STUDY ON DYNAMIC BLOCKING INJUNCTIONS IN THE EUROPEAN UNION

IPR ENFORCEMENT
CASE-LAW COLLECTION
This study has been prepared by the EUIPO in cooperation with the Centre for International Intellectual Property Studies (CEIPI) (main authors: Giancarlo Frosio, Oleksandr Bulayenko), University of Strasbourg.

A list of national experts that answered to a standardised questionnaire is available in Annex IV.
FOREWORD

The rise in online activity and especially the online provision and consumption of copyright protected content received an additional boost due to the COVID-19 pandemic. In addition to legitimate offerings there are also many websites offering illegal downloads of music, films, games and/or illegal live broadcasts of sporting and cultural events.

This underlines the relevance to further explore the effectiveness of existing legal remedies against IPR infringement.

Such remedies can include website blocking injunctions through Domain Name System (DNS) blocking, Internet Protocol (IP) address blocking, or through Uniform Resource Locator (URL) filtering and can be an effective means of preventing the continuation of IPR infringement.

However, different requirements across the EU apply regarding the evidence required to obtain blocking orders, and especially forward-looking injunctions (or dynamic injunctions), which can be used to prevent the continuation of IPR infringement.

This study and the relevant case law collected in collaboration with the Observatory legal expert group provides an overview of static and dynamic blocking injunctions in the EU and the Member States available for rights holders who wish to effectively combat online piracy and protect their rights.

It analyses the availability of such injunctions, their scope, technical implementation, and their effectiveness in reducing infringement and aims to help various stakeholders, Member States and other legal professionals to implement and/or improve the application of dynamic blocking injunctions.

Christian ARCHAMBEAU
EUIPO Executive Director
# TABLE OF CONTENT

**FOREWORD** ........................................................................................................................................ 2

**TABLE OF CONTENT** ......................................................................................................................... 4

**EXECUTIVE SUMMARY** .................................................................................................................. 8

**BACKGROUND** .................................................................................................................................... 10
  - Structure, Purpose and Scope of the Study ......................................................................................... 10
  - Methodology ...................................................................................................................................... 10
  - Terminology used ............................................................................................................................... 12
  - Abbreviations ................................................................................................................................... 12

**ANALYSIS ON DYNAMIC BLOCKING INJUNCTIONS** ...................................................................... 14

1. Introduction ........................................................................................................................................... 14
2. Blocking Injunctions and Dynamic Blocking Injunctions in Europe ............................................. 16
   2.1 Definition ....................................................................................................................................... 16
   2.2 Legislation ...................................................................................................................................... 17
   2.3 Proposed legislation ....................................................................................................................... 18
   2.4 Case-law ....................................................................................................................................... 18
   2.5 Administrative orders .................................................................................................................... 20
   2.6 Soft law ....................................................................................................................................... 21

   3.1 The fundamental rights framework ............................................................................................... 22
   3.2 Proportionality .............................................................................................................................. 27
   3.2.1 EU law ..................................................................................................................................... 27
   3.2.2 National standards ................................................................................................................... 28
3.2.3 Injunction against some but not all access providers ..................29
3.2.4 Risk of over- and under-blocking ........................................30

4. Availability and Issuance Requirements ........................................31
4.1 Blocking injunctions .................................................................31
4.1.1 Availability .......................................................................31
4.1.2 Subject matter .................................................................31
4.1.3 Targeted intermediaries .......................................................32
4.1.4 Issuance requirements .........................................................32
4.1.5 Necessity of the decision on the merits ...................................33
4.1.6 Contributory liability .........................................................33
4.1.7 Ex parte and inter partes proceedings ......................................33
4.1.8 Preliminary and/or final injunctions .......................................34
4.1.9 Duration of blocking injunctions ..........................................34
4.1.10 Blocking injunctions in civil and criminal cases ......................35
4.2 Dynamic blocking injunctions ....................................................35
4.2.1 Availability ..........................................................35
4.2.2 Statutory notion ...............................................................36
4.2.3 Case-law ..........................................................36
4.2.4 Unavailability and fundamental rights balancing ....................39
4.3 Live blocking injunctions ........................................................39
4.3.1 Availability ..........................................................39
4.3.2 Unavailability ..........................................................41

5. Scope of Dynamic Blocking Injunctions .........................................41
5.1 Subject matter ..................................................................41
5.1.1 Broadcasting live sporting events .........................................41
5.1.2 TPMs ..................................................................42
5.2 Targeted intermediaries ..........................................................43
5.3 Targeted websites, content and internet resources .......................43
5.4 Number of websites subject to blocking ....................................44
5.5 Exceptions ..................................................................44
5.6 Confidentiality ..................................................................44
5.7 Temporal scope ..................................................................45
5.8 Territorial scope...........................................................................................................46

6. Evidence ......................................................................................................................47
   6.1 Specific procedural rules............................................................................................47
   6.2 Type of evidence ........................................................................................................47
   6.3 Evidence to show infringement..................................................................................47
   6.4 Additional evidence .................................................................................................47
   6.5 Evidence for dynamic blocking ................................................................................48
   6.6 Notification of (repeated) infringements .................................................................48

7. Implementation of Blocking Injunctions ...................................................................49
   7.1 Technical solutions available ....................................................................................49
   7.2 Implementation costs ...............................................................................................50

8. Follow-up to Dynamic Blocking Injunctions .............................................................52
   8.1 Renewal and update .................................................................................................52
   8.2 Converting static into dynamic injunctions ..............................................................53
   8.3 Recurring penalties .................................................................................................54
   8.4 Enforcement and fines ............................................................................................54
   8.5 Remedies against the injunction ..............................................................................55

   9.1 Extraterritorial enforcement ....................................................................................55
   9.2 Legal entanglements ...............................................................................................57

10. Effectiveness of Dynamic Blocking Injunctions .........................................................58

11. Conclusions and Key Findings ..................................................................................59

**CASE-LAW OF THE CJEU** .........................................................................................63

**CASE-LAW OF NATIONAL COURTS** .........................................................................68

Belgium .............................................................................................................................68
Denmark ................................................................. 71
Finland ................................................................. 74
France ................................................................. 76
Germany ............................................................... 80
Italy ................................................................. 83
Ireland ............................................................... 85
Netherlands .................................................. 90
Spain ............................................................... 94
Sweden .............................................................. 96
United Kingdom .................................................. 99

ANNEX I: OVERVIEW TABLE PRELIMINARY RULINGS .................. 106
ANNEX II: OVERVIEW TABLE NATIONAL CASE-LAW .................... 110
ANNEX III: GLOSSARY .................................................. 133
ANNEX IV: LEGAL EXPERTS .............................................. 136
EXECUTIVE SUMMARY

This study and case-law collection offers an overview of static and dynamic blocking injunctions in the EU and the Studied Member States (SMS). The overview is based on questionnaires and a comparative review of the case-law and the legal framework of the SMS.

Blocking injunctions find their legal basis in Article 18(1) of the e-commerce Directive, Article 8(3) of the InfoSoc Directive and Article 11 of the IPRED. The compatibility of blocking injunctions with EU law has been confirmed by a number of Court of Justice of the European Union (CJEU) judgments, which also support the availability of dynamic blocking injunctions. However, while static blocking injunctions are available in all the SMS, dynamic blocking injunctions are not or, at least, their availability has not yet been tested in the courts in some of the SMS.

The availability of static and dynamic blocking injunctions largely depends on the proper balancing of rights and interests of persons concerned by the measures. This balancing is undertaken through the consideration of different fundamental rights and of the overall proportionality of the injunctions. Overall, static and dynamic blocking injunctions should be available, according to the doctrine of ‘fair balance’ among fundamental rights, only if they are strictly targeted to bring the infringement to an end and if they do not disproportionately impinge on fundamental rights, do not impose ‘excessive obligations’ on intermediaries and address the risk of over- and under-blocking.

Requirements for obtaining a blocking injunction differ in the SMS. However, there are still some common general requirements and procedural rules that apply in most SMS, including the need to demonstrate the rights holder’s status and ownership of rights, evidence of alleged infringement, proportionality, appropriateness and/or reasonableness of the requested measure.

Dynamic blocking injunctions have been granted in most of the SMS, including Denmark, France, Ireland, Italy, the Netherlands, Spain, Sweden and the UK. However, so far, the number of dynamic blocking injunctions issued in the SMS has been limited. In most SMS, there is no explicit statutory notion of dynamic blocking injunctions — and defining their requirements — on the basis of an expansive interpretation of pre-existing norms. As a subspecies of dynamic blocking injunctions, some SMS (Ireland, Spain and the UK) have made available live blocking injunctions with the principal goal of limiting infringement of rights to live (sports) events. In other SMS, live blocking injunctions are not available or, at least, their availability has not been tested in court yet.

With regard to the scope of dynamic blocking injunctions, the subject matter, targeted intermediaries, targeted websites, temporal and territorial scope vary to different extents in the SMS. Copyright infringement is the main target of these measures in the SMS, but there does not seem to be any specific limitation to the subject matter that can be covered by a dynamic injunction. Similarly, although dynamic blocking injunctions have been customarily granted against internet access service providers in most SMS, these measures can be used against any party deemed an intermediary under Article 8(3) of the InfoSoc Directive and Article 11 of the IPRED. In most SMS, there are no limitations on the number of websites that can be blocked. The law does not regulate dynamic blocking injunctions nor their duration in most SMS, but these measures might be limited in time by judicial decisions. In general, injunctions can order the blocking of content regardless of the location where
the infringement took place or the location of the users accessing the infringing content, as long as the activities target the consumers and internet users of Member States (MS).

There are no specific procedural rules on the requirements for and the admissibility of evidence for static and dynamic blocking injunctions in the SMS.

The implementation of blocking injunctions mainly focuses on technical solutions and the implementation costs. In most SMS, the injunction usually specifies the technical solution to be applied. If that is not the case, such as in Denmark, France, Italy, Spain and Sweden, courts might, however, suggest technical solutions to meet the scope of the injunction. Both Internet Protocol (IP) address and domain name system (DNS) blocking are the most common technical solutions applied by blocking injunctions in the SMS. The SMS have treated the allocation of the costs of implementing blocking measures rather inconsistently. The intermediaries bear the costs of implementing a blocking injunction in the large majority of the SMS. In fewer SMS, costs might be shared between the intermediary and rights holders, or assigned to intermediaries only.

Follow-up actions to dynamic blocking injunctions play an important role in the measures’ effectiveness and the overall balance of interests. In some SMS, specific procedures are available for renewing, updating or extending static and dynamic blocking injunctions, while they are not available in others. In this context, there does not seem to be any specific distinctions between procedural rules for renewal and update of static and dynamic injunctions among the SMS. In addition, the SMS do not have any specific procedure available to convert a static blocking injunction into a dynamic one. Instead, a new procedure on the merits has to be started. In addition, most SMS provide for the enforcement of the order, fines, and recurring penalties. Finally, there are remedies available to challenge blocking injunctions in all the SMS under traditional civil procedure rules. The remedies are generally available to the intermediaries and the alleged infringers concerned by the injunction. In a few SMS, these remedies are also available to affected individual internet users, or in some SMS via collective actions.

Discussing the extraterritorial scope of injunctions against online intermediaries, recent CJEU jurisprudence concluded that EU law does not impose or preclude worldwide measures. Instead, it is up to national courts to decide whether extraterritorial injunctions could be imposed according to their own balancing of fundamental rights and application of international norms. In this context, blocking injunctions must be targeted and specific with a territorial scope not broader than what is necessary to achieve its objective, according to fundamental right balancing and international law, including the doctrine of comity.

Static and dynamic blocking case-law shows multiple instances of legal entanglement among national courts of different SMS. Legal entanglements can be considered a form of informal cross-border cooperation and occur when national courts refer to judgments in other jurisdictions.

An additional important factor to evaluate availability, scope and proportionality of blocking injunction is their effectiveness in reducing infringement. The effectiveness of blocking injunctions is usually not explicitly assessed in most SMS. Effectiveness might not require 100 % success as long as the remedy is seriously discouraging internet users from accessing the infringing content. Effectiveness is considered in certain jurisdictions an additional requirement to justify targeted and specific blocking injunctions that fairly balance fundamental rights and impose proportionate, not excessive obligations on access providers and other intermediaries.

The overview of static and dynamic blocking injunctions in the EU and the SMS shows a complex web of a variety of approaches in EU MS that is sometimes hard to untangle. Against this backdrop, this
study provides a set of key findings that might serve as a reference for the further development of policies and practices in the field.

BACKGROUND

Structure, Purpose and Scope of the Study

The study on Dynamic Blocking Injunctions in the EU encompasses two main parts: (i) an extensive theoretical part – a comparative study dealing with various aspects of the applicability of dynamic blocking injunctions; and (ii) a case-law collection presenting selected CJEU preliminary rulings providing guidance on the interpretation and application of certain EU norms setting up the legal framework for allowing the granting of dynamic blocking injunctions, as well as judgments of national courts where dynamic blocking injunctions have actually been ordered.

The purpose of the study is to describe the legal framework for blocking injunctions in the EU and SMS and, specifically, forward-looking/dynamic injunctions (including proposed legislation, initiatives and voluntary measures). Additionally, it provides an overview of existing case-law. The study identifies similarities and differences between the practices in various MS with regard to different aspects of dynamic blocking injunctions such as requirements, balance of rights, scope, implementation, costs and effectiveness.

This study provides an overview of legal principles, case-law and practices applicable to dynamic blocking injunctions in the EU and a selected 12+1 MS (Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Lithuania, the Netherlands, Spain, Sweden and the UK(1)), thus representing MS of different sizes, geographical regions and legal traditions.

Methodology

The study relies on an extensive review of literature, EU law, CJEU case-law, regulations, practices, and jurisprudence of the SMS. Attention is given also to the case-law of the European Court of Human Rights (ECtHR).

The review of regulation, case-law, and practices of the SMS to a large extent relies on the information provided by legal experts through a standardised questionnaire. The list of legal experts involved can be found in Annex IV. The questionnaire inquired about the availability of blocking injunctions and, specifically, of dynamic blocking injunctions, their scope, required and/or admissible evidence,

(1) The UK left the EU on 31 January 2020, when the withdrawal agreement entered into force. During the transitional period lasting until 31 December 2020, the UK continued to apply EU law. For ease of terminology, this study refers to all studied countries as (Studied) Member States, even though it fully acknowledges that the UK is no longer part of the EU.
balancing of rights and interests, distribution of costs and remedies for non-compliance. Due to the number and length of the questionnaires, they are not attached as an annex to the study (2). Questionnaire results were supplemented with desk research, which has served the purpose, inter alia, to complement and/or fill in any possible gaps or inconsistencies in the questionnaire responses, as well as to double-check and confirm the correctness of the information collected with the questionnaires.

The case-law collection (3) on blocking injunctions was prepared by the European Observatory on Infringements of Intellectual Property Rights (Observatory) (4), through the Knowledge Circle Enforcement (KCE) of the EUIPO as part of a series of case-law collection studies (5). The judgments included in the case-law collection have been identified through both the EUIPO’s internal database eSearch Case Law and publicly accessible online sources. Individual contributors, that is, members of the KCE, prepared summaries and provided information on decisions from jurisdictions and in languages with which they are familiar. Members of the Legal Expert Group of the Observatory (6) have been invited to suggest additional decisions from courts in different MS, the most relevant of which were included in the case-law collection. The selected cases are listed in the study by country and decision date. Apart from the CJEU decisions, the case-law collection reports national court decisions from 10+1 MS (Belgium, Denmark, Finland, France, Germany, Italy, Ireland, the Netherlands, Spain, Sweden and the UK). The case-law collection includes decisions published before 30/11/2020. These jurisdictions represent different regions of the EU, as well as small and large MS, and were selected according to the availability of relevant case-law in the 27+1 EU MS.

The section of the study titled ‘Analysis on dynamic blocking injunctions’ was prepared under a procurement contract with CEIPI by Giancarlo Frosio and Oleksandr Bulayenko, who also drafted the section titled ‘Executive Summary’. Giancarlo Frosio is an Associate Professor at the Center for International Intellectual Property Studies (CEIPI), University of Strasbourg; Non-resident fellow at Stanford Law School CIS, Stanford University; Faculty Associate at Nexa Center, Polytechnic and University of Turin. Oleksandr Bulayenko is a Researcher and Educational Coordinator at the CEIPI and Associated Researcher at the Institute for Information Law (IViR), University of Amsterdam.

For a list of legal experts providing country-specific information about law, jurisprudence and practices in the SMS, see Annex IV.

(2) The 12+1 questionnaires averaged 150 pages and can be consulted upon request.

(3) The case-law collection is limited to 10+1 Member States and does not include Greece and Lithuania, for which relevant information has only been collected via questionnaires redacted by national legal experts.


(5) See for example IPR Enforcement Case-law Collection, The Liability and Obligations of Intermediary Service Providers in the European Union, EUIPO, August 2019.

Terminology used

The list provided in Annex III: GLOSSARY gives some references for the terminology used in this study.

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG</td>
<td>Advocate General</td>
</tr>
<tr>
<td>AGCOM</td>
<td>Autorità per le Garanzie nelle Comunicazioni (Italy)</td>
</tr>
<tr>
<td>AJA</td>
<td>Administration of Justice Act (Denmark)</td>
</tr>
<tr>
<td>CDPA</td>
<td>Copyright, Design and Patents Act (UK)</td>
</tr>
<tr>
<td>CEL</td>
<td>Code de droit économique / Wetboek van economisch recht / Code of Economic Law (Belgium)</td>
</tr>
<tr>
<td>CFREU</td>
<td>Charter of Fundamental Rights of the European Union</td>
</tr>
<tr>
<td>CIS</td>
<td>Center for Internet and Society at Stanford Law School</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission nationale de l'informatique et des libertés (France)</td>
</tr>
<tr>
<td>CoC</td>
<td>Code of Conduct</td>
</tr>
<tr>
<td>CPI</td>
<td>Code de la propriété intellectuelle / Intellectual Property Code (France)</td>
</tr>
<tr>
<td>DBI</td>
<td>Dynamic Blocking Injunction</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention of Human Rights</td>
</tr>
<tr>
<td>ECHHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDPPI</td>
<td>Committee for the Notification of Copyright and Related Rights Infringement on the Internet (Greece)</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUIPO</td>
<td>European Union Intellectual Property Office</td>
</tr>
<tr>
<td>EWHC</td>
<td>Hight Court of England and Wales</td>
</tr>
<tr>
<td>FAPL</td>
<td>Football Association Premier League</td>
</tr>
<tr>
<td>HADOPI</td>
<td>Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (France)</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IECA</td>
<td>Court of Appeal of Ireland</td>
</tr>
<tr>
<td>IEHC</td>
<td>High Court of Ireland</td>
</tr>
</tbody>
</table>
IP
Internet Protocol

IPR
Intellectual Property Right

IPRED

IPTV
Internet Protocol Television

ISP
Internet service provider

ISPA
Internet Service Providers Association

ITU
International Telecommunication Union

MPA
Motion Picture Association

OLG
Oberlandesgericht / Court of Appeal (Germany)

SMS
Selected/Studied Member States

TGI
Tribunal de Grande Instance / District Court (France)

TJ
Tribunal judiciaire / District Court (France)

TPM
Technological Protection Measure

UEFA
Union of European Football Associations

UK
United Kingdom of Great Britain and Northern Ireland

UN
United Nations

UNESCO
United Nations Educational, Scientific and Cultural Organization

URL
Uniform Resource Locator
ANALYSIS ON DYNAMIC BLOCKING INJUNCTIONS

by
Giancarlo Frosio and Oleksandr Bulayenko

On the basis of the analysis of norms, cases and practices in the EU and 12+1 selected MS (Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Lithuania, the Netherlands, Spain, Sweden and the UK) (Studied Member States or SMS) (§), this study identifies, describes and compares key aspects of blocking injunctions, with special emphasis on dynamic blocking injunctions. These aspects include the availability of static and dynamic blocking injunctions, their scope, balancing of rights and interests, required and/or admissible evidence, technical solutions applied and the implementation of dynamic blocking injunctions in the different jurisdictions.

1. Introduction

Blocking injunctions or blocking orders against so-called innocent third parties have become increasingly popular in Europe (§), especially with regard to online copyright – and more recently also...

(§) The authors are thankful to Fraser Simpson and Natasha Mangal, U.S. attorney, Ph.D. candidate at the CEIPI and Queen Mary University of London, for their research and editing contribution to the study.

(§§) When no further specific citations are given, Member States-specific information provided in this analysis and benchmarking refers to the information collected and reported through the national questionnaires (see Methodology).

trade mark – infringement (19). Their validity under EU law was confirmed by the CJEU in the *UPC Telekabel* decision (11). To put the EU practice on blocking injunctions into an international perspective it is worth noting that outside the EU website blocking of copyright-infringing sites has been authorised in countries such as Argentina, India, Indonesia, Malaysia, Mexico, South Korea and Turkey (12). In December 2014, Singapore amended its Copyright Act to enable rights holders to obtain website-blocking orders (13), and in 2015 Australia introduced website-blocking provisions to its Copyright Act (14). In the United States, although blocking orders are not customarily issued (15), internet access providers enjoying liability safe harbours may still be ordered by a court to perform injunctions ‘to block access, to a specific, identified, online location outside the United States’ (16). Blocking injunctions have also been coupled by the availability of forward-looking or dynamic blocking injunctions (DBI) both in Europe and other jurisdictions (17), such as Australia, India, Mexico and Singapore (18). These measures have been made available with the end of curbing intellectual property rights (IPR) infringement online, although negative effects on fundamental rights have also been highlighted (19).

While the availability of static blocking injunctions is recognised, dynamic blocking injunctions are not available in all SMs, and their scope and requirements vary among jurisdictions. This study identifies,


(12) See Swiss Institute of Comparative Law, *Filtering, blocking and take-down of illegal content on the Internet, a study commissioned by the Council of Europe, 20 December 2015*.


(14) See Copyright Amendment (Online Infringement) Act 2015 (Cth).

(15) There is only one early case that was voluntarily withdrawn by the plaintiff. See Arista Records, Inc. v AT&T Broadband Corp., 2002 WL 34593743 (S.D.N.Y., 16 August 2002) (with the plaintiffs seeking an injunction against internet backbone operators to block the Chinese website Listen4Ever). Rather than website blocking, U.S. authorities pursued domain name seizures as an alternative. In 2011, entities owning the rights to broadcast sporting events prevailed on U.S. authorities to seize the rojadirecta.com and .org domain names as part of the *Operation in Our Sites* anti-piracy campaign. Finally, upon US courts finding Rojadirecta non-infringing, the U.S. Department of Justice agreed to return the Rojadirecta domain names to the registrant. See Giancarlo Frosio, Alalalai!... Rojadirecta is Up for Battle Again in Italy, CIS Blog (6 September 2013). More recently, a US court has ordered ‘any Internet search engines, web hosting and Internet service providers, domain name registrars, and domain name registries [to] cease facilitating access to any or all domain names and websites though which ... Sci-Hub engages in unlawful access to, use, reproduction, and distribution of the [American Chemical Society] marks or copyrighted works’. The court ordered domain names registries and/or registrars to place Sci-Hub’s domain names on hold or such other status to render the names/websites non-resolving. See American Chemical Society v. John Does 1-99, et al., 1:17-cv-00726-LMB-JFA (E.D. Va., 3 November 2017).

(16) DMCA, § 512 (j) (1) (B) (ii).

(17) See Berdien B.E. van der Donk. How dynamic is a dynamic injunction? An analysis of the characteristics and the permissible scope of dynamic injunctions under European Law after CJEU C-18/18 (Glawischnig-Piesczek) (2020) 15 JIPLP 602–616.


analyses, and compares key aspects of the legal framework for static and dynamic blocking injunctions in the EU and selected MS.

2. Blocking Injunctions and Dynamic Blocking Injunctions in Europe

2.1 DEFINITION

Blocking injunctions (20) are among the remedies made available by the InfoSoc Directive and IPRED to protect IPR throughout the EU, although these measures are not implemented and applied in a uniform manner among the MS (21). The term (22) ‘blocking injunction’ refers to ‘an order requiring an internet intermediary to implement technical measures directed at preventing or disabling access to a specific internet location’ (23). Internet site-blocking injunctions can be implemented through DNS blocking, IP address blocking, or through uniform resource locator (URL) filtering.

A second category of blocking orders might also be available: so-called forward-looking or dynamic blocking injunctions, which are meant to allow flexibility so as to cover repeated infringements and, thus, enhance the effectiveness of the measures for rights holders. The Commission’s Guidance on the IPRED defines DBI as ‘injunctions which can be issued, for example, in cases in which materially infringing content is hosted. As they do not block access to the content but merely delist search engines’ entries that might lead to the location where the infringing content is hosted.

(20) Alongside blocking injunctions targeting access providers, injunctions have also been granted against search engine operators (e.g. in the form of de-listing/de-indexing and/or removing links directing to infringing content) and hosting providers (e.g. ordering the removal/takedown or ‘staydown’ of specific infringing items). These injunctions can also be dynamic, if they ‘staydown’, filter or delist content proactively, i.e. filtering/removing any new instances of infringing content already taken down that might be reuploaded online or delisting any new search engine’s entries leading to certain websites hosting infringing content, which have been already blocked in a different form and reappearing online elsewhere; however, these injunctions are outside the scope of this review, which focuses on blocking injunctions, whether static, dynamic or live. In particular, injunctions against search engines to delist content cannot be included within the category of blocking injunctions as they do not block access to the content but merely delist search engines’ entries that might lead to the location where the infringing content is hosted.

(21) Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, COM(2017)0708 final and SWD(2017) 432 final (the ‘Guidance’), Brussels, 29/11/2017, p. 1. Differences relate, among others, to the conditions to establish the urgency of a request, the type of evidence admissible, the type of intermediaries that can be subject to an injunction, the way in which judicial or administrative authorities can address imminent or repetitive infringements, or the availability of catalogue- or repertoire-wide injunctions.


(23) Jaani Riordan, The Liability of Internet Intermediaries, OUP, Oxford, UK, 2016, p. 461. See also Thomas Riis, Thomas Elholm, Ana Nordberg, et al., Study on Legislative Measures Related to Online IPR Infringements, study commissioned by the EU IPO, September 2018, p. 42 et seq.: ‘If an IPR infringing activity takes place on or through a dedicated website … it will be an effective way to disrupt the current activities and to prevent them from taking place in the future if the access to the website by the internet users in general is blocked’.
address or URL, and which are drafted in a way that makes it possible to also cover the new IP address or URL, without the need for a new judicial procedure to obtain a new injunction’ (24).

A third category of blocking orders, or more appropriately a subcategory of DBI, goes under the name of live blocking orders, which allow the repeated blocking of a site every time a live broadcast is in process. Live blocking allows for new servers to be identified by the rights holder and notified to access providers for blocking. It also ensures that old servers are not blocked after the end of a certain time (25).

2.2 Legislation

The legal basis of blocking injunctions can be found in multiple EU provisions. First, Article 18(1) of the e-commerce Directive instructs MS to ensure the availability of court actions against information society services’ activities to terminate any alleged infringement and prevent further impairment of involved interests (26). Meanwhile, the e-commerce Directive also limits the scope of its liability exemptions (‘mere conduit’, hosting and caching) by providing that the exemptions ‘shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information’ (27). The e-commerce Directive, thus, makes it possible for MS to make available blocking orders, issued by both judicial and administrative authorities, and confirms their consistency with EU law. However, a positive obligation to provide injunctions and legal redress to rights holders for IPR infringement within an EU law framework comes, instead, from the InfoSoc Directive. The InfoSoc Directive clarifies that the availability of these injunctions is made necessary because ‘in the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases, such intermediaries are best placed to bring such infringing activities to an end’ (28). Therefore, the InfoSoc Directive provides that ‘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’ (29). The limited copyright scope of the injunctions is then extended to IPR enforcement at large by the IPRED, which provides that ‘Member States shall also ensure that rightsholders are in a position to apply for an injunction against

(26) Directive (EC) 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-commerce Directive), Article 18(1). See also IPRED, Article 11 (providing that ‘Member States 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’).
(27) ibid., Article 14(3).
(29) ibid., Article 8(3).
intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC’ (35).

2.3 Proposed legislation

Some provisions in the recently proposed Digital Service Act (DSA) might also serve to harmonise the notion of injunctions against providers of digital or intermediary services. First, the DSA states that providers of intermediary services, including also access providers who are the target of blocking injunctions (31), must specify to the issuing judicial or administrative authority the action taken and the moment it was taken, upon receiving an order to act against illegal content (32). Second, the orders should be harmonised by including, inter alia, (i) a statement of reasons explaining why the information is illegal content under the law; (ii) one or more exact uniform resource locators and, where necessary, additional information enabling the identification of the illegal content; and (iii) information about redress available to the intermediary service and the provider of the content (33). Finally, the DSA sets up a system of national Digital Service Coordinators and providers that ‘[t]he Digital Services Coordinator from the Member State of the judicial or administrative authority issuing the order shall, without undue delay, transmit a copy … to all other Digital Services Coordinators’ (34).

2.4 Case-law

Whilst conditions and method for blocking injunctions are a matter of national law, the scope of these injunctions, and in particular whether blocking orders are compatible with EU law, has been confirmed by the CJEU through a number of decisions. Firstly, the CJEU confirms that the notion of ‘intermediary’ is broad, in particular, encompassing (Internet) access service providers, which is relevant for our purposes (35). In justifying this interpretation of the notion of intermediaries, the CJEU explains in UPC Telekabel that ‘given that the internet service provider is an inevitable actor in any transmission of an infringement over the internet between one of its customers and a third party, since, in granting access to the network, it makes that transmission possible …, it must be held that an internet service provider … is an intermediary whose services are used to infringe a copyright or related right within the meaning of Article 8(3) of [the InfoSoc] Directive 2001/29’ (36). In general, the CJEU clarifies that for an economic operator to be considered as an ‘intermediary’, it is sufficient that they provide, inter alia, a service capable of being used to infringe IPRs.

(36) UPC Telekabel, para. 32.
Secondly, in *Mc Fadden*, the CJEU clarifies that the ‘mere conduit’ exemption, pursuant to Article 12(1) of the e-commerce Directive, does not preclude a person from claiming injunctive relief from an access provider against the continuation of an infringement occurring through that access provider’s network (37). Therefore, injunctions must be available in MS to order an access provider to prevent continuation of the infringement. This implies that copyright holders can seek injunctions to stop future infringements, given that these injunctions respect the balance between the interests at stake and protect fundamental rights (38).

Thirdly, the CJEU makes clear that blocking orders would fall under Article 8(3) InfoSoc Directive and Article 11 IPRED (39). Besides the general compatibility of blocking injunctions with EU law, *UPC Telekabel* also clarifies that blanket injunctions are compliant with EU law (40). The CJEU was called to answer the question of whether blocking injunctions should be an obligation of means or an obligation of results. Confirming the latter interpretation of blocking injunctions, the CJEU spelled out the availability under EU law of blocking injunctions that just instruct on the blocking of a certain website without specifying the technical means that should be deployed by the access providers to block access to the relevant infringing content. Therefore, access providers will be liable for non-compliance with the blocking orders regardless of any consideration of the technicalities involved in reaching the result prescribed by the order.

Finally, reaching this conclusion, *UPC Telekabel* also plays a relevant role in potentially supporting the availability under EU law of dynamic blocking injunctions, which are in fact broader injunctions that impose an obligation of results via the blocking of identical or equivalent websites with different IP addresses or URLs, rather than a narrower obligation of using specific technical means to block a specific IP address or URL (41). In addition, the availability of dynamic blocking injunctions is apparently confirmed by the CJEU in *L’Oréal*, when stating that injunctions pursuant to Article 11 of the IPRED must be available ‘to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind’ (42). Although discussing injunctions as part of the activities of a hosting provider, such as eBay, by concluding that injunctions may be aimed at stopping existing infringements and also preventing

(37) See 15/09/2016, C-484/14, Tobias Mc Fadden v Sony Music Entertainment Germany Gmbh, EU:C:2016:689 (Mc Fadden), para. 79.

(38) ibid., para. 101.

(39) *UPC Telekabel*, para. 40. See also 14/06/2017, C-610/15, Stichting Brein v Ziggo BV and XS4All Internet BV [2017], EU:C:2017:456 (ordering the Dutch access providers Ziggo and XS4ALL to block the torrent search engine The Pirate Bay).

(40) ibid., para. 64.

(41) In this context, the conclusions of 03/10/2019, C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Ltd [2019], EU:C:2019:821 (Glawischnig-Piesczek) might also be applied by analogy. In *Glawischnig-Piesczek*, the CJEU has broadened the scope of monitoring ‘in a specific case’ with reference to content identified as illegal by national courts, as in the case of a defamatory comment posted by an anonymous Facebook user. In this case, a platform like Facebook might be requested to block and remove identical content and content with equivalent meaning; however, the elements of equivalent information should be specifically identified in the injunction and the digital service provider should not carry out any independent assessment of the content. Therefore, an argument can be made that blocking injunctions can be applied dynamically to identical or equivalent websites and content to be blocked as long as no independent assessment must be carried out by the access provider subject to the blocking order. See also OGH 30.03.2020, ORF/Facebook, 4Ob36 / 20b [4.1]-[4.5] (Austria) (applying Glawischnig-Piesczek and concluding that, for an injunction to be lawful under EU law, content similar in its core should be identifiable ‘at first glance’ or determined by ‘technical means’ which would not impose excessive control obligations on Facebook).

further infringements, the CJEU confirms that injunctions with a dynamic scope would be compatible with EU law. This conclusion can be applied *mutatis mutandis* to dynamic blocking of infringing websites by access providers. The Commission has stated that ‘whilst this issue is not expressly addressed in IPRED, the Commission considers that, under the condition that necessary safeguards are provided for, such injunctions can be an effective means to prevent the continuation of an IPR infringement’ (43).

2.5 Administrative orders

In line with the provision in Article 14(3) of the e-commerce Directive, some SMS have adopted enforcement models in which administrative authorities are also competent to issue website-blocking orders, as is in the case of Greece, Italy, Lithuania and Spain (44). The following administrative authorities are competent to order blocking injunctions: (i) the Committee for the Notification of Copyright and Related Rights Infringement on the Internet (EDPPI) (45) (Greece); (ii) the Autorità per le Garanzie nelle Comunicazioni (AGCOM) (Italy); (iii) the Radio and Television Commission of Lithuania (46) (Lithuania); and (iv) the Comisión de Propiedad Intelectual, Sección Segunda (Spain) (47). Italy has also endorsed this model, by empowering AGCOM, the Italian Communication Authority, to deal with online copyright enforcement, including the power of issuing blocking orders (48). Furthermore, at the end of a procedure that occurs online, if the AGCOM decision-making body is satisfied that the alleged infringement has occurred, and the infringing website is hosted outside Italy, it can order ‘mere conduit’ (Internet) service providers to block access to the website (49). This has led to more than 700 domain names being blacklisted, according to data from 2019 (50), a number that will be growing faster given that the 2018 amended Regulation enables rights holders to request AGCOM to adopt a fast track procedure to issuing dynamic blocking orders (51). In Greece, Italy and Spain, use of the administrative procedure does not prevent the filing of civil or criminal actions, the latter being enforceable.

(43) Guidance, supra fn 21, p. 21. The IPRED communication guidance also aggregates and confirms the abovementioned principles deriving from case-law.

(44) See Alessandro Cogo and Marco Ricolfi, ‘Administrative Enforcement of Copyright Infringement in Europe’, in Giancarlo Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability*, OUP, Oxford, UK, 2020, pp. 586-602. Please consider that Portugal has also provided an administrative authority, the Inspeção-geral das Atividades Culturais, with copyright enforcement powers. In Belgium, the government had been working on a draft bill aimed at better fighting online copyright infringement (notably via a federal administration department), but there is nothing concrete at the moment.

(45) See Law 2121/1993, Article 66E.

(46) See Law on Copyright and Related Rights, Article 78.

(47) See Spanish Copyright Act, Article 195.

(48) See Regolamento in materia di tutela del diritto d’autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70 (‘AGCOM Regulation’). See also, for an English commentary of the main provisions and procedures, Giancarlo Frosio, *Italian Communication Authority Approves Administrative Enforcement of Online Copyright Infringement*, Stanford CIS Blog, 17 December 2014.

(49) AGCOM Regulation, Article 8, para. 4.

(50) Cogo and Ricolfi, p. 607.

(51) AGCOM, *Delibera n. 490/18/CONS, Modifiche al Regolamento in materia di tutela del diritto d’autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70*, di cui alla delibera n. 680/13/CONS, available at www.shorturi.at/ipsIM (providing, inter alia, that the Directorate for Media Services, on request from the rights holder, can extend the effects of an already issued blocking order if it deems that the violation is actually the same). See also Cogo and Ricolfi, p. 607 ft. 142.
available in Italy and Spain. In Greece, if the same applicant has already brought the same claim before the ordinary courts, the case will be filed by the EDPPI. In Lithuania, the Vilnius Regional Administrative Court will sanction injunctions made by the Radio and Television Commission of Lithuania.

In Germany, it seems possible that administrative authorities under general criminal procedural law and specific administrative law provisions may request blocking, but there is only limited practice to date. Usually, blocking injunctions are requested under civil law as per Section 7(4) of the German Telemediengesetz (TMG), which implements EU law (Article 8(3) InfoSoc Directive and Article 11 IPRED). In France, administrative authorities can order blocking injunctions for infringement of criminal provisions other than IP (e.g. child pornography or terrorism).

