THE RESPECT FOR FREEDOM OF EXPRESSION AND THE EXERCISE OF STATE JURISDICTION ONLINE IN INTERNATIONAL HUMAN RIGHTS LAW

SARA SOLMONE

A thesis submitted in partial fulfilment of the requirements of the University of East London for the degree of Doctor of Philosophy

Royal Docks School of Business and Law

September 2020

ABSTRACT

This thesis focuses on the exercise of State jurisdiction online and the fulfilment of freedom of expression in the cyberspace. In particular, the thesis aims to answer the following research questions: when and under what conditions can online acts be considered to have happened within a State's jurisdiction according to human rights law? Is the extraterritorial exercise of State jurisdiction to regulate online content compliant with the freedom of expression provisions contained in human rights law? These questions are investigated through the analysis of key domestic Internet-related cases where States have exercised jurisdiction over cross-border online content extraterritorially. This analysis highlights the negative implications of these extraterritorial exercises of State jurisdiction on freedom of expression online. On the other hand, the thesis investigates the meaning of State jurisdiction online according to the European Convention of Human Rights, the American Convention of Human Rights, the African Charter on Human and Peoples' Rights and the International Covenant on Civil and Political Rights. The aim of this analysis is to understand how the jurisdictional models developed by the human rights courts work in an online environment. The analysis highlights the difficulties presented by the application of the spatial and personal models of jurisdiction to online acts and investigates the extraterritorial effects model, which might be better suited to deal with online acts. Finally, the thesis explores whether the extraterritorial exercises of State jurisdiction examined in the first part of the thesis are compliant with the accessibility and foreseeability requirements of the 'prescribed by law' criterion of the human rights conventions. The analysis of this point concludes that, although the domestic laws authorising these exercises of jurisdiction are compliant with these requirements, their interpretation by the Courts should evolve to take into account the special, borderless nature of online content.

ACKNOWLEDGMENTS

I would like to thank the members of my supervisory team for their help throughout the PhD. I was fortunate enough to be supported by two brilliant academics, two strong, professional, and empathetic women, Prof. Chandra Sriram and Dr Edel Hughes, who provided me with insightful academic feedback and helped me complete the thesis. Chandra, your emphasis on the importance of "finding my voice" and your insightful feedback have helped me greatly. Just like all those who knew you, I am deeply saddened that our time together ended so soon. Thanks for all your help. I miss you.

Edel, I will never be able to thank you enough for your help and support throughout the PhD, especially this last part. Your academic expertise, your encouragements and your empathy have helped me very much. It has been a pleasure to work with you and I will miss greatly our coffee meetings at the British Library.

I would also like to thank my Director of Studies, Barry Collins, and Dr Annalisa Meloni. Annalisa, thanks for your feedback on the thesis, your input and for always being available when I needed someone to talk to.

Special thanks to my parents and my friends, my chosen family, Lino, Gaby-Ann, Mary and Miky, for supporting me through thick and thin.

Finally, thanks to my husband, Antonio, who has been putting up with me for 15 years. I truly could not have completed the PhD without you unwavering love and support. I love you.

DEDICATION

To the tiny human growing inside my belly. I love you so much. This thesis is for you.

'È per te il profumo delle stelle
È per te il miele e la farina
È per te il sabato nel centro
Le otto di mattina
È per te la voce dei cantanti
La penna dei poeti
È per te una maglietta a righe
È per te la chiave dei segreti
È per te ogni cosa che c'è ninna na, ninna eh
È per te ogni cosa che c'è ninna na, ninna eh'

Lorenzo Cherubini, Per te

1. Introduction

This thesis focuses on the exercise of State jurisdiction online and on the fulfilment of freedom of expression in the cyberspace. This chapter will introduce the research questions and objectives, illustrate the research methodology and the theoretical framework, and review the themes explored by the authors who have investigated the subjects on which the thesis focuses, with a view to identifying the knowledge gaps that this thesis endeavours to fill.

1.1 Research questions and objective

This thesis focuses on the exercise of State jurisdiction online and on the fulfilment of freedom of expression in the cyberspace. The aim of the thesis is twofold: on the one hand, the thesis aims to shed light on the extraterritorial exercise of prescriptive jurisdiction over content published online. In particular, the thesis explores whether this extraterritorial exercise of jurisdiction is compliant with the freedom of expression obligations contained in regional and international human rights conventions such as the European Convention of Human Rights (ECHR), the American Convention of Human Rights (ACHR), the African Charter on Human and Peoples' Rights (ACHPR) and the International Covenant on Civil and Political Rights (ICCPR). On the other hand, the thesis investigates the meaning of online State jurisdiction according to human rights law. The objective of this analysis is to understand whether and how the concept of State jurisdiction according to the human rights conventions changes when acts are committed online instead of in the physical environment.

This thesis aims to answer the following research questions:

1. When and under what conditions can online acts be considered to have happened within a State's jurisdiction according to human rights law?

2. Is the extraterritorial exercise of State jurisdiction to regulate online content compliant with the freedom of expression provisions contained in human rights law?

The decision to focus on the fulfilment of freedom of expression online is due to the fact that freedom of expression is one of the fundamental human rights most affected by multiple and conflicting exercises of State jurisdiction online. This is because, due to the global and immediately accessible nature of online content, content published online becomes available in multiple States simultaneously. However, States have different laws and what is legal in the country of upload might well be illegal in the places where the content is downloaded or simply accessed. This means that when States exercise jurisdiction over online content that is not linked to their country, because, for example, the content has been published by foreign parties from abroad, they affect the freedom of expression of foreign Internet users who have the right to access content that is perfectly legal in their country.

Overall, through focussing on the two research questions, the thesis aims to explore the meaning of fulfilling freedom of expression online according to the human rights conventions. This objective is achieved by clarifying the jurisdictional sphere of application of the human rights conventions to online acts and examining whether the obligations contained in the human rights conventions regarding freedom of expression change when applied to acts committed online.

1.2 Thesis outline

The thesis is divided into seven chapters. Chapter 1 provides an overview of the research by introducing the research questions and objectives, by illustrating the research methodology and the theoretical framework, and by reviewing the themes explored by the authors who investigated the subjects on which the thesis focuses. Chapter 1 also identifies the knowledge gaps that this thesis endeavours to fill.

In order to answer the two research questions, Chapters 2 and 3 introduce specific instances of extraterritorial exercise of State jurisdiction online, namely the access-based jurisdictional approach and the global application of domestic laws to content published online. In particular, these chapters examine the main characteristics of these extraterritorial exercises of State jurisdiction online through the analysis of key Internet-related cases discussed before domestic and regional Courts. The aim of Chapters 2 and 3 is to ultimately highlight the problems that these exercises of State jurisdiction online pose to State sovereignty and the fulfilment of freedom of expression on the Internet.

Chapter 4 focuses on the rules regulating the exercise of State jurisdiction online according to both public international law and human rights law. The aim of Chapter 4 is

to set the scene for the analysis conducted in Chapters 5 and 6 which will address the first and second research questions respectively. Chapter 4 therefore highlights the differences between the meaning of State jurisdiction according to public international law and human rights law and underlines some grey areas that exist as far as the jurisdictional rules are concerned.

Chapter 5 addresses the first research question by investigating the meaning of online State jurisdiction according to human rights law. In order to achieve this objective, Chapter 5 first explores the meaning of State jurisdiction online according to public international law and then focuses on an analysis of the jurisprudence of the European Court of Human Rights (ECtHR), the Human Rights Committee (HRC), the Inter-American Court and Commission on Human Rights and the African Court and Commission on Human and Peoples' Rights with the aim of understanding how these Courts have approached the subject of State jurisdiction online. Chapter 5 then concludes by examining the application of the spatial, personal and extraterritorial effects models of State jurisdiction to online acts.

Finally, Chapter 6 answers the second research question which aims at understanding whether the exercises of extraterritorial jurisdiction examined in Chapters 2 and 3 are compliant with the freedom of expression provisions of the human rights conventions. In particular, the analysis conducted in this chapter focuses on whether the extraterritorial application of domestic laws to regulate online content meets the accessibility and predictability requirements of the 'prescribed by law' criterion with which restrictions on freedom of expression must comply to be considered legitimate in human rights law. In order to answer this question, Chapter 6 illustrates the regime for the protection of freedom of expression both online and offline according to the human rights conventions and examines the conditions that restrictions to freedom of expression must meet to be justified according to the ECHR, the ICCPR, the ACHR and the ACHPR. In particular, the analysis conducted in Chapter 6 focuses on the meaning of prescribed by law according to the human rights conventions and on an analysis of the criteria used by the human rights courts to define when restrictions to freedom of expression can be considered as accessible and predictable. Finally, the analysis conducted in Chapter 6 concludes with examining a series of extra-legal factors that affect the how the accessibility and predictability requirements of the laws that apply to online acts committed by foreign parties work in an online environment.

The thesis ends with Chapter 7 which summarizes the main conclusions reached in the previous chapters.

1.3 The concept of extraterritorial exercise of State jurisdiction

The background on which this research is set stems from two arguments. First, the rules related to the exercise of State jurisdiction online are uncertain according to both public international law and human rights law. Secondly, multiple States have and still are exercising their jurisdiction extraterritorially to regulate content published online. The first question that this thesis aims to answer centres on whether the extraterritorial exercise of State jurisdiction over online content is compliant with the freedom of expression provisions contained in the human rights conventions. To answer this question, this research focuses on two specific ways in which States have exercised their jurisdiction extraterritorially over content published online: jurisdiction based on access to online content (access-based jurisdictional approach), and jurisdiction based on the existence of a territorial connection between the country exercising jurisdiction and the party responsible for the publication of content online (the territorial connection approach).

The first approach, the access-based jurisdiction, is characterised by the exercise of State jurisdiction over content published online but uploaded from and hosted in a foreign State by a foreign defendant based on the fact that that content is accessible from within the territory of the country exercising jurisdiction (ex. a party located in State X uploads content online from that State, where the content is also hosted. State Y exercises jurisdiction over that content based on the fact that it has been published online and is therefore accessible within the territory of State Y). In the access-based jurisdictional approach the extraterritorial dimension of the exercise of State jurisdiction arises by the combination of two criteria: the fact that the defendant is foreign (location of the defendant) and the fact that the content published online has been uploaded from and is hosted outside the domestic forum (location of uploading and hosting).

