragraphs II, III and IV of this article shall be void.

– Provisions relating to remedial measures

o Evidentiary measures

Article L. 332-1 of the IPC<sup>184</sup>

The police commissioners and, where there are no police commissioners, the *juges d'instance* [first instance judges in small claims courts], are held, upon the request of any author of a copyrighted work protected under book I of this code, of its rightholders, assigns or successors, to seize examples constituting an illicit copy of this work or any specimen, product, apparatus, device, component or means undermining the technological measures and the information mentioned respectively in articles L. 331-5 and L. 331-11;

If the seizure should result in a slowing or a suspension of representations or public performances that are pending or already announced, a special authorization must be granted by the president of the *Tribunal de Grande Instance* [Court of First Instance], by order rendered upon request. The president of the *Tribunal de Grande Instance* may also order, in the same way:

- 1 The suspension of any pending manufacture tending to illicit reproduction of a work or to the undermining of the technological measures and the information mentioned respectively in articles L. 331-5 et L. 331-11;
- 2 The seizure, any day at any time, of specimens constituting an illicit copy of the work, already manufactured or being manufactured, or specimens, products, apparatus, devices, components or means, manufactured or being manufactured, undermining the technological measures and the information mentioned respectively in articles L. 331-5 and L. 331-11, the revenues generated, as well as the illicit specimens; it may also order the actual seizure of material and instrument used to produce or illicitly distribute the works, as well as any related documents;

---

<sup>184</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740305&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=1526820720&oldAction=rechCodeArticle>

3 The seizure of revenues generated by any reproduction, representation or broadcasting, by any means, of a creative work, carried out by infringing copyright or resulting from an undermining of the technological measures and the information mentioned respectively in articles L. 331-5 and L. 331-11;

4 (Abrogated);

5 The actual seizure of illicit works or suspected infringing copyright products, or their delivery to a third party in order to prevent their introduction or their circulation in commercial channels;

The president of the *Tribunal de Grande Instance* may, in the same way, order the measures provided in 1° to 5° upon the request of rightholders of related rights as defined in book II of this code.

The president of the *Tribunal de Grande Instance* may, in the orders provided above, order the prior creation of guarantees by the seizing party.

o Criminal provisions

▪ General provision

Article L. 335-3 of the IPC<sup>185</sup>

Any reproduction, representation or publication, by any means whatsoever, of a creative work infringing the author's copyright, as defined and regulated by law, is also a counterfeiting misdemeanour.

Infringing one of the rights defined in article L. 122-6 of the author of a computer program is also a counterfeiting misdemeanour.

The recording of all or part of a cinema or audiovisual work in a movie theatre is also a counterfeiting misdemeanour.

▪ Works other than computer programs

Article L. 335-3-2 of the IPC<sup>186</sup>

I. The fact of knowingly removing or altering, for purposes other than research, any piece of information referred to in article L. 331-11, by an individual intervention not requiring the use of an existing technological application, device or a component, designed or specifically adapted for this purpose, with the aim of infringing a copyright, concealing or facilitating such an infringement, is punishable by a fine of €3,750.

II. The fact of knowingly providing or proposing to another person, directly or indirectly, means designed or specifically adapted to remove or alter, even partially, a piece of information referred to in article L. 331-11, with the aim of infringing a

---

<sup>185</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740345&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=661444293&oldAction=rechCodeArticle>

<sup>186</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000020740295&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

copyright, concealing or facilitating such an infringement, by one of the following ways, is punishable by 6-month imprisonment and a fine of €30,000:

- manufacturing or importing, for purposes other than research, a technological application, a device or a component;
- possessing for sale, lending or rental, offering to the same ends or offering to the public in any manner a technological application, device or component;
- offering a service to this end;
- inducing the use or commissioning, conceiving, organizing, reproducing, distributing or disseminating an advertisement for one of the abovementioned processes.

III. The fact of knowingly importing, distributing, making available to the public in any form whatsoever or of disclosing to the public, directly or indirectly, a work from which a piece of information listed in article L. 331-11 has been removed or altered with the aim of infringing a copyright, concealing or facilitating such an infringement, is punishable by 6-month imprisonment and a fine of €30,000.

IV. These provisions do not apply to acts performed for the purposes of research or computer security, within the limits of the rights provided for in this code.

Article L. 335-4-1 of the IPC<sup>187</sup>

I. The fact of knowingly undermining, for purposes other than research, an effective technological measure within the meaning of article L. 331-5, in order to alter the protection of a performance, a sound recording, a video recording or a broadcast by a decoding it, decrypting it or any other individual intervention intended to circumvent, neutralize or remove a protection or control mechanism is punishable by a fine of €3,750 when this infringement is carried out by means other than the use of an existing technological application, device or component mentioned in section II below.

II. The fact of knowingly providing or proposing to another person, directly or indirectly, the means designed or specifically adapted to undermine an effective technological measure within the meaning of article L. 331-5, by one of the following ways, is punishable by 6-month imprisonment and a fine of €30,000:

- manufacturing or importing, for purposes other than research, a technological application, a device or a component;
- possessing for sale, lending or rental, offering to the same ends or offering to the public in any manner a technological application, device or component;
- offering a service to this end;
- inducing the use or commissioning, conceiving, organizing, reproducing, distributing or disseminating an advertisement for one of the abovementioned processes.

---

<sup>187</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006279238&cidTexte=LEGITEXT000006069414&dateTexte=20100105&oldAction=rechCodeArticle>

III. These provisions do not apply to acts performed for the purpose of computer security, within the limits of the rights provided for in this code.

Article L. 335-4-2 of the IPC<sup>188</sup>

I. The fact of knowingly removing or altering, for purposes other than research, any piece of information referred to in article 331-11, by an individual intervention not requiring the use of an existing technological application, device or a component, designed or specifically adapted for this purpose, with the aim of infringing a related right, concealing or facilitating such an infringement, is punishable by a fine of €3,750.

II. The fact of knowingly providing or proposing to another person, directly or indirectly, the means designed or specifically adapted to remove or alter, even partially, a piece of information referred to in article L. 331-11, with the aim of infringing a related right, concealing or facilitating such an infringement, by one of the following means, is punishable by 6-month imprisonment and a fine of € 30,000:

- manufacturing or importing, for purposes other than research, a technological application, a device or a component;
- possessing for sale, lending or rental, offering to the same ends or offering to the public in any manner a technological application, device or component;
- offering a service to this end;
- inducing the use or commissioning, conceiving, organizing, reproducing, distributing or disseminating an advertisement for one of the abovementioned processes.

III. The fact of knowingly importing, distributing, making available to the public in any form whatsoever or of disclosing to the public, whether directly or indirectly, a performance, a sound recording, a video recording or a broadcast, from which a piece of information listed in article L. 331-11 has been removed or altered with the aim of infringing a related right, concealing or facilitating such an infringement, is punishable by 6-month imprisonment and a fine of €30,000.

IV. These provisions do not apply to acts performed for the purpose of computer security, within the limits of the rights provided for in this code.

---

<sup>188</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000020740291&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000020740291&cidTexte=LEGITEXT000006069414&dateTexte=20100105)



Article L. 335-5 of the IPC<sup>189</sup>

In the event of a sentence on the basis of one of the offences defined in articles L. 335-2 to L. 335-4-2, the court may order the total or partial closing, permanently or temporarily, for a term of no more than five years, of the establishment used to commit the offence.

A temporary closing may not result in the termination or the suspension of the employment agreement, nor any financial loss to the concerned employees. When a permanent closing results in the redundancy of employees, it results, in addition to the notice indemnity and the termination indemnity, to the damages provided for in articles L. 122-14-4 and L. 122-14-5 of the Labour Code in the event of a termination of an employment contract. The failure to pay these indemnities is punishable by 6-month imprisonment and a fine of €3,750.

Article L. 335-6 of the IPC<sup>190</sup>

Individuals who are guilty of one of the violations provided for in articles L. 335-2 to L. 335-4-2 may also be sentenced, at their expense, to stop the commercial distribution of items deemed to be counterfeits and any thing that was used or intended to be used to commit the offence.

The court may order the confiscation of all or part of the revenues received through the offence as well as those relating to any counterfeit or illicitly reproduced sound recordings, video recordings, objects and specimens as well as any material specifically installed to commit the misdemeanour.

It may order the destruction, at the expense of the sentenced party, or the return to the damaged party of the items and things withdrawn from commercial distribution or confiscated, without prejudice to any damages.

It may also order, at the expense of the sentenced party, the posting of the decision or the publication of the decision setting forth the sentence, in accordance with article 131-35 of the Criminal Code.

Article L. 335-8 of the IPC<sup>191</sup>

Legal entities who are held criminally responsible of offences, as provided in article 121-2 of the Criminal Code, of the offences defined in articles L. 335-2 to L. 335-4-2 will be liable, in addition to the fine provided for in article 131-38 of the Criminal Code, for the penalties provided for in article 131-39 of this same code.

---

<sup>189</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000021212290&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000021212290&cidTexte=LEGITEXT000006069414&dateTexte=20100105)<http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006279187&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=686492523&oldAction=rechCodeArticle>

<sup>190</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000006279193&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000006279193&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

<sup>191</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000020631671&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000020631671&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

The restriction mentioned in 2° of article 131-39 of the same code applies to the activity during the exercise of which or at the occasion of the exercise of which the offence was committed.

Legal entities who are held criminally responsible may also be sentenced, at their expense, to withdraw the items that are deemed to be counterfeits from commercial distribution along with any thing that was used or was intended to be used to commit the offence.

The court may order the destruction, at the expense of the sentenced party, or the return to the damaged party of the items and things withdrawn from commercial distribution or confiscated, without prejudice to any damages.

- Databases

Article L. 342-3-1 of the IPC<sup>192</sup>

The effective technological measures within the meaning of article L. 331-5 that are appropriate for preventing or limiting the uses of a database that the producer has not authorized in application of article L. 342-1 benefit from the protection provided for in article L. 335-4-1.

The database producers that rely on the technological protection measures mentioned in the first paragraph must take appropriate measures so that their implementation will not deprive the beneficiaries of the exceptions defined in article L. 342-3 of their effective benefit, in accordance with the conditions provided for in 2° of article L. 331-31 and in articles L. 331-7 to L. 331-10, L. 331-33 to L. 331-35 and L. 331-37.\_

Any dispute relating to the ability to benefit from the exceptions defined in article L. 342-3 that involve a technological measure mentioned in the first paragraph of this article is submitted to the High Authority for the work broadcast and protection of the rights on the internet provided for in article L. 331-12.

Article L. 342-3-2 of the IPC<sup>193</sup>

Information in electronic format relating to the regime of the rights of the database producer, within the meaning of article L. 331-11, benefit from the protection provided for in article L. 335-4-2.

- Computer programs

---

<sup>192</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021212267&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=162413276&oldAction=rechCodeArticle>

<sup>193</sup> [http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v\\_2?idArticle=LEGIARTI000020740287&cidTexte=LEGITEXT000006069414&dateTexte=20100105](http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=9FC7A191047982C010EB4B952EFFAB73.tpdjo08v_2?idArticle=LEGIARTI000020740287&cidTexte=LEGITEXT000006069414&dateTexte=20100105)

Article L. 122-6 of the IPC<sup>194</sup>

Subject to the provisions of article L. 122-6-1, the exploitation right of the author of a computer program shall include the right to do or to authorize:

1 the permanent or temporary reproduction of a computer program, partially or as a whole by any means and in any form. Insofar as loading, displaying, running, transmission or storage of this computer program require such reproduction, these acts shall be performed only with the authorization of the author;

2 the translation, adaptation, arrangement or any other alteration of a computer program and the reproduction of the computer program thereof;

3 the offer for sale or for free, including rental, of the copy or copies of the computer program by any process. However, the first sale of a copy of a computer program on the territory of a Member State of the European Community or of a State party to the agreement on the European Economic Area by the author or with his consent shall exhaust the right of offering this copy in all Member States, with the exception of the right to authorize later rental of a copy.

▪ Border measures

Article L. 335-10 of the IPC<sup>195</sup>

Customs administration may, at the written request of a rightholder of any copyright or any related right, which request shall be accompanied by proof of his right as provided by decree of the *Conseil d'Etat*, withhold in the course of its controls any products alleged by him to be infringing that right.

The *procureur de la République* [attorney general], the plaintiff and the party declaring or in possession of the products shall be informed without delay, by the customs services, of the withholding measure that they have taken.

The withholding measure shall be lifted as of right if the plaintiff fails, within 10 working days following notification of the withholding of the products, to prove to the customs services:

- either that preservation measures under article L. 332-1 have been taken;
- or that he has initiated proceedings before a civil court or a criminal court and has provided the necessary guarantees to cover his liability in the event of the infringement claim being eventually considered unfounded.

For the purpose of the initiation of the legal proceedings referred to in the previous paragraph, the plaintiff may require the customs administration to communicate the names and addresses of the sender, the importer and the consignee of the withheld products, or of the holder thereof, as well as the quantity thereof,

---

<sup>194</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006278919&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=1921712598&oldAction=rechCodeArticle>

<sup>195</sup> <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006279207&cidTexte=LEGITEXT000006069414&dateTexte=20100105&fastPos=1&fastReqId=564381123&oldAction=rechCodeArticle>

notwithstanding the provisions of article 59bis of the *Code des douanes* [Customs Code] concerning the professional secrecy to which officers of the customs administration are bound.

The withholding mentioned in the first paragraph shall not concern the products that have European status, which are legally manufactured or released for free circulation in a member state of the European Community and intended, after having entered the customs territory as defined in the first article of Customs Code, to be released on the market of another Member State of the European Community, to be legally marketed.

Annex 3  
English Law<sup>196</sup>

Section 296 CDPA: Circumvention of technical devices applied to computer programs<sup>197</sup>

- (1) This section applies where—
  - (a) a technical device has been applied to a computer program; and
  - (b) a person (A) knowing or having reason to believe that it will be used to make infringing copies—
    - (i) manufactures for sale or hire, imports, distributes, sells or lets for hire, offers or exposes for sale or hire, advertises for sale or hire or has in his possession for commercial purposes any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of the technical device; or
    - (ii) publishes information intended to enable or assist persons to remove or circumvent the technical device.
- (2) The following persons have the same rights against A as a copyright owner has in respect of an infringement of copyright—
  - (a) a person—
    - (i) issuing to the public copies of, or
    - (ii) communicating to the public,

the computer program to which the technical device has been applied;

- (b) the copyright owner or his exclusive licensee, if he is not the person specified in paragraph (a);
  - (c) the owner or exclusive licensee of any intellectual property right in the technical device applied to the computer program.
- (3) The rights conferred by subsection (2) are concurrent, and sections 101(3) and 102(1) to (4) apply, in proceedings under this section, in relation to persons with concurrent rights as they apply, in proceedings mentioned in

---

<sup>196</sup> The CDPA is generally available through the following website <http://www.statutelaw.gov.uk>. Sections 296- 296ZF (“Circumvention of protection measures”) are available at the following link: <http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&parentActiveTextDocId=0&activetextdocid=2250730&versionNumber=2>  
Section 296ZG (“Rights Management Information”) is available at the following link: <http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&parentActiveTextDocId=0&activetextdocid=3519544&versionNumber=1>

<sup>197</sup> Substituted by SI 2003/2498, regs 3, 24(1). Date in force: 31 October 2003: see SI 2003/2498, reg 1; for savings and transitional provisions see regs 30–40 thereof.

those provisions, in relation to a copyright owner and exclusive licensee with concurrent rights.

- (4) Further, the persons in subsection (2) have the same rights under section 99 or 100 (delivery up or seizure of certain articles) in relation to any such means as is referred to in subsection (1) which a person has in his possession, custody or control with the intention that it should be used to facilitate the unauthorised removal or circumvention of any technical device which has been applied to a computer program, as a copyright owner has in relation to an infringing copy.
- (5) The rights conferred by subsection (4) are concurrent, and section 102(5) shall apply, as respects anything done under section 99 or 100 by virtue of subsection (4), in relation to persons with concurrent rights as it applies, as respects anything done under section 99 or 100, in relation to a copyright owner and exclusive licensee with concurrent rights.
- (6) In this section references to a technical device in relation to a computer program are to any device intended to prevent or restrict acts that are not authorised by the copyright owner of that computer program and are restricted by copyright.
- (7) The following provisions apply in relation to proceedings under this section as in relation to proceedings under Part 1 (copyright)—
  - (a) sections 104 to 106 of this Act (presumptions as to certain matters relating to copyright); and
  - (b) section 72 of the [Senior Courts Act 1981], section 15 of the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 and section 94A of the Judicature (Northern Ireland) Act 1978 (withdrawal of privilege against self-incrimination in certain proceedings relating to intellectual property);  
and section 114 of this Act applies, with the necessary modifications, in relation to the disposal of anything delivered up or seized by virtue of subsection (4).
- (8) Expressions used in this section which are defined for the purposes of Part 1 of this Act (copyright) have the same meaning as in that Article.

Section 296ZA CDPA: Circumvention of technological measures<sup>198</sup>

- (1) This section applies where—
  - (a) effective technological measures have been applied to a copyright work other than a computer program; and
  - (b) a person (B) does anything which circumvents those measures knowing, or with reasonable grounds to know, that he is pursuing that objective.
- (2) This section does not apply where a person, for the purposes of research into cryptography, does anything which circumvents effective technological

---

<sup>198</sup> Substituted, together with ss 296, 296ZB–296ZF, for s 296 as originally enacted, by SI 2003/2498, regs 3, 24(1). Date in force: 31 October 2003: see SI 2003/2498, reg 1; for savings and transitional provisions see regs 30–40 thereof.

measures unless in so doing, or in issuing information derived from that research, he affects prejudicially the rights of the copyright owner.