2.6 Soft law

‘Soft law’ arrangements such as codes of conduct (CoC) or voluntary measures have been established in several of the SMS (52). In Denmark and the UK, self-regulatory measures were established between stakeholders in relation to IP. In Denmark, the most notable arrangement is the ‘Code of Conduct for handling decisions on blocking access to services, infringing intellectual property rights’ between the Telecommunications Industry and the Rights Alliance (53). There is a voluntary CoC in place between the major search engines that operate in the UK, including Google, Bing and Yahoo, and other relevant stakeholders in relation to the demotion of copyright-infringing websites. In Belgium, a general CoC adhered to by members of the Belgian Internet Service Providers Association (ISPA) (54) sets up a central contact point within the judicial police to receive complaints about illegal activity on the internet, including copyright infringement. In Finland, there is a voluntary mechanism to block foreign websites, but its scope is limited to child pornography. The Finnish police maintains a record of foreign child pornography websites, and ISPs may use it to prevent access to them (55). A specific regulatory framework for developing codes of conduct exists in Italy, which provides that (i) business, professional or consumer associations or organisations promote the adoption of codes of conduct that inform the Ministry of Productive Activities and the European Commission of any useful information on their application and their impact on practices and habits related to e-commerce; (ii) the code of conduct, if adopted, must be made available electronically and will be drawn up, in addition to Italian and English, at least in one other EU language; and (iii) when drawing up codes of conduct, the protection of minors and human dignity must be guaranteed. Internet service providers can implement codes of self-conduct, regulating the review of claims concerning (among others) any unlawful behaviour by their clients (56).

(52) In some SMS, such as the Netherlands, ISPs have been reluctant to enter into a CoC with the copyright industry.
(53) The recently revised version of the CoC is dated 18 May 2020 and is available at: https://rettighedsalliancen.dk/ (in Danish).
(55) See Act on measures to prevent the distribution of child pornography (2006/1068).
(56) See Legislative Decree 70/2003, Article 18.

3.1 The fundamental rights framework

The balancing of rights and interests should guide the issuance of static and dynamic blocking injunctions and their availability. First, in order to guarantee proportional balancing of fundamental rights, DBI must be consistent with the constitutional legal framework set up by the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights or ECHR) (58), as interpreted by the ECtHR and, in particular, by the Charter of Fundamental Rights of the European Union (EU Charter) (59), as interpreted by the CJEU. In this regard, the fundamental right to freedom of expression, under Article 10 ECHR and Article 11 EU Charter, does not solely guarantee the right to impart information but also to the right of the public to receive information (60), including the ‘right to internet access’, a right that is becoming fundamental in the eyes of many (61). The rationale behind the ‘right to internet access’ is that ‘the Internet, by facilitating the spreading of knowledge, increases freedom of expression and the value of citizenship’ (62). The Council of Europe expressly stated that access to the internet is a ‘fundamental right’ in a response to a proposal on ‘three-strikes’ legislation (63). In a June 2009 decision on the first HADOPI law, the French Constitutional Council stated that ‘[i]n the current state of the means of communication and given the generalised development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, [the right to freedom of expression] implies freedom to access such services’ (64). The status of the fundamental right of the right of access to the internet has been highlighted by several high-
profile organisations, including the UN Human Rights Council\(^{(65)}\) and the ITU-UNESCO Commission\(^{(66)}\). The ECtHR concluded, after conducting a survey of legislations in 20 Council of Europe MS, that:

> [t]he right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens\(^{(67)}\).

This makes any action that affects the accessibility of the internet an interference with the rights guaranteed by Article 10 ECHR\(^{(68)}\). In particular, websites, as means of dissemination of information, benefit from the protection afforded under Article 10 ECHR, since ‘any restriction imposed on such means necessarily interferes with the right to receive and impart information’\(^{(69)}\). The European Commission echoed this by stating: ‘[a]ny limitations to access to the Open Internet can impact on end-users’ freedom of expression and the way in which they can receive and impart information … there are many instances when unjustified blocking and throttling occurs’\(^{(70)}\). Consequently, a Google service facilitating the creation and sharing of websites\(^{(71)}\), as well as a video-hosting website\(^{(72)}\) and a website enabling users to share digital content\(^{(73)}\), were regarded as means of information dissemination. Article 10 ECHR and Article 11 EU Charter provide at least five conditions that can be extracted from the practice of the European Courts and that a court must consider when ruling on a website-blocking case. First, the manner of the site usage. Second, the effect on legitimate communication caused by blocking the site. Third, the public interest in accessing the information. Fourth, whether the information is available in another form. Fifth, the effect on internet users and intermediaries under Article 10 ECHR\(^{(74)}\).

---


\(^{(66)}\) See Kaitlin Mara, ITU-UNESCO Broadband Commission Aims at Global Internet Access, IPWatch, 10 May 2010.

\(^{(67)}\) Yildirim, supra fn 60, para. 31.

\(^{(68)}\) See Cengiz, supra fn 60, para. 57.

\(^{(69)}\) Yildirim, supra fn 60, para. 50. See also Cengiz, supra fn 60, para. 56.


\(^{(71)}\) See Yildirim, supra fn 60, para. 49.

\(^{(72)}\) See Cengiz, supra fn 60, para. 54.

\(^{(73)}\) See Neij and Sunde Kolmisoppi v Sweden (dec.) App. no. 40397/12 (ECtHR, 19 February 2013).

In the recent cases of Vladimir Kharitonov v Russia (75), OOO Flavus and Others v Russia (76), Bulgakov v Russia (77), and Engels v Russia (78), the ECtHR addressed the problem of wholesale blocking. Where the authorities targeted entire websites without distinguishing between the legal and illegal content, it was found to be the equivalent of banning a newspaper or television station (79). This ‘deliberately disregards the distinction between the legal and illegal information the website may contain, and renders inaccessible large amounts of content which has not been identified as illegal’ (80). The ECtHR examined blocking measures where whole websites were blocked due to a single piece of content, as well as continued blocking even after the infringing content had been removed (81). All these measures were found to be unlawful, including in cases regarding prohibited e-books (82) and information about filter-bypassing technologies (83). Shortcomings identified by the ECtHR included the broad discretion to impose blocking measures afforded by law to an executive agency, causing content to be blocked arbitrarily and excessively. Therefore, the powers of state authorities must be clearly circumscribed to minimise the impact of these measures on internet access (84). The ECtHR also drew attention to the lack of procedural guarantees, notably the absence of court orders sanctioning blocking measures, impact assessments prior to implementation, advance notification to affected parties and proportionality assessments in court decisions, before implementing blocking measures (85). Therefore, although website-blocking orders are not per se contrary to Article 10 ECHR, this particular measure should be considered within a balanced legislative framework that contains robust safeguards against abuse.

Similarly, although the CJEU has confirmed the availability of blocking orders under EU law, the CJEU case-law has also recognised users’ rights as enforceable against injunctions that might curb their freedom of expression online (86). First, in the McFadden judgment, the CJEU has confirmed that injunctions against access providers to prevent the continuation of an infringement occurring through their network are available only if such injunctions respect the balance between the interests at stake and protect fundamental rights, with special emphasis on the right to protection of intellectual property, the provider’s freedom to conduct business, and the freedom of information of the recipients of the service (87). According to the CJEU, in order not to impinge on fundamental rights, measures adopted to implement a blocking order must be strictly targeted by (1) bringing to an end a third-party’s copyright or related right infringement, (2) without thereby affecting internet users using the online

(75) App. no. 10795/14 (ECtHR, 23 June 2020) (‘Kharitonov’). For commentary, see Elena Izyumenko, European Court of Human Rights Rules That Collateral Website Blocking Violates Freedom of Expression (2020) 15(10), JIPLP 774-775.
(76) App. nos 12468/15, 23489/15 and 19074/16 (ECtHR, 23 June 2020) (‘Flavus’).
(77) App. no. 20159/15 (ECtHR, 23 June 2020) (‘Bulgakov’).
(78) App. no. 61919/16 (ECtHR, 23 June 2020) (‘Engels’).
(79) Kharitonov, supra fn 75, para. 38; Flavus, supra fn 76, para. 37.
(80) ibid.; Bulgakov, supra fn 77, para. 34.
(81) ibid., para. 30.
(82) ibid.
(83) Engels, supra fn 78, para. 29.
(84) Kharitonov, supra fn 75, paras 38, 43.
(85) ibid., paras 43, 45.
(86) UPC Telekabel, supra fn 11, para. 57. See also Christophe Geiger and Elena Izyumenko, ‘Blocking Orders’, pp. 566-585 (highlighting the difficult coexistence between blocking orders and fundamental rights, including freedom of expression and freedom to conduct a business).
(87) Mc Fadden, supra fn 37, paras 80-101.
services in order to lawfully access information\(^{(88)}\). Otherwise, the users’ right of freedom of information would be unjustly limited, and measures cannot be issued. The CJEU has also acknowledged that the blocking of websites involves the right of freedom of expression of internet access providers\(^{(89)}\). This has been highlighted by the Advocate General (AG) in the case of *Telekabel*: “[a]lthough it is true that, in substance, the expressions of opinion and information in question are those of the ISP’s customers, the ISP can nevertheless rely on that fundamental right by virtue of its function of publishing its customers’ expressions of opinion and providing them with information’\(^{(90)}\). The AG made reference to ECtHR precedent that provided ‘Article 10 guarantees freedom of expression to “everyone”, [with] [n]o distinction [being] made in it according to the nature of the aim pursued or the role played by natural or legal persons in the exercise of that freedom’\(^{(91)}\). Furthermore, the ECtHR noted that although ‘publishers do not necessarily associate themselves with the opinions expressed in the works they publish, … by providing authors with a medium they participate in the exercise of the freedom of expression’\(^{(92)}\).

In all SMS, fundamental rights must be considered by courts when balancing rights and interests in issuing blocking orders. In fact, ordinary courts, administrative courts and authorities in the SMS have been specifically referring to fundamental rights balancing either directly or indirectly\(^{(93)}\). Freedom of expression and information is broadly cited (e.g. in Belgium, Denmark\(^{(94)}\), France, Ireland, Italy, the Netherlands, Sweden and the UK), followed by the freedom to conduct a business (e.g. in Belgium, Ireland, the Netherlands and Sweden), right to property (e.g. in France, Sweden and the UK) and the protection of personal data (e.g. in Ireland). Fundamental rights analysis is based on different instruments depending on the SMS, including the ECHR and the EU Charter (e.g. in Belgium, France\(^{(95)}\), Ireland\(^{(96)}\), Italy and the UK\(^{(97)}\)), national constitutions (e.g. in Denmark\(^{(98)}\) and Italy\(^{(99)}\)).

\(^{(88)}\) See *UPC Telekabel*, supra fn 11, para. 57.

\(^{(89)}\) See on this issue extensively, Geiger and Izyumenko ‘The Role of Human Rights in Copyright Enforcement Online’, supra fn 74, 43 ff.

\(^{(90)}\) See *UPC Telekabel*, 2013, Opinion of AG Villalón ECLI:EU:C:2013:781, para. 82 (hereafter ‘Telekabel, Opinion of AG Villalón’).

\(^{(91)}\) Öztürk v Turkey App. no. 22479/93 (ECtHR, 28 September 1999) para. 49.

\(^{(92)}\) Ibid.

\(^{(93)}\) Some exceptions apply. For example, some Spanish courts have not explicitly considered fundamental rights. See Juzgado de lo Mercantil no. 7, Madrid [Commercial Court no. 7 of Madrid], 11 February 2020, Telefónica Audiovisual Digital y. Vodafone España et al., decision no. 2174/2019, ECLI: ES:JMM:2020:2 (‘Commercial Court of Madrid 2174/2019’). Finnish courts seem to make only indirect references to fundamental rights. When assessing the reasonability of the measures, the Finnish Market Court, although considering possible effects of an injunction on all parties involved, has not however directly cited fundamental rights and freedoms. The court has only made reference to the Copyright Act and its preparatory works, where the rights are tightly connected to several fundamental rights protected by the Finnish Constitution, such as freedom of expression and right of access to information, protection of property, and the right to work and the freedom to engage in commercial activity.

\(^{(94)}\) The freedom of expression was said to be the only fundamental rights mentioned in Danish cases. Reference to fundamental right balancing seems to be rarer than in other SMS.

\(^{(95)}\) See TGI Paris, 15 December 2017, no. 17/13471 (‘TGI Paris 17/13471’).

\(^{(96)}\) See Sony Music Entertainment (Ireland) & Ors v UPC Communications Ireland Ltd [2016] IECA 231 (mentioning freedom to receive or impart information; right to protection of personal data; and freedom to conduct a business).


\(^{(98)}\) § 77 of the Danish Constitution (freedom of expression).

\(^{(99)}\) Section 21 of the Italian Constitution (freedom of expression).
and/or IP provisions, with special emphasis on communication to the public (e.g. in Belgium and Germany).

In France and the UK, judges have been specifically discussing the balancing between freedom of expression and information and the right to property, while considering the limitations that blocking injunctions can impose on freedom of expression. French courts held that in balancing freedom of expression as protected by Article 10 of the ECHR and the rights of authors or producers, it should be borne in mind that the latter suffer serious prejudice as a result of the hundreds of thousands of visitors to the disputed sites\(^{(100)}\). Therefore, French courts, after having considered freedom of expression and information, and on occasions the freedom to conduct a business, upheld blocking measures as strictly necessary to preserve the plaintiffs’ rights as they make it possible to prevent or stop massive copyright infringement, as long as they are targeted towards precisely identified domain names and limited in time. In the UK, courts have reached similar conclusions. For instance, in *Newzbin2* the judge noted that:

in general, I am satisfied that the order sought by the Studios is a proportionate one. It is necessary and appropriate to protect the Article 1 First Protocol rights of the Studios and other copyright owners. Those interests clearly outweigh the Article 10 rights of the users of Newzbin2, and even more clearly outweigh the Article 10 rights of the operators of Newzbin2. They also outweigh BT’s own Article 10 rights to the extent that they are engaged. The order is a narrow and targeted one, and it contains safeguards in the event of any change of circumstances\(^{(101)}\).

In *EMI Records*, and in the context of website blocking orders targeting copyright-infringing BitTorrent websites, the judge held, in a similar fashion, that IPRs:

clearly outweigh the Charter Article 11 rights of the users of the Websites, who can obtain the copyright works from many lawful sources. They even more clearly outweigh the Article 11 rights of the operators of the Websites, who are profiting from infringement on an industrial scale. They also outweigh the Defendants’ Article 11 rights to the extent that they are engaged\(^{(102)}\).

The same balancing has been found in the case of live blocking. In *Football Association Premier League (FAPL) Ltd v British Telecommunications plc* [2017] EWHC 480 (Ch), a UK court has compared FAPL’s copyright, access providers’ freedom to conduct a business and internet users’ freedom to impart or receive information by finding that (i) FAPL, as well as its licensees BT and Sky, had a legitimate interest in curtailing the infringement of its copyright; (ii) given FAPL’s role in supporting sport in the UK and the substantial contributions it has made and its licensees to the UK economy, there was a public interest in combating infringements of its rights; (iii) the orders sought would not impair the substance of the access providers’ right to conduct a business as it would not interfere with the provision of their services to their customers or require investment in new

\(^{(100)}\) See TGI Paris 17/13471, supra fn 95.

\(^{(101)}\) *Newzbin2*, supra fn 97, para. 200.

\(^{(102)}\) *EMI Records*, supra fn 97, para. 107.
technology (103); and (iv) the freedom of internet users to impart or receive information did not extend to a right to engage in copyright infringement.

In sum, the availability of static and dynamic website blocking injunctions is compelled on international courts, such as the ECtHR and CJEU, by the need to find a proportional equilibrium between competing rights – given the scale of the costs of online enforcement – according to the doctrine of ‘fair balance’ among fundamental rights (104). According to this principle, as construed by the CJEU, the ECtHR and national courts, blocking injunctions should be available only if they are strictly targeted to bring infringement to an end and if they do not impinge on fundamental rights. The same applies to dynamic blocking, which actually, on one side, increases targeting and efficiency of IP enforcement and, on the other side, could expand over-blocking of non-infringing material. Targeting and efficiency are especially enhanced by live blocking injunctions, which allow for new servers to be identified, while over-blocking is limited by de-blocking older servers after a brief period of time.

3.2 Proportionality

3.2.1 EU law

Second, in balancing rights and interests when issuing DBI, competent courts and authorities need also to comply with Article 3 of the IPRED and the general principles of EU law. Therefore, these measures must (1) be fair and equitable; (2) not be unnecessarily complicated or costly; (3) not entail unreasonable time limits or unwarranted delays; (4) be effective, proportionate and dissuasive; (5) be applied in such a manner as to avoid the creation of barriers to legitimate trade; and (6) provide for safeguards against their abuse (105). In consideration of Recital 41 of the e-commerce Directive, which strives for a balance of different interests at stake, an injunction under Article 18(1) therein should not impose an ‘excessive obligation’ on the internet service provider (106). In addition, Recitals 58 and 60 of the e-commerce Directive clarify that, ‘[i]n order to allow the unhampered development of electronic commerce’, EU rules and the measures ‘must be clear and simple, predictable and consistent with the rules applicable at international level’ (107).

(103) The orders would only impose additional operating costs on the access providers, while any risk of reputational damage, particularly in the event of over-blocking, was not considered to be significant.


(105) IPRED, Article 3.

(106) Glawischnig-Piesczek, supra fn 41, para. 44 (discussing obligation of hosting providers).

(107) e-commerce Directive, supra fn 26, Recital 60.
3.2.2 National standards

In most SMS, courts must assess the proportionality of the measure, which is usually done on a case-by-case basis according to several national standards, for example.

(i) In Belgium, France and Ireland, courts have concluded that the mere fact that an injunction is not capable of ending illegal activities does not make it disproportionate, as long as it is sufficient that the injunction seriously discourages internet users from engaging in infringing activities, making the infringement more difficult (108). In light of these proportionality considerations, Belgian courts generally order DNS blocking, which is easier to bypass, rather than IP blocking, which is more effective for rights holders but more costly, more difficult to implement and riskier because of the undesirable collateral effects it may cause for intermediaries.

(ii) In France, courts held blocking measures proportionate. They do not apply the principle of subsidiarity according to which the implementation of measures should only take place after measures have been taken against those directly liable for the infringement (109).

(iii) In Denmark, blocking injunctions can be applied as a last resort, if other remedies cannot be effectively applied, as, according to general principles, injunctions should not be issued when they can be replaced by penalties, damages and securities (110). In particular, courts should not grant injunctions ‘if it will cause harm or inconvenience to the other party which is manifestly inconsistent with the party’s interest in issuing the prohibition or injunction’ (111).

(iv) German courts have concluded that the presence of just some legal content is insufficient to prevent a website been blocked and that a case-by-case assessment must always be performed by the courts. In particular, the operator of a website, whose business model is based on copyright infringement, cannot hide behind a tiny fraction of legal content, to the extent that the Bundesgerichtshof (BGH), the German Federal Court of Justice, has found blocking reasonable for websites containing only 4% legal content (112). A similar standard seems to be applied by the CJEU as well in Ziggo, which requires a de facto substantial non-infringing uses standard for avoiding primary liability and, thus, for imposing blocking injunctions pursuant to Article 8(3).

---


(109) See TGI Paris 17/13471, supra fn 95.

(110) See Administration of Justice Act (AJA), § 414, 1 (stating ‘Prohibitions or injunctions cannot be issued when it is deemed that the general rules of the law on penalties and damages and possibly a security offered by the counterparty provide the party with sufficient protection’).

(111) ibid., § 414, 2.

of the InfoSoc Directive on access providers (113). Apparently, a substantial non-infringing uses approach – that excludes defences based on limited availability of legal content on the websites for which blocking injunctions are sought – might emerge as an EU-wide standard for blocking injunctions.

(v) Some SMS have clarified that blocking injunctions cannot lead to general monitoring. In Finland, the Market Court referred to the Government’s Proposal for the amendment of the Copyright Act in 2015, stating that blocking injunctions cannot lead to general monitoring obligation for intermediaries (114). The Market Court should take into consideration to what extent the order would prevent other legitimate activities, especially the right of the third parties to receive and impart information, and whether the nature and severity of the allegedly copyright-infringing activities would outweigh those (115). In imposing dynamic measures against Google, French courts clarified that they did not consist of a general monitoring and filtering obligation, since Google is simply asked to delist mirror sites of the sites listed in the decision.

(vi) In the UK, courts are always required to assess the proportionality of a blocking injunction, ensuring that the order is appropriate, even if the terms have already been agreed by the parties. In Dramatico Entertainment, the High Court affirmed ‘where … the terms of the orders have been negotiated between the parties [the Court must still] independently … consider the proportionality of the proposed orders from the perspective of individuals affected by them who are not before the Court’ (116).

3.2.3 Injunction against some but not all access providers

In Ireland and Spain, a blocking injunction requested against a few but not all ISPs (e.g. against 2 out of 10 existing ones) can be rejected on the basis of proportionality considerations. Spanish courts have been considering the need to preserve homogeneity among ISPs, so that the implementation of blocking orders does not result in a migration of clients to those ISPs that do not implement blocking (117). In most SMS, however, that is not the case (e.g. in Belgium, Finland, France, Germany, Italy and the UK). In France, courts noted, in validating the selective application of the blocking injunction, that the clientele of the defendants represented the majority of French internet users, which justifies the measures (118). In Italy, courts gave a negative answer to the same question (119). In the


(115) ibid., 54.

(116) Dramatico Entertainment Ltd v British Sky Broadcasting Ltd & Others [2012] EWHC 1152 (Ch), para. 11.

(117) See Commercial Court of Madrid 2174/2019, supra fn 93.

(118) e.g. Google search engine.

(119) Italian Supreme Court, 17 July 2015, no. 31022 (‘With reference to preventive seizure, the judicial authority, if the conditions of the “fumus commissi delicti” and the “periculum in mora” are met, may order, in compliance with the principle of proportionality, the preventive seizure of an entire website or a single telematic page, requiring the provider of internet services, even in an emergency, to obscure an electronic resource or to prevent access to users in accordance with Articles 14, 15 and 16 of Legislative Decree no. 70 of 9 April 2003, as the equalization of computer data with things in the
UK, in *Newzbin2*, Arnold J stated that he could ‘see nothing in Recital (59), Article 8(3) or section 97A which obliges rightsholders to seek injunctions against all relevant intermediaries. As with any other legal remedy, the [applicants] are entitled to decide against whom to seek the remedy’ *(120).*

### 3.2.4 Risk of over- and under-blocking

In most SMS, dynamic injunctions address the risk of over- and under-blocking (e.g. in Denmark, France, Germany, Ireland, Italy, the Netherlands, Sweden and the UK), although some might be lacking in that respect (e.g. Lithuania and Spain). A number of different strategies have been put in place in the SMS to address the risk.

(i) In France, case-law makes rights holders responsible for informing intermediaries if some of the ‘access roads’ to the illicit websites mentioned in the decision are no longer active or no longer give access to infringing content.

(ii) In Ireland, the measures to address over-blocking are agreed in advance between the parties and then approved by the Court.

(iii) In Italy, dynamic injunctions usually balance conflicting interests of rights holders and access providers by limiting the scope of injunctions so as to avoid over-blocking *(121).*

(iv) In the Netherlands, the absence of the alleged infringers in the procedure means that the judge has to be cautious about measures concerning access to the internet *(122).* If an order or measure imposed as a result of these proceedings should at any future time appear to be no longer compatible with a fair balance between the fundamental rights concerned because of changed circumstances, Dutch law provides sufficient possibilities for the adequate protection of those fundamental rights which the CJEU has in mind in the *UPC Telekabel* judgment.

(v) In the UK, courts must take into account the risks of over- or under-blocking of access providers. In this respect, the orders must ‘contain a number of safeguards against abuse, such as permitting both the ISPs and the operators of the target websites to apply to the Court to discharge or vary the orders in the event of any material change of circumstances’ *(123).* For example (i) where an IP address ceases to be a location that enables access to the infringing content, or (ii) where a target website moves to an IP address where the server at that IP address hosts a site or sites that are not part of a target website, the access provider, or any affected third party, must be able to challenge the decision with the court.

---


*(121) See for example Court of Milan, 3 September 2019 (ordering to block access to ‘the aliases resulting from changes to the second level domain relating to all current sites-showcase and those associated with the main servers indicated provided that – in addition to referring to the same illegal content considered above – the subjective connection with the subjects responsible for the illegal activity currently in place is objectively detectable also through communications from the subjects responsible to their respective subscribers of specific indications to reach another site otherwise named’).*

*(122) Court of The Hague, Brein v Ziggo/XS4All, 11 January 2012, § 4.44.*

*(123) See Cartier Int’l v British Sky Broadcasting [2014] EWHC 3354 (Ch), para. 262 (Cartier 2014).*
Risk of over-blocking is tightly scrutinised in live blocking orders. In the UK, which has more widely used this measure so far, the applicant (i) must reasonably believe that any server notified for blocking has the sole or predominant purpose of enabling or facilitating access to infringing streams; and (ii) must not know or have reason to believe, that the server is being used for any other substantial purpose. Further, to reduce the risk of over-blocking, the list of servers to be blocked is reset periodically (in the later Premier League cases as often as weekly) \(^{(124)}\) in order to ensure that servers are not blocked for longer than necessary.

4. Availability and Issuance Requirements

4.1 Blocking injunctions

4.1.1 Availability

In all the SMS, blocking injunctions are available in the context of (alleged) IPR infringements. The legal basis for blocking injunctions is provided by national legal instruments transposing Article 8(3) of the InfoSoc Directive and Article 11 of the IPRED and/or other national legislation \(^{(125)}\).

4.1.2 Subject matter

Traditionally issued to block access to copyright-infringing websites \(^{(126)}\), blocking injunctions have been broadening their scope to different IPRs, including trade marks, and potentially other IPRs. Blocking injunctions apply to different subject matter depending on the different jurisdictions. France, Greece and Ireland have an emphasis on copyright and related rights, while Belgium, Finland, Germany, Italy, Lithuania, the Netherlands, Spain and the UK have broader coverage expanding to IPRs in general \(^{(127)}\). Obviously, in the SMS, website blocking is also available as a remedy against other miscellaneous forms of infringement of civil and criminal law, including defamation, child pornography, and dangerous and terrorist speech.


\(^{(125)}\) Unlike most SMS, Germany has not implemented this provision by statute, relying instead on the courts to develop jurisprudence concerning contributory infringement into an instrument effectively implementing Article 8(3), via the application of the so-called Störerhaftung doctrine. See infra fn 161. In this context, in 2015 the Bundesgerichtshof (BGH), the German Federal Court of Justice, has ordered website blocking for the first time in two landmark decisions. In these cases, the BGH ordered access providers to block access to websites providing links to predominantly illegal content. See BGH, Störerhaftung des Access-Providers, supra fn 112.

\(^{(126)}\) See for example Nordemann, supra fn 35, pp. 363-366 (noting that website blocking has primarily concerned infringements of the rights of communication to the public).

\(^{(127)}\) As well as including copyright infringement, such as circumvention of technical measures. See infra para. 5.1.2.
4.1.3 Targeted intermediaries

In the SMS, blocking injunctions have been granted against the following intermediaries: (i) any 'intermediaries' whose services are used by a third party to infringe relevant IPRs (e.g. Belgium (including DNS registries), Finland (128), France, Greece, Italy, Lithuania (preliminary injunctions), the Netherlands, Spain); (ii) internet access providers/internet service providers (Germany, Denmark, Ireland, Lithuania (final injunctions), Sweden and the UK). In Denmark, blocking injunctions could also be applied to 'web hosting service providers'. In Germany, the notion also includes DNS resolver providers (in the case of DNS blocks) (129) and Wi-Fi providers.

4.1.4 Issuance requirements

Requirements for obtaining a blocking injunction differ in the SMS. There are, however, some common general requirements, including: (i) to provide evidence of the allegedly infringed entitlements such as ownership of the rights and the status of the rights holder acting to protect relevant interests (e.g. in Germany, Italy and Spain); (ii) to demonstrate that the blocking injunction is aimed at an **infringing service provider and/or whose services are being used to infringe** (e.g. in Belgium, Denmark, Finland, France, Greece, Italy, Lithuania, the Netherlands (130), Sweden and the UK), which implies also the provision of evidence of the alleged infringement (131); (iii) that the requested blocking injunction is proportionate (e.g. in Belgium, Germany (132), Ireland, the Netherlands (133), Spain, Sweden and the UK); (iv) that the requested blocking injunction is appropriate (e.g. Sweden and the UK) and/or necessary (e.g. Ireland), which sometimes is understood as the requirement to demonstrate that there is 'no other reasonable option' (Germany) (134) or that without the requested blocking injunction the rights holders will be severely prejudiced (e.g. Denmark, Finland and Lithuania); (v) that the requested blocking injunction is 'reasonable' (e.g. Finland, Germany (135) and Ireland) (136).

(128) In Finland, the concept of 'intermediary' does not apply, for instance, to 'community subscribers or property intranet owners'.

(129) See OLG Köln, GRUR 2021, 70 – Herz Kraft Werke.

(130) See Copyright Act, Article 26d; Related Rights Act, Article 15e.

(131) This requirement is complemented by other criteria in some SMS, e.g. Sweden requires that the service is 'complicit' and the UK requires that the service has 'actual knowledge' of the infringement.

(132) See below fn 134.

(133) See Copyright Act, Article 26d; Related Rights Act, Article 15e.

(134) In particular, according to German courts, there must be no alternative option or no way to reach the infringer itself directly, who must not have responded to the request to cease the infringing conduct. In summary, German courts require the order to be an 'ultima ratio' as a requirement for issuing a blocking injunction. See for example Landgericht München I of 7 June 2019, MMR 2019, 555 ff, (as part of a series of so-called Goldesel decisions).

(135) Ibid.

(136) Some requirements, however, might have been endorsed by some SMS, and not by others. For example, while in Sweden blocking injunctions should be 'effective' and in the Netherlands 'subsidiarity' and 'prevailing interest' should be considered, in Spain the 'subsidiarity' (i.e. the need to start proceedings against the infringer itself previously or at the same time when starting an action against the ISPs), and 'effectiveness' have been expressly ruled out as requirements. Instead, in Spain, injunctions must be 'objective' and 'non-discriminatory'. 
4.1.5 Necessity of the decision on the merits

A decision on the merits (i.e. on the IPR infringement), whether a full review for issuing a permanent injunction or a partial review for issuing interim measures, would be necessary in all SMS for granting a blocking injunction (e.g. in Belgium, Denmark, France, Germany, Ireland, Italy, Lithuania (137), Spain, Sweden, the Netherlands and the UK). Customarily, a full decision on the merits would not be necessary and blocking injunctions can be issued upon a partial review of the merits in interim proceedings, which should be followed by a final permanent decision on the merits. For example, in Italy, blocking injunctions can be issued in the course of urgency proceedings, based on a preliminary assessment of the merits (‘fumus boni iuris’), while the merits of the case can be fully analysed and decided in a subsequent judgment. In any event, if the judgment on the merits is not started, injunctions issued in the course of an urgency proceedings and not revoked will stay in force.

4.1.6 Contributory liability

In general, and in accordance with the principle that these measures apply to so-called innocent third parties, intermediary contributory liability is not requested for imposing blocking injunctions on access providers and other intermediaries (138). Among the SMS, only Germany (139) and Sweden require an intermediary’s contributory liability. In Sweden the access provider’s subscribers must be able to access the unauthorised works via the internet connection that was provided by that access provider for the access provider to have *medverkat* (collaborated/contributed) to copyright infringement. The Patents and Market Court also found that this requirement must be interpreted in the light of Article 8(3) of the InfoSoc Directive.

4.1.7 Ex parte and inter partes proceedings

In Belgium, Denmark, Finland, Germany, the Netherlands, Sweden and the UK, proceedings to obtain a blocking order can theoretically be *ex parte* and *inter partes*. However, reservations are commonly made with regard to *ex parte* proceedings, for example: (i) in Denmark, *ex parte* proceedings were said to be the exception, only applied if it is presumed that the purpose of the injunction will be defied if the counterparty is notified; (ii) in Finland, courts can order *ex parte* interim injunctions, however, the longer-term final blocking injunctions require the intermediary to be heard; (iii) in Germany, *ex parte* proceedings are limited by a requirement of ‘urgency’ (140); (iv) in the Netherlands, the law would

---

(137) In case of injunctions issued by the Radio and Television Commission.

(138) See in general, Husovec, supra fn 9.

(139) In Germany, this results from the application of the *Störerhaftung* doctrine (see infra fn 161), rather than contributory liability, which is a notion unknown to the German legal system and does not match exactly the liability arising as a result of the *Störerhaftung* doctrine.

(140) In fact, this is a general requirement whenever an interim injunction is applied for. Strictly speaking, laches are applied for lack of legal interest if the applicant waits too long before seeking judicial redress. This requirement closely resembles the *periculum in mora* applied by Italian and Spanish courts in interim proceedings. In any event, ‘urgency’ is not consistently applied, nor does a legal definition exist, and German courts’ views differ substantially. According to the case-law of the Court of Appeal (Oberlandesgericht – OLG) of Munich, which has not been confirmed yet by other Courts of Appeals in Germany, urgency means that the applying rights holder must not have delayed action for more than 1 to 2 months (urgency
require IPR infringement by the intermediary for issuing blocking injunctions ex parte\(^{(141)}\); (v) in Sweden, proceedings for an interim injunction can be ex parte, however, to date, no ex parte proceedings have resulted in a dynamic blocking order; (vi) in Belgium, such a possibility is limited to situations of extreme urgency or absolute necessity (the latter concept being narrowly construed by the courts); (vii) finally, in the UK, ex parte blocking injunctions are possible ‘in principle’, however, the applicants have typically adopted the following process in practice: (a) the operator of the target website is notified of the infringement but is not joined to the proceedings; (b) the intermediary being formally served with the application does not oppose orders for blocking injunctions; (c) applications are then dealt without a hearing unless there is a novel point on which the court requires or would benefit from oral submissions. The proceedings are only inter partes in Greece, Ireland and Spain even if the defendants do not actively participate in the legal proceedings, e.g. they remain neutral or do not oppose the application. In Lithuania, the proceedings in court are inter partes whereas before the administrative authority they are ex parte.

4.1.8 Preliminary and/or final injunctions

In most SMS, blocking injunctions can be requested as both preliminary and final injunctions (Belgium, Denmark, Finland, Germany\(^{(142)}\), Greece, Italy, Lithuania, the Netherlands, Spain and Sweden). In the three remaining SMS, France, Ireland and the UK, site blocking can be requested only as final injunctions. In France, the decision is issued under an accelerated procedure on the merits of the case.

4.1.9 Duration of blocking injunctions

In some SMS, the temporal validity of blocking injunctions is not explicitly limited, such as in Belgium, Denmark (in principle), Germany, Italy and Spain. In some SMS, however, unlimited duration is applied with caveats. In Ireland, the duration must be ‘reasonable’. In Lithuania\(^{(143)}\) and the Netherlands, the injunction is valid for the duration of the infringement. In Sweden, there are no statutory requirements, but courts have set time limits. Some SMS, instead, might limit the duration of blocking injunctions or have a mixed regime: (i) in Finland, copyright blocking orders are available for a maximum of 1 year at a time (but copyright discontinuation orders and trade mark injunctions would be unlimited in time); (ii) in France, courts make injunctions available for a period of 18 months; (iii) in Greece, unlimited duration only applies to blocking injunctions from civil courts, blocking of IP addresses via the administrative procedure can be up to 6 months, while blocking of domain names, including subdomains, must last at least 3 years.

\(^{(141)}\) See Code of Civil Procedure, Article 1019e.

\(^{(142)}\) As mentioned above, however, preliminary injunctions are issued under a very restrictive ‘urgency’ requirement.

\(^{(143)}\) A preliminary injunction would be valid during the enforcement procedure.
In some SMS, blocking injunctions can be reviewed (i.e. amended), at a later stage. For example, in Lithuania, the Radio and Television Commission must be informed about the removal of the copyright infringement and the decision will be reviewed at that time. In the Netherlands, a measure can be reviewed, at any time, if it appears to be no longer compatible with a fair balance between fundamental rights because of changed circumstances. In Ireland, the court will usually give liberty to the parties to apply to court (on notice) in the event of any change in circumstances. In those SMS without a limit to the duration of blocking injunctions, there are no mechanisms for a review (i.e. amendment) at a later stage (e.g. Finland, Ireland, Italy, Spain and Sweden).

4.1.10 Blocking injunctions in civil and criminal cases

In multiple SMS, blocking injunctions can be ordered only in civil cases, e.g. in France, Greece, Ireland and the Netherlands (144). In the remaining SMS, blocking injunctions can be potentially ordered both in civil and criminal cases. However, in some of these SMS, the injunctions have been actually granted in civil cases only, such as in the UK. In Finland, blocking orders are considered non-contentious civil cases, however, the principle of adhesion allows combining civil claims as a part of criminal procedures, if the claims concern the same event. In Spain, it is highly likely that the civil proceedings will be suspended until the conclusion of the criminal proceedings.

4.2 Dynamic blocking injunctions

4.2.1 Availability

Dynamic blocking injunctions are available – and have been granted – in most SMS, including Denmark (145), France (146), Ireland (147), Italy (148), the Netherlands (149), Spain (150), Sweden (151), and the UK (152).

