Building Respect for IP

Study*: The localization of IP infringements in the online environment: From Web 2.0 to Web 3.0 and the Metaverse*

September 2023

WIPO
WORLD INTELLECTUAL PROPERTY ORGANIZATION

The Localization of IP Infringements in the Online Environment: From Web 2.0 to Web 3.0 and the Metaverse

Prepared by Eleonora Rosati, Professor of Intellectual Property Law, Stockholm University.[*]

STUDY COMMISSIONED BY THE BUILDING RESPECT FOR IP DIVISION
GLOBAL CHALLENGES AND PARTNERSHIPS SECTOR
WORLD INTELLECTUAL PROPERTY ORGANIZATION

Geneva, 2023

[*] Professor of Intellectual Property Law (Stockholm University). Email: eleonora@elawnora.com. The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO. All Internet sources were last accessed on 7 August 2023.

EXECUTIVE SUMMARY

Over time, technological advancements have resulted in novel ways both to exploit content and to infringe rights – including intellectual property rights (IPRs) – vesting in them. Legislative instruments have consistently clarified that pre-existing rights continue to apply to new *media*, i.e., means to disseminate intangible assets, including in digital and online contexts. In terms of rights enforcement, however, the progressive dematerialization of content and dissemination modalities has given rise to challenges, including when it comes to determining *where* an alleged IPR infringement has been committed.

The importance of such an exercise cannot be overstated: it is *inter alia* key to determining (i) whether the right at issue (e.g., a registered IPR) is enforceable at the outset, (ii) which law applies to the dispute at hand, as well as – in accordance with certain jurisdictional criteria – (iii) which courts are competent to adjudicate it. For example, determining that the relevant infringement has been committed in country A serves in turn to determine: (i) if the right at issue is enforceable at all, given that IPRs are territorial in nature. So, if the IPR in question is a national trademark, the infringement needs to be localized in the territory of the country where the right is registered; (ii) whether, e.g., country A's law is applicable to the dispute at hand; and (iii) if, e.g., the courts in country A have jurisdiction to adjudicate the resulting dispute.

This said, questions of applicable law and jurisdiction should not be conflated. Answering the former serves to ensure that a court does not have to apply more than one law, but rather only focus on the initial act of infringement to identify the law applicable to the proceedings. *Vice versa*, such a need to ensure that only one law is applicable does not exist in the context of jurisdiction rules, which frequently provide for more than one forum.

The localization exercise described above has proved to be particularly challenging when the infringing activity is committed in a digital or online context. For infringements occurring in Web 2.0 situations, courts around the world have nevertheless progressively developed various approaches to localize the infringing activity, by considering the place where (a) the defendant initiated the infringing conduct (causal event criterion), (b) the infringing content may be accessed (accessibility criterion), and (c) the infringing conduct is targeted (targeting criterion). While none of these criteria is devoid of shortcomings, targeting has progressively gained traction in several jurisdictions around the world. Proof of targeting depends on a variety of factors, including language, currency, possibility of ordering products or services, relevant top-level domain, customer service, availability of an app in a national app store, etc. Overall, what is required to establish targeting is a substantial connection with a given territory.

Another development is currently underway: it is the transition from the already interactive dimension of Web 2.0 to the even better integrated and more immersive reality of Web 3.0 (if not already Web 4.0!). It is expected that such a transition will be made possible by the rise of augmented reality, blockchain, cryptocurrencies, artificial intelligence, and non-fungible tokens for digital assets. In this sense, the progressive evolution of the metaverse will be pivotal. Even though the concept of metaverse has existed for over thirty years, it has recently been revamped. Thanks to the advent of the new technologies just mentioned, it is hoped that the "new" metaverse will be characterized by four main features: interoperability across networked platforms; immersive, three-dimensional user experience; real-time network access; and the spanning of the physical and virtual worlds. In all this, different metaverses have been developed already, which fall into two main categories: centralized and decentralized. The distinction is drawn based on whether the metaverse at issue is owned and ruled by a single entity, e.g., a company, or whether it is instead characterized by a dispersed network and decentralized ownership structure, e.g., a decentralized autonomous organization.

While, as stated, it appears reasonable to consider the treatment of Web 2.0 situations as reasonably settled, the transition from Web 2.0 to Web 3.0 has the potential to pose new challenges to the interpretation and application of the criteria discussed above. The present study is concerned

precisely with the legal treatment of such a transition. Specifically, this study seeks to answer the following questions: Can the same criteria and notions developed in relation to other dissemination *media* find application in the context of IPR infringements carried out through and within the metaverses? Does the distinction between centralized and decentralized metaverses have substantial implications insofar as the localization of IPR infringements is concerned?

The IPRs considered are copyright, trademarks and designs. The analysis is limited to infringements committed outside of contractual relations and adopts an international and comparative perspective, without focusing on any specific jurisdiction. While examples from different legal systems are provided and reviewed as appropriate, by choosing such an approach it is hoped that a lens is offered through which the main questions at the heart of the present study may be answered in terms that are as broad and helpful as possible to different legal systems. Also of relevance to the question of enforceability of IPRs online and on the metaverse is the consideration of the subjects against whom claims may be brought and their legal basis: in this sense, the alleged IPR infringement that requires localizing may not only trigger direct/primary liability but also the liability of subjects other than the direct infringer, including information society service providers whose services are used to infringe.

The study is structured as follows. Sections 1 and 2 detail the background to the present analysis, as well as its relevant objectives and approach. Section 3 addresses conflicts of laws issues. It reviews the relevant framework for the localization of IPR infringements in cross-border situations, having regard to international and regional instruments, as well as selected national experiences. This section further draws a distinction between unregistered and registered IPRs. Section 4 focuses specifically on digital and online situations and reviews academic and judicial discourse on localization approaches for the purpose of determining applicable law and, where relevant, jurisdiction. A discussion of the criteria based on causal event, targeting and accessibility – including their shortcomings – is also undertaken. Section 5 subsequently considers different types of subjects against whom infringement claims may be advanced, available remedies, and the type of resulting liability. Section 6 is specifically concerned with the different kinds of metaverse and determines whether the findings of the preceding sections may find satisfactory application in relation to this new *medium*, at least in principle.

Insofar as the main questions presented above are concerned, the one asking whether the same criteria and notions developed in relation to other media may find application in the context of IPR infringements carried out through and within the metaverses is answered in the affirmative. It is further submitted that the distinction between centralized and decentralized metaverses – while of substantial relevance to the determination of enforcement options – may not have significant implications insofar as the localization of IPR infringements is concerned.

Overall, this study offers as a main conclusion (Section 7) that, as things currently stand, the existing legal framework – as interpreted by courts in several jurisdictions in relation to Web 2.0 scenarios – appears to offer sufficiently robust guidance for the localization of IPR infringements, including those committed through the metaverse(s). All this is nevertheless accompanied by the caveat that substantial challenges might arise in terms of retrieving evidence that would serve to establish a sufficiently strong connecting factor with a given territory, for the purpose of both determining applicable law and jurisdiction. Furthermore, the diversity of remedies and enforcement options currently available across different jurisdictions begs the question whether the time has come for undertaking a more extensive harmonization of both aspects at the international and/or regional levels.

***

MAIN ABBREVIATIONS

AG	Advocate General
AI	Artificial intelligence
Brussels I recast	Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351, 20 December 2012, 1–32
CDPA	Copyright, Designs and Patents Act 1988
CDR	Community design right
CJEU	Court of Justice of the European Union
CR	Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, OJ L 3, 5 January 2002, 1–24
DAO	Decentralized autonomous organization
Digital Services Act	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC, OJ L 277, 27 October 2022, 1–102
DMCA	Digital Millennium Copyright Act
DSM Directive	Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17 May 2019, 92–125
Ecommerce Directive	Directive 2000/31/EC 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, OJ L 178, 17 July 2000, 1–16
Enforcement Directive	Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30 April 2004), OJ L 195, 2 June 2004, 16–25
EU	European Union
EUIPO	European Union Intellectual Property Office
EUTM	European Union trademark
EUTMR	Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification), OJ L 154, 16 June 2017, 1–99
FTA	Free-trade agreement
InfoSoc Directive	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, OJ L 167, 22 June 2001, 10–19
IPR	Intellectual property right
ISSP	Information society service provider
NFT	Non-fungible token
OCSSP	Online content-sharing service provider
P2P	Peer-to-peer
Rome II	Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations, OJ L 199, 31 July 2007, 40–49
UGC	User-generated content
UK	United Kingdom
USA	United States of America

CONTENTS

EXECUTIVE SUMMARY 4

MAIN ABBREVIATIONS 6

CONTENTS 7

1. SETTING THE SCENE: FROM WEB 2.0 TO WEB 3.0 AND THE METAVERSE 8

2. OBJECTIVES AND APPROACH OF THE STUDY 11

3. LOCALIZATION OF IPR INFRINGEMENTS IN CROSS-BORDER SITUATIONS: RELEVANT FRAMEWORK 13

   3.1. *Unregistered IPRs* 13

      3.1.1. International Framework 14

      3.1.2. The EU Experience 14

      3.1.3. Other National Experiences 16

   3.2. *Registered IPRs* 16

4. LOCALIZATION OF CROSS-BORDER IPR INFRINGEMENTS: THE ONLINE DIMENSION 19

   4.1. *Targeting* 20

   4.2. *Localization of the Alleged Infringement Under EU Law* 22

      4.2.1. Article 7(2) Brussels I Recast 22

      4.2.2. Article 125(5) EUTMR 23

5. TYPES OF INFRINGERS AND THEIR LIABILITY 25

   5.1. *From Safe Harbors to Primary/Direct Liability of Certain ISSPs* 26

   5.2. *Intermediaries as "Best Placed" to Bring Infringing Activities to an End* 28

6. LOCALIZATION OF IPR INFRINGEMENTS ON THE METAVERSE 31

   6.1. *Example 1: Copyright infringement* 31

   6.2. *Example 2: Trademark and design rights infringement* 33

   6.3. *Additional considerations: Centralized/decentralized metaverses and identification/localization of the direct infringer* 33

7. CONCLUSION 34

***

1. SETTING THE SCENE: FROM WEB 2.0 TO WEB 3.0 AND THE METAVERSE

> "From a technical point of view, the internet is a worldwide means of communication: a user can access any website from anywhere on Earth or transmit a message to a recipient who is located anywhere else. However, things look different from a legal perspective […]. Thus, there is a fundamental contradiction between the borderless and global nature of the internet on the one hand, and the territorially limited rights and obligations attached to various online activities on the other. There are two possible approaches to resolving this contradiction: we may attempt to "territorialise" the internet through geoblocking or to extend the territorial competence of the relevant authorities so that it covers more countries, thereby allowing those authorities to regulate online activities globally[1]."

It was in this way that Maciej Szpunar, First Advocate General (AG) at the Court of Justice of the European Union (CJEU), opened his Opinion in *Grand Production*, C-423/21, a referral for a preliminary ruling (eventually withdrawn[2]) on the allocation of liability under European Union (EU) copyright law for the circumvention of geoblocks. The "fundamental contradiction" highlighted by AG Szpunar has characterized Web 2.0, that is the second phase of the internet that started with the advent of peer-to-peer (P2P) technologies and social media networks and an overall more interactive user experience than Web 1.0. As will be explained, there is no reason to think that – at least in the short and medium term – it will not also characterize the ever more integrated reality of Web 3.0 (if we have not entered Web 4.0 already[3]) and the application and enforcement of intellectual property rights (IPRs) to *inter alia* the metaverse[4].

But will the advent of Web 3.0 challenge or even change how an IPR infringement is localized?

The importance of such a determination, which will be also illustrated by means of fictional scenarios tackling the infringement of both unregistered and registered IPRs in metaverse contexts, cannot be overstated: it is *inter alia* key to determining (i) whether the right at issue (e.g., a registered IPR) is enforceable at the outset, (ii) which law applies to the dispute at hand, as well as – in accordance with certain jurisdiction criteria – (iii) which courts are competent to adjudicate it.

To answer all this, it might be useful to make a further, preliminary observation. It stems from the answer to the following question: what do the printing press, the photocopying machine, the television, the Internet, three-dimensional printers, and the metaverse have in common? As it has been simply – yet effectively – observed, they are all *media* in the Latin meaning of the word: they are *means* to disseminate content, not different places in a geographic sense[5].

---

1 CJEU, Opinion of Advocate General Szpunar, *Grand Production*, C-423/21, EU:C:2022:818, paras 1-2.

2 CJEU, *Grand Production*, C-423/21, EU:C:2023:130.

3 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the Next Technological Transition*, 11 July 2023, COM(2023) 442.

4 For a discussion of the notion of metaverse, see M. Maciejewski, *Metaverse. Study requested by the JURI Committee* (European Parliament: 2023), PE 751.222, §1.1. and further below in this section. For a discussion of the notion of virtual worlds, see F. Di Porto – D. Foá, *Defining Virtual Worlds: Main Features and Regulatory Challenges* (July 2023), available at https://cerre.eu/wp-content/uploads/2023/07/CERRE-Virtual-Worlds-Issue-Paper-0723.pdf, 8-16.

5 Such a point was made in the context of the panel discussion on 'The Metaverse and NFTs: New Frontiers for Trademarks and Copyrights?' during the 30th Annual Intellectual Property Conference organized by the Emily C. and John E. Hansen Intellectual Property Institute at Fordham Law School (New York City, NY, USA) on 13-14 April 2023.

Historically, new *media* have entailed new ways to exploit content and immaterial assets understood broadly and, together with all that, infringe relevant rights vesting therein. Nevertheless, their advent has not required relevant principles and rules to be systematically rewritten anew each and every time. On the contrary, existing rules have often proved to be sufficiently – yet not necessarily unproblematically – adaptable to new and emerging *media*. All this has been the case having regard to both the applicability and enforceability of IPRs[6].