- (3) The following persons have the same rights against B as a copyright owner has in respect of an infringement of copyright—
  - (a) a person—
    - (i) issuing to the public copies of, or
    - (ii) communicating to the public,the work to which effective technological measures have been applied; and
  - (b) the copyright owner or his exclusive licensee, if he is not the person specified in paragraph (a).
- (4) The rights conferred by subsection (3) are concurrent, and sections 101(3) and 102(1) to (4) apply, in proceedings under this section, in relation to persons with concurrent rights as they apply, in proceedings mentioned in those provisions, in relation to a copyright owner and exclusive licensee with concurrent rights.
- (5) The following provisions apply in relation to proceedings under this section as in relation to proceedings under Part 1 (copyright)—
  - (a) sections 104 to 106 of this Act (presumptions as to certain matters relating to copyright); and
  - (b) section 72 of the [Senior Courts Act 1981], section 15 of the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 and section 94A of the Judicature (Northern Ireland) Act 1978 (withdrawal of privilege against self-incrimination in certain proceedings relating to intellectual property).
  - (6) Subsections (1) to (4) and (5)(b) and any other provision of this Act as it has effect for the purposes of those subsections apply, with any necessary adaptations, to rights in performances, publication right and database right.
  - (7) The provisions of regulation 22 (presumptions relevant to database right) of the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032) apply in proceedings brought by virtue of this section in relation to database right.

Section 296ZB CDPA: Devices and services designed to circumvent technological measures<sup>199</sup>

- (1) A person commits an offence if he—
  - (a) manufactures for sale or hire, or
  - (b) imports otherwise than for his private and domestic use, or
  - (c) in the course of a business—

---

<sup>199</sup> Substituted, together with ss 296, 296ZA, 296ZC–296ZF, for s 296 as originally enacted, by SI 2003/2498, regs 3, 24(1). Date in force: 31 October 2003: see SI 2003/2498, reg 1; for savings and transitional provisions see regs 30–40 thereof.

- (i) sells or lets for hire, or
  - (ii) offers or exposes for sale or hire, or
  - (iii) advertises for sale or hire, or
  - (iv) possesses, or
  - (v) distributes, or
- (d) distributes otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner,
- any device, product or component which is primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures.
- (2) A person commits an offence if he provides, promotes, advertises or markets—
- (a) in the course of a business, or
  - (b) otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner,
- a service the purpose of which is to enable or facilitate the circumvention of effective technological measures.
- (3) Subsections (1) and (2) do not make unlawful anything done by, or on behalf of, law enforcement agencies or any of the intelligence services—
- (a) in the interests of national security; or
  - (b) for the purpose of the prevention or detection of crime, the investigation of an offence, or the conduct of a prosecution,
- and in this subsection “intelligence services” has the meaning given in section 81 of the Regulation of Investigatory Powers Act 2000.
- (4) A person guilty of an offence under subsection (1) or (2) is liable—
- (a) on summary conviction, to imprisonment for a term not exceeding three months, or to a fine not exceeding the statutory maximum, or both;
  - (b) on conviction on indictment to a fine or imprisonment for a term not exceeding two years, or both.
- (5) It is a defence to any prosecution for an offence under this section for the defendant to prove that he did not know, and had no reasonable ground for believing, that—
- (a) the device, product or component; or
  - (b) the service,
- enabled or facilitated the circumvention of effective technological measures.

Section 296ZC CDPA: Devices and services designed to circumvent technological measures: search warrants and forfeiture



- (1) The provisions of sections 297B (search warrants), 297C (forfeiture of unauthorised decoders: England and Wales or Northern Ireland) and 297D (forfeiture of unauthorised decoders: Scotland) apply to offences under section 296ZB with the following modifications.
- (2) In section 297B the reference to an offence under section 297A(1) shall be construed as a reference to an offence under section 296ZB(1) or (2).
- (3) In sections 297C(2)(a) and 297D(15) the references to an offence under section 297A(1) shall be construed as a reference to an offence under section 296ZB(1).
- (4) In sections 297C and 297D references to unauthorised decoders shall be construed as references to devices, products or components for the purpose of circumventing effective technological measures.

Section 296ZD CDPA: Rights and remedies in respect of devices and services designed to circumvent technological measures

- (1) This section applies where—
  - (a) effective technological measures have been applied to a copyright work other than a computer program; and
  - (b) a person (C) manufactures, imports, distributes, sells or lets for hire, offers or exposes for sale or hire, advertises for sale or hire, or has in his possession for commercial purposes any device, product or component, or provides services which—
    - (i) are promoted, advertised or marketed for the purpose of the circumvention of, or
    - (ii) have only a limited commercially significant purpose or use other than to circumvent, or
    - (iii) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, those measures.
- (2) The following persons have the same rights against C as a copyright owner has in respect of an infringement of copyright—
  - (a) a person—
    - (i) issuing to the public copies of, or
    - (ii) communicating to the public, the work to which effective technological measures have been applied;
  - (b) the copyright owner or his exclusive licensee, if he is not the person specified in paragraph (a); and
  - (c) the owner or exclusive licensee of any intellectual property right in the effective technological measures applied to the work.

- (3) The rights conferred by subsection (2) are concurrent, and sections 101(3) and 102(1) to (4) apply, in proceedings under this section, in relation to persons with concurrent rights as they apply, in proceedings mentioned in those provisions, in relation to a copyright owner and exclusive licensee with concurrent rights.
- (4) Further, the persons in subsection (2) have the same rights under section 99 or 100 (delivery up or seizure of certain articles) in relation to any such device, product or component which a person has in his possession, custody or control with the intention that it should be used to circumvent effective technological measures, as a copyright owner has in relation to any infringing copy.
- (5) The rights conferred by subsection (4) are concurrent, and section 102(5) shall apply, as respects anything done under section 99 or 100 by virtue of subsection (4), in relation to persons with concurrent rights as it applies, as respects anything done under section 99 or 100, in relation to a copyright owner and exclusive licensee with concurrent rights.
- (6) The following provisions apply in relation to proceedings under this section as in relation to proceedings under Part 1 (copyright)—
  - (a) sections 104 to 106 of this Act (presumptions as to certain matters relating to copyright); and
  - (b) section 72 of the [Senior Courts Act 1981], section 15 of the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 and section 94A of the Judicature (Northern Ireland) Act 1978 (withdrawal of privilege against self-incrimination in certain proceedings relating to intellectual property);  
and section 114 of this Act applies, with the necessary modifications, in relation to the disposal of anything delivered up or seized by virtue of subsection (4).
- (7) In section 97(1) (innocent infringement of copyright) as it applies to proceedings for infringement of the rights conferred by this section, the reference to the defendant not knowing or having reason to believe that copyright subsisted in the work shall be construed as a reference to his not knowing or having reason to believe that his acts enabled or facilitated an infringement of copyright.
- (8) Subsections (1) to (5), (6)(b) and (7) and any other provision of this Act as it has effect for the purposes of those subsections apply, with any necessary adaptations, to rights in performances, publication right and database right.
- (9) The provisions of regulation 22 (presumptions relevant to database right) of the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032) apply in proceedings brought by virtue of this section in relation to database right.

Section 296ZE CDPA: remedy where effective technological measures prevent permitted acts

- (1) In this section—

“permitted act” means an act which may be done in relation to copyright works, notwithstanding the subsistence of copyright, by virtue of a provision of this Act listed in Part 1 of Schedule 5A;

“voluntary measure or agreement” means—

- (a) any measure taken voluntarily by a copyright owner, his exclusive licensee or a person issuing copies of, or communicating to the public, a work other than a computer program, or
- (b) any agreement between a copyright owner, his exclusive licensee or a person issuing copies of, or communicating to the public, a work other than a computer program and another party,

the effect of which is to enable a person to carry out a permitted act.

- (2) Where the application of any effective technological measure to a copyright work other than a computer program prevents a person from carrying out a permitted act in relation to that work then that person or a person being a representative of a class of persons prevented from carrying out a permitted act may issue a notice of complaint to the Secretary of State.

- (3) Following receipt of a notice of complaint, the Secretary of State may give to the owner of that copyright work or an exclusive licensee such directions as appear to the Secretary of State to be requisite or expedient for the purpose of—

- (a) establishing whether any voluntary measure or agreement relevant to the copyright work the subject of the complaint subsists; or
- (b) (where it is established there is no subsisting voluntary measure or agreement) ensuring that the owner or exclusive licensee of that copyright work makes available to the complainant the means of carrying out the permitted act the subject of the complaint to the extent necessary to so benefit from that permitted act.

- (4) The Secretary of State may also give directions—

- (a) as to the form and manner in which a notice of complaint in subsection (2) may be delivered to him;
- (b) as to the form and manner in which evidence of any voluntary measure or agreement may be delivered to him; and
- (c) generally as to the procedure to be followed in relation to a complaint made under this section;

and shall publish directions given under this subsection in such manner as in his opinion will secure adequate publicity for them.

- (5) It shall be the duty of any person to whom a direction is given under subsection (3)(a) or (b) to give effect to that direction.
- (6) The obligation to comply with a direction given under subsection (3)(b) is a duty owed to the complainant or, where the complaint is made by a representative of a class of persons, to that representative and to each person in the class represented; and a breach of the duty is actionable accordingly

(subject to the defences and other incidents applying to actions for breach of statutory duty).

- (7) Any direction under this section may be varied or revoked by a subsequent direction under this section.
- (8) Any direction given under this section shall be in writing.
- (9) This section does not apply to copyright works made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.
- (10) This section applies only where a complainant has lawful access to the protected copyright work, or where the complainant is a representative of a class of persons, where the class of persons have lawful access to the work.
- (11) Subsections (1) to (10) apply with any necessary adaptations to—
  - (a) rights in performances, and in this context the expression “permitted act” refers to an act that may be done by virtue of a provision of this Act listed in Part 2 of Schedule 5A;
  - (b) database right, and in this context the expression “permitted act” refers to an act that may be done by virtue of a provision of this Act listed in Part 3 of Schedule 5A; and
  - (c) publication right.

#### Section 296ZF CDPA: Interpretation of sections 296ZA to 296ZE

- (1) In sections 296ZA to 296ZE, “technological measures” are any technology, device or component which is designed, in the normal course of its operation, to protect a copyright work other than a computer program.
- (2) Such measures are “effective” if the use of the work is controlled by the copyright owner through—
  - (a) an access control or protection process such as encryption, scrambling or other transformation of the work, or
  - (b) a copy control mechanism,  
which achieves the intended protection.
- (3) In this section, the reference to—
  - (a) protection of a work is to the prevention or restriction of acts that are not authorised by the copyright owner of that work and are restricted by copyright; and
  - (b) use of a work does not extend to any use of the work that is outside the scope of the acts restricted by copyright.
- (4) Expressions used in sections 296ZA to 296ZE which are defined for the purposes of Part 1 of this Act (copyright) have the same meaning as in that Article.

#### Section 296ZG CDPA: Electronic rights management information

- (1) This section applies where a person (D), knowingly and without authority, removes or alters electronic rights management information which—
  - (a) is associated with a copy of a copyright work, or
  - (b) appears in connection with the communication to the public of a copyright work, and
 

where D knows, or has reason to believe, that by so doing he is inducing, enabling, facilitating or concealing an infringement of copyright.
- (2) This section also applies where a person (E), knowingly and without authority, distributes, imports for distribution or communicates to the public copies of a copyright work from which electronic rights management information—
  - (a) associated with the copies, or
  - (b) appearing in connection with the communication to the public of the work,
 

has been removed or altered without authority and where E knows, or has reason to believe, that by so doing he is inducing, enabling, facilitating or concealing an infringement of copyright.
- (3) A person issuing to the public copies of, or communicating, the work to the public, has the same rights against D and E as a copyright owner has in respect of an infringement of copyright.
- (4) The copyright owner or his exclusive licensee, if he is not the person issuing to the public copies of, or communicating, the work to the public, also has the same rights against D and E as he has in respect of an infringement of copyright.
- (5) The rights conferred by subsections (3) and (4) are concurrent, and sections 101(3) and 102(1) to (4) apply, in proceedings under this section, in relation to persons with concurrent rights as they apply, in proceedings mentioned in those provisions, in relation to a copyright owner and exclusive licensee with concurrent rights.
- (6) The following provisions apply in relation to proceedings under this section as in relation to proceedings under Part 1 (copyright)—
  - (a) sections 104 to 106 of this Act (presumptions as to certain matters relating to copyright); and
  - (b) section 72 of the [Senior Courts Act 1981], section 15 of the Law Reform (Miscellaneous Provisions) (Scotland) Act 1985 and section 94A of the Judicature (Northern Ireland) Act 1978 (withdrawal of privilege against self-incrimination in certain proceedings relating to intellectual property).
- (7) In this section—
  - (a) expressions which are defined for the purposes of Part 1 of this Act (copyright) have the same meaning as in that Part; and
  - (b) “rights management information” means any information provided by the copyright owner or the holder of any right under copyright which identifies

the work, the author, the copyright owner or the holder of any intellectual property rights, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information.

- (8) Subsections (1) to (5) and (6)(b), and any other provision of this Act as it has effect for the purposes of those subsections, apply, with any necessary adaptations, to rights in performances, publication right and database right.
- (9) The provisions of regulation 22 (presumptions relevant to database right) of the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032) apply in proceedings brought by virtue of this section in relation to database right.

Schedule 5A: Permitted Acts to which Section 296ZE applies:

Part 1 Copyright Exceptions

section 29 (research and private study)

section 31A (making a single accessible copy for personal use)

section 31B (multiple copies for visually impaired persons)

section 31C (intermediate copies and records)

section 32(1), (2) and (3) (things done for purposes of instruction or examination)

section 35 (recording by educational establishments of broadcasts)

section 36 (reprographic copying by educational establishments of passages from published works)

section 38 (copying by librarians: articles in periodicals)

section 39 (copying by librarians: parts of published works)

section 41 (copying by librarians: supply of copies to other libraries)

section 42 (copying by librarians or archivists: replacement copies of works)

section 43 (copying by librarians or archivists: certain unpublished works)

section 44 (copy of work required to be made as condition of export)

section 45 (Parliamentary and judicial proceedings)

section 46 (Royal Commissions and statutory inquiries)

section 47 (material open to public inspection or on official register)

section 48 (material communicated to the Crown in the course of public business)

section 49 (public records)

section 50 (acts done under statutory authority)

section 61 (recordings of folksongs)  
section 68 (incidental recording for purposes of broadcast)  
section 69 (recording for purposes of supervision and control of broadcasts)  
section 70 (recording for purposes of time-shifting)  
section 71 (photographs of broadcasts)  
section 74 (provision of sub-titled copies of broadcast)  
section 75 (recording for archival purposes)]

#### Part 2: Rights in Performances Exceptions

paragraph 4 of Schedule 2 (things done for purposes of instruction or examination)  
paragraph 6 of Schedule 2 (recording of broadcasts by educational establishments)  
paragraph 7 of Schedule 2 (copy of work required to be made as condition of export)  
paragraph 8 of Schedule 2 (Parliamentary and judicial proceedings)  
paragraph 9 of Schedule 2 (Royal Commissions and statutory inquiries)  
paragraph 10 of Schedule 2 (public records)  
paragraph 11 of Schedule 2 (acts done under statutory authority)  
paragraph 14 of Schedule 2 (recordings of folksongs)  
paragraph 16 of Schedule 2 (incidental recording for purposes of broadcast)  
paragraph 17 of Schedule 2 (recordings for purposes of supervision and control of broadcasts)  
paragraph 17A of Schedule 2 (recording for the purposes of time-shifting)  
paragraph 17B of Schedule 2 (photographs of broadcasts)  
paragraph 20 of Schedule 2 (provision of sub-titled copies of broadcast)  
paragraph 21 of Schedule 2 (recording of broadcast for archival purposes)

#### Part 3 Database Right Exceptions

regulation 20 of and Schedule 1 to the Copyright and Rights in Databases Regulations 1997 (SI 1997/3032)

Annex 4  
German Law

I. General Provisions

Article 53 of the German Copyright Act<sup>200</sup>

- (1) The making of single copies of a work by a natural person for private use is permitted using any medium, insofar as these neither directly nor indirectly serve commercial purposes, provided that a manifestly illegally produced or publicly accessible original is not used for the reproduction. Anyone permitted to make such copies may also have the copies made by another person, subject to doing so free of charge, or if the copies are printed on paper or a similar medium using a photomechanical method or any other method having a similar effect.
- (2) It is permitted to make or have single copies made by another person
1. for personal scientific use, if and to the extent the copy is required for this purpose and it does not serve a commercial purpose,
  2. to be included in a personal archive, if and to the extent the copy is required for this purpose and a personal copy of the work is used as the original for reproduction,
  3. for one's own information regarding topical issues, if it is a work broadcast by radio,
  4. for any other personal use
- a) of small parts of published works or individual contributions that have appeared in newspapers or periodicals,
  - b) if it is a work that has been out-of-print for at least two years.
- This shall also apply in the case of sentence 1 no. 2 only if additionally
1. the copies are printed on paper or a similar medium using a photomechanical method or other method having a similar effect or
  2. an exclusively analog use occurs or
  3. the archive is operated in the public interest and neither directly nor indirectly pursues an economic or commercial purpose.
- This shall apply in the cases of sentence 1 No. 3 and 4 only if in addition one of the conditions set forth in sentence 2 No. 1 or 2 is met.
- (3) Making copies, or having copies made for personal use is permitted of small parts of published works or individual contributions that have appeared in newspapers or periodicals or made publicly accessible
1. for illustrative instructional purposes in schools, in non-commercial institutions of training and education and in vocational institutions in the number required for those participating in instruction

---

<sup>200</sup> [http://www.gesetze-im-internet.de/urhg/\\_98.html](http://www.gesetze-im-internet.de/urhg/_98.html)



2. for State examinations and examinations in schools, universities, in non-commercial institutions of training and education and in vocational institutions in the number required for those participating in instruction,  
  
if and to the extent the copy is required for this purpose. Copying a work, intended for instructional purposes in schools is always only permitted with the authorization of the copyright-holder.
- (4) Copying
  - a) graphic recordings of works of music,
  - b) a book or a newspaper essentially concerning a complete copy, to the extent of not being copied by hand, is always only permitted with the consent of the copyright-holder or subject to the conditions set forth in Paragraph 2 Sentence 1 No. 2 or for personal use if the work has been out-of-print for at least two years.
- (5) Paragraph 1, Paragraph 2 Sentence 1 No. 2 through 4 and Paragraph 3 No. 2 shall not apply to database works, the elements of which are only accessible with the aid of electronic media. Paragraph 2 Sentence 1 No. 1 and Paragraph 3 No. 1 shall apply to such database works provided that the scientific and instructional use is not for commercial purposes.
- (6) Copies may neither be distributed nor used for publication. However, it is permitted to lend lawfully produced copies of newspapers and out-of-print works or any works in which small damaged or lost parts have been replaced by reproductions.
- (7) The recording of public lectures, performances or showings of a work on video or audio media, the execution of plans and drafts of works of fine art and the reconstruction of a work of architecture are always only permitted with the consent of the copyright holder.