---

(144) See Copyright Act, Article 26d; Related Rights Act, Article 15e.
(145) See for example Maritime and Commercial Court (Sø- & Handelsretten), Case Number A-51-17, 21 February 2018, Fritz Hansen A/S and Others (represented by Rettighedsalliancen SMF.) v Telia Danmark A/S and Dominidesign Furniture LTD.; and District Court of Frederiksberg - Copenhagen - 05/12/2017 - RettighedsAlliancen etc. v TDC A/S.
(146) See for example TGI Paris 17/13471, supra fn 95; and TGI Paris, 19/01744 of 23 May 2019.
(147) See for example EMI v Eircom [2009] IEHC 411; EMI v UPC [2013] IEHC 274; Sony Music Entertainment (Ireland) & Ors v UPC; Communications Ireland Limited [2016] IECA 231; and Twentieth Century Fox Film Corporation & Ors v Eircom Limited & Ors [2018] IEHC 54.
(148) See for example Court of Milan 14 January 2020; Court of Milan, 24 December 2019; and Court of Milan, 12 April 2018.
(150) See for example Commercial Court of Barcelona 15/2018, supra fn 93.
(152) See for example Twentieth Century Fox Film Corp v British Telecommunications plc [2011] EWHC 2714; and Football Association Premier League Ltd v British Telecommunications plc [2017] EWHC 480 (Ch).
4.2.2 Statutory notion

The notion of dynamic blocking injunction is usually not defined by the law of the SMS. In fact, dynamic injunctions have been defined by law only in Lithuania\(^{(153)}\). Therefore, although there is no explicit statutory notion of dynamic blocking injunctions in most SMS, courts have interpreted the current laws to include them. General IP provisions providing remedies for infringement\(^{(154)}\) and the national implementation of Article 11 of the IPRED, which also provides that the judge can order intermediaries to take measures to prevent new infringements\(^{(155)}\), have served as a legal basis for dynamic blocking injunctions. This also implies, thus, that there are no specific requirements for the grant of a dynamic blocking injunction over the requirements in place for a standard blocking order.

4.2.3 Case-law

On the basis of this expansive interpretation of the norms, courts have been granting dynamic blocking injunctions in most SMS and setting up all necessary requirements. However, so far, the number of dynamic blocking injunctions issued in each of the SMS has been rather limited\(^{(156)}\), with the exception of the UK. In Newzbin2, Lord Justice Arnold clarifies the rationale for the wide acceptance of dynamic blocking injunctions by UK courts:

> I do not consider that the Studios should be obliged to return to court for an order in respect of every single IP address or URL that the operators of Newzbin2 may use. In my view the wording proposed by the Studios strikes the appropriate balance. If there is a dispute between the parties as to whether the predominant purpose of an IP address or URL is to enable or facilitate access to Newzbin2, they will be able to apply to the court for a resolution of the dispute. In saying this, I do not mean that BT will be obliged to check IP addresses or URLs notified by the Studios. It will be the Studios' responsibility accurately to identify IP addresses and URLs to be notified to BT\(^{(157)}\).

In fact, in the UK any grant of a blocking injunction is considered dynamic as they include provisions that require the ISP to actively block any additional IP addresses, URLs and/or domain names that

\(^{(153)}\) See Order of the Minister of Culture of the Republic of Lithuania on Approval of the Description of the Procedure for Imposition of Mandatory Instructions on Internet Access Service Providers of 20 November 2019, No. V-771 (TAR, 2019-11-26, Nr. 2019-18793), Article 5 (providing ‘[t]he Commission’s decisions on imposing the mandatory instructions on internet access service providers shall provide for dynamic blocking – they shall instruct to block current and future internet domain names identifying the websites, which are used for unlawfully communicating copyright content to the public, i.e. the instruction shall cover current and future copies of the websites’).

\(^{(154)}\) See for example in Denmark, AJA, §413; in France, Intellectual Property Code (CPI), Article 336-2; in Ireland, Copyright and Related Rights Act 2000, Section 40(5A); in Sweden, Trademark Act (2010:1877), Section 8 Article 3; Article 35 b of the Design Protection Act (1970:485) and Article 57 b of the Patent Act (1967:837) (providing that ‘[b]y request of the (rightsholders), his or her legal proprietor or a person who holds a license to use the (IPR), the court may, under penalty of a fine, prohibit anyone who commits or contributes to an action of infringement or violation to proceed with the action’).

\(^{(155)}\) See L’Oréal-eBay, supra fn 42.

\(^{(156)}\) As per the information collected, e.g. only two cases in the Netherlands, only cases against Google in France, only three cases in Sweden (e.g. PMT 7262-18); no dynamic blocking injunctions have so far been issued in Greece.

\(^{(157)}\) See Newzbin2, supra fn 97, para. 12.
host the content or may be notified by the rights holders during the duration of the order\(^{(158)}\). This notification procedure operates without either party having to make any further application to the court. This allows the rights holders to respond to efforts made by the website operators to circumvent the orders by changing the location of the target website. UK website blocking orders also require rights holders to notify the ISPs of IP addresses, URLs and/or domain names that should no longer be blocked, for example, where an IP address/URL which has been notified for blocking ceases to be a location whose sole or predominant purpose is to enable or facilitate access to a target website.

As mentioned, although in a more limited fashion, dynamic blocking injunctions have been issued by courts in most SMS. In Denmark, courts will usually grant dynamic blocking injunction with the following wording: ‘The injunction also applies to other domains that provide access to the same Internet services and which the [plaintiff] makes the defendant explicitly aware of, in which connection the [plaintiff] undertakes to legally and financially vouch for that such other domains provide access to the Internet services to which this Decision relates’. In Ireland, dynamic blocking injunctions have been granted in a number of cases for copyright infringement\(^{(159)}\). In the Netherlands, dynamic blocking injunctions have been issued against access providers for the blocking of The Pirate Bay by providing the following definition: ‘in the event that The Pirate Pay becomes accessible through other / additional IP addresses, to block access by their customers to such other/additional IP addresses and/or (sub)domain names, and keep them blocked, after notification of the correct IP addresses and/or (sub)domain names by Brein to each of the Providers individually’\(^{(160)}\).

Judicial application of established civil law theories might also achieve the same results as dynamic/forward-looking injunctions proper. In Germany, for example, the so-called Kerntheorie might lead to the same result as dynamic blocking injunctions\(^{(161)}\). According to Kerntheorie, infringements similar in their core (Kern) trigger a duty to review and notice-and-stay-down. In the so-called Internet Auction cases I–III, the German Federal Court of Justice repeatedly decided that notified trade mark infringements oblige internet auction platforms, such as eBay, to investigate future offerings, manually or through software filters, in order to avoid trade mark infringement\(^{(162)}\). This jurisprudence comes down to conclusions resembling closely those of the CJEU in L’Oréal. Therefore, it might theoretically also support the availability of forward-looking injunctions in the form of website-blocking orders against access providers. In fact, German courts have been so far applying Kerntheorie only to

\(^{(158)}\) See for example Twentieth Century Fox Film Corp v British Telecommunications plc [2011] EWHC 2714.

\(^{(159)}\) See for example EMI v Eircom [2009] IEHC 411; and Sony Music Entertainment (Ireland) & Ors v UPC Communications Ireland Limited [2016] IECA 231.

\(^{(160)}\) Ziggo et al., supra fn 149, §3.8.6.

\(^{(161)}\) This theory would apply under the more general umbrella of the Störerhaftung doctrine. In Germany, intermediary liability in copyright is almost invariably handled through the doctrine of Störerhaftung – as an alternative to joint tortfeasance for which intermediaries hardly qualify. This doctrine, based on BGB, §1004, grants a permanent injunctive relief to the proprietor against anybody who has caused an interference. Störer means interferer with the property, who will be liable unless it is unreasonable to burden the interferer with a duty to examine whether their behaviour could interfere with the (intellectual) property of a third person. See for example BGH, Mar. 11, 2004, I ZR 304/01, https://www.beckmannundnorda.de/bghrolex.html; Broder Kleinschmidt, An International Comparison of ISP’s Liabilities for Unlawful Third Party Content, 18 Int’l J. of L. & Info. Tech. 332, 346–347 (2010).

\(^{(162)}\) See for example BGH 11 March 2004, Rolex v Ebay/Ricardo (aka Internetversteigerung I), I ZR 304/01, GRUR 2004, 860 (DE), para. 31 (noting ‘[w]henever the defendant’s attention has been drawn to a clear infringement of rights not only is it obliged to block access to the specific offer […] it must also ensure that such trade mark infringements will as far as possible not occur in the future. […] The defendant is obliged to react to these cases by subjecting offers of Rolex watches to a special examination’); BGH, 19 April 2007, Rolex v eBay (a.k.a. Internetversteigerung II), I ZR 35/04, GRUR 2007, 708 (DE); BGH, 30 April 2008, Rolex v Ricardo (a.k.a. Internetversteigerung III), Case I ZR 73/05, GRUR 2008, 702 (DE).
ordering the take-down of infringing content against hosting providers. However, a recent decision from the Munich Higher Regional Court might suggest an expansion of the scope of proactive forward-looking injunctions. The Munich court has apparently imposed dynamic blocking injunction on access providers to block the website kinox.to, by applying the duty of care provided for under the Störerhaftung doctrine (163). The decision may be possibly interpreted as granting a dynamic blocking injunction as far as it does not seem to be limited to the particular domain kinox.to but to the business of kinox as a whole, irrespective of the domain name (164). It is worth noting, however, that the BGH Internet Access Auction cases set precise boundaries to the proactive filtering obligations that can be imposed on intermediaries, in line with the general principle that injunctions under Article 18(1) e-commerce Directive should not limit freedom to conduct a business by imposing an ‘excessive obligation’ on the host provider (165). The German Supreme Court has always stressed that proactive monitoring obligations cannot go as far as endangering a platforms’ business models if it is a legal business model (166). For example, internet auction platforms, such as eBay, could not be asked to manually check all entries because that would be economically unfeasible (167).

In any event, however, the admissibility of dynamic blocking injunctions has been debated. In Belgium, case-law seems to be divided on the subject of dynamic blocking injunctions against intermediaries (168). From a broad civil procedure perspective, courts seem convinced that it is necessary to appear before the judge for each new infringement and refuse to grant a broad measure that would also apply to future infringements (169). Therefore, in a recent decision, the blocking order only concerned domain names and subdomain names explicitly included in a list drawn up by the claimant, to the exclusion of all other domain names (170). However, in criminal matters, the dynamic blocking injunction seems to be more accepted without actually being named. In 2013, the Cour de Cassation (Court of Cassation) upheld a criminal injunction which implied that all internet access providers in Belgium must disable access to the content hosted on the servers linked to the domain name thepiratebay.org, by the technical process of reverse IP domain check (171) as well as any


(164) ibid.

(165) Glawischning-Plesczek, supra fn 41, para. 44.

(166) See supra fn 162.


(171) The search for any domain name that refers to a given IP address.
domain name that refers to this server notified to the access providers by the Federal Crime Computer Unit or the Regional Crime Computer Unit (172). Again, in Italy, it has been argued that they are against the long-standing principle of Italian civil procedure that the scope of interim injunctions must be clearly defined and limited. Finally, Italian courts have widely accepted dynamic blocking injunctions as admissible because otherwise rights holders would be forced to bring a new case against every access provider for each website hosting contents in breach of their IPR (173).

4.2.4 Unavailability and fundamental rights balancing

Instead, dynamic blocking injunctions are not available in Finland, and their availability has not yet been tested in court in Germany (174) and Greece. In Finland, new IP addresses or domain names cannot be added to the scope of an existing blocking order without filing a new application to the Market Court, as clearly stated in the preparatory documents of the Copyright Act (175). The preparatory works of the Copyright Act underline, on the one hand, the technical limitations of what blocking injunctions can do against widespread unauthorised dissemination of works on the internet, and on the other hand, the risks and detriments that a broader dynamic approach to blocking injunctions would impose on the other fundamental rights and freedoms. Copyright protection should, thus, (i) consider a balanced safeguarding of all competing rights at stake; (ii) not lead to unreasonable restrictions on the rights of both copyright holders and users of works; (iii) not affect communications to the public more than strictly necessary for protecting copyright; and (iv) any limitations should be based on observable objective criteria (176). As a consequence, blocking orders can be used only in case of severe copyright infringements and their impact on the interests of other stakeholders, including intermediaries and third parties, must be taken into account. Therefore, blocking orders were limited in their length and their scope was set to specifically pre-determined identifiers, so that the continuation of the measures must be subject to regular court proceedings to assess whether the grounds for the injunction still exist (177).

4.3 Live blocking injunctions

4.3.1 Availability

As a subspecies of dynamic blocking orders, some SMS have made available live blocking orders with the principal goal of limiting infringement of rights for live (sports) events. Live blocking orders are

---


(173) See Court of Milan, 12 April 2018; Court of Milan, 24 December 2019; Court of Milan, 14 January 2020.

(174) But see above the discussion of the German Kerntheorie, under which the effect of a dynamic blocking injunction might be achieved with normal injunctions.

(175) See Finnish Market Court (Markkinoikeus), MAO:311/18, 7.6.2018 and Government’s Proposal 181/2015 vp, pp. 25 and 37 (stating that an injunction can be changed and new IP address added in the scope with a new application. See also Government’s Proposal vp 201/2018 vp. on trade marks.


available in Ireland (178), Spain and the UK. Provisions in this regard have also been recently enacted in Greece but have not yet been tested in practice. The UK, a pioneer in this field, has a system of live blocking orders that allows the repeated blocking of a site every time a live broadcast is in process (179). These live blocking orders are dynamic insofar as the orders provide for the list of target servers to be reset on a regular basis during the lifetime of the order. This allows for new servers to be identified by the rights holder and notified to the defendants for blocking, and ensures that old servers are not blocked after a certain time, unless they continue to be observed as sources of infringing footage. In the live blocking decision in \textit{FAPL v BT}, the High Court noted that the dynamic order sought in that case differed from those previously granted as ‘although it is standard practice for orders under section 97A of the CDPA to enable the IP address or URL of the target website to be updated as and when necessary, the Order provides for the list of Target Servers to be “re-set” each match week during the Premier League season. This allows for new servers to be identified by FAPL and notified to the defendants for blocking each week, and ensures that old servers are not blocked after the end of a week unless they continue to be observed as sources of infringing footage’ (180).

Live blocking injunctions are available in Spain under five judicially formulated conditions: (i) blocking access to the websites using all web resources (URLs, domains, IP addresses) and via the HTTP and HTTPS protocols within 72 hours after notification of the decision; (ii) informing the plaintiff of the effective execution of the blocking order, identifying all the web resources blocked (URLs, domains, IP addresses) and the HTTP and HTTPS protocols, along with the day, hour and minute at which each web resource was blocked; (iii) the blocking measures are limited in time, namely three years (2019-2022), without prejudice to the suspension of the blocking order if it is established that the blocked website resource is disabled on the Internet, as it does not provide illegal content; (iv) the decision orders the blocking of ‘pirate websites’ (i.e. related with the blocked ones), that the plaintiff identifies in a new list that will be sent directly and simultaneously to all the ISPs, on a weekly basis; and (v) those new sites must be blocked within a maximum of 3 hours of being notified (181).

In the \textit{Ecatel} case, the Dutch Court ordered that the live blocking measures be implemented within a very short timeframe. The case was brought by the English Premier League against Ecatel, a provider of dedicated servers located in Amsterdam (182). The live blocking measure had to be implemented within 30 minutes upon receiving the notice from the rights holder (or a designated third party) of the newly identified live streaming sources (183) (as opposed to the more standard 24 hours for complying). Of course, short timeframes are of essence for providing protection to the broadcasting rights of events that customarily last a very limited time, usually below 2 hours. For the sake of comparison it is worth mentioning that EU Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online proposes the competent authorities to act against online

\footnotesize{(178) The court is able to grant a live blocking injunction, under Section 40(5A) of the Copyright and Related Rights Act 200, as in the cases of \textit{The Football Association Premier League Ltd v Eircom & Ors} [2019] IEHC 615 (‘FAPL 2019’) and \textit{FAPL} 2020, supra fn 108.

(179) See for example \textit{Football Association Premier League Ltd v British Telecommunications plc} [2017] EWHC 480 (Ch); \textit{Union Des Associations Européennes De Football v British Telecommunications plc} [2017] EWHC 3414 (Ch); \textit{FAPL} 2018, supra fn 124; \textit{Matchroom Boxing Limited v British Telecommunications plc} [2018] EWHC 2443 (Ch).

(180) \textit{FAPL} 2018, supra fn 124, para. 25.

(181) See Commercial Court of Madrid 2174/2019, supra fn 93 (ordering the blocking of a total of 31 websites and 44 URLs for three sporting seasons, i.e. until 25 May 2022).


(183) Ibid. para. 5.1.
terrorist content within 1 hour. Such short deadlines are likely to force intermediaries to develop new technical solutions and will have an impact on the costs of implementation.

4.3.2 Unavailability

In other SMS, live blocking is not available yet or, at least, their availability has not yet been tested in court (184). However, there is an ongoing debate on whether live blocking injunctions should be provided for by legislation or granted by courts. In France, for example, a discussion regarding live blocking, in particular of sporting events, has emerged in connection to the Draft Law on audiovisual communication and cultural sovereignty in the digital age (185). The proposal would enable owners of broadcasting rights over sporting events to (i) obtain, under a single procedure, a dynamic decision extending the effectiveness of the measures to block or delist the illicit sites or services identified on the day of the decision to other sites or services likely to appear during the competition; (ii) enjoy measures that last a maximum of 12 months, and may be implemented in accordance with a provisional timetable modelled on the official competition calendar; (iii) undertake these actions, including as a preventive measure, so that the decision can be taken in a timely manner as regards the temporality of each sporting event or competition, in order, in particular, to effectively protect competitions lasting a few days or weeks; and (iv) rely on a regulator acting as a trusted third party to facilitate the identification of ‘pirate sites’ or services, particularly mirror services.

5. Scope of Dynamic Blocking Injunctions

5.1 Subject matter

As with blocking injunctions, there does not seem to be in the SMS any specific limitation to the subject matter that can be covered by a dynamic blocking injunction, which might include any IPR infringement. However, copyright infringement is by far the major target of dynamic injunctions in the SMS. Additionally, dynamic and live blocking injunctions have emerged as the most efficient tools to address online streaming infringements of live sporting events, a sensitive market for rights holders. A further development concerns the blocking of access to websites offering devices and software that allow for the circumvention of technological protection measures (TPMs).

5.1.1 Broadcasting live sporting events

National case-law has been increasingly concerned with blocking injunctions for combating illegal broadcasting of live sporting events, including online transmission (internet protocol TV or IPTV). These orders, such as in the case of FAPL v BT, are live blocking orders (see supra para. 4.3) that only have effect at the broadcast time of the live match/event footage. This is especially relevant when

(184) There is, apparently, no reason to believe that such measures could not be granted in most SMS, at least those where dynamic blocking orders have been already granted, such as Belgium, Denmark, France, Italy, the Netherlands and Sweden.

(185) Projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l’ère numérique (MICE1927829L).
considering sports matches (football, boxing, etc.). These live blocking orders allow new servers to be blocked every week to prevent the continued infringement of IPRs but only come into force when the broadcast is taking place (186).

5.1.2 TPMs

A further development in the scope of blocking orders is the blocking of access to websites offering devices and software that allow for the circumvention of TPMs (187). The novel legal question is whether rights holders are entitled to seek injunctions against intermediaries, not only when the target websites directly engage in copyright infringement, but also when they provide devices aimed at circumventing TPMs and, thus, allow copyright infringement to occur. This question should be answered considering that the protection offered by Article 6 of the InfoSoc Directive not only encompasses the manufacture and distribution of devices, but also includes the advertising thereof and the provision of services (i.e. modding services). To date, in Europe there have been some instances – including in Italy, Spain and the UK – in which an application based, inter alia, on the protection against TPM circumvention has been granted.

The High Court of England and Wales issued a website-blocking order against five of the main UK retail ISPs to block access to four websites advertising, distributing, offering for sale and/or selling devices that allowed TPMs on Nintendo Switch games consoles to be circumvented. Eventually, the order sought by the applicant company was granted. From the Nintendo case, it seems plausible to infer that Article 8(3) of the InfoSoc Directive (as transposed) could be the legal basis for copyright holders to request an injunction against an intermediary whose services – ones that made available devices that allowed for circumventing TPMs – were used to infringe copyright. Actually, in the Nintendo case, the Court found that the TPMs installed by the applicant were aimed at protecting against acts which required its authorisation, while the operators of the target websites used the ISPs’ services ‘to infringe copyright’ by making available the circumventing devices. It was the use of these devices that resulted in the unauthorised reproduction and other unlawful uses of copyrighted content, such as videogames, including their artwork, text and soundtracks.

A different matter altogether would be whether blocking orders are available against websites making available devices aimed at circumventing TPMs that protect against acts for which no authorisation is needed, as the use is, for example, covered by exceptions or limitations, or the content protected by the TPMs is in the public domain. According to the Advocate General Szpunar in VG Bild Kunst opinion, Article 6 of the InfoSoc Directive relates to the protection of the rights holders against acts which require their authorisation (188). Therefore, if this is not the aim of the circumventing devices, blocking injunctions should not be available.

(186) See supra para. 4.3. See also Illegal IPTV in the European Union, EUIPO, November 2019, p. 7, paras 1.2.1, 1.4.1, 1.6.5, 4.2.3, 5.1.3, 5.2.1; Etude de l’impact économique de la consommation illicite en ligne de contenus audiovisuels et de retransmissions d’événements sportifs, HADOPI, 2 December 2020 (claiming that piracy has led to an economic loss of 1.03 billion Euros in the audiovisual and sport sector in 2019); Deloitte, European Citizens and Intellectual Property: Perception, Awareness, and Behaviours, EUIPO, 23 March 2017, 68-70 (discussing European perception of piracy, including sporting events).

(187) See InfoSoc Directive, Article 6-7 (providing to rights holders a right against the circumvention of effective TPMs that protect access to and use of protected works and against the manufacture and commercialisation of devices primarily designed to circumvent TPMs and with limited commercial use than to circumvent).

5.2 Targeted intermediaries

Although, generally speaking, dynamic blocking injunctions can be granted against any party deemed an intermediary under Article 8(3) InfoSoc Directive and Article 11 IPRED, they have only been granted against access service providers in most SMS. In any event, there is no reason that an injunction cannot be granted against other intermediaries that can block access to websites hosting infringing content, such as DNS registries and/or registrars.

5.3 Targeted websites, content and internet resources

Dynamic blocking injunctions can be applied to (i) the same content infringed multiple times, as in the case of Denmark, Italy and the Netherlands; (ii) the same infringer, as in Ireland; or (iii) to both, the same infringer and the same infringed content, as in Greece and Sweden. In these scenarios, the injunction orders the blocking of access to certain content, whenever and wherever it is made available online, or to all content made available by a certain uploader. As mentioned earlier (189), according to Glawischneg-Piesczek, content that is identical or equivalent, and thus to a great extent similar, to content previously subject to a takedown injunction could be kept unavailable without the need of obtaining a new court order. An argument could be made that the conclusions of the CJEU’s decision might be extended by analogy to dynamic blocking injunctions as well; however, Glawischneg-Piesczek applies to defamatory content rather than IPR-infringing content and to content removal, rather than website blocking, which is as such a more invasive enforcement practice.

Here is some more detailed information from some of the SMS regarding the websites that could be dynamically blocked.

- In France, the only new domains that can be delisted are those that constitute new access paths to the targeted sites that access providers and other intermediaries can automatically detect.
- In Lithuania, the law prescribes specific instructions for identifying copies of websites that should be dynamically blocked. These copies should include websites that give access to the same activity as the primary website. A copy must have at least two of the following signs: (1) its internet domain name is identical or almost identical to the primary website (several letters, figures, other characters are added or removed, the domain ending changes and so on); (2) its content is identical or almost identical to the primary website (it communicates to the public identical copyrighted content (or a part of it) as indicated in the request, identical works are communicated to the public at a similar time and so on); (3) its visual expression is identical or almost identical to the primary website (the same graphic presentation, identical trade mark and/or service mark and so on); (4) its user interface is identical or almost identical to the primary website (identical menu categories/options and so on); (5) its manager or administrator is the same as of the primary website or the available data enables one to arrive at the reasonable conclusion that it is the same (190).
- In the Netherlands, it is the rights holders’ responsibility to supply correct IP addresses and/or (sub)domain names infringing the same content that must be blocked by the intermediaries.

(189) See supra fn 41.
(190) See the Order of the Minister of Culture of the Republic of Lithuania on Approval of the Description of the Procedure for Imposition of Mandatory Instructions on Internet Access Service Providers, Article 6.
• In Spain, dynamic blocking injunctions apply to any method to infringe the same content by domains, subdomains and IP addresses whose main purpose is to circumvent blocking methods.

• In the UK, (1) access providers that are subject to a website-blocking order must block or attempt to block access to the target websites, their domains and subdomains and any other IP address or URL notified to them by the applicants or their agents whose sole or predominant purpose is to enable or facilitate access to a target website. (2) In case of live blocking orders, the scope of the order would include the notification to the access provider of an IP address to be blocked if the IP address is being used during the live event to communicate to the public without authorisation live audiovisual footage of that event, or live footage immediately preceding the event.\(^{(191)}\)

5.4 Number of websites subject to blocking

In all SMS providing for dynamic blocking injunctions, other than Greece, there are no limitations on the number of websites that can be blocked. Each application before the Greek administrative authority may include up to 50 domain names and IP addresses; however, Greek courts have no limitations on the number of websites.

5.5 Exceptions

In the UK, special safeguards are provided in an attempt to keep these orders balanced and to avoid abuse. Upon notification to the applicant, exceptions to temporarily suspend the obligations in the order are available to: (i) correct or investigate over-blocking of material which is, or is reasonably suspected to be, caused by the steps taken; (ii) ensure the reliable operation of its Internet Watch Foundation blocking system, if it reasonably considers that this operation is otherwise likely to be impaired; (iii) maintain the integrity of its internet service or the functioning of its blocking system; (iv) upgrade, troubleshoot or maintain its blocking system; or (v) avert or respond to an imminent security threat to its networks or systems.\(^{(192)}\) In addition to the respondents, other parties are permitted to apply for an exception to the order, including (a) the operator of any target server having an IP address notified under the order; (b) the operator of any website or video-streaming service who claims to be adversely affected by this order; and other third parties directly or indirectly affected by the order.

5.6 Confidentiality

The issue of the confidentiality of blocking injunctions has been discussed in the UK. UK courts concluded that parts of a blocking order could be kept confidential if otherwise disclosure would undermine the purpose of the order, since to do so would help those seeking to circumvent the blocking system. However, other applicants for related website-blocking orders will still be able to have access to the order in its entirety to be able to take advantage of the order’s information.\(^{(193)}\)

\(^{(191)}\) Matchroom Boxing Ltd and another v British Telecommunications plc and others [2020] EWHC 2868 (Ch), Annex A, para. 2.

\(^{(192)}\) ibid, Annex A, para. 15.

\(^{(193)}\) See for example ibid., paras 25-26. See also FAPL v BT [2017] EWHC 480 Ch and [2018] EWHC 1828 (Ch).
practice of access to information by third parties with a legitimate interest is also highlighted by the Football Association Premier League cases, where FAPL had shared details with Matchroom and other third parties. In fact, the dynamic web blocking arrangements were developed by a team working for FAPL at considerable cost and were now made available with other organisations and private parties on agreed terms.

5.7 Temporal scope

Blocking injunctions might have a limited duration or not, depending on the SMS. As, customarily, the law does not regulate dynamic blocking injunctions nor their duration, they might be limited in time by judicial decisions according to specific time periods (e.g. a number of months or years) or to the duration of the infringement. For example.

- In France, once a dynamic blocking injunction has been granted, the defendant has 15 days to implement the measures, and once implemented the injunction will last 18 months.
- In Greece, the EDPPPI sets the duration of the order in cases of IP addresses to a maximum 6 months, while in cases of domain names, including subdomain names, the duration cannot be less than 3 years.
- In Ireland, to date, live blocking injunctions granted by courts have been limited to a calendar year; however, for other blocking injunctions, the duration must be reasonable.
- In the UK, access providers must implement dynamic blocking orders within 10 working days of the notification of the original order and any subsequent updates from the rights holders. No time limitations apply to orders granted under Section 97A CDPA. However, courts have been applying a ‘sunset clause’ to live blocking orders that means the injunction expires after a certain date. The live blocking order granted in the Matchroom case expired after 2 years unless extended by a further order of the court (194), while those granted to the Football Premier League and UEFA are in force on a ‘per season’ basis (195).

In other SMS, however, dynamic blocking injunctions are apparently granted without a time limit. In Lithuania, a dynamic injunction is valid as long as there is a copyright infringement on the specific website. In the Netherlands, a blocking order can remain in place as long as it is compatible with a fair balance between the fundamental rights. In Spain, there are no time limits on blocking injunctions; it is entirely up to the judge to decide on a case-by-case basis, although judges tend to put a time limit on dynamic blocking of sporting events. In Sweden, there is no limitation as to how long a dynamic blocking injunction can be enforced; however, in the case PMT 7262-18 the judge did enforce a time limit (196). Finally, neither Denmark or Italy apply time limits when granting dynamic blocking injunctions.

---

(194) See for example Matchroom Boxing Ltd and another v British Telecommunications plc and others [2020] EWHC 2868 (Ch), Annex A, paras 9-10 (the case involved an application made by Matchroom (a company that runs boxing events) regarding a website-blocking injunction).

(195) See supra fn 179.

5.8 Territorial scope

In the SMS, blocking injunctions commonly apply to access providers under the jurisdiction of the MS and infringing acts having effects in the territory of the MS. Therefore, in general, injunctions can order the blocking of content regardless of the location where the infringement took place or the location of the users accessing the infringing content, as long as the activities target the consumers and internet users of the MS. Arrangements in the SMS reflect quite consistently these general principles.

- In Denmark, courts are only able to issue blocking orders against internet access providers if they have jurisdiction, while companies can be ordered to block content regardless of the location in which the infringement took place or the location of the users that are accessing the information.
- In the Netherlands, dynamic injunctions can only be granted against access providers under Dutch jurisdiction, whether located in the Dutch territory or anywhere else.
- In France, dynamic blocking injunctions can only be granted in response to a request by an internet user on French territory; the place of establishment of the sites to be delisted is not taken into consideration.
- In Ireland, the blocking injunctions granted to date are limited to Ireland and legal proceedings can be instituted in Ireland against foreign defendants or relate to foreign websites where the infringing activities occur in Ireland (namely, the activities target Irish consumers/internet users).
- In Italy, only access providers located in Italian territory are subjected directly to blocking injunctions, although content can be blocked from content providers located overseas by enforcing a blocking order against Italian ‘mere conduit’ providers.
- In Spain, dynamic blocking injunctions are limited to the Spanish territory, meaning that injunctions granted in Spain cannot extend to providers or customers outside of Spain. However, websites that are available in Spain, even if based outside of the country, are subject to blocking injunctions.
- In Sweden, the principle of territoriality regarding IPRs can act as a limitation to the geographical scope of the injunction.
- In the UK, the necessity to show infringing acts in the UK/under UK law operates as a geographical limitation. Blocking injunctions are able to target services that are operated outside of the UK, and often do. In principle, they could also operate against an intermediary established outside the UK, however, this is currently theoretical as such no orders have been granted against non-UK based access providers. So far, orders have therefore been limited to restricting access to websites by UK subscribers of those access providers’ services.

Cross-border enforcement of dynamic blocking injunctions granted by courts in other countries (EU and non-EU) is a complex matter. Dynamic blocking injunctions granted in other EU MS might be enforceable under EU Regulation No. 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (e.g. Italy, Spain, Sweden). Dynamic blocking injunctions granted by countries outside of the EU are usually not enforceable in the SMS, unless legal provisions on international legal cooperation in civil matters by execratur procedure are available (e.g. Spain).
6. Evidence

6.1 Specific procedural rules

There is no specific procedural rule governing the admissibility of evidence for blocking injunctions and, in general, there is no difference regarding the evidence required by courts and other bodies issuing injunctions, although in some SMS only courts can issue these injunctions (197).

6.2 Type of evidence

For the court to grant a blocking injunction, the evidence required and its admissibility is the same as in other civil cases, and the applicant is required to provide documental evidence, factual witness evidence and/or expert evidence.

6.3 Evidence to show infringement

In all SMS, the standard evidence to be provided must show that an IPR infringement has occurred. This includes, in particular, evidence that (1) the applicant holds the IPRs; (2) the applicant’s rights have been infringed; and (3) the defendant’s services are being used by third parties to infringe on these rights. In urgency proceedings, these requirements are scrutinised with less rigour than in a full judgment on the merits. Italy requires that rights holders prove prima facie evidence of: (a) their title (‘fumus boni iuris’) and its breach; and (b) of the ongoing breach and of the consequent impossibility to wait for a full judgment on the merits (‘periculum in mora’). In Denmark, the plaintiff does not necessarily need to prove the IPR infringement. It will suffice to ‘make it probable’ that the infringement is taking place. In Finland, for blocking orders, the rights holders are required to provide evidence about significant amounts of copyright-infringing material being made available to the public or that their rights are otherwise obviously and severely prejudiced. Additionally, they must present the measures they have taken in order to identify the alleged infringer.

6.4 Additional evidence

For the more targeted evidence required to obtain a blocking injunction, at least in Ireland and the UK, it must also show that the injunction is proportionate, and it will not affect any fundamental rights. With regard to the evidence of infringement, and of the fact that the defendant’s services are used by third parties to infringe the applicant’s rights, specific examples of statistical and technical evidence include:

- In Finland, accepted evidence in court proceedings has included written documents, such as in the form of testimonies and statements, probatory samplings, online metrics, technical reports and expert testimony hearings (198).

(197) See supra para. 2.5.
(198) See Market Court MAO:243/16 and MAO:311/18 (FIN).
• In France, in order to establish evidence on the sampling methods in order to prove the massive nature of the infringing acts on the websites to be blocked, the judges will consider (i) the number of monthly visits to the content; (ii) the type of works present on the site (film present in cinemas, online, etc.); (iii) the number of accessible works; (iv) the percentage of protected works; and (v) the methods of access to these sites.
• In Germany, during preliminary injunction proceedings courts require screenshots and other documentation, testimony and affidavits.
• In Greece, injunctions have been granted on the basis of evidence concerning the similarity of the database (structure and content), of the graphics, of the user interface and of indexing.
• In Spain, in order for a blocking injunction to be granted the claimant must show (i) evidence of infringement; and (ii) graphic evidence of illegal content. In some cases the claimant shows a statistical report on the amount of illegal content on the website, however, this is not a strict requirement.

6.5 Evidence for dynamic blocking

As per dynamic blocking injunctions, most SMS have no special requirements regarding the admissibility of evidence for dynamic blocking injunctions. In Italy, however, although not officially required, it seems plausible to conclude that the rights holder should prove the dissemination of illegal content on websites changing domain names and/or IP address over the course of time. In Spain, if the dynamic injunction is granted by an administrative body, additional evidence is required, namely: an Excel document listing about 50-100 works present on the website (title; URL; ownership); proof of ownership of each work; a navigation certificate showing that works are on the site (how the site works, how the download is carried out); a report on the website traffic; the relevance of the website; information showing the audience in Spain and the position of the site in the ranking of Spanish websites; and, a report on the financing of the website, advertising, revenue, etc.

6.6 Notification of (repeated) infringements

In several SMS, beneficiaries of the injunction do not have to notify the intermediaries of infringements or repeated infringements (e.g. in France, Finland, Greece, Lithuania, Ireland, Sweden and the UK). However, notification might be requested in a minority of the SMSs (e.g. in Denmark, Italy, the Netherlands and Spain). (1) Where notification is not required, infringements might be identified in the following ways: (i) in France, courts consider that intermediaries, either access providers or search engines, must prevent future infringements and must be able to identify on their own new ‘access paths’ leading to the sites identified in the decision; (ii) in Greece, rights holders may submit evidence proving that there is a violation of the decision or a threat of reiteration of the infringement, including evidence concerning the similarity of the database (structure and content), of the graphics, of the user interface and of indexing; (iii) in Ireland, the mechanisms for identifying repeated infringements are generally agreed in advance between the parties and then approved by the court; (iv) in Lithuania, the Radio and Television Commission of Lithuania monitors infringements itself and the beneficiaries of the injunction can notify the Commission about repeated infringements; (v) in Sweden, the rights holders may notify the intermediary of repeated infringements but they are under no obligation to do so. (2) Where notification is required, evidence of repeated infringements can be shown by rights holders by providing access providers with: (i) in Denmark, the same kind of proof provided for...
obtaining the initial blocking injunction (199); (ii) in Italy, evidence that new aliases refer to websites hosting content falling within the scope of the injunction; (iii) in the Netherlands, statistical and technical evidence, as well as screenshots, to support the infringement claims; (iv) in Spain, a list of the new websites circumventing the blocking of the original websites mentioned in the injunction, by showing, for example, evidence of the redirection through HTTP response status codes showing the status of a domain when a user tries to connect to it or via graphic evidence of the redirection.

7. Implementation of Blocking Injunctions

7.1 Technical solutions available

There are several available mechanisms to block illegal content, including IP address blocking, DNS blocking, URL filtering, deep packet inspection, domain name-related measures, and ingress and egress filtering (200).

In most SMS, the injunction usually specifies the technical solution to be applied, such as in Finland (201), Germany (202), Greece, Ireland, Lithuania, the Netherlands (203), and the UK. In the UK, blocking orders typically state that the ISPs must use certain – or equivalent – technical solutions/systems to implement the blocking measures; however, in Ireland and the UK, the choice of technical means is commonly agreed between rights holders and ISPs, then vetted by the court. However, injunctions usually do not specify the technical solution in Denmark, France, Italy, Spain and Sweden, leaving the choice to the intermediary concerned. Nevertheless, the following wording is often, if not always, used by Danish injunctions: 'The defendant is instructed to implement a technical solution, such as a DNS blocker, which is capable of preventing defendant's clients from accessing the Internet services to which the domains listed in claim 1 currently provide access'. In Spain, blocking orders usually suggest DNS blocking, but leave the decision as to the specific technical solution to be decided by the ISPs.