In terms of substantive principles and rules, legislatures and courts have consistently held IPRs applicable to the exploitation of protected subject-matter through new *media*. If we take copyright as an example, the 1996 WIPO Internet Treaties (WCT and WPPT) set down international norms aimed at preventing unauthorized access to and use of creative works on the Internet and/or other digital networks. Among other things, the WCT and WPPT *clarified* that pre-existing rights would continue to apply in the digital environment, including – but not necessarily limited to – the Internet. In turn, courts have consistently held exclusive rights enforceable in digital and online contexts. So, in interpreting Directive 2001/29[7] ("InfoSoc Directive") – by which the EU legislature implemented the WIPO Internet Treaties into the EU legal order – the CJEU has held both the relevant rights harmonized therein – reproduction, communication/making available to the public, and distribution – and exceptions and limitations thereto applicable in analog and online/digital contexts alike[8].

The same is true for jurisdictions that did not expressly transpose the rights mandated by the WIPO Internet Treaties: for example, US Congress did not amend US law to include explicit references to "making available" when it implemented the WIPO Internet Treaties through the adoption of the Digital Millennium Copyright Act 1998 (DMCA). Yet, the protection required under the making available right has been found to be substantially guaranteed in the context of digital on-demand transmissions through available (pre-existing) provisions of the US Copyright Act[9].

The considerations above apply to other IPRs too. So, the notion of "use" of a trademark for the purpose of establishing *prima facie* infringement has never been limited to analog uses only[10]. Similarly, courts have not restricted the enforceability of design rights to unauthorized uses solely in offline situations[11]. All this suggests that the conclusion above shall extend to Web 3.0 and the metaverse as a new *medium* of dissemination of content and other immaterial assets and, in turn, infringement of the IPRs vesting therein.

A term first used in the 1992 science fiction novel *Snow Crash* by Neal Stephenson, the metaverse has been relevant to at least some parts of our lives for a while already[12]. Over the past couple of years or so, the concept has been nevertheless revamped. All this has been prompted by technological advancements, including augmented reality, blockchain, the widespread availability of

---

6 In this sense, E. Rosati, 'IP and the metaverse: New problems, new rules?' (2022) 11/2022 Alicante News 1, 1-3.

7 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, *OJ L 167, 22.6.2001, 10–19.*

8 In greater detail, see E. Rosati, *Copyright and the Court of Justice of the European Union* (Oxford University Press:2023), 2nd edn, Chapters 5 and 6. See also the discussion in P. Mézei – G.C. Arora, 'Copyright and metaverse', in M. Cannarsa – L.A. Di Matteo (eds), *Research Handbook on Metaverse and the Law* (Edward Elgar: in press), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4444608, §3.2.

9 United States Copyright Office, *The Making Available Right in the United States: A Report of the Register of Copyrights* (2016), available at https://www.copyright.gov/docs/making_available/.

10 Recently see, e.g., CJEU, *Louboutin*, C-148/21 and C-184/21, EU:C:2022:1016. See also the discussion in, A Kotelnikov, 'Trade marks and visual replicas of branded merchandise in virtual worlds' (2008) 2008/1 Intellectual Property Quarterly 110, 122-128, regarding the applicability of trademark law to virtual worlds.

11 See, e.g., CJEU, *Nintendo*, C-24/16 and C-25/16, EU:C:2017:724.

12 An example is the gaming sector. Launched in the early 2000s virtual world platforms *The Sims* and *Second Life* are among the earliest applications of the metaverse: see https://www.ea.com/games/the-sims and https://secondlife.com/.

cryptocurrencies, artificial intelligence (AI) and the use of non-fungible tokens (NFTs) for digital assets[13]. Such developments could allow the transition to and fulfilment of the promises of Web 3.0, that is the possibility for builders and users to cooperate more closely than has been the case so far[14]. The "new" metaverse is hoped to be characterized by four main features: interoperability across networked platforms; immersive, three-dimensional user experience; real-time network access; and the spanning of the physical and virtual worlds[15].

Commentators have enthusiastically referred to the "new" metaverse as presenting "a once-in-a-generation opportunity to reinvent the consumer experience"[16] and enabling (together with AI and the rest of Web 3.0) "unprecedented business opportunities, impressive societal advancements and life-altering changes to how humans interact with the digital world"[17]. At the time of writing and with the seeming exception of metaverse engineers' salaries[18], such a promise appears however yet to be fulfilled[19].

For the present purposes, it is also important to highlight that the concept of metaverse does not refer to a single entity. Instead, different metaverses have been developed already[20], which fall into two main categories: centralized and decentralized. The distinction is drawn based on whether the metaverse at issue is owned and ruled by a single entity, e.g., a company, or whether it is instead

---

13 See also International Trademark Association, *White Paper – Trademarks in the Metaverse* (April 2023), available at https://www.inta.org/wp-content/uploads/public-files/perspectives/industry-research/20230406_METAVERSE_REPORT.pdf, 15-16. For a discussion of the potential use of NFTs in the field of entertainment, see F Teomete Yalabik, 'Future of NFTs in the entertainment industry: No longer the 'Wild West' of intellectual property law?' (2023) 14(1) European Journal of Law & Technology, available at https://ejlt.org/index.php/ejlt/issue/view/72, §3.

14 S. O'Neill, 'What's The Difference Between Web 1.0, Web 2.0, And Web 3.0?' (7.1.2022) LXA, available at https://www.lxahub.com/stories/whats-the-difference-between-web-1.0-web-2.0-and-web-3.0.

15 C.L. Saw – Z.W.S. Chan, 'The subsistence and enforcement of copyright and trademark rights in the metaverse' (19.5.2023) SMU Centre for AI & Data Governance Research Paper No. 03/2023, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4452938; International Trademark Association, *White Paper – Trademarks in the Metaverse* (April 2023), available at https://www.inta.org/wp-content/uploads/public-files/perspectives/industry-research/20230406_METAVERSE_REPORT.pdf, 13. See also: J.M. Garon, 'Legal implications of a ubiquitous metaverse and a Web3 future' 106 Marquette Law Review 163, 165-171; B.C. Cheong, 'Avatars in the metaverse: potential legal issues and remedies' (2022) 3 International Cybersecurity Law Review 467, 469; and the review of scholarly characterizations of the metaverse as contained in P. Mézei – G.C. Arora, 'Copyright and metaverse', in M. Cannarsa – L.A. Di Matteo (eds), *Research Handbook on Metaverse and the Law* (Edward Elgar: in press), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4444608, §1.

16 M. Purdy, 'Building a great customer experience in the Metaverse' (3 April 2023) Harvard Business Review, available at https://hbr.org/2023/04/building-a-great-customer-experience-in-the-metaverse.

17 B. Constantly, 'Convergence of Web3, AI and metaverse: Navigating the great reset for investors' (11.4.2023), Forbes, available at https://www.forbes.com/sites/forbesfinancecouncil/2023/04/11/convergence-of-web3-ai-and-metaverse-navigating-the-great-reset-for-investors/?sh=79594c8c4e7e.

18 J. Bote, 'Engineers for Meta's troubled metaverse reportedly paid 'mind-boggling' sums' (7 April 2023) SFGATE, available at https://www.sfgate.com/tech/article/metaverse-engineers-mind-boggling-pay-17885279.php; N. Nix, 'Meta paid VR developers salaries of up to $1 million. Facebook's owner is now in financial trouble.' (7.4.2023) The Washington Post, available at https://www.washingtonpost.com/technology/2023/04/07/meta-developer-salary-metaverse-investment/.

19 M. Harrison, 'Mark Zuckerberg abandons metaverse as shiny new toy appears' (7 April 2023) The Byte, available at https://futurism.com/the-byte/mark-zuckerberg-abandons-metaverse; J. Speakman, 'Is the metaverse on its last legs? Decentraland's free fall raises questions' (11 April 2023) Be in Crypto, available at https://beincrypto.com/metaverse-last-legs-decentralands-free-fall-questions/.

20 According to some reports, there would be approximately forty metaverses: see A. Cela, 'Is the structure of the metaverse centralized or decentralized? (7 December 2022) TechStar, available at https://www.techstar.it/en/blog/is-the-structure-of-metaverse-centralized-or-decentralized/.

characterized by a dispersed network and decentralized ownership structure, e.g., a decentralized autonomous organization (DAO)[21]. On centralized metaverses like Roblox or Fortnite, user-generated content (UGC) is owned and licensed by users to the platform operator in accordance with the platform's own terms of use[22], while in decentralized metaverses like Decentraland, no license is granted to the platform operators in relation to UGC (though such content must comply with the relevant platform's content policy)[23]. Furthermore, while the "corporate veil" entails that any legal liability of a company as a legal person is separate and distinct from any liability of its members, there appears to be no clear demarcation between the liability of a DAO and that of its members, with the result that the type of legal structure of a DAO appears to resemble that of a general partnership[24].

2. OBJECTIVES AND APPROACH OF THE STUDY

As stated, the application of substantive IPRs to different *media* is uncontroversial. Nevertheless, besides determining the appropriate scope of protection, an issue that has given rise to uncertainties when considering the enforceability of such rights in digital/online contexts is the one relating to the *localization* of alleged infringements thereof as a matter of substantive law. In this study, the localization of the infringement refers to the place in which the tort is deemed to occur as a matter of the substantive law applicable to the case. The localization of the infringement in this sense is relevant to the proof of liability (did the act complained of occur within the territorial extent of the substantive law?) and to the jurisdiction of the court (did the act complained of take place within the territorial jurisdiction of the court?). In all this, however, questions of applicable law and jurisdiction should not be conflated. Answering the former serves to ensure that a court does not have to apply more than one law, but rather only focus on the initial act of infringement to identify the law applicable to the proceedings. *Vice versa*, such a need to ensure that only one law is applicable does not exist in the context of jurisdiction rules, which frequently provide for more than one forum.

As will be detailed in what follows, in online contexts the divide between centralized and decentralized situations has given rise to uncertainties and contrasting answers; yet solutions have been identified over time which, substantially, present an overall homogeneity in terms of eventual outcomes. In this sense and as an example, targeting has emerged as a criterion to root jurisdiction in several countries with regard to both registered and unregistered IPRs. The localization of the alleged infringement has also enabled the establishment of the competence of the court seised in accordance with relevant criteria under regional (where applicable) and national law. For example, under EU law, the place of the event giving rise to the subsequent damage caused by the infringing activity – that is: where the infringing activity originated from – is one of the criteria to establish jurisdiction under Regulation 1215/2012 (Brussels I recast)[25]. The same is true under Article 5(3) of the Lugano Convention with regard to cross-border disputes between member states of the European Free Trade Agreement

---

21 I. Ogundare, 'Centralized vs decentralized metaverse: Complete guide' (16.2.2023) Coinspeaker, available at https://www.coinspeaker.com/guides/centralized-vs-decentralized-metaverse-complete-guide/; C. Ebun-Amu, 'What is a DAO? Decentralized autonomous organizations explained' (4.6.2021) Make Use Of, available at https://www.makeuseof.com/what-is-a-dao/.

22 See, e.g., clause 10 of ("Ownership of Roblox IP/UGC Created within an Experience") of Roblox's terms of use, available at https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use, and clause 5 ("User Generated Content") of Fortnite's end user license agreement, available at https://www.fortnite.com/eula.

23 See, e.g., clause 12.4 ("Ownership and management of LAND, Non-fungible tokens (NFTs) and Content created by users") of Decentraland's terms of use, available at https://decentraland.org/terms/.

24 This is the conclusion that the US District Court for the Southern District of California reached in *Sarcuni et al v bZx DAO, et al*, Case No.: 22-cv-618-LAB-DEB.

25 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351, 20 December 2012, 1–32.

Association[26]. Under both Regulation 2017/1001[27] (EUTMR) and Regulation 6/2002[28] (CR), the courts of the EU member state in which the act of infringement has been committed or threatened shall *inter alia* have jurisdiction in relation to proceedings concerning the alleged infringement of, respectively, an EU trademark (EUTM) or Community design right (CDR).

Considering all that precedes, the present study seeks to answer the following questions: Can the same criteria and notions developed in relation to other *media* find application in the context of IPR infringements carried out through and within the metaverses? Does the distinction between centralized and decentralized metaverses have substantial implications insofar as the localization of IPR infringements is concerned?

The IPRs considered are copyright, trademarks and design rights. The analysis is limited to infringements committed outside of contractual relations and adopts an international and comparative perspective, without focusing on any specific jurisdiction. While examples from different legal systems will be provided and reviewed as appropriate, by choosing such an approach it is hoped that a lens is offered through which the main questions at the heart of the present study may be answered in terms that are as broad and helpful as possible to different legal systems. Also of relevance to the question of enforceability of IPRs online and in the metaverse is the consideration of the subjects against whom claims may be brought and their legal basis: in this sense, the alleged IPR infringement that requires localizing may not just trigger direct/primary liability but also the liability of subjects other than the direct infringer, including information society service providers (ISSPs, also generally known as internet service providers or ISPs) whose services are used to infringe.

The study is structured as follows. Section 3 addresses conflicts of laws issues in general terms. To this end, it reviews the relevant framework for the localization of IPR infringements in cross-border situations, having regard to international and regional instruments, as well as selected national experiences. It draws a distinction between unregistered and registered IPRs. Section 4 focuses specifically on digital and online situations and reviews academic and judicial discourse on localization approaches for the purpose of determining the territorial aspects of liability and, where relevant, jurisdiction. A discussion of the criteria based on causal event, targeting and accessibility – including their shortcomings – is also undertaken. Section 5 subsequently considers different types of subjects against whom infringement claims may be advanced, available remedies, and the type of resulting liability. This overview will subsequently be relevant to the discussion of the growing role of intermediaries in the online IPR enforcement process and, with that, their likely perduring centrality in relation to infringements committed on the metaverse, including where the identity and localization of direct infringers proves challenging. Section 6 is specifically concerned with the different kinds of metaverse and determines whether the findings of the preceding sections may find satisfactory application in relation to this new *medium*, at least in principle. In identifying outstanding issues and – with those – directions for future policy and research work, Section 7 offers as a main conclusion that, as things currently stand, the existing legal framework – as interpreted by courts in several jurisdictions in relation to Web 2.0 scenarios – appears to offer sufficiently robust guidance to the localization of IPR infringements committed through the metaverse(s). All this is nevertheless accompanied by the awareness that substantial challenges might arise in terms of retrieving evidence that would serve to establish a sufficiently strong connecting factor with a given territory, for the purpose of both determining applicable law and jurisdiction[29]. Furthermore, the diversity of remedies

---

26 Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 339, 21 December 2007, 3–41.