#### Article 69f Infringement of Rights

- (1) The right holder may require from their owners or proprietors that all unlawfully manufactured or distributed copies or all copies intended for unlawful distribution be destroyed. Article 98(2) and (3) shall apply mutatis mutandis.
- (2) Paragraph (1) shall apply mutatis mutandis to any means of which the sole intended purpose is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

#### Article 95a of the German Copyright Act<sup>201</sup>

- (1) Effective technological measures for the protection of works protected by this law or of other material protected by this law may not be circumvented without authorization of the right holder, if the actor knows or should know that the circumvention takes place in order to enable access to such a work or material, or to enable its use.

---

<sup>201</sup> [http://www.gesetze-im-internet.de/urhg/\\_95a.html](http://www.gesetze-im-internet.de/urhg/_95a.html)

- (2) Technological measures for the purpose of this law are technologies, devices and components, which in the normal course of their operation, are designed to prevent or restrict acts, in respect of protected works or other subject matter protected by this law, which are not authorized by the right holder. Technological measures are effective, if the use of a protected work or other material protected by this law is controlled by the right holder through application of an access control, a protection process such as encryption, scrambling or other transformation, or a copy control mechanism, which achieves the protection objective.
- (3) Prohibited are production, import, distribution, sale, rental, advertisement for sale or rental and possession for commercial purposes, of devices, products or components as well as the provision of services, which are
  1. promoted, advertised or marketed for the purpose of circumvention of effective technological measures, or
  2. have only a limited commercially significant purpose or use other than to circumvent effective technological measures, or
  3. are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of effective technological measures.
- (4) Tasks and powers of public authorities remain unaffected by the prohibitions of sections (1) and (3) for the purpose of protection of public security or in criminal proceedings.

Article 95b of the German Copyright Act<sup>202</sup>

- (1) If a right holder uses technological measures in accordance with this law, he is obligated to make available the necessary means which enable the use covered by the following limitations to the beneficiaries of those limitations, if they have legal access to the protected work or protected material:
  1. Article 45 (administration of justice and public safety),
  2. Article 45a (people with disabilities),
  3. Article 46 (collections for religious, school or instructional use), with the exception of religious use,
  4. Article 47 (school broadcasts),
  5. Article 52a (making publicly available for teaching and research),
  6. Article 53 (reproduction for private and other personal uses)
    - a) section 1, as far as it concerns reproductions on paper or any similar medium effected by the use of any kind of photographic technique or by some other process having similar effects,
    - b) section 2 sentence 1 no.1,

---

<sup>202</sup> [http://www.gesetze-im-internet.de/urhg/\\_95b.html](http://www.gesetze-im-internet.de/urhg/_95b.html)

- c) section 2 sentence 1 no.2 in connection with sentence 2 no.1 (photocopy on paper) or 3,
- d) section 2 sentence 1 no.3 and 4 in each case in connection with sentence 2 no.1 and sentence 3,
- e) section 3,

7. Article 55 (reproduction by broadcasting organizations).

Contractual agreements excluding such obligations are null and void.

- (2) Any person who violates the obligations of section 1 can be compelled by the beneficiary of one of the mentioned limitations to make available the necessary means for the realization of the respective rights. If the means offered correspond to an agreement between associations of right holders and of beneficiaries of the mentioned limitations, then it is assumed that the means are sufficient.
- (3) Sections 1 and 2 shall not apply if works and other related material are made available to the public on agreed contractual terms in such way that members of the public may access them from a place and at a time individually chosen by them.
- (4) Technological measures that are adapted for the fulfilment of the obligations of section 1, including those applied in implementation of voluntary agreements, enjoy legal protection under Article 95a.

Article 95c of the German Copyright Act<sup>203</sup>

- (1) Information for the management of rights of the right holders shall not be removed or changed if the respective information is attached to a reproduction of a work or material if it is shown in the course of public communication of such a work or subject matter and when the removal or change happens consciously unauthorized and if the acting person knows or should know that he thereby provokes, allows, relieves or conceals the violation of copy protected contents or other protected material.
- (2) Information for the management of rights in terms of this law is electronic information to identify works or other protected material, the author or any other right holder, information about the modalities and conditions for the use of the works or other protected material as well as numbers and codes by the help of which information like that is expressed.
- (3) It is prohibited to distribute, initiate distribution, send, play in public or make publicly available works or other protected material if information for the protection of rights was removed or changed without due authorization if the acting person knows or should know that such use infringes copyrights or related rights or provokes, allows, relieves or conceals related rights.

---

<sup>203</sup> [http://www.gesetze-im-internet.de/urhg/\\_95c.html](http://www.gesetze-im-internet.de/urhg/_95c.html)

#### Article 95d of the German Copyright Act<sup>204</sup>

- (1) Protected works and other protected material by technological measures have to be labeled, in a clearly visible manner, including information on the properties of the applied technological measures.
- (2) Any person who applies technological protection measures on works or other protected material has to provide his name or firm name and address for service, in order to enable the assertion of claims according to Article 95b Sec. 2. S. 1 does not apply to Article 95b Sec. 3.

#### II. Provisions relating to remedial measures

#### Article 97 of the German Copyright Act<sup>205</sup>

- (1) Against any person who infringes a copyright or any other right protected by this law, the injured party may bring an action for injunctive relief requiring the infringer to cease and desist if there is a danger of repetition of the acts of infringement. The action for injunctive relief also persists when a repetition of the acts of infringement occurs for the first time.
- (2) A person who commits the infringement intentional or negligent is liable for damages. The injured party may instead demand surrender of the profits derived by the infringer from the infringement. The damages may also be calculated on the basis of the profits derived from the infringement. Authors of scientific publications (Article 70), photographers (Article 72) and performers (Article 73) may, if the infringement was intentional or negligent, recover, as justice may require, a monetary indemnity for the injury caused to them even if no pecuniary loss has occurred.

#### Article 97a of the German Copyright Act<sup>206</sup>

- (1) The infringed party shall remind the infringing party before he institutes proceedings against the latter and give him the opportunity to settle the issue by signing a cease-and-desist declaration with an appropriate penalty. Compensation for expenses can be demanded if the reminder was legitimate.
- (2) Damages for legal fees for a first reminder of an only insignificant infringement shall not exceed 100 Euro.

#### Article 98 of the German Copyright Act<sup>207</sup>

- (1) The injured party may require destruction of all copies manufactured, illegally distributed or intended for unlawful distribution that are in the possession or are the property of the infringer. Sentence 1 is applicable as well to the devices owned by the infringer that were mainly intended to produce copies.

---

<sup>204</sup> [http://www.gesetze-im-internet.de/urhg/\\_95d.html](http://www.gesetze-im-internet.de/urhg/_95d.html)

<sup>205</sup> [http://www.gesetze-im-internet.de/urhg/\\_97.html](http://www.gesetze-im-internet.de/urhg/_97.html)

<sup>206</sup> [http://www.gesetze-im-internet.de/urhg/\\_97a.html](http://www.gesetze-im-internet.de/urhg/_97a.html)

<sup>207</sup> [http://www.gesetze-im-internet.de/urhg/\\_98.html](http://www.gesetze-im-internet.de/urhg/_98.html)

- (2) Any person who infringes copyright or any other right protected by this law can demand the recall or the destruction of such illegally produced or distributed copies.
- (3) Instead of the measures provided for in section (1), the injured party may demand that all copies that are the property of the infringer be surrendered to him in return for equitable remuneration that may not exceed the cost of manufacture.
- (4) The measures under sections (1) and (2) are excluded when the measure is disproportionate in the individual case. The interests of third parties have to be considered.
- (5) Buildings as well as separable pieces of copies and measures that can be produced and distributed are not excluded under sections (1) until (3).

Article 101 of the German Copyright Act<sup>208</sup>

- (1) Any person who infringes copyright or any other right protected by this law for commercial purposes has to provide to the injured party information as to the origin and distribution channels of such copies, without delay. A commercial purpose may be the result of the number of infringements as well as its severity.
- (2) In cases of obvious infringement or in cases where the infringed party has filed a suit against the infringing party, the claim can, regardless of Sec. 1, also be brought against third parties who, in the course of business,
  1. had infringing copies in their possession,
  2. made use of infringing services,
  3. provides services used for an infringement or
  4. cooperated with a person who committed No.1, 2 or 3 and helped him with the production or distribution,

unless the person would have a right to refuse to give evidence in terms of Articles 383 to 385 of the German Civil Code of Procedure against the infringing party. In a claim pursuant to sentence 1, the court may abate legal proceedings against the infringer until the requested information is provided. The person who is obligated to give information can demand compensation for necessary expenses from the infringed party.
- (3) The person required to give information shall give particulars of
  1. the name and address of the manufacturer, the supplier and other prior owners of the copies, of the trade customer or of the principal, and
  2. of the quantity of copies that have been manufactured, dispatched, received or ordered, as well as the price paid for the copy.
- (4) Sec. 1 and 2 are excluded in case of disproportionality.

---

<sup>208</sup> [http://www.gesetze-im-internet.de/urhg/\\_101.html](http://www.gesetze-im-internet.de/urhg/_101.html)

- (5) In case the information provided is intentionally or grossly negligent wrong, the person who is obligated to provide the information is liable for all damages resulting thereof.
- (6) A person who has given information without being obligated to do so in terms of Sec. 1 or 2 is only liable towards third parties if he was aware of the fact that he did not have to do so.
- (7) In case an infringement is obvious, the obligation to provide information may be imposed by an injunction in compliance with Articles 935 through 945 of the German Code of Civil Procedure.
- (8) Such information may only be used in criminal proceedings or in proceedings under the law on minor offences against the person required to give information, or against a dependent person under Article 52 Sec. 1 of the Code of Criminal Procedure, in respect of an act committed before the information was given, with the consent of the person required to give the information.
- (9) In case provision of information requires the use of traffic data (Article 3 No.30 of the Telecommunications Act), a prior judicial notice about the admissibility of the use of the traffic data submitted by the injured party is required. The District Court where the person who is obligated to give the information has his residence, his domicile or a permanent establishment is admissible regardless of the amount in dispute. The Act on voluntary jurisdiction with the exception of Article 28 Sec. 2 and 3 is applied mutatis mutandis. Charges have to be paid by the injured party. Against the ruling of the District Court an appeal subject to a time-limit is admissible to the Higher Regional Court. It is only permitted when the decision is based on a violation of law. The ruling of the Higher Regional Court is incontestable. Further claims to information on personal information shall remain unaffected.
- (10) Sec. 1 in conjunction with Sec. 9 is a limitation of Article 10 of the German Constitution.

Article 108b of the German Copyright Act<sup>209</sup>

- (1) Anyone
  1. who intends to gain access to or provide access to a third party to a work protected by this law or any other object of protection protected by this Law or to facilitate the use thereof by circumventing an effective technological measure without the consent of the right holder
  2. knowingly and without authorization
    - a) removes or alters legal information originating from the right holder if any of the information concerned is affixed to a reproduction of a work or any other object of protection, or appears in connection with the public reproduction of such a work or object of protection.

---

<sup>209</sup> [http://www.gesetze-im-internet.de/urhg/\\_108b.html](http://www.gesetze-im-internet.de/urhg/_108b.html)

- b) distributes, introduces for the purpose of distribution, broadcasts, publicly reproduces or makes publicly available a work or any other object of protection in respect of which legal information was removed or altered without authorization.

and thereby causes, facilitates, enables or conceals the infringement of copyrights or other related protective rights to at least a slightly negligent extent,

shall, if the act is not performed exclusively for the own private use of the offender or persons personally associated with the offender or is related to such use, be punishable by up to one year of imprisonment or by fine.

- (2) Anyone manufacturing, introducing, distributing, selling or renting a device, a product or a part for commercial purposes in violation of Section 95a Sec. 3 shall also be punishable.
- (3) An offender acting for commercial purposes in the cases set forth in paragraph 1 shall be punishable by up to three years of imprisonment or by fine.





資料 B

現地報告書（米国編）

（英文）



Research Issues for Research and Study of Each Country's Legal Framework  
Concerning Technological Measures to Protect Contents

**United States**

**Part Two Research Issues (Inquiry Items)**

**1. International Rules**

***(1) Whether the research subject country is a party to any treaties that have provisions concerning technological measures to protect contents (e.g., WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty).***

The United States is party to the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) (collectively, the "WIPO Treaties"). Article 11 of the WCT and Article 18 of the WPPT ("Obligations concerning Technological Measures") provide that: "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

Article 12 of the WCT and Article 19 of the WPPT ("Obligations concerning Rights Management Information") provide that:

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

***(2) Whether the FTAs/EPAs to which the research subject country is a party include any provisions concerning technological measures to protect contents. If they are included, the substance thereof.***

Accession to the WIPO Treaties is a key term in most FTAs to which the United States became a party in the last decade, including FTAs with Australia, Bahrain, Chile, Jordan, Oman, Morocco, Singapore, Peru and the six Central American parties to CAFTA (Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras and Nicaragua).<sup>1</sup> NAFTA and the FTA with Israel were negotiated prior to the WIPO Treaties. As a result, those treaties do not incorporate accession terms or an explicit prohibition against the circumvention of technological protection measures. Nevertheless, NAFTA's intellectual property provisions demonstrate a commitment to provide comprehensive intellectual property protections.

The first FTA entered into after the passage of the DMCA was with Jordan. That FTA contained a brief general commitment to prohibit the trafficking of circumvention devices backed by both civil and criminal penalties.<sup>2</sup> However, the FTAs entered into since then, contain more detailed provisions regarding circumvention devices which largely mimic the provisions of DMCA legislation discussed further below. Annex 1 sets forth the relevant provisions of the FTA entered into with Australia, Korea (pending) and Singapore. There is generally little variation between the provisions of FTAs relation to the protection of technological measures. However, there are some differences worth mentioning:

The Chile FTA requires each party to prohibit the *knowing (or with reason to know)* circumvention of an access control or the trafficking of circumvention devices. The DMCA does not contain this qualification, instead prohibiting even unknowing circumvention of a technological measure. Thus the terms of the FTA differ slightly from what has been codified in the U.S. Like Chile, the Singapore and Australia FTAs also introduce a qualification that the user violates the prohibition of circumvention of technological measure only if he does so knowingly. The FTAs with Morocco, Bahrain, CAFTA, Oman, Peru, Korea, Panama, and Columbia, however, are consistent with the US DMCA and do not contain knowledge requirement to find a user liable for circumvention. The remainder of the provisions, however, largely parallel many of the exemptions from prohibition present in the DMCA such as periodic exemptions as promulgated by an administrative body, reverse engineering, encryption research, protection of minors, security measures testing, protection of personal information, law enforcement and educational institutions.

## **2. Laws of the Research Subject Country Concerning Technological Measures to Protect Contents**

---

<sup>1</sup> FTAs with Columbia, Korea and Panama are pending.

<sup>2</sup> Agreement between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area, U.S.-Jordan, Oct. 24, 2000 Article 4(13). ("In applying the prohibition under Article 11 of the WCT and Article 18 of the WPPT on circumvention of effective technological measures that are used by authors, performers and producers of phonograms in connection with the exercise of their rights and that restrict unauthorized acts in respect of their works, performances and phonograms, each Party shall prohibit civilly and criminally the manufacture, importation or circulation of any technology, device, service or part thereof, that is designed, produced, performed or marketed for engaging in such prohibited conduct, or that has only a limited commercially significant purpose or use other than enabling or facilitating such conduct.")

**(1) Laws concerning technological measures to protect contents. Whether there are any provisions of laws, rules, orders or the like that concern technological measures to protect contents in the research subject country. If so, the specific substance of the provisions of such laws, rules, orders or the like. If the originals thereof are not written in English, they should be translated into English.**

The Digital Millennium Copyright Act (DMCA),<sup>3</sup> enacted in 1998, significantly revised and amended the U.S. Copyright Act.<sup>4</sup> The key elements of the revisions with respect to anti-circumvention are addressed in Chapter 12 including Sections 1201 and 1202 to the Copyright Act which contain the following key prohibitions:

- A prohibition of the circumvention of a technological measure that effectively controls access (an “access control”) to a work protected under federal copyright law.<sup>5</sup>
- A prohibition of the manufacture, importation, offering to the public, provision or otherwise trafficking (collectively, “trafficking”) in any technology, product, service, device, component that (i) is primarily designed to circumvent an access control or a technological measure that protects a right<sup>6</sup> of a copyright owner (a “rights control”),<sup>7</sup> (ii) has limited commercial purpose other than circumvention of an access control or rights control<sup>8</sup> or (iii) is marketed for such purposes.<sup>9</sup>
- A prohibition of the removal or alteration of copyright management information (“CMI”).<sup>10</sup>

---

<sup>3</sup> Pub. L. No. 105–304, 112 Stat. 2860 (1998)

<sup>4</sup> 17 U.S.C. §§ 101-805, 1001-1332.

<sup>5</sup> 17 U.S.C. § 1201(a)(1)(A).

<sup>6</sup> The Copyright Act grants the exclusive right to owners of copyright to copy, perform, distribute, display, create derivative works of copyrighted works. 17 U.S.C. §106.

<sup>7</sup> 17 U.S.C. §§ 1201(a)(2)(A) and 1201(b)(A).

<sup>8</sup> 17 U.S.C. §§ 1201(a)(2)(B) and 1201(b)(B).

<sup>9</sup> 17 U.S.C. §§ 1201(a)(2)(C) and 1201(b)(C).