Both IP address and DNS blocking are the most common technical solution applied by blocking injunctions in most of the SMS, including Finland, Greece, the Netherlands and the UK. In several SMS, DNS blocking alone was the most common and/or the only technical solution used, such as in Denmark, France, Lithuania (where so far only DNS blocking can be ordered), and Spain. In France, dynamic blocking injunctions have been granted against Google to delist from Google’s search results not only the infringing sites listed in the injunction but also the ‘access paths’ (new domain names) that the search provider is technically capable of identifying (204).

(199) If the injunction mentions specific websites, and the infringing activities are then moved to another website, the rights holder must inform the intermediary of the new locations to have these new websites blocked as well.


(201) The technical means of blocking are specified in court decisions, but they are based on the requests of the parties, with priority being given to the views of the intermediary.

(202) The specification of a technical solution is mandatory according to the BGH. See BGH, Dead Island, I ZR 64/17, 26 July 2018 (mandating DNS blocking).

(203) See Ziggo et al., supra fn 149 (where the technical solutions to block The Pirate Bay have been specified).

7.2 Implementation costs

The allocation of enforcement costs – that is, whether the rights holders or the online intermediaries should sustain the costs of blocking – becomes a key factor in reviewing the proper balance between the freedom to conduct business and blocking orders. The allocation of the costs of implementing blocking measures has been treated inconsistently across the EU. Considerable fragmentation in approaches to intermediary liability – and in particular in sensitive matters such as the allocation of enforcement costs – is especially critical. Fragmentation in this context brings about legal uncertainty and higher transaction costs that reflect on the sustainability of the business models of online intermediaries in Europe.

EU law and CJEU jurisprudence say little in this regard and leave the decision to the national courts on the basis of their national law. The CJEU in *UPC Telekabel* only reminds that ‘[an injunction] constrains its addressee in a manner which restricts the free use of the resources at his disposal because it obliges him to take measures which may represent a significant cost for him’ (205).

Intermediaries are bearing the costs of implementing a blocking injunction in several SMS, including Belgium (206), Denmark, Finland (207), France, Germany (208), Greece, Italy, Lithuania, the Netherlands, Spain and Sweden. This is justified under the assumption that intermediaries (i) should contribute to the fight against online infringement; (ii) internalise value thanks to the infringement occurring on their networks; and (iii) are best positioned to end online infringements. The French Cour de cassation in the *Allostreaming* case (209), a copyright infringement case, established that the blocking costs were entirely the responsibility of the ISPs as long as those measures are proportionate. The Court noted that EU provisions:

> do not prevent the costs of the measures strictly necessary for safeguarding the rights in question … from being borne by the technical intermediaries, even when such measures may present significant costs for the intermediaries. The aforementioned Directives 2000/31 and 2001/29 … foresee that notwithstanding the principle of non-responsibility of the intermediaries, the ISPs and hosting providers are required to contribute to the fight

(205) *UPC Telekabel*, supra fn 11, para. 57.

(206) Although in Belgium the question of cost allocation still remains open (there is no decision expressly ruling on the issue), a judgment from the Antwerp court seems to conclude that the costs might be borne by the intermediary as long as the ‘measures are within a range of the intermediary’ and as long as the intermediaries ‘should be able to act as intermediaries at an acceptable cost’. See Court of Appeal of Antwerp, 26 September 2011, A&M, 2012, p. 220.

(207) In Finland, the applicant might have an obligation to recompense the intermediary if the legal action is cancelled or dismissed or the interim order expires before the applicant institutes permanent injunction proceedings. See Section 60 f (1) and (2) of the Copyright Act; Section 64(6) of the Trademark Act; Section 57 b (5) of the Patents Act; Section 35a(5) of the Registered Designs Act.

(208) In Germany, the intermediaries are deemed to be secondary infringers, thus they are defendants in the proceedings, rather than innocent third parties, and, as losing party, they have to bear the costs.

against the illegal content and, in particular, against the infringement of copyright and related rights, when they are best positioned to put an end to such violations (210).

In Italy, costs are internalised by the intermediaries under the assumption that costs should be borne by the entities making technically possible the breach of relevant IPRs. Again, according to the Amsterdam Court of Appeal in Ziggo et al., the blocking order asked for does not demand unbearable sacrifices from the access provider, cannot be deemed as unreasonable, and can be regarded as a relatively minor encroachment of the freedom of entrepreneurship of Ziggo et al (211). In Spain, the HDFull decision has established that:

[companies engaged in information services intermediation derive an economic benefit from access to websites, more specifically through advertisements shown in such pages. Therefore, it is legitimate and consistent with the proportionality principle that they financially contribute to blocking or delisting measures by electing the implementation of measures that are most appropriate as stated in paragraph 52 of the UPC Telekabel Wien GmbH judgment (212).

In contrast to the practice in most MS, the UK Supreme Court in Cartier (213), a trade mark infringement case, allocated the costs of blocking and delisting to rights holders, noting that ‘the ordinary principle is that unless there are good reasons for a different order an innocent intermediary is entitled to be indemnified by the rights holder against the costs of complying with a website-blocking order’. Prior to this decision, however, UK courts have justified the allocation of costs to intermediaries in the following terms: (i) exposure of intermediaries to an injunction under Article 8(3) of the InfoSoc Directive is a quid pro quo for immunity under the safe harbours set out in the e-commerce Directive; (ii) as the ISP makes a profit from the provision of access to the infringing target services, the costs of implementing the order can be regarded as a cost of carrying on that business; (iii) the cost of implementing the order is a factor that can be taken into account when assessing the proportionality of the injunction but that cost to the ISPs ‘would be modest and proportionate’ (214).

It is worth noting that the UK Court of Appeal, reviewing the Cartier case, had instead decided that the costs of enforcement had to be equally divided between the two parties (215). Recently, in France, the Tribunal judiciaire de Paris (formerly known as the Tribunal de Grande Instance de Paris before 17 July 2019) has specified that the plaintiffs had to warn the ISPs in case of closure or disappearance of the sites listed in the court decision in order to avoid excessive blocking costs. In addition, an access provider can ask for a release of the measures ordered which led to an over-blocking (this after having approached the plaintiffs in vain) (216). Other courts in Europe, such as the Irish Court of Appeal in the

---

(211) Ziggo et al., supra fn 149.
(212) See Commercial Court of Barcelona 15/2018, supra fn 93.
(214) Newzbin2, supra fn 97, para. 200.
(215) See for example Cartier Int’l AG and others v British Telecommunications plc and another [2017] Bus L.R. 1 [100]–[128] (CA) (UK).
(216) TJ Paris, 16 janvier 2020, RG 19/14013.
Sony Music case (217), although deciding on costs for setting up a graduate response scheme rather than website blocking, came down to a different ratio in allocating costs, imposing 80% of the costs to the online intermediaries and 20% to the rights holders.

8. Follow-up to Dynamic Blocking Injunctions

8.1 Renewal and update

In some SMS, specific procedures are available for renewing, updating or extending static and dynamic blocking injunctions, while they are not available in others. Renewal would apply to an injunction whose duration has expired, while updating or extension would apply to measures still in place, usually within the framework of an interim action. In this context, there does not seem to be any specific distinctions between procedural rules for renewal and update of static and dynamic injunctions among the SMS. Specific arrangements for renewal and update, then, might apply depending on the jurisdiction and a few principles can be extracted.

(i) In most SMS (e.g. Denmark, Finland, France, Italy, Ireland, the Netherlands, Spain and Sweden), renewal or update of an injunction is usually only possible within the framework of a new procedure on the merits. This is done by filing a new complaint and no specific procedure exists. In order to extend a previous blocking injunction, the rights holders must prove that the requirements for issuing the injunction are still in existence, e.g. that the IP address or the domain name has not been repurposed and that the copyright infringement still continues.

(ii) Time limits might be applied to blocking injunctions depending on the jurisdictions and the type of injunctions. In Ireland, for example, currently live blocking orders must be renewed every year, whereas dynamic blocking injunctions are for an indefinite duration.

(iii) If injunctions without time limit are issued (e.g. Italy and Spain), however, review is possible only if the decision which contains the order is subject to an appeal. If the decision becomes final, there is no possibility to modify its content. The conditions for an appeal vary depending on the type of decision. In Italy, for example, injunctions set forth in an interim injunction can be revoked: (i) if an appeal against the injunction (in Italian legal jargon, reclamo) is filed (within a deadline of 15 days from the notification of the injunction) and upheld by the court (218); (ii) if a full judgment on the merit is launched and it ends with the acknowledgement of the inexistence of the rights for which the injunction was granted (219).

(iv) In France, blocking injunctions can be renewed when expired or updated, ‘unless the parties have reached a better agreement’. However, this conclusion is not consistently accepted. In 2013 the Tribunal de Grande Instance de Paris refused to grant an extension, stating ‘as the applicable legislation stands, the present court has no means of enabling a review of the execution of its decision, either directly or through the intermediary of a public official who would

(217) See Sony Music Entertainment Ireland Ltd v UPC Communications Ireland Ltd [2016] IECA 231 (Ire.) (‘[b]ecause the defendant is the company which profits – albeit indirectly – because it derives revenue from its subscribers who are engaged in this practice, it is the defendant who should, in my view, be primarily liable for the costs’).

(218) See Italian code of civil procedure, Article 669 terdecies.

(219) ibid, Articles 669 octies.
be responsible for it’ (220). The judge thus recalled that, in principle, any new request for blocking must be the subject of new summons, but left open the alternative hypothesis of a ‘better agreement between the parties’ (221).

Specific procedures for renewing injunctions without starting new proceedings are possible in some of the SMS. In Denmark, although there is no review mechanism in place regarding dynamic blocking injunctions, there is the possibility for the injunction to be cancelled if ‘the conditions for the court’s notice of prohibition or injunction are no longer fulfilled’ (222). In Ireland, for both website and live blocking injunctions, the courts will usually allow the parties to apply to the court in the event of any change in circumstances. In the Netherlands, given that an injunction can remain in place for as long as the balance between the fundamental rights remains, an intermediary can start court proceedings to lift the injunctions if the balance of fundamental rights is no longer present. In Greece, renewal of blocking measures is specifically provided for by law as part of the administrative enforcement procedures before the EDPPI:

If, after the issuance of the decision by the … EDPPI and its enforcement, there is an infringement or a reiteration of the infringement of the content referred to in said decision is threatened by any technical way, the applicant may submit an application to the Committee asking for the issuance of a new decision without having to pay a new fee for the case examination of paragraph 3, by submitting the evidence proving that there is violation of the decision or threat of reiteration of the infringement in accordance with the above (223).

In the UK, although there is no specific review for blocking orders, the parties to proceedings and any affected third parties can apply to the court in certain prescribed circumstances. In particular, dynamic blocking injunctions have been extended beyond the initial two-year term by application to the court with supporting evidence that, for example, the target websites were still in operation.

In keeping with dynamic blocking orders, in Italy, usually, rights holders will inform ISPs on new aliases related to the content included in the scope of the blocking injunctions. In the UK, under a voluntary scheme, update notifications are typically sent on a monthly basis, although interim notifications will be sent in certain circumstances (e.g. if an IP address that has been notified for IP address blocking becomes shared with a non-target website).

8.2 Converting static into dynamic injunctions

The above conclusions also apply to the possibility of amending an already existing order so as to convert it into a forward-looking/dynamic injunction. However, static blocking orders cannot be converted into dynamic blocking orders in most SMS. No specific procedure is available to do this, and a new procedure on the merits has to be started, with the exceptions and all the caveats mentioned above (e.g. Greece, Ireland, Spain and the UK).

(220) TGI Paris, 28 novembre 2013, no. 11/60013.
(221) Ibid.
(222) AJA §426,2,1.
8.3 Recurring penalties

The enforcement of the order, with fines and recurring penalties, might be available. Recurring penalty payments are available in most SMS under the umbrella of the IPRED, that states ‘where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance’ (224). In Belgium (225), France, and Italy, rights holders may ask the court to provide for a penalty (so-called astreinte) to be paid by ISPs for each day of inobservance of static and dynamic blocking injunctions (226). In Greece, the EDPPI will impose a fine of EUR 500 (five hundred euros) up to EUR 1 000 (a thousand euros) for each day of non-compliance with the blocking injunction. In Finland, the Market Court can order the intermediary to act on threat of a fine if there is a suspicion that the intermediary would not otherwise enforce the order (227). The same applies to Sweden, where access providers must pay a recurring penalty if they do not comply with the order. In the Netherlands, the Court of Appeal of Amsterdam has imposed fines on access providers Ziggo and XS4ALL for each time they violate The Pirate Bay blocking orders. The fines were EUR 10 000 (ten thousand euros), plus a penalty of EUR 10 000 (ten thousand euros) for every day or part of a day that said violation continued, to a maximum of EUR 500 000 (five hundred thousand euros) (228).

8.4 Enforcement and fines

In Denmark, recurring penalty payments are not available, but if the defendant does not comply with the blocking order the plaintiff can request the bailiff to enforce the order (229). Non-compliance with an injunction is also subject to the payment of a fine or, in grave cases, imprisonment for up to 4 months (230). The plaintiff must prove non-compliance and must initiate a separate court action in order to apply the abovementioned sanctions (231). In Ireland, failure to comply with an injunction can result in attachment and committal proceedings being issued. In Italy, non-compliance with a blocking injunction is usually assessed by a technical expert who certifies the continued presence online of content falling within the scope of the injunction. A rights holder may enforce an obligation of payment for the corresponding amount (e.g. by starting a seizure of assets of the non-compliant party). In Sweden, non-compliance is assessed by the court upon request from the rights holders.

(224) IPRED, Article 11.
(225) See Judicial Code, Article 1385ter (the astreinte is an ancillary pecuniary penalty, which is enforced in the event that the main penalty is not enforced within the prescribed time).
(226) Cf. Section 614 bis, Italian code of civil procedure.
(227) See Government’s Proposal 181/2015 vp, p. 54.
(228) See Ziggo et al., supra fn 149.
(229) Cf. AJA § 424.
(230) Cf. AJA § 430, 1.
(231) ibid., in fine.
8.5 Remedies against the injunction

There are remedies available to challenge blocking injunctions in all the SMS under traditional civil procedure rules (232). (i) The remedies are generally available to the intermediaries and the alleged infringers concerned by the injunction. (ii) In addition, in several SMS, individual internet users who have been affected also have a right to a remedy (e.g. in Finland, Germany, Greece, Ireland (233), the Netherlands (234) and the UK (235)). According to the German BGH, in applying the CJEU’s UPC Telekabel judgment, individual internet users have the right to a legal remedy by starting an action against their access provider on the basis of their contractual relationship. In Sweden, the interests of internet users are also protected by the Swedish Post and Telecom Authority, which must communicate injunctions and orders in fulfilment of EU obligations (236). (iii) Finally, class actions by internet users against blocking injunctions are available in the Netherlands. In other SMS, they seem to be either unavailable (e.g. in Ireland) and/or, a priori, not intended to apply to injunctions against intermediaries (e.g. in Belgium and Finland) (237).

9. International Private Law, Comity, and Legal Entanglements

9.1 Extraterritorial enforcement

International private law issues have been increasingly relevant in the debate regarding injunctions against online intermediaries (238). In particular, open questions pertain regarding the possible extraterritorial scope of static and dynamic blocking injunctions. Two major cases have been decided by the CJEU, against Google and Facebook, dealing respectively with the enforcement of privacy and

(232) In Lithuania, such remedies were reported to be available only in cases where the injunction is ordered by a court.

(233) Irish Courts have granted permission to operators of any server having an IP address notified under the injunction, any operator of a website or video streaming service, any hosting provider and any customer of the ISP, to apply on notice to vary or discharge the order insofar as it affects them. See FAPL 2019, supra fn 178, 615 and FAPL 2020, supra fn 108, 332.

(234) See Ziggo et al., supra fn 149, §3.5.5 (It notes that in the event of changed circumstances, the court can be approached also by third parties who have an interest in this matter, to assess whether compliance with the order under the new circumstances can still be demanded and/or whether the order must be amended).

(235) See Cartier 2014, supra fn 123.

(236) See Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services. However, as internet users are not part of the court case, they have no right of action, although their rights are considered by the court when assessing the proportionality of the injunction.

(237) See for collective redress actions in Belgium, Title 2, Book XVII, CEL; in Finland, Act on class action 444/2007, which applies only in the context of civil cases between a consumer and a business.

(238) See Giancarlo Frosio, Enforcement of European Rights on a Global Scale, in Elenonora Rosati ed., Routledge Handbook of European Copyright Law, Routledge, London, UK, forthcoming 2021, available at https://ssrn.com/abstract_id=3650521 (including also a review of international cases imposing global effects of national injunctions and noting how global injunctions have increasingly become a characteristic trend of recent online enforcement, which leads to insurmountable jurisdictional conflicts that can break the internet).
personality rights. In fact, the CJEU has not yet undertaken any specific review of global IPR enforcement, nor global enforcement of blocking injunctions or DBI, as the cases mentioned refer, respectively, to global delisting of the right to be forgotten entries in Google Search (239) and the removal of defamatory content from Facebook (240). However, the conclusions so far endorsed by the CJEU seem consistent enough to provide clear guidance for the potential global reach of enforcement of rights under the EU legal framework.

In CNIL, the CJEU concluded that, presently, EU law does not make it compulsory for search engines to dereference on all versions of the search engine (241). However, an important observation of the court was that, although EU law presents no provision that requires global dereferencing, ‘it also does not prohibit such a practice’ (242). This means that a national supervisory or judicial authority may still order the operator of a search engine to carry out a global dereferencing after assessing the right to privacy and the right to freedom of information. In a later case brought against Facebook, the CJEU apparently confirmed and further clarified these conclusions. In Glawischnig-Piesczek, the CJEU was asked whether the injunction against Facebook to remove content defaming an Austrian politician can apply worldwide. Confirming the availability of an injunction with a worldwide effect, the CJEU noted that Article 18(1) of the e-commerce Directive does not provide any limitation on the scope of measures that the MS can adopt. They have been given broad discretion to implement necessary measures (243), which includes extending the territorial scope of the injunction worldwide. While doing so, in consideration of Recitals 58 and 60 of the e-commerce Directive, the measures should be consistent with relevant international law (244).

The CJEU concluded that EU law does not impose or preclude worldwide measures. Instead, it is up to national courts to decide whether extraterritorial delisting should be imposed according to their own balancing of fundamental rights and application of international norms. This is apparently an obvious conclusion from an EU law standpoint. Final case-by-case balancing of rights is a prerogative of national courts, rather than the CJEU. Although the CJEU does not clarify the scope of international law to which injunctions issued by MS may be subject, it is most likely referring to comity. If the CJEU was indeed referring to comity, MS would not pass global injunction orders without balancing competing sovereign interests. As a long-established approach, in case of conflict between local territorial law and the law applicable to particular activities on the internet, MS apply the ‘comity doctrine’ or ‘sovereign-deference doctrine’ and apply significant restraint in protecting individuals within their sphere of control. Comity has been described as ‘a sort of intercourt diplomacy’ (245). According to a widely used definition,

(240) Glawischnig-Piesczek, supra fn 41.
(241) CNIL, supra fn 239, para. 64.
(242) ibid, para. 72 (emphasis added).
(243) See Glawischnig-Piesczek, supra fn 41, para. 29.
[c]omity in the legal sense, is neither a matter of absolute obligation on the one hand nor of mere courtesy and good will upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, and to the rights of its own citizens or of other persons who are under the protection of its laws (246).

In a recent case, the AG Saugmandsgaard Øe has referred to Glawischnig-Piesczek in discussing the conditions to be met to apply for an injunction against an intermediary for copyright infringement under Article 8(3) of the InfoSoc Directive (247). The AG confirms that EU law, however, requires the injunctions to be proportionate (248). In this context, proportionality would imply that the resources of the provider must be taken into account, especially in light of the complexity of detecting equivalent files that use the work in the same way (249). Moreover, AG Saugmandsgaard continues, an obligation to block cannot ‘prevent users of a platform from uploading legal content and, in particular, legally using the work concerned’ (250). This might imply that, upon national courts’ determination, worldwide blocking orders affecting users’ rights in that fashion cannot be reasonably expected by a provider. Therefore, whenever, the worldwide blocking or takedown prevents users uploading or using content that is legal in their jurisdiction, that obligation would be unreasonable. Similarly, worldwide blocking and the taking down of equivalent content seems equally unreasonable according to the AG’s reasoning, given the enormous transaction costs involved with identifying whether an infringement is equivalent in each jurisdiction worldwide. In contrast, taking down or blocking access worldwide to identical mechanical reproductions of a protected work – which is a blatant infringement according to international copyright norms – might be reasonably expected of a provider, if national courts order so and having considered international norms and comity principles.

The recently proposed Digital Service Act (DSA) seems to pick up on this very point by noting, among the conditions that must be met by ‘orders to act against illegal content’, that the territorial scope of the order, on the basis of the applicable rules of Union and national law, including the Charter, and, where relevant, general principles of international law, does not exceed what is strictly necessary to achieve its objective’ (251). So, blocking injunctions, once again, should be targeted and specific with a territorial scope as broad and as limited as, what is necessary to achieve its objective. On one side, the territorial – and extraterritorial scope – will be determined by EU and national law, but also by the proportional balancing of fundamental rights that emerges from the EU Charter. On the other side, the territorial scope should be, however, limited by international law principles, including comity, according to what the CJEU established in CNIL and Glawischnig-Piesczek.

9.2 Legal entanglements

Finally, it is worth noting that blocking and dynamic blocking case-law shows multiple instances of ‘legal entanglement’ among national courts of different MS. Legal entanglements can be considered

(247) 16/07/2020, C-682/18 and C-683/18, Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C-682/18) and Elsevier Inc. v Cyando AG (C-683/18), EU:C:2020:586, Opinion of AG Saugmandsgaard Øe.
(248) ibid. para. 222.
(249) ibid.
(250) ibid.
(251) DSA, supra fn 31.
a form of informal cross-border cooperation (252), and occur when national courts refer to judgments in other jurisdictions. There are examples for Belgium and the Netherlands, as well as in the UK and Ireland. For example, in the recent High Court of Ireland UEFA judgment, dealing with a dynamic blocking order against ISPs with the aim of combating the illegal IPTV streaming of live sporting events (football games) (253), the Irish judge refers several times to the judgments of the High Court of England and Wales in similar (if not identical) cases, stating: ‘I completely agree. Those observations apply equally to the facts of this case’ (254) and ‘I agree and accept that those reasons are relevant for the purposes of the present application’ (255). Interesting is also the statement in paragraph 18: ‘My attention has been drawn to the judgment of Arnold J. in the High Court of England and Wales’ (256). This might be an indication that parties seeking dynamic blocking injunctions may make good use of references to similar cases in other jurisdictions. It seems likely that similar judgments in other jurisdictions will be considered by the respective judges as long as they are brought to their attention.

10. Effectiveness of Dynamic Blocking Injunctions

Benefits and challenges associated with blocking injunctions have been studied in literature at length (257) and are mentioned in this study in terms of compliance with fundamental rights, fair balance and proportionality of injunctions, with a special emphasis on the risk of over and under-blocking. However, an additional important factor to evaluate the availability, scope and proportionality of blocking injunction is their effectiveness in reducing infringement. The effectiveness of blocking injunctions is usually not explicitly assessed in most SMS (e.g. Italy and Spain). However, it has been considered by some SMS’ courts. In particular, UK courts have on multiple occasions reviewed whether the injunctions were effective and found that the evidence indicates that blocking orders are reasonably effective and cause a material reduction in the number of UK users who access infringing websites (258). In Ireland, effectiveness does not require 100 % success as long as the remedy has a significant persuasive effect (259). In the Netherlands, the court mentioned (260) the ‘Alexa list’, which contains information about websites and lists them from most to least visited. When blocking injunctions were issued against The Pirate Bay in the past, it went down on the list, whereas, when these injunctions were lifted, it went back up again. Therefore, the court confirmed that the blocking of the website is actually an effective measure.

Finland has no formal mechanisms to assess the effectiveness of static and dynamic blocking injunctions. However, after the Market Court issues the order, the affected parties themselves are

(252) See EUIPO, Study on cooperation in online legal measures, forthcoming.
(253) High Court of Ireland (Commercial), 2020 No. 6450 P of 29 September 2020, UEFA v EIRCOM et al.
(254) ibid., para. 19, 33, 34 and 40.
(255) ibid., para. 34.
(256) ibid., para. 18 (emphasis added). See also paras 10, 33 and 40.
(257) See supra fn 9.
(258) See for example EMI v Sky, para. 105; Football Association Premier League Ltd, supra fn 179, para. 49.
(259) See FAPL 2020, supra fn 108.
responsible for monitoring the effectiveness of the injunction as well as their necessity (261). The Market Court can, then, assess the necessity of the injunctions if the parties either seek to renew, extend or challenge the order by filing an application to the court.

In some jurisdictions courts also base the availability of blocking injunctions on empirical data showing at least that internet users are seriously discouraged from accessing the infringing content and that there is a reduction in the numbers of users accessing this content. In addition, static and dynamic blocking injunctions should be regularly reviewed on the basis of their effectiveness and necessity. In summary, in certain jurisdictions effectiveness is an additional requirement to justify targeted and specific blocking injunctions that fairly balance fundamental rights and impose proportionate, but not excessive obligations, on access providers and other intermediaries.

11. Conclusions and Key Findings

The overview of static and dynamic blocking injunctions in the EU and the SMS shows a complex web made up of a variety of approaches in EU MS that is sometimes hard to disentangle. In this regard, this study provides a set of key findings that might serve as a reference for the further development of policies and practices in the field.

(1) Blocking injunctions find their legal basis in Article 18(1) of the e-commerce Directive, Article 8(3) of the InfoSoc Directive and Article 11 of the IPRED. The compatibility of blocking injunctions with EU law has been confirmed by a number of CJEU judgments, which would also support the availability of dynamic blocking injunctions. However, while static blocking injunctions are available in all the SMS, dynamic blocking injunctions are not or, at least, their availability has not yet been tested in the courts in some of the SMS.

(2) The availability of static and dynamic blocking injunctions largely depends on the proper balancing of rights and interests. Firstly, in order to guarantee proportional balancing of fundamental rights, dynamic blocking injunctions must be consistent with the constitutional legal framework set forth by the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights or ECHR), as construed by the European Court of Human Rights (ECtHR) and, in particular, by the Charter of Fundamental Rights of the European Union (EU Charter), as interpreted by the CJEU. In all SMS, fundamental rights must be considered by courts when balancing rights and interests in issuing dynamic blocking injunctions. In this regard, ordinary courts, administrative courts and authorities in the SMS have mostly been explicitly referring to fundamental rights balancing, with a special emphasis on freedom of expression and information, freedom to conduct a business, the right to property and the protection of personal data. Secondly, in most SMS, courts must assess the proportionality of the measure according to Article 3 IPRED and general principles of EU law. This is usually done on a case-by-case basis according to several national standards. In this context, dynamic injunctions should address the risk of over- and under-blocking. These risks are addressed by courts in most although not all SMS. In light of the above, static and dynamic

(261) See Government’s Proposal 181/2015 vp, p. 56 as cited by Market Court, MAO:243/16, para. 57 and MAO:311/18, para. 49 (noting that the applicant is in the best position to monitor the effectiveness of the injunctions).
blocking injunctions should be made available, according to the doctrine of ‘fair balance’ among fundamental rights, only if they are strictly targeted to bring the infringement to an end and if they do not disproportionately impinge on fundamental rights, do not impose ‘excessive obligations’ on intermediaries and address the risk of over- and under-blocking.

(3) **Requirements** for obtaining a blocking injunction differ in the SMS. There are, however, some common general requirements and procedural rules that apply in most SMS, including, (i) the need to demonstrate rights holder status and ownership of rights, evidence of alleged infringement, proportionality, appropriateness and/or reasonableness of the requested measure; (ii) a decision on the merits, whether a full review for issuing a permanent injunction or a partial review for issuing interim measures, would be necessary in all SMS; (iii) proceedings to obtain a blocking order can be *ex parte* and *inter partes* in some SMS, although reservations are commonly made with regard to *ex parte* proceedings; (iv) in general, intermediary contributory liability is not requested for imposing blocking injunctions on access providers and other intermediaries; and (v) in some SMS, the temporal validity of blocking injunctions is not explicitly limited, while in others an unlimited duration is applied with caveats.

(4) **Dynamic blocking injunctions** have been granted in most of the SMS, including Denmark, France, Ireland, Italy, the Netherlands, Spain, Sweden and the UK. However, so far, the number of dynamic blocking injunctions issued in the SMS has been limited. In most SMS, there is no explicit statutory notion of dynamic blocking injunctions: Therefore, courts have been granting dynamic blocking injunctions – and defining their requirements – on the basis of an expansive interpretation of pre-existing norms. General IPR rules providing remedies for infringement and the national implementation of Article 11 of the IPRED, which has been interpreted by the CJEU so that the judge can order intermediaries to take measures to prevent new infringements, have served as a legal basis for dynamic injunctions. This also implies, thus, that there are no specific requirements for the grant of a dynamic blocking injunction over the requirements in place for static blocking injunctions. As a subspecies of dynamic blocking injunctions, some SMS (Ireland, Spain and the UK) have made available live blocking injunctions with the principal goal of limiting infringement of rights to live (sporting) events. In other SMS, live blocking injunctions are not available or, at least, their availability has not yet been tested in court. As a recent development, in the UK and Spain, injunctions have been made available to block access to websites offering devices and software that allow for the circumvention of technological protection measures (TPMs).

(5) With regard to the **scope of dynamic blocking injunctions**, subject matter, targeted intermediaries, targeted websites, temporal and territorial scope vary to different extents in the SMS. In particular, (i) although copyright infringement is the major target of these measures in the SMS, there does not seem to be any specific limitation to the subject matter that can be covered by a dynamic injunction; (ii) generally, dynamic blocking injunctions can be granted against any party deemed an intermediary under Article 8(3) of the InfoSoc Directive and Article 11 of the IPRED, although they have been customarily granted against access service providers in most SMS; (iii) most SMS have no limitations on the number of websites that can be blocked; (iv) blocking injunctions might have a limited duration or not, depending on the MS, however, even though the law does not regulate dynamic blocking injunctions nor their duration,
they might be limited in time by judicial decisions; and (v) in the SMS, blocking injunctions commonly apply to access providers under the jurisdiction of the MS and to infringing acts having effects in the territory of the MS. Therefore, in general, injunctions can order the blocking of content regardless of the location where the infringement took place or the location of the users accessing the infringing content, as long as the activities target MS’ consumers and internet users.

(6) In general, there are no specific procedural rules on the requirements for and the admissibility of evidence for blocking injunctions in the SMS. The same is true with regard to dynamic blocking injunctions specifically. For courts to grant a blocking injunction, the evidence required and admissible is the same as in other civil cases, and the applicant is required to provide documental evidence, factual witness evidence and/or expert evidence. In several SMS, beneficiaries of the injunction do not have to notify the intermediaries of infringements or repeated infringements; however, notification might be requested in a minority of the SMS.

(7) Implementation of blocking injunctions mainly focuses on the technical solutions and implementation costs. There are several available mechanisms to address blocking of illegal content. In most SMS, the injunction usually specifies the technical solution to be applied. If that is not the case, such as in Denmark, France, Italy, Spain and Sweden, courts might, however, suggest technical solutions to meet the scope of the injunction. Both IP address and DNS blocking are the most common technical solutions applied by blocking injunctions in the SMS. The allocation of the costs of implementing blocking measures has been treated quite inconsistently across the SMS. EU law and CJEU jurisprudence say little in this regard and leave the decision to the national courts on the basis of their national law. The intermediaries bear the costs of implementing a blocking injunction in the large majority of the SMS. In fewer SMS, costs might be shared between the intermediary and rights holders, or assigned to intermediaries only, such as in the UK.

(8) Follow-up actions to dynamic blocking injunctions play an important role in the measures’ effectiveness and overall balance of interests concerned. (i) In some SMS, specific procedures are available for renewing, updating or extending static and dynamic blocking injunctions, while they are not available in others. In this context, there does not seem to be any specific distinctions between procedural rules for renewal and update of static and dynamic injunctions among the SMS. (ii) There is no specific procedure available to convert static into dynamic blocking injunctions in the SMS. Instead, a new procedure on the merits has to be started. (iii) In addition, the enforcement of the order, with fines and recurring penalties, might be available in most SMS. (iv) Finally, there are remedies available to challenge blocking injunctions in all the SMS under traditional civil procedure rules. The remedies are generally available to the intermediaries and the alleged infringers concerned by the injunction. In a few SMS, these remedies are also available to affected individual internet users, while in some SMS collective actions are available.

(9) Discussing the extraterritorial scope of injunctions against online intermediaries, recent CJEU jurisprudence concluded that EU law does not impose or preclude worldwide measures. Instead, it is up to national courts to decide whether extraterritorial injunctions should be
imposed according to their own balancing of fundamental rights and application of international norms. The proposed Digital Service Act (DSA) also noted that the territorial scope of orders to act against illegal content, on the basis of the applicable rules of EU and national law, including the Charter, and, where relevant, general principles of international law, should not exceed what is strictly necessary to achieve its objective. So, blocking injunctions must be targeted and specific with a territorial scope not broader than what is necessary to achieve its objective, according to fundamental right balancing and international law, including the doctrine of comity.

(10) Static and dynamic blocking case-law shows multiple instances of legal entanglement among national courts of different SMS. Legal entanglements can be considered a form of informal cross-border cooperation and occur when national courts refer to judgments from other jurisdictions.

(11) An additional important factor to evaluate availability, scope and proportionality of blocking injunctions is their effectiveness in reducing infringement. The effectiveness of blocking injunctions is usually not explicitly assessed in most SMS. However, it has been considered by some SMS’ courts, in particular in the UK and the Netherlands. Effectiveness might not require that the injunctions are 100 % successful, as long as the remedy is seriously discouraging internet users from accessing the infringing content.
CASE-LAW OF THE CJEU

27/03/2014, C-314/12, UPC TELEKABEL WIEN GMBH V CONSTANTIN FILM VERLEIH GMBH, WEGA FILMPRODUKTIONSGESELLSCHAFT MBH, EU:C:2014:192

NORMS

Article 8(3) of Directive 2001/29/EC.

FACTS

Having established that a website was offering, without their agreement, either a download or ‘streaming’ of some of the films which they had produced, Constantin Film and Wega, two film production companies, referred the matter to the court responsible for hearing applications for interim measures with a view of obtaining, on the basis of Article 81(1a) of the German Copyright Act (Urheberrechtsgesetz), an order ordering UPC Telekabel Wien GmbH, an internet service provider, to block the access of its customers to the website at issue, inasmuch as that site makes available to the public cinematographic works over which Constantin Film and Wega hold a right related to copyright without their consent.

SUBSTANCE

The website operating under the domain name kino.to enables users to access a wide range of films protected by copyright via streaming or downloading. The plaintiffs, the film production companies Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft GmbH, hold related rights in some of these films. The plaintiffs sought a court order obliging the defendant, the Austrian ISP UPC Telekabel Wien GmbH, to block the website. The Commercial Court, Vienna, granted an injunction prohibiting the defendant from providing its customers with access to the website. In particular, the site’s domain name and current IP address should be blocked. Both parties lodged appeals, and the Oberlandesgericht Wien (Higher Regional Court, Vienna) partially reversed the order of the court of first instance. Lastly, the Oberster Gerichtshof (Supreme Court, Austria) asked the CJEU to clarify whether a person who makes protected subject matter available to the public on a website without the agreement of the rights holder is using the services of the ISP in the sense of Article 8(3) D 2001/29. It also asked, amongst other questions, whether the blocking measures ordered were compatible with EU law, and notably with fundamental rights, where they prohibit in general terms (i.e. without ordering specific measures) an ISP from allowing its customers access to a certain website where the material provided is exclusively or predominantly without the rights holder’s consent, when that injunction does not specify the measures that the access provider must take and when that ISP can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures.

According to the CJEU, ISPs fall under Article 8(3) D 2001/29, and the term ‘intermediary’ covers any person who carries a third party’s infringement of a protected work or other subject matter in a network (para. 30). Neither the wording of Article 8(3) nor any other provision of D 2001/29 indicates that a specific relationship between the person infringing copyright or a related right and the intermediary is required (para. 35). Therefore, Article 8(3) D 2001/29 must be interpreted as meaning that a person
who makes protected subject matter available to the public on a website without the agreement of the rights holder, for the purpose of Article 3(2) D 2001/29, is using the services of the ISP (para. 40). The CJEU ruled that the fundamental rights recognised by EU law do not preclude a court injunction prohibiting an ISP from allowing its customers access to a website placing protected subject matter online without the agreement of the rights holders when that injunction does not specify the measures which the ISP must take, provided the following conditions are fulfilled: the ISP can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures; the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available; those measures have the effect of preventing unauthorised access to the protected subject matter, or of making access difficult; the measures seriously discourage internet users who are using the services in question from accessing the infringing subject matter. The national authorities and courts need to establish whether these conditions are fulfilled (para. 64).

15/09/2016, C-484/14, TOBIAS MCFADDEN V SONY MUSIC ENTERTAINMENT GERMANY GMBH, EU:C:2016:689

NORMS

Article 12(1) of Directive 2000/31/EC read in conjunction with Article 12(3) of that Directive.