27 Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification), *OJ L 154, 16 June 2017, 1–99*.

28 Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, *OJ L 3, 5 January 2002, 1–24.*

29 See also European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *An EU initiative*

and enforcement options currently available across different jurisdictions begs the question whether the time has come for undertaking a more extensive harmonization of both aspects at the international and/or regional level.

3. LOCALIZATION OF IPR INFRINGEMENTS IN CROSS-BORDER SITUATIONS: RELEVANT FRAMEWORK

A shared feature of IPRs, which is also clear considering the principle of independence of rights under several international instruments[30], is their territorial nature. In turn, the protection available in any given territory depends on the law of that territory, with regard to both substantive provisions and available remedies.

This said, the rather extensive international and (where relevant) regional and bilateral/multilateral (e.g., in the context of free-trade agreements (FTAs)) harmonization efforts undertaken over a prolonged period of time have had the effect of reducing the differences between national IPR regimes. Harmonization has occurred through the adoption of minimum standards of protection but also in the form of maximum harmonization or even unification.

IPR enforcement provisions have been harmonized too, though mostly on a *de minimis* basis. At the international level, a special mention is due to the 1994 TRIPS Agreement which, among other things, introduced detailed norms on enforcement of IPRs. The standards set in Part III of the TRIPS Agreement are minimum ones. As a matter of fact, following the adoption of the TRIPS Agreement, there has been a tendency towards exceeding the obligations it contains and adopting, as a result, TRIPS-plus IPR enforcement provisions[31]. Regarding enforcement, common rules have also been introduced at the regional level. In the EU, Directive 2004/48[32] (Enforcement Directive) lays down minimum standards concerning the enforcement of all IPRs, in the sense that it does not prevent individual EU member states from introducing or maintaining measures that are more protective[33].

Having regard to the IPRs with which the present study is concerned and considering relevant rules on the localization of infringements, a distinction to draw is that between unregistered (copyright, unregistered trademarks[34] and designs) and registered (registered trademarks and designs) IPRs.

3.1. UNREGISTERED IPRs

The present sub-section discusses the legal framework for cross-border infringements of unregistered IPRs. With a specific focus on copyright (though the same conclusions apply *mutatis mutandis* to

on Web 4.0 and virtual worlds: a head start in the next technological transition, 11 July 2023, COM(2023) 442, 10, noting that the metaverse might pose enforcement challenges.

30 Articles 4*bis* of the Paris Convention and 5(2) of the Berne Convention. See also the discussion in European Union Intellectual Property Office, *International Judicial Cooperation in Intellectual Property Cases. Study on Legislative Measures Related to Online Intellectual Property Infringements – Phase 2* (2021), available at https://op.europa.eu/en/publication-detail/-/publication/ea3f0ee0-86d1-11eb-ac4c-01aa75ed71a1, 29-30.

31 L. van Greunen – I. Gobac, 'Building respect for intellectual property – The journey towards balanced intellectual property enforcement' (2021) 24(1-2) Journal of World Intellectual Property 167, 169.

32 Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30 April 2004), OJ L 195, 2 June 2004, 16–25.

33 CJEU, *Stowarzyszenie "Oławska Telewizja Kablowa"*, C-367/15, EU:C:2017:36, para 23. Recently, see also CJEU, Opinion of Advocate General Szpunar in *Telia Finland*, C-201/22, EU:C:2023:400, para 1, noting how procedural aspects of enforcement remain subjected to heterogeneous national laws (and approaches) in the EU.

34 Article 6*bis* of the Paris Convention mandates protection of well-known marks, irrespective of their registration status.

other unregistered IPRs), the relevant legislative framework consists of international, (where applicable) regional and national legislation, with substantive and enforcement aspects being regulated at all levels.

3.1.1. International Framework

At the international level, the principal (though not only) legislative instruments governing copyright and, to a much lesser extent, its enforcement are the Berne Convention and the WIPO Internet Treaties.

First adopted in 1886 and revised multiple times (most recently in 1979), the Berne Convention is based on the three basic principles of national treatment, automatic protection and independence of protection. It also provides for several points of attachment – nationality, member state of residence of the author and place of first publication. It is commonly – though not uncontroversially[35] – understood that Article 5(2) of the Berne Convention adopts a *lex loci protectionis* (law of the place of protection) approach to the localization of copyright infringements[36].

The WIPO Internet Treaties set down international norms aimed at preventing unauthorized access to and use of creative works on the Internet or other digital networks. Both the WCT, which expressly requires compliance with Articles 1 to 21 of the Berne Convention, and the WPPT had as their key objective to update and supplement the then major existing WIPO treaties on copyright and related rights (respectively, the Berne Convention and the Rome Convention) primarily to respond to developments in technology and in the marketplace. As detailed above (Section 1), both instruments clarified that existing rights continue to apply in the digital environment and created new online rights, whilst allowing contracting countries to enjoy a certain flexibility in establishing exceptions or limitations to rights in the digital environment.

3.1.2. The EU Experience

At the EU level, harmonization of individual EU member states' laws on unregistered IPRs has occurred in relation to both substantive law (the requirements for and scope of protection) and conflict of laws / international private law rules determining jurisdiction and applicable law in cross-border infringement disputes. The former have been harmonized through both directives and regulations[37]. The latter have been generally harmonized through regulations. In terms of determination of the law applicable to the infringement of unregistered IPRs in situations arisen in tort, the *lex generalis* (general law) is found in Regulation 864/2007 (Rome II)[38]. Article 8(1) Rome II adopts a *lex loci protectionis* criterion to determine the applicable law in cross-border infringements of unregistered IPRs, thus derogating from the *lex loci damni* (law of the place of the damage) under Article 4(1) Rome II[39]. The approach mandated under Rome II is relevant to all unregistered IPRs.

---

35 M.E. Ancel – N. Binctin – J. Drexl – M. van Eechoud – J.C. Ginsburg – T.. Kono – G Lee – R. Matulionyte – E. Treppoz – D. Moura Vicente, 'International Law Association's Guidelines on intellectual property and private international law ("Kyoto Guidelines"): Applicable law' (2021) 12(1) JIPITEC 44, 45. See also J Lau, '(Let's) Playing by the rules: A choice of law rule for communication of copyright materials from video games to the public, through Let's Plays' (2023) 49 Computer Law and Security Review 1, 8-9.

36 See the discussion in S Ricketson – JC Ginsburg, *International Copyright and Neighbouring Rights. The Berne Convention and Beyond* (Oxford University Press:2022), 3rd edn, §§20.02-20.03.

37 Under EU law, a regulation is binding in its entirety and is directly applicable in all the member states of the EU. A directive is binding as to the result to be achieved by the member states, but leaves to the national authorities the choice of form and methods through national implementation (see Article 288 of the Treaty on the Functioning of the European Union (TFEU)).

38 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations, *OJ L 199, 31 July 2007, 40–49.*

39 On the difficulties of localizing the damage in Web 3.0 scenarios, see the discussion in Y El Hage – M Lehmann – E Prevost, 'Roundtable on the method of localisation in digital space' (2022) 2022/6 International Business Law Journal 725, 746-755.

Under EU law, the localization of the infringing activity may *also* serve to establish judicial competence. The relevant rules for unregistered IPRs and registered national IPRs are those contained in Articles 4 and 7(2) Brussels I recast. The general rule in Article 4 of the Brussels I recast is that "persons domiciled in a [EU] Member State shall, whatever their nationality, be sued in the courts of that [EU] Member State". The special rule contained in Article 7(2) provides, as an alternative, that "A person domiciled in a Member State may be sued in another Member State in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur". The purpose of EU law in this field is not to unify the procedural rules of the EU member states, but rather to determine which court has jurisdiction in disputes concerning civil and commercial matters in relations between EU member states and to facilitate the enforcement of judgments[40].

Over time, Article 7(2) Brussels I has received a fairly broad[41] and autonomous[42] – yet at times oscillating[43] – interpretation. Nonetheless, it is "settled case-law"[44] that the place where the harmful event occurred or may occur can be either the place where the damage occurred or the *place of the event giving rise to it*, so that the defendant may be sued – at the option of the plaintiff – in the courts for either of those places[45]. It is generally understood in the case law of the CJEU and scholarly literature that, where it is not possible to identify a single center of gravity, the focus should be on the event at the start, rather than that at the end of the story[46]. Some commentators have nevertheless suggested that, in situations in which the damage is delocalized, an appropriate localization criterion might be that of the country where the relevant website has its statistically largest audience[47]. That said, the choice of where to bring proceedings has *inter alia* implications for the damages that may be claimed: the CJEU has clarified that if one launches litigation in an EU member state other than the one of domicile/establishment of the defendant, i.e., the member state where the allegedly infringing

---

40 In this sense CJEU: *Nothartová*, C-306/17, EU:C:2018:360, para 28, referring to *Hypoteční banka*, C-327/10, EU:C:2011:745, para 37. Outside of these situations, determination of jurisdiction shall remain a matter of national law to be decided having regard to individual EU member states' private international law rules.

41 D. Jerker – B. Svantesson, *Private International Law and the Internet* (Wolters Kluwer:2012), 2nd edn, 257.

42 T. Kono – P. Jurĉys, 'General report' in T. Kono (ed), *Intellectual Property and Private International Law* (Hart:2012), 53.

43 *Ibid*, 53-54.

44 Recently, CJEU: *Gtflix Tv*, C-251/20, EU:C:2021:1036, para 27, referring to CJEU *Bolagsupplysningen and Ilsjan*, C-194/16, EU:C:2017:766, para 29 and the case law cited therein. For a summary of the current CJEU understanding of Article 7(2) Brussels I recast, see DJB Svantesson – I Revolidis, 'From *eDate* to *Gtflix*: Reflections on CJEU case law on digital torts under Art. 7(2) of the Brussels Ia Regulation, and how to move forward', in P. Alapanta – A. Anthimos – P. Arvanitakis (eds), *National and International Legal Space - The Contribution of Prof. Konstantinos Kerameus in International Civil Procedure* (Sakkoulas Publications:2022), pre-print available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4353065, §4.

45 CJEU: *Bier*, 21-76, EU:C:1976:166, para 19; *Shevill*, C-68/93, EU:C:1995:61, paras 20-21; *Zuid-Chemie*, C-189/08, EU:C:2009:475, para 23; *eDate Advertising*, C-509/09 and C-161/10, EU:C:2011:685, para 41; *Wintersteiger*, C-523/10, EU:C:2012:220, para 19; *Melzer*, C-228/11, EU:C:2013:305, para 25; *Pinckney*, C-170/12, EU:C:2013:635, para 26; *Kainz*, C-45/13, EU:C:2014:7, para 23; *Hi Hotel HCF*, C-387/12, EU:C:2014:215, para 27; *Coty Germany (anciennement Coty Prestige Lancaster Group)*, C-360/12, EU:C:2014:1318, para 32; *Hejduk*, C-441/13, EU:C:2015:28, para 18. See also the discussion in A Briggs, *Civil Jurisdiction and Judgments* (Routledge:2021), 267-268.

46 A. Briggs, *Civil Jurisdiction and Judgments* (Routledge:2021), 282.

47 Y. El Hage – M. Lehmann – E. Prevost, 'Roundtable on the method of localization in digital space' (2022) 2022/6 International Business Law Journal 725, 732-734, though the authors do not fully explain how such an audience is to be measured and what criteria are to be employed in this regard.

content is accessible, then the court thus seised is only competent to adjudicate on the damages occurred on that specific territory[48].

3.1.3. Other National Experiences

A position *substantially* in line with the EU experience reviewed above may be also found in other jurisdictions, including common law systems. In essence, while questions of applicable law are answered in the same way as in the EU given the implicit guidance in this sense in international instruments like the Berne Convention (see above at §3.1.1), jurisdiction in those legal systems may be established, first, in accordance with a personal jurisdiction criterion, which requires determining if the defendant is sufficiently connected to the place where the court is located (e.g., because they reside there[49]) so that the resulting decision – which would not necessarily be rendered under the law of the country where the court seised is located[50] – would be binding (and enforceable) upon them. Such a rule does not seem to differ in its underlying rationale from the jurisdiction criterion found in *inter alia* Article 4 Brussels I recast. Second, judicial competence needs to be rooted in a subject-matter criterion, which refers to the power of a court to decide in a matter depending on the nature of the claim or controversy brought before it[51]. Again, in its underlying rationale, such a criterion bears several points of resemblance with *inter alia* Article 7(2) Brussels I recast. All this said, the doctrine of *forum non conveniens* could also serve to establish jurisdiction with another court on grounds of efficacy and convenience, e.g., having regard to location of parties, witnesses, facts, and evidence (*including* where the infringing acts were committed), and the law(s) applicable to the dispute[52].

With specific regard to infringement claims under the US Copyright Act in which the alleged infringement presents an extraterritorial element, there is no clear consensus among US courts whether to analyze the extraterritoriality when determining jurisdiction or, instead, when assessing the substance of the claim. Views are divided regarding whether the allegedly infringing activity must or must not take place wholly within the US territory to determine substantive law and jurisdiction[53]. This said, federal courts have determined that it is an infringing performance under the Act to upload content onto a foreign website and subsequently direct the uploaded content to the US, e.g., by making such content available for viewing from the US[54].