<sup>10</sup> 17 U.S.C. 1202 (b). The term "copyright management information" means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:

- (1) The title and other information identifying the work, including the information set forth on a notice of copyright.
- (2) The name of, and other identifying information about, the author of a work.
- (3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.
- (4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.
- (5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other

The provisions of Chapter 12 of Title 17 of the DMCA (17 U.S.C. §1200 – 1205) are set forth in Annex 2.

The practical effect of the DMCA has been an expansion of the scope of copyright in the U.S. by creating a claim for unauthorized access to works of authorship and makes distributors of circumvention products directly liable for actual or statutory damages.

It is important to note, that while the act of circumventing an access control is actionable under Section 1201, the act of circumvention of a rights control is not. For example, a measure that limits the ability of a user to copy of a work of authorship is a right control as copying is a right granted under copyright. Thus, a user who has legitimately acquired “access” to a work protected under copyright (i.e., has purchased a authentic copy), may make use of a circumvention method in order to copy a work or exercise any other copyright related rights and not violate Section 1201.

This omission was intentional as lawmakers recognized that acts of infringement, that is, exercising an exclusive right protected by the copyright act without authorization of the copyright owner, is already prohibited by Section 501 and the remainder of Chapter 5 of the Copyright Act which provides adequate remedies.<sup>11</sup> At the same time, the DMCA preserves the fair use exemption from claims of infringement.

Therefore a party that circumvents a rights control and who commits a purportedly infringing act, depending on the specifics of the circumventor’s use, is either liable under traditional infringement law or may fall under an exception such as fair use.<sup>12</sup> For example, if a rights control is circumvented and the circumventor then makes and sells unauthorized copies of that work in a manner that would infringe the owner’s copyright, then the circumventor-infringer would be liable under traditional provisions of the Copyright Act dealing with infringement but not under Section 1201. The drafters of the DMCA, however, also recognized that not all use of copyright related rights by a non-owner results in an infringement. Therefore, a user who circumvents a rights control may make fair use copies and not be liable under either Section 1201 or copyright law in general.

**(2) *Substance of restrictions provided for in such laws:***

---

identifying information about, a writer, performer, or director who is credited in the audiovisual work.

(6) Terms and conditions for use of the work.

(7) Identifying numbers or symbols referring to such information or links to such information.

(8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.

<sup>11</sup> 17 U.S.C. §§501-513

<sup>12</sup> 17 U.S.C. §107 (providing that “fair use” of a copyrighted work, including for purposes of criticism, comment, news reporting, teaching, scholarship or research does not infringe a copyright)

***(a) What are the technologies restricted by the laws? (Definitions and specific examples or the like of the restricted technologies, products and programs should be described.)***

The prohibitions in the DMCA are technology-neutral. The text does not specifically define or provide examples of restricted circumventing technologies.

***(b) What are the products and programs restricted by the laws? (Definitions and specific examples or the like of the restricted technologies, products and programs should be described.)***

Similarly, the provisions of the DMCA do not explicitly restrict specific products and programs. Rather, the provisions prohibit specific acts that may involve certain technologies, products (including computer programs), services, devices, components or parts thereof when used to circumvent access and rights controls (collectively, “circumvention products”). As explained above, the DMCA prohibits (i) the circumvention of the access controls of a work protected under federal copyright law and (ii) the trafficking of circumvention products.

The DMCA defines “circumvention” as “avoiding, bypassing, removing, deactivating or otherwise impairing a technological measure.”<sup>13</sup> A “technological measure controls access,” if the measure, “in the ordinary course of its operations, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to a work.”<sup>14</sup> A technological measure protects the rights of an owner of copyright if the measure, “in the ordinary course of its operations, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner.”

Courts have thus interpreted that for a technological measure to be “effective,” the plaintiff does not have to show that the measure prevents all access or that the method is particularly strong or foolproof.<sup>15</sup> Instead, the measure is evaluated with respect to the ordinary course of use of the protected work. However, the plaintiff seeking protection under Section 1201 must not defeat his own technological measure by making underlying content widely available without protection.<sup>16</sup>

The statute does not single out specific prohibited circumvention products. The text, however, provides the standards by which to measure whether a circumvention product falls under the provisions of Section 1201. The suspected circumvention product being trafficked must

---

<sup>13</sup> 17 U.S.C. §1201(a)(3)(A)

<sup>14</sup> 17 U.S.C. §1201(a)(3)(B)

<sup>15</sup> Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), judgment entered, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), aff'd on other grounds, 273 F.3d 429, (2d Cir. 2001) (court rejected the defendants' arguments that the weak cipher used by the plaintiffs did not effectively control access to the plaintiffs' copyrighted work).

<sup>16</sup> Agfa Monotype Corp. v. Adobe Systems, Inc., 404 F. Supp. 2d 1030 (N.D. Ill. 2005) (Embedding bits, which indicated font embedding licensing rights to other programs, did not “effectively control access” to a protected work because specifications for the fonts had been available for free download from the Internet, and embedding bits were not encrypted, scrambled or authenticated).

- 1) be primarily designed or produced for circumvention purposes prohibited by the DMCA;
- 2) have only limited commercially significant purpose or use other than to circumvent; or
- 3) be marketed for such circumvention purposes.

The DMCA is concerned with the trafficking and use of products that can circumvent (i.e. avoid, bypass, remove, deactivate or otherwise impair) a technical measure. Additionally, the drafters were also addressing, (and with respect to technological measures, effectively overruling) the rule established in the *Betamax* case.<sup>17</sup> Where the rule in *Betamax* allows for the trafficking in devices that could be used to infringe a copyright (e.g. an analog video recorder) when there are “substantial non-infringing uses” of the device, the DMCA requires a suspected unlawful circumvention avoid falling into three category of products. The first is with regard to the intent of the manufacturer, the second deals with the device’s actual or possible uses and the third is concerned with the manner in which the device is marketed to the public.

Where *Betamax* offered a way out for suspected products by only requiring a substantially non-infringing use, the DMCA provides three ways for a product to fall into a prohibited category. If a device or service is primarily designed for circumvention purposes, then it falls under the prohibitions of Section 1201. If the product was designed for other purposes unrelated to circumvention but the device does not have a significant commercial purpose other than to be used as a circumvention device, then it falls under the prohibitions of Section 1201. Thus, with respect to the second category of devices, the intent of the designer is irrelevant but the actual purposes the device is distributed and used for are what determine whether the device is prohibited. Finally, with respect to the third category, the sales and marketing activities of a distributor are relevant. Here a device may have been designed for non-circumvention purposes, it may also have significant commercial uses other than circumvention but nonetheless the device may be marketed as circumvention device. A good example of this would be an ordinary magic marker and the way they can be used at one time to circumvent a technological measure on music CDs.<sup>18</sup>

Case law has developed over the last ten years that illustrates how the prohibitions in the DMCA have been applied to various devices, software products and services.

Devices that allow an unauthorized user access to copyrightable content such as cable and satellite TV transmissions have presented little difficulty to

---

<sup>17</sup> Sony Corp of America v. Universal City Studios, 464 U.S. 417 (1984).

<sup>18</sup> Music CD’s contained certain technological measures to prevent a user from recording or “ripping” the content onto a computer hard drive. A student discovered that this measure was easily circumvented by taking an ordinary marker and marking the edges of the CD, which then allowed the CD to be ripped on to the memory of a personal computer. In applying Section 1201 to determine whether the marker is a possible prohibited circumvention device the breadth of the prohibition of the DMCA is seen. Markers are not designed for circumvention and have numerous other uses other than to be used as an anti-circumvention device. However, if, for example, a marker company began to market its markers as a tool that can be used to defeat the technological measure then such marketing could covert an ordinary marker into a circumvention devices prohibited by Section 1201.



courts in finding a violation of Section 1201.<sup>19</sup> In addition, devices that allow videogame players to modify the features of the game through the use of “game enhancers”<sup>20</sup> or modification chips that circumvent measures that prevent the use of pirated copies of videogames<sup>21</sup> have been found to violate Section 1201. In *Sony v. Gamemasters*, the “game enhancer” devices allowed users to (i) modify the rules of a game allowing a user to “cheat” by making the gamer easier to play by, for example, granting the user an infinite number of “lives” or unlimited ammunition, (ii) allowed users in the U.S. access to games exclusively sold in Japan or Europe and (iii) allowed users to play “backup” copies of the game DVD’s making bootleg or pirated copies playable on the plaintiff’s consoles.

The most high profile cases regarding Section 1201 to date involve software programs that circumvent DVD protection schemes.<sup>22</sup> These programs can decrypt the standard digital encryption scheme (known as “CSS”). Once decrypted the user can access or make infringing uses (e.g., copy) of the DVD’s content. Also falling within the scope of the DMCA are software programs that allow a user to capture streaming media in a protected format and copy such content to an unprotected format<sup>23</sup> enabling the use or reproduction of a copyrighted work beyond what the content owner has authorized (for example copy, burning, region controls, use controls which limit the number of times a work can be accessed).

Additionally, services that bypass the content owner’s own services and authentication schemes have also been the target of litigation. Again, videogame cases provide illustrative examples of services that violate the anti-circumvention provisions of the DMCA.<sup>24</sup> Both *Davidson & Associates v. Jung*<sup>25</sup> and *MDY*

---

<sup>19</sup> See e.g., *U.S v. Whitehead* 532 F.3d 991 (9<sup>th</sup> Cir. 2008), *DirecTV v. Borrow*, 2005 US Dist LEXIS 1328 (N.D. Ill. 2005); *Comcast of Ill. v. Hightech Electronics*, 2004 US Dist LEXIS 14619 (N.D. Ill. 2004); *DirectTV v. Ferguson*, 328 F.Supp2d 904 (N.D. Ind. 2004).

<sup>20</sup> *Sony Computer Entertainment America, Inc. v. Gamemasters* 87 F.Supp.2d 976 (N.D. Cal. 1999).

<sup>21</sup> *Sony Computer Entertainment America, Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 81 U.S.P.Q.2d 1045 (N.D. Cal. 2006).

<sup>22</sup> *RealNetworks, Inc v. DVD Copy Control Assoc., Inc.* 2009 WL 2475338 (N.D. Cal.) (Software at issue: Realnetwork’s RealDVD software which stored an image (copy) of the DVD’s content on a computer hard drive and allowed users to playback directly from the hard drive (without the original disc) and to copy the image on to a blank DVD disk) The case has also been known as *MCAA v. RealNetworks* originally filed in 2008, *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. Cal. 2004) (Software at issue: 321 Studio’s DVD Copy Plus and DVD-X Copy software which allowed users to make “back-up” copies of DVDs or copy a portion of the video content of a DVD onto blank media.), *Universal City Studios, Inc. v. Corley* 273 F.3d 429 (2<sup>nd</sup> Cir. 2001) (Software at issue: Defendant posted a link to the DeCSS software which decrypts the film industry’s standard DVD encryption technology).

<sup>23</sup> *RealNetworks, Inc. v. Streambox*, 2000 WL 127311 (W.D. Wash. 2000) (finding that program that allowed users modify plaintiff RealNetworks digital media software products and to capture protected streams of digital content removing copy protection controls violated Section 1201).

<sup>24</sup> *MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 616 F. Supp. 2d 958 (D. Ariz. 2009), *subsequent determination*, 2009 WL 649719 (D. Ariz. 2009). *Davidson & Associates v. Jung*, 422 F.3d 630 (8<sup>th</sup> Cir. 2005). This case is also known as the *Blizzard Entertainment v. “bnetd” programmer*.

*Industries, LLC v. Blizzard Entertainment, Inc.*<sup>26</sup> feature services that were an alternative to the authorized online gaming service provided by the game producer. Both services were found to be in violation of Section 1201 because they went beyond the mere hosting of online gaming but also allowed players with pirated copies to play the game by circumventing the game producer's authentication protocol.

Services that can violate the DMCA can also go beyond traditional notions of protectable content such as music or films. In *Ticketmaster v. RMG Technologies*,<sup>27</sup> the court agreed with plaintiff Ticketmaster and found that RMG most likely violated the DMCA. By "scrapping" the plaintiff's content, the defendant's service allowed users to circumvent Ticketmaster's access control over its website that sold tickets allowing users the ability to purchase multiple tickets simultaneously against the stated policy and controls Ticketmaster had put in place. Here the court treated the website and its functionality as a retail outlet of event tickets as protectable content as software.

The DMCA, however, has limits. Courts have also attempted to define the contours of what falls outside the protection of the anti-circumvention provisions of the DMCA. Most notably are two cases where the courts struggled to find prohibited acts. In both *Lexmark International v. Static Control Components*<sup>28</sup> and *Chamberlain Group v. Skylink Technologies*,<sup>29</sup> the plaintiffs attempted to leverage the newly enacted prohibitions in the DMCA to exert control over the aftermarket for spare parts and supplies. In both, the defendant manufacturer found a way to "circumvent" the plaintiffs' embedded software that blocked non-authorized replacement parts<sup>30</sup> from operating with the plaintiff's products. Employing slightly different rationales, both courts found that the DMCA did not cover the defendant's devices.

In *Lexmark*, the defendant Static Control Components (SCC), produced replacement microchips that enabled printer cartridge remanufacturers to refill laser toner cartridges and sell them more cheaply. Lexmark claimed that the chips circumvented Lexmark's access control technologies and infringed its copyrights by "reverse engineering" its printer toner cartridges in the course of developing its replacement chips. The copyrights in question were to Lexmark software contained on its toner cartridge chips. The court found that the underlying work that was used through circumvention of authentication protocols did not qualify for protection under copyright law. The printer software which operated the printing hardware was purely functional and not protected expression. The court distinguished the content of the printer software against video games, DVDs and concluded that the protocols did not control access but rather simply service to block operative elements of the hardware. Thus, the access controls were not a

---

<sup>25</sup> 422 F.3d 630 (8th Cir. 2005).

<sup>26</sup> 616 F. Supp. 2d 958 (D. Ariz. 2009).

<sup>27</sup> Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

<sup>28</sup> 253 F. Supp. 2d 943, 66 U.S.P.Q.2d (BNA) 1405 (E.D. Ky. 2003)

<sup>29</sup> Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 72 U.S.P.Q.2d (BNA) 1225 (Fed. Cir. 2004), cert. denied, 2005 WL 218463 (U.S. 2005).

<sup>30</sup> Printer cartridges in the case of *Lexmark* and garage door openers in the case of *Chamberlain*.

technological measure that protected access to a copyrightable work and therefore did not fall under the prohibitions of the DMCA.<sup>31</sup>

The court in *Chamberlain*, however, conceded that the plaintiff's garage door opener software was protectable but held that the purpose of the access control was not to protect against infringement but rather was intended to ensure plaintiff's control over the replacement parts market.<sup>32</sup> The court reasoned that Congress did not intend on creating a new property right with respect to protection of access to a work.<sup>33</sup> Rather the court believed lawmakers wanted to grant copyright owners additional remedies when copyrights are violated. Therefore, the court read into the DMCA's access control circumvention prohibition that the access control was placed to protect against possible infringement. This interpretation may be odds with the legislative history and seems to conflate access controls and rights controls by, in effect, giving protection to an access control only if it is intent to protect a rights under the Copyright Act. Legislative history seems to imply that Congress did intend to grant to copyright owners additional control over the use or "access" to content.<sup>34</sup>

***(c) What are the actions that are restricted by the laws? (All restricted actions should be described.) Specifically, explicit descriptions should be given as to whether the following are restricted actions:***

- (i) manufacture of circumvention devices or the like (including programs);***
- (ii) provision of circumvention devices or the like (including programs);***
- (iii) export and import of circumvention devices or the like (including programs);***
- (iv) possession of circumvention devices or the like (including programs);***
- (v) provision of circumvention services;***
- (vi) circumvention (reproduction by circumvention); and***
- (vii) dissemination of advertisements/information regarding circumvention devices or the like (including programs) or circumvention services or circumvention method.***

Except with respect to the class of works or certain exempted users,<sup>35</sup> Section 1201 expressly prohibits the trafficking of circumvention products. Mere possession of a circumvention product, even possession with some intent to

---

<sup>31</sup> Section 1201 prohibits circumvention of access controls to works "protected under this chapter [the Copyright Act]." Therefore, access to a work that is not copyrightable is not protected by Section 1201.

<sup>32</sup> *Chamberlain*, 381 F.3d at 1201. See also Aaron K. Perzanowski, Rethinking Anticircumvention's Interoperability Policy, 42 U.C. DAVIS L. REV. 101, 130 (2008).

<sup>33</sup> Copyright protects the right to copy, prepare derivative works, distribute, perform, display and publish. 17 U.S.C. §106.

<sup>34</sup> Ginsburg, Jane., *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience* (August 2005). Columbia Public Law Research Paper No. 05-93 at 15-16. Available at SSRN: <http://ssrn.com/abstract=785945>.

<sup>35</sup> See Section 3, *infra*.

distribute, is not prohibited. Importation of circumvention devices is explicitly prohibited and US customs may seize circumvention devices.<sup>36</sup> Exporting is not explicitly addressed but “offering to the public, provision and otherwise trafficking” are likely broad enough acts to also include exporting.

Advertisements regarding circumvention devices, services or methods may be construed, depending on the circumstances as “offering to the public.” For example, courts have found that simply linking to websites where a user can obtain a circumvention product is “trafficking” for purposes of Section 1201.<sup>37</sup> Whether the disclosure of instructions or information regarding a circumvention method is an “offer to the public,” “provision” or “otherwise trafficking” of a circumvention product has not been decided. In *Coupons, Inc. v. Stottlemire*,<sup>38</sup> an individual was sued for posting on a website forum a description of a method to circumvent plaintiff’s coupon printing software along with software that would apply such method of circumvention. The case, however, was settled leaving the questions presented concerning liability under the DMCA for such acts unanswered.