FACTS

Mr Tobias McFadden was offering free wireless local area network (WLAN) without a password of any kind or protection to his clients. A protected musical work was made available to the public using his WLAN. Sony Music Entertainment Germany GmbH (Sony Music), the producer of the phonogram of the protected work at issue, gave Mr McFadden a formal notice to respect its rights over the phonogram. Mr McFadden brought an action for a negative declaration. The referring court dismissed Mr McFadden’s action and upheld the counterclaims of Sony Music, which mainly consisted of the payment of damages on the ground of liability for infringement, an injunction against the infringement and the reimbursement of the costs of litigation. Mr McFadden appealed the judgment on the ground of exemption from liability stemming from Article 12(1) of Directive 2000/31/EC as transposed in German law. Sony Music argued that Mr McFadden should be held liable for direct infringement, and alternatively, for indirect infringement as he had not taken steps to protect his WLAN. The Landgericht München I (Regional Court, Munich I, Germany) asked the CJEU to clarify the meaning of Article 12(1) of Directive 2000/31/EC. The German court asked, among others, two questions relevant for allowing dynamic blocking injunctions, namely whether: (1) the expression 'not liable for the information transmitted' precludes, as a matter of principle, or in any event in relation to a first established copyright infringement, any claims for injunctive relief, damages, the payment of the costs of giving formal notice or court costs which a person affected by a copyright infringement might make against the access provider where indirect liability could be established when a service provider does not secure its network with a password, and a third party uses it to infringe a copyrighted work; and (2) the Member States may not permit a national court, in substantive proceedings, to make an order requiring an access provider to refrain in future from enabling third parties to make a particular copyright-protected work available for electronic retrieval from an online exchange platform via a specific internet connection.

SUBSTANCE

On the first question the CJEU found that Article 12(1) of Directive 2000/31 must be interpreted as precluding a person harmed by the infringement of its rights over a work from claiming compensation
from a provider of access to a communication network on the ground that such access was used by a third party to infringe its rights and the reimbursement of the costs of giving formal notice or court costs incurred in relation to its claim for compensation. However, that article must be interpreted as meaning that it does not preclude such a person from claiming injunctive relief against the continuation of that infringement, and the payment of the costs of giving formal notice and court costs from a communication network access provider whose services were used in that infringement where such claims are made for the purposes of obtaining, or follow the grant of injunctive relief by a national authority or court to prevent that service provider from allowing the infringement to continue.

With regard to the second question, the CJEU held that having regard to the requirements deriving from the protection of fundamental rights and to the rules laid down in Directives 2001/29 and 2004/48, Article 12(1) of Directive 2000/31, read in conjunction with Article 12(3) of that Directive, must be interpreted as, in principle, not precluding the grant of an injunction such as that at issue in the main proceedings, which requires, on pain of payment of a fine, a communication network access provider to prevent third parties from making a particular copyright-protected work or parts thereof available to the general public from an online (peer-to-peer) exchange platform via the internet connection available in that network, where that provider may choose which technical measures to take in order to comply with the injunction, even if such a choice is limited to a single measure consisting in password-protecting the internet connection, provided that those users are required to reveal their identity in order to obtain the required password and may not therefore act anonymously, a matter which it is for the referring court to ascertain.

All in all, the CJEU ruled that copyright holders can seek injunctions to stop future infringements, where such injunctions respect the balance between the interests at stake and protect fundamental rights (notably, the right to protection of intellectual property, the provider’s freedom to conduct business, and the freedom of information of the recipients of the service).

03/10/2019, C-18/18, GLAWISCHNIG-PIESZCZEK V FACEBOOK IRELAND LIMITED, EU:C:2019:821

NORMS

Article 14(1) and (3), Article 15(1) and Article 18(1) of Directive 2000/31/EC.

FACTS

Ms Eva Glawischnig-Piesczek, an Austrian politician, sued Facebook Ireland in the Austrian courts seeking an order that Facebook Ireland remove a comment published by a user on that social network harmful to her reputation, as well as allegations which were identical and/or of an equivalent content.

The Facebook user in question had shared on that user’s personal page an article from the Austrian online news magazine oe24.at entitled ‘Greens: Minimum income for refugees should stay’. That had the effect of generating on that page a ‘thumbnail’ of the original site, containing the title, a brief summary of the article and a photograph of Ms Glawischnig-Piesczek. That user also published, in connection with that article, a comment that the Austrian courts found to be harmful to the reputation of Ms Glawischnig-Piesczek, and which insulted and defamed her. This post could be accessed by any Facebook user.

Against that background, the Oberster Gerichtshof (Supreme Court, Austria) asked the CJEU to interpret the Directive on electronic commerce.
Under that Directive, a host provider such as Facebook is not liable for stored information if it has no knowledge of its illegal nature or if it acts expeditiously to remove or to disable access to that information as soon as it becomes aware of it. That exemption does not, however, prevent the host provider from being ordered to terminate or prevent an infringement, including by removing the illegal information or by disabling access to it. However, the Directive prohibits any requirement for the host provider to monitor generally information which it stores or to seek actively facts or circumstances indicating illegal activity.

**SUBSTANCE**

The CJEU answered the Oberster Gerichtshof that the Directive on electronic commerce, which seeks to strike a balance between the different interests at stake, does not preclude a court of a Member State from ordering a host provider:

(a) to remove information which it stores, the content of which is identical to the content of information that was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;

(b) to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content (thus, the host provider may have recourse to automated search tools and technologies);

(c) to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law, and it is up to Member States to take that law into account.

**FACTS**

Stichting Brein is a Dutch foundation, which safeguards the interests of copyright holders. Ziggo and XS4ALL are internet access providers. A large number of subscribers to both Ziggo and XS4ALL shared copyright-protected content via the peer-to-peer (P2P) platform The Pirate Bay (TPB), with the help of torrent software. Stichting Brein requested a court order against Ziggo and XS4ALL to block all domain names and IP addresses related to TPB. The Court of First Instance upheld this request, but the Appeal Court rejected it. The High Court of the Netherlands found that the actions of the online
sharing platform TPB make protected works available to the public without the rights holders’ consent. It has also been established that subscribers to Ziggo and XS4ALL, through this platform, make protected works available without the rights holders’ consent and thus infringe the copyright and related rights of those rights holders. The High Court was not able to establish, however, whether the actions of TPB could also be considered as a ‘communication to the public’. The High Court asked the CJEU whether making available and managing a sharing platform on the internet that allows its users to locate protected works and share them in the context of a P2P network, constitutes ‘communication to the public’ (Article 3(1) of 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).

SUBSTANCE

The Court stated that the concept of ‘a communication to the public’, within the meaning of Article 3(1) of Directive 2001/29/EC, should be assessed individually for each case. The concept contains two cumulative criteria: an ‘act of communication’ and ‘a public’. To assess whether there is an ‘act of communication’ several, complementary criteria need to be taken into account: the deliberate nature of the action, the use of specific technical means different from those previously used or allowing a ‘new public’ to be reached and the profit-making nature of the communication. In applying these criteria to the case, the Court found that making protected works available on the sharing platform constitutes an ‘act of communication’. To reach this conclusion it referred to previous case-law. The question remained, however, whether TPB itself could be held liable for this act of communication, as the protected works were placed online by TPB users and not by TPB itself. The Court ruled that the TPB operators play an essential role in making protected works available, as they make the platform available and manage it. Without this platform it would be impossible or very difficult for users to share the protected works. Therefore, making an online sharing platform available, that provides its clients with access to protected works, and managing it, is liable to constitute an ‘act of communication’ for the purposes of Article 3(1) of Directive 2001/29/EC. The Court found that there was a ‘public’ since at least all the platform users, who were proven to be a large number, could access the works at any time, simultaneously. Furthermore, there was a ‘new public’ that had not been taken into account by the copyright holders when they authorised the initial communication. Since the operators were informed that the platform was used to provide access to works published without authorisation, they expressed their intention to make protected works available. Furthermore, the large number of torrent files on TPB indicates that the operators could not have been unaware thereof.
CASE-LAW OF NATIONAL COURTS

Belgium

COURT OF APPEALS OF ANTWERP 3399-2011/8314, 26 SEPTEMBER 2011, BELGIAN ANTI-PIRACY FEDERATION (BAF) V. TELENET AND BELGACOM

NORMS

Article 87(1) par.2, of the Belgian Law of 30 June 1994 on Copyright and Neighbouring Rights (Copyright Act) (now Article XVII.14, par.4 CEL);
Article 21(1) of the Belgian Act of 11 March 2003 on certain legal aspects of information society services (the ‘e-commerce Act’) (now Article XII.20 CEL).

FACTS

In 2010, the Belgian Anti-piracy Federation (BAF) applied for an injunction in a cease and desist proceeding against two Belgian ISPs. They asked that the two ISPs be ordered to block access for their users to the website The Pirate Bay.

In first instance, the Antwerp Commercial Court rejected the claim made by BAF, considering the order disproportionate and unnecessary. BAF lodged an appeal before the Antwerp Court of Appeal.

SUBSTANCE

The Court of Appeal overturned the lower court’s decision.

After finding that the website The Pirate Bay was infringing copyright on a massive scale, the Court of Appeal of Antwerp ordered Telenet and Belgacom to cease the infringements by applying DNS blocking to an exhaustive list of 11 domain names provided by BAF, under pain of a penalty payment of EUR 1 000 per day. The Court rejected BAF’s claim to apply IP-blocking technology and to extend the blocking order to other The Pirate Bay websites that BAF offered to identify and send to the ISPs.

Against the issuance of this injunction, Telenet and Belgacom argued that their role as ISPs prevented them from being held liable for the copyright violations committed by their customers and that such an order would put them under a general obligation of monitoring their network. In addition, they contended that the blocking order was disproportionate and inefficient – a blocking order being easily circumvented – and not only would not lead to the cessation of the infringements, but that it would also block legitimate information. They held that the appellant should have first directed its legal action against the direct infringer (subsidiarity principle). Eventually, they alleged that this order would conflict with other fundamental rights and freedoms, and would place them in a competitive disadvantage regarding other Belgian ISPs.

The Court held that according to Article 87(1) par.2 of the Copyright Act, it was entitled to issue an injunction against the ISPs, in their quality of intermediaries whose services are used by a third party
to infringe a copyright or related right, and reminded them that their liability for copyright infringement was not at stake. The Court also added that the liability exemption regime provided for under Article 12 of the e-commerce Directive was not an obstacle to the issuance of this injunction order.

Then the Court stated that Telenet and Belgacom were under no general obligation to monitor their network (Article 15 of the e-commerce Directive) and held that the blocking order was not disproportionate. In the Court’s view, most of The Pirate Bay websites are indeed infringing and the few material not copyright protected can be accessed by internet users through other channels. The Court also ruled that to be proportionate, it was enough that the blocking order contribute to the reduction of the infringing activity. The Court clarified that there was no subsidiarity principle obliging BAF to first lodge an action against the direct infringer.

When performing the balancing exercise between the fundamental rights and freedoms in the case in question, the Court stated that the ISPs had failed to demonstrate any valid interests that outweigh the copyright protection of BAF’s members facing the diffusion on a massive scale of their protected works via The Pirate Bay websites.

Regarding the alleged risk of competitive disadvantage, the Court considered that there was no such risk given that Telenet and Belgacom are the biggest ISPs in Belgium.

The Court also explained that, technically speaking, it was not impossible for ISPs to make their website unavailable to their customers. It refers to the blocking orders already issued by the Prosecutor in other areas such as child pornography.

However, the Court decided that DNS blocking of the list of websites provided by BAF was the most acceptable solution in the case in question. It would prevent any undesirable effects caused by the IP blocking technical solution, such as blocking legitimate information.

**COURT OF CASSATION P.13.0550.N/1, 22 OCTOBER 2013, BELGIAN ANTI-PIRACY FOUNDATION V BELGACOM**

**NORMS**

Articles 39 bis and 89 of the Belgian Code of criminal procedure;
Article 21(1) of the Belgian Act of 11 March 2003 on certain legal aspects of information society services (the ‘e-commerce Act’) (now Article XII.20 CEL);

**FACTS**

Civil proceedings

In 2010, the Belgian Anti-piracy Federation (BAF) applied for an injunction in a cease and desist proceeding against two Belgian ISPs in order to stop their customers accessing the content hosted by the server associated with various The Pirate Bay domain names.

The Court of Appeal of Antwerp, after finding that The Pirate Bay websites were infringing copyright, ordered Telenet and Belgacom to cease the infringements by applying DNS blocking to an exhaustive list of 11 domain names provided by BAF, under pain of a penalty payment of EUR 1 000 per day. The Court rejected the claim to extend the blocking order to other The Pirate Bay websites.
Criminal proceedings

However, after finding out that The Pirate Bay websites were quickly accessible again through other domain names, the applicants issued a criminal procedure for copyright infringement asking the judge to order the ISPs to block access to the content provided by The Pirate Bay without specifying an exhaustive list of domain names or imposing a time limit on the injunction.

The request was accepted. By an order of 6 April 2012, the investigating judge of the Malines Court of First Instance required all internet operators of services providers to make access to the content hosted by the server associated to the main domain names thepiratebay.org impossible. He further specified that they could use all technically possible means, including, at least, the blocking of domain names redirecting to the server associated to the domain name thepiratebay.org. The judge added that the list of domain names to be blocked would be set and provided by the police (i.e. the RCCU (Regional Computer Crime Unit) of Malines and the FCCU (Federal Computer Crime Unit)).

The three Belgian providers (Telenet, Tecteo and Brutele) took the case to the Court of Appeal, who maintained the injunctive relief (ruling of 14 February 2013). The Court specified that the investigating judge could rightly order the necessary provisional measures to put an end to the damage caused to the civil party. The ISPs eventually went to the Belgian Supreme Court which ruled on points of law.

SUBSTANCE

The plaintiffs first questioned the legal basis of the measure. They argued that Articles 39 bis and 89 of the Belgian Code of criminal procedure do not empower investigating judges to require all internet operators and service providers to block access to all The Pirate Bay domains. They also contended that such an injunction, not limited to an exhaustive list of domain names and not limited in time, infringes Article 21 of the Belgian e-commerce Act (implementing Article 15 e-commerce Directive) and Article 52.1 Charter of the Fundamental Rights of the EU.

This is because, according to them, the injunction does not specify the means to be employed in order to comply with the obligation imposed on them and does not specify the domain names which must be blocked. In their view, a law imposing a temporary monitoring obligation on internet service providers must be sufficiently clear and predictable. The plaintiffs also requested the Supreme Court ask preliminary questions to the CJEU. By their questions, they asked in essence whether Recital 47 and Article 15 of the e-commerce Directive authorise a national legislation to impose, on an information society service provider within the framework of a judicial investigation, the obligation to make inaccessible illegal content on the internet without specifying the means to be used for this purpose, nor indicating exhaustively the domain names that should be blocked.

The Courts first held that Article 39 bis of the Belgian Code of criminal procedure does not exclude a measure to be ordered against third parties, other than those having stored the data themselves. More generally, the Court confirmed that the investigating judge could rightly rely on this provision to order the national internet access providers to stop access to the content hosted by the server associated to the main domain name thepiratebay.org, by using all technical means possible, including at least the blocking of all domain names which refer to this server. The domain names to be blocked were provided by the police (RCCU and FCCU). (§14)

The Court also found that such an order would only remove the internet users’ access to the data stored on The Pirate Bay but would not prevent The Pirate Bay operators from having access to their website (§16), nor delete the content of such website (§19).
The Court recalled that the prohibition of general monitoring provided for in Article 15(1) e-commerce Directive does not prevent a competent national authority from imposing temporary monitoring obligations in specific cases (§23). It found that the order at stake does not constitute a general monitoring obligation because it does not require the service provider to monitor the information it transmits or stores or to actively seek information revealing illicit activities. (§24)

The Court also referred to the Court of Appeal reasoning according to which, there is no general monitoring obligation provided that the list of domain name to be blocked will be provided by the police. (§25)

The court dismissed the case and refused to ask questions to the CJEU.

**Denmark**

MARITIME AND COMMERCIAL COURT (SØ- & HANDELSRETTEN), CASE NUMBER A-51-17, 21 FEBRUARY 2018, FRITZ HANSEN A/S AND OTHERS (REPRESENTED BY RETTIGHEDSALLIANCEN SMF.) V. TELIA DANMARK A/S AND DOMINIDESIGN FURNITURE LTD

**NORMS**

Paragraphs 2(1)-2(3), 413(3), 414(2) of the Danish Law on Copyright; Paragraph 1 of the Law on Commercial Practices (Markedsføringsloven).

**FACTS**

Rettigheds Alliancen is a Danish association defending the interests of affiliated rights holders from the film, music, literature, image, design and media industries on the internet. Fritz Hansen A/S, Louis Poulsen Lighting A/S, Carl Hansen & Søn Møbelfabrik A/S and Fredericia Furniture A/S (hereinafter Fritz Hansen and Others), all members of Rettigheds Alliancen, have copyrights for furniture and lamps, of which replicas have been offered for sale on various websites (www.dominidesign.com, www.privatefloor.com, www.interiorfox.com, www.italiadesigns.com, www.bauhausitalia.com, www.vertigointeriors.com and www.122design.com). The sale of replicas on those websites to customers in Denmark has been confirmed when Rettigheds Alliancen made several test purchases. Following those test purchases, Rettigheds Alliancen contacted the websites and informed them about the infringement of their client’s copyright rights. Only the owners of two of those websites responded, with one denying the allegations and the other one claiming that they are closing their business. Telia Denmark A/S is a Danish telecommunications and internet service provider and a member of the intertrade organisation Teleindustrien. Teleindustrien and Rettigheds Alliancen have an agreement concerning blocking access to services which infringe intellectual property rights in Denmark.

Rettigheds Alliancen, representing its clients, requested that Telia Denmark A/S be prohibited from providing its customers in Denmark with access to the internet websites which have been confirmed to sell replicas of copyrighted furniture and lamps. Furthermore, it requested an order for Telia Denmark A/S to implement a technical solution, for example DNS blocking, capable of preventing customers in Denmark from accessing those websites and to expand that order also to other websites.
providing the same service (i.e. selling replicas of copyrighted design items to Danish customers), if those websites are confirmed to do so by Rettigheds Alliancen.

Telia Danmark A/S requested that this prohibition be refused. Dominidesign Furniture Ltd., an Irish undertaking, providing the website www.dominidesign.com, joined the proceedings at a later stage. They requested that the application for an interim prohibition and injunction be refused, or alternatively that the case be dismissed. They furthermore argued that Denmark is not the relevant jurisdiction in this case since, at the time of the main proceedings, the content of their website was not in Danish, and it was not possible to pay in the Danish currency or to order the goods featured on their website from Denmark.

**SUBSTANCE**

The Maritime and Commercial Court found that Denmark has jurisdiction in relation to the action in question. As the evidence showed, before the main proceedings started, Rettigheds Alliancen was able to purchase replicas of furniture and lamps, the copyright of which is owned by Fritz Hansen and Others, from www.dominidesign.com and other websites (as listed above and included in the Court’s file), and the products were subsequently delivered to Denmark. These products were thus made available to the public in Denmark for the purposes of paragraph 2(3)(1) of the Law on Copyright. Consequently, these websites infringe the copyrights owned by Fritz Hansen and Others under paragraph 2(2) of the Law on Copyright, in conjunction with subparagraph (1) thereof. In 2018, after the infringement proceedings had been initiated, Dominidesign Furniture Ltd. updated their general terms and conditions to include a provision that no delivery may take place to Denmark. However, the Court found that this per se does not exclude the risk of further infringements of the same kind under paragraph 413(2) of the Law on Copyright.

As regards the injunction against Telia Danmark A/S as an internet provider, the Court found that it should be straightforward for Telia Danmark A/S to block access to the websites in question. The imposition of a prohibition on Telia Danmark A/S will therefore not give rise to harm or prejudice which is significantly disproportionate in relation to the interests which Rettigheds Alliancen and Fritz Hansen and Others have in notification of a prohibition and injunction under paragraph 414(2) of the Law on Copyright. In that connection, the Court further noted that the Code of Conduct agreed between Teleindustrien and Rettigheds Alliancen assumes that it will be possible to direct a claim for prohibition at individual network operators.

Therefore, the Court ordered Telia Danmark A/S to implement a technical solution, for example DNS blocking, that is capable of preventing customers in Denmark from accessing the listed websites that are selling replicas of Fritz Hansen and Others’ copyrighted furniture and lamps. The order also applies to other websites that provide access to the same internet services and which are notified to Telia Danmark A/S by the Rettigheds Alliancen under the agreed Code of Conduct. In that respect, Rettigheds Alliancen undertakes legally and financially to guarantee that those websites are providing access to the internet services to which the decision of the Court relates.
STUDY ON DYNAMIC BLOCKING INJUNCTIONS
IPR ENFORCEMENT CASE-LAW COLLECTION

DISTRICT COURT OF FREDERIKSBERG - COPENHAGEN - 05/12/2017 - RETTIGHEDSALLIANCEN ETC. V TDC A/S262

NORMS

§ 2(2) of the Copyright Act. 1, cf. 3, No. 3, cf. 4, No. 1, cf. § 65, paragraph 1. 1 and 6 and § 66(1). 1 and 2 and 67(1). 1 and 2;
§ 2(1) of the Copyright Act. 4, No. 1;
Article 3(1) and Article 8(1) Directive 2001/29/EC.

FACTS

The judgment concerns the question of whether the ISP must be prohibited from providing access to its customers in Denmark to internet services that make available or share works to which the applicants have copyrights.

The applicants are an association that works to counteract the illegal use of films, TV shows, music, literature, etc. on the internet.

Popcorn Time offers free films and TV shows over the internet on the Danish market. It is a decentralised system: films and TV series with accompanying metadata, subtitles, etc. are available on various websites which form part of the system that is crucial for the user’s ability to play films and TV shows through the system. Popcorn Time operates like a media player with a built-in application.

The applicants wrote in May 2017 to the websites that are subject to the injunction application and urged them to terminate the infringements of the copyright holders’ rights.

SUBSTANCE

The court establishes that the applicants are the rights holders. Due to the lack of permission, the access to the content referred to on the internet provided by the Popcorn Time system is in violation of the applicants’ rights (Article 3(1) of the InfoSoc Directive, cf. § 2(2) of the Copyright Act. 1, cf. 3, No. 3, cf. 4, No. 1, cf. § 65, paragraph 1. 1 and 6, § 66, subsection 1 and 2 and 67(1). 1 and 2., § 2(1) of the Copyright Act. 1, cf. 2).

The court states that the Popcorn Time system (constituting a service similar to a media player, as detailed in paragraphs 41 and 42 of the decision CJEU ‘Film Player’ (26/04/2017, C-527/15, Stichting Brein v Jack Frederik Wullems, EU:C:2017:300) makes copyrighted films and television series accessible to the public over the internet (transfer to the public) without the permission of the copyright owners.

As the Popcorn Time system makes use of the websites mentioned in the claim for the illegal viewing of films and television series, it is possible to prohibit the websites in question (§ 413 of the Procedural Code). The ISP’s transmission of data objectively infringes the applicants’ copyright. The Member States must ensure that rights holders may apply for a prohibition on intermediaries whose services are used by third parties to infringe copyrights or related rights (Article 8(1) and (3) of the InfoSoc Directive).

(262) Not available via free online resources.
The applicants proved that they are the rights holders, that the ISP’s conduct requires the injunctions as requested and that the applicants’ ability to exercise their rights will be lost if they need to wait the duration of the full legal dispute.

When website addresses are DNS-blocked on the basis of a court decision, telecommunications industry members will also block additional website addresses if the applicant claims that these website addresses also provide access to the service covered by the court order ('Code of Conduct for handling decisions on blocking access to IPR services'). The blocking presupposes that the applicants agree to indemnify the ISP financially in this regard. The applicants’ claims are upheld (§ 413 of the Procedural Code). Since the ISP’s customers will not be able to claim compensation against the ISP, no bail need be imposed for the cancellation of the prohibition and the injunction. Each party should bear its own costs.

The ISP is ordered to implement a technical solution, such as a DNS blocker, that is suitable for preventing the ISP’s customers from accessing the internet services currently accessible through the website addresses, as well as for other website addresses that provide access to the same internet services, which the applicants will expressly notify to the ISP, and in connection with which the applicants must demonstrate that these website addresses provide access to the internet services to which this decision relates.

Neither party will pay costs to the other party.

Finland

THE FINNISH MARKET COURT (MARKKINAOIKEUS), MAO:311/18, 07/06/2018

NORMS

Article 60 e (1), (2) and (3) of the Finnish Copyright Act;
Article 8(3) Directive 2001/29/E.

FACTS

The applicants are film companies (Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Paramount Pictures Corporation, Twentieth Century Fox Film Corporation, Universal City Studios Productions LLLP and Warner Bros. Entertainment Inc.) and rights holders. The intermediaries are internet service providers (Blue Lake Communications Oy, DNA Oyj, Elisa Oyj, Kaisanet Oy, Lounea Palvelut Oy, MPY alvelut Oyj and Telia Finland Oyj).

The injunction is sought against Rarbg and Yify-torrent internet services by removing their domain names rarbg.to, rarbg.com, rarbgmirror.com, rarbg.is, rarbgproxy.com, rargungblock.com, rarbg.unblockall.org, rarbg.bypassed.st, rarbg.unblocker.cc and yify-torrent.org from the internet service providers’ name servers and blocking the internet service providers’ customers access to the IP addresses 185.37.100.122, 185.37.100.121, 185.37.100.123 and 46.148.16.26.
SUBSTANCE

The court found the intermediary parties were involved as internet access providers. The target websites are available through the intermediaries, and the court stated that the parties cover most of the Finnish bandwidth making the injunction measure effective.

The court assessed that the applicants sufficiently showed that the alleged infringers are not identifiable or the possibility to identify them through international procedurals are uncertain based on an overall assessment. The court found that the identification of the alleged infringers was not successful as the purposive efforts of the administrators of the websites to hide their own identities and being primarily domiciled outside the EU would result in unreasonable measures having to be taken in the matter.

According to the evidence submitted, the court found that the infringement of making copyrighted content available to the public without the consent of rights holders was significant. The court referred to the evidence that the infringing websites were popular and that the majority of the content on the websites was unauthorised content in the film and TV programme category. In addition, the court noted that Yify-torrent was not as popular as Rarbg in Finland, but it had experienced a significant increase in visitors and it specialised in films. The court noted that the alleged infringers cannot be considered to be unaware of the infringing content because they have purposively hidden their identities and they have received income from advertisements.

The applicants argued that it would be unreasonable to also identify the administrators of the proxy sites that direct to the main infringing websites. The court found that the proxy sites cannot be included in the injunction because the applicants did not show any measures taken to identify their administrators. The court noted that all the conditions for the injunction must be met for each IP address or domain name that is subject to the application. Therefore, the request to block rargungblock.com, rarbg.unblockall.org, rarbg.bypassed.st, rarbg.unblocker.cc was dismissed.

Assessing the proportionality of the injunction, the court found that the majority of the available content is likely protected by copyright and without authorisation and there are no other relevant purposes for the website services. Therefore, the court did not find the injunction unreasonable for the alleged infringer, the recipient of the material (the user) or the author. The court also noted that the parties were given an opportunity to be heard and they have not opposed the application nor presented evidence that the injunction is unreasonable.

The court found that the third parties’ right to receive and send messages is not endangered by blocking the IP addresses in question. The court assessed that the evidence submitted by the applicants showed sufficiently that there are no other domain names behind those IP addresses. The court also noted that there is legal 1 year time limit for an injunction and that the applicants have the possibility to delete domain names and IP addresses from the scope of the injunction.

The court did not provide separate injunctions for possible changes or adding changes as the applicants did not provide anything that would suggest that they requested something else or more than what is already provided for by law. An injunction is limited to a maximum of 1 year and an extension can only be applied for with another injunction under the law. The Government Proposal states that an injunction can be changed and new IP addresses added with a new application.

The Finnish Market court ruled that Blue Lake Communications Oy, DNA Oyj, Elisa Oyj, Kaisanet Oy, Lounea Palvelut Oy, MPY Palvelut Oyj and Telia Finland Oyj must block their customers from accessing the Rarbg and Yify-torrent internet services by deleting the domain names rarg.to,
rarbg.com, rarbgmirror.com, rarbg.is and yify-torrent.org and by blocking the IP addresses 185.37.100.122, 185.37.100.121, 185.37.100.123 and 46.148.16.26. The injunction was set to be in place for 1 year, stating that the measures need to be put in place within 1 week of the entry into force of the injunction and that the measures can be deleted at the earliest 1 week before the injunction expires.

France

PARIS TGI, 23 MAY 2019, RG 19/01744

NORMS

Article 8(3) Directive 2001/29/CE;
Article L. 322-6 Code la propriété intellectuelle (Intellectual Property Code (France));

FACTS

In a previous decision, Film Industry Associations had achieved blocking measures against internet service providers because copyright- and neighbouring rights-protected content were broadcast on a number of IP infringing websites.

In the decision in question, they requested a dynamic de-indexing injunction against a search engine operator, Google, with the justification that internet users could easily circumvent the blocking measures already ordered against ISPs. By using the term blocking injunction and a dynamic de-indexing injunction, the applicants meant ordering the search engine operator to prevent the appearance of results leading to websites via domain names mentioned in the decision, but also via future access paths that the search engine operator would also be able to track.

SUBSTANCE

The applicants asked for blocking injunctions and a dynamic de-indexing injunction against the search engine, explaining that the first does not suffice, given that they can be circumvented by the users. However, the search engine operator has the technical means to prevent this without having to bear excessive costs for this purpose, as they would be able to choose which technical measures to apply in order to ensure the implementation of the order.

After balancing rights and interests, especially by drawing on a CJEU decision, 27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192, the Court considered that the previous blocking measures ordered against ISPs were not sufficient to avoid IPR infringements, notably because internet users could circumvent the measures via virtual private networks. It held that the search engine operator should take all appropriate measures to prevent these infringements. Stopping internet users accessing the content of the infringing websites was not considered disproportionate compared to the importance of the protection of the IP rights at stake. In addition, the operator’s freedom to conduct a business was not prejudiced because the search engine operator has the capacity and technical means to identify alternative access paths to the infringing websites and to prevent their listing.
By stating that there is no need to limit de-indexing measures to only the identified domain names, and by using the adverb ‘notably’ when mentioning them, the Court indirectly ordered a dynamic de-indexing injunction, including examining the possibility of extending the measures to future domain names, even if not specifically mentioned in the decision.

The Court also ordered that during the period of implementation of the blocking and de-indexing measures the applicants were to inform the search engine operator if any of the infringing websites or access paths were no longer active or if the protected content was removed.

The measures would be implemented within 15 days of the notification of the decision and for a period of 18 months.

PARIS TGI, 7 MARCH 2019, 18/14194

NORMS

Articles L. 111-1, L. 121-1, L. 122-1 to L. 122-4 Code de la propriété intellectuelle (Intellectual Property Code (France)) (copyright infringement);
Article L. 336-2 Code de la propriété intellectuelle (Intellectual Property Code (France)).

FACTS

The applicants are scientific publishing companies involved in publications and data analyses that address researchers, students, professors, and health and science professionals.

These publications, protected by copyright, were reproduced on websites, where they were accessible via several domain names, without prior authorisation.

Therefore, the publishing companies requested dynamic blocking injunctions against the French internet service providers to prevent the infringement of their copyright. They referred to domain names that would be identified in the decision, but also to domain names and access paths not currently identified that would be activated or available after the issuing of the blocking order.

SUBSTANCE

The Court, after assessing the evidence submitted, concluded that the applicants’ copyright was indeed sufficiently demonstrated and proven. It thus ordered ISPs to implement all appropriate measures to prevent access from France by their internet users under contract in that territory, by any effective means, to the sites mentioned accessible via the domain names referred, within 15 days of the notification of the decision and for a period of 12 months from the implementation of the measures ordered.

The blocking measures would only concern the disputed sites that were expressly and restrictively listed in the applicants’ request. Any measure affecting another website would have to be authorised by a judicial authority, because ISPs are not obliged to monitor content under current legislation and publishers do not have the right to have access to websites blocked without the prior control of the judicial authority.

The measures should be proportionate, adequate and strictly necessary to achieve the aim pursued and ensure the protection of the rights at stake. There should be a balance between the fundamental
rights involved, so that the injunction does not unduly and unnecessarily affect them. Therefore, the blocking injunction should only concern the infringing websites expressly and restrictively mentioned in the decision.

The costs of the necessary measures to be taken should be borne by the ISPs, as they were the ones to choose the technical means they would use for this purpose, even if the implementation costs were likely to be significant.

The Court also mentioned that ISPs should contribute to the fight against illegal content, and in particular against the infringement of copyright and related rights, since they are the most appropriate ones to do so and in the best position to put an end to these kinds of infringements.

PARIS TGI, 13 JULY 2018, 18/55236

NORMS

Article L. 336-2 Code de la propriété intellectuelle (Intellectual Property Code (France)); Articles 808 and 809 Code de procédure civile (French code of civil procedure); Articles 122-1, 122-2, 122-3, 122-4, 215-1 Code de la propriété intellectuelle (Intellectual Property Code (France)).

FACTS

A number of Film Industry Associations and a public administrative establishment had achieved blocking measures against internet service providers with previous court decisions, because copyright- and neighbouring rights-protected contents were broadcast on various IP infringing websites.

The same applicants asked for an update to these measures against ISPs because the infringing websites were found to be accessible again via new domain names. Therefore, they requested new blocking orders including the new domain names and access paths to the protected content.

SUBSTANCE

The Court, by assessing the requested and provided official reports and evidence, verified that the infringing websites were still accessible via new domain names.

Taking the findings of the previous decisions into consideration, especially regarding the fact that ISPs should be the ones to bear the costs of implementing the measures ordered by the Court and the fact that in the process of striking a balance between rights such as the freedom of expression, the freedom to conduct a business and the principle of proportionality, the protection of IP rights was found to be of significant importance and the blocking order would not prejudice the freedom of expression and the ISPs’ freedom to conduct a business, the updated blocking orders were granted.

The Court, in light of Directive 2001/29/EC, ordered the ISPs to implement all the efficient and appropriate measures to prevent access to the infringing websites throughout France by their internet users.

The ISPs should bear the costs and freely choose any effective means to block access to the sites listed in the decision that were again accessible via the new domain names.
The measures would be implemented within 15 days of the notification of the decision and last until 15 December 2018 for the domain names listed in it.

**SUPREME COURT (COUR DE CASSATION), 6 JULY 2017 16-17.217**

**NORMS**


**FACTS**

The decision refers to previous court decisions regarding the request made by Film Industry Associations to order French ISPs to block access to websites leading to copyright-protected content and the main search engine operators to stop listing them. It also refers to the updating of such orders without the need of a new court procedure.

The Court of Appeal of Paris had stated that ISPs and search engines must cover the costs of the injunctions because the rights holders were not in the position to sustain these measures financially. The ISPs requested that the rights holders be the ones to bear the costs of the dereferencing procedure of the infringing websites.

**SUBSTANCE**

At stake before the Supreme Court was the cost of blocking measures. The Court upheld the decision issued by the Court of Appeal and stated that, even if it held that ISPs are not responsible for the infringing acts, they should be the ones to bear the costs that are strictly necessary for the safeguarding of the rights at stake (copyright and related rights), even if these measures are likely to represent a significant cost for them (based on the Article 8(3) D 2001/29/EC and L 336-2 of the Intellectual Property Code (France)).

With regard to the balance of rights, the Court found that such blocking orders do not prejudice their freedom to conduct a business, given that they are free to choose the technical measures to be taken to achieve this result. However, the financial stability of the rights holders and their associations would be in a worse position if they also had to bear the blocking costs, taking also into consideration that their rights are already at stake by the infringing websites. A fair balance should be ensured between the IP rights (Article 17(2) CFREU) at stake and the ISPs’ freedom to conduct a business (Article 16 CFREU). In light of **UPC Telekabel**, the fact that the cost of the measures is to be borne by the intermediary does not infringe the freedom to conduct a business provided that they can choose the technical measures to implement the blocking order. The case would be different if such measures required unbearable sacrifices, which is an issue that the ISP would have to prove.
The Court added that ISPs, as intermediaries, even if not responsible for the infringements in question, should also contribute to the safeguarding of copyright and neighbouring rights given that they are in the best position to actually stop these kinds of infringements.

Germany

REGIONAL COURT OF MUNICH I, CASE NO.: 7 O 17752/17, 1 FEBRUARY 2018, LEGAL DISPUTE FOR PRELIMINARY INJUNCTION, COPYRIGHT INFRINGEMENT ‘FACK JU GOHTE 3 VIA KINOX.TO

NORMS

Sec. 7(4) German Telemedia Act (TMG);
Sec. 8(1) German Telemedia Act (TMG).

FACTS

The applicant is a film distributor and purports to have ownership of the exploitation rights for the film ‘Fack Ju Göhte 3’, in particular the exclusive right of making available to the public from places and at times individually chosen by the user as per Sec. 19a German Copyright Act, including the exclusive right for Germany to retrieve the film free of charge via streaming and downloading, as well as the associated rights of reproduction. The respondent provides cable connections, and supplies millions of customers with internet connections.

The applicant seeks, by way of an injunction based on copyright law, that the respondent be ordered to block access to the website of the provider Kinox.to that is illegally offering a range of TV series and films, including ‘Fack Ju Göhte 3’. The website provides links to file hosting services, which enable streaming of the respective films. The content is stored on the servers of the file hosting services in such a way that users can, by clicking on the link, retrieve the stream for free at a time and from a place individually chosen by the user.

SUBSTANCE

In its reasoning, the Munich Court refers to the decision of the German Federal Court of Justice (BGH) of 26 November 2015, case no. I ZR 174/14 - Störerhaftung des Access-Providers and to Article 8(3) of Directive 2001/29/EC.