3.2. REGISTERED IPRs

Like unregistered IPRs, for registered IPRs the criterion to use in choice of law determinations is a *lex loci protectionis* one which, in turn, complies with the territorial nature of IPRs. As stated, under EU law, the localization of the infringing activity may *also* serve to establish judicial competence. The relevant rules for unregistered IPRs and registered national IPRs are found in Articles 4 and 7(2) Brussels I recast. Specifically regarding registered IPRs, the type and extent of the protection afforded to them shall be in accordance with the law of the country where they were registered. To exemplify, a national trademark registration is governed by that country's trademark law. If one sought

48 *CJEU, Pinckney*, C-170/12, EU:C:2013:635, paras 44-47.

49 For example, in *Lucasfilm Limited and others v Ainsworth and another* [2011] UKSC 39, para 105, the UK Supreme Court found that English courts could exercise jurisdiction in a claim against persons domiciled in England for infringement of copyright committed in the USA in breach of US copyright law.

50 For example, in *Sony/ATV Music Publishing LLC & Anor v WPMC Ltd & Anor* [2015] EWHC 1853 (Ch) (01 July 2015), Arnold J. (as he then was) established the jurisdiction of the High Court of England and Wales over UK-based defendants but decided the substance of the dispute under US copyright law.

51 A. Bennett – S. Granata, *When Private International Law Meets Intellectual Property Law. A Guide for Judges* (WIPO:2019), available at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1053.pdf, 32.

52 See further W.F. Patry, *Patry on Copyright* (Thomson Reuters:2023), March 2023 update, §§17.209-17.210.

53 *Cf* the review of relevant authorities conducted in *Shropshire v Canning*, 809 F.Supp.2d 1139 (N.D.Cal., 2011), 1143-1147, and *IMAPizza, LLC v. At Pizza Limited*, 334 F.Supp.3d 95 (D.D.C., 2018), 117-118.

54 *Spanski Enterprises, Inc. v Telewizja Polska, S.A*, No. 17-7051 (D.C. Cir. 2018).

to obtain protection across multiple territories, generally speaking, they would need to take specific steps in this sense, e.g., through application for national registration in each of the territories concerned. A detailed discussion of the territorial elements of infringement is undertaken further below (Section 4).

Albeit not of direct relevance to locating infringements, it is furthermore important to recall that the extent of protection for the registered IPRs considered in the present contribution is linked to the relevant classes and goods and services designated within the Nice Classification and Locarno Classification. Insofar as trademarks are concerned, the protection available under the designated Nice classes may not automatically extend to, e.g., the metaverse. In Europe, for a trademark registration to be protected in relation to virtual goods and NFTs, it appears necessary to extend the registration to Class 9 of the Nice Classification and to do so with sufficient clarity and precision[55]. The most recent edition of the Nice Classification at the time of writing has also incorporated the term "downloadable digital files authenticated by non-fungible tokens [NFTs]" in Class 9[56].

In this context, two further observations may be made. On the one hand, it may not be guaranteed that protection already available for "real" goods extends to downloadable virtual goods[57]. On the other hand, courts in different jurisdictions – including the USA[58], Italy[59] and Spain[60] – have acknowledged the extension of the protection available for "real" goods to the digital version thereof,

---

55 The European Union Intellectual Property Office ('EUIPO') has indeed held that, while a designation for 'non-fungible tokens' or 'virtual goods' alone will not be sufficiently clear and precise, a designation for, e.g., 'downloadable virtual goods, namely, virtual clothing' shall be acceptable for the purpose of registration: European Union Intellectual Property Office (EUIPO), *Trade Mark Guidelines*, Edition 2023, Part B, Section 3, §6.25. While this approach appears shared across different jurisdictions, it may be too early to say if it will also entail a uniformity of approach in terms of filing and prosecution strategies worldwide: International Trademark Association, *White Paper – Trademarks in the Metaverse* (April 2023), available at https://www.inta.org/wp-content/uploads/public-files/perspectives/industry-research/20230406_METAVERSE_REPORT.pdf, 20-23.

56 For designs, the position of the EUIPO is that if the design at issue is for a product for a virtual environment only, including *inter alia* the metaverse, it is necessary for the applicant to indicate it as such. The design will then be classified in Class 14-04 of the Locarno Classification with the indication 'screen displays'. If the applicant seeks to protect their design for both a physical product and virtual environments, they shall indicate both the class which corresponds to the former and Class 14-04 as screen display: European Union Intellectual Property Office (EUIPO), *Designs for Virtual Environments* (2 March 2023), available at https://euipo.europa.eu/ohimportal/en/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/content/id/13510155.

57 See for example the decision of the Examination Division of the EUIPO of 8 February 2023 in relation to trademark application No. 018647205 for the sign:

58 *Hermès International, et al. v. Mason Rothschild*, 2023 WL 1458126 (S.D.N.Y., 2023).

59 Tribunale di Roma, ordinanza 20.7.2022, case No 32072/2022 (Italy), commented in E. Rosati, 'Can an NFT infringe one's own trade mark rights? Yes, says Rome Court of First Instance' (11 November 2022) The IPKat, available at https://ipkitten.blogspot.com/2022/11/can-nft-infringe-ones-own-trade-mark.html.

60 Juzgado de lo Mercantil Barcelona, AJM B 1900/2022 - ECLI:ES:JMB:2022:1900A, commented in M. Morán Ruiz, 'Can the owner of an artistic work convert it into an NFT for its use in the Metaverse?' (22 November 2022) The IPKat, available at https://ipkitten.blogspot.com/2022/11/guest-post-can-owner-of-artistic-work.html.

including in the context of unauthorized minting (that is: creation[61]) and commercialization of NFTs[62]. As mentioned above, early case law developed in Web 3.0 situations thus indicates that classification considerations have not had a bearing on the localization of IPR infringements and the enforceability thereof.

Like what Article 7(2) of the Brussels I recast stipulates in relation to *inter alia* national trademarks, for EUTMs Article 125(5) EUTMR provides that infringement proceedings (with the exception of actions for a declaration of non-infringement of a EUTM) may be brought "in the courts of the EU Member State in which the act of infringement has been committed or threatened"[63]. In any event, the courts of the EU member state in which the act of infringement is committed have jurisdiction only in respect of acts of infringement committed within the territory of that state (Article 126(2) EUTMR), with the result that the extent of the territorial jurisdiction of the court seised is narrower (including having regard to the damages that can be compensated) than if proceedings were brought, in accordance with Article 125(1) EUTMR, where the defendant is established or domiciled[64]. The question that arises is whether, despite the express inapplicability of Article 7(2) of the Brussels I recast to EUTM infringement actions, the concept of act of infringement within Article 125(5) EUTMR has the same meaning as place where the harmful event occurred or may occur within the former. In *Coty*, C-360/12, the CJEU answered this point in the negative[65]. It follows that the grounds for jurisdiction pursuant to Article 125(5) EUTMR are narrower than those within Article 7(2) Brussels I recast, since they only grant jurisdiction to the courts in the EU member state where the event giving rising to the damage occurred, not also those located in the EU member state where such damage produces its effects. Given that the wording used in Article 125(5) EUTMR also appears in the CR (Article 82(5)), such conclusion extends to CDRs.

Under US trademark law, it is worth noting that the US Supreme Court recently held that §1114(1)(a) and §1125(a)(1) of the Lanham Act are not extraterritorial and extend only to claims where the infringing use in commerce is domestic[66].

4. LOCALIZATION OF CROSS-BORDER IPR INFRINGEMENTS: THE ONLINE DIMENSION

Technological advancements and the increasing digitalization of content and related distribution channels, alongside the growing availability and affordability of reproduction devices, have facilitated

61 Amongst others, see A. Guadamuz, 'The treachery of images: Non-fungible tokens and copyright' (2021) 16(12) Journal of Intellectual Property Law & Practice 1367, 1368-1372, and K. Garbers-von Boehm – H. Haag – K. Gruber, *Intellectual Property Rights and Distributed Ledger Technology with a Focus on art NFTs and Tokenized Art. Study Requested by the JURI Committee* (European Parliament:2022), available at https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)737709, 15.

62 See also the discussion in C. Tenkhoff – P. Grotkamp – S. Burgess-Tate, 'Brands in the metaverse: The concept of 'interdimensional confusion' between the physical and the virtual space under EU trade mark law' (2023) 72(7) GRUR International 643, 647, considering it possible to establish similarity between 'real' and 'virtual' goods for the purpose of the confusion test under EU trademark law.

63 This, of course, implies an alternative forum to the other fora of Article 125, not that proceedings may be brought simultaneously in different courts: CJEU, Opinion of Advocate General Szpunar in *AMS Neve*, C-172/18, EU:C:2019:276, para 31.

64 CJEU, *AMS Neve*, C-172/18, EU:C:2019:674, para 39-40. The narrower jurisdiction conferred under Article 125(5) may be explained by considering the circumstance that, given the unitary nature of the EUTM system, when an EUTM is infringed, each EU member state may be the place where the infringement has occurred.

65 CJEU, *Coty*, C-360/12, EU:C:2014:1318, para 34.

66 *Abitron Austria GmbH v. Hetronic International, Inc*., 600 U.S. ---- (U.S., 2023), on which see M Chon – C Haight Farley, 'Trademark extraterritoriality: *Abitron v Hetronic* doesn't go the distance' (17 July 2023) Technology & Marketing Law Blog, available at https://blog.ericgoldman.org/archives/2023/07/trademark-extraterritoriality-abitron-v-hetronic-doesnt-go-the-distance-guest-blog-post.htm.

the dissemination and consumption of assets protected by IPRs, both lawfully and unlawfully. All this, in turn, has prompted a change in the way in which not only content is accessed and monetized, but also revenues are shared. To exemplify by reference to copyright, over the past few years, licensed Internet streaming has substantially grown, while sales of actual copies (whether in analog or digital format) have become less key[67]. From a rights perspective, all this has also led to a somewhat lesser emphasis on reproduction, and issues surrounding the communication and making available of content coming to the fore. Furthermore, with specific reference to revenue sharing, a global policy debate has emerged regarding both the relationship between Internet platforms and right holders and authors and performers and their contractual counterparts. Both have fed into reform discourses undertaken in multiple countries and at both national and regional levels[68].

In turn, all this has given rise to uncertainties insofar as IPR enforcement is concerned, including questions of localization of the relevant infringing activity. Nevertheless, over time, courts across different jurisdictions have managed to overcome these challenges and applied existing legal principles and rules in relation to new and emerging infringement modalities, including in the context of decentralized, e.g., P2P infringement scenarios.

In general terms, while the *lex loci protectionis* approach to conflicts of laws determinations has not resulted in too significant hurdles, determination of judicial competence in cross-border infringement situations has proved more challenging. Courts in different jurisdictions have nevertheless adopted three main criteria to determine their competence (i) accessibility: the court seised is competent if it is located in a country from which the allegedly infringing content is accessible[69]; (ii) causal event: judicial competence lies with the courts located in the territory where the defendant initiated the allegedly infringing conduct; (iii) targeting: courts located in the territory at which the allegedly

---

67 Insofar as the music industry is concerned, Internet streaming (both ad-supported streams and subscription audio streams) accounted for 67 percent of the overall revenues worldwide in 2022: see International Federation of the Phonographic Industry, *Global Music Report* (2023), available at https://globalmusicreport.ifpi.org/, 11. The growing relevance of Internet streaming may also be detected in the film sector: the 2021 global figures reveal that online video subscriptions (e.g., to Netflix and Amazon Prime) increased, surpassing the one billion mark in 2020 and growing 14 percent in 2021 to reach 1.3 billion: see Motion Picture Association, *2021 THEME Report* (2022), available at https://www.motionpictures.org/wp-content/uploads/2022/03/MPA-2021-THEME-Report-FINAL.pdf, 3. Insofar as audiovisual television, cinema, video and on-demand audiovisual services in Europe are concerned, the streaming market grew by 32% in 2021 compared to the previous year: European Audiovisual Observatory, *Yearbook 2022/2023 – Key Trends* (21 March 2023), available at https://www.obs.coe.int/en/web/observatoire/industry/key-trends, 50.

68 Besides the policy discourse that eventually culminated in the adoption of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17 May 2019, 92–125 ('DSM Directive') and its Articles 15, 17, and 18-23 in the EU, reference could be made to the *Economic of Music Streaming* inquiry in the UK (see https://committees.parliament.uk/work/646/economics-of-music-streaming/), the *News Media Bargaining Code* in Australia (see https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code), the US Copyright Office's studies on the functioning of Section 512 and copyright protections of press publishers (see, respectively, United States Copyright Office *Section 512 of Title 17 – A Report of the Register of Copyrights* (2020), available at https://www.copyright.gov/policy/section512/section-512-full-report.pdf, and United States Copyright Office, *Study on Ancillary Copyright Protections for Publishers* (2022), available at https://www.copyright.gov/policy/publishersprotections/), and also the recent Writers Guild of America and SAG-AFTRA strikes (see, e.g., E Batey, 'No end in sight for writers strike following Friday meeting' (5 August 2023) Vanity Fair, available at https://www.vanityfair.com/hollywood/2023/08/no-end-in-sight-for-writers-strike-following-friday-meeting, and M James – W Lee, 'Hollywood actors on strike, but many A-list celebrities still working. Inside side deals debate' (3 August 2023) Los Angeles Times, available at https://www.latimes.com/entertainment-arts/business/story/2023-08-03/actors-strike-sag-aftra-side-deals-independent-films-hollywood.