However, in 2001, encryption researchers who were about to publish a paper that described a method of circumvention, were threatened with legal action under the DMCA. The researchers then sued the content and digital encryption companies for declaratory judgment that their activities did not violate the DMCA. The case was dismissed but the content and encryption companies disavowed any intent to sue under the DMCA.<sup>39</sup>

Finally, courts have also determined that certain acts were not actionable under Section 1201 including, for example, the unauthorized use of a validly created username and password to access a computer system<sup>40</sup> and where certain blocking software malfunctioned allowing unauthorized user’s access to copyrighted content.<sup>41</sup>

### **(3) Exclusions**

**(a) Are any exclusions of application, exceptions, restrictive provisions or the like provided for in the provisions concerning technological measures to protect contents? If they are provided for, what is the specific substance thereof?**

#### *(i) Triennial Rulemaking*

The DMCA grants authority to the Register of Copyrights to recommend to the Librarian of Congress exemptions from the anti-circumvention provisions of

---

<sup>36</sup> See Section 4(c), *infra*

<sup>37</sup> See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

<sup>38</sup> 588 F. Supp. 2d 1069 (N.D. Cal. 2008).

<sup>39</sup> See [http://w2.eff.org/IP/DMCA/Felten\\_v\\_RIAA/](http://w2.eff.org/IP/DMCA/Felten_v_RIAA/)

<sup>40</sup> *Egilman v. Keller & Heckman, LLP.*, 401 F. Supp. 2d 105 (D.D.C. 2005), *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, 307 F. Supp. 2d 521 (S.D. N.Y. 2004)

<sup>41</sup> *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627 (E.D. Pa. 2007).

Section 1201 of the Copyright Act for users of certain classes of works. The drafters of the DMCA recognized that circumvention of a technological measure is often necessary in order for users of copyrighted works to use copyrighted material in a manner which under other circumstances would be infringing but were nonetheless lawful. For example, lawful acts under the doctrines of fair use (such as the copying of a copyrighted work for educational use) or reverse engineering (modification of code to allow for interoperability).<sup>42</sup> The exemptions, which were initially effective in 2000, are issued every three years and expire upon the issuance of the new exemptions. The following, promulgated in 2006, are the currently effective exemptions:<sup>43</sup>

1. Audiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.
2. Computer programs and videogames distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.
3. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.
4. Literary works distributed in E-book format when all existing E-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.
5. Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network.
6. Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely

---

<sup>42</sup> 17 U.S.C. §1201 (a)(1)(C).

<sup>43</sup> The current exemptions were set to expire on October 27, 2009 and a new set of exemptions were to be promulgated to be effective for another 3 year period. The Register of Copyright has not yet made its recommendations and thus issued an interim ruling on October 27, 2009, under which the current exemptions had been extended indefinitely although the Register was expected to make its recommendation shortly thereafter but as of the date of this report no further information is available. 74 Fed Reg 55138.

for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

Annex 3 offers a table that shows the development of the exemptions over each of the triennial rulemaking periods since the enactment of the DMCA.

*(ii) Reverse Engineering – Interoperability*

Courts have long recognized the benefits to consumers of allowing competitors to reverse engineer<sup>44</sup> each other's projects, so long as such reverse engineering does not otherwise infringe on a patent or other intellectual property right.<sup>45</sup> The DMCA thus exempts reverse engineering for the purposes of "interoperability" from the prohibitions in Section 1201.<sup>46</sup> The reverse engineering exemption in the DMCA is, however, limited by a narrow construction of "interoperability" which requires that (i) the circumvention be "for the sole purpose"

---

<sup>44</sup> Reverse engineering is the process of "starting with the known product and working backward to find the method by which it was developed." UNIF. TRADE SECRETS ACT § 1 cmt. 2 (amended 1985).

<sup>45</sup> See Aaron K. Perzanowski, Rethinking Anticircumvention's Interoperability Policy, 42 U.C. DAVIS L. REV. 101, 109 (2008). See also *Sega Entertainment Inc. v. Accolade, Inc.*, 977 F.2d 1510, 1527-28 (9th Cir. 1992) (holding that intermediate copying by defendant of plaintiff's copyrighted software was fair use and necessary to examine the unprotected parts of the software necessary to create its own programs that would interoperate with plaintiff's game console).

<sup>46</sup> 17 U.S.C. §1201(f) provides in relevant part:

**Reverse engineering.** (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

of interoperability and (ii) that such reverse engineering involve interoperability between computer programs.

To date, the reverse engineering defense has not been employed successfully against a DMCA related claim and few decisions have directly addressed the exemption.<sup>47</sup> In *Reimerdes*, the court first pointed out that the works which were being decrypted using the circumventing product distributed by the defendant (known as “DeCSS”) were films and not computer programs and thus did not qualify for the exemption offered by §1201(f).<sup>48</sup> The court also later interpreted a requirement under §1201(f)(3) that the person disseminating the circumventing product must be the same person who had performed the reverse engineering or had developed and employed the technological means to circumvent<sup>49</sup>

Subsequent court decisions that attempted to apply §1201(f) may have muddied the waters for further alleged authorized circumventors by misinterpreting the text of the statutes and congressional intent.<sup>50</sup> For example, in *Davidson & Associates v. Jung*<sup>51</sup>, the lower court appeared to read a consent requirement into the reverse engineering exemption. In addition, the court may not have properly weighed the defendant’s efforts to work with the copyright owner to prevent the use of their alternate online game platform by gamers who primarily used the services to play unauthorized copies of the game.<sup>52</sup>

### *(iii) Other codified exceptions*

Other exemptions codified in the Copyright Act include exemptions for non-profit libraries, archives and educational institutions solely to determine whether to acquire works,<sup>53</sup> law enforcement, intelligence and other government activities,<sup>54</sup>

---

<sup>47</sup> *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 323 (S.D.N.Y. 2000) (holding that the circumventions sole purpose be for purposes of interoperability). Surprisingly, the two cases dealing with physical goods, *Lexmark* and *Chamberlain* did not address the more obvious reverse engineering defenses. In both cases, however, the party who reversed engineered the plaintiff’s technological measure was not found to have violated the DMCA.

<sup>48</sup> *Reimerdes*, 82 F. Supp. 2d at 218.

<sup>49</sup> *Id* at 320.

<sup>50</sup> See generally *Perzanowski* at 133-141 (arguing that courts have not properly complied with Congress’ intent when it drafted 1201(f)).

<sup>51</sup> *Davidson & Associates v. Jung*, 422 F.3d 630 (8th Cir. 2005).

<sup>52</sup> *Perzanowski* at 139.

<sup>53</sup> 17 U.S.C. §1201 (d) provides in relevant part:

**Exemption for nonprofit libraries, archives, and educational institutions.** (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph--(A) may not be retained longer than necessary to make such good faith determination; and (B) may not be used for any other purpose.

encryption research,<sup>55</sup> circumvention to identify and disable technological measures that collect or disseminate personally identifying information<sup>56</sup> and circumvention to testing, investigate, correct security flaw or vulnerabilities.<sup>57</sup>

---

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

<sup>54</sup> 17 U.S.C. §1201 (e) provides in relevant part:

**Law enforcement, intelligence, and other government activities.** This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term “information security” means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.”)

<sup>55</sup> 17 U.S.C. §1201 (g) provides in relevant part:

**Permissible acts of encryption research.** Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work; (B) such act is necessary to conduct such encryption research; (C) the person made a good faith effort to obtain authorization before the circumvention; and (D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986

<sup>56</sup> 17 U.S.C. §1201 (i) provides in relevant part:

**Circumvention permitted.** Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if -- (A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected; (B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination; (C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and (D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

<sup>57</sup> 17 U.S.C. §1201 (j) provides in relevant part:

**Permissible acts of security testing.** Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.



**(b) In the case where any provisions concerning technological measures to protect contents are included in a copyright act, what are the relationships between provisions to prohibit circumvention of technological measures and rights restriction provisions?**

The DMCA's additions to the Copyright Act do not supersede any of the existing rights, remedies, limitations or defenses to copyright infringement, including fair use, that have been historically available under the Copyright Act.<sup>58</sup>

**(4) Remedial measures**

**(a) What are the civil and criminal remedies? (All remedial measures should be considered.) Specifically, consider focusing on whether any measures that respond to the following actions are provided for, and if they are provided for, describe the specific measures.**

- (i) manufacture of circumvention devices or the like (including programs);**
- (ii) provision of circumvention devices or the like (including programs);**
- (iii) export and import of circumvention devices or the like (including programs);**
- (iv) possession of circumvention devices or the like (including programs);**
- (v) provision of circumvention services;**
- (vi) circumvention (reproduction by circumvention); and**
- (viii) dissemination of advertisements/information regarding circumvention devices or the like (including programs) or circumvention services or circumvention method.**

For any violation of the prohibitions in §§1201 and 1202 of the Copyright Act, both civil and criminal penalties can apply. In addition to awarding actual damages, the court also has broad authority to grant injunctive and monetary relief including actual damages, profits and attorney's fees.<sup>59</sup> Repeat offenders may incur treble damages.<sup>60</sup>

A plaintiff, however, may elect to seek statutory damages instead of actual damages, for each violation of §1201 of \$200-\$2500 per act of circumvention, device, product, component, offer or performance of service.<sup>61</sup> Similarly, an injured claimant may seek statutory damages of \$2500-\$25,000 per violation of §1202 (removal of CMI).<sup>62</sup>

---

<sup>58</sup> 17 U.S.C. §1201(c). *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004) (Holding that DMCA granted copyright holders additional legal protections, but neither rescinded the basic bargain granting the public noninfringing and fair uses of copyrighted materials, nor prohibited various beneficial uses of circumvention technology, such as those exempted under the Act).

<sup>59</sup> 17 U.S.C. §1203(b) and (c)

<sup>60</sup> 17 U.S.C. §1203(c)(4)

<sup>61</sup> 17 U.S.C. §1203(c)(3)(A)

<sup>62</sup> 17 U.S.C. §1203(c)(3)(A)

Criminal penalties may follow if the violations are found to be willful and for commercial or private financial gain. Criminal fines may range from maximums of \$500,000 or \$1,000,000 or imprisonment for up to 5 years for a first offense or 10 years for subsequent offenses.<sup>63</sup>

The penalty provisions of the DMCA are similar to what the Copyright Act provides for acts of infringement. In addition to actual damages, disgorgement of profits and attorney's fees, the Copyright Act allows for statutory damages. Statutory damages are computed for every work that is infringed and the court can award anywhere from \$750 to \$30,000 as it sees just. In cases of willful infringement the award can reach as high as \$150,000 per work. Conversely, in cases of inadvertent infringement the award could be reduced to \$200 or in some cases refrain from awarding any amount if the defendant can prove it had reasonable grounds for believe that the infringing use was a fair use and the defendant was working on behalf of an educational institution or a public broadcaster. The Copyright Act also provides criminal penalties for willful infringement ranging from imprisonment up to 5 years and fines up to \$250,000.<sup>64</sup>

**(b) Who is capable of requesting the remedial measures set forth in (a) above?**

Any person injured by the circumvention may exercise a civil claim under Chapter 12 of the Copyright Act.<sup>65</sup> A plaintiff alleging a violation of the DMCA's anti-circumvention provision must prove: (1) ownership of a valid copyright<sup>66</sup> on a work (2) effectively controlled by a technological measure, which has been circumvented (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.<sup>67</sup> Criminal prosecution is not dependent on a petition of any person.

**(c) Are there any border measures pertaining to export and/or import of violational devices or the like, or any administrative measures to deter violation provided for? If they are provided for, what is the specific substance of the measures?**

While counterfeit goods including DVDs, videogames, CDs are frequently the subject of seizures, circumvention devices are not specifically targeted by US

---

<sup>63</sup> 17 U.S.C. §1204(a)

<sup>64</sup> 17 U.S.C. §506, 18 U.S.C. §2319

<sup>65</sup> Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 55 U.S.P.Q.2d (BNA) 1873 (S.D.N.Y. 2000), judgment entered, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), aff'd on other grounds, 273 F.3d 429, 60 U.S.P.Q.2d (BNA) 1953 (2d Cir. 2001), RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D. Wash. 2000))

<sup>66</sup> It is also likely that an exclusive licensee of a copyright could show sufficient injury to be able to bring a claim.

<sup>67</sup> Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096 (C.D. Cal. 2007), Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004).

customs regulations. In 2004, the Bureau of Customs and Board Projection published a proposed rule to explicitly include provisions for the detention and seizure of articles that violate §1201 of the DMCA, however, to date this rule has not been made final and the accompanying amendments have not been made to the U.S. Code.<sup>68</sup> The Bureau has nonetheless implemented the prohibitions of the DMCA through internal enforcement guidelines, which provide that devices that violate the DMCA are subject to search and seizure under current law as such devices fall under the general power of the U.S. Customs Agency to seize articles that violate the Copyright Act.<sup>69</sup>

**(5) Restrictions on so-called “non-reacting devices.” Whether there are any restrictions provided for by way of laws, rules, orders, or the like against so-called “non-reacting devices,” which are devices that do not detect protective technological measures (i.e., copy protect signals and access protect signals) attached to contents, and allow copying of contents and replaying of unlawful reproductions as a result. If so, the specific restriction clauses. Describe the substance of any such restrictions.**

Non-reactive devices are not explicitly addressed by the DMCA nor, to our knowledge, by any court decisions. However, the standard of prohibited device does not distinguish by the method of circumvention. Such devices may violate § 1201 if they

- 1) are primarily designed or produced for circumvention purposes prohibited by the DMCA;
- 2) have only limited commercially significant purposes or use other than for such circumvention purposes; or
- 3) are marketed for such circumvention purposes

Thus any device that renders an effective technological measure inactive whether by overriding or actively counteracting a technological measure or by simply ignoring it would still be a circumvention device. However, once digital information is converted to a human-perceptible (analog) form, it is a relatively simple matter to digitally recapture that analog reproduction without violating Section 1201. Since the conversion to analog signals is part of the intended operation of digital playback devices, recapturing the content is not a circumvention of the technological measures intended to protect the content from unauthorized use. This is known as the “analog hole” in digital protection schemes. This has led to legislation to mandate that certain playback devices be manufactured with certain content protection technologies to prevent exploitation of the analog hole. Analog devices that do not have these features which may be considered “non-reactive” devices are addressed in DMCA Section 1201(k) which makes it unlawful

---

<sup>68</sup> Recordation Of Copyrights And Enforcement Procedures To Prevent The Importation Of Piratical Articles, 69 Fed. Reg. 59562 (October 5, 2004)

<sup>69</sup> *Id.*, 19 U.S.C. 1595a(c)(2)(C) (Providing that “[m]erchandise may be seized and forfeited if . . . it is merchandise . . . in which . . . copyright . . . violations are involved . . .”) [

to traffic in certain analog devices such as video recorders without conforming to certain copy protection technologies.<sup>70</sup>

Similarly, the Audio Home Recording Act of 1992 introduced Chapter 10 into the Copyright Act<sup>71</sup> and deals with digital audio recording devices which are devices designed or marketed for the primary purpose of, and that is capable of, making a digital audio copied recording for private use. Chapter 10 mandates that such digital audio recording devices conform to the Serial Copy Management System (SCMS) and that royalties be paid to content owners by manufacturers of such devices and the blank media used by consumers to make records.

The provisions of the Audio Home Recording Act are somewhat anachronistic today as the vast majority of home recording is done through home computers on to hard drives which are not considered “digital audio recording devices” as they are not primarily designed or used for audio recording. In addition, MP3 playback devices were found in *RIAA v. Diamond Multimedia Systems, Inc*<sup>72</sup> to be excluded from the definition of digital audio recording devices. In 2002, the Consumer Broadband and Digital Television Promotion Act<sup>73</sup> was proposed which would have overruled the *Diamond* decision and mandated additional measures to address the analog hole but the bill has not progressed since its introduction and is being considered at this time.

In, *Macrovision v. Sima Products Corporation*,<sup>74</sup> Macrovision sued Sima to block the sale of the Sima CopyThis! and GoDVD products, which are designed to digitize analog video, such as the analog video outputs of DVD players and analog VCRs. The Macrovision Analog Copy Protection signals often embedded in these analog outputs, however, do not survive the digitizing process, and therefore are not embedded in the outputs of the Sima devices. Macrovision argued that this violates the DMCA's prohibition on circumvention. While the court granted a preliminary injunction, Sima and Macrovision settled their dispute before the appeal could be decided, leaving for undecided whether Macrovision's analog signals qualify for DMCA protection.

### **3. Data Regarding Precedents, Enforcement Status, Damage Status, Etc.**

#### **(1) Precedents relating to technological measures to protect contents.**

The following are among the most significant judicial decisions interpreting the DMCA since its enactment in 1998:

---

<sup>70</sup> Generally, the DMCA mandates that analog video recording conform to the “automatic gain control” and the “four-line colorstripe” copy control technologies. 17 U.S.C. §1201(k)(1).

<sup>71</sup> 17 U.S.C. §§1001-1010.

<sup>72</sup> 180 F.3d 1072 (9th Cir. 1999).

<sup>73</sup> 107th Congress, 2nd session, S. 2048.

<sup>74</sup> 2006 WL 1063284.

- i. Sony Computer Entertainment America, Inc. v. Gamemasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999)

**Content:** Videogame

**Device:** “Game Enhancer” device that allowed users to play games imported from other territories.

**Facts:** The “game enhancer” devices allowed users to (i) modify the rules of a game allowing a user to “cheat” by making the gamer easier to play by, for example, granting the user an infinite number of “lives” or unlimited ammunition, (ii) allowed users in the U.S. access to games exclusively sold in Japan or Europe and (iii) allowed users to play “backup” copies of the game DVD’s making bootleg or pirated copies playable on the plaintiff’s consoles. Plaintiff sought a preliminary injunction against the sale of such devices.

**Holding:** The court held that the plaintiff would likely prevail in its claim that Game Enhancer device was a circumvention product whose primary function was to circumvent a technological measure that control access to a work and thus granted a preliminary injunction. This early decision confirmed the notion that access controls intended to protect against use “region encoded” content was protected under the DMCA even though the ability to geographically limit a bona fide purchaser’s access to a work he had purchased is not among the rights granted to copyright owners under the copyright right act.