Since the respondent is not associated with Kinox.to in any way the Court ruled out a liability as perpetrator or accessory. However, as internet service provider the respondent did make an adequately causal contribution to the rights’ infringements committed via Kinox.to. Without the internet connection provided by the respondent, its users would not be able to access the service of Kinox.to. The respondent should be seen as a party in breach of a duty of care (Störer) because if it has been notified of a clear rights infringement it is, at the very least, subject to due diligence obligations as an internet service provider, provided that any monitoring obligations do not economically jeopardise its business model or disproportionately complicate its activities.

The Court recognised that the applicant first took reasonable actions against the perpetrators themselves. However, even though these actions per se were successful (one of the managing directors of the operational entity behind Kinox.to was arrested) the service continued unhindered and
the film ‘Fack Ju Göhte 3’ was still available on Kinox.to. In support of its claim against the internet service provider the applicant submitted evidence that in countries in which access to comparable sites has been blocked – also by foreign sister companies of the respondent – the number of illegal downloads has reduced considerably.

The Court found that the service Kinox.to is obviously aimed at distributing content obtained in violation of copyright, has a highly criminal nature and is not worthy of protection. To this extent the concern of over-blocking does not even come into question. The costs to be incurred by the respondent in order to install the necessary equipment to block access (DNS and IP) has been considered as being not disproportionally high by the Court. For the respondent, as the largest internet provider in Germany, the assessment of proportionality of the necessary measures only requires a slight effort. The Court considered its finding to be in line with the decision of the CJEU, *UPC Telekabel* (27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192). The respondent was given the choice of how it would specifically implement the prohibition.

The Court made it also explicitly clear that the operative provisions do not relate solely to the domain kinox.to but rather to the overall service Kinox.to, which is offered under that company name, irrespective of the respective domain. A limitation of the prohibition to the URL which can be seen in the submitted evidence (showing examples of website screenshots only) has therefore not been applied for nor has it been intended by the Court.

The Court prohibited the respondent, on penalty of a fine to be set for each act of non-compliance, of up to EUR 250 000, or alternatively imprisonment in the case of non-payment, or imprisonment of up to 6 months, or up to 2 years in the case of repeated offences, with the imprisonment or alternative imprisonment in the case of non-payment to be levied on the members of the board of the respondent, from providing their customers with internet access to the film ‘Fack Ju Göhte 3’, to the extent that this film is retrievable on the website service currently known as Kinox.to. The Court ordered also that the costs of the legal dispute were to be borne by the respondent.

**REGIONAL COURT OF MUNICH I, CASE NO 37 O 2516/18, 7 JUNE, 2019**

**NORMS**

Article 8(3) Directive 2001/29/EC;
Sec. 7(4) German Telemedia Act (TMG);
Sec. 8(1) and (2) German Telemedia Act (TMG);
Sec. 10(1), 19a, 85(2) German Copyright Act;
Article 14(1) of the German Constitution (Grundgesetz);
Article 16 and Article 17(2) of the Charter of Fundamental Rights of the European Union.

**FACTS**

The applicants are Germany’s largest record companies in terms of turnover and own the exclusive copyright on use of the titles of a list of CD-albums according to Article 85 of the German Copyright Act. The respondent is a well-known telecommunications undertaking. It operates a telephone network through which, on the one hand, it directly provides retail customers with digital subscriber line (DSL) internet access and, on the other hand, provides network access to other service providers. Through the internet access offered by the respondent, access is provided also to a third-party website
retrievable via different URLs that makes available to users the copyright-protected works of the applicants (CD-albums) without the latter's consent. The applicants seek that the respondent be ordered to block access to the said website for its users.

SUBSTANCE

The Court found that, first, the provision of Sec. 7(4) of the German TMG that refers explicitly to the liability of wireless internet operators does not exclude the blocking right against cable (wired) internet service providers. This understanding is in line with the provisions of Article 8(3) of Directive 2001/29/EU and Article 11 of Directive 2004/48/EU.

The Court considered further that Sec. 7(4) TMG serves, inter alia, the purpose of implementing the obligation of Member States laid down in Article 8(3) of Directive 2001/29/EC to ensure that rights holders can take legal action against intermediaries whose services are used by a third party to infringe copyright or related rights. Sec. 7(4) of the TMG must therefore be interpreted in conformity with the Directive as meaning that a telemedia service assisted an infringement of the law by allowing its customers access to infringing content on the internet that has been made publicly available by third parties. It is irrelevant whether the infringing content was uploaded via the respondent’s internet access or whether customers of the respondent actually accessed that content.

The applicants have no other means than recourse to the respondent to remedy the infringement of their rights. In that regard, it was for the applicants to show that they had taken reasonable steps to reveal the identity of the website operator. In particular, the involvement of the state investigative authorities by means of criminal charges or private investigations by, for example, a detective or other companies carrying out investigations into illegal offerings on the internet can be considered (Federal Court of Justice judgment of 26/11/2015 – I ZR 174/14 – paragraph 87, juris). The applicants satisfied those requirements by initiating state investigations and carrying out private inquiries, although they were unable to identify the operators of the websites.

The Court assessed the balance of fundamental rights and found that DNS blocking is a reasonable and proportionate measure within the meaning of Sec. 7(4), second sentence of the German TMG.

Finally, the Court made also assessed the effectiveness of the blocking measure to ensure effective protection of the applicant’s fundamental right to property by preventing, or at least hindering, unauthorised access to protected objects and by reliably deterring internet users from accessing them and found that DNS blocking is an effective measure. The danger of over-blocking has not been considered material since the legal content available on the website was estimated at below 4 % of the overall content.

The respondent was ordered to block the access of its users by means of DNS blocking to the internet service retrievable from certain URLs using certain IP addresses as long as explicitly listed album publications are accessible by means of file-sharing or share hosting via that service. The Court ordered the implementation costs of the blocking measures and the proceedings costs to be borne by the respondent.
Italy

COURT OF MILAN – ORDINANZA N. 42163/2019 R.G. OF 05 OCTOBER 2020, SKY ITALIA, LEGA SERIE A V CLOUDFLARE AND OTHERS

NORMS

Article 156 et seq. of the Italian Copyright Act;
Article 669bis et seq. of the Italian Civil Procedural Code;
Article 8(3) Directive 2001/29/EC.

FACTS

The TV platform Sky Italy and Italy’s top football league Lega Nazionale Professionisti Serie A filed a legal action before the Court of Milan against Cloudflare Inc. and other internet service providers. Both organisations requested a dynamic blocking injunction pursuant to Article 156 et seq. of Italian Copyright Act implementing Article 8(3) of Directive 2001/29/EC with the aim of combating the illegal distribution of audiovisual content.

SUBSTANCE

On 5/10/2020, the Court of Milan issued a dynamic blocking injunction ordering the blocking of current and future domain names and IP addresses of several IPTV services for the illegal distribution of audiovisual content. The Court confirmed the question already discussed in September 2019 inaudita altera parte. Major Italian ISPs such as TIM, Vodafone, Fastweb, Wind and Tiscali, alongside the hosting provider OVH and the content delivery network (CDN) operator Cloudflare Inc. were involved in the decision. The question as to whether Cloudflare Inc. could be found liable for hosting infringing content was specifically raised. However, the Court deemed it unnecessary to look at the potential liability regime of such a service under the Italian law implementing the e-commerce Directive provided that pursuant to Article 156 et seq. of the Italian Copyright Act (implementing Article 8(3) of Directive 2001/29), an injunction can be issued against intermediaries regardless of any liability of their own.

The defendant claimed that the Court had no jurisdiction in the case. It also argued that it was only providing a transitory data storage service and, as a consequence, it could not be found liable for hosting directly the infringing content.

The Court rejected the defendant’s arguments, ruling that its conduct ‘could facilitate, through the mere activity of the storage of static data, the third-parties copyright-infringing activity’. Furthermore, the Court ruled that all the defendants, with their activity of ‘intermediaries’, are in any case object of the dynamic injunction according to Article 156 et seq. Italian Copyright Act and Article 669bis et seq. c.p.c. The Court expressly stated that the classification between hosting providers, caching and ‘mere conduit’ services was irrelevant in the case, provided that the possibility to issue an injunction against an intermediary on the basis of Article 156 et seq. of Italian Copyright Act does not depend on the intermediary’s liability for the (alleged) infringement at stake.

(263) Not available via free online resources.

NORMS

Articles 14, 15, 16 d.lgs. n. 70/2003;
Recitals 45 and 47, Article 15 Directive 2000/31/EU;
Article 11 Directive 2004/48/EU;
Recitals 45 and 47 Directive 2001/29/EU.

FACTS

After having been granted an interim injunction in July 2017 (R.G. 9224/2017) concerning the website Dasolo, regardless of the top level domain, later that year, the rights holder (AM) discovered that the platform had once again changed name and through a new domain (italiashare.info) was still making links available for the download of unlawful copies of its magazines. AM requested the ISPs subject to the first injunction take the appropriate measures to block access to the new versions of the platform, but without success. The ISPs, in fact, claimed that AM’s request would be outside the scope of the injunction against them. Therefore, AM had to apply for a new injunction concerning the website italiashare.info, which it obtained inaudita altera parte on 14/11/2017.

The ISPs contested the legitimacy of the claimant's requests. In particular, the ISPs argued that they are 'mere conduit' providers and are not responsible for the unlawful activities of third-parties, and that the measures requested by AM would result in a general monitoring obligation, which is contrary to national and EU provisions. The court should also hear from the actual infringers in the context of such proceedings.

During the injunction hearing, AM requested that the ISPs be ordered to block access not just to the domain indicated in the application (which in the meantime had changed again to italiashare.life and then to italiashare.net), but also any domain names that would redirect to the platform.

SUBSTANCE

The Court rejected the need that, in proceedings against ISPs, the actual infringers should also be heard.

The Court noted that enforcement measures must be proportionate and not excessively costly. That being said, an ISP is under an obligation to promptly inform the relevant authorities should it become aware of any infringements committed by users of its service, and this is irrespective of any liability of the intermediary for the infringements themselves. In any case, intermediaries may be the addressees of injunctions against them.

The Court then noted that AM’s rights were repeatedly infringed through the different domain names under which the infringing platform operated. Furthermore, the Court, recalling the CJEU’s UPC Telekabel judgment (27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192), ruled that it is compatible with the e-commerce Directive to request an ISP to take the most appropriate measures to block access, not just to the domain names identified in the relevant injunction, but also to any further domain names under which infringements relating to the same rights are committed.
If the ISP’s obligation resulting from a certain injunction was limited to the domain names indicated therein, this would make the measure issued pointless: it is in fact likely that, at the time of issuing the injunction, the infringer is already operating under a different domain name.

However, to be compatible with the prohibition of general monitoring obligations, a dynamic injunction must include an obligation from the relevant rights holder to provide the targeted ISPs with a prior, specific notification concerning the new domain names through which infringements are committed.

The Court referred to the need to balance all interests at stake, namely diritto d’autore, free enterprise and the right to information.

The Court fixed penalty payments for non-compliance for the ISPs.

As regards the issue of cost allocation, the Court held that, since the measure requested was distinct from an assessment of any liability of the ISPs, by balancing different interests, the costs relating to technical expenses, being strictly necessary and concerning the measure requested by the rights holder, should be borne, provisionally, by the rights holder itself.

**Ireland**

**HIGH COURT OF IRELAND (COMMERCIAL), 2020 NO. 6450 P OF 29 SEPTEMBER 2020, UEFA V EIRCOM LIMITED T/A EIR ET AL.**

**NORMS**

Sections 17(1), 17(2), 37(1)(b), 40(1)(a) and 40(5A) of the Irish Copyright and Related Rights Act 2000 (2000 Act);

Article 8(3) Directive 2001/29/EC.

**FACTS**

The plaintiff (UEFA) is the governing body of association football in Europe. It organises a large number of well-known European-wide club competitions including the UEFA Champions League, the UEFA Europa League and the UEFA Super Cup. Among other IP rights, UEFA owns the rights to the transmission to viewers of the live match broadcast, the title sequences, logos protected by copyright as original artistic works, copyright on music recordings, notably the famous UEFA Champions League anthem, etc. The defendants are the five main retail ISPs in Ireland. UEFA seeks an injunction (live blocking) requiring the defendant ISPs to block access to the IP addresses of servers that are being used, or that it is supposed will be used, by non-parties for the purpose of making available to the public the copyright works of UEFA without its consent. The defendant ISPs are what are described as ‘mere conduits’ and it is not alleged that they have been guilty themselves of any copyright infringement whatsoever. Some of the defendants are neither supporting nor opposing the application and are adopting a neutral position. Others are supporting the orders sought by UEFA.

In many aspects the judgment is similar to the orders that have been made in the Courts of England and Wales in favour of this plaintiff (UEFA) and others in *Union Des Associations Européennes de Football v British Telecommunications plc & Ors* [2017] EWHC 3414 (Ch) (Arnold J.).
SUBSTANCE

The judge considers that the law regarding web blocking or live blocking orders or injunctions is well established and refers to previous case-law.

As to why orders are sought against streaming servers, the Court refers to the reasoning provided by Judge Arnold (High Court of England and Wales) in the Football Association Premier League Limited v British Telecommunications plc & Others [2017] EWHC 480 (Ch) (FAPL(UK)), namely: the streaming servers constitute the:

   crucial link in the chain by which an unauthorised copy of footage of a Premier League match is transmitted to the consumer. A single server may be accessed using a number of different user interfaces. For example, the same stream on the same server may be accessed via multiple apps, web sites and add-ons for set top boxes. If access to that server is blocked, all of those access mechanisms will be disrupted.

In summary, in order for the Court to grant a website-blocking order, the Court must be satisfied of the following:

1. the defendant ISPs’ services are being used to infringe copyright;
2. the proposed order will have the effect of preventing or terminating that infringement, or that it at least makes it more difficult or discourages it;
3. the proposed order will not impose ‘unbearable sacrifices’ on ISPs (to use the terminology used by the CJEU in UPC Telekabel (27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192)); and
4. the proposed order will not unnecessarily deprive internet users of the possibility of lawfully accessing content online.

The Court accepted that each of the defendants is a ‘mere conduit’ and as such they are not liable for any copyright infringement arising from the activities of their subscribers under Irish law implementing Directive 2000/31. An ISP (the defendants are ISPs) are subject only to the grant of the sui generis type of injunction sought by UEFA in this application. The act of infringement in question is the illegal streaming of UEFA competition matches in this jurisdiction by unauthorised third parties. The Court held that the unauthorised streaming of sporting events is a communication to the public.

Even if the defendants did not oppose the application, the Court performed an assessment (taking into account the evidence presented by the plaintiff) in order to establish whether the order sought is lawful and that it is appropriate for the Court to grant the injunction sought. In performing the assessment the Court applied the following test and considered whether the injunction is: (i) necessary; (ii) that the costs involved were not excessive or disproportionate and that the order itself should not be unduly complicated; (iii) that the cost-sharing proposals were fair and reasonable; (iv) that the order respected the fundamental rights of the parties affected, including internet users; and (v) that the duration of the proposed injunction and the provisions for review were reasonable. Based on the evidence submitted the Court answered all of the above questions in the affirmative.

In particular, the Court considered the order necessary for the purpose of protecting the plaintiff’s rights since it is seen as an effective method of targeting unauthorised streaming of live sporting events. The risk of ‘over-blocking’ is very low and the fundamental rights of the users are respected since they have the right to apply to the Court to discharge or vary the order. The duration of the order,
namely until the 31/07/2021, or the day after the last match period of the 2020/2021 UEFA competition season, whichever is later, has been considered sufficient and reasonable.

The Court concluded that the order sought is clearly appropriate. It will not impose any undue burden on the rights of internet users and will only impose a burden on the defendants which is appropriate and proportionate.

IRELAND, SONY MUSIC ENTERTAINMENT (IRELAND) LIMITED & ORS -V- UPC COMMUNICATIONS IRELAND LIMITED [2015] IEHC 317

NORMS

Articles 1 and 3 Directive 2002/21/EC;
Articles 12 and 15 Directive 2000/31/EC;
Recitals 11 and 12, Articles 1(1) and 8 Directive 2001/29/EC;
Regulation 2 of S.I. 59 (amends the Copyright and Related Rights Act 2000 by inserting a new subsection 40 (5A));
Section 37 Copyright and Related Rights Act 2000.

FACTS

The plaintiffs are all record companies. They are owners of copyright and have exclusive licences of sound recordings, which are a subject of daily illegal download and upload. The illegal actions are made on the internet. UPC (the defendant) is an internet service provider in Ireland. UPC’s subscribers are also involved in the piracy of the rights holders’ music.

The record companies first wrote a letter to UPC informing it about the infringing actions its subscribers were doing using its service. In the letter they proposed a graduated response strategy (GRS) that the ISP could voluntarily implement to prevent such actions. UPC declined any voluntary actions towards customers without a court order. UPC opposed these actions because it was of the opinion that an injunction is not an appropriate response to internet piracy, but rather requires a legislative response.

The record companies requested an injunction in court. Their primary request consisted of a GRS in which UPC must send cease and desist letters to its subscribers, threaten them with a suspension of services, suspend them after the third notification for a week and after a fourth notification terminate their contract. At the end the court granted an injunction for the GRS, but without the 1 week service suspension and with some adjustments.

SUBSTANCE

The Court was not deciding on whether the infringements occurred, the scale of the illegal actions or whether the defendant’s service is used for such actions. All these facts were agreed on by both parties. Facts about internet piracy were also used from a previous case – EMI Records (Ireland) Ltd. and Others v Eircom.

In summarising all the legislative obligations, the Court acknowledged that an injunction would need to follow the criteria stated below:

1. any injunction should be fair and equitable;
2. any injunction should not be unnecessarily complicated or costly;
3. any injunction should not entail unreasonable time limits or unwarranted delays;
4. any injunction should be effective, proportionate and dissuasive;
5. any injunction should be applied in a manner that avoids the creation of barriers to legitimate trade;
6. any injunction should provide for safeguards against its abuse;
7. any injunction granted should respect the fundamental rights of a subscriber;
8. any injunction granted should ensure that there is a prior, fair and impartial procedure which includes the right to be heard of the person concerned;
9. any injunction granted should ensure that there is a right of effective and timely judicial review of such an injunction.

There was no real dispute between the parties about criteria 5, 6, 7 and 9 above.

The problem with criterion 2 was that a computer system would need to be developed. The new technology would be needed to process information given by the plaintiffs and finding the accounts connected to it. They estimated approximately 5,000 notifications per month. The ‘low-tech’ possibility would be very expensive, as a large administrative burden would be placed on the defendant. A ‘high-tech’ solution of an automated process would be much better in the long run. The defendant’s views were taken into account in this deliberation. The Court decided that even though the new system would be costly and complicated, it would not be unnecessarily so.

On the issue of whether the remedies would be effective, proportionate and dissuasive if the Court decided that the writing of letters do meet the criteria, evidence from the Eircom protocol (the plaintiffs’ experience from the previous injunction) confirmed the Court’s decision.

The Court analysed the problem with prior, impartial procedure, and specifically the right to be heard by the person concerned. The correspondence regarding suspension/termination would be done by a person within the defendant’s company and would not qualify as a third party, impartial person. Here the plaintiffs proposed and both parties agreed to appoint an impartial arbitrator (for example a retired judge) that would consider all suspension/termination applications. In a second judgment ([2015] IEHC 386, 21/05/2015) the judge explained that it would not be appropriate for the court to order a reluctant defendant to take part in a quasi-judicial procedure. It decided that it is simpler that it moves directly to a Norwich Pharmacal order. A Norwich Pharmacal order is an order of the court that the defendant disclose to the plaintiffs the names and addresses of its subscribers in respect of whom there is a prima facie demonstration of wrongful activity. This procedure arises in circumstances where parties are aware that other parties are engaged in wrongful activity. The plaintiffs would make such an application, receive the subscribers’ identity and seek an order for the termination of their contract.

THE HIGH COURT OF IRELAND (COMMERCIAL), EMI RECORDS (IRELAND) LIMITED & ORS V. UPC COMMUNICATIONS IRELAND (LIMITED) & ORS, [2013] IEHC 274

NORMS

Section 40(5A) of the Copyright and Related Rights Act 2000;
S.I. No. 59 of 2012, the European Union (Copyright and Related Rights) Regulations 2012 which inserted s. 40(5A) into the Copyright and Related Rights Act 2000 (2000 Act). Section 40(5A) and Section 205.
FACTS

The rights holders are recording companies who record and release music and video for sale. They applied for an injunction requiring the defendants (internet service providers) to block or otherwise disable access by their subscribers to the website known as The Pirate Bay, and related domain names, IP addresses and URLs, together with such other domain names, IP addresses and URLs related to the main names as may be reasonably notified by the plaintiffs to the defendants from time to time.

The parties after discussions agreed on a draft order which was analysed and accepted by the Court. Three main issues were especially considered: (i) the appropriateness of the order; (ii) whether new applications will have to be made to the Court in case The Pirate Bay website changes its location; and (iii) the costs of proceedings.

SUBSTANCE

As regards the factual background and the legal principles to be applied the present judgment refers to the judgment of Charleton J. delivered on 11 October 2010, in EMI Records (Ireland) Ltd. & Ors. v UPC Communications Ireland Ltd. [2010] IEHC 377.

The judgment confirms that the plaintiffs are entitled to a blocking injunction in accordance with the terms of the draft order and protocol (not available publicly) submitted to the court. The costs associated with implementing the order should be borne by each of the defendants.

The judgment finds it proportionate and reasonable that new applications would not be required to be made to the Court if The Pirate Bay website changes its location on the internet, as detailed in the draft order and protocol.

As regards the costs, the Court rules that the defendants – except the second defendant – will bear their own costs, reasoning that although none of them are wrongdoers, the infringement has caused (and continues to cause) substantial financial damage to the plaintiffs. As regards the second defendant, the plaintiffs agreed to pay the costs on the basis that it did not actively participate in the proceedings.


NORMS

Section 37 of the Copyright and Related Rights Act 2000;
Section 40 of the Copyright and Related Rights Act 2000;

Data protection acts, 1988-2003:
s.1 Data protection act 1988 and section 2, 2A, 2B, 2C and 2D of the Data protection act 1988, as amended.

FACTS

The plaintiffs are record companies and owners of copyright (not just music). Copyright infringement is taking place on the internet. The illegal downloading and uploading of copyrighted music (and other
copyrighted creations) is performed by subscribers using the defendant’s internet service. The plaintiffs sued the defendant, but stopped the process to try to reach a settlement. The settlement was presented in the judgment of 2010.

**SUBSTANCE**

In the judgment the Court does not analyse or discuss in length the questions of whether infringements are taking place, how they are being carried out or what kind of injunction it will grant. The parties after a first attempt in court reached a settlement in which they agreed on the Protocol they will use. The only issues the Court does go into are issues connected to privacy and data protection.

The Court found three possible issues with the implementation of the injunction. First, it looked into the question of whether the information/data collected in such a procedure would be personal data. The Court’s opinion is that neither of the plaintiffs have any interest in identifying any living person infringing copyright or requesting it from the defendant. The second issue addressed was the processing of data, and more specifically if such processing represents “unwarranted [processing] by reasons of prejudice to the fundamental rights and freedoms or legitimate interests of the data subjects”. The Court viewed the processing as necessary for both the performance of the contract and for compliance with a legal obligation cast upon the courts. There cannot be a constitutional right to privacy that extended to the organisation of crime. The Court determined that there is nothing disproportionate and therefore the actions were not unwarranted. The third issue the Court analysed was the fact that two private entities would process data and then communicate the decision to terminate a user’s internet service. All parties involved are not interested in the detection or prosecution of criminal offences. In conclusion, the Court agreed that the graduated response is lawful and that the settlement can be implemented.

**Netherlands**

**AMSTERDAM COURT OF APPEAL, CASE NUMBER 200.243.005/01, 2 JUNE 2020, ZIGGO B.V. AND XS4ALL INTERNET B.V. v. STICHTING BREIN [BREIN FOUNDATION]**

**NORMS**

Article 26d of the Dutch Copyright Act; Article 15 of the Dutch Neighbouring Rights Act.

**FACTS**

Brein is a Dutch foundation defending the interests of affiliated rights holders related to music and film works, as well as computer games. Ziggo and XS4ALL are internet access providers. Subscribers of the latter two companies made use of The Pirate Bay (TPB) – a BitTorrent index offering material protected by copyright and/or related rights. The TPB administrators and users have (usually) no authorisation to carry out the reserved actions. Therefore, TPB and its users are held by judgments in previous instances to be infringing copyright. Brein requested an injunction that would make it impossible for subscribers of Ziggo and XS4ALL to access web addresses that directed internet traffic to TPB by blocking the IP addresses and (sub)domain names through which TPB operates and the (sub)domain names through which TPB can be reached for their subscribers, on pain of forfeiture of penalty payments.
SUBSTANCE

The Amsterdam Court of Appeal referred to the UPC Telekabel judgment recalling in detail the findings of the CJEU. Based on the review of the judgment the Amsterdam Court of Appeal had to assess whether the orders claimed by Brein are compatible with the fair balance that, pursuant to the Charter of the European Union, it is necessary to strive for between the three relevant fundamental rights in case (i.e. (intellectual) property, freedom of information and freedom of entrepreneurship). The Amsterdam Court of Appeal had to assess also whether the order requested by Brein is compatible with this fair balance between the fundamental rights concerned since the order was different from the one at issue in the main proceedings of UPC Telekabel.

In performing these assessments the Amsterdam Court of Appeal came to the conclusions that: (i) since the content on TPB is predominantly if not exclusively illegal (90% to 95%), the denial of access to lawfully available information that results for the subscribers from the blocking of the website is proportionate to the extent and seriousness of the copyright infringement committed on TPB website; (ii) the claimed blocking under the circumstances of the case has a sufficient effect in preventing or at least complicating unauthorised access to protected works and that users who avail themselves of the services of Ziggo and XS4ALL are seriously discouraged from gaining access to those works; (iii) the order claimed does not demand unbearable sacrifices from Ziggo and XS4ALL, cannot be deemed as unreasonable, and can be regarded as a relatively minor encroachment on the freedom of entrepreneurship of Ziggo and XS4ALL. Based on the foregoing considerations the Amsterdam Court of Appeal found that the blocking claimed by Brein is compatible with the fair balance between the fundamental rights of (intellectual) property, the freedom of information and the freedom of entrepreneurship.

In addressing Ziggo and XS4ALL’s arguments the Amsterdam Court of Appeal found also that the claimed blocking does not infringe the general monitoring prohibition laid down in Article 15(1) of the Directive 2000/31 EC, does not violate the principle of net neutrality that the internet service providers must observe and is not contrary to the legal protection of personal data. Most importantly the Amsterdam Court of Appeal explicitly noted that the dynamic aspect of the claimed blocking contributes significantly to its effectiveness.

The Amsterdam Court of Appeal ordered Ziggo and XS4ALL to cease and desist their services used to infringe copyright and related rights of rights holders whose interests are defended by Brein, within 10 (ten) working days, by blocking and keeping blocked access by their clients to specific and clearly identified domain names/(sub)domain names and IP addresses through which TPB operates as well as other (sub)domain names indicated in a list submitted to the court by Brein and attached to the judgment as long as TPB operates through these (sub)domain names and IP addresses. The Amsterdam Court of Appeal ordered Ziggo and XS4ALL also, in the event that TPB starts to operate via other/additional IP addresses and/or (sub)domain names than those aforementioned, to block and keep blocked access by their customers to these other/additional IP addresses and/or (sub)domain names, within 10 (ten) working days of the notification of the correct IP addresses and/or (sub)domain names by Brein by fax, registered letter or email to Ziggo and XS4ALL separately. Failure to comply with the above orders triggers the payment of fines and penalties.

NORMS

Article 26d of the Dutch Copyright Act;
Article 8(3) Directive 2001/29/EC;
Articles 11, 16, 17(2) of the Charter of Fundamental Rights of the European Union.

FACTS

FAPL is the organiser of the Premier League competition of English professional football. The matches, which are broadcast on licensed television channels, are available in the Netherlands via a paid subscription. Ecatel is an internet service provider that also rents out dedicated servers.

In 2014, FAPL requested an immediate injunction against Ecatel for hosting illegal streaming platforms that infringed the plaintiff’s copyright. The court ordered the defendant to cease and desist the services used by the streaming platforms. The defendant had the order revised in the following summary proceedings and the plaintiff filed an appeal.

In the present case, the plaintiff requests an order against the defendant to cease and desist any service used by third parties to infringe its copyright and trade mark rights by stopping and holding the service concerned within 30 minutes of the receipt of an electronic notification by FAPL, permanently or only during the broadcast, subject to an immediately payable penalty for non-compliance. It also asked for compensation for previous infringements and for damages.

SUBSTANCE

The Court analysed the creative choices made during a broadcast of a football match and found that the broadcasts are considered works that are entitled to copyright protection. It also mentioned that the fixation requirement cannot be applied because, naturally, the recording of the broadcast takes place during the actual creation of such a work.

Ecatel can be considered an intermediary, according to Article 26d of the Dutch Copyright Act, as its servers are used both as origin nodes and edge nodes of the illegal streams. The Court, citing the CJEU UPC Telekabel case (27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192), stated that Article 8(3) of Directive 2001/29/EC does not require a contractual relationship between the copyright infringer and the intermediary. Furthermore, Ecatel is a host provider for streaming websites.

The Court assessed the conflict between FAPL’s copyright, Ecatel’s freedom of entrepreneurship and the internet users’ freedom of information (Articles 17(2), 16 and 11 of the Charter of Fundamental Rights of the EU respectively) and found that the requested order does not prejudice the defendant’s freedom of entrepreneurship, because ‘null routing’ of the server is relatively simple, involves little cost and will have to be done only after prior notification by the plaintiff and only for the limited duration of each football match.

With regard to proportionality, the defendant’s claim that legal content will also be blocked by ‘null routing’ was rejected, because, if it applied a notice-and-takedown policy to stop infringements, this would simplify the procedure and ensure access to legal material for the users. The users’ right to information was not found to be prejudiced, as the blocking of the illegal streams might affect access
to legal content only during the broadcasts in question and only if the stream has not already been blocked in any other way.

As for the effectiveness criterion, the court cited again the *UPC Telekabel* judgment, according to which, measures are effective if they can prevent or delay unauthorised access to copyrighted works and they seriously discourage users from accessing them; therefore, if Ecatel blocks the streams in question, it will become more complicated for users to access them via other sources.

The measure also complies with the principle of subsidiarity, as most providers of streaming platforms cannot be easily identified and brought to justice because of their remote locations and the rapid change of server addresses. Added to this are the technical difficulties to trace the ‘origin node’ of each stream.

Finally, the Court ordered Ecatel to cease and desist any service used by third parties to infringe FAPL’s copyright within 30 minutes of the receipt of an electronic notification from FAPL that has identified an illegal stream and during the broadcast game, subject to an immediately payable penalty for each illegal stream.

**RECHTBank Midden Nederland C/16/448423/ KG ZA 17-382, 12 January 2018 (Stichting Brein v. KPN B.V. and Others) ECLI:NL:RBMNE:2018:114**

**NORMS**

Article 26d of the Dutch Copyright Act (Auteurswet);
Article 8(3) Directive 2001/29/EC.

**FACTS**

The plaintiff, Stichting Brein, is the Association for the Protection of the Rights of the Entertainment Industry of the Netherlands. The defendants, KPN, T-Mobile, Tele2, Zeelandnet and CAIW, are internet service providers, operating within the territory of the Netherlands. The Pirate Bay is a BitTorrent index website that allows its users to illegally gain access to material that is protected by copyright. The plaintiff requested that the Court orders the ISPs in question to block access by their customers to all (sub)domain names and IP addresses of The Pirate Bay, as well as to all its future or additional (sub)domain names and IP addresses within three working days after the plaintiff’s notification. Alternatively, to impose any measure the Court deemed appropriate against the ISPs in order to prevent their users from having access to the website.

**SUBSTANCE**

The Court mainly assessed whether the blocking injunction that the plaintiff requested complied with the principles of proportionality and effectiveness, taking also into account the defendants customers’ right to freedom of information (Article 10 ECHR).

With regard to the effectiveness, the Court mentioned the ‘Alexa list’ which contains information about websites and lists them from most to least visited. When blocking injunctions were issued against The Pirate Bay in the past, it went down on the list, whereas, when these injunctions were lifted, it went
back up again. Therefore, the Court confirmed that the blocking of the website is actually an effective measure.

Furthermore, the Court referred to the Ziggo v Brein case in which the ISP XS4ALL blocked all requested addresses in one working day. It also held that, since Brein has created a tool to monitor that the IP addresses and domain names are still accurate, there is no risk that the users will lose access to legal content. Therefore, the measure is also in line with the principle of proportionality.

The users’ right to freedom of information is still protected according to the Court, since there is only a small amount of legal files on the website compared to the illegally shared ones. In any case, the legal content can be accessed by the users on other legal websites, and, as a consequence, the right to freedom of information can still be exercised.

Finally, and bearing in mind what has been mentioned above, the Court concluded that the balance of interests is in favour of Brein and ordered the ISPs to cease and desist their services, which are used to infringe copyright and related rights, by blocking access to the domain names, subdomains and IP addresses of The Pirate Bay. Additionally, it ordered the defendants to block and keep their customers’ access to other or additional IP addresses and/or (sub)domain names blocked, within three working days of a notification by Brein.

Spain


NORMS

Article 21.1 of the Spanish Ley de Enjuiciamiento Civil (LEC);
Article 395 LEC;
Article 394(1) LEC;
Articles 455 and following LEC.

FACTS

In November 2019, TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. (broadcaster) sued the main Spanish internet access providers for not taking measures to stop access to websites offering unlicensed distribution of live football matches through illicit Internet Protocol Television (IPTV) services. The defendants acquiesced to all the claims and measures asked by the applicant.

SUBSTANCE

In this judgment, the defendants gave their acquiescence to the applicant’s arguments and claims. According to Spanish law, in such cases the Court issues an order without entering into the merits of the case, unless the claim was done in bad faith, goes against the public order or prejudices the rights of third parties. In this particular case, the Court did not enter into the merits of the case and, therefore, did not analyse the legal framework applicable to dynamic blocking injunctions.
The judge upheld the claim and ordered the defendants to take several actions to cease the unlawful activities identified. The costs had to be borne by the defendants, since they gave their acquiescence in the response to the claim (in such cases the defendants are obliged by law to bear the costs).

The blocking injunctions imposed by the Court are twofold:

(i) **Static blocking injunctions:**

- the sued ISPs had to block, within 72 hours of the notification of the judgment, the URLs, domain names and IP addresses from 44 pirate sites and services;
- the ISPs should block at the level of both HTTP and HTTPS protocols, and were expected to take any access prevention action they could;
- the injunction is limited to 3 years, covering three football seasons 2019-2022;
- ISPs will have to report back to Telefónica Audiovisual Digital and notify the exact time when they blocked access to newly added web resources.

(ii) **Dynamic blocking injunctions:**

- the authorised broadcaster will update weekly the blocking list with new entries (sites, IP addresses, URLs) related to the 44 pirates sites mentioned in the judgment and send it directly and simultaneously to the ISPs without a new court order;
- ISPs will be given 3 hours to respond to new entries;
- the dynamic injunction lasts until 25 May 2022.

The judgment is now final (no appeal against the judgment in the 20 days after the judgment was notified).

**DECISION NO. 15/2018 OF THE COMMERCIAL COURT NO. 6 OF BARCELONA, 12 JANUARY 2017 (HDFULL CASE):**

**NORMS**

Articles 138(3) and 139(1)(h) Spanish Copyright Act (SCA);
Article 10 Spanish Law 34/2002 on Services of the Information Society and Electronic Commerce;
Article 8(3) Directive 2001/29/EC;
Articles 9(1) and 11 Directive 2004/48/EC.

**FACTS**

On 12 January 2017, Barcelona’s Commercial Court nº 6 (Juzgado de lo Mercantil nº 6 de Barcelona) ruled on copyright infringement in the context of a dispute between COLUMBIA PICTURES INDUSTRIES INC and others (plaintiffs) and the local ISPs TELEFÓNICA ESPAÑA, VODAFONE ESPAÑA, ORANGE ESPAGNE and XFERA MOVILES (defendants) because protected works were being made available to users without the authorisation of the rights holders.

The plaintiff requested local ISPs to block or prevent the access of their users to the pages HDFull.tv and Repelis.tv. These pages were infringing the right of communication to the public regulated in the Revised Text of the Law on Intellectual Property, by making protected works available to users without the authorisation of the rights holders.
SUBSTANCE

In the judgment, the judge upheld the claims and declared the plaintiffs to be ‘the exclusive holders and assignees of the rights of reproduction, distribution and public communication of the protected works listed in the appeal’.

On the proportionality of the measures claimed by the plaintiffs, the Court considered that the refusal of access to a website on which infringing material is made available by internet service providers to their customers seems proportionate since its purpose is to prevent access to infringing websites whose owners could not be identified or located.

The ruling orders the operators, by virtue of Articles 138(3) and 139(1)(h) of the Spanish Copyright Act, to block the access of their users from Spanish territory to the pages HDFull and Repelis. Along with blocking access to the website, operators must also block the proxies that allow access to the content, to prevent access to other domains and IP addresses whose purpose is to facilitate the circumvention of technological protection measures (TPMs) and thereby allow access to users.

The defendants must inform the Court and the plaintiffs immediately of the technical measures and steps taken to implement the judgment and they must bear any costs arising as a direct consequence of the technical implementation of the blocking measures ordered.

Sweden

SVENSKA PATENT- OCH MARKNARDSDOMSTOLEN (SWEDISH PATENT AND MARKET COURT), CASE NO PMT 7262-18 [9 DECEMBER 2019]

NORMS

Article 53b of the Swedish Copyright Act;
Article 3(3) Directive 2001/29/EC;
Article 8(3) Directive 2001/29/EC.