69 This was for example that approach that AG Szpunar recently recommended in his Opinion in *Grand Production*, C-423/21: CJEU, Opinion of Advocate General Szpunar in *Grand Production*, C-423/21, EU:C:2022:818, para 25.

infringing content is targeted have jurisdiction. All these criteria are flawed in some respects[70]. It should be nevertheless noted that targeting in particular has gained traction as a criterion to determine applicable law and jurisdiction in several jurisdictions and in respect of different IPRs. As such, it shall be discussed in greater detail below.

4.1. TARGETING

In relation to both registered and unregistered IPRs, in the absence of any internationally agreed approach[71], a criterion employed in different jurisdictions to localize alleged infringements in tortious situations for purposes of jurisdiction and applicable law has been the targeting of the defendant's activities towards a certain territory. In the EU, for example, targeting has been expressly employed by the CJEU to localize the infringement of copyright, the *sui generis* database right and trademarks (and, implicitly, designs too). Targeting is also a criterion expressly endorsed by *inter alia* the *lex generalis* contained in Regulation 2022/2065[72] (Digital Services Act) to extend the scope of application of that legislation to providers of intermediary services that are not established in the EU. A targeting approach is well established under the law of the UK and, with that, the IP laws of Commonwealth countries. US courts have also adopted a targeting approach in relation to personal jurisdiction, but do not appear to consider targeting in determining the location of the infringement as such when considering the substance of the claim[73]. A more detailed review of the EU and UK experiences is offered below.

Starting with the EU experience, in *Nintendo*, C-24/16 and C-25/16, the CJEU interpreted the notion of "country in which the act of infringement [of the intellectual property right at issue] was committed" as referring to the law of the country where the initial act of infringement, at the origin of the allegedly wrongful conduct, was committed or might have been committed. In the context of online infringements, that initial act consists of the act of activating the process of placing online the offer for sale of the infringing design[74].

---

70 For example, the accessibility criterion presents the risk of conferring jurisdiction even in situations in which no real damage has occurred on a certain territory, so that the relevant tort is virtually non-existent. The causal event criterion could prove challenging in situations in which there are multiple infringing activities and/or the origin of the infringing conduct is difficult to match to a certain territory. Targeting could result in multiple laws applying to the infringement at issue, with related risks of forum shopping. As such, a possible solution could be to follow an ubiquitous infringement rule modelled, e.g., on the Max Planck CLIP Principles (European Max Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Principles on Conflict of Laws in Intellectual Property* (2011), Article 3.603) and to allow the court seised to decide on remedies for infringing conducts occurred outside the country where the court has its seat. All this said, it should be acknowledged that none of the proposals advancing a ubiquitous infringement principle has been implemented yet. See further J. Lau, '(Let's) Playing by the rules: A choice of law rule for communication of copyright materials from video games to the public, through Let's Plays' (2023) 49 Computer Law and Security Review 1, 11-13, further advocating an interpretation of the *lex loci protectionis* principle as the place of incorporation of the plaintiff. But *cf* critically Y. El Hage – M. Lehmann – E. Prevost, 'Roundtable on the method of localization in digital space' (2022) 2022/6 International Business Law Journal 725, 730-732.

71 But *cf* Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet adopted by the Assembly of the Paris Union for the Protection of Industrial Property and the General Assembly of the World Intellectual Property Organization (WIPO) at the Thirty-Sixth Series of Meetings of the Assemblies of the Member States of WIPO September 24 to October 3, 2001, constituting an attempt to provide a framework for the application of existing industrial property laws relating to marks in online contexts. Of particular interest are Articles 2 and 3, concerning use of a sign on the Internet and the factors to consider to determine commercial effect on a given territory.

72 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC, OJ L 277, 27 October 2022, 1–102.

73 See, e.g., *Twentieth Century Fox Film Corp. v iCraveTV*, 2000 WL 255989 (W.D.Pa.); *Shropshire v. Canning*, 809 F.Supp.2d 1139 (N.D.Cal., 2011); *Crunchyroll, Inc. v. Pledge*, 2014 WL 1347492 (N.D.Cal., 2014); *Spanski Enterprises, Inc. v. Telewizja Polska*, S.A., 883 F.3d 904 (C.A.D.C., 2018).

74 CJEU, *Nintendo*, C-24/16 and C-25/16, EU:C:2017:724, paras 108 and 111.

That said, on multiple occasions in the IP field, including having regard to copyright and other (registered) IPRs, the CJEU has rejected such a causal event approach and opted instead for a targeting approach. This has been explicitly adopted, as stated, in relation to: (i) the EUTMR in *L'Oréal and Others*, C-324/09, in order to determine whether the committed acts - advertisement for sale and sale through a platform targeting EU-based consumers of infringing goods located in a third country – constituted an infringement under the EUTMR[75]; (ii) databases and the *sui generis* (database) right under Article 7 of Directive 96/9[76] in *Football Dataco and Others*, C-173/11[77]; (iii) the right of distribution under Article 4 of the InfoSoc Directive in *Donner*, C-5/11[78].

Proof of targeting of the public located in a specific member state could be inferred from, e.g., the existence of a certain language website, the content and distribution channels of the trader's own advertising materials and its cooperation with delivery service providers providing their services in a certain member state[79]. Besides other CJEU case law like *L'Oréal and Others*, C-324/09, which further details how targeting may be established (see below at §4.2.2), it is now clarified in the Digital Services Act that proof of targeting towards the EU territory could be obtained based on the factual circumstances at issue. Recital 8 provides that targeting of activities towards one or more EU member states can be determined based on several factors, including use of a language or a currency generally employed in that EU member state, or the possibility of ordering products or services, or the use of a relevant top-level domain. Targeting towards an EU member state could be also derived from the availability of an app in the relevant national app store, the provision of local advertising or advertising in a language used in that member state, or the handling of customer relations such as by providing customer service in a language generally used in that member state. The same recital also states that mere technical accessibility of a website from the EU cannot, on that ground alone, be considered as establishing a substantial connection to the EU territory.

Targeting has been employed as a criterion to localize the relevant infringing activity and, with that, establish the jurisdiction of the court seised in several other jurisdictions too. For example, courts in the UK and Commonwealth countries consider targeting a criterion that may be employed to localize the allegedly infringing activity.

In the copyright field, UK courts have consistently held that, even though the question of whether a website is targeted to a particular country is a multi-factorial one, which depends on all relevant circumstances[80], where a communication to the public originating outside the territory of the UK is received inside its territory and is targeted at its public, that act will be treated as occurring within the UK[81]. Recently, in *TuneIn*, the High Court of England and Wales, first, and, then, the Court of Appeal held that the operators of an online platform would be liable for undertaking acts of communication to the public without a license from concerned right holders because their service targeted and gave

---

75 CJEU, *L'Oréal and Others*, C-324/09, EU:C:2011:474. As is detailed below at §4.2.2, targeting has been subsequently upheld as a localization criterion specifically having regard to the international jurisdiction rule in Article 125(5) EUTMR.

76 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27 March 1996, 20–28.

77 CJEU, *Football Dataco and Others*, C-173/11, EU:C:2012:642, paras 32-34.

78 CJEU, *Donner,* C-5/11, EU:C:2012:370, para 27.

79 *Ibid*, para 29.

80 *Omnibill (Pty) Ltd v Egpsxxx Ltd & Anor* [2014] EWHC 3762 (IPEC) (17 November 2014), para 12, on which *cf* critically K. Frolova, 'The UK public is a titillating target: a case comment on *Omnibill v Egpsxx*' (2015) 37(6) European Intellectual Property Review 383, 387.

81 *EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2013] EWHC 379 (Ch) (28 February 2013), para 38.

access to UK-based users to Internet radio stations from around the world not licensed to operate in the UK[82].

UK courts have applied targeting in other fields of IP, including trademarks. For example, in *Merck*, the Court of Appeal of England and Wales referred specifically to the CJEU decisions in *Pammer*, C-585/08 and *L'Oréal and Others*, C-324/09 (see below at §4.2.2) and the circumstances indicated therein that could serve to establish targeting as referred to therein. Ultimately, the English court reasoned "that an offer for sale of goods bearing a trademark will amount to use of the trademark in the territory covered by the registered trademark and will fall within the exclusive right conferred by that registration if, having regard to all the circumstances, it may be concluded that the activity is targeted at consumers in that territory"[83]. Even after the completion of the UK departure from the EU, a targeting approach has been employed in *Lifestyle Equities* in relation to the Trade Marks Act 1994: there, the Court of Appeal of England and Wales clarified that targeting of the UK territory could be inferred from factors like consumers' perception[84], the intention to use a trademark, shipment availability, currency and language of the relevant website and details of import duties[85].

4.2. LOCALIZATION OF THE ALLEGED INFRINGEMENT UNDER EU LAW

It follows from the discussion above that the localization of the place of the alleged IPR infringement may also be employed as a jurisdiction criterion. This is true with regard to both registered and unregistered IPRs.

4.2.1. Article 7(2) Brussels I Recast

While the CJEU has had an opportunity to interpret the notion of place where the damage produces effect in relation to Article 7(2) Brussels I recast on a number of occasions in the copyright field[86], for the notion of "event giving rise to the damage" the CJEU has so far limited itself to holding that such a place cannot be considered as conferring jurisdiction to courts located in a member state in which the alleged infringer has not acted[87]. In *Hejduk*, C-441/13 the CJEU found that the event giving rise to the damage is where the activation of the process for the technical display of the allegedly infringing content is undertaken. In a case like the one at issue there, the acts, or omissions liable to constitute such an infringement could only be localized at the place where the defendant had its seat, since that is where the defendant took and carried out the decision to place the allegedly infringing reproductions online on a particular website[88].

Such an approach had been previously adopted with regard to national trademarks in *Wintersteiger*, C-523/10[89]. Overall, the CJEU suggested that the place where the event giving rise to the damage occurred would be the place where the alleged infringer is established. This is because such a place would *likely* be the place where the relevant act of infringement took place, relevant evidence may be

82 *Warner Music UK Ltd & Ors v Tunein Inc* [2019] EWHC 2923 (Ch) (01 November 2019); *Warner Music UK Ltd & Anor v Tunein Inc* [2019] EWHC 3374 (Ch) (18 December 2019); *Tunein Inc v Warner Music UK Ltd & Anor* [2021] EWCA Civ 441 (26 March 2021).

83 *Merck KGaA v Merck Sharp & Dohme Corp & Ors* [2017] EWCA Civ 1834 (24 November 2017), para 158.

84 The relevance of the consumers' perception was also upheld in CJEU, *Louboutin*, C-148/21 and C-184/21, EU:C:2022:1016, paras 44-48.

85 *Lifestyle Equities CV v Amazon UK Services Ltd* [2022] EWCA Civ 552.

86 CJEU: *Pinckney*, C-170/12, EU:C:2013:635; *Hi Hotel*, C-387/12, EU:C:2014:215; *Hejduk*, C-441/13, EU:C:2015:28.

87 CJEU, *Hi Hotel HCF*, C-387/12, EU:C:2014:215, paras 31-32.

88 CJEU, *Hejduk*, C-441/13, EU:C:2015:28, para 25.

89 CJEU, *Wintersteiger*, C-523/10, EU:C:2012:220, para 37.

retrieved, and proceedings may be conducted. Such a conclusion is in line with the Opinion of AG Cruz Villalón in the same case[90].

As discussed in greater detail elsewhere[91] and further below, such an approach is unconvincing because – besides the risk of "encouraging" those who undertake IPR-infringing activities on a commercial scale to relocate to countries which present greater barriers to an effective or even meaningful enforcement of copyright and related rights against them[92] – it flattens the special jurisdiction criterion onto the place of domicile/establishment of the defendant, thus failing to offer an alternative to the general jurisdiction criterion in Article 4 Brussels I recast. The shortcomings of limiting jurisdiction only to the courts located in the place of the causal event have been highlighted both by AGs Darmon[93] and Léger[94] and the CJEU in *Shevill*, with the latter highlighting how such an interpretation could render Article 7(2) "meaningless"[95]. In addition, with particular regard to online infringement cases, determination of the defendant's domicile/establishment may not always be a straightforward process[96]. This is why it is more appropriate to adopt a targeting approach also under Article 7(2) Brussels I recast, as the CJEU has done with specific regard to jurisdiction rooted within the place of infringement for EUTMs in Article 125(5) EUTMR.

4.2.2. Article 125(5) EUTMR

A targeting approach has been employed to localize the infringing activity and thus root jurisdiction within Article 125(5) EUTMR insofar as EUTMs are concerned. Given that the wording of Article 125(5) EUTMR is the same as Article 86(2) CR for CDRs, targeting shall also apply with reference to EU-wide design rights.

As early as *Coty*, C-360/12, the CJEU clarified that jurisdiction within Article 125(5) EUTMR is narrower than under Article 7(2) of the Brussels I Regulation recast, since only courts in the member state where the alleged EUTM infringement has been committed would have competence to adjudicate the relevant dispute. Simple accessibility of the allegedly infringing goods/services would not be enough, also due to the very language of the EU trademark instruments[97]. If accessibility from an EU member state was sufficient for advertisements displayed on an online marketplace that obviously targets solely customers in third countries to be within the scope of EU trademark law, this would result in an undue extension of the application of EU law[98]. All this said, the judgment in *L'Oréal and Others*, C-324/09 does not expressly and unambiguously address the question of jurisdiction linked to the place of the event giving rise to the damage. To this end, it is therefore necessary to consider the more recent decisions in *AMS Neve*, C-172/18 and *Lännen MCE*, C-104/22. Both employ a targeting approach.

In *AMS Neve*, C-172/18, the CJEU considered that an action for EUTM infringement may be brought before the courts of the EU member state where the consumers targeted by the allegedly infringing activity are located, irrespective of whether the activation process for the

90 CJEU, Opinion of Advocate General Cruz Villalón in *Wintersteiger*, C-523/10, EU:C:2012:90, para 26.

91 E. Rosati, 'International jurisdiction in online EU trade mark infringement cases: where is the place of infringement located?' (2016) 38(8) European Intellectual Property Review 482, 490-491.