In the second approach, the territorial connection approach, the exercise of State jurisdiction is based on the existence of a territorial connection between the country exercising jurisdiction and the defendant. In other words, in this approach, the courts exercise jurisdiction over defendants that are located or operate within their territory. However, the extraterritorial dimension of this exercise of jurisdiction is represented by the fact that the courts extend the application of domestic laws to regulate either online content that is hosted within the jurisdiction of other States or actions that are committed online outside the domestic borders (ex. State X requires access to data that are stored in State Y because the party responsible for administering the data is located in State X; or State X applies its domestic laws to regulate certain online acts controlled by a defendant

located in that State not only when these acts are committed within the borders of State X but also when they are committed abroad).

These two ways of exercising jurisdiction extraterritorially do not exhaust all the possible ways in which States exercise jurisdiction extraterritorially over online content. Exercising jurisdiction based on the targeting test, for example, could be interpreted as an extraterritorial exercise of State jurisdiction over content published online. Indeed, according to the targeting test, a State exercises jurisdiction over content published online by a foreign defendant in a foreign forum based on the fact that the online content targeted an audience located in the State exercising jurisdiction. In that case, the location of the defendant and the location of the uploading and hosting of the online content are the extraterritorial elements. The exercise of State jurisdiction in the targeting test case could be interpreted as an application of the effects doctrine, since targeting an audience located in the State exercising jurisdiction could be considered as an act that produced effects in that State. Notwithstanding the fact that there are multiple ways in which States exercise jurisdiction extraterritorially over content published online, this research focuses on the access-based jurisdiction and on the territorial connection because these two approaches have particularly relevant implications as far as fulfilling freedom of expression online is concerned. Ultimately, this research is focussed on understanding whether the extraterritorial exercise of State jurisdiction online is compliant with the freedom of expression obligations of the human rights conventions. Therefore, the research examines the two approaches that seem to be particularly problematic in this regard.

1.4 Methodology

This thesis relies on the doctrinal analysis method. The doctrinal analysis method is particularly suitable to the thesis' research objectives. Indeed, the first research question investigates the meaning of online State jurisdiction according to the human rights conventions. As to the second research question, this aims at understanding whether territorial connection and the access-based jurisdictional approaches are compliant with the freedom of expression requirements of the human rights conventions. Therefore, this research aims at critically evaluating whether some forms of the law as it currently stands are compliant with the requirements of other areas of law as well as at investigating what the current law is. For this reason, this research is a 'research in law', rather than being a

'research about law'.[1] This study locates and analyses 'the primary documents of the law in order to establish the nature and parameters of the law'.[2] In other words, this is a doctrinal research because it shares the same objectives and characteristics that have been used to describe the doctrinal research method. According to some commentators, this research method is the best placed to understand the law as it stands, because it 'adopts language and concepts that are internal rather than external to the law' and 'advance[s] the sorts of arguments that, roughly speaking, a court might be willing to listen to'.[3] However, the very possibility to determine the law as it stands as if the law were an '"objective reality"' is contested by exponents of various legal theories.[4] According to critical legal theory, for example, the law does not exist as an objective reality and the main characteristic of the legal language is law's indeterminacy.[5] Nonetheless, as observed by Hutchinson and Duncan, 'if we take legislation as an example, the laws are passed by parliament and the words are written down. In that sense there is a positive statement of the law'.[6] It is this positive statement of the law, in particular primary and secondary sources of both domestic and international law, that this research investigates.

Consistent with the doctrinal research method, this research has first identified the primary and secondary sources examined throughout the thesis and then has analysed these sources by relying upon the techniques of deductive logic, inductive reasoning and analogy.[7] The technique of deductive logic has been used to deduce whether a given norm applies to a specific situation. Deductive logic, for example, has been used to analyse whether and how the requirements of the freedom of expression clauses of human rights conventions apply to the two jurisdictional approaches identified by the research. Inductive reasoning and analogy have been applied to infer the existence of a general rule from the analysis of specific cases and to identify similar situations respectively. An example of the use of these techniques can be found in the selection and analysis of the case-law examined in Chapters 2 and 3 of the thesis, where both inductive logic and analogy have allowed to identify similar patterns arising from the various cases examined

[1] Arthurs, H.W. (1983) Law and Learning: Report to the Social Sciences and Humanities Research Council of Canada by the Consultative Group on Research and Education in Law, Information Division, Social Sciences and Humanities Research Council of Canada, Ottawa (as cited in Paul Chynoweth, 'Legal Research' in Andrew Knight and Les Ruddock (ed), *Advanced Research Methods in the Built Environment* (Wiley-Blackwell 2008) 30).
[2] Terry Hutchinson and Nigel Duncan 'Defining and describing what we do: doctrinal legal research' (2012) 17 Deakin LR 83, 113.
[3] Stephen A Smith 'Taking law seriously' (2000) 50 U. Toronto L.J. 241, 255.
[4] Hutchinson and Duncan (n 2) 110.
[5] Martti Koskenniemi, 'Letter to the editors of the symposium', (1999) 93 AJIL 351, 354.
[6] Hutchinson and Duncan (n 2) 110.
[7] Chynoweth (n 1) 32-33; Hutchinson and Duncan (n 2) 111.

and infer the existence of a common denominator between the cases, i.e. the fact that these cases belonged to the same jurisdictional approach.

The line of enquiry followed by this research is both descriptive and interpretive. Indeed, as mentioned earlier, the thesis aims on the one hand at clarifying the meaning of online State jurisdiction according to the human rights conventions. In this regard, the thesis is descriptive as it is focussed on elucidating what the existing human rights law rules are with regard to the meaning of online State jurisdiction. On the other hand, the research is interpretive as it aims at critically evaluating whether some forms of the law as it currently stands (the two jurisdictional approaches identified) are compliant with the requirements of other areas of law (freedom of expression clauses of the human rights conventions).

Finally, it is worth mentioning that this thesis is also centred on the interconnection between public and private international law. Indeed, the thesis analyses *inter alia* some key private international law Internet-related cases and examines the exercise of State jurisdiction by the domestic country through the lenses of the public international law jurisdictional criteria. The deep connection between private and public international law has been increasingly recognised throughout the years. In this regard, Mills has observed that there is 'a functional and doctrinal overlap' between public and private international law and that private international law constitutes a 'hidden ('private') dimension of international law'.[8] This is because the question of whether an exercise of State jurisdiction is allowed by the domestic rules of private international law must be distinguished by the question of whether such an exercise of jurisdiction is justified by public international law.[9] Ultimately, as underlined by Mills,

> '[n]ational courts may take a range of distinct policy considerations into account in determining whether domestic 'jurisdiction' may or should be exercised, including factors which are not reflected in international rules of jurisdiction. Domestic law might even compel a national court to breach international limits, giving rise to non-compliance with international law. But the presence of additional domestic considerations does not deny the relevance of international limits, and the existence of those limits has shaped and continues to shape national rules of private international law'.[10]

The interconnection between private and public international law is therefore central to the analysis of the cases examined in Chapters 2 and 3.

---

[8] Alex Mills 'Rethinking jurisdiction in international law' (2014) 84 BYIL 187, 200.
[9] ibid 202.
[10] ibid.

1.4.1 Case selection

This research has relied on three inclusion criteria to select the cases that are examined in Chapters 2 and 3. The first criterion is the online nature of the action brought before the domestic courts. This criterion has been defined quite broadly, to include both the act of uploading content online (e.g. publishing content on a website) and acts where at least one constitutive element happens online (e.g. online search queries performed using a Search engine). Throughout the thesis, the expressions "online action/act" and "content uploaded online" are therefore used interchangeably. The second case inclusion criterion is the extraterritorial dimension of the case and, more specifically, the extraterritorial dimension of the online act or content upon which jurisdiction is exercised. This criterion is defined by the fact that this online act/content is linked to the territory of a foreign State or multiple States. This extraterritorial element can take different forms: e.g. the content has been uploaded in a foreign State or is hosted in a foreign State or the online action that the domestic court tries to regulate is performed by individuals in foreign States (such as search queries performed on a search engine by Internet users located in foreign States). The third case inclusion criterion is the language of the case: the cases included in the research are only those cases in English or for which an English translation could be identified. This inclusion criterion has resulted in the fact that the majority of the cases selected are related to a specific geographic area, corresponding mainly to Europe, North America and Australia. These geographic areas, however, also correspond to those jurisdictions for which data related to Internet case-law are relatively readily available. Indeed, the sources that this research relied upon to select the cases analysed (see below) have a sizeable amount of information related to the above-mentioned countries.

The combination of the first two selection criteria has allowed to identify only those cases where the national courts had to determine whether an online act linked to a foreign State could be brought within the jurisdiction of the courts examining the case. In other words, the domestic courts in the cases analysed in the thesis had to determine the minimum contacts that had to occur between an online act linked to a foreign State and the domestic forum for the domestic court to have jurisdiction over the act. Therefore, the cases that were not included in the research are those Internet-related cases where, although an act happened online, it was so clearly linked to the territory of the State exercising jurisdiction (for example because the content had been uploaded there from a person living in that State) that there were no doubts that the domestic court had jurisdiction. In other words, the cases included in this research are '[…] only […] (those) cases in which the

distinguishing features of the Internet create uncertain results when deciding'.[11] The expression 'distinguishing features of the Internet' in this context refers to the extraterritorial dimension of the online act upon which jurisdiction is exercised.

As mentioned above, in the two jurisdictional approaches on which this research focuses, the two inclusion criteria have taken different forms. In the access-based jurisdictional approach, the extraterritorial dimension of the exercise of State jurisdiction is given by the combination of two elements: the fact that the defendant is foreign (location of the defendant) and the fact that the content published online has been uploaded from and is hosted outside the domestic forum (location of uploading and hosting). In the territorial connection criterion, the extraterritorial dimension of the exercise of jurisdiction is represented by the fact that the domestic courts exercise jurisdiction over content that is hosted within the jurisdiction of other States or over online actions committed outside the domestic borders. In that case, however, unlike the access-based jurisdictional approach, the defendant is located within the territory of the State exercising jurisdiction.