- ii. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D. N.Y. 2000)

**Content:** Motion picture DVDs

**Device:** Software (“DeCSS”) that decrypted digitally encrypted movies on DVD

**Facts:** Defendant’s website began to offer the DeCSS software through links to other websites which allowed for download of the DeCSS software. Defendants claimed that the purpose of such software was not to pirate DVD but rather to allow playback through DVD drives installed in systems operating under the Linux operating system. Defendants also claimed that use of the software for uses protected under fair use doctrine was not prohibited.

**Holdings:** The court reject the Linux and fair use arguments. The Linux argument failed as none of the statutory exemptions applied to such circumventive purposes. For example, the reverse engineering exemption did not apply as the interoperability sought with respect to Linux computers related to access to film content and not “computer programs.” The court dismissed “fair use” by stating the DMCA did not include an express “fair use” exemption and distinguished the *Betamax* case from the present one as being inapplicable as *Betamax* did not deal with circumvention of technological measures. The court thus decided that (1) posting decryption software violated the DMCA provision prohibiting trafficking in technology that circumvented measures controlling access to copyrighted works; (2) posting hyperlinks to other web-sites offering decryption software violated the DMCA; (3) the DMCA anti-trafficking provision was content-neutral as

applied to computer program; (4) the DMCA did not violate First Amendment as applied to defendants and decryption software; (5) defendants failed to establish anti-trafficking provision was overly broad on grounds that it prevented noninfringing fair use of movies; (6) application of anti-trafficking provision to enjoin defendants from hyper-linking to other web-sites offering decryption software did not violate First Amendment; and (7) plaintiffs were entitled to injunction enjoining defendants from posting decryption software or hyperlinking to other web-sites that made software available.

- iii. Real Networks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D. Wash. 2000)

**Content:** Steaming Digital Media

**Devices:** Software programs (Streambox VCR, the Ripper, and the Ferret ) that allow user to record streamed audio and video by circumventing the plaintiff's access and rights controls, covert from one digital format to another and modify the plaintiff's software search functionality.

**Facts:** Defendant's software mimicked the plaintiff's RealPlayer software, fooling plaintiff's service to stream content without copy protection.

**Holding:** Parts of the defendant's software violated the DMCA. However, the court also held that, digital formats are not in of themselves a technological measure without some evidence that the format is used to effectively protect an access or a right control.

- iv. U.S. v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002)

**Content:** E-books

**Device:** Software that allows user to make copies, access E-books on different hardware and print the underlying text.

**Facts:** Defendant, a Russian software company based in Moscow, sold a software product called the "Advanced eBook Processor" which removed use restrictions from Adobe Acrobat PDF files and files formatted for the Adobe eBook Reader. This allowed for use of the files in non-Adobe eBook reader programs and stripped away the controls that prevented copying and printing. Adobe complained to the US authorities and the Defendant was indicted by the US government for alleged violations of the DMCA. Defendant appealed the indictment and argued that the First Amendment exempted the use of the software.

**Holdings:** The court upheld the indictments holding that (1) the DMCA anti-circumvention provision is not unconstitutionally vague; (2) Defendant's software contained expression, thus implicating First Amendment; (3) To the extent that the DMCA targets computer code, Congress sought to ban the code not because of what the code says, but rather because of what the code does, and therefore, the DMCA's restriction on speech is content neutral, and subject to intermediate scrutiny; (4) the DMCA is not unconstitutional restriction of speech, under intermediate scrutiny test; (5) the DMCA is not unconstitutionally overbroad; (6) the DMCA does not violate

intellectual property clause. (Note: Adobe eventually dropped its complaint but the government continued its prosecution. At trial, the jury acquitted the Defendant of the charges.)<sup>75</sup>

- v. Lexmark Intern., Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004)

**Content:** Software embedded into plaintiff's printer hardware which controlled the loading of toner.

**Device:** Computer chip used in third-party remanufactured toner cartridges to mimic microchip contained in manufacturer's toner cartridges,

**Holdings:** (1) Manufacturer failed to show likelihood of success on merits of claim that seller's computer chip violated the DMCA by circumventing authentication sequence used by manufacturer's printers; manufacturer failed to show likelihood of success on merits of claim that seller's computer chip violated the DMCA by providing access to manufacturer's toner loading program; and (2) manufacturer failed to show that seller did not satisfy the DMCA's interoperability defense.<sup>76</sup>

- vi. Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004), cert. denied, 2005 WL 218463 (U.S. 2005)

**Content:** Software embed in plaintiff's garage door hardware.

**Device:** Universal remote control which circumvented plaintiff's code which prevented operation of the hardware with a remote control not supplied by plaintiff.

**Holding:** Defendant's universal transmitter did not violate the DMCA's anti-circumvention provision.<sup>77</sup>

- vii. 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004)

**Content:** Motion Pictures

**Device:** Software for copying digital versatile discs (DVDs)

**Holdings:** (1) Software violated anti-circumvention provisions of the DMCA, and (2) anti-circumvention provisions of the DMCA were constitutional.

- viii. Sony Computer Entertainment America, Inc. v. Divineo, Inc., 457 F. Supp. 2d 957 (N.D. Cal. 2006)

---

<sup>75</sup> Russian Company Cleared Of Illegal Software Sales, N,Y, TIMES, December 18, 2002, at C4, available at <http://www.nytimes.com/2002/12/18/business/technology-russian-company-cleared-of-illegal-software-sales.html?pagewanted=1>. The software developer, Dimitry Sklarov, was arrested and also charged individually with criminal violations of the DMCA, however, all charges were dropped against Mr. Sklarov in exchange for his testimony. <http://www.freesklyarov.org/>

<sup>76</sup> Lexmark is discussed in Section 2(b), supra.

<sup>77</sup> Chamberlain is discussed in Section 2(b), supra.

**Content:** Videogames

**Device:** HDLoader program which allows users to save a copy of a playstation video gram from the CD-Rom to a hard drive and “mod chips” which allows users to circumvent plaintiff’s authentication technology.

**Holdings:** (1) seller of circumvention devices violated the DMCA by trafficking in devices that were primarily designed or produced for the purpose of circumventing a videogame system's authentication system which otherwise controlled access to software played on the system, including copyright holder's own copyrighted videogames; (2) statutory award for violations of the DMCA would be enhanced to \$800 per violation on the grounds that violator failed to respond fully in discovery and that his violations of the DMCA were willful; and (3) award of costs and attorney fees was appropriate.

- ix. Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005)

**Content:** Videogames

**Device:** Alternative videogame service software.

**Facts:** BnetD was an open source program that let gamers play popular Blizzard titles like Warcraft with other gamers on servers that don't belong to Blizzard's Battle.net service.

**Holding:** Defendants' development of alternative service violated the DMCA's anti-circumvention and anti-trafficking provisions.

The case is being appealed and could on review provide an opportunity to clarify the DMCA’s reverse engineering exemption.

- x. MDY Industries, LLC v. Blizzard Entertainment, Inc., 616 F. Supp. 2d 958 (D. Ariz. 2009)

**Content:** Videogames

**Device:** A “bot”<sup>78</sup> program named “Gilder” which modified the plaintiff’s online game, World of Warcraft, by allowing players to automate the gameplaying portions of the game.

**Facts:** Through the use of defendant’s Gilder program, users avoided detection by plaintiff’s server side program “Warden” that would reveal use of the unauthorized “bot” program in contravention of the End-User License Agreement between Blizzard and the gamers.

**Holdings:** The court distinguished between elements of the game maintained on the Plaintiff’s services which the “Warden” program controlled access to and the portions of the program that resided on the user’s hard drive and Warden did not control. The court found that “Warden” was a technological measure which controlled access to the elements of a copyrightable work accessible only through the server. The court also found that the defendant’s President could be

---

<sup>78</sup> For example, a “bot” will allow a player to leave his computer unattended while the “bot” software played the game in his stead. This would enable a player to collect points or other in-game benefits without having to actually spend the hours devoted to the game.



held personally liable for corporation's tortious interference of contract that the company had with its customers; and was liable for corporation's vicarious copyright infringement, contributory copyright infringement, and the DMCA violations. This case is pending appeal.<sup>79</sup>

- xi. Real Networks, Inc v. DVD-Copy Control Association, 2009 WL 2475338.

**Content:** Motion Pictures

**Device:** Software product which allows copying of content of DVDs

**Facts:** Defendant's RealDVD software which was designed to allow consumers to copy their DVDs to their computers for later playback. Real also had intended to launch a line of consumer electronics devices that would have combined a DVD player with a hard drive. Real had obtained a license from DVD-CCA for its products. Internally the project was known as "Vegas" as in "what happens in Vegas, Stays in Vegas" which give evidence of what the most significant use (unauthorized copying of DVDs) of the product would be for most users.

**Holdings:** The judge concluded that the RealDVD products were not authorized by the DVD-CCA license agreements, and that Real had violated the DMCA's ban on trafficking in circumvention devices when it distributed the RealDVD products. The software product violated access-control provision of the DMCA and it violated copy-control provision of the DMCA.

**(2) Enforcement status relating to technological measures to protect contents.<sup>80</sup>**

Content owners have been quite active in enforcing their rights under the DMCA. Not all disputes result in litigation. Often, simply the threat of action, communicated through a cease and desist notice, has been effective in deterring acts that would violate the anti-circumvention provisions.<sup>81</sup> A search on Westlaw reveals that to date, over 100 cases have referenced the anti-circumvention provisions of the DMCA.

While the DMCA contains criminal penalties, there have been very few high profile criminal prosecutions under the Section 1201. In U.S. v. Elcom Ltd.,<sup>82</sup> a Russian computer scientist, Dmitry Sklyarov, was arrested, jailed for three weeks

---

<sup>79</sup> One potential avenue for appeal lies in Section 117 of the copyright act would allow the type of infringement at issue in this case. 17 U.S.C. §117 ("it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided: (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner...").

<sup>80</sup> Statistical information not readily available.

<sup>81</sup> Examples of such cease and desist letters can be found at <http://www.chillingeffects.org/anticircumvention/notice.cgi>

<sup>82</sup> 203 F. Supp. 2d 1111 (N.D. Cal. 2002)

and prosecuted for trafficking a program that decrypted Adobe E-books. The charges against Sklyarov were eventually dropped in exchange for cooperation with a prosecution of Sklyarov's employer Elcom under §1201. The company, however, was acquitted.<sup>83</sup> In *U.S. v. Whitehead*, the defendant was sentenced to 1,000 hours of community service and 5 years of supervised release and restitution of \$50,000 and in a separate case, Mohsin Mynaf was sentenced to 24 months and order to pay over \$200,000 for violating Section 1201.<sup>84</sup>

**(3) Damage status relating to technological measures to protect contents (Include statistical data if any. Hearings or the like should be conducted in the research as appropriate.)<sup>85</sup>**

There have only been a handful of cases where a court has calculated statutory damages under the DMCA. The easiest cases involve the sale of physical devices. In *Sony Computer Entertainment American, Inc. v. Fililpiak*,<sup>86</sup> the court applied an amount within the statutory range to the total number of units sold taking into account the expenses saved by not having to obtain a license agreement, the revenues lost by the plaintiff and the defendant's intent and willfulness totaling over 6 million dollars of damages.<sup>87</sup>

#### **4. Research on Technological Trends**

**(1) Technologies that are currently used pertaining to technological measures to protect contents. (Information should be assembled according to category.)**

Please see the discussion in the report for the European Union.

---

<sup>83</sup> See note 75, *supra*

<sup>84</sup> *U.S. v. Whitehead* 532 F.3d 991 (9<sup>th</sup> Cir. 2008), dealt with the sentencing of the Defendant, Mr. Whitehead, who was convicted for the purchasing, sale and distribution of software code necessary to reprogram DirecTV access cards. The access cards allowed users to access the DirecTV feed without paying the subscription fee. Mr. Whitehead paid a co-conspirator to continually update the software to circumvent the latest DirecTV security measures and collected \$400,000 from the sale of counterfeit DirecTV access cards worth over one million dollars. <http://www.justice.gov/criminal/cybercrime/whiteheadConviction.htm>.

*U.S. v. Mynaf* (E.D. Cal.), involved more than 4,500 bootlegged videotapes found in Defendant Mynaf's residence and in a facility he rented. Federal agents discovered a movie videocassette reproduction lab with equipment used to manufacture counterfeit movie videocassettes and labels. The equipment included approximately eighteen videocassette recorders, equipment used to bypass videocassette copyright protections, and printers. Mr. Mynaf, who plead guilty to the charges, utilized some of the equipment, including the SIMA Video Copy Master, to circumvent a technological measure that effectively controls access to copyrighted works. <http://www.cybercrime.gov/mynafSent.htm>.

<sup>85</sup> Statistical information not readily available.

<sup>86</sup> 406 F. Supp. 2d 1068 (N.D. Cal. Dec. 27, 2005).

<sup>87</sup> *Id.* at 1075.

**(2) Whether there are any new technologies pertaining to technological measures to protect contents, such as digital watermarking. If any, the nature thereof. (Information should be assembled according to category.)**

A technological measure that has been on the verge of adoption is the “broadcast flag.” This is information embedded into the data stream of a digital television program which can set the parameters on the ability for consumers to record and playback the program. For example, a program can be aired with parameters that would prevent a digital video recorder (DVR) from recording the program for viewing at a later time. Similarly, the broadcast flag can allow for recording but can set limits on the ability of the view to replay the broadcast. The flag can allow, for example, only a fix number of playbacks or will only allow playback up to a certain date.

In 2005 the Federal Communications Commission (FCC) issued a ruling which compelled manufactures of HDTV’s to provide for the broadcast flag.<sup>88</sup> However, in *American Library Association v. FCC*,<sup>89</sup> the court ruled that the FCC had exceeded its authority in promulgating the rule. To date, no similar rule has been issued but broadcasters continue to lobby for it and equipment manufacturers and broadcasters are free to otherwise implement such a protocol.

Please also see the discussion in the report for the European Union.

**(3) Whether laws are succeeding in covering the technologies pertaining to technological measures to protect contents that are currently used and to new technologies.**

As a result of the technology-neutral manner in which they are drafted, the anti-circumvention prohibitions of the DMCA will continue to cover new technological measures and the circumvention technologies that arise to defeat them. However, if success of the DMCA were to be measured by asking whether it has eliminated or significantly reduced piracy of copyrighted works, then most observers would agree that the anti-circumvention laws have not succeeded. Nonetheless, the protections of the DMCA have most likely served simultaneously as a deterrent to mass infringement and has also provided a fostering environment for new products and services by content providers.

First as deterrent, the DMCA has successfully prevented large companies from marketing goods that are found to be subject to the prohibitions of Section 1201. The best example is Real Network’s RealDVD. As a result of the ruling in *Real Networks v. DVD Copy Control Association*,<sup>90</sup> a major player in the digital media space has had to alter its business plans and incurred significant costs in litigating the matter.

---

<sup>88</sup> 47 CFR 73.9002(b).

<sup>89</sup> 406 F.3d 689 (D.C. Cir. 2005).

<sup>90</sup> 2009 WL 2475338.

However, obtaining programs that provide the same functionality, as RealDVD is not difficult. If a user is interested enough, the tools need to decrypt a DVD access control is not more than an Internet search away. Coupled with the continued availability of file sharing platforms, digital piracy will continue to be a significant issue.

Second, the protections afforded by the anti-circumvention provisions of the DMCA, have provided some cover for large content providers to experiment with new business models and modes of distribution. Thus, the ability to view or purchase programs through online services like iTunes, Hulu or the individual online presences of the broadcast networks, is to some extent supported by the protections (if perhaps illusory) of the DMCA.

## **5. Controversy within the Country**

### ***(1) Arguments against restrictions concerning technological measures to protect contents made within the country. Additionally, what arguments have been made in relation to information access rights and the right to know?***

The anti-circumvention provisions of the DMCA have withstood challenges based on first amendment freedom of speech,<sup>91</sup> Commerce Clause, Intellectual Property Clause<sup>92</sup> and fair use.<sup>93</sup>

While proponents of the DMCA have argued that the act was necessary to allow copyright law to catch up to the technological changes that have threatened to undermine the content industries, others believe that the anti-circumvention provisions of the DMCA have upset the balance between content owners and consumers.

#### *Fair Use*

Copyright law, up until now, concerned itself with most public performances and large level piracy. The concerns of the content industries, because of the widespread availability of peer-to-peer networks or other file swapping services, are now much more focused on “private” performances and individual copying. This focus and new restrictions on private performance threatens the viability of a number of doctrines that have up until now allowed private enjoyment of content while at the same time addressing infringements acts that were more likely to inflict significant damage.

The lynchpin of the fair use doctrine with respect to private copying was the famous “Betamax” case.<sup>94</sup> The court held that so long as products such as VCR’s had substantial non-infringing uses, the makers of such products could not be held

---

<sup>91</sup> Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 55 U.S.P.Q.2d (BNA) 1873 (S.D.N.Y. 2000), judgment entered, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), aff’d on other grounds, 273 F.3d 429, 60 U.S.P.Q.2d (BNA) 1953 (2d Cir. 2001)

<sup>92</sup> U.S.C. Const. Art. 1, § 8, cls. 3, 8; 17 U.S.C.A. § 1201(a)(2), (b)(1). 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004), U.S. v. Elcom Ltd., 203 F. Supp. 2d 1111, 62 U.S.P.Q.2d (BNA) 1736 (N.D. Cal. 2002)..

<sup>93</sup> Universal City Studios, Inc. v. Corley, 273 F3d 429 (2d Cir. 2001)

<sup>94</sup> Sony Corp of America v. Universal City Studios, 464 U.S. 417 (1984).

liable for the infringing actions of user of such products. Since uses such as “time shifting” (i.e. recording a video program for later viewing at more convenient time) were deemed fair use, the plaintiff’s suit against a maker of a device that may also be used to infringe was not liable for contributory infringement. The DMCA turns that ruling a bit on its head by outlawing devices or products whose “primary purposes” is to circumvent, regardless of whether such circumvention product was also used for non-fringing purposes. Through the creation of a new type of “infringement” (i.e., circumvention), content owners can effectively cut off all ability for the public to make fair use of the works.