92 Y. El Hage – M. Lehmann – E. Prevost, 'Roundtable on the method of localization in digital space' (2022) 2022/6 International Business Law Journal 725, 730.

93 CJEU, Opinion of Advocate General Darmon in *Shevill,* C-68/93, EU:C:1994:303, paras 42-58.

94 Opinion of Advocate General Léger in *Shevill,* C-68/93, EU:C:1994:303, paras 9-11.

95 CJEU, *Shevill*, C-68/93, EU:C:1995:61**,** para 27.

96 Y. Lahlou – L. Sinopoli – P. Guez, 'Chronicle of conflict of law in business matters' (2013) 3 International Business Law Journal 217, 220.

97 CJEU, *L'Oréal and Others*, C-324/09, EU:C:2011:474, para 64.

98 *Ibid*, para 64.

display of the goods/services at issue took place elsewhere (including outside of the EU)[99]. An interpretation according to which the event giving rise to the damage is where the alleged infringer set up their website and activated the display of their advertising and offers for sale would not be correct because it would establish jurisdiction of the courts where the defendant is based and thus render the jurisdiction criterion of (now) Article 125(5) ineffective[100]. The unlawful advertising for sale of goods/services must thus be regarded as taking place in the EU member state at which such activity is directed, irrespective of whether a sale has actually occurred[101]. Such a conclusion is further supported by the consideration that courts in that member state are particularly suited to assessing whether the alleged infringement does exist[102].

Subsequently, in *Lännen MCE*, C-104/22, the CJEU clarified the elements to consider to establish targeting and thus determine the competence of the court seised. For an advertisement of infringing goods/services to be targeted at a certain EU member state it is not required that such goods/services are expressly and unambiguously available for supply to consumers therein. Targeting may be also established having regard to other factors, insofar as they serve to prove "a sufficient connecting factor with the Member State in which the court seised of the infringement action is situated"[103]. There is no need for the court seised to examine the substance of the action during this phase[104]: "a reasonable presumption that acts of infringement may have been committed or threatened on the territory of a Member State is sufficient"[105].

As was held in *Pammer*, C-585/08 and C-144/09, consideration may be given to the following, non-exhaustive factors in order to establish targeting of the EU territory: the international nature of the activity; use of a language or a currency other than the language or currency generally used in the member state in which the trader is established; mention of telephone numbers with an international code; outlay of expenditure on an Internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other member states; use of a top-level domain name other than that of the member state in which the trader is established; and/or mention of an international clientele composed of customers domiciled in various member states[106]. Even in situations in which, as was the case here, it is not possible to determine the geographic areas of delivery of the goods/services at issue, a sufficient connecting factor may be the circumstance that the trader paid the operator of the local version of an Internet search engine to display paid advertisement[107].

---

99 CJEU, *AMS Neve*, C-172/18, EU:C:2019:674, para 49. Regarding the refusal of the CJEU to localize the infringing activity where the activation process was undertaken, *cf* critically L Lundstedt, '*AMS Neve and Others* (C-172/18): Looking for a greater 'degree of consistency' between the special jurisdiction rule for EU trade marks and national trade marks' (2020) 69(4) GRUR Int 355, 363, finding the eventual outcome appropriate in light of the earlier decision in L'Oréal and Others, C-324/09.

100 CJEU, *AMS Neve*, C-172/18, EU:C:2019:674, paras 50 and 51.

101 *Ibid*, para 54.

102 *Ibid*, para 57.

103 CJEU, *Lännen MCE*, C-104/22, EU:C:2023:343, para 36.

104 *Ibid*, para 37.

105 *Ibid*, para 39.

106 CJEU, *Pammer*, C-585/08 and C-144/09, EU:C:2010:740, para 93.

107 *Lännen MCE*, C-104/22, EU:C:2023:343, paras 48-50. *Cf* L Lundstedt, 'CJEU on jurisdiction over targeted Trade Mark Regulation' (8 May 2023), EAPIL Blog, available at https://eapil.org/2023/05/08/cjeu-on-

5. TYPES OF INFRINGERS AND THEIR LIABILITY

A further distinction that is relevant to draw for the purpose of the present analysis is that between different types of infringers and their liability. Enforcement initiatives may be obviously taken against direct infringers but also against ISSPs whose services are used to infringe IPRs. Insofar as the latter are concerned, an additional, twofold categorization is required.

The first concerns the type of liability of ISSPs arising because and as a consequence of users' infringing activities. In this sense, while several legal systems provide for "safe harbors" of ISSPs in relation to users' infringements, a recent trend in the IP field – especially in, but not necessarily limited to, the EU and the UK – is that of a greater responsibilization of certain types of ISSPs. As a result, in some jurisdictions an ISSP may no longer just be subjected to secondary/accessory liability in relation to UGC should the safe harbors be deemed inapplicable, but also primary/direct liability, thus excluding safe harbor availability at the very outset. The second distinction concerns the availability of injunctions against intermediaries irrespective of any legal liability on their side. Such a possibility does exist in several jurisdictions around the world.

Both aspects shall be concisely elaborated further in what follows as they are also relevant to the enforceability of IPRs in the metaverse, including in situations in which direct infringers are difficult to identify and/or locate, and so might be the localization of the infringing activity. In this sense, Web 3.0 will – if anything – exacerbate the problems already arisen in Web 2.0 situations in connection with user anonymity. An additional challenge in the context of infringing conduct undertaken in Web 3.0 and metaverse contexts is likely to relate to the very attributability of infringing conducts. For example, if one created an AI avatar of oneself by using OpenAI[108] and that avatar infringed third-party rights, who would bear liability? While OpenAI's terms of use provide a (partial) answer insofar as OpenAI's own liability is concerned by excluding liability arising out of products or services developed through or offered in connection with OpenAI's services[109], the liability of users of OpenAI for infringing activities undertaken by their own AI-based products is still very much uncharted territory[110].

Overall, when focusing on enforcement possibilities, including online, initiatives against direct infringers are not the only option. A number of elements – ranging from the already mentioned anonymity on the Internet and localization challenges to economic efficiency and effectiveness concerns – have led over time to an increasingly important role being played by ISSPs and intermediaries more generally. Furthermore, some of the options available by involving these subjects in the enforcement process could allow to overcome the territoriality of IPRs and the shortcomings that such a feature has given rise to. All this will be elaborated further below at §6.3 with specific regard to IPR localization and enforcement possibilities relating to the metaverse.

---

jurisdiction-over-targeted-actions-under-the-eu-trade-mark-regulation/, suggesting that – where ambiguous – a trader should take steps to 'extraterritoralize' their website and relevant offerings.

108 Snapchat influencer Caryn Marjorie recently did exactly that: her own CarynAI interacts with her fans on her behalf. See B Cost, 'I made a sexy AI robot of myself – You can date me for $1 a minute' (11.5.2023) New York Post, available at https://nypost.com/2023/05/11/influencer-turns-herself-into-sexy-ai-robot-you-can-date-for-1/. On the challenges of assigning legal responsibility to avatar owners, software coders or metaverse operators, see the discussion in F. Mostert – W.T. Yeoh, 'Meta-Worse, a lawyer's mega paradise' (2022) 17(3) Journal of Intellectual Property Law & Practice 211, 211-212.

109 See clause 7 of OpenAI's terms of use, available at https://openai.com/policies/terms-of-use.

110 Some commentators have nevertheless already advanced the view that liability of avatars might be separated from that of their creators through incorporation processes not dissimilar to those of a limited liability company: see the discussion in BC Cheong, 'Avatars in the metaverse: potential legal issues and remedies' (2022) 3 International Cybersecurity Law Review 467, 479-481.

5.1. FROM SAFE HARBORS TO PRIMARY/DIRECT LIABILITY OF CERTAIN ISSPS

In the second half of the 1990s, US Congress adopted two pieces of legislation – the Communication Decency Act of 1996 and the DMCA – which provide for a qualified insulation of ISSPs from the liability that would result from illegal activities carried out by users of their services. The system known as "safe harbors", including notice-and-takedown, has subsequently been introduced into many countries' legal systems, including in relation to IPRs.

For example, in 2000, the EU legislature adopted Directive 2000/31[111] (Ecommerce Directive), which provides that, in principle and insofar as certain conditions are satisfied, ISSPs are not liable for infringements committed by users of their services. In 2022, the EU legislature adopted the Digital Services Act. While being aimed at "ensuring a safe, predictable and trustworthy online environment" [112] also by means of due diligence obligations concerning the design and provision of online services, this regulation maintains and modernizes the safe harbor immunities already found in the Ecommerce Directive[113].

As stated, safe harbor provisions have been gradually introduced into the legal systems of several countries around the world. As a recent example, in 2023 Hong Kong reformed its law by introducing safe harbors for ISSPs in relation to copyright, including a notice-and-takedown regime[114]. It can further be observed that the adoption of DMCA-style safe harbors has found its way into certain legal systems as a result of the conclusion of FTAs and relevant legal obligations therein. For example, Australia's safe harbor provisions were introduced into the Copyright Act 1968 in 2004 to comply with that country's FTA with the USA[115]. As another example, in 2020, the United States-Mexico-Canada Agreement entered into force, replacing the 1989 North America Free Trade Agreement. As a result of the copyright provisions it contains, Mexico undertook a reform of its copyright law in 2020, *inter alia* introducing a notice-and-takedown system in part modelled on the DMCA[116].

Generally speaking, and as stated, the safe harbors are *qualified* immunities. In the US, liability of an ISSP eligible *in principle* for the safe harbors could subsist in accordance with the server test, as adopted by the 9th Circuit in *Perfect 10*[117]. Such a test requires considering where the infringing content is hosted: if it is hosted on the defendant's own server, then liability would subsist upon ruling out available defenses, e.g., fair use; if the content is instead hosted on a third-party server and is merely embedded or linked to by the defendant, then no liability could subsist. The server test was recently upheld in *Instagram*[118], in which the 9th Circuit concluded that such a test had not been effectively overturned by the US Supreme Court 2014 decision in *Aereo*[119] and confirmed that it is not limited in application to certain ISSPs (e.g., search engines) only. In all this, however, it should be also noted that some other recent case law has regarded the server test "settled law" in the 9th Circuit

111 Directive 2000/31/EC 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, OJ L 178, 17.7.2000, 1–16.

112 Recitals 3 and 12 of the Digital Services Act.

113 See further M. Husovec – I. Roche Laguna, 'Digital Services Act: A short primer' (18.7.2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4153796.

114 Copyright (Amendment) Ordinance 2022, Division IIIA (Sections 88A-88J).

115 See https://www.dfat.gov.au/trade/agreements/in-force/ausfta/official-documents/Pages/official-documents.

116 Ley Federal del Derecho de Autor, as reformed by Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal del Derecho de Autor (1.7.2020).

117 *Amazon.com, Inc*., 508 F.3d 1146 (9th Cir., 2007).

118 *Instagram, LLC*, No. 22-15293 (9th Cir., 2023).

119 *American Broadcasting Co. v. Aereo*, 573 U.S. 431 (2014).

but not necessarily elsewhere[120]. For example, the application of the server test was rejected in *Goldman*, a case concerning the liability of certain news publications as arising from embedding a photograph published by third parties on Twitter without the right holder's authorization. The US District Court, SD New York reasoned that "[t]he plain language of the Copyright Act, the legislative history undergirding its enactment, and subsequent Supreme Court jurisprudence provide no basis for a rule that allows the physical location or possession of an image to determine who may or may not have 'displayed' a work within the meaning of the Copyright Act"[121].

In the EU, the CJEU has premised the availability of the Ecommerce Directive safe harbors upon the condition that the ISSP at issue does not play an active role, which is such as to give it knowledge of or control over the infringing content[122]. In turn, where the relevant safe harbor is deemed inapplicable, liability of the ISSP could be established on a secondary/accessory/indirect basis. In the EU, this type of liability remains formally unharmonized: that means that it shall be a matter for individual EU member states to regulate[123]. That said, in 2017, the CJEU ruled for the first time that the operator of an Internet platform (*The Pirate Bay*) that facilitates the distribution of unlawful content could be held liable on a primary/direct basis for copyright infringement[124].

The CJEU subsequently clarified that the establishment of primary/direct liability of a platform operator under copyright depends on the consideration of several factors, which allow to conclude that the role of the platform operator is both indispensable and deliberate. Such factors relate to the consideration of whether the platform operator: (i) refrains from implementing appropriate technological measures that can be expected from a diligent operator in the specific circumstances at issue to counter copyright infringements on its platform *credibly* and *effectively*; (ii) participates in selecting protected content illegally communicated to the public; (iii) provides tools specifically intended for the illegal sharing of protected content or (iv) knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform. The mere circumstance that a platform operator has abstract knowledge that illegal content may be shared by its users is insufficient, and so is the circumstance that it operates on a for-profit basis. However, in either case, the assessment leads to a different outcome if a right holder has provided a specific notification and the platform operator has refrained from acting expeditiously to remove or disable access to that content[125].

In 2022, the CJEU further acknowledged the possibility of primary/direct liability *also* under trademark law with regard to an online marketplace that hosts listings for infringing products. Liability would stem from the business model adopted by the platform operator and would further require consideration of consumers' perception[126].

In parallel with the most recent judicial developments in the EU outlined above, in 2019 the EU legislature also adopted its DSM Directive. This contains a provision – Article 17 – that is premised on the consideration that certain types of ISSPs, which the DSM Directive refers to as online content-

120 See the review conducted in *Goldman v Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018), 591-592.

121 *Ibid*, 593.

122 CJEU: *Google France and Google*, C-236/08 to C-238/08, EU:C:2008:389, para 114; *L'Oréal and Others*, C-324/09, EU:C:2011:474, para 123. See also CJEU, *SNB-REACT*, C-521/17, EU:C:2018:639, para 52.