The cases examined in Chapters 2 and 3 of the thesis have been collected by relying on two different sources: the database Internet & Jurisdiction and the journal Leading Internet Case-Law. The Internet & Jurisdiction database is an open-access resource whose purpose is to monitor jurisdictional trends around the world. The cases added to the database date back to February 2012 and are selected by Internet jurisdiction experts that are members of the I&J Observatory. The I&J Observatory is currently composed of 30 members from a variety of academic institutions and research centres around the world.[12] According to the I&J website, the members of the I&J Observatory select the top 20 cases to be added to the database on a monthly basis after having ranked them.[13] The cases' ranking criteria relied upon by the I&J Observatory members are not specified. As to the Leading Internet Case-Law journal, it is a journal for Internet law practitioners that publishes legal analysis of Internet-related case law from various countries. The Journal's contributors are legal and industry professionals. The UK, US, Germany, China, Italy,

[11] University of Geneva 'Geneva Internet Disputes Resolution Policies 1.0' (*Geneva Internet Disputes Resolution Policies 1.0*) <https://geneva-internet-disputes.ch/> accessed: July 2017), 3.

[12] The full list of the I&J Observatory members can be found at Internet & Jurisdiction Policy Network, 'I&J Observatory Members' (*Internet & Jurisdiction*) <https://www.internetjurisdiction.net/work/observatory/members> accessed: 03 September 2020.

[13] Internet & Jurisdiction Policy Network, 'I&J Observatory' (*Internet & Jurisdiction*) <https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMjAtMDcifQ==> accessed 21 May 2018.

France and the Netherlands are among the jurisdictions covered by the journal.[14] Similarly to the Internet & Jurisdiction database, the cases selection criteria relied upon by the journal's contributors are not specified.

The cases analysed in Chapters 2 and 3 of the thesis have been selected by searching the above-mentioned databases using keywords or filters. The keyword used for the journal Leading Internet Case-Law is 'jurisdiction'. As to the Internet & Jurisdiction database, the database provides pre-determined filters that can be used to select relevant cases. The filter relied upon to select the cases examined in the thesis is "Court" in the filter category named "Actor".

1.5 Theoretical framework

This research draws on modern positivism as a theoretical framework.

Modern positivism is particularly suitable to this research due to the "deeply pragmatic nature" of this thesis, which is oriented towards understanding where existing human rights law stands as far as the subject of online State jurisdiction is concerned. In other words, this research builds on the analysis of the law as it is (*lex lata*), rather than suggesting how this should be (*lex ferenda*). The distinction between *lex lata* and *lex ferenda* is the distinction upon which the modern positivist method is constructed.

The positivist method (both in its classical and modern versions) has attracted the views of many scholars.[15] Some of them have emphasised the advantages of this research method, among which figure its clarity and legitimacy.[16] Many authors have, on the other hand, critiqued positivism. Among the disadvantages that have been identified figure its indeterminacy and lack of objectivity, especially in relation to asserting the existence of customary international norms.[17] Another critique that has been made to positivism refers to its inaccuracy when it comes to determining what the current law is. This inaccuracy

[14] Wildy & Sons Ltd 'Leading Internet Case Law' (*Wildy & Sons Ltd*) <https://www.wildy.com/isbn/2399-0015/e-commerce-law-reports-print-online-law-reports-online-cecile-park-publishing> accessed: 03 September 2020.

[15] Anne-Marie Slaughter and Steven R Ratner, 'The method is the message' (1999) 93 AJIL 410; Bruno Simma and Andreas L Paulus, 'The responsibility of individuals for human rights abuses in internal conflicts: a positivist view' (1999) 93 AJIL 302; Siegfried Wiessner and Andrew R Willard, 'Policy-oriented jurisprudence and human rights abuses in internal conflict: toward a world of public order of human dignity', (1999) 93 AJIL 316; Mary Ellen O'Connell, 'New International Legal Process', (1999) 93 AJIL, 334; Koskenniemi (n 5), 351; Hilary Charlesworth, 'Feminist method in international law', (1999) 93 AJIL 379.

[16] 'As an adjunct to positivism, classic ILP shares positivism's great advantage, its claim to legitimacy not found in other methods, including new ILP. Positivism can arguably demonstrate its legitimacy'. O'Connell (n 15) 349.

[17] ibid 350.

has been considered a direct consequence of the fact that positivism does not take into account the factors that influence the creation and application of the law, such as 'the personality, political inclinations, gender and cultural background of the decision makers, as well as the mood of the times, and other societal factors'.[18]

In this perspective, one of the major advantages of the positivist method, pragmatism, is at the same time one of its core limits. Indeed, it can be argued that pragmatism is one of positivism's strongest assets because it allows scholars to develop a clear research path that is centred on a rigorous analysis of international law norms. At the same time, though, this advantage can become a limitation. Indeed, the positivist analysis builds on the notion that States are the main subjects of international law and that international law norms are mainly expression of States' will. In doing so, positivism fails to take into proper account the role that actors other than States, such as private citizens, corporations, and third sector organisations, play in influencing the creation and the application of international law norms. In other words, the positivist approach is, to an extent, too simplistic. Indeed, it can be inadequate to reflect the complexity of the interactions between the various stakeholders that populate today's international sphere. This is especially true in relation to cyberspace, where States' sovereignty finds a limit in the power and the technological expertise of the Internet Service Providers. Another example of the complexities that the modern positivist framework does not allow to capture, especially in regard to the law applicable to cross-border online acts, is found in the way that the accessibility and foreseeability requirements of the 'prescribed by law' criterion of the human rights conventions have been so far interpreted. Indeed, as will be examined in Chapter 6, the classic interpretation of these requirements that derives from an analysis of the human rights norms and the case-law interpreting these norms shows that the way in which these two criteria have been interpreted is short-sighted. This is because it does not take into account some extra-legal factors that influence the accessibility of domestic laws to foreign parties. These extra-legal factors, such as common knowledge and intermediaries, are exactly the kind of factors that, due to their extra-legal nature, are not taken into account in a positivist framework, notwithstanding the fact that they have repercussions on how the legal concepts of accessibility and foreseeability work online.

Despite the limitations that are necessarily connected with adopting a positivist approach, modern positivism is particularly suited to answer the above-mentioned research questions. This is because this analysis is primarily centred on understanding the

[18] Wiessner and Willard (n 15) 320.

role played by States in granting the fulfilment of human rights online according to the human rights conventions.

1.6 Literature review

In the current debate concerning State jurisdiction and human rights in cyberspace, there are many questions that have been addressed. In particular, the debates in the scholarly community have focussed on issues ranging from the concept of sovereignty and State jurisdiction in cyberspace to common jurisdictional principles arising from Internet-related cases to the way in which jurisdiction has been interpreted according to human rights treaties.

The ongoing debate among the scholars who have examined the concept of State jurisdiction on the Internet shows that there is currently no agreement as to how States should exercise jurisdiction online.[19] Notwithstanding this, some authors have argued that some common principles of jurisdiction are emerging through the analysis of State practice.[20] However, the limit that has emerged from the analysis of the literature produced on this subject is that the theme of online State jurisdiction according to human rights treaties seems relatively unexplored. Indeed, some authors have focused on the analysis of the jurisdictional issues arising from the online violation of a specific human right. Others have analysed the meaning of State jurisdiction online according to public international law. However, there are not many studies that bring these two areas together by investigating the overall theme of online jurisdiction according to the human rights conventions. This research aims at contributing to filling this knowledge gap.

In relation to the meaning of State jurisdiction according to the multilateral human rights treaties, some scholars have argued that the concept of State jurisdiction according to human rights treaties differs from the concept of State jurisdiction according to general

[19] Alisdair Gillespie, 'Jurisdictional issues concerning online child pornography' (2012) 20 Int J Law Info Tech 151; Mika Hayashi, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace' (2006) 6 In.L. 284; Robert Uerpmann-Wittzack, 'Principles of International Internet Law' (2010) 11 German L. J. 1245; Bernhard Maier, 'How has the law attempted to tackle the borderless nature of the internet?' (2010) 18 Int J Law Info Tech 142; Mohammad Mahabubur Rahman and others 'Cyberspace claiming new dynamism in the jurisprudential philosophy' (2009) IJLMA, 51, 274; Joanna Kulesza, *International Internet Law* (1st edn, Routledge 2012); Joanna Kulesza and Roy Balleste, 'Signs and Portents in Cyberspace: the Rise of a Jus Internet as New Order in International Law' (2013) 23 Fordham Intell. Prop. Media & Ent. L.J. 1311; Pardis Moslemzadeh Therani and Nazura Abdul Manap 'A rational jurisdiction for cyberterrorism' (2013) 29 Com. L & S Rev 689; Dina I. Oddis 'Combating Child Pornography on the Internet: The Council of Europe Convention on Cybercrime' (2002) 16 Temp. Int'l & Comp. L. J. 477.

[20] Maier (n 18); Gillespie (n 18); M Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 55, Rule 9; Michael A Geist 'Is There a There There - Toward Greater Certainty for Internet Jurisdiction' (2001) 16(3) Berkeley Tech LJ 1345.

international law.[21] This thesis further explores this topic with the aim of understanding if the concept of cyberspace jurisdiction according to human rights conventions is different from the concept of jurisdiction according to international law.