### First Sale

Another long accepted doctrine that the DMCA threatens to overturn is the first sale doctrine. The first sale doctrine allows a purchaser of a copy of work of authorship to access that work whenever, and how often, the purchaser would like. Thus, the purchaser of a book can read it, once, twice or ten times, without asking the content owner for permission. This reader can also lend the book to a friend anywhere in the world, again, without asking for the copyright owner’s consent. The rationale is that the owner’s right over that specific copy is “exhausted” after that first sale.

Digital media, however, allows content owners to exert control over of the use of copies of works beyond what was technically possible or allowed under the first sale doctrine. Content owners can now sell works with limited rights to access. An early example of this type of control is region encoding. DVDs that are intended for sale in Europe are not playable in the United States and vice versa. However, it was typically not illegal for a consumer to purchase content in one country yet intend to use it in another. The DMCA now has made this a violation and perhaps a crime. The region code of a DVD is essentially an access control and any circumvention of that control in order to have access (i.e., watch) the DVD could violate the DMCA even when the user has obtained a legitimately authorized copy.

### Anticompetitive behavior

Finally, some commentators question whether the DMCA has strengthened the ability of content owners to engage in anticompetitive behavior. The use of technological measures to discourage lawful competition hurts consumers by limited choice and, in the end, limiting continued technological progress by helping establish enterprises with excessive market power.

For example, Apple’s stranglehold on the online music player and online retail markets are, in part, due to the difficulty in other formats to play on the hardware devices or for other hardware devices to play Apple’s proprietary format. In 2004, Real Networks created a product called Harmony, which attempted to bridge the gap by making the Real Networks’ audio format playable on the iPod. This ability would be a boon for Real Networks’ effort in getting its Rhapsody online music subscription and retail service off the ground.

Apple responded strongly by accusing Real Networks of using the “tactics and ethics of a hacker”<sup>95</sup> in creating its product and threaten to enforce Section 1201 of the DMCA. Even though reverse engineering is generally encouraged as a matter of policy, the narrow scope of the Section 1201(f) exemption and content owner-

---

<sup>95</sup> Andrew Stein, Apple: RealNetworks hacked iPod, CNN Money July 29, 2004, [http://money.cnn.com/2004/07/29/technology/apple\\_real/](http://money.cnn.com/2004/07/29/technology/apple_real/)

friendly precedents ultimately persuaded Real Networks to abandon its efforts to make its format compatible.

**(2) Status of request from industries against restrictions concerning technological measures to protect contents. (Are they satisfied with the current provisions mentioned above or would they prefer more or less restrictive provisions? This may vary depending on the industry. Can be analyzed according to each industry area).**

The content industries are, as expected, proponents of the provisions. The MPAA (Motion Picture Association of America) and the RIAA (Recording Industry Association of America) were among the strongest supporters of the legislation and continue to push for its enforcement. The MPAA has lobbied for DMCA-type legislation at the state level<sup>96</sup> and the RIAA has made headlines suing private individuals.

The music industry, however, recently seems to have taken a different route. While, DVD are still protected from unauthorized copying through encryption methods such as CSS, after a long battle with users and the embarrassing “root kit” incident<sup>97</sup> in which thousands of computers were loaded with software without the owner’s consent, most DRM protection measures on music files and CD have been eliminated. For example, CD’s are widely playable and rippable on any PC and, in addition, Apple’s iTunes and Real Networks’ Rhapsody sell largely unprotected music files. Many groups, however, are unhappy with the provisions of the DMCA and the manner it has been applied. Generally, academics, libraries and non-profit civil liberties groups,<sup>98</sup> have opposed the enactment of the original bill and are critical of the broad manner in which the copyright owners have sought to enforce it.

**(3) Whether there are trends in amendments to laws. If so, what are the trends?**

There are no major amendments to the DMCA being considered at this time. However a number of bills in the US Congress have been proposed which affect copyright.

In 2004, the Inducing Infringement of Copyright Act was proposed applying vicarious liability on anyone who, “intentionally induces, aids, abets, counsels or procures infringement.” Such a broad prohibition would implicate may peer-to-peer services or any party who supplies a device that may be used to infringe once again attacking the longstanding fair use rights ushered in by the *Betamax* decision.

In 2005, the Digital Transition Content Security Act was introduced with the intent of protecting against the “analog hole” requiring that certain analog

---

<sup>96</sup> <http://w2.eff.org/IP/DMCA/states/>

<sup>97</sup> T Mulligan, Deirdre K. and Perzanowski, Aaron, The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident. Berkeley Technology Law Journal, Vol. 22, p. 1157, 2007. Available at SSRN: <http://ssrn.com/abstract=1072229>

<sup>98</sup> See <http://www.eff.org/>; <http://www.chillingeffects.org/>, <http://www.ala.org/ala/issuesadvocacy/copyright/activelegislation/dmca/dmcaDigitalMillennium.cfm>

conversion devices preserve digital content security by mandating the use a video DRM technology VEIL (Video Encoded Invisible Light).

Also of interest is the Audio Broadcast Flag Licensing Act, introduced in 2006, which attempted to mandate a “broadcast flag” for audio content transmitted digitally to prevent unauthorized copying.

At this time, it is not known whether any of these bills could become law.

## **Annex 1**

### **Australia Chapter 17**

7. (a) In order to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that authors, performers, and producers of phonograms use in connection with the exercise of their rights and that restrict unauthorised acts in respect of their works, performances, and phonograms, each Party shall provide that any person who:
- (i) knowingly, or having reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, or phonogram, or other subject matter; or
  - (ii) manufactures, imports, distributes, offers to the public, provides, or otherwise traffics in devices, products, or components, or offers to the public, or provides services that:
    - (A) are promoted, advertised, or marketed for the purpose of circumvention of any effective technological measure;
    - (B) have only a limited commercially significant purpose or use other than to circumvent any effective technological measure; or
    - (C) are primarily designed, produced, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure,

shall be liable and subject to the remedies specified in Article 17.11.13. Each Party shall provide for criminal procedures and penalties to be applied where any person is found to have engaged wilfully and for the purposes of commercial advantage or financial gain in any of the above activities. Each Party may provide that such criminal procedures and penalties do not apply to a non-profit library, archive, educational institution, or public non-commercial broadcasting entity.

- (b) Effective technological measure means any technology, device, or component that, in the normal course of its operation, controls access to a protected work, performance, phonogram, or other protected subject matter, or protects any copyright.
- (c) In implementing sub-paragraph (a), neither Party shall be obligated to require that the design of, or the design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as the product does not otherwise violate any measures implementing sub-paragraph (a).
- (d) Each Party shall provide that a violation of a measure implementing this paragraph is a separate civil or criminal offence and independent of any infringement that might occur under the Party's copyright law.



- (e) Each Party shall confine exceptions to any measures implementing sub-paragraph (a) to the following activities, which shall be applied to relevant measures in accordance with sub-paragraph (f):
- (i) non-infringing reverse engineering activities with regard to a lawfully obtained copy of a computer program, carried out in good faith with respect to particular elements of that computer program that have not been readily available to the person engaged in those activities, for the sole purpose of achieving interoperability of an independently created computer program with other programs;
  - (ii) non-infringing good faith activities, carried out by an appropriately qualified researcher who has lawfully obtained a copy, unfixed performance, or display of a work, performance, or phonogram and who has made a good faith effort to obtain authorisation for such activities, to the extent necessary for the sole purpose of identifying and analysing flaws and vulnerabilities of technologies for scrambling and descrambling of information;
  - (iii) the inclusion of a component or part for the sole purpose of preventing the access of minors to inappropriate online content in a technology, product, service, or device that itself is not prohibited under the measures implementing sub-paragraph (a)(ii);
  - (iv) non-infringing good faith activities that are authorised by the owner of a computer, computer system, or computer network for the sole purpose of testing, investigating, or correcting the security of that computer, computer system, or computer network;
  - (v) non-infringing activities for the sole purpose of identifying and disabling a capability to carry out undisclosed collection or dissemination of personally identifying information reflecting the online activities of a natural person in a way that has no other effect on the ability of any person to gain access to any work;
  - (vi) lawfully authorised activities carried out by government employees, agents, or contractors for law enforcement, intelligence, essential security, or similar governmental purposes;
  - (vii) access by a non-profit library, archive, or educational institution to a work, performance, or phonogram not otherwise available to it, for the sole purpose of making acquisition decisions; and
  - (viii) non-infringing uses of a work, performance, or phonogram in a particular class of works, performances, or phonograms, when an actual or likely adverse impact on those non-infringing uses is credibly demonstrated in a legislative or administrative review or proceeding; provided that any such review or proceeding is conducted at least once every four years from the date of conclusion of such review or proceeding.
- (f) The exceptions to any measures implementing sub-paragraph (a) for the activities set forth in sub-paragraph (e) may only be applied as follows, and only to the extent that they do not impair the adequacy of legal protection or

the effectiveness of legal remedies against the circumvention of effective technological measures:

- (i) any measures implementing sub-paragraph (a)(i) may be subject to exceptions with respect to each activity set forth in sub-paragraph (e);
- (ii) any measures implementing sub-paragraph (a)(ii), as they apply to effective technological measures that control access to a work, performance, or phonogram, may be subject to exceptions with respect to activities set forth in sub-paragraph (e)(i), (ii), (iii), (iv), and (vi); and
- (iii) any measures implementing sub-paragraph (a)(ii), as they apply to effective technological measures that protect any copyright, may be subject to exceptions with respect to the activities set forth in sub-paragraph (e)(i) and (vi).

8. In order to provide adequate and effective legal remedies to protect rights management information:

(a) each Party shall provide that any person who without authority, and knowing, or, with respect to civil remedies, having reasonable grounds to know, that it would induce, enable, facilitate, or conceal an infringement of any copyright:

- (i) knowingly removes or alters any rights management information;
- (ii) distributes or imports for distribution rights management information knowing that the rights management information has been removed or altered without authority; or
- (iii) distributes to the public, imports for distribution, broadcasts, communicates, or makes available to the public copies of works, performances, or phonograms, knowing that rights management information has been removed or altered without authority,

shall be liable and subject to the remedies specified in Article 17.11.13. Each Party shall provide for criminal procedures and penalties to be applied where any person is found to have engaged wilfully and for purposes of commercial advantage or financial gain in any of the above activities. Each Party may provide that these criminal procedures and penalties do not apply to a non-profit library, archive, educational institution, or public non-commercial broadcasting entity;

(b) each Party shall confine exceptions to measures implementing sub-paragraph (a) to lawfully authorised activities carried out by government employees, agents, or contractors for the purpose of law enforcement, intelligence, essential security, or similar government purposes;

(c) rights management information means:

- (i) electronic information that identifies a work, performance, or phonogram; the author of the work; the performer of the performance; the producer of the phonogram; or the owner of any right in the work, performance, or phonogram; or
- (ii) electronic information about the terms and conditions of the use of the work, performance, or phonogram; or

- (iii) any electronic numbers or codes that represent such information,
- when any of these items is attached to a copy of the work, performance, or phonogram or appears in connection with the communication or making available of a work, performance, or phonogram to the public. Nothing in this paragraph shall obligate a Party to require the owner of any right in the work, performance, or phonogram to attach rights management information to copies of the work, performance, or phonogram, or to cause rights management information to appear in connection with a communication of the work, performance, or phonogram to the public.

**Korea**  
**Chapter 18**

7. (a) In order to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that authors, performers, and producers of phonograms use in connection with the exercise of their rights and that restrict unauthorized acts in respect of their works, performances, and phonograms, each Party shall provide that any person who:

- (i) knowingly, or having reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, phonogram, or other subject matter; or
- (ii) manufactures, imports, distributes, offers to the public, provides, or otherwise traffics in devices, products, or components, or offers to the public or provides services, that:
  - (A) are promoted, advertised, or marketed by that person, or by another person acting in concert with, and with the knowledge of, that person, for the purpose of circumvention of any effective technological measure;
  - (B) have only a limited commercially significant purpose or use other than to circumvent any effective technological measure; or
  - (C) are primarily designed, produced, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure,

shall be liable and subject to the remedies set out in Article 18.10.13.13 Each Party shall provide for criminal procedures and penalties to be applied when any person, other than a nonprofit library, archive, educational institution, or public noncommercial broadcasting entity, is found to have engaged willfully and for purposes of commercial advantage or private financial gain in any of the foregoing activities. Such criminal procedures and penalties shall include the application to such activities of the remedies and authorities listed in subparagraphs (a), (b), and (e) of Article 18.10.27 as applicable to infringements, mutatis mutandis.

- (b) In implementing subparagraph (a), neither Party shall be obligated to require that the design of, or the design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as the product does not otherwise violate any measures implementing subparagraph (a).
- (c) Each Party shall provide that a violation of a measure implementing this paragraph is a separate cause of action, independent of any infringement that might occur under the Party's law on copyright and related rights.
- (d) Each Party shall confine exceptions and limitations to measures implementing subparagraph (a) to the following activities, which shall be applied to relevant measures in accordance with subparagraph (e):<sup>14</sup>

- (i) noninfringing reverse engineering activities with regard to a lawfully obtained copy of a computer program, carried out in good faith with respect to particular elements of that computer program that have not been readily available to the person engaged in those activities, for the sole purpose of achieving interoperability of an independently created computer program with other programs;
  - (ii) noninfringing good faith activities, carried out by an appropriately qualified researcher who has lawfully obtained a copy, unfixed performance, or display of a work, performance, or phonogram and who has made a good faith effort to obtain authorization for such activities, to the extent necessary for the sole purpose of research consisting of identifying and analyzing flaws and vulnerabilities of technologies for scrambling and descrambling of information;
  - (iii) the inclusion of a component or part for the sole purpose of preventing the access of minors to inappropriate online content in a technology, product, service, or device that itself is not prohibited under the measures implementing subparagraph (a)(ii);
  - (iv) noninfringing good faith activities that are authorized by the owner of a computer, computer system, or computer network for the sole purpose of testing, investigating, or correcting the security of that computer, computer system, or computer network;
  - (v) noninfringing activities for the sole purpose of identifying and disabling a capability to carry out undisclosed collection or dissemination of personally identifying information reflecting the online activities of a natural person in a way that has no other effect on the ability of any person to gain access to any work;
  - (vi) lawfully authorized activities carried out by government employees, agents, or contractors for the purpose of law enforcement, intelligence, essential security, or similar governmental purposes;
  - (vii) access by a nonprofit library, archive, or educational institution to a work, performance, or phonogram not otherwise available to it, for the sole purpose of making acquisition decisions; and
  - (viii) noninfringing uses of a work, performance, or phonogram in a particular class of works, performances, or phonograms when an actual or likely adverse impact on those noninfringing uses is demonstrated in a legislative or administrative proceeding by substantial evidence, provided that any limitation or exception adopted in reliance on this clause shall have effect for a renewable period of not more than three years from the date the proceeding concludes.
- (e) The exceptions and limitations to measures implementing subparagraph (a) for the activities set forth in subparagraph (d) may only be applied as follows, and only to the extent that they do not impair the adequacy of legal protection or the effectiveness of legal remedies against the circumvention of effective technological measures:

- (i) Measures implementing subparagraph (a)(i) may be subject to exceptions and limitations with respect to each activity set forth in subparagraph (d).
  - (ii) Measures implementing subparagraph (a)(ii), as they apply to effective technological measures that control access to a work, performance, or phonogram, may be subject to exceptions and limitations with respect to activities set forth in subparagraph (d)(i), (ii), (iii), (iv), and (vi).
  - (iii) Measures implementing subparagraph (a)(ii), as they apply to effective technological measures that protect any copyright or any rights related to copyright, may be subject to exceptions and limitations with respect to activities set forth in subparagraph (d)(i) and (vi).
- (f) Effective technological measure means any technology, device, or component that, in the normal course of its operation, controls access to a protected work, performance, phonogram, or other protected subject matter, or protects any copyright or any rights related to copyright.

8. In order to provide adequate and effective legal remedies to protect rights management information:

- (a) Each Party shall provide that any person who without authority, and knowing, or, with respect to civil remedies, having reasonable grounds to know, that it would induce, enable, facilitate, or conceal an infringement of any copyright or related right,
  - (i) knowingly removes or alters any rights management information;
  - (ii) distributes or imports for distribution rights management information knowing that the rights management information has been removed or altered without authority; or
  - (iii) distributes, imports for distribution, broadcasts, communicates or makes available to the public copies of works, performances, or phonograms, knowing that rights management information has been removed or altered without authority,

shall be liable and subject to the remedies set out in Article 18.10.13. Each Party shall provide for criminal procedures and penalties to be applied when any person, other than a nonprofit library, archive, educational institution, or public noncommercial broadcasting entity, is found to have engaged willfully and for purposes of commercial advantage or private financial gain in any of the foregoing activities. These criminal procedures and penalties shall include the application to such activities of the remedies and authorities listed in subparagraphs (a), (b), and (e) of Article 18.10.27 as applicable to infringements, *mutatis mutandis*.

- (b) Each Party shall confine exceptions and limitations to measures implementing subparagraph (a) to lawfully authorized activities carried out by government employees, agents, or contractors for the purpose of law enforcement, intelligence, essential security, or similar governmental purposes.

- (c) Rights management information means:
- (i) information that identifies a work, performance, or phonogram; the author of the work, the performer of the performance, or the producer of the phonogram; or the owner of any right in the work, performance, or phonogram;
  - (ii) information about the terms and conditions of the use of the work, performance, or phonogram; or
  - (iii) any numbers or codes that represent such information,  
when any of these items is attached to a copy of the work, performance, or phonogram or appears in connection with the communication or making available of a work, performance, or phonogram to the public.
- (d) For greater certainty, nothing in this paragraph shall be construed to obligate a Party to require the owner of any right in the work, performance, or phonogram to attach rights management information to copies of the work, performance, or phonogram, or to cause rights management information to appear in connection with a communication of the work, performance, or phonogram to the public.