123 Recently, see the discussion in CJEU, Opinion of Advocate General Szpunar in *Louboutin*, C-148/21 and C-184/21, EU:C:2022:422, paras 78-79. See also F. Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar:2020), §§2.16-2.17.

124 CJEU, *Ziggo*, C-610/15, EU:C:2017:456.

125 CJEU, *YouTube*, C-682/18 and C-683/18, EU:C:2021:503.

126 CJEU, *Louboutin*, C-148/21 and C-184/21, EU:C:2022:1016.

sharing service providers (OCSSPs)[127], do directly perform copyright-restricted acts by hosting UGC and giving the public access to it. As a result, not only are they required to make best efforts to secure the authorization of relevant right holders to undertake such activities, but they are also ineligible at the outset for the hosting safe harbor immunity insofar as acts falling within the scope of application of Article 17 are concerned. According to some commentators, providers of virtual worlds like Linden (which runs *Second Life*) are likely to be classified as OCSSPs[128]. In turn, this suggests that the applicability of Article 17 of the DSM Directive to operators of metaverse platforms is not only possible but likely foreseeable.

5.2. INTERMEDIARIES AS "BEST PLACED" TO BRING INFRINGING ACTIVITIES TO AN END

Irrespective of both the applicability of the safe harbors and any liability of the intermediary at hand as discussed above at §5.1, in several countries around the world it is possible for right holders to apply for injunctions against intermediaries to bring infringing activities to an end and to prevent new infringements of the same kind from occurring. For example, in the EU[129] and the UK[130], intermediary injunctions are available in relation to both copyright and other IPRs. Under EU law, injunctions may be issued by courts or other competent authorities, e.g., administrative authorities[131]. In any event, the principles set in Article 3 of the Enforcement Directive need to be complied with[132]. The notion of "intermediary" itself is also both loose and broad. For an economic operator to be considered an "intermediary" and, as such, the addressee of an injunction, it is sufficient that they provide – even among other things – a service capable of being used by one or more other persons to infringe one or more IPRs[133].

The number of countries, including outside Europe, where injunctions against intermediaries are available is growing also because sometimes, as has been the case with safe harbors, FTAs mandate them[134]. The reason why intermediaries should be involved in the enforcement process through injunctions against them – and why this proves particularly helpful in the online context – is crystallized in recital 59 in the preamble to the InfoSoc Directive:

---

127 Article 2(6) of the DSM Directive defines an OCSSP as follows: 'a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organizes and promotes for profit-making purposes. See further E. Rosati, *Copyright in the Digital Single Market. Article-by-Article Commentary to the Provisions of Directive 2019/790* (Oxford University Press: 2021), 315-324.

128 This is so upon condition that recital 62 in the preamble to the DSM Directive is not given decisive normative weight: see B. Kinikoglu, 'Liabilities of virtual world developers as intermediary service providers: the case of *Second Life*' (2023) 13(1) Queen Mary Journal of Intellectual Property 121, 138.

129 Article 8(3) of the InfoSoc Directive; Article 11, third sentence of the Enforcement Directive.

130 Section 97A of the Copyright, Designs and Patents Act 1988 ('CDPA'); section 37(1) of the Senior Courts Act 1981.

131 On the rise of administrative online copyright enforcement models across the EU, see G. Frosio – O. Bulayenko, 'Website blocking injunctions in flux: Static, dynamic and live' (2021) 16(10) Journal of Intellectual Property Law & Practice 1127, 1131-1132, and A. Cogo – M. Ricolfi, 'Administrative enforcement of copyright infringement in Europe' in G. Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press: 2020), 586-610.

132 The provision requires that measures, procedures and remedies shall be fair and equitable and not unnecessarily complicated or costly, or such as to entail unreasonable time-limits or unwarranted delays. Furthermore, it is required that measures, procedures and remedies are effective, proportionate and dissuasive. They must be also applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.

133 CJEU, *Mc Fadden*, C-484/14, EU:C:2016:689, paras 41-42.

134 This is for example the case of New Zealand having regard to its FTAs with both the EU and the UK, as it is discussed in GW Austin, 'Legislating for site-blocking orders' (2023) New Zealand Law Review, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4393233.

> 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. (emphasis added)

The economic logic of granting injunctions against intermediaries such as Internet access providers is thus that they are the "lowest cost avoiders" of infringement[135]. Overall, this supports the idea – now also endorsed by the Digital Services Act – that voluntary implementation by intermediaries of content moderation systems is economically efficient[136].

Over time, courts in different jurisdictions have been imposing different types of injunctions against intermediaries, including de-indexing, payment freezing, disclosure obligations and website blocking orders.

De-indexing consists of requiring an Internet intermediary, e.g., a search engine, to delist infringing (piracy/counterfeiting) websites. This measure has the advantage of disallowing consumers from finding structurally infringing websites through search engines. Delisting leaves however the offending website unaffected[137].

Disclosure orders are another possibility. In the EU, it is possible to obtain the disclosure of information on a suspected infringer from an Internet intermediary under the framework of the Enforcement Directive, though the actual conditions and requirements vary significantly across EU member states[138], also because this piece of EU legislation – as stated – only contains measures of minimum harmonization[139]. The same result is achieved in the USA by obtaining third-party discovery in *John Doe* actions against the (unnamed) infringer[140].

Website blocking is considered, in a number of countries around the world, an enforcement method that can effectively target structurally infringing sites[141]. In 2011, the High Court of England and Wales utilized section 97A CDPA to grant the first injunction to block access to a structurally infringing website[142]. Since then, the High Court of England and Wales has ordered to block access to hundreds of websites, with applications being filed by a diverse group of copyright owners (including film studios, the recording industry, Football Association, Premier League, UEFA, publishers) targeting

---

135 Accordingly, 'it is economically more efficient to require intermediaries to take action to prevent infringement occurring via their services than it is to require right holders to take action directly against infringers': *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014), para 251.

136 For a (critical) discussion of intermediaries' proactive enforcement measures, see N. Elkin-Koren, 'After twenty years: revisiting copyright liability of online intermediaries', in S. Frankel – D Gervais (eds), *The Evolution and Equilibrium of Copyright in the Digital Age* (Cambridge University Press:2014), 45-48.

137 *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) (17 October 2014), paras 210-214.

138 See T. Riis – T. Elholm – A. Nordberg – S. Schwemer – K. Wallberg, *Study on Legislative Measures Related to Online IPR Infringements* (EUIPO:2018), available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Study_on_legislative_measures_related_to_online_IPR_infringements/2018_Study_on_legislative_measures_related_to_online_IPR_infringements_EN.pdf, 38-41, for the details of the types of measures available across the EU.

139 See, e.g., CJEU, *Constantin Film*, C-264/19, EU:C:2020:542.

140 See, e.g., *Strike 3 Holdings, Inc. v. Doe*, 2023 WL 3958405 (D.Mass., 2023).

141 United States Copyright Office, *Section 512 of Title 17 – A Report of the Register of Copyrights* (2020), available at https://www.copyright.gov/policy/section512/section-512-full-report.pdf, 58-61. Specifically on the EU experience, see J.B. Nordemann, 'Website blocking under EU copyright law', in E. Rosati (ed) *Routledge Handbook of EU Copyright Law* (Routledge:2021), 361-362.

142 *Twentieth Century Fox Film Corp & Ors v British Telecommunications Plc* [2011] EWHC 1981 (Ch) (28 July 2011).

different types of structurally infringing websites (including, more recently, cyberlockers and streamripping sites/apps[143]), and with the types of blocking orders sought evolving over time.

All this said, the availability of this remedy, which is granted against non-party Internet access providers, remains limited. Some jurisdictions have recently introduced it (the first website blocking order of this kind in Canada was issued in 2019[144]), but in others it remains unavailable (an instance being the USA[145]). It is important to note that website blocking orders may be granted by courts or other competent authorities, but there are also instances in which website blocking is the result of voluntary agreements between Internet intermediaries (notably Internet access providers) and right holders[146].

As stated, website blocking orders have undergone an evolution over time, and currently competent authorities in several jurisdictions have been granting, in addition to traditional website blocking orders: (i) dynamic injunctions, which order the blocking of an infringing website not only in relation to a specific domain name or IP address but also in relation to any further domain names or IP addresses under which materially the same website becomes available (mirror sites)[147]; and (ii) live injunctions, which require targeted intermediaries to block access not to a website but rather streaming servers giving unauthorized access to copyright works and other protected subject-matter for a period of time that corresponds to when the relevant content is being streamed[148].

---

143 Respectively, *Capitol Records & Ors v British Telecommunications Plc & Ors* [2021] EWHC 409 (Ch) (25 February 2021) and *Young Turks Recordings Ltd & Ors v British Telecommunications Plc & Ors* [2021] EWHC 410 (Ch) (25 February 2021), commented in greater detail in E. Rosati, 'High Court grants, for the first time, website blocking orders targeting cyberlocker and streamripping sites/app and considers that CJEU won't follow AG Opinion in *YouTube/Cyando*' (27.02.2021) The IPKat, available at https://ipkitten.blogspot.com/2021/02/high-court-grants-for-first-time.html, and Y.H. Lee, 'United Kingdom copyright decisions 2021' (2022) 53(3) International Review of Intellectual Property and Competition Law 396, 400-402.

144 *Bell Media Inc. v Goldtv.biz*, 2019 FC 1432.

145 United States Copyright Office, *Section 512 of Title 17 – A Report of the Register of Copyrights* (2020), available at https://www.copyright.gov/policy/section512/section-512-full-report.pdf, 193-196.

146 F. Mostert – J. Lambert, *Study on IP Enforcement Measures, Especially Anti-piracy Measures in the Digital Environment* (WIPO:2019), available at https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_14/wipo_ace_14_7-annex1.pdf, 18.

147 See, e.g.: Tribunale di Milano, ordinanze 11 June 2018 and 18 June 2018 (Italy); *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2018] EWHC 1828 (Ch) (18 July 2018) (UK); Patent- och marknadsöverdomstolen, PMT 13399-19 (Sweden). See also European Union Intellectual Property Office, *Illegal IPTV in the European Union* (2019), available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IPTV_in_the_European_Union_Full_en.pdf, 66 and, more recently, European Union Intellectual Property Office, *Study on Dynamic Blocking Injunctions in the European Union* (2021), available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Dynamic_Blocking_Injuctions/2021_Study_on_Dynamic_Blocking_Injuctions_in_the_European_Union_FullR_en.pdf.

148 In Europe, the first live injunction was issued in the UK: *The Football Association Premier League Ltd v British Telecommunications Plc & Ors* [2017] EWHC 480 (Ch) (13 March 2017). On the availability of dynamic injunctions in the EU, see further European Union Intellectual Property Office, *Study on Dynamic Blocking Injunctions in the European Union* (2021), available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Dynamic_Blocking_Injuctions/2021_Study_on_Dynamic_Blocking_Injuctions_in_the_European_Union_FullR_en.pdf, 39-41. See also European Union Intellectual Property Office, *IPR Enforcement Case-Law Collection - The Liability and Obligations of Intermediary Service Providers in the European Union* (2019), available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IPR_Enforcement_Case_Law_Collection/2019_IPR_Enforcement_Case_Law_Collection_en.pdf, 20-21.

Recently, the European Commission also released a recommendation detailing ways to combat illegal streaming of live events, in particular sport events. Building on relevant EU legislative instruments, the idea is to encourage EU member states and private parties to use the tools available in EU law to tackle the illegal online transmission of live content – including live blocking injunctions – more efficiently[149].

6. LOCALIZATION OF IPR INFRINGEMENTS ON THE METAVERSE

Having reviewed the main criteria for and approaches to the localization of IPR infringements and their application by courts in different jurisdictions in relation to Web 2.0 scenarios, this section considers whether and to what extent the existing guidance from legislation and, above all, courts may also be relevant for the localization of the place of infringement of the IPRs included in the present analysis as committed on different types of metaverse. To this end, two fictional scenarios are presented, the first concerning unregistered IPRs (copyright) and the second registered IPRs (trademarks and designs). For the sake of completeness, the analysis further encompasses the role that the online intermediaries referred to above in Section 5 could play in relation to IPR enforcement in Web 3.0 contexts and the metaverse.

6.1. EXAMPLE 1: COPYRIGHT INFRINGEMENT

A is an Italian national who resides in the UK and is the author of a photograph first published in the UK. A finds out that B, who resides in the USA, has shared a copy of A's work on the metaverse of company X, established in Japan, without A's authorization. The allegedly infringing copy may be viewed without particular territorial restrictions, including from the UK. What law shall govern the potential dispute between A and B and where could A take legal action against B?

In terms of applicable law, as discussed above at §3.1.1, the Berne Convention provides for several points of attachment, including nationality of the author, member state of the Berne Union where they reside and place of first publication of the work. In the present example, both Italian and UK laws are potentially applicable in accordance with such points of attachment: Italy is the country of which A is a national and the UK is the country where A resides and the work was first published. As things currently stands, it appears unlikely that the metaverse – as a new medium of content dissemination – will challenge or even question the applicability of substantive copyright provisions based on the Berne points of attachment[150].

Turning to the localization of B's *prima facie* infringing activity, the following appear to be the main possibilities, in line with the discussion in Section 4. First, B's activity may be localized – in accordance with a causal event criterion – where the allegedly infringing conduct, which appears at least to consist of an unauthorized reproduction and communication/making available of A's work to the public, originated. In this case, such a process might have occurred where B resides (USA) but might have also occurred elsewhere (for example, B was abroad when they shared the relevant content). If A chooses to sue B in the USA, there is clearly no bar as to personal jurisdiction, as B is resident within the jurisdiction. Under existing case law, it appears that B is sufficiently connected to the place where the court is located so that the resulting decision would be binding (and enforceable) upon them.