1.6.1 The international law rules applicable to cyberspace: State sovereignty and State jurisdiction online

One of the themes that have been explored regarding the international law rules applicable to cyberspace is the meaning of State sovereignty online. The view whereby the principle of State sovereignty applies to acts that happen online and States must not violate the sovereignty of other States when conducting these acts has received the approval of various academic and governmental experts, especially in the field of international security.[22] This argument is based on the assertion that sovereignty is an enforceable rule of international law whose violation constitutes an international illicit act. However, there is an opposing view according to which, rather than being an international law rule enforceable per se, sovereignty is merely reflected in specific international law norms, such as the rules against the use of force and the prohibition of intervention.[23] Despite the disagreement, the '"sovereignty-as-a-rule"'[24] view seems to be prevailing in the field of international security, where it received the approval of various experts, including the Group of International Experts that produced the Tallinn Manual 2.0 on the International Law Applicable to Cyber-Operations and the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Communication Technologies.[25]

There is, however, no agreement as to how the international law norms related to sovereignty should be interpreted in cyberspace. For example, the Tallinn Manual 2.0 argues that a State that conducts cyber-operations against another State while physically

---

[21] Marko Milanović, 'From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties' (2008) 8 Hum. Rts. L. Rev. 411.
[22] Eric Talbot Jensen, 'The Tallinn Manual 2.0: Insights and Highlights' (2017), 48 Geo J Int'l L 735, 741; UN. Secretary-General and UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security : note / by the Secretary-General, (22 July 2015) A/70/174; Michael Schmitt 'US Transparency Regarding International Law in Cyberspace' (*Just Security*, 15 November 2016) <https://www.justsecurity.org/34465/transparency-international-law-cyberspace/> accessed 12 June 2018; Gary Corn 'Tallinn Manual 2.0 – Advancing the Conversation' (*Just Security*, 15 February 2017) <https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/#more-37812> accessed 12 June 2018.
[23] Talbot Jensen (n 22) 741; Schmitt (n 22); Corn (n 22).
[24] Talbot Jensen (n 22) 741;
[25] Talbot Jensen (n 22) 741; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (n 22) 12.

present on the territory of that State infringes the latter's sovereignty.[26] What remains unclear is whether the same act would constitute a violation of sovereignty if the cyber-operation was conducted remotely (i.e. from the territory of the State launching the operation) rather than on the territory of the State against which the operation is directed. In this regard, some have claimed that a remote cyber-operation does not constitute a violation of State sovereignty per se.[27] However, there is disagreement on the factors that should be taken into account to determine when a violation of State sovereignty arises as a consequence of a remote cyber-operation. According to some commentators, the way in which the operation is conducted and the effects that it produces on the targeted State should be the factors that determine when a violation of State sovereignty occurs.[28] In any case, various sources have highlighted the lack of State practice in this area and the overall need for States to clarify their views on sovereignty in cyberspace.[29] In this regard, sovereignty appears to be one of the areas that are most likely to evolve in the immediate future.[30]

Another debate that is related to the international law rules regarding State sovereignty in cyberspace is that concerning whether States should exercise sovereignty over the delegation of country code Top-Level Domain names (ccTLD). The Internet Corporation for Assigned Names and Numbers (ICANN) is the private not-for-profit organisation registered in California responsible for assigning Top Level Domain names (TLDs) to operators. This operation is known as delegation of the TLD to a delegee. TLDs are divided into generic TLDs, such as .com, and country code TLDs, such as .us. While both TLDs function in the same way, they are administered differently.[31] Indeed, generic TLDs are assigned to a given operator through a contract with ICANN. However, the delegation of ccTLDs is less regimented and is mostly left to 'consensual relationships between ICANN, the delegee and governments'.[32] Some States have claimed the right to exercise control over the related ccTLD as an expression of their sovereignty.[33] In particular, some documents adopted by ICANN's Governmental Advisory Committee (GAC) and by the stakeholders of the World Summit on the Information Society (WSIS), expressed the belief that no State should be involved in decisions regarding another

[26] Talbot Jensen (n 22) 741.
[27] Schmitt (n 22).
[28] ibid; Talbot Jensen (n 22) 756-757.
[29] Talbot Jensen (n 22) 743-744; Corn (n 22); Schmitt (n 22).
[30] Talbot Jensen (n 22) 743-744; Schmitt (n 22).
[31] Milton L Mueller and Farzaneh Badiei 'Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country-Code Top Level Domains' (2017) 18 Colum Sci & Tech L Rev 435, 445.
[32] ibid 443.
[33] ibid 439-440; Uerpmann-Wittzack (n 16) 1256-1258.

State's ccTLDs. Those documents also stated that public policy decisions regarding ccTLDs rested with the respective government.[34]

The State sovereignty claim over ccTLDs has found the approval of some commentators, who have observed how the principle of territorial sovereignty has adapted to cyberspace and has extended to ccTLDs which can be considered as part of State territory.[35] However, other authors have rejected this sovereignty claim as unfounded.[36] In particular, they have observed that, while it is true that ccTLDs refer to geographical areas that in most cases can be reconducted to States, they do not necessarily correspond to sovereign States (ex. the Isle of Man, which is part of the UK, has its own ccTLD, .im).[37] Instead, these areas match the geographical territories identified by an international standard, the ISO-3166-1 which was used to develop ccTLDs.[38] In addition, the mere correspondence between a ccTLD and a given State is not enough according to international law to justify the exercise of sovereignty.[39] These arguments seem particularly convincing. Indeed, the territorial jurisdiction principle establishes that States can control any business located within their territory, including domain names registries. However, there is no international law rule that establishes that merely referring to a geographical area that can be reconducted to a given State is enough for that State to exercise jurisdiction.[40]

Closely related to the theme of State sovereignty online is the meaning of State jurisdiction in cyberspace according to international law. This theme has been approached by various scholars from different angles. Some authors have focussed on the well-

[34] 'It is recalled that the Governmental Advisory Committee (GAC) to ICANN has previously adopted the general principle that the Internet naming system is a public resource in the sense that its functions must be administered in the public or common interest. The WSIS Declaration of December 2003 states that "policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues." This is in the context that, "Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders', Governmental Advisory Committee 'Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains' (ICANN Archives, 5 April 2005) <https://archive.icann.org/en/committees/gac/gac-cctld-principles.htm> accessed: 11 September 2020, [1.6]; 'Countries should not be involved in decisions regarding another country's countrycode Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanism', World Summit on the Information Society, Tunis Agenda for the Information Society (18 November 2005) WSIS-05/TUNIS/DOC/6(Rev.1)-E, [63]; Mueller and Badiei (n 30) 451-454, 464; Uerpmann-Wittzack (n 16) 1258.

[35] Uerpmann-Wittzack (n 16) 1256.

[36] Mueller and Badiei (n 30) 459-460.

[37] ibid 444.

[38] ibid 459-460.

[39] ibid 462.

[40] On this point see also Mueller and Badiei (n 30) 489.

established public international law principles of jurisdiction, in order to understand whether and how these principles change when applied to cyberspace. In this regard, some authors have examined the way in which the objective territorial principle and the effects doctrine function online. These two jurisdictional principles can be interpreted as two extensions of the principle of territorial jurisdiction.[41] According to the objective territorial principle, a State can exercise jurisdiction over a given act when at least one of the latter's constitutive elements, its effect, takes place physically within the State's territory.[42] As to the effects doctrine, this can be described as the exercise of State jurisdiction over acts that produce significant effects within the national territory, even if they have happened entirely abroad.[43] In this case, the link between the exercise of State jurisdiction and the act upon which jurisdiction is exercised is represented solely by the latter's effects. The absence of a territorial connection between the State exercising jurisdiction and the act upon which jurisdiction is exercised is one of the main reasons why the effects doctrine has been criticised for not offering a clear limit to the exercise of extraterritorial jurisdiction.[44] In contrast, the objective territorial principle can be seen as offering such a limit.[45] However, according to some commentators, in Internet-related cases the difference between the objective territorial principle and the effects doctrine loses significance since the former tends to merge with the latter.[46] This is because it is very difficult to establish when an online act happens within the territory of a given State and when it produces adverse effects there. Therefore, both principles have been interpreted as offering uncertain limits to the exercise of extraterritorial jurisdiction.[47] However, some authors have argued that there is a tendency on national courts' part to limit the effects doctrine by looking at whether other connecting factors exist that could link a webpage to the country exercising jurisdiction. An example of this point can be found in the reliance of the Federal Court in the *Töben* case on the fact that the Holocaust affected Germany in a special way.[48]

The way in which States have tried to adapt to the apparently borderless nature of the Internet is another theme that has been debated in the scholarly community. Some authors

[41] Hayashi (n 16) 288.
[42] ibid.
[43] ibid.
[44] ibid.
[45] ibid 289.
[46] Hayashi (n 16) 298-301; Uerpmann-Wittzack (n 16) 1255.
[47] Hayashi (n 16) 289, 301.
[48] Bundesgerichtshof, Toeben (Federal Court), Judgment of 12 December 2000, case 1 StR 184/00, 46 Entscheidungen Des Bundesgerichtshoifns Strafsachen(B Ghst) 212 (2001) = 54 Neue Juristischew Ochenschrift (NJW) 624 (2001), also available through http://www.bundesercht hofd/, 628 (2001) (as cited in Uerpmann-Wittzack (n 16) 1255-1256).

have focussed on the role played by the domestic courts in dealing with Internet-related cases. In particular, some commentators argue that there is a tendency on the domestic courts' part to identify the virtual space by relying on the same criteria that are usually applied to the physical space.[49] According to this view, Courts have not tried to invent a new rule of jurisdiction applicable to Internet-related cases and have rather maintained a sense of territory.[50] Other authors have identified some common principles of jurisdiction that arise from the analysis of the criteria that different legal systems rely upon to establish jurisdiction in Internet-related cases.[51] Some authors, for example, have selected three areas of law, namely defamation law, data protection and privacy law, and gambling and have identified some themes that are common across the various legal systems examined.[52] Among the principles identified are the country of origin approach, location of the equipment, destination at which the publication of online material was directed, effects doctrine and creation of artificial borders.[53] The conclusion reached in this regard is that different areas of law have used differing approaches according to the policy objective to be achieved.[54]

The comparative approach has been adopted also by those authors that have focussed on how different legal systems have regulated one specific Internet-related crime. For example, some commentators have compared the criteria used in England and Wales to allocate jurisdiction in relation to online child pornography with the criteria in force in the United States.[55] In this regard, the theory brought forward is that in England and Wales the terminatory principle has been replaced by the '"substantial measure"' principle, according to which British courts have jurisdiction over a crime when a substantial part of the activities that constitute that crime takes place in Britain.[56] As to the US

[49] Hayashi (n 16) 297-298, 302.
[50] ibid 302.
[51] Maier (n 16). The legal systems Maier he has taken into account in his article differ according to the area of law examined. In regard to the criteria used to allocate jurisdiction in the field of defamation law, Maier has compared the approach used in the Brussels Regulations (Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L012 (as cited in Maier (n 16) 150) with the approach used in the United Kingdom, Australia and United States. In reference to the law of data protection and privacy, Maier has examined the European Data Protection Directive 1995 (Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (as cited in Maier (n 16) 157-158). Finally, in relation to gambling, the legal systems taken into account by Maier are the United Kingdom, the United States and the EU system represented by the Electronic Commerce directive (Council Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), [2000] OJ L178 (as cited in Maier (n 16) 165).
[52] ibid 160-174.
[53] ibid 172-174.
[54] ibid 175.
[55] Gillespie (n 16).
[56] ibid 161.