FACTS

AB Svensk Filminustri and others (the rights holders) are companies operating in the film industry. Telia Sverige AB (Telia) is an internet service provider. Telia’s customers have been able to access the services of The Pirate Bay, Nyafilmer and Fmovies, where protected material was made available. Most of the content available through these services were copyrighted. The rights holders brought an action against Telia, demanding that they be required to block access for their customers to services that contribute to the infringement.

SUBSTANCE

The Court cited CJEU case-law (27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192), according to which an internet service provider is considered to be an intermediary in the meaning of Article 8(3) of the InfoSoc Directive. The CJEU has further stated in 07/07/2016, C-494/15, Tommy Hilfiger, EU:C:2016:528, that Member States should ensure that intermediaries, whose services are used by third parties to infringe IP rights, regardless of the intermediary’s own liability, may be obliged to take
actions to prevent these infringements, and new similar infringements. The Court stated that Telia is an internet provider in the meaning of the InfoSoc Directive. The Court found that there has been infringement in an objective sense, and that Telia therefore has joint responsibility.

The Court considered the proportionality of the prohibition given under Article 53b by taking into account the interests of the rights holders, Telia’s freedom of trade and the internet users’ freedom of information. The Court assessed the risk of over-blocking access to domain names. The Court pointed out that it is clear from the present case that the services at issue in this case changed their domain names and/or used proxy services to circumvent any blocking measure. The rights holders had revised their list of domain names several times during the written proceedings. The Court stated that it would be unreasonable to find a prohibition under the threat of a fine disproportional because there is a possibility of changing domain names so that after the change, some of the domain names and URLs would no longer lead to the services. The Court also stated that the injunction is not an open injunction but an injunction that specifies the access of four services defined in the judgment to be prevented by technical blocking measures. Furthermore, it is time-limited, and a new Court examination can take place if necessary.

The Court assessed the appropriateness and effectiveness of the measures. The Court pointed out that it is not a legal requirement for a prohibition under the threat of a fine that the measure should stop the infringement. It is enough that the measure makes it more difficult to access the protected material. The Court stated that a requirement for Telia to block, in addition to the domain names used for the infringing activity, services that may arise in the future through domain names and URLs ensures that the measure is appropriate and effective to achieve the desired purpose. Therefore, an injunction should not merely be aimed at certain specific domain names and URLs but also be aimed at the services. Telia is not required to take any other blocking measures than technical blocking of customers’ access to domain names and URLs that lead to the services or to have constant and total monitoring over the internet. The company may be reasonably required to act in the event of becoming aware that the services are available through certain domain names or URLs, such as being informed from time to time by the rights holders. The Court assessed that if such activity falls within the prohibition, it may be reasonable to require prompt action to take adequate blocking measures, which should be expected to take place within 2 to 3 weeks of the date of the notification.

The Court found that the legislation does not impose any requirement that the rights holders should first turn to the direct infringer and not the internet provider. The Court considered that the investigations into the case show that it is very difficult to contact the persons behind the services and even harder to stop the infringement activity through such contacts. In the Court’s view, it is not necessary for the rights holders to first turn to those behind the services in order to consider the measure proportionate. The Court considered the measure defined in the judgment as proportionate in balancing all conflicting interests.

The Swedish Patent and Market Court prohibited Telia from making the protected material set out in the judgment available to the public. To comply with the prohibition, Telia is required to prevent access, by technical blocking measures, to The Pirate Bay, Nyafilmer and Fmovies services via domain names and URLs listed in the judgment. Telia is also required to take reasonable steps to block access to these specified services through other domain names and URLs than those specified in the judgment. The prohibition is given under the threat of a SEK 500 000 fine over a period of 3 years.

Telia has appealed before the Swedish Patent and Market Court of Appeal.
SWEDISH PATENT AND MARKET COURT OF APPEAL – CASE PMT 13399-19 TELIA SVERIGE AB V SVENSK FILMINDUSTRI AND OTHERS (29 JUNE 2020)

NORMS

Article 53 b (first sentence) of the Swedish Copyright Act;
Article 8(3) Directive 2001/29/EC.

FACTS

The rights holders (AB Svensk Filmindustri and others) are companies operating in the film industry. Telia Sverige AB (Telia) is an internet service provider. Telia’s customers had been able to access the services of The Pirate Bay, Nyafilmer, Fmovies and several other related proxies and mirror sites, where protected material was made available.

In 2018, upon a request of the rights holders the Swedish Patent and Market Court ordered Telia (by way of an interim ruling) to block access to a number of infringing websites by imposing a dynamic blocking injunction (a summary of the case is provided below). Telia appealed the ruling before the Swedish Patent and Market Court of Appeal.

SUBSTANCE

The Swedish Patent and Market Court of Appeal (Patent och Marknadsöverdomstolen) upheld the ruling and confirmed the dynamic blocking injunction ordered by the previous instance and agreed that Telia, as an internet provider, had contributed in copyright infringement by providing internet connection to its subscribers, who thereby had access to certain cinematographic works that had been unlawfully made available through certain online services.

After balancing the interests of the parties, the Court of Appeal confirmed the earlier instance’s conclusions, but it deemed it necessary to clarify the arrangement and form of the dynamic blocking injunction in such a way as to target the services of The Pirate Bay, Nyafilmer, Fmovies and Dreamfilm in their entirety. The Court of Appeal stated that it was not necessary to identify the persons administering the services or to describe the services in question. Instead, it was essential to clearly describe the characteristics, structure and operation of the services. Furthermore, the Court clarified that domain names and URL’s related to search engines such as Google and Yahoo do not fall under the scope of the injunction, nor should it cover the situations where links to the services are included in posts on Facebook or Twitter.

Therefore, the Court stated, contrary to what has been decided in the previous instance, that it would not be appropriate or proportionate to require Telia to also monitor new domain names and URL’s that infringe the rights holder’s copyrights. Instead, the rights holders should notify Telia of specific domain names and URL’s that Telia should block and Telia was given a 3 week timeframe in which to implement the necessary measures. The Court confirmed the injunction to be in force for 3 years in order to be efficient.
United Kingdom


NORMS


FACTS

The plaintiff (Matchroom) runs boxing events. The respondents are the biggest internet service providers in the United Kingdom. Matchroom seeks a website-blocking injunction to prevent access to certain IP addresses that are being used to infringe their copyright relating to live streams of the events. A website-blocking injunction had already been granted to Matchroom in September 2018, extended and varied in May 2019 and ceased to have effect on 1 October 2020. The plaintiff requested an extension of the said order, but the Court treated the filing as a new application for a website-blocking injunction.

The applicant submitted that it would be appropriate for the Court to make the order sought on the basis of the reasons held by the Court to justify the making of the orders in FAPL v British Telecommunications plc [No 1] and FAPL v British Telecommunications plc [No 2] [2017] EWHC 1877 (Ch). One of the respondents supported the application, the rest did not oppose it.

SUBSTANCE

According to the witness statements provided by the applicant and one of the respondents the dynamic blocking orders ‘had significant positive impact in reducing in UK consumers’ access to infringing live streams of Matchroom boxing events’, that ‘blocking has worked smoothly in practice’ and that over-blocking is not a concern.

The applicant requested that certain parts of the order are kept confidential. The reason was that all of its information (list of targeted IP addresses, detection conditions and requirements which an IP address must satisfy in order for it to be notified that it will be blocked) would, if publicly available, undermine the purpose of the order itself. That is because it would help those seeking to circumvent the website-blocking system to avoid it in various ways. The Court agreed that the applicant and the broadcasters have a clear interest in maintaining the confidentiality of the arrangements. The opposite bears a tangible risk of undermining the blocking and assisting the infringers. However, the Court decided that other applicants for related website-blocking orders should be able to have access to the order in its entirety in order to be able to take advantage of the information contained therein (the scope, the IP addresses, the ways they will be blocked, etc.).

The Court ordered the disabling of access to each of the IP addresses for the target servers as defined in a confidential schedule notified by the applicant to the respondents. The blocked access should be unblocked as soon as reasonably practicable after the expiry of the event.

The Court set out in detail also the rules for giving notifications to the applicant, the time for compliance, the duration of the order and the possibility for the applicant to apply for extensions of the
operation, the notifications to third parties, the suspension of blocking measures, permission to apply on notice to vary or discharge the order insofar as it affects particular persons (not only limited to the respondents but also third parties such as users) and confidentiality.

The order contains five schedules in total. Schedule 1 includes a list of Matchroom events to be blocked. The schedule is subject to variations, in particular as far as additions of events are concerned which are to be notified from time to time to the respondents according to the rules set out in the order. Schedule 2 contains a list of target servers (not disclosed to the public) and is subject to any changes (additions or removals) from time to time which are notified to the respondents according to the rules set out in the order. Schedule 3 contains the detection and notification criteria which are also omitted from the public version of the order. Schedule 4 contains the technical means of blocking. Schedule 5 is a list specifying what is considered confidential material.


NORMS


FACTS

The claimant (FAPL) is the governing body of the football competition known as the Premier League. FAPL owns the copyright in films comprising television footage of all Premier League matches, and in artistic works that appear within that footage. The defendants are the six main retail ISPs in the United Kingdom. It is worth mentioning that the defendants are not merely ISPs. Some of them have an interest in the subject matter of FAPL’s rights (exclusive licensees of broadcasting and internet transmission rights for Premier League footage in the UK). The FAPL seeks an injunction against the defendants requiring them to take measures to block, or at least impede, access by their customers to streaming servers which deliver infringing live streams of Premier League footage to UK consumers.

In some respects the application is similar to one by FAPL that led to a blocking order being made for a website, known as FirstRow Sports, for the reasons given in Football Association Premier League Ltd v British Sky Broadcasting Ltd [2013] EWHC 2058 (Ch), [2013] ECDR 14 (FAPL v Sky). The current application differs in a number of respects, however, and in particular in that it is directed at streaming servers rather than a website.

SUBSTANCE

In view of the facts and aims described above (blocking infringing IP addresses and live stream servers), the FAPL sets out a list of IP addresses of servers that the defendants are required by the order to block access to or attempt to block in the first instance. In addition, FAPL identified a subset of infringing streaming servers, which should also be blocked.
In order to try to achieve the request of the defendants, an order is granted taking into account four fundamental aspects.

1. The order is a live blocking order which only has effect at the times when live Premier League match footage is being broadcast.
2. The order provides for the list of target servers to be reset each match week during the Premier League season. This allows for new servers to be identified by FAPL and notified to the defendants for blocking each week, and ensures that old servers are not blocked after the end of a week unless they continue to be observed as sources of infringing footage.
3. The order is limited in time. It will only last until the end of the 2016/2017 Premier League season. The intention is to assess its effectiveness and any other issues encountered. FAPL would be then able to apply for a similar order to cover the 2017/2018 season, with any changes that may seem appropriate in the light of the previous season’s experience.
4. The order requires a notice to be sent to each hosting provider each week when one of its IP addresses is subject to blocking. The hosting providers and the operator of any website or streaming service claiming to be affected by the order are given permission to apply to set aside or vary the order as well as the operators of the target servers and any customer of the defendants who claims to be adversely affected by the order.

In exercising its discretion as to whether to issue an order or not, the Court assessed the proportionality of the order having regard to the competing rights of those affected by it.

While the defendants contend that this order may affect their freedom to conduct their business, as well as the freedom of internet users to share or receive information, the FAPL maintains that the order will be effective and dissuasive in that it will substantially reduce copyright infringements. Moreover, FAPL contends that the available alternative measures are either ineffective or incomplete in addressing this problem.

The Court considered that the order is not unnecessarily complicated or costly and that it avoids creating barriers to legitimate trade. The safeguards against misuse contained in the order are correctly tailored, bearing in mind in particular the short duration of the order.

Overall, there is proportionality between the rights of the applicant and the defendants, as it does not prejudice the rights of the latter to conduct their business and protects the copyright of the plaintiff.

ENGLAND AND WALES HIGH COURT (CHANCERY DIVISION), IL-2018-000155 OF 20 SEPTEMBER 2018, MATCHROOM BOXING LIMITED AND MATCHROOM SPORT LIMITED V BRITISH TELECOMMUNICATIONS PLC ET AL.

NORMS


FACTS

Matchroom (the claimants) is the holder of the copyright in live streams of footage of professional boxing matches. One of the defendants, SKY UK LIMITED, is broadcasting the events organised by Matchroom and pays Matchroom a substantial fee for the broadcasting. Matchroom requested an injunctive order, addressing access providers, of blocking the streaming of such live events in infringement of its rights.
SUBSTANCE

According to the judge, the case presented similarities with the previous case-law [2017] EWHC FAPL v BT I 2017 (Ch) (See above), in both the type of order requested and the reasons justifying the decision. The judge specified however that in the case at issue, it was not possible to identify the servers hosting the broadcast content in infringement of the applicant’s copyright in the same way as had been done in the previous case, due to the irregular timing of the events. The judge acknowledged that the monitoring techniques applied to prevent the infringing acts were different. The judge kept the details confidential, in order to prevent circumvention, and stated the presence of evidence demonstrating that there was no greater risk of over-blocking than in that case. Following this, the judge acknowledged the impossibility of listing all the matches within the relevant period, as the relevant events were not fixed sufficiently far in advance. The judge established in 2 years the duration of the order and for the events to be notified to the defendants at least 4 weeks in advance. In light of the evidence and for ‘essentially the same reasons’ given in the mentioned precedent, the judge granted the order, considering the blocking measure proportionate. In particular, the judge deemed it would not impair the rights of the defendants to carry on business. The judge also considered the interference with the rights of internet users to impart or receive information ‘justified by a legitimate aim, namely preventing infringement … on a large scale’ and proportionate to that aim, being ‘effective and dissuasive’ with ‘no equally effective but less onerous measures … available’. The judge stated that this measure would avoid the creation of barriers to legitimate trade and is not ‘unduly complicated or costly’. The order was considered to contain sufficient safeguards against misuse.

HIGH COURT (CHANCERY DIVISION), CARTIER INTERNATIONAL AG v BRITISH SKY BROADCASTING LTD [2014] EWHC3354 (CH), 17 OCTOBER 2014

NORMS

Article 5 Directive 2008/95/EC;
Recitals 7, 8, 17, 20, 40, 42, 45-48 and 50 Directive 2000/31/EC;
Articles 2(a), (b) and (d), 12, 13, 14, 15, 18(1) and 20 Directive 2000/31/EC;
Recital 59 and Article 8(3) Directive 2001/29/EC;
Recitals 17, 23 and 32 and Articles 3, 9(1)(a) and 11 Directive 2004/48/EC;
Articles 11, 16, 17, 51 and 52 of the Charter of Fundamental Rights of the European Union;
12/07/2011, C-324/09, L’Oréal-eBay, EU:C:2011:474;
Section 37(1) of the Senior Courts Act 1981;
Samsung Electronics (UK) Ltd v Apple Inc [2012] EWCA Civ 1339;
s. 10(1) and (4) of the Trade Marks Act 1994;

FACTS

The claimants, collectively known as Richemont, are owners of a large number of trade marks registered in the United Kingdom for luxury brands including Cartier, IWC, Montblanc and others. The defendants are five main retail ISPs in the United Kingdom. Richemont sought an injunction obliging the ISPs to block or impede access to six websites selling counterfeit goods bearing trade marks belonging to the claimants. This type of order, based on section 97A of the Copyright, Designs and Patents Act 1988, was frequently applied for to address online copyright infringement. Therefore, it was unclear whether the Court had jurisdiction to issue this type of order to address trade mark
infringement and if so, what are the threshold conditions and principles to be applied when deliberating the injunction.

**SUBSTANCE**

Considering the decision of the Court of Appeal in *Samsung Electronics (UK) Ltd v Apple Inc [2012] EWCA Civ 1339*, the Court observed that the breadth of the Court’s jurisdiction expressed in section 37(1) of the Senior Courts Act 1981 indicates that the Court’s power to grant injunctions can be exercised in new and innovative ways. Therefore, upon a purely domestic interpretation of law, the Court has jurisdiction to grant the order sought by Richemont. Nonetheless, the Court indicated that the same conclusion would be reached if s.37(1) of the Senior Courts Act 1981 was to be interpreted in accordance with Article 11 of the Council Directive 2004/48/EC.

Although Parliament has not laid down threshold conditions for the exercise of the High Court’s jurisdiction to grant an injunction against an intermediary on the basis of an intellectual property infringement committed by another, the Court’s discretion is not entirely unfettered. It is clear from *L’Oréal-eBay* that the Court must exercise its power under section 37(1) consistently with the provisions of Articles 3 and 11 of the Council Directive 2004/48/EC and Articles 12 to 15 of the Council Directive 2000/31/EC.

Therefore, firstly, the High Court indicated that the ISPs must be intermediaries within the meaning of the third sentence of Article 11. Secondly, either the users and/or the operators of the website must be infringing the claimant’s trade marks. Thirdly, the users and/or the operators of the website must use the ISPs’ services to do that. Moreover, the ISPs need to have an actual knowledge of the infringement. In the present case, that knowledge was obtained through notifications and evidence submitted by the claimant.

While deliberating if the injunction should be granted, the High Court considered if the relief sought by the claimant is necessary, effective, dissuasive, not unnecessarily complicated or costly, and if it does not create unnecessary barriers to trade. Moreover, the Court considered if the relief is proportionate and fair and equitable, thus striking a ‘fair balance’ between the applicable fundamental rights. Overall, Justice Arnold was satisfied that these conditions are fulfilled and decided to grant the injunction sought by Richemont.

The injunction granted bound the ISPs to block access to the websites infringing the claimant’s websites through IP and URL blocking based on the notifications submitted by the claimant. It also addressed IP address re-routing.

**CARTIER INTERNATIONAL AG V BRITISH SKY BROADCASTING LTD [2016] EWCA CIV 658**

**NORMS**

FACTS

In an appeal from the High Court decision in Cartier International AG v British Sky Broadcasting Ltd [2014] EWHC3354 (Ch), the United Kingdom's main retail internet service providers questioned the legal basis for an injunction obliging them to block or attempt to block access to certain websites selling and advertising counterfeit copies of the respondent's goods. Amongst other arguments, the ISPs argued that it was not within Court's jurisdiction to grant this type of order but even if it was, the threshold conditions were not satisfied. The appellants also submitted that the High Court judgment erred in relation to who should bear the costs of implementing the order.

SUBSTANCE

The Court of Appeal approved the High Court's interpretation of section 37(1) of the Senior Courts Act 1981 which suggests that the practice of the courts is not unchangeable and the injunctions are not limited to wrongdoers. In an analogy to the Norwich Pharmacal decision, once an innocent internet service provider is aware that its services are being used by someone to infringe an intellectual property right, then it becomes subject to a duty to take proportionate measures to prevent such infringements. Moreover, there was a principled basis for injunctions against the ISPs. The operator of the infringing websites had to rely on the ISPs services to sell counterfeit goods to UK customers. Even if innocent, the ISPs were being essential actors in the infringing activities. In the light of the CJEU judgment in L’Oréal-eBay, Article 11 of the Council Directive 2004/48/EC provides a principled basis for extending the practice of the court in relation to the grant of injunctions to encompass, where appropriate, the services of an intermediary, such as one of the ISPs, that have been used by a third party to infringe a registered trade mark.

The Court of Appeal also considered that the orders granted by the High Court did not give rise to any illegitimate or otherwise inappropriate limitation on the exercise of the rights and freedoms recognised by the Charter. Moreover, the High Court judge rightly observed that the court’s discretion to grant website-blocking orders must be exercised consistently with Articles 3 and 11 of the Council Directive 2004/48/EC and Articles 12 to 15 of the Council Directive 2000/31/EC.

In terms of the implementation costs of the orders, the judge was entitled to require the ISPs to bear them. The judge took a proper account of the Council Directive 2004/48/EC, the guidance given by the Court of Justice in L’Oréal-eBay and his own decision in Twentieth Century Fox Film Corp v British Telecommunications plc.

CARTIER INTERNATIONAL AG V BRITISH TELECOMMUNICATIONS PLC [2018] UKSC 28

NORMS

Articles 12, 13, 14 and 18 Directive 2000/31/EC;
Articles 3, 8 and 11 Directive 2004/48/EC;
Ashworth Hospital Authority v MGN Ltd [2002] 1 WLR 2033;
Rugby Football Union v Consolidated Information Services Ltd (formerly Viagogo Ltd) [2012] 1 WLR 3333;
Singularis Holdings Ltd v PricewaterhouseCoopers [2015] AC 1675;
Twentieth Century Fox Film Corp v British Telecommunications plc [2012] 1 All ER 806;
Twentieth Century Fox Film Corp v British Telecommunications plc (No 2) [2012] 1 All ER 869.
FACTS

Five main UK retail ISPs appealed against an order obliging them to bear the costs of implementing website-blocking orders. These orders were sought by the respondents, owners of multiple luxury brands, whose trade marks have been infringed by the target websites. Previously, the High Court held that it holds the jurisdiction to issue this kind of order in cases of trade mark infringement and that the costs should lay with the intermediaries. This reasoning was later reaffirmed by the Court of Appeal.

The ISPs brought the issue of who should bear the costs of injunctions before the Supreme Court of the United Kingdom.

SUBSTANCE

In regards to the legal basis for the injunctions, the Supreme Court emphasised the long-standing jurisdiction of the English courts to, in certain circumstances, order parties to assist those whose rights have been infringed by a wrongdoer. This jurisdiction was not limited to provision of information or to cases in which proceedings against a wrongdoer were anticipated. Once the intermediary was notified of the infringement, it had a duty to stop facilitating the activities of the wrongdoer, and the court had the equitable jurisdiction to intervene. Therefore, the website-blocking order made in this case could have been made quite apart from the power derived from European law, on ordinary principles of equity found under English law.

The Supreme Court indicated that issues of the implementation costs were a matter of English law, within the broad limits set by the EU principles of effectiveness and equivalence, and the requirement that any remedy should be fair, proportionate and not unnecessarily costly. As a matter of English law, the ordinary principle is that unless there are good reasons for a different order, an innocent intermediary is entitled to be indemnified by the rights holder against the costs of complying with a website-blocking order. In relation to the website-blocking orders, this position is no different in principle from the established position in domestic law in relation to injunctions granted to require an innocent party to assist the claimant in the assertion of its rights against a wrongdoer. Overall, there was no legal basis for requiring a party to shoulder the burden of remedying an injustice if they had no legal responsibility for the infringement, and ISPs were not obliged to do so simply because they benefited financially from the content available on the internet.
## ANNEX I: OVERVIEW TABLE PRELIMINARY RULINGS

<table>
<thead>
<tr>
<th>Case reference</th>
<th>Type of party whose liability/obligations are discussed</th>
<th>Type of act discussed in relation to infringement</th>
<th>Main findings of the CJEU</th>
<th>Legal provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>27/03/2014, C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192</td>
<td>Internet service provider</td>
<td>A website offering, without the agreement of the rights holders, either a download or ‘streaming’ of a wide range of films protected by copyright.</td>
<td>ISPs fall under Article 8(3) D 2001/29, and the term ‘intermediary’ covers any person who carries a third-party’s infringement of a protected work or other subject matter in a network. No specific relationship between the person infringing copyright or a related right and the intermediary is required. A person who makes protected subject matter available to the public on a website without the agreement of the rights holder, for the purpose of Article 3(2) D 2001/29, is using the services of the ISP. The fundamental rights recognised by EU law do not preclude a court injunction prohibiting an ISP from permitting its customers access to a website placing protected subject matter online without the agreement of the rights holders when that injunction does not specify the measures which the ISP must take, provided the following conditions are fulfilled: - the ISP can avoid incurring coercive penalties for breach of that injunction by showing that it has taken all reasonable measures; - the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available; - those measures have the effect of preventing unauthorised access to the protected subject matter, or of making access difficult; - the measures seriously discourage internet users who are using the</td>
<td>Article 8(3) of Directive 2001/29/EC.</td>
</tr>
<tr>
<td>Case reference</td>
<td>Type of party whose liability/obligations are discussed</td>
<td>Type of act discussed in relation to infringement</td>
<td>Main findings of the CJEU</td>
<td>Legal provisions</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>15/09/2016, C-484/14 Tobias McFadden v Sony Music Entertainent Germany GmbH, EU:C:2016:689</td>
<td>Business owner operating free anonymous access to a wireless local area network, WLAN (for use by its customers)</td>
<td>Making a musical work available on the internet free of charge without the consent of the rights holders (third parties – users of the internet connectio n).</td>
<td>Offering free of charge Wi-Fi to the general public constitutes an ‘information society service’ if done for the purpose of advertising the goods sold or services supplied by that service provider. Exemption from liability for third-party infringement when the process is: - technical; - automatic; - passive. A provider cannot be held liable for direct infringement if a user unlawfully uses his free Wi-Fi. Therefore, copyright holders cannot claim compensation, though they can seek proportional injunctions to stop future infringements. One means to achieve this would be to protect the communication network with a password which would oblige the users to reveal their identity.</td>
<td>Article 12(1) Directive 2000/31/EC read in conjunction with Article 12(3) of that Directive</td>
</tr>
<tr>
<td>03/10/2019, C-18/18 Glawischneg-Piesczek v Facebook Ireland Limited EU:C:2019:821</td>
<td>Social media platform (host provider)</td>
<td>Publishing a comment harmful to the reputation of a user accessible by all users of the platform</td>
<td>The e-commerce Directive, which seeks to strike a balance between the different interests at stake, does not preclude a court of a Member State from ordering a host provider: - to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information; - to remove information which it stores, the content of which is equivalent to the content of information which was</td>
<td>Articles 14, 15(1) and 18(1) Directive 2000/31/EC</td>
</tr>
</tbody>
</table>
### STUDY ON DYNAMIC BLOCKING INJUNCTIONS
#### IPR ENFORCEMENT CASE-LAW COLLECTION

<table>
<thead>
<tr>
<th>Case reference</th>
<th>Type of party whose liability/obligations are discussed</th>
<th>Type of act discussed in relation to infringement</th>
<th>Main findings of the CJEU</th>
<th>Legal provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>14/06/2017, C-610/15 Stichting Brein v Ziggo BV and XS4ALL Internet BV, EU:C:2017:456</td>
<td>Online peer-to-peer sharing platform (third party)</td>
<td>Making available and managing an online peer-to-peer file-sharing platform</td>
<td>previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content (thus, the host provider may have recourse to automated search tools and technologies); - to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law, and it is up to Member States to take that law into account.</td>
<td>Article 3(1) Directive 2001/29/EC</td>
</tr>
<tr>
<td>4.</td>
<td>Internet access providers</td>
<td></td>
<td></td>
<td>Article 8(3) Directive 2001/29/EC</td>
</tr>
</tbody>
</table>

**Complementary criteria for an act of communication:**
- the deliberate nature of the action;
- the use of specific technical means different from those previously used or which enable reaching a 'new public';
- the profit-making nature of the communication.

**Knowledge requirement:**
- platform operators were informed that the platform was used to provide access to works published without authorisation;
<table>
<thead>
<tr>
<th>Case reference</th>
<th>Type of party whose liability/obligations are discussed</th>
<th>Type of act discussed in relation to infringement</th>
<th>Main findings of the CJEU</th>
<th>Legal provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- platform operators expressed their intention to make protected works available;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- the large number of torrent files indicates that the platform operators could not have been unaware.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Profit-making purpose:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>It is clear that the platform is managed for the purpose of obtaining profit.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Considering the above, peer-to-peer platform operators could be held liable for this act of communication since they play an essential role in making protected works available, as they provide and manage the platform (indexation of metadata, provision of a search engine, etc.).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## ANNEX II: OVERVIEW TABLE NATIONAL CASE-LAW

<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM).</th>
<th>Relief sought</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
<th>Legal provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Belgium) Court of Appeals of Antwerp 3399-2011/8314, 26 September 2011, Belgian Anti-piracy Federation (BAF) v Telenet and Belgacom</td>
<td>Internet Service Provider</td>
<td>Third party Providing access to The Pirate Bay, where copyright was infringed on a massive scale</td>
<td>Relief sought: Blocking access to certain domain names</td>
<td>According to Article 87(1) par.2 of the Copyright Act, it is possible to issue an injunction against the ISPs, since they are intermediaries whose services are used by a third party to infringe a copyright or related right. The Court said that the liability exemption regime provided for under Article 12 of the e-commerce Directive was not an obstacle to the issuance of this injunction order. The Court stated that ISP's are under no general obligation to monitor their network and held that the blocking order was not disproportionate. The Court also ruled that to be proportionate, it was enough that the blocking order contribute to the reduction of the infringing activity. The Court clarified that there was no subsidiarity principle obliging BAF to first lodge an action against the direct infringer.</td>
<td>Article 87(1) par.2, of the Belgian Law of 30 June 1994 on Copyright and Neighbouring Rights implementing Article 8(3) of the InfoSoc Directive (D 2001/29/EC). Article 21(1) of the Belgian Act of 11 March 2003 on certain legal aspects of information society services implementing Article 15(1) of the e-commerce Directive.</td>
<td>The Court of Appeal overturned the lower court's decision. The Court of Appeal of Antwerp ordered ISP's to cease the infringements by applying DNS blocking to an exhaustive list of 11 domain names, under constraint of a penalty payment of EUR 1 000 per day. Article 87(1) par.2, of the Belgian Law of 30 June 1994 on Copyright and Neighbouring Rights implementing Article 8(3) of the InfoSoc Directive (D 2001/29/EC). Article 21(1) of the Belgian Act of 11 March 2003 on certain legal aspects of information society services implementing Article 15(1) of the e-commerce Directive.</td>
<td></td>
</tr>
<tr>
<td>(Belgium) Court of Cassation P.13.0550.N/1, 22 October 2013 Belgian Anti-piracy Foundation v Belgacom</td>
<td>Internet Service Provider</td>
<td>Third party Providing access to 'The Pirate Bay', where copyright was infringed on a massive scale</td>
<td>Relief sought: Extending the blocking order to all The Pirate Bay websites (blocking access</td>
<td>The Courts held that Article 39 bis of the Belgian Code of criminal procedure does not exclude a measure to be ordered against third parties, other than those having themselves stored the data. The court confirmed that the investigating judge could rightly rely on this provision to order the national internet access providers to stop access to the content hosted by the server associated to the main domain name.</td>
<td></td>
<td>The court dismissed the case and refused to ask questions to the CJEU.</td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(Denmark)</strong> Maritime and Commercial Court (Se-Handelsretten), case No: a-51-17 of 21 February 2018, Fritz Hansen A/S and Others (Represented by Rettighedsalliancen Smf.) v Telia Danmark A/S and Dominidesign Furniture Ltd.</td>
<td>Internet service provider &amp; an undertaking operating an online shop</td>
<td>The sale of replicas of Danish design furniture and lamps on websites, infringing the copyrights of the rights holders. Providing access to websites which sell replicas and infringe the copyrights of the rights holders. Relief sought: Blocking access to websites.</td>
<td>The infringing products were made available to the public in Denmark. Consequently, the websites infringed the applicants' copyrights. The Court found that it should be straightforward for the ISP to block access to the websites in question. The imposition of an injunction on the ISP did not give rise to harm or prejudice which is significantly disproportionate in relation to the interests of the parties. The Court noted that in the Code of Conduct agreed between the intertrade organisation and Rettigheds Alliancen it is assumed that it will be possible to direct a claim for prohibition at individual network operators. Paragraphs 2(1)-2(3), 413(3), 414(2) of the Danish Law on Copyright; Paragraph 1 of the Law on Commercial Practices (Markedsføringsloven).</td>
<td>Articles 39 bis and 89 of the Belgian Code of criminal procedure; Article 21(1) of the Belgian e-commerce Act implementing Article 15(1) of the e-commerce Directive; Article 52(1) of the Charter of Fundamental Rights of the European Union.</td>
<td>Order to implement a technical solution, for example DNS blocking, which is capable of preventing the customers in Denmark from accessing the websites that are selling replicas of the applicant's copyrighted furniture and lamps. Order to prevent access to other websites that give access to the same internet services and which the ISP has been informed of by the rights holders’ representative.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(Denmark)</strong> District Court of Frederiksberg, Copenhagen, case</td>
<td>Internet service provider</td>
<td>Providing access to internet services which make available or share works to Access to free films and TV shows on the internet provided by the Popcorn Time system is in</td>
<td></td>
<td></td>
<td>Order to implement a technical solution, such as a DNS blocker, that is suitable for preventing the ISP’s customers from accessing the internet services currently</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs) Legal provisions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 December 2017, RettighedsAlliance n etc. v TDC A/S</td>
<td>which the applicants have copyrights. Relief sought: Blocking access to internet services accessible through websites.</td>
<td>violation of the applicants' exclusive rights. As the Popcorn Time system makes use of the websites mentioned in the claim for the illegal viewing of films and television series, it is possible to prohibit the websites in question. The ISP's transmission of data objectively infringes the applicants' copyright. § 2(2) of the Copyright Act. 1, cf. 3, No. 3, cf. 4, No. 1, cf. § 65, paragraph 1. 1 and 6 and § 66(1), 1 and 2 and 67(1). 1 and 2; § 2(1) of the Copyright Act. 4, No. 1; Article 3(1) and Article 8(1) Directive 2001/29/EC.</td>
<td>accessible through the website addresses. Order to prevent access to other website addresses that provide access to the same internet services, which the applicants will expressly notify to the ISP, and in connection with which the applicants must demonstrate that these website addresses provide access to the internet services to which this decision relates. Each party should bear its own costs. Neither party was ordered to pay costs to the other party.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Finland) The Finnish Market Court, case No: MAO:311/18 of 07 June 2018, Columbia Pictures Industries, Inc., and Others v Blue Lake Communications Oy, and Others</td>
<td>Providing access to domain names which make available or share works to which the applicants have copyrights. Infringement of making copyrighted content available to the public without the consent of rights holders. Relief sought: Removing certain domain names, blocking access</td>
<td>The amount of infringing copyrighted content made available to the public without the rights holders' consent was significant. The target websites are available through the intermediaries, and the parties cover most of the Finnish bandwidth, thus making the injunction measure effective. The alleged infringers are not identifiable or the possibility to identify through international procedurals are uncertain based on an overall assessment. Assessing the proportionality of the injunction, the court found that most of the available content is likely protected by copyright and there is no other relevant purpose for the website services.</td>
<td>Order the ISP’s to block access from their customers to certain infringing internet services by deleting the domain names and by blocking the IP addresses from the ISP’s name servers. The request to block proxy sites was dismissed and was not included in the injunction, because the applicants did not show any measures taken to identify the administrators of the proxy sites. The court did not order the ISP’s to prevent access to other websites as the applicants did not provide anything that would suggest that they requested something else or more than what is already provided for by law.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(France) Search engine operator</td>
<td>Third party. Access to search results leading to websites that infringe rights holders’ rights. Relief sought: Request of a dynamic de-indexing injunction; blocking the search results leading to certain domain names.</td>
<td>Therefore, the court did not find the injunction unreasonable. The third parties’ right to receive and send messages is not endangered by blocking the IP addresses in question. Article 60 e(1)-(3) of the Finnish Copyright Act; Article 8(3) Directive 2001/29/EC.</td>
<td>The Court indirectly ordered a dynamic de-indexing injunction, examining the possibility of extending the measures to future domain names. The Court also ordered that during the period of implementation of the blocking and de-indexing measures the applicants were to inform the search engine operator if any of the infringing websites or access paths were no longer active or if the protected content was removed. The measures would be implemented within 15 days of the notification of the decision and for a period of 18 months.</td>
<td></td>
<td>The injunction was set to be in place for 1 year.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM).</td>
<td>Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>(France) Paris TGI, 7 March 2019, 18/14194</td>
<td>Internet Service Provider</td>
<td>Third party. Reproduction of copyright-protected publications on websites, accessible via several domain names, without prior authorisation.</td>
<td>Blocking access to the domain names and access paths not currently identified that would be activated or available after the issuing of the blocking order.</td>
<td>Articles L. 111-1, L. 121-1, L. 122-1 to L. 122-4 Code de la propriété intellectuelle (Intellectual Property Code (France)) (copyright infringement); Article L. 336-2 Code de la propriété intellectuelle (Intellectual Property Code (France)).</td>
<td>The lack of a general monitoring obligation prohibits the court from ordering the ISPs to implement appropriate measure affecting websites not listed in the publishers’ request. The measures should be proportionate, adequate and strictly necessary to achieve the aim pursued and ensure the protection of the rights at stake. There should be a balance between the fundamental rights involved, so that the injunction does not unduly and unnecessarily affect them. Therefore, the blocking injunction should only concern the infringing websites expressly and restrictively mentioned in the decision.</td>
<td>The Court ordered ISPs to implement all appropriate measures to prevent access from France, by their internet users under contract in that territory, by any effective means, to the sites mentioned accessible via the domain names referred, within 15 days of the notification of the decision and for a period of 12 months from the implementation of the measures ordered. The blocking measures would only cover the disputed sites that were expressly and restrictively listed in the publishers’ request. The costs of the necessary measures to be taken should be borne by the ISPs.</td>
<td></td>
</tr>
<tr>
<td>(France) Paris TGI, 13 July 2018, 18/55236</td>
<td>Internet Service Provider</td>
<td>Third party. Broadcasting of copyright- and neighbouring rights-protected content on various infringing websites that were accessible via new domain names.</td>
<td>Blocking access to the infringing websites</td>
<td>Article L. 336-2 Code de la propriété intellectuelle (Intellectual Property Code (France)); Articles 808 and 809 Code de procédure civile (French code of civil procedure); Articles 122-1, 122-2, 122-3, 122-4, 215-1 Code de la propriété intellectuelle (Intellectual Property Code (France)).</td>
<td>The Court found that ISPs should be the ones to bear the costs of implementing the measures ordered by the Court and that in the light of Directive 2001/29/EC, ordered the ISPs to implement all efficient and appropriate measures to prevent access to the infringing websites throughout France by their internet users. The ISPs should bear the costs and freely choose any effective means to block the access to the sites listed in the decision that were again</td>
<td>The Court granted the updated blocking orders. Moreover, the Court, in the light of Directive 2001/29/EC, ordered the ISPs to implement all efficient and appropriate measures to prevent access to the infringing websites throughout France by their internet users. The ISPs should bear the costs and freely choose any effective means to block the access to the sites listed in the decision that were again</td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs) Legal provisions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(France) Supreme Court (Cour de Cassation), 6 July 2017 16-17.217</td>
<td>Internet Service Provider; Search engine operators</td>
<td>domain names and access paths. Third party. Providing access to websites hosting copyright-protected content. Relief sought: blocking access to websites; stop listing these websites on search engine results.</td>
<td>the process of striking a balance between rights, such as the freedom of expression, the freedom to conduct a business and the principle of proportionality, the protection of IP rights was found to be of significant importance and the blocking order would not prejudice the freedom of expression and the ISPs’ freedom to conduct a business.</td>
<td>Article L 336-2 of Code de la propriété intellectuelle (Intellectual Property Code (France)); Article 8(3) Directive 2001/29/EC; Article 12 Directive 2000/31/EC; Loi No 2004-575 of 21 June 2004 (French implementation of the e-commerce Directive (2000/31/EC)); CJEU, 27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192, § 47, 50-53.</td>
<td>The Court's decision refers to previous court decisions. The Supreme Court upheld the decision issued by the Court of Appeal and stated that, even if it held that ISPs are not responsible for the infringing acts, however they should be the ones to bear the costs that are strictly necessary for the safeguarding of the rights at stake (copyright and related rights), even if these measures are likely to represent a significant cost for them (based on the Article 8(3) D 2001/29/EC and L 336-2 of the Intellectual Property Code (France)). The Court stated that a fair balance should be ensured between the IP rights (Article 17(2) CFREU) at stake and the ISPs’ freedom to conduct a business (Article 16 CFREU).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM).</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Germany) Regional Court of Munich I, Case No.: 7 O 17752/17, 1 February 2018, legal dispute for preliminary injunction, copyright infringement 'Fack ju Göhte 3' via kinox.to</td>
<td>Internet service provider (cable internet)</td>
<td>Providing access to a website illegally offering copyright-protected content – TV series and films. Relief sought: blocking access to the website Kinox.to.</td>
<td>In light of UPC Telekabel judgment, the fact that the cost of the measures is to be borne by the intermediary does not infringe the freedom to conduct a business provided that they can choose the technical measures to implement the blocking order.</td>
<td>Sec. 7(4) and 8(1) German Telemedia Act (TMG). In its reasoning the Munich Court refers to the decision of the German Federal Court of Justice (BGH) of 26 November 2015, case no. I ZR 174/14 – Störerhaftung des Access-Providers and to Article 8(3) Directive 2001/29/EC. The respondent should be seen as a party in breach of a duty of care (Störer) because it is subject to due diligence obligations as an internet service provider at least if it has been notified of a clear rights infringement and provided any monitoring obligations do not economically jeopardise its business model or disproportionately complicate its activities. The service Kinox.to has a highly criminal nature and is not worthy of protection. To this extent the concern of over-blocking does not even come into question. The costs to be incurred by the respondent in order to install the necessary equipment to block access (DNS and IP) has been considered not disproportionally high by the Court. The respondent was given a choice of how it would</td>
<td>The Court prohibited the respondent from providing their customers with internet access to the film 'Fack Ju Göhte 3', to the extent that this film is retrievable on the website service currently known as KINOX.TO. The prohibition carried the threat of a fine, to be set for each act of non-compliance, of up to EUR 250 000.00, or alternatively imprisonment in the case of non-payment, or imprisonment of up to 6 months, up to 2 years in the case of repeat offence, with the imprisonment or alternative imprisonment in the case of non-payment to be levied on the members of the board of the respondent. The Court made it also explicitly clear that the operative provisions do not relate solely to the domain kinox.to but to the overall service Kinox.to, which is offered under that company name, irrespective of the respective domain. A limitation of the prohibition to the URL which can be seen in the submitted evidence (showing examples of website screenshots only) has therefore not been applied for nor has it been intended by the Court. The Court ordered also the costs of the legal dispute to be borne by the respondent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM)</td>
<td>Third party act?</td>
<td>Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>------------------------------------------------------</td>
<td>------------------</td>
<td>--------------</td>
<td>---------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>(Germany) Regional Court of Munich I, Case No 37 O 2516/18, 7 June, 2019</td>
<td>Internet access provider</td>
<td>A third-party website retrievable via different URLs which makes available to users the applicants' copyright-protected works (CD-albums) without their consent. Block access to the said website for its users.</td>
<td></td>
<td></td>
<td>specifically implement the prohibition.</td>
<td></td>
<td>The Court assessed the balance of fundamental rights and found that DNS blocking is a reasonable and proportionate measure within the meaning of Sec. 7(4), second sentence of the German TMG. The court assessed also the effectiveness of the blocking measure to ensure effective protection of the applicant's fundamental right to property by preventing or at least hindering unauthorised access to protected objects and found that the DNS blocking is an effective measure. The danger of over-blocking has not been considered material since the legal content available on the website was estimated at below 4% of the overall content. The respondent was ordered to block the access of its users by means of DNS blocking to the internet service retrievable from certain URLs using certain IP addresses as long as explicitly listed album publications are accessible by means of file-sharing or share hosting via that service. The Court ordered the costs of the implementation of the blocking measures and the costs of the proceedings to be borne by the respondent.</td>
</tr>
</tbody>
</table>