A second option might be to adopt an accessibility criterion: B's activity may be localized where the unauthorized copy of A's work may be accessed. As it appears that there are no restrictions to the

[149] European Commission, *Commission Recommendation of 4 May 2023 on Combating Online Piracy of Sports and Other Live Events*, Brussels, 4.5.2023, C(2023) 2853 final.

[150] *Cf* C.L. Saw – Z.W.S. Chan, 'The subsistence and enforcement of copyright and trademark rights in the metaverse' (19 May 2023) SMU Centre for AI & Data Governance Research Paper No. 03/2023, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4452938, §II.

visualization of the work in question, this implies that the place of infringement could be anywhere in the world.

A third option, which appears to be the most appropriate under Italian/EU and UK laws, also considering existing case law of the CJEU, consists of localizing the *prima facie* infringing activity of B in the country at which such activity is targeted. Under both UK and EU law, targeting may serve as a criterion to determine both the applicable law and jurisdiction of relevant courts. As discussed above, what is required to this end is the establishment of "a sufficient connecting factor" with the territory where the court seised is located, in order to reasonably presume that the *prima facie* infringing activity may be localized therein. In this sense, a non-exhaustive list of factors could contribute to establishing targeting, including the language and currency used (in this sense, the combination of a language spoken *and* currency used in one country – e.g., English and British pound sterling – would make it rather straightforward to establish targeting of the UK territory as opposed to, e.g., the use of Italian as a language and the Euro as a currency insofar as the Italian territory is concerned), local top-level domains, telephone numbers with an international code, availability of the relevant app in the national app store, content of any advertising activity undertaken by the infringer, etc.

Proof of targeting shall depend on the circumstances at issue and shall be ultimately a matter of fact. While an infringement committed on the metaverse could present some additional challenges compared to a Web 2.0 scenario – for example having regard to the use of AI avatars, cryptocurrencies, automatic translation tools, lack of local top-level domains or a physical shipping destination – as things currently stand, there seems to be still room to identify suitable connecting factors that would ultimately serve to establish targeting. For example, despite automatic translation tools, it is possible to choose a primary language for one's own metaverse experience when creating an account and many security questions are premised on the connection between the user and a territory[151]. Another consideration is that cryptocurrencies need to be purchased by using "traditional" currencies and are subject to a conversion rate[152]. Furthermore, the app of a particular metaverse platform would need to be downloaded/purchased from a local app store. All this suggests that, by undertaking a multi-factor assessment, it remains possible *in principle* to identify one or multiple territories targeted by the alleged infringer.

All the above indicates that a *lex loci protectionis* criterion paired with a targeting approach could also lead to the localization of the place of infringement in situations in which an unregistered IPR is *prima facie* infringed on the metaverse. In turn, the localization of the place of infringement could also serve to establish the jurisdiction of the court seised.

In all this, it is relevant to recall that where to seek protection in accordance with the *lex loci protectionis* criterion and where to sue, e.g., by deciding to seize the court of the place of infringement in lieu of the court of the place where the defendant is domiciled/established or where the damage is felt, have very substantial implications. In terms of substantive law, there might be differences in terms of, e.g., available defenses and exceptions and limitations to copyright. In terms of judicial competence, there might be different possibilities in terms of remedies and available damages. Although not relevant to the present example given the lack of EU domicile/residence of B, it is worth recalling that, in light of existing CJEU case law and as detailed above, deciding to bring proceedings before the court where the damage produces effect (in accordance with Article 7(2) Brussels I recast) instead of seising the court

151 So, when creating an account on *Second Life*, security questions include: 'What city were you born in?' or 'What street did you grow up on?'

152 For example, *Second Life*'s Linden Dollars may be purchased on Second Life subject to market rates. See https://tinyurl.com/32b862sh. On 3 May 2023, L$ 1 corresponded to USD 0.01. When undertaking relevant transactions, users of *Second Life* are also informed that the LindeX exchange will automatically match your order with the market rate that will fulfil the most quickly, based on the number of L$ you wish to buy.'

of the EU member state where the defendant is domiciled/established means that, in the former case, the plaintiff shall only recover the damages suffered on the territory where the court is located. *Vice versa*, no limitations in terms of damages subsist should one sue in accordance with the general jurisdiction criterion under Article 4 Brussels I recast.

6.2. EXAMPLE 2: TRADEMARK AND DESIGN RIGHTS INFRINGEMENT

Brazilian company A is the owner of a registered CDR and a registered EUTM. A finds out that company B, established in India, has made available for sale on the metaverse of company Z, established in Australia, virtual clothing that appears to infringe A's design right and also carries a sign identical to A's trademark. Where could A sue B and what law would govern the resulting dispute with B?

As detailed above, in the case of registered IPRs the applicable law is determined according to where the relevant right is registered. The scope of the protection afforded under designs and trademarks shall also depend on the relevant goods or services designated under relevant classes in the Locarno and Nice Classification, respectively.

In relation to infringing activities carried out via the Internet, courts in different jurisdictions have adopted a targeting approach. As it has been detailed above (Section 4), targeting may be established through a variety of factors. The establishment of a sufficient connecting factor serves to determine the jurisdiction of the court seised. In the EU, that would be so having regard to the interpretation of the relevant international jurisdiction criterion in Articles 125(5) EUTMR and 86(2) CR. Both allow infringement proceedings to be brought "in the courts of the Member State in which the act of infringement has been committed or threatened". This means that, if A so wished, it could sue B in the EU. Unlike Brussels I recast, the jurisdiction conferred under Article 125(5) EUTMR is not limited to defendants domiciled in the EU. In any event, the courts of the EU member state in which the act of infringement is committed would have jurisdiction only in respect of acts of infringement committed within the territory of that state, with the result that the extent of the territorial jurisdiction of the court seised is narrower than if proceedings were brought where the defendant is established or domiciled in accordance with Article 125(1) EUTMR/86(1) CR.

It follows from the foregoing that A could bring proceedings for *prima facie* infringement of its CDR and EUTM in *inter alia* any EU member state at which B's conduct is targeted, irrespective of the circumstance that B is established in India. Even though the rights at issue are unitary in character, with the result that they might be infringed anywhere in the EU, a court seised based on the "place of the infringement" criterion would only have competence to award the damages to compensate the prejudice suffered on the territory where that court is located. Ultimately, as with the previous example, proof of targeting would be key. Importantly, as IPRs like those at issue in this example are protected where they are registered, for A to be able to enforce its rights, it is necessary that protection is invoked for the relevant territory (in this case: the EU).

6.3. ADDITIONAL CONSIDERATIONS: CENTRALIZED/DECENTRALIZED METAVERSES AND IDENTIFICATION/LOCALIZATION OF THE DIRECT INFRINGER

Would it make a difference if the metaverse on which the unlawful activities referred to in Examples 1 and 2 above have been committed was decentralized (instead of centralized) and/or the infringer could not be identified or located?

As seen throughout the present analysis, in the past, the circumstance that infringing activities were committed in decentralized settings, e.g., P2P file-sharing networks, did not prevent courts in several jurisdictions to declare their judicial competence and adjudicate the actions brought before them. It is therefore submitted that the circumstance that a certain reality – whether of Web 2.0 or Web 3.0 – is decentralized shall not entail the inapplicability of substantive IPRs and/or prevent the enforceability thereof. In any event, as seen above with regard to realities like DAOs, a legal separation between members' personal liability and the

entity's own liability might not subsist, with the result that the former might potentially bear liability for infringements committed by the latter or other members thereof.

In a centralized situation (as it is in the examples for companies established, respectively, in Japan and Australia), it appears that the entity in charge of it – for example, a corporate entity – could be held liable for users' infringing activities subject to substantially the same considerations undertaken above at §5.1. In this sense, in situations in which the type of liability potentially subsisted on a secondary/indirect/accessory basis, it would be necessary to determine the applicability (if available in principle) of the relevant safe harbor. In situations in which liability subsisted in principle on a primary/direct basis, the relevant requirements for such a liability to subsist would need to be determined. With specific regard to NFT-trading platforms, it should be noted that their liability has been already established in some jurisdictions[153].

Furthermore, as seen above at §5.2, irrespective of any liability thereof, in several jurisdictions around the world it is possible to request injunctions against intermediaries to bring existing infringements to an end and prevent new infringements of the same kind from occurring. In this sense, as stated, the notion of intermediary is loose and broad; in turn, any provider of a service that is used to infringe could be the addressee of an injunction, including Internet access providers, domain name registrars, search engines, hosting providers (websites, social media, websites, online marketplaces, etc.), payment providers, etc. As access to and use of a metaverse will require an active Internet connection (at least in principle), as is the case for Web 2.0 situations, injunctions against intermediaries (including Internet access providers) will remain available to right holders seeking to bring infringing activities to an end and prevent new infringements of the same type from occurring, irrespective of where the relevant IPR infringement may be localized.

Insofar as the position of direct infringers and the localization of their infringing activity is concerned, it thus follows that the type of metaverse at issue – centralized or not – would not necessarily make a substantial difference in this respect. If the approach taken to localize the infringing activity is based on an accessibility or targeting criterion, then the circumstance that the infringer may not be identified or located[154] – while potentially relevant to the range of enforcement options available – would not prevent the relevant IPR infringement from being localized and, with that, allow the concerned right holder to take suitable enforcement initiatives.

7. CONCLUSION

This study has sought to answer the following questions: Can the same criteria and legal fictions developed in relation to other dissemination *media* find application in the context of IPR infringements carried out through and within the metaverses? Does the distinction between centralized and

---

153 This has been the case, for example, in China in *Shenzhen QiCeDieChu Cultural and Creativity Co v Hangzhou Bigverse Technology Co.* (2022), Hangzhou Internet Court Civil, First Judgment No. 1008, 20 April 2022, discussed in B. Xiao, 'Chinese court rules on NFT transactions and responsibility of trading platforms' (2022) 17(8) Journal of Intellectual Property Law & Practice 604, 605-606. For a European perspective on the potential liability of NFT marketplace platforms' operators, see B. Bodó – A. Giannopoulou – P. Mezei – J.P. Quintais, 'The rise of NFTs: these aren't the droids you're looking for' (2022) 44(5) European Intellectual Property Review 267, 278-280.

154 *Cf* M. Ryan, 'Intellectual property considerations and challenges in the metaverse' (2023) 45(2) European Intellectual Property Review 80, 83, noting that the identification of the direct infringer in the context of an infringing activity carried out on the metaverse may turn out to be 'one giant obstacle'.

decentralized metaverses have substantial implications insofar as the localization of IPR infringements is concerned? As seen, the first question may be generally answered in the affirmative, while the second question appears to warrant an answer in the negative.

The analysis has shown that existing principles and rules have proved to be sufficiently adaptable over time to address and be applied to new and emerging exploitation and infringement modalities. This leads to conclude that the same is likely to prove true – at least in general terms – having regard to Web 3.0 situations and the metaverse. After all, "[i]n answering questions with previously uncontemplated technologies [a c]ourt must not be distracted by new terms or new forms of content, but turn instead to familiar guiding principles"[155].

This said, infringing activities carried out on the metaverse have the potential to raise specific challenges in terms of localization of the relevant IPR infringement, at least at an evidentiary level. Not only do Web 3.0 and the metaverse have the potential to make the identification and localization of direct infringers more complex, but – as explained – the very attributability of infringing conducts (for examples infringing activities undertaken by AI avatars) may raise significant questions. Nevertheless, such challenges are not entirely unprecedented: if we take the position of ISSPs, the progressive evolution of business models has been accompanied by an evolution of the type of liability that could be attributed to, e.g., operators of hosting platforms – whether in relation to copyright or trademark infringements carried out by users/sellers or the availability for sale of NFTs. The same has occurred with regard to the types of injunctions available against "innocent" intermediaries. Another point of reflection is the interplay between state-mandated and private enforcement of IPRs. If the "new" metaverse becomes a fully integrated reality, the question of whether and to what extent private companies may enforce their own terms of use has the potential to become even more relevant and pressing than it has been so far[156].

Decentralized contexts give rise to specific challenges too, but once again not entirely unprecedented. As seen, the applicability of IPRs and the localization of relevant infringements has already come before courts in relation to P2P file-sharing situations in several jurisdictions around the world. As such, the questions of interpretation that decentralized metaverses pose may not be entirely novel. This said, a greater reflection regarding the legal nature of DAOs and the type of liability that can be attributed to their members in relation to infringing conduct undertaken by others within the organization appears warranted.

On a broader policy and legislative level, the progressive advancement of digital and Internet-based technologies has resulted in the "fundamental contradiction" that AG Szpunar referred to in his Opinion in *Grand Production*, C-423/21. It is unlikely that the advent of Web 3.0 and the "new" metaverse will change this. In all this, a key question remains: should a more even and better integrated level playing field for the exercise and enforcement of IPRs be guaranteed, also considering that – specifically regarding enforcement tools – the level of harmonization at the international and, where available, regional level is mostly based on a *de minimis* approach? That – it is submitted – is a key issue. The transition from Web 2.0 to Web 3.0 and the realization of a fully integrated metaverse have made such a question one the answer to which could and should not be delayed much longer.

***

155 *Goldman v Breitbart News Network, LLC*, 302 F.Supp.3d 585 (S.D.N.Y. 2018), 586.

156 See, e.g., the discussion in F. Mostert, 'Free speech and internet regulation' (2019) 14(8) Journal of Intellectual Property Law & Practice 607, and J. Cooper, 'Why we need "meta jurisdiction" for the metaverse (12 February 2021) The Hill, available at https://thehill.com/opinion/technology/583529-why-we-need-meta-jurisdiction-for-the-metaverse/.

World Intellectual Property Organization
34, chemin des Colombettes
P.O. Box 18
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 338 91 11
Fax: + 41 22 733 54 28

For contact details of WIPO's
External Offices visit:
www.wipo.int/about-wipo/en/offices