jurisdictional approach, these commentators have referred to the criteria employed to assess federal jurisdiction over online child pornography. This approach has been defined it as the '"per-se approach"', whereby the Internet is considered as an instrument of interstate commerce per-se, irrespective of whether or not the data are transmitted between servers located in different States.[57]

Another theme that has been explored is the possibility of considering cyberspace as a new jurisdictional area. Some scholars have examined whether the jurisdictional regime reserved to international spaces - such as the high seas and outer space – could be applied to the Internet. According to this view, cyberspace could be considered as a fourth international space and should be governed by rules that are similar to those applicable to the other three international spaces.[58] According to the proponents of this argument, one of the advantages of this approach is that this way the '"sovereign-less character"' of cyberspace could adequately be addressed.[59] The idea of cyberspace as an international space has, however, attracted critiques. The main objection to this theory is that cyberspace is intrinsically different from the other international spaces and that it does not share their same characteristics: being a physical territory, being completely separate from the territory of sovereign States, and not trespassing the national borders.[60] At the same time, however, it has been pointed out that, although cyberspace cannot be regarded as a physical territory in itself, it nonetheless retains some physical characteristics. Indeed, it is a network of computers and servers that are located within the States' territories. Therefore, it would be unrealistic to believe that the States would renounce to 'their sovereign rights to establish cyberspace as a form of international space'.[61]

Finally, other authors have called for the rise of a new branch of international law, namely *Ius Internet*, establishing an a-territorial and supranational space of interactions between people located in different territories. According to this view, the only way to regulate cyberspace would be through international law.[62] Kulesza refers to the few global acts, soft law documents, and theses presented in the international law doctrine regarding cyberspace, affirming that until now these instruments constitute the body of International Internet Law (IIL).[63] In Kulesza's opinion, IIL can be defined as the public international framework for Internet governance, covering issues ranging from civil law, trade law,

[57] ibid 165.
[58] Rahman and others (n 16).
[59] ibid 287.
[60] Gillespie (n 16) 157-158.
[61] ibid 158.
[62] Kulesza (n 16); Kulesza & Balleste (n 16); Therani & Manap (n 16).
[63] Kulesza, (n 16) 137.

administrative law, financial law, and criminal law. Finally, the author explores the possibility of creating an Internet Framework Convention that would incorporate the emerging IIL principles, tackle the issues related to electronic communication, and propose a multi-stakeholder regime.[64]

1.6.2 The concept of State jurisdiction according to the multilateral human rights conventions

Another theme that has been explored by scholars relates to the concept of State jurisdiction according to some of the existing human rights conventions. In particular, these scholars aim to determine whether the concept of State jurisdiction differs between human rights conventions and public international law.[65]

In this respect, Milanović has analysed the jurisdictional clauses contained in eight human rights conventions[66], by dividing them into two categories: single jurisdiction clauses that define the applicability of the treaty as a whole, and multiple jurisdiction clauses related to specific rights or obligations under the treaty. The thesis expressed by Milanović is that the meaning of the term jurisdiction under human rights treaties is related to 'a sort of factual power that a State exercises over persons or territory'.[67] This concept does not include the notion of legal competence and is different from the definition of jurisdiction according to general international law, which defines the right of each State to regulate conducts and events.[68]

Milanović has examined the jurisprudence of the European Court of Human Rights (ECtHR) regarding the exercise of extraterritorial jurisdiction. In his opinion, not only has the ECtHR developed a concept of jurisdiction that is different from the one according

---

[64] ibid. 153.
[65] M Gondek, 'Extraterritorial application of the European Convention on Human Rights: territorial focus in the age of globalization' (2005) 52 Netherl I L Rev 349.
[66] Milanović (n 21). The human rights conventions examined by Milanović are: Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR) (ETS 5), 213 UNTS 222, entered into force 3 September 1953 (as cited in Milanović (n 21) 412); International Covenant on Civil and Political Rights 1966 (ICCPR) 999 UNTS 171, entered into force 23 March 1976 (as cited in Milanović n (21) 412); Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty, (1990) 29 ILM 1464, entered into force 11 July 1991 (as cited in Milanović (n 21) 413); International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families 1990 (Migrant Workers Convention) 2220 UNTS 93, entered into force 1 July 2003 (as cited in Milanović (n 21) 413); American Convention on Human Rights 1989 (ACHR) OAS TS 36, 1144 UNTS 123, entered into force 18 July 1978 (as cited in Milanović (n 21) 413); UN Convention on the Rights of the Child 1989 (CRC) 1577 UNTS 3, entered into force 2 September 1990 (as cited in Milanović (n 21) 413); Convention on the Elimination of all forms of Racial Discrimination 1965 (CERD) 660 UNTS 195, entered into force 4 January 1969 (as cited in Milanović (n 21) 414); Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1984 (CAT) 1465 UNTS 85, entered into force 26 June 1987 (as cited in Milanović (n 21) 414).
[67] Milanović (n 21) 417.
[68] ibid 417, 422.

to general international law, but it has done so assuming that this concept equates to the concept of jurisdiction as established in general international law.[69] In order to explain Milanović's thesis, it is useful to briefly summarise the ECtHR's jurisprudence regarding the exercise of extraterritorial jurisdiction. According to the *Loizidou*[70] ruling, one State militarily occupying another State's territory exerts its jurisdiction and must therefore respect the European Convention. In other words, the Court affirmed that the contracting State's 'obligation to secure, in such an area, the rights and freedoms set out in the Convention, derives from the fact of such control whether it is exercised directly, through its armed forces, or through a subordinate local administration'.[71] In contrast, in the *Banković* case, the Grand Chamber of the Court stated that, due to the regional nature of the ECHR, a State that bombs another State that is outside the legal space of the Convention is not exercising jurisdiction according to Article 1.[72] In 2004, in the *Issa* decision, the Court referred to military operations conducted in a six-week period by Turkey in Northern Iraq against an alleged terrorist who had fled there.[73] The Court maintained that, in principle, these operations could be considered as being conducted in the jurisdiction of the perpetrating State rather than the State on whose territory these operations are occurring. However, the perpetrating State must have full control over the territory in question, regardless of the fact that this territory does not fall in the juridical space of the contracting States.[74] Milanović has observed that exercising effective overall control over a territory does not necessarily correspond to exercising jurisdiction according to international law. Indeed, in his opinion, to exercise jurisdiction, a State would need to extend the application of its domestic laws to the occupied territory.[75] The author also observed that, although in the *Banković* case the Court apparently reached a different conclusion than the one adopted in the *Loizidou* case, this case 'did not go far enough in bringing the Court's case law back into conformity with general international law'.[76]

[69] ibid 417.
[70] *Loizidou v. Turkey* App no 15318/89 (ECHR, 18 December 1996).
[71] *Loizidou v. Turkey* App no 15318/89 Preliminary objections (ECHR, 23 March 1995) para. 62.
[72] *Banković and Others v. Belgium and Others* App no 52207/99 (ECtHR, 12 December 2001) para 80.
[73] *Issa and Others v. Turkey* App no 31821/96 (ECtHR, 30 March 2005).
[74] ibid paras 69, 71, 74.
[75] Milanović (n 21) 423.
[76] ibid 425.

In this regard, it is worth mentioning an argument that is partially linked to the theme of the jurisprudence of the ECtHR: the development of positive obligations under the ECHR arising from the jurisprudence of the Court.[77]

Mowbray has observed that, rather than articulating a specific theory of the positive obligations arising from the Convention, the ECtHR has developed implied positive obligations across the articles of the ECHR. The Court relied upon two justifications to explain why this approach was adopted. The first justification is the necessity to ensure that the relevant rights are practical and effective in their exercise. The second is the Court's intention to reduce the number of long and expensive fact-finding missions by imposing the positive obligations on States to conduct effective investigations into crimes such as killings and disappearances.[78]

The author defines the positive obligations developed by the Court as forms of positive actions that the States are required to take in order to effectively guarantee the fulfilment of the rights enshrined in the Convention. In other words, "passive non-interference by governmental authorities with persons' Convention rights is not sufficient to ensure that many of those rights are fully and effectively respected".[79]

Mowbray has identified two main groups of positive obligations: those related with different stages of the criminal system, and those concerned with the duty of States to conduct effective investigations into claims that serious violations of Convention rights have occurred. In his opinion, the Court's case law regarding positive obligations has eroded the "generational gap between Convention rights and later generation of international human rights".[80]

1.7 Novel elements of the research

The analysis of the literature produced around the concept of online State jurisdiction and the respect for human rights in cyberspace shows that there are some gaps in the scholarly debate regarding these areas.

First, most of the research that has been produced and published so far reveals that there is currently no agreement as to what jurisdiction means when it is applied to cyberspace. By investigating the concept of cyberspace jurisdiction according to human

[77] Alastair Mowbray, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights* (1st edn, Hart Publishing 2004).
[78] ibid 221-222.
[79] ibid.
[80] ibid 231.

rights conventions, my research will contribute to clarifying the meaning of this term in the field of human rights law. By fulfilling this objective, the thesis will contribute to clarifying the meaning of online jurisdiction in the broader field of international internet law.

The second knowledge gap that can be identified in the literature is that the authors who have analysed the meaning of cyberspace jurisdiction have not properly investigated the meaning that this term acquires as it applies to human rights treaties. Instead, most authors have primarily analysed the jurisdictional issues that derive from online violations of a specific human right. Therefore, the overall theme of cyberspace jurisdiction according to the human rights conventions is considerably unexplored. Equally, the scholars who have investigated the concept of State jurisdiction in human rights conventions have not properly clarified the meaning of the concept of online State jurisdiction in terms of these conventions. Therefore, the novel element that my research will introduce is an explanation of the connection between State jurisdiction online and State jurisdiction according to human rights conventions. These two fields have so far mostly been approached separately.

In conclusion, by developing this research, the thesis will contribute to adding clarity and robustness to a field of study, international internet law, in which multiple areas remain relatively new and unexplored.