**Singapore  
Article 16**

7 (a) In order to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that authors, performers, producers of phonograms, and their successors in interest use in connection with the exercise of their rights and that restrict unauthorized acts in respect of their works, performances, and phonograms, each Party shall provide that any person who:

- (i) knowingly, or having reasonable grounds to know, circumvents without authority any effective technological measure that controls access to a protected work, performance, phonogram, or other subject matter; or
- (ii) manufactures, imports, distributes, offers to the public, provides, or otherwise traffics in devices, products, or components or offers to the public or provides services, which:
  - (A) are promoted, advertised, or marketed for the purpose of circumvention of any effective technological measure, or
  - (B) have only a limited commercially significant purpose or use other than to circumvent any effective technological measure, or
  - (C) are primarily designed, produced, or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure;

shall be liable and subject to the remedies provided for in Article 16.9.5. Each Party shall provide that any person, other than a nonprofit library, archive, educational institution, or public noncommercial broadcasting entity, that is found to have engaged willfully and for purposes of commercial advantage or private financial gain in such activities shall be guilty of a criminal offense.

- (b) For purposes of this paragraph, effective technological measure means any technology, device, or component that, in the normal course of its operation, controls access to a protected work, performance, phonogram, or other subject matter, or protects any copyright or any rights related to copyright.
- (c) Paragraph 7(a) obligates each Party to prohibit circumvention of effective technological measures and does not obligate a Party to require that the design of, or the design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure. The absence of a requirement to respond affirmatively shall not constitute a defense to a claim of violation of that Party's measures implementing paragraph 7(a).
- (d) Each Party shall provide that a violation of the law implementing this paragraph is independent of any infringement that might occur under the Party's law on copyright and related rights.
- (e) Each Party shall confine exceptions to the prohibition referred to in paragraph 7(a)(ii) on technology, products, services, or devices that



circumvent effective technological measures that control access to, and, in the case of clause (i) below, that protect any of the exclusive rights of copyright or related rights in a protected work, to the following activities, provided that they do not impair the adequacy of legal protection or the effectiveness of legal remedies that the Party provides against the circumvention of effective technological measures:

- (i) noninfringing reverse engineering activities with regard to a lawfully obtained copy of a computer program, carried out in good faith with respect to particular elements of that computer program that have not been readily available to the person engaged in such activity, for the sole purpose of achieving interoperability of an independently created computer program with other programs;
  - (ii) noninfringing good faith activities, carried out by an appropriately qualified researcher who has lawfully obtained a copy, performance, or display of a work, and who has made a good faith effort to obtain authorization for such activities, to the extent necessary for the sole purpose of identifying and analyzing flaws and vulnerabilities of technologies for scrambling and descrambling of information;
  - (iii) the inclusion of a component or part for the sole purpose of preventing the access of minors to inappropriate online content in a technology, product, service, or device provided that such technology, product, service or 7(a)(ii); and
  - (iv) noninfringing good faith activities that are authorized by the owner of a computer, computer system, or computer network for the sole purpose of testing, investigating, or correcting the security of that computer, computer system, or computer network.
- (f) Each Party shall confine exceptions to the prohibited conduct referred to in paragraph 7(a)(i) to the activities listed in paragraph 7(e) and the following activities, provided that such exceptions do not impair the adequacy of legal protection or the effectiveness of legal remedies the Party provides against the circumvention of effective technological measures:
- (i) access by a nonprofit library, archive, or educational institution to a work not otherwise available to it, for the sole purpose of making acquisition decisions;
  - (ii) noninfringing activities for the sole purpose of identifying and disabling a capability to carry out undisclosed collection or dissemination of personally identifying information reflecting the online activities of a natural person in a way that has no other effect on the ability of any person to gain access to any work; and (iii) noninfringing uses of a particular class of works when an actual or likely adverse impact on such noninfringing uses with respect to such particular class of works is credibly demonstrated in a legislative or administrative proceeding, provided that any exception adopted in reliance on this clause shall have effect for a period of not more than four years from the date of conclusion of such proceeding.

(g) Each Party may also provide exceptions to the prohibited conduct referred to in paragraph 7(a) for lawfully authorized activities carried out by government employees, agents, or contractors for the purpose of law enforcement, intelligence, national defense, essential security, or similar government activities.

8. In order to provide adequate and effective legal remedies to protect rights management information:

(a) each Party shall provide that any person who without authority, and knowingly, or, with respect to civil remedies, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any copyright or related right,

(i) knowingly removes or alters any rights management information;

(ii) distributes or imports for distribution rights management information knowing that the rights management information has been altered without authority; or

(iii) distributes, imports for distribution, broadcasts, communicates, or makes available to the public copies of works or phonograms, knowing that rights management information has been removed or altered without authority,

shall be liable and subject to the remedies in Article 16.9.5. Each Party shall provide that any person, other than a nonprofit library, archive, educational institution, or public noncommercial broadcasting entity, who is found to have engaged willfully and for purposes of commercial advantage or private financial gain in such activities shall be guilty of a criminal offense.

(b) For purposes of this paragraph, rights management information means information which identifies a work, performance, or phonogram; the author of the work, the performer of the performance, or the producer of the phonogram; or the owner of any right in the work, performance, or phonogram; information about the terms and conditions of the use of the work, performance, or phonogram; and any numbers or codes that represent such information, when any of these items is attached to a copy of the work, performance, or phonogram or appears in conjunction with the communication or making available of a work, performance, or phonogram to the public. Nothing in this paragraph obligates a Party to require the owner of any right in the work, performance, or phonogram to attach rights management information to copies of it or to cause rights management information to appear in connection with a communication of the work, performance, or phonogram to the public.

## **Annex 2**

### **17 U.S.C. §1200 - 1205**

#### **Chapter 12<sup>1</sup>**

#### **Copyright Protection and Management Systems**

- \* **1201. Circumvention of copyright protection systems**
- \* **1202. Integrity of copyright management information**
- \* **1203. Civil remedies**
- \* **1204. Criminal offenses and penalties**
- \* **1205. Savings clause**

#### **§ 1201. Circumvention of copyright protection systems<sup>2</sup>**

- (a) **Violations Regarding Circumvention of Technological Measures.** — (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.
- (B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).
- (C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine —
- (i) the availability for use of copyrighted works;
  - (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;
  - (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
  - (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

- (v) such other factors as the Librarian considers appropriate.
  - (D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.
  - (E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.
- (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —
- (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
  - (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
  - (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.
- (3) As used in this subsection —
- (A) to “circumvent a technological measure” means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and
  - (B) a technological measure “effectively controls access to a work” if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.
- (b) Additional Violations. — (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —
- (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

- (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
  - (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.
- (2) As used in this subsection —
- (A) to “circumvent protection afforded by a technological measure” means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and
  - (B) a technological measure “effectively protects a right of a copyright owner under this title” if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.
- (c) Other Rights, Etc., Not Affected. — (1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.
- (2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.
- (3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).
- (4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.
- (d) Exemption for Nonprofit Libraries, Archives, and Educational Institutions. — (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph —
- (A) may not be retained longer than necessary to make such good faith determination; and
  - (B) may not be used for any other purpose.

- (2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.
- (3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1) —
  - (A) shall, for the first offense, be subject to the civil remedies under section 1203; and
  - (B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).
- (4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.
- (5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be —
  - (A) open to the public; or
  - (B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.
- (e) Law Enforcement, Intelligence, and Other Government Activities. — This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term “information security” means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.
- (f) Reverse Engineering. — (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.
- (2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such

interoperability, to the extent that doing so does not constitute infringement under this title.

- (3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.
- (4) For purposes of this subsection, the term “interoperability” means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.
- (g) Encryption Research. —
  - (1) Definitions. — For purposes of this subsection —
    - (A) the term “encryption research” means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and
    - (B) the term “encryption technology” means the scrambling and descrambling of information using mathematical formulas or algorithms.
  - (2) Permissible acts of encryption research. — Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if —
    - (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
    - (B) such act is necessary to conduct such encryption research;
    - (C) the person made a good faith effort to obtain authorization before the circumvention; and
    - (D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.
  - (3) Factors in determining exemption. — In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include —
    - (A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was

disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

- (B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and
  - (C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.
- (4) Use of technological means for research activities. — Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to —
- (A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and
  - (B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).
- (5) Report to Congress. — Not later than 1 year after the date of the enactment of this chapter, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on —
- (A) encryption research and the development of encryption technology;
  - (B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and
  - (C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

The report shall include legislative recommendations, if any.

- (h) Exceptions Regarding Minors. — In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which —
- (1) does not itself violate the provisions of this title; and
  - (2) has the sole purpose to prevent the access of minors to material on the Internet.
- (i) Protection of Personally Identifying Information. —
- (1) Circumvention permitted. — Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a



technological measure that effectively controls access to a work protected under this title, if —

- (A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;
- (B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;
- (C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and
- (D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures. —

This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security Testing. —

- (1) Definition. — For purposes of this subsection, the term “security testing” means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.
- (2) Permissible acts of security testing. — Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.
- (3) Factors in determining exemption. — In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include —
  - (A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

- (B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.
- (4) Use of technological means for security testing. — Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2), provided such technological means does not otherwise violate section (a)(2).
- (k) Certain Analog Devices and Certain Technological Measures. —
- (1) Certain analog devices. —
  - (A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any —
    - (i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;
    - (ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;
    - (iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;
    - (iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter; or
    - (v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.
  - (B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in —
    - (i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

- (ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology.

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder “conforms to” the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

- (2) Certain encoding restrictions. — No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying —
  - (A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;
  - (B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;
  - (C) from a physical medium containing one or more prerecorded audiovisual works; or
  - (D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).

In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

- (3) Inapplicability. — This subsection shall not —
  - (A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

- (B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or
  - (C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).
- (4) Definitions. — For purposes of this subsection:
- (A) An “analog video cassette recorder” means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.
  - (B) An “analog video cassette camcorder” means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.
  - (C) An analog video cassette recorder “conforms” to the automatic gain control copy control technology if it —
    - (i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or
    - (ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.
  - (D) The term “professional analog video cassette recorder” means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.
  - (E) The terms “VHS format,” “8mm format,” “Beta format,” “automatic gain control copy control technology,” “colorstripe copy control technology,” “four-line version of the colorstripe copy control technology,” and “NTSC” have the meanings that are commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter.
- (5) Violations. — Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an “act of circumvention” for the purposes of section 1203(c)(3)(A) of this chapter.

**§ 1202. Integrity of copyright management information<sup>3</sup>**

- (a) False Copyright Management Information. — No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement —
  - (1) provide copyright management information that is false, or

- (2) distribute or import for distribution copyright management information that is false.
- (b) Removal or Alteration of Copyright Management Information. — No person shall, without the authority of the copyright owner or the law —
  - (1) intentionally remove or alter any copyright management information,
  - (2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or
  - (3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law, knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.
- (c) Definition. — As used in this section, the term “copyright management information” means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:
  - (1) The title and other information identifying the work, including the information set forth on a notice of copyright.
  - (2) The name of, and other identifying information about, the author of a work.
  - (3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.
  - (4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.
  - (5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.
  - (6) Terms and conditions for use of the work.
  - (7) Identifying numbers or symbols referring to such information or links to such information.
  - (8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.
- (d) Law Enforcement, Intelligence, and Other Government Activities. — This section does not prohibit any lawfully authorized investigative, protective,

information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term “information security” means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(e) Limitations on Liability. —

(1) Analog transmissions. — In the case of an analog transmission, a person who is making transmissions in its capacity as a broadcast station, or as a cable system, or someone who provides programming to such station or system, shall not be liable for a violation of subsection (b) if —

(A) avoiding the activity that constitutes such violation is not technically feasible or would create an undue financial hardship on such person; and

(B) such person did not intend, by engaging in such activity, to induce, enable, facilitate, or conceal infringement of a right under this title.

(2) Digital transmissions. —

(A) If a digital transmission standard for the placement of copyright management information for a category of works is set in a voluntary, consensus standard-setting process involving a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to the particular copyright management information addressed by such standard if —

(i) the placement of such information by someone other than such person is not in accordance with such standard; and

(ii) the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title.

(B) Until a digital transmission standard has been set pursuant to subparagraph (A) with respect to the placement of copyright management information for a category of works, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to such copyright management information, if the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title, and if —

(i) the transmission of such information by such person would result in a perceptible visual or aural degradation of the digital signal; or

(ii) the transmission of such information by such person would conflict with —

- (I) an applicable government regulation relating to transmission of information in a digital signal;
  - (II) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted by a voluntary consensus standards body prior to the effective date of this chapter; or
  - (III) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted in a voluntary, consensus standards-setting process open to participation by a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems.
- (3) Definitions. — As used in this subsection —
- (A) the term “broadcast station” has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and
  - (B) the term “cable system” has the meaning given that term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

**§ 1203. Civil remedies<sup>4</sup>**

- (a) Civil Actions. — Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation.
- (b) Powers of the Court. — In an action brought under subsection (a), the court —
  - (1) may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation, but in no event shall impose a prior restraint on free speech or the press protected under the 1st amendment to the Constitution;
  - (2) at any time while an action is pending, may order the impounding, on such terms as it deems reasonable, of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation;
  - (3) may award damages under subsection (c);
  - (4) in its discretion may allow the recovery of costs by or against any party other than the United States or an officer thereof;
  - (5) in its discretion may award reasonable attorney's fees to the prevailing party; and
  - (6) may, as part of a final judgment or decree finding a violation, order the remedial modification or the destruction of any device or product involved in the violation that is in the custody or control of the violator or has been impounded under paragraph (2).

- (c) Award of Damages. —
- (1) In general. — Except as otherwise provided in this title, a person committing a violation of section 1201 or 1202 is liable for either —
- (A) the actual damages and any additional profits of the violator, as provided in paragraph (2), or
- (B) statutory damages, as provided in paragraph (3).
- (2) Actual damages. — The court shall award to the complaining party the actual damages suffered by the party as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages, if the complaining party elects such damages at any time before final judgment is entered.
- (3) Statutory damages. — (A) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1201 in the sum of not less than \$200 or more than \$2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.
- (B) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1202 in the sum of not less than \$2,500 or more than \$25,000.
- (4) Repeated violations. — In any case in which the injured party sustains the burden of proving, and the court finds, that a person has violated section 1201 or 1202 within three years after a final judgment was entered against the person for another such violation, the court may increase the award of damages up to triple the amount that would otherwise be awarded, as the court considers just.
- (5) Innocent violations. —
- (A) In general. — The court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation.
- (B) Nonprofit library, archives, educational institutions, or public broadcasting entities. —
- (i) Definition. — In this subparagraph, the term “public broadcasting entity” has the meaning given such term under section 118(g).
- (ii) In general. — In the case of a nonprofit library, archives, educational institution, or public broadcasting entity, the court shall remit damages in any case in which the library, archives, educational institution, or public broadcasting entity sustains the burden of proving, and the court finds, that the library, archives, educational institution, or public broadcasting entity was not aware and had no reason to believe that its acts constituted a violation.



## **§ 1204. Criminal offenses and penalties<sup>5</sup>**

- (a) In General. — Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain —
  - (1) shall be fined not more than \$500,000 or imprisoned for not more than 5 years, or both, for the first offense; and
  - (2) shall be fined not more than \$1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.
- (b) Limitation for Nonprofit Library, Archives, Educational Institution, or Public Broadcasting Entity. — Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118(g)).
- (c) Statute of Limitations. — No criminal proceeding shall be brought under this section unless such proceeding is commenced within five years after the cause of action arose.

## **§ 1205. Savings clause**

Nothing in this chapter abrogates, diminishes, or weakens the provisions of, nor provides any defense or element of mitigation in a criminal prosecution or civil action under, any Federal or State law that prevents the violation of the privacy of an individual in connection with the individual's use of the Internet.

### Chapter 12 Endnotes

<sup>1</sup>The WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998 added chapter 12, entitled “Copyright Protection and Management Systems,” to title 17. Pub. L. No. 105-304, 112 Stat. 2860, 2863. The WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998 is title I of the Digital Millennium Copyright Act. Pub. L. No. 105-304, 112 Stat. 2860.

<sup>2</sup>The Satellite Home Viewer Improvement Act of 1999 amended section 1201(a)(1)(C) by deleting “on the record.” Pub. L. No. 106-113, 113 Stat. 1501, app. I at 1501A-594.

<sup>3</sup>In 1999, section 1202 was amended by inserting “category of works” for “category or works,” in subsection (e)(2)(B). Pub. L. No. 106-44, 113 Stat. 221, 222.

<sup>4</sup>The Satellite Home Viewer Improvement Act of 1999 amended section 1203(c)(5)(B) in its entirety. Pub. L. No. 106-113, 113 Stat. 1501, app. I at 1501A-593.

<sup>5</sup>The Satellite Home Viewer Improvement Act of 1999 amended section 1204(b) in its entirety. Pub. L. No. 106-113, 113 Stat. 1501, app. I at 1501A-593.

**Annex 3**  
**Section 1201(a)(1)(C) Rulemaking Since 2000**

2000	2003	2006	2009 (forthcoming)
<i>No analogous exemption in 2000 or 2003</i>		Audiovisual works included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors	
Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage, or obsolescence	Computer programs and videogames distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace	Computer programs and videogames distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace	
	Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete	Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete	Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace
<i>No analogous exemption in 2000</i>	Literary works distributed in E-book format when all existing E-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the E-book's read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format	Literary works distributed in E-book format when all existing E-book editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format	
<i>No analogous exemption in 2000 or 2003</i>		Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network	

**Annex 3**

**Section 1201(a)(1)(C) Rulemaking Since 2000**

2000	2003	2006	2009 (forthcoming)
<i>No analogous exemption in 2000 or 2003</i>		Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities	
Compilations consisting of lists of websites blocked by filtering software applications	Compilations consisting of lists of Internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites, but not including lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of email	<i>No longer exempted</i>	



2010年3月発行

コンテンツの技術的手段に係る各国法制度調査研究報告書  
(平成21年度)

西村あさひ法律事務所

〒107-6029 東京都港区赤坂 1-12-32 アーク森ビル(総合受付 28階)

電話 03-5562-8500 (代表)

FAX 03-5561-9711/12/13/14

<http://www.jurists.co.jp/>

禁無断転載