The Court also considered that Section 7(4) TMG serves inter alia the purpose of implementing the obligation of Member States laid down in Article 8(3) of Directive 2001/29/EC to ensure that rights holders can take legal action against intermediaries, whose services are used by a third party to infringe copyright or related rights. Section 7(4) of the TMG must therefore be interpreted in conformity with the Directive as meaning that a telematica service assisted an infringement of the law by allowing its customers access to infringing content on the internet which has been made publicly available by third parties. The applicants have no other means than recourse to the defendant to remedy the infringement of their rights. In that regard, it was for the applicants to show that they had taken reasonable steps to reveal the identity of the website operator. The applicants satisfied those requirements by initiating state investigations and carrying out...
<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM). Third party act?</th>
<th>Relief sought</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Italy) Court of Milan – Ordinanza N. 42163/2019 R.G. of 5 October 2020, Sky Italia, Lega Serie A V Cloudflare and Others</td>
<td>Internet Service Provider</td>
<td>Third party. Illegal distribution of copyright-protected audiovisual content. Relief sought: blocking of current and future domain names and IP addresses of several IPTV services.</td>
<td></td>
<td>private inquiries, although they were unable to identify the operators of the websites.</td>
<td></td>
<td>The Court of Milan issued a dynamic blocking injunction ordering the blocking of current and future domain names and IP addresses of several IPTV services for illegal distribution of audiovisual content. The Court ruled that all the defendants, with their activity of ‘intermediaries’, are in any case subject to the dynamic injunction according to Article 156 et seq. Italian Copyright Act and Article 669bis et seq. c.p.c. The Court expressly stated that the classification between hosting providers, caching and ‘mere conduit’ services was irrelevant in the case, provided that the possibility to issue an injunction against intermediaries regardless of any liability of their own.</td>
</tr>
<tr>
<td>(Italy) Tribunale di Milano, R.G. N. 51624/2017, ECLI:IT:TRIBMI:2018:51624/2017, 18/06/2018</td>
<td>Internet Service Provider</td>
<td>Third party. Making links available for the download of unlawful copies of AM’s magazines by the website Dasolo (which later changed its domain name). Relief sought: blocking access to any domain names that would redirect to the</td>
<td></td>
<td></td>
<td></td>
<td>The Court referred to the need to balance all interests at stake, namely diritto d’autore, free enterprise, right to information. The Court fixed penalty payments for non-compliance for the ISPs. As regards the issue of cost allocation, the Court held that, since the measure requested was distinct from an assessment of any liability of the ISPs, by balancing different interests, the costs relating to technical expenses, strictly necessary and concerning the measure requested by the rights</td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| (Ireland) High Court of Ireland (Commercial), 2020 No. 6450 P of 29 September 2020, UEFA v Eircom Limited T/A EIR et al. | Retail internet service providers | platform connected to the website Dasolo. infringements themselves. The Court confirmed that AM’s rights were repeatedly infringed through the different domain names under which the infringing platform operated and recalled the UPC Telekabel judgment (27/03/2014, C-314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, EU:C:2014:192), and ruled that it is compatible with the e-commerce Directive to request an ISP to take the most appropriate measures to block access, not just to the domain names identified in the relevant injunction, but also to any further domain names under which infringements relating to the same rights are committed. However, to be compatible with the prohibition of general monitoring obligations, a dynamic injunction must include an obligation by the relevant rights holder to provide the targeted ISPs with a prior, specific notification concerning the new domain names through which infringements are being committed. | The Court accepted that each of the defendants is a ‘mere conduit’ and as such they are not liable for any copyright infringement arising out of activities of their subscribers under Irish law implementing Directive 2000/31/EC. ISPs are subject only to the grant of the sui generis type of injunction sought by UEFA. The Court held that the unauthorised streaming of sporting events is a communication to the public. | The Court considered the order necessary for the purpose of protecting the plaintiff’s rights since it is seen as an effective method of targeting unauthorised streaming of live sporting events. The risk of ‘over-blocking’ is very low and the fundamental rights of the users are respected since they have the right to apply to the Court to discharge or vary the order. The duration of the order, namely until the 31/07/2021, or the day after the last match period of the 2020/2021 UEFA
Even if the defendants did not oppose the application, the Court performed an assessment (taking into account the evidence presented by the plaintiff) in order to establish whether the order sought is lawful and that it is appropriate for the Court to grant the injunction sought. In performing the assessment the Court applied the following test and considered whether the injunction is: (i) necessary; (ii) that the costs involved were not excessive or disproportionate and that the order itself should not be unduly complicated; (iii) that the cost-sharing proposals were fair and reasonable; (iv) that the order respected the fundamental rights of the parties affected, including internet users and (v) that the duration of the proposed injunction and the provisions for review were reasonable.

Based on the presented evidence the Court answered all of the above questions to the affirmative.

Sections 17(1), 17(2), 37(1)(b), 40(1)(a) and 40(5A) of the Irish Copyright and Related Rights Act 2000 (2000 Act);

Article 8(3) Directive 2001/29/EC.

In summarising all the legislative obligations, the Court acknowledged that an injunction would need to follow the criteria stated below:

1. any injunction should be fair and equitable;
2. any injunction should not be unnecessarily complicated or costly;

The Court granted an injunction of GRS, but without the 1 week service suspension and with some adjustments. Facts about internet piracy were also used from a previous case – EMI records (Ireland) Ltd. And Others v Eircom (2010).

The problem with criterion 2 was that a computer system would need to be developed. The Court decided...
## Case Study on Dynamic Blocking Injunctions in IPR Enforcement Case:

<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM). Third party act?</th>
<th>Relief sought</th>
<th>Reasoning/criteria applied</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ireland Limited [2015] IEHC 317</td>
<td>internet service provider involved in the piracy of the rights holders' music. Relief sought:</td>
<td>Injunction of a graduated response strategy (GRS), explaining the actions that the internet service provider would voluntarily implement in order to prevent infringing actions. The plaintiffs’ primary request consisted of a GRS in which the internet service provider must send cease and desist letters to its subscribers, threaten them with a suspension of services, after the third notification suspend them for a week and after a fourth notification terminate their contract.</td>
<td>3. any injunction should not entail unreasonable time limits or unwarranted delays; 4. any injunction should be effective, proportionate and dissuasive; 5. any injunction should be applied in a manner that avoids the creation of barriers to legitimate trade; 6. any injunction should provide for safeguards against its abuse; 7. any injunction granted should respect the fundamental rights of a subscriber; 8. any injunction granted should ensure that there is a prior, fair and impartial procedure which includes the right to be heard of the person concerned; 9. any injunction granted should ensure that there is a right of effective and timely judicial review of such an injunction.</td>
<td>that even though the new system would be costly and complicated, it would not be unnecessarily so. On the issue of whether the remedies would be effective, proportionate and dissuasive if the Court decided that the writing of letters do meet the criteria, evidence from the Eircom protocol (the plaintiffs’ experience from the previous injunction) confirmed the Court's decision. The Court analysed the problem with prior, impartial procedure, and specifically the right to be heard by the person concerned. The Court decided to order a Norwich Pharmacal order, which is an order of the court that the defendant disclose to the plaintiffs the names and addresses of its subscribers in respect of whom there is a prima facie demonstration of wrongful activity. This procedure arises in circumstances where parties are aware that other parties are engaged in wrongful activity. The plaintiffs would make such an application, receive the subscribers’ identity and seek an order for the termination of their contract.</td>
<td>Legal provisions</td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM).</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| (Ireland) The High Court of Ireland (Commercial) EMI Records (Ireland) Limited & Ors v UPC Communications Ireland (Limited) and Ors. [2013] IEHC 274 | Internet service providers | Providing access for the internet service providers’ subscribers to the website The Pirate Bay, and related domain names, IP addresses and URLs, where copyrights of the plaintiffs’ (record companies) music and videos were infringed. Third-party act. | Three main issues were especially considered:  
- i) the appropriateness of the order;  
- ii) whether fresh applications will have to be made to the Court in case The Pirate Bay website changes its location; and  
- iii) the costs of proceedings. | Article 3 Directive 2004/48/EC; Section 37 Copyright and Related Rights Act 2000. | The judgment confirmed that the plaintiffs are entitled to a blocking injunction in accordance with the terms of the draft order and protocol (not available publicly) submitted to the court. The costs associated with implementing the order should be borne by each of the defendants. The judgment found it proportionate and reasonable that new applications would not be required to be made to the court if The Pirate Bay website changes its location on the internet, as detailed in the draft order and protocol. The costs associated with implementing the order should be borne by each of the defendants. The Court ruled that the defendants – except the second defendant – will bear their own proceeding costs, reasoning that although none of them are wrongdoers, the infringement has caused (and continues to cause) substantial financial damage to the plaintiffs. As regards the second defendant, the plaintiffs agreed to pay the costs on the basis that it did not actively participate in the proceedings. |
### STUDY ON DYNAMIC BLOCKING INJUNCTIONS

**IPR ENFORCEMENT CASE-LAW COLLECTION**

<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Ireland) The High Court of Ireland EMI Records (Ireland) Limited &amp; Ors v Eircom Limited [2010] IEHC 108</td>
<td>Internet service provider</td>
<td>Illegal downloading and uploading of copyrighted music (and other copyrighted creations) performed by subscribers using the defendant’s internet service. Third-party act. Settlement between the parties.</td>
<td>In the judgment the Court did not analyse or discuss in length the questions of whether infringements are taking place, how they are being carried out or what kind of injunction it will grant. The only issues the Court did go into are issues connected to privacy and data protection.</td>
<td>Section 37 of the Copyright and Related Rights Act 2000; Section 40 of the Copyright and Related Rights Act 2000; Data protection acts, 1988-2003: s.1 Data protection act 1988 and section 2, 2A, 2B, 2C and 2D of the Data protection act 1988, as amended.</td>
<td>The Court found three possible issues with the implementation of the injunction. First, it looked into the question of whether the information/data collected in such a procedure would be personal data. The Court's opinion is that neither of the plaintiffs have any interest in identifying any living person infringing copyright or requesting it from the defendant. The second issue addressed was the processing of data, and more specifically if such processing represents &quot;unwarranted [processing] by reasons of prejudice to the fundamental rights and freedoms or legitimate interests of the data subjects&quot;. The Court viewed the processing as necessary for both the performance of the contract and for compliance with a legal obligation cast upon the courts. There cannot be a constitutional right to privacy that extended to the organisation of crime. The Court determined that there is nothing disproportionate and therefore the actions were not unwarranted. The third issue the Court analysed was the fact that two private entities would process data and then communicate the decision to terminate a user's internet service. All parties involved are not interested in the detection or prosecution of criminal offences. In conclusion, the Court agreed that the graduated response is lawful and that the settlement can be implemented.</td>
</tr>
<tr>
<td>Case</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Netherlands) Amsterdam Court of Appeal, case no. 200.243.005/01, 2 June 2020, ZIGGO B.V. and XS4ALL Internet B.V. v Stichting Brein [Brein Foundation]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of defendant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet access providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type of act allegedly affecting exclusive right (©/TM).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party act?</td>
</tr>
<tr>
<td>Relief sought</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reasoning/criteria applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Amsterdam Court of Appeal referred to the UPC Telekabeli judgment recalling in detail the findings of the CJEU.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Amsterdam Court of Appeal came to the conclusions that (i) since the content on The Pirate Bay is predominantly if not exclusively illegal (90% to 95%) the denial of access to lawfully available information which results for the subscribers from the blocking of the website is proportionate to the extent and seriousness of the copyright infringement committed on TPB website; (ii) the claimed blocking under the circumstances of the case has a sufficient effect in preventing or at least complicating unauthorised access to protected works and that users who avail themselves of the services of Ziggo and XS4ALL are seriously discouraged from gaining access to those works; (iii) the order claimed does not demand unbearable sacrifices from Ziggo and XS4ALL, cannot be deemed as unreasonable, and can be regarded as a relatively minor encroachment on the freedom of entrepreneurship of Ziggo and XS4ALL. Based on the foregoing considerations the Amsterdam Court of Appeal found that the blocking claimed by Brein is compatible with the fair balance between the fundamental rights of (intellectual) property, the freedom of information and the freedom of entrepreneurship. The Amsterdam Court of Appeal found also that the claimed blocking does not infringe the general monitoring prohibition laid down in</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Amsterdam Court of Appeal ordered Ziggo and XS4ALL to cease and desist their services used to infringe copyright and related rights of rights holders whose interests are safeguarded by Brein, within 10 (ten) working days, by blocking and keeping blocked access by their clients to specific and clearly identified domain names/(sub) domain names and IP addresses through which TPB operates as well as other (sub)domain names indicated in a list submitted to the Court by Brein and attached to the judgment, as long as TPB operates through these (sub)domain names and IP addresses. The Amsterdam Court of Appeal ordered Ziggo and XS4ALL also, in the event that TPB starts to operate via other/additional IP addresses and/or (sub)domain names than those aforementioned, to block and keep blocked access by their customers to these other/additional IP addresses and/or (sub)domain names by Brein by fax, registered letter or email to Ziggo and XS4ALL separately. Failure to comply with the above orders triggers the payment of fines and penalties.</td>
</tr>
<tr>
<td>Case</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>(Netherlands) Rechtbank Den Haag, C/09/485400 / HA ZA 15-367, 24 January 2018, (FAPL LTD. V ECATEL LTD.), ECLI:NL:RBDHA:2018:615</td>
</tr>
<tr>
<td>Case</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>(Netherlands) Rechtbank Midden Nederland C/16/448423/ KGZA 17-382, 12 January 2018 (Stichting Brein v KPN B.V. and others) ECLI:NL:RBMNE:2018:114</td>
</tr>
<tr>
<td>(Spain) Commercial Court Nº 7 of Madrid</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Spain) Commercial Court Nº 7 of Madrid</td>
<td>Internet Access Provider</td>
<td>Article 21.1 Ley de Enjuiciamiento Civil (LEC);</td>
<td>The blocking injunctions imposed by the Court are two folded:</td>
</tr>
</tbody>
</table>

126
<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
</table>
| (Juzgado de lo Mercantil nº 7 de Madrid), 2174/2019 of 11/02/2020 (Telefónica Audiovisual Digital, S.L.U. v Vodafone España, S.A.U., Et Al.) | websites offering unlicensed distribution of live football matches through illicit Internet Protocol Television (IPTV) services. Relief sought: Blocking access to websites offering IPTV services. | Article 395 LEC, Article 394(1) LEC; Articles 455 and following LEC. According to Spanish law, in cases where the defendants acquiesce to the applicant’s arguments and claims, the Court issues an order without entering into the merits of the case, unless the claim was done in bad faith, goes against the public order or prejudices the rights of third parties. In this case, the Court did not enter into the merits of the case and, therefore, did not analyse the legal framework applicable to dynamic blocking injunctions. | | (i) Static blocking injunctions:  
• The sued internet access providers had to block, within 72 hours of the notification of the judgment, the URLs, domain names and IP addresses from 44 pirate sites and services;  
• The ISPs should block at the level of both HTTP and HTTPS protocols, and were expected to take any access prevention action they could;  
• The injunction is limited to 3 years, covering three football seasons 2019-2022.  
• ISPs will have to report back to Telefónica Audiovisual Digital and notify the exact time when they blocked access to the newly added web resources.  
(ii) Dynamic blocking injunctions:  
• The authorised broadcaster will update weekly the blocking list with new entries (sites, IP addresses, URLs) related to the 44 pirates sites mentioned in the judgment and send it directly and simultaneously to the ISPs without a new court order;  
• ISPs will be given 3 hours to respond to new entries;  
• The dynamic injunction lasts until 25 May 2022. The judgment is now final. |
<p>| (Spain) Decision No. 15/2018 of the Commercial Court no. 6 of Barcelona, | Internet Service Provider | Copyright infringement through the illegal display of content. Relief sought: blocking or | Articles 138(3) and 139(1)(h) of the Spanish Copyright Act (SCA); Article 10 Spanish Law 34/2002 on Services of the Information Society and Electronic Commerce; | The ruling orders the operators, by virtue of Articles 138(3) and 139(1)(h) of the Spanish Copyright Act, to block the access of the ISPs’ users from Spanish territory to the pages HDFull and Repelis. |</p>
<table>
<thead>
<tr>
<th>Case Details</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM)</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 January 2017 (Hdfull Case):</td>
<td>Internet service provider</td>
<td>Preventing the access of the ISPs’ users to the pages HDFull.tv and Repelis.tv.</td>
<td>On the proportionality of the measures claimed by the plaintiffs, the Court considered that the refusal of access to a website on which infringing material is made available by internet service providers to their customers seems proportionate since its purpose is to prevent access to infringing websites whose owners could not be identified or located.</td>
<td>Article 8(3) Directive 2001/29/EC; Articles 9(1) and 11 Directive 2004/48/EC.</td>
<td>The operators must also block the proxies that allow access to the content, to prevent access to other domains and IP addresses whose purpose is to facilitate the circumvention of technological protection measures and thereby allow access to users.</td>
</tr>
<tr>
<td>(Sweden) Swedish Patent and Market Court of Appeal, case No: PMT 13399-19 of 29 June 2020, Telia Sverige AB v Svensk Filmindustri and Others</td>
<td>Internet service provider</td>
<td>Providing access to internet services, where copyright-protected material was made available.</td>
<td>The ISP had contributed in copyright infringement by providing internet connections to its subscribers, who thereby had access to certain cinematographic works that had been unlawfully made available through certain online services.</td>
<td>§53B (first sentence) of the Swedish Act on Copyright in Literary and Artistic Works (1960:729) (the Copyright Act); Article 8(3) Directive 2001/29/EC.</td>
<td>Confirmation of the dynamic blocking injunction ordered by the previous instance. Clarifying the arrangement and form of the dynamic blocking injunction. Clarifying that it was not necessary to identify the persons administering the services or to describe the services in question. Instead, it was essential to clearly describe the characteristics, structure and operation of the services. Clarification that domain names and URLs related to search engines do not fall under the scope of the injunction, nor should it cover situations where links to the services are included in posts on social media. It is not appropriate or proportionate to require the ISP to also monitor new domain names and URLs that infringe the rights holders’ copyrights. Instead, the rights holders should notify the ISP of the specific domain names and URLs it should block and the ISP was given...</td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>(Sweden) Swedish Patent and Market Court (Svenska Patent- och Marknadsdomstolen), case No: PMT 7262-18 of 9 December 2019, Telia Sverige AB v Svensk Filmindustri and Others</td>
<td>Internet service provider</td>
<td>Providing access to internet services, where copyright-protected material was made available. Relief sought: blocking access to internet services accessible through websites.</td>
<td>The ISP had provided internet connection to its subscribers, who thereby had access to certain cinematographic works that had been unlawfully made available through certain online services. The court found that there has been infringement in an objective sense, and that the ISP therefore has joint responsibility. The legislation does not impose any requirement that the rights holders should first turn to the direct infringer and not the ISP. The services at issue in this case changed their domain names and/or used proxy services to circumvent any blocking measure. The requirement for the ISP to block, in addition to the domain names used for the infringing activity, services that may arise in the future through other domain names and URLs, ensures that the measure is appropriate and effective to achieve the desired purpose. Article 1, 2 and 53b of the Swedish Copyright Act (1960:729); Article 3(3) and 8(3) D 2001/29/EC.</td>
<td>Prohibit the ISP from making the protected material set out in the judgment available to the public. Order the ISP to block access to a number of infringing websites by imposing a dynamic blocking injunction. Order to take reasonable steps to block the access to the specified services through domain names and URLs other than those specified in the judgment. Requirement to act in the event of becoming aware that the services are available through certain domain names or URLs, such as being informed from time to time by the rights holders. Requirement to react promptly to take adequate blocking measures in 2 to 3 weeks of the date of the notification. The ISP is not required to take any other blocking measures than technical blocking of customers’ access to domain names and URLs that lead to the services or to have constant and total monitoring over the internet. The prohibition is given under the threat of a SEK 500 000 fine over a period of 3 years.</td>
<td>a 3 week timeframe in which to implement the necessary measures. Confirmation for the injunction to be in force for 3 years in order to be efficient.</td>
</tr>
<tr>
<td>(United Kingdom)</td>
<td>Internet service providers</td>
<td>Illegal IPTV streaming of live sporting events.</td>
<td>The services of the internet providers are used for infringing copyright and the ISPs have</td>
<td>Dynamic blocking order issued.</td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>High Court of Justice business and property courts of England and Wales, case No: IL-2018-000155 of 29 October 2020, Matchroom v British Telecommunicatios plc et al.</td>
<td>Providing access to certain IP addresses that are being used to infringe copyright relating to live streams of events.</td>
<td>actual knowledge of it. In such a case the High Court (in Scotland, the Court of Session) has the power to grant an injunction against the ISPs. Section 97A of the Copyright, Designs and Patents Act 1988.</td>
<td></td>
<td>Disabling access to current and future IP addresses as indicated by the copyright holder. Parts of the order kept confidential in order to avoid undermining the blocking methods and assisting the infringers. The blocked access should be unblocked as soon as reasonably practicable after the expiry of the event. Safeguards provided for the ISPs and third parties in order to avoid over-blocking.</td>
<td></td>
</tr>
<tr>
<td>(United Kingdom) England and Wales High Court (Chancery division), HC-2017-000458 of 13 March 2017, the Football Association Premier League limited v British telecommunication s plc et al.</td>
<td>Internet service providers (ISPs) Some of the defendants are exclusive licensees of broadcasting and internet transmission rights for Premier League footage in the UK.</td>
<td>Illegal IPTV streaming of live sporting events (football matches). Providing access to certain IP addresses that are being used to infringe copyright relating to live streams of events.</td>
<td>Section 97A of the Copyright, Designs and Patents Act 1988; Article 8(3) Directive 2001/29/EC.</td>
<td>Dynamic blocking order issued. The order is ‘live’ since it only has effect at the times when live Premier League match footage is being broadcast. New servers can be identified by the rights holder and notified to the defendants each week. The order is limited in time. Safeguards provided for the ISPs and third parties in order to avoid over-blocking. Proportionality achieved between the rights of the applicant and the defendants.</td>
<td></td>
</tr>
<tr>
<td>(United Kingdom) England and Wales High Court (Chancery Division), IL-2018-000155 of 20 September 2018, Matchroom Boxing Limited and</td>
<td>Internet service providers (ISPs)</td>
<td>Illegal IPTV streaming of live sporting events (boxing matches). Providing access to servers hosting the copyrighted content broadcast in infringement of</td>
<td>Section 97A of the Copyright, Designs and Patents Act 1988.</td>
<td>Dynamic blocking order issued. The blocking measure was considered proportionate, effective and dissuasive. Duration limited to 2 years. Details regarding the monitoring techniques applied to prevent the infringing acts have been kept confidential in the order to avoid circumvention.</td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td>Type of defendant</td>
<td>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</td>
<td>Reasoning/criteria applied</td>
<td>Legal provisions</td>
<td>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Matchroom sport Limited v British Telecommunications plc et al.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The interference with the rights of internet users to impart or receive information ‘justified by a legitimate aim, namely preventing infringement … on a large scale’. The order was considered to contain sufficient safeguards against misuse.</td>
</tr>
<tr>
<td>(United Kingdom) High Court (Chancery division), Cartier International AG v British Sky Broadcasting LTD [2014] EWHC3354 (CH), 17 October 2014</td>
<td>Internet service providers (ISPs)</td>
<td>Trade mark rights for luxury goods. Websites selling counterfeit goods. Block or impede access to six websites selling counterfeit goods bearing trade marks belonging to the claimants.</td>
<td>Article 5 Directive 2008/95/EC; Recitals 7, 8, 17, 20, 40, 42, 45-48 and 50 Directive 2000/31/EC; Articles 2(a), (b) and (d), 12, 13, 14, 15, 18(1) and 20 Directive 2000/31/EC; Recital 59 and Article 8(3) Directive 2001/29/EC; Recitals 17, 23 and 32 and Articles 3, 9(1)(a) and 11 Directive 2004/48/EC; Articles 11, 16, 17, 51 and 52 of the Charter of Fundamental Rights of the European Union; 12/07/2011, C-324/09, L’Oréal-eBay, EU:C:2011:474; Section 37(1) of the Senior Courts Act 1981; Samsung Electronics (UK) Ltd v Apple Inc [2012] EWCA Civ 1339; s. 10(1) and (4) of the Trade Marks Act 1994; s. 97A Copyright, Designs and Patents Act 1988.</td>
<td>Dynamic blocking order granted. It was considered that the relief sought by the claimant is necessary, effective, dissuasive, not unnecessarily complicated or costly, and that it does not create unnecessary barriers to trade. The Court considered that the relief is proportionate and fair and equitable, thus striking a ‘fair balance’ between the applicable fundamental rights. The injunction granted bound the ISPs to block access to the websites infringing the claimant’s rights through IP and URL blocking based on the notifications submitted by the claimant. The costs of implementing the measures is to be borne by the ISPs.</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- Dynamic blocking order (DBI) refers to an injunction that blocks access to a website where the order is not limited to wrongdoers.
- The Court considered that the relief is proportionate and fair and equitable, thus striking a ‘fair balance’ between the applicable fundamental rights.
<table>
<thead>
<tr>
<th>Case</th>
<th>Type of defendant</th>
<th>Type of act allegedly affecting exclusive right (©/TM). Third party act? Relief sought</th>
<th>Reasoning/criteria applied</th>
<th>Legal provisions</th>
<th>Outcome (DBI ordered, conditions, balance of rights, obligations, remedies, implementation costs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[2016] EWCA Civ 658</td>
<td>Websites selling counterfeit goods. Block or impede access to six websites selling counterfeit goods bearing trade marks belonging to the claimants.</td>
<td>Articles 12 to 15 Directive 2000/31/EC; Section 37(1) of the Senior Courts Act 1981; Norwich Pharmacal Co v Customs and Excise Commissioners [1974] AC 133; Twentieth Century Fox Film Corp v British Telecommunications plc [2011] EWHC 2714 (Ch).</td>
<td>Legal provisions</td>
<td>Legal provisions</td>
<td>right, then the ISP becomes subject to a duty to take proportionate measures to prevent such infringements. ISPs considered an essential actor in infringing activities. The costs of implementing the measures is to be borne by the ISPs.</td>
</tr>
</tbody>
</table>
# ANNEX III: GLOSSARY

The definitions below give some references for the terminology used in the case-law collection.

<table>
<thead>
<tr>
<th>TERM USED</th>
<th>MEANING/REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Injunction</strong></td>
<td>An order aimed at prohibiting the continuation of infringement (264).</td>
</tr>
<tr>
<td><strong>Website-blocking injunction</strong></td>
<td>‘A blocking injunction is an order requiring an internet intermediary to implement technical measures directed at preventing or disabling access to a specific internet location’ (265).</td>
</tr>
<tr>
<td><strong>Dynamic injunction</strong></td>
<td>Injunctions which can be issued, for example, in cases in which materially the same website becomes available immediately after issuing the injunction with a different IP address or URL, and which are drafted in a way that makes it possible to also cover the new IP address or URL, without the need for a new judicial procedure to obtain a new injunction (266).</td>
</tr>
<tr>
<td><strong>Information society service</strong></td>
<td>Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (267).</td>
</tr>
<tr>
<td><strong>Internet/online intermediary</strong></td>
<td>Brings together or facilitates transactions between third parties on the internet.</td>
</tr>
<tr>
<td></td>
<td>Gives access to, hosts, transmits and indexes content, products and services originated by third parties on the internet, or provides internet-based services to third parties (268).</td>
</tr>
</tbody>
</table>

(264) Article 11(1) IPRED.

(265) Jaani Riordan, The Liability of Internet Intermediaries, Oxford, UK, 2016, p. 461. See also a study commissioned by the EUIPO, Study on Legislative Measures Related to Online IPR Infringements, EUIPO, September 2018, available at [https://euipo.europa.eu/olemporal/en/web/observatory/observatory-publications](https://euipo.europa.eu/olemporal/en/web/observatory/observatory-publications), p. 42 et seq.: ‘If an IPR infringing activity takes place on or through a dedicated website … it will be an effective way to disrupt the current activities and to prevent them from taking place in the future if the access to the website by the internet users in general is blocked’.


<table>
<thead>
<tr>
<th><strong>Internet access provider/internet service provider (ISP)</strong></th>
<th>Provides subscribers with a data connection allowing access to the internet through physical infrastructure (^{(269)}).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Live blocking order</strong></td>
<td>Blocking order impeding access to streaming servers during a specific timeframe (^{(270)}).</td>
</tr>
<tr>
<td><strong>Online content-sharing provider</strong></td>
<td>Provider of an information society service whose main purpose, or one of its main purposes, is to store and provide public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users which it organises and promotes for profit-making purposes (^{(271)}).</td>
</tr>
<tr>
<td><strong>Online intermediation service / online platform</strong></td>
<td>Information society service; that allows business users to offer goods or services to consumers, to help start direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; and that is provided to business users on the basis of contractual relationships between the provider of those services and business users, which offer goods or services to consumers (^{(272)}). Examples: online e-commerce marketplaces, including collaborative ones on which business users are active, online software applications services, such as application stores, and online social media services, irrespective of the technology used to provide such services (^{(273)}).</td>
</tr>
<tr>
<td><strong>Online search engine</strong></td>
<td>A digital service that allows users to input queries in order to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found (^{(274)}).</td>
</tr>
</tbody>
</table>

\(^{(269)}\) OECD, The Economic and social role of internet intermediaries, April 2010, p. 11.

\(^{(270)}\) See England and Wales High Court (Chancery Division) — HC-2017-000458 ([2017] EWHC 480 (Ch)) — 13 March 2017.


\(^{(273)}\) Recital 11 of the proposed Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services.

\(^{(274)}\) Article 2(5) of the proposed Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services.
<table>
<thead>
<tr>
<th>Payment service provider</th>
<th>Any natural or legal person which provides payment systems through credit or directly or indirectly associated with a bank account for enabling transactions ((^{275})).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search engine operator</td>
<td>Any natural or legal person which provides, or which offers to provide, online search engines to consumers ((^{276})).</td>
</tr>
<tr>
<td>Online social media providers</td>
<td>'Online social media providers are online platforms that host, enable and encourage the exchange of user-generated and other content between individuals through social interaction.' ((^{277})).</td>
</tr>
</tbody>
</table>


# ANNEX IV: LEGAL EXPERTS

<table>
<thead>
<tr>
<th>Studied Member States</th>
<th>Legal experts</th>
</tr>
</thead>
</table>
| **Belgium**           | Azizollahoff Nathan, Lawyer, Brussels, Belgium  
Debled Alexandre, Lawyer, Brussels, Belgium  
Karolina Zhytnikova, IP Lawyer, Paris, France (278) |
| **Denmark**           | Knud Wallberg, Attorney-at-law, PhD, Denmark |
| **Finland**           | Tuomas Mylly, Professor of Commercial Law at the University of Turku, Director of IPR University Center, Finland  
Ulla-Maija Mylly, TIAS Collegium Postdoctoral Researcher at University of Turku, Finland  
Samuli Melart, Doctoral Candidate in Law, University of Turku, Finland |
| **France**            | Mathilde Persuy, Intellectual Property and Anti-Piracy Lawyer, France  
Olivia Bacin, IP Lawyer, Paris, France |
| **Germany**           | Prof. Jan Bernd Nordemann  
Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |
| **Greece**            | Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |
| **Ireland**           | Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |
| **Italy**             | Ludovico Anselmi, Partner in the IP & TMT Department of law firm Orsinger Ortu – Avvocati Associati |
| **Lithuania**         | Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |
| **Netherlands**       | Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association) |

(278) Karolina Zhytnikova translated the questionnaire from French to English.
<table>
<thead>
<tr>
<th>Country</th>
<th>Names and Positions</th>
</tr>
</thead>
</table>
| Spain    | Sorin Berbece, Legal Counsel (Motion Picture Association)  
Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |
| Sweden   | Julia Demitz, Legal Officer at the Swedish Patent and Registration Office (PRV)  
Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |
| UK       | Okke Delfos Visser, Head of Legal Department & Senior Vice-President (Motion Picture Association)  
Sorin Berbece, Legal Counsel (Motion Picture Association) |