1.8 Conclusion

This thesis focuses on two specific ways in which States are exercising jurisdiction extraterritorially in relation to content published online: the access-based jurisdictional approach and the territorial connection requirement. The research aims at answering the following two research questions: first, are these two extraterritorial jurisdictional approaches compliant with the freedom of expression requirements of the human rights conventions? Secondly, what does online State jurisdiction mean according to the human rights conventions? This research relies on the doctrinal analysis research methodology and on the modern positivist theoretical framework. The analysis of the literature produced in this chapter around the concept of online State jurisdiction and respect for human rights in cyberspace shows in particular two knowledge gaps that this research aims to fill. The first gap is related to the uncertain meaning of State jurisdiction online. The second is the fact that two areas, the meaning of State jurisdiction according to human rights conventions and the meaning of State jurisdiction according to public international

law have so far been examined separately. Consequently, the meaning of online State jurisdiction according to the human rights convention has been relatively unexplored.

The next chapter will focus on the access-based jurisdictional approach and will illustrate the key characteristics of this approach together with the implications that it has on the fulfilment of freedom of expression in cyberspace.

2. The access-based jurisdictional principle in Internet-related cases

2.1 Introduction

This chapter discusses the key characteristics of the access-based jurisdictional principle and explores the main critiques that this approach has attracted. The main claim put forward in this chapter is that the access-based jurisdictional approach impacts negatively on the freedom of expression of foreign-based Internet users and it represents an unpredictable exercise of extraterritorial jurisdiction. To substantiate this claim, section two will introduce the main characteristics of the access-based approach, while section three will provide an outline of some key cases where national courts in Europe, North America and East Asia established jurisdiction based on the accessibility of online content. Section four will critically analyse this jurisdictional approach, while section five will focus on the implications that this approach has on the fulfilment of freedom of expression in cyberspace. Finally, section six will summarize the main conclusions of the analysis conducted in the previous sections.

2.2 The access-based jurisdictional approach

The Internet has posed multiple challenges to the human rights protection regime, one of which involves the definition of the concept of State jurisdiction in cyberspace. Jurisdiction, according to some authors, is the area of international law most affected by cyberspace.[1] Indeed, currently there is a high level of uncertainty as to the meaning of State jurisdiction online, as interpreted by both general international law and human rights law.

One of the reasons why it is difficult to ascertain the meaning of State jurisdiction in cyberspace is the apparently borderless nature of the Internet. Indeed, as observed by many commentators, traditionally State jurisdiction has been established by relying primarily on the territorial criterion i.e. a State can exercise jurisdiction over acts

[1] Some of the issues explored in this chapter were addressed in Sara Solmone 'Establishing Jurisdiction Online: the Problem of the Access-based Jurisdictional Principle' (*RIPE Labs*, 16 October 2017) < https://labs.ripe.net/Members/sara_solmone/establishing-jurisdiction-online> accessed: 14 September 2020. Mika Hayashi, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace' (2006) 6 In.L. 284.

committed within its territory and over people located within its borders.[2] However, the acts committed online happen in a *prima facie* non-physical environment, where it is not always possible to clearly identify both the perpetrator of an unlawful act and the territory in which the act originated. It is also equally unclear where the unlawful act produced its adverse effects. Indeed, once published online, content becomes immediately accessible to everybody everywhere. For all these reasons, it appears particularly difficult to establish which State would be entitled to apply its own laws to regulate acts committed online.

Currently, multiple and conflicting national laws are simultaneously being applied by States to regulate content published online.[3] Indeed, as stated in an issue paper published in 2014 by the Council of Europe High Commissioner for Human Rights, several States have simultaneously applied their national laws to regulate 'activities of individuals who are not nationals of those States and who live outside their respective territories'.[4] Due to the uncertainty as to the rules governing the exercise of State jurisdiction online several national courts have established jurisdiction over content published online and hosted abroad on the basis of the fact that that content could be accessed from within the territory of the States where the courts are located.

This phenomenon can be described as the access-based jurisdictional approach. According to this approach, the accessibility from within the territory of a given State of content published online from abroad is deemed to be a sufficient link for the national courts of that State to establish jurisdiction over it.

The distinctive characteristic of the access-based jurisdictional approach is that when establishing whether they have jurisdiction over the content published online the courts are not concerned with establishing where that content was uploaded from or which country it was targeting. Indeed, according to general international law, a State can exercise jurisdiction over acts committed in full or in part within its territory, or over acts directed against its nationals or carried out by them. A State can also exercise jurisdiction over acts that were committed elsewhere but produced negative effects within its territory. The peculiarity of the access-based jurisdictional approach is that no jurisdictional link exists between the content published online and the country exercising jurisdiction other than the fact that that content can be accessed by Internet users located within the territory

[2] Hayashi (n 1) 284; Robert Uerpmann-Wittzack, 'Principles of International Internet Law' (2010) 11 German L. J. 1245, 1253.
[3] Uta Kohl, 'Ignorance is no Defence, but is Inaccessibility? On the Accessibility of National Laws to Foreign Online Publishers' (2005) 14 Info.& Comm.Tech.L. 25.
[4] Douwe Korff, The rule of law on the Internet and in the wider digital world, Council of Europe Commissioner for Human Rights, 2014, 56.

of the State exercising jurisdiction. Indeed, as explained below, the parties responsible for the publication of the material online are usually foreign parties located in foreign States where they claim that the material has been uploaded from and is stored. Besides, the content is perfectly legal in the country where the party responsible for its publication operates.

Another important characteristic of the access-based jurisdictional approach is that, as some authors rightly observe, this principle seems to incorporate both the objective territorial principle and the effects doctrine.[5] In other words, the rationale behind its application by national courts is not always clear. More specifically, it is unclear whether the act of publishing content online is equated to having committed an act within the territory of the State where that content can be accessed or whether publishing content online, although occurring abroad, has produced an adverse effect within the territory of the country establishing jurisdiction. In this regard, the authors arguing that the objective territorial principle and the effects doctrine tend to merge when applied to cyberspace are correct.[6]

Having introduced the main characteristics of the access-based jurisdictional approach, the next section will provide an overview of key cases discussed before national and regional courts where this approach has been adopted.

2.3 Case selection

The cases examined in the next paragraphs are heterogeneous: they are related to different jurisdictions and different areas of law. These cases have been discussed before the national courts of Australia, US, Ireland, Canada, Hong Kong, UK, France and the Court of Justice of the European Union (CJEU). Eight out of nine cases are civil cases while the remaining one, *R v Perrin*, is a criminal one.[7] Seven cases deal with defamation (*Dow Jones v Gutnick,*[8] *Young v New Haven Advocate*,[9] *Coleman v MGN Limited,*[10] *Breeden v Black*,[11] *Yeung v Google Inc.*,[12] *eDate Advertising GmbH v X and Olivier*

[5] Hayashi (n 1) 298-301; Uerpmann-Wittzack (n 2) 1254-1255.
[6] ibid 298-299, 301.
[7] *R v Perrin* [2002] EWCA Crim 747.
[8] *Dow Jones and Company Inc v Gutnick* (2002) 210 CLR 575.
[9] *Young v New Haven Advocate et al*, 184 F. Supp. 2d 498 (W.D. Va. 2001); *Young v New Haven Advocate et al*, 315 F.3d 256 (4th Cir. 2002).
[10] *Coleman v MGN Limited* [2012] IESC 20 [4] (Denham CJ).
[11] *Breeden v Black* 2012 SCC 19 666.
[12] *Yeung, Sau Shing Albert v Google Inc.* HCA 1383/2012 (5 August 2014).

Martinez Robert Martinez v MGN Limited [13] and *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB*[14]), and two with the publication of content that violates criminal law (*R v Perrin* and *UEJF et Licra v Yahoo! Inc. et Yahoo France*[15]). Moreover, while eight out of nine cases are related to acts committed by defendants located in a foreign State, the case of *Young v New Haven* examines an inter-state dispute between parties situated in two different States within the United States.

Notwithstanding these differences, these cases all outline the difficulties that national courts face when establishing jurisdiction in Internet-related disputes over defendants located outside the domestic forum. Indeed, the national courts in these cases were faced with the same challenge: establishing when an act committed online by defendants located in another State can be said to have happened within the domestic court's jurisdiction. More importantly, the national courts in these cases have all given the same answer to this question: jurisdiction can be exercised in the country where the content published online can be accessed.

The case selection was conducted by relying on a theoretically informed, research question-driven approach. Indeed, the cases that were selected are those in which the access-based jurisdictional approach was adopted. The rationale behind this choice lies in the fact that this research aims to shed light on the distinctive characteristics and critiques of the use of the access-based jurisdictional criterion. These aspects emerge from the analysis of the cases where this approach has been adopted, irrespective of the country in which it was used, the area of law affected and the civil or common law nature of the legal system in place.

Establishing jurisdiction based on access would appear to be quite common among national courts, at least in the geographic areas covered by the cases selected. Indeed, many scholars investigating this subject agree that establishing jurisdiction based on access has become an increasingly popular and acceptable way for States to exercise jurisdiction over content posted online.[16] An example of this point can be found in the

---

[13] Joined Cases C–509/09 and C-161/10 *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* [2011] ECR I–10269.

[14] Case C-194/16 *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* [2017] ECLI:EU:C:2017:766.

[15] TGI Paris, référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* as reported in Juriscom.net 'TGI Paris, référé, 22 mai 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France' (*Juriscom.net*) < http://juriscom.net/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/> accessed 19 February 2017.

[16] Kohl 'Ignorance is no Defence' (n 3) 25-26, 37; Korff (n 4) 56. According to the Geneva Internet Disputes Resolution policy, the accessibility criterion has been mostly discredited and abandoned outside the EU community law. To substantiate this claim, the policy at page 4 refers to a series of national cases in England, France and the United States where this approach has been rejected, University of Geneva 'Geneva Internet Disputes Resolution Policies 1.0' (*Geneva Internet Disputes Resolution Policies 1.0*)

CJEU *eDate Advertising* case which shows that according to EU law the accessibility of online content from within the territory of a Member State can be a sufficient basis for that State to exercise jurisdiction over the content.[17] In addition, some authors underline how the access-based jurisdictional approach has been adopted by States transversally across different areas of law, rather than being associated with (or confined to) a specific area. Khol, for example, refers to a variety of documents and national laws that span from consumer protection to gambling and from defamation to obscenity when outlining some instances where this approach was adopted.[18] However, other commentators highlight how the access-based approach appears to be particularly common in a specific area of law, such as defamation.[19]

2.3.1 The *Dow Jones v Gutnick* case

The case of *Dow Jones and Company Inc v Gutnick* was decided in December 2002 by the High Court of Australia (HCA). The defamation proceedings were initiated in October 2000 by Mr. Gutnick, an Australian businessman and resident, who brought a case before the Supreme Court of Victoria. Mr. Gutnick sought compensation for damage to his reputation that he alleged had happened in Victoria. The harm to reputation was said to be caused by the publication of a defamatory article by the US-based Dow Jones on the subscription website WSJ.com, where the allegedly defamatory article was published as part of the *Barron's Online* journal.

Dow Jones applied to Hedigan J from the Supreme Court of Victoria asking for the current proceedings to be set aside and any further proceedings on the matter to be

---

<https://geneva-internet-disputes.ch/> accessed: July 2017), 4. However, this point is debatable. Indeed, the cases examined in this chapter show that as of 2017 this approach was still in use at least in the countries mentioned in the chapter. This view is also confirmed by other scholars, such as Michael Geist, who underline how some States have recurred to the access criterion to establish jurisdiction in cross-borders cases. See Michael Geist 'Courts adopt aggressive approach in cross-border Internet jurisdiction cases' (*The Star.com*, 5 January 2013). <https://www.thestar.com/business/2013/01/05/courts_adopt_aggressive_approach_in_crossborder_internet_jurisdiction_cases.html#.UOrJtuIHp7w.twitter> accessed 15 November 2017.

[17] *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* (n 13). See section 2.3.6 for an analysis of the *eDate* case.

[18] Kohl 'Ignorance is no Defence' (n 3) 26, 37. The documents cited by Khol are: European Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, No 44/2001 of 22 December 2000, OJ L 012, 16/01/2001 p. 1-23 (as cited by Kohl (n 3) 37); US v. Ross [1999] WL 782749 (SDNY) (as cited by Kohl (n 3) 37); National Sporttotaliser Foundation v. Ladbrokes Ltd District Court, The Hague, 27 January 2003 (as cited by Kohl (n 3) 37); Australian Securities and Investments Commission, Offers of Securities on the Internet, Policy Statement 141 (10 February 1999, reissued 2 March 2000), PS 141.5, 141.14, 141.16 (as cited by Kohl (n 3) 37); Dow Jones & Co Inc v. Gutnick [2002] HCA 56 (as cited by Kohl (n 3) 37); R v. Perrin [2002] EWCA 747 (as cited by Kohl (n 3) 37); R v. Tdben BGH, Urt. v. 12.12.2000-1 StR 184/00 (LG Mannheim), reproduced in Neue Juristische Wochenschrift, 8, p. 624 (as cited by Kohl (n 3) 37).

[19] Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 (2) Int J Law Info Tech 142, 149-157.

stayed.[20] Dow Jones claimed that the Supreme Court of Victoria did not have jurisdiction to hear the case as the publication of the allegedly defamatory article had happened in the United States, and more specifically in New Jersey, where the article was uploaded on the Dow Jones' servers. Hedigan J dismissed Dow Jones' appeal since he found that the defamation of Mr. Gutnick had happened in Victoria, where the article could be downloaded and was therefore comprehensible by readers located there.[21] The Court of Appeal of Victoria, dismissed Dow Jones' appeal and upheld the primary judge's decision.[22] The case was therefore brought to the High Court of Australia (HCA).

In its judgment, the HCA explained that Australian common law choice of law requires the judges to apply the law of the place of the tort, which in the present case is defamation. The judges then explained the main elements of the tort of defamation. They stated that under Australian law defamation is defined as damage to reputation due to the publication of defamatory material. The HCA also added that the tort of defamation is usually located at the place where the damage to reputation occurs. In addition, the judges clarified that since the actionable wrong is the damage to reputation, for the tort of defamation to exist, not only has the material to be published, it must also be made available to the reader in comprehensible form.[23] This is because it is only when the material is comprehended by a third party that the damage to reputation occurs.[24] Indeed, the Court specified that publication of defamatory material must be interpreted as 'a bilateral act - in which the publisher makes it available and a third party has it available for his or her comprehension'.[25] Therefore, the Court found that the respondent's claim that the damage to his reputation had happened in Victoria was correct. Indeed, Mr. Gutnick had a reputation in Victoria and it was in Victoria that the material published online could be downloaded and was therefore comprehensible to readers. As stated by the Court

> '[i]n the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed'.[26]

[20] *Dow Jones and Company Inc v Gutnick* (n 8) [5].
[21] ibid [7].
[22] ibid [8].
[23] ibid [25]-[26].
[24] ibid [26].
[25] ibid.
[26] ibid [44].

2.3.2 The *Young v New Haven Advocate* case

Legal proceedings in the case of *Young v New Haven Advocate* were initiated by Mr. Young, an American citizen who lived and worked in Virginia as a warden in the Wallens Ridge State Prison.[27] On 12 May 2000 Mr. Young sued two Connecticut-based newspapers, the New Haven Advocate and the Hartford Courant, their editors, and two journalists who worked for the newspapers. The appellant's claim was related to the publication of some allegedly defamatory articles on the newspapers' respective websites.[28] The articles were focused on the transfer of some inmates from Connecticut to Virginia. Mr. Young claimed that the articles contained allegations that he was a racist and favoured the mistreatment of the Wallens Ridge inmates.[29] The proceedings were brought before Virginia Western District Court.

The defendants asked the Court to dismiss the proceedings due to lack of personal jurisdiction over them. Indeed, the defendants, who were based in Connecticut, claimed that they did not operate in Virginia and neither their articles nor their websites targeted a Virginia audience. On the other hand, Mr. Young contended that the fact that the defendants maintained the websites and had published the articles online equated to conducting business activities in Virginia.[30] Therefore, according to the plaintiff's claim, Virginia Western District Court had jurisdiction to hear the case.

In its decision of 10 August 2001, the District Court found that it had jurisdiction over the Connecticut-based defendants pursuant to section 8.01-328(A) (3) of the Code of Virginia.[31] Point (3) establishes that Virginian courts have jurisdiction over non-resident defendants who cause tort or injuries by an act or omission committed in Virginia.[32] The District Court found that the defendants had acted within the territory of Virginia because they had published allegedly defamatory articles on their websites, which were accessible in Virginia.[33] In addition, the judges found that the exercise of personal jurisdiction over the defendants did not violate the requirements of due process because of two main facts.[34] First, the articles published online were related to events that had happened in Virginia and at least one of those articles expressly mentioned Mr.

---

[27] *Young v New Haven Advocate et al* W.D. (n 9) 500.
[28] *Young v New Haven Advocate et al*, 4th Cir. (n 9) 501.
[29] ibid.
[30] ibid 502.
[31] Va.Code Ann. § 8.01-328.1(A) (3).
[32] 'A court may exercise personal jurisdiction over a person, who acts directly or by an agent, as to a cause of action arising from the person's […] Causing tortious injury by an act or omission in this Commonwealth' ibid.
[33] *Young v New Haven Advocate et al* W.D. (n 9) 508.
[34] ibid 511.

Young, a Virginia resident.[35] Secondly, when posting those articles online, the defendants knew that that material was accessible to Virginia residents and that therefore any potentially defamatory content related to a Virginia resident was going to produce harm in Virginia.[36] In this regard, the Court added that since content published online is accessible to a worldwide audience, it is 'physically "present" in different locations at one time' and can therefore be subjected to multistate jurisdiction.[37] Finally, the Court found that the exercise of personal jurisdiction was legitimate because Virginia had a proper interest in preventing its residents being subjected to online defamation.[38] Therefore, the District Court denied the defendants' motion to dismiss for lack of personal jurisdiction.[39]

The defendants appealed to the Fourth Circuit Court of Appeal, which issued its decision on 13 December 2002. Unlike the District Court, the Court of Appeal accepted the defendants' claim that Virginia courts lacked personal jurisdiction over them and therefore reversed the District Court's order.[40] Indeed, the judges found that Virginia Courts could not exercise jurisdiction over the out-of-state defendants since neither their websites nor their articles were directed at a Virginia audience. In this regard, the Court stated that the mere publication of content online by people living outside a given State is not sufficient to bring them within the jurisdiction of that State or within the jurisdiction of any State from which that content is accessible. The consequence of adopting this jurisdictional approach would be to violate the due process principle, which regulates the exercise of State jurisdiction over out-of-State residents.[41] The judges found that '[s]omething more than posting and accessibility is needed' for a State to establish jurisdiction over online content posted by Internet users located in another State.[42] More specifically, 'an intent to target and focus' on the audience located in a given State is necessary for that State to establish jurisdiction over the person responsible for the publication of that content online.[43]

The criteria relied upon by the Court to establish whether the two newspapers had intentionally targeted Virginia were the absence of advertisement aimed at a Virginia audience, Connecticut-based weather and traffic information, and links to Connecticut

[35] ibid 508.
[36] ibid.
[37] ibid 509.
[38] ibid 510.
[39] ibid 511.
[40] *Young v New Haven Advocate et al* 4th Cir. (n 9) 3.
[41] ibid 10.
[42] ibid.
[43] ibid.

institutions.[44] The judges then turned to the content of the allegedly defamatory articles to determine whether the articles targeted Virginia. In this case as well, the Court found that the articles were focussing on events and policies that affected Connecticut, rather than Virginia.[45] Therefore, because both the websites and the articles were not manifestly targeting Virginia, the Court of Appeal concluded that the defendants did not have 'sufficient Internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them'.[46]

2.3.3 The *Coleman v MGN Limited* case

John Coleman, an Irish citizen living in Ireland, brought legal proceedings against MGN Limited, the England-based editorial group which publishes, sells and supplies the newspaper Daily Mirror. The proceedings were brought before the High Court of Ireland. Mr. Coleman alleged that he had been defamed by MGN due to the publication of two articles and a photograph of him accompanying the articles. The articles and the picture appeared in March and September 2003's printed editions of the Daily Mirror. Although Mr Coleman's name was not mentioned in the articles, he claimed that he had been defamed due to the juxtaposition of the picture and the articles. Since the articles talked about excessive alcohol consumption in the UK, Coleman claimed that it could be inferred that their content was referring to him.

Originally, Mr Coleman's claim was confined to the circulation on the Irish territory of printed copies of the Daily Mirror.[47] MGN asked the High Court to decline jurisdiction, but Charleton J dismissed the defendant's request. MGN appealed to the Supreme Court against the High Court's decision. The company argued that Irish Courts lacked jurisdiction because the alleged defamation had happened in England, where MGN was established.[48] In addition, the appellant pointed out that there was no evidence of the circulation of the relevant printed editions of the Daily Mirror on the Irish territory.[49]

In the proceedings before the Supreme Court, however, Mr Coleman's claim changed to focus exclusively on the publication of the said articles and picture on the Internet. More specifically, the plaintiff's argument was that the damage to his reputation had happened on the Irish territory because the Daily Mirror was published online at the time

[44] ibid 10-11.
[45] ibid 11.
[46] ibid.
[47] *Coleman v MGN Limited* (n 10) [4].
[48] ibid [7].
[49] ibid.

of the proceedings before the Supreme Court, in 2012.[50] It could therefore be assumed that in 2003 the defamatory material had been published online as well, and was accessible from within Ireland's territory.[51] The Supreme Court dismissed Mr. Coleman's argument because it evidenced several 'fatal flaws'.[52] Indeed, although the appellant's claim shifted from the publication of printed copies of the newspaper to its online publication, it was never pleaded that the relevant material had been published online.[53] More importantly, the Court found that for the tort of defamation to be established, it is essential to produce evidence of publication of the defamatory material within the domestic jurisdiction. However, the Court stated that no evidence had been produced showing that the defamatory content or the Daily Mirror itself had been published online in 2003. In addition, there was no evidence that the defamatory material had been accessed from within the territory of Ireland. For these reasons, the Supreme Court established that it did not have jurisdiction on the subject matter of the case.[54]

The approach followed by the Supreme Court to deny jurisdiction over this case seems to confirm the access-based jurisdictional criterion. Indeed, had Mr. Coleman produced evidence of both the online publication of the defamatory material and actual access to it within the Irish territory, the Supreme Court would have held that the tort of defamation had happened in Ireland. This is irrespective of where the material had been uploaded from, or where it was hosted.

2.3.4 The *Breeden v Black* case

Lord Black is a businessman with an established reputation both in Canada and internationally. He was a Canadian citizen until 2001, when he abandoned the citizenship to become part of the House of Lords in the UK.[55] Between 2004 and 2005, Lord Black brought six libel actions in the Ontario Superior Court of Justice against ten defendants.[56] The defendants were directors, advisors and vice-president of the company International, of which Lord Black was a chairman. International was both incorporated and headquartered in the United States.[57] All the defendants lived in the United States, except for two of them who lived in Ontario and Israel respectively.[58]

[50] ibid [10].
[51] ibid.
[52] ibid [14].
[53] ibid.
[54] ibid.
[55] *Breeden v Black* (n 11) [3].
[56] ibid [1], [5].
[57] ibid [3].
[58] ibid [8].

Lord Black claimed that he had been defamed due to the publication on the company's website of some reports and press releases containing allegations that he had received illegitimate payments from International. The plaintiff brought the libel actions in Ontario since the defamatory content published on the website was accessed, read and republished in Ontario by three newspapers.[59]

The defendants asked the motion judge to stay the case because there was no real and substantial connection between the actions and Ontario. Alternatively, they maintained that US courts were a more appropriate forum.

The motion judge dismissed these arguments and found that the defamation had happened in Ontario due to three main reasons. First, the content published on the website was accessible in Ontario, where it was republished by the three newspapers. Second, Lord Black had a reputation in Ontario. Finally, it was reasonably foreseeable for the defendants to anticipate that the publication of that content would have caused damage to the plaintiff's reputation in Ontario.[60]

The Ontario Court of Appeal upheld the motion judge's decision because it found that the clear and substantial connection requirement was satisfied. In addition, the Court stated that it was not necessary to determine whether a targeting approach should be adopted in Canadian law.[61] In other words, according to the Court, it was not necessary to determine whether the content published online was targeting a Canadian audience. Notwithstanding this, the judges emphasized that the relevant content did target Ontario because the press releases contained contact information directed at Canadian media.[62]

The defendants appealed against the Court of Appeal's decision and brought the case before the Supreme Court of Canada. They maintained that in transnational libel claims jurisdiction should be exercised only in the forum that has a real and substantial connection with the 'substance of the action'.[63] The defendants claimed that the 'substance of the action' could be found in Lord Black's actions, which constituted the subject matter and conduct giving rise to the case. Since these actions had happened in the United States, the defendants claimed that there was no real and substantial connection between Canada and the case.[64]

[59] ibid [6].
[60] ibid [11].
[61] ibid [13].
[62] ibid.
[63] ibid [15].
[64] ibid.

The Supreme Court found that the appellants were liable for the tort of defamation in Canada because the defamation had happened there.[65] Indeed, it was in Ontario that the defamatory content displayed on the website was published to a third party: the three newspapers which accessed the material, read and republished it.[66] The Court added that according to Canadian law, each republication of a defamatory statement can be considered as a new publication. Besides, the original publisher of the defamatory statement is responsible for its republications if it authorizes them or if the republication 'is the natural and probable result of the original publication'.[67] Finally, the Supreme Court concluded that Ontario was a convenient forum because the appellants had failed to unequivocally show that US courts constituted a clearly more appropriate forum.[68]

2.3.5 The *Yeung v Google Inc.* case

Albert Yeung, a businessman and managing director of the Hong Kong-based Emperor Group, brought a defamation complaint against Google Inc. before the High Court of the Hong Kong Special Administrative Region.[69] The complaint was related to the Google Search Autocomplete search function.

Yeung alleged that when searching for his name on Google.com, Google.com.hk and Google.com.tw the autocomplete suggestion "triad" came up.[70] The plaintiff therefore claimed to have been defamed by Google Inc. and asked for compensation, adding that the company had failed to remove the defamatory content notwithstanding the several requests received.[71]

Google Inc. argued that the Hong Kong Court lacked personal jurisdiction over it. Besides, the defendant maintained that there was no good arguable case or serious issue to be treated on the merits of the case brought by the plaintiff.[72] For this reason, Google Inc. asked the Court to either declare that it had no jurisdiction over the case or alternatively to refuse to exercise any jurisdiction it may have.

Due to the scope of this analysis, the only part of the judgment that will be examined in this chapter is that related to establishing where Mr. Yeung's alleged defamation happened.

---

[65] ibid [20].
[66] ibid.
[67] ibid.
[68] ibid [29].
[69] *Yeung, Sau Shing Albert v Google Inc.* (5 August 2014) (n 12) [2].
[70] ibid [4]. According to Cambridge Dictionary, triad is 'a secret Chinese organization involved in illegal activities such as selling drugs' Cambridge Dictionary 'Triad' (Cambridge Dictionary) <https://dictionary.cambridge.org/dictionary/english/triad> accessed 27 July 2020.
[71] *Yeung, Sau Shing Albert v Google Inc.* (5 August 2014) (n 12) [10].
[72] ibid [15].

Yeung argued that the tort of defamation had happened in Hong Kong, since the damage to reputation had either been sustained there or it had happened following an act committed in Hong Kong.[73] More specifically, the plaintiff maintained that the defamation had occurred in Hong Kong because it was there that the defamatory content could be accessed (i.e. downloaded) and was therefore published to a third party.[74]

The Court confirmed this view, by stating that in defamation cases the damage to reputation occurs when the defamatory content is published or made available to a third party. When the defamatory content is published online, the content is believed to have been published in the place where the material is 'viewed/downloaded'.[75] The other condition for the exercise of jurisdiction by the domestic forum is that the plaintiff has a reputation there.[76] Therefore, the Court concluded that 'an internet publisher who places material on the internet will be responsible for the effects of his action whenever the damage occurs'.[77]

Google accepted the principles set out by the Court regarding defamation through online publication.[78] However, it contended that the plaintiff had failed to prove that there had been publication to a third party. In this regard, Yeung argued that the proof of publication to a third party was represented by the fact that the IT department of his company had been able to download and print the defamatory words. Google's counter argument was that the IT department could not be considered as a genuine third party, since the people in the IT department worked for Yeung and had been expressly tasked to find the defamatory material.[79]

The Court dismissed Google's point and found that the IT department did constitute a genuine third party, irrespective of the fact that its members were employed by Yeung. Indeed, the people working for Mr. Yeung could still be considered as a party other than Yeung that accessed the defamatory content.[80]

Overall, the Court dismissed all Google's claims and awarded the costs to the plaintiff.[81] In September 2014, Google filed a motion for the Leave to Appeal Against the Order, which was granted by the Court in October 2014.[82] In particular, Google argued

[73] ibid [18].
[74] ibid [19].
[75] ibid [37].
[76] ibid.
[77] ibid.
[78] ibid [39].
[79] ibid.
[80] ibid [41]-[42].
[81] ibid [184].
[82] *Yeung, Sau Shing Albert v Google Inc* HCA 1383/2012 (29 October 2014) [4], [38].

that, due to the lack of sufficient publication to a third party, allowing the libel action to proceed before the domestic Court would have been a disproportionate exercise of jurisdiction.[83] The High Court granted Google's leave to appeal because it found that, due to the novelty of this area of law, the Court of Appeal's guidance was needed on how to proportionally exercise jurisdiction and avoid unnecessary expensive and lengthy defamation proceedings.[84] There has been no decision regarding Google's appeal to date.[85] This case is therefore still ongoing.

2.3.6 The CJEU approach to establishing jurisdiction based on access: the *eDate Advertising* and the *BOÜ* case

The *eDate Advertising* case is a joined case discussed by the Court of Justice of the European Union (CJEU) on 25 October 2011.[86] The case concerns the interpretation of article 5(3) of the Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters and article 3(1) and (2) of the Directive 2003/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects on information society services.[87] This case was referred to the CJEU by the German Federal Court of Justice, the Bundesgerichtshof, and the Paris Regional Court, Tribunal de Grande Instance (TGI). The case concerns the liability of the Austria-based eDate Advertising and the England-based MGN Limited before the German and French courts respectively for an alleged infringement of personality rights due to the publication of content online. In particular, the Austrian company eDate Advertising was asked by X, a German resident, to refrain

[83] ibid [7].
[84] ibid [21].
[85] Columbia University Global Freedom of Expression, 'Dr. Yeung, Sau Shing Albert v. Google Inc.' (*Columbia University Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/dr-yeung-sau-shing-albert-v-google-inc/> accessed 28 July 2020.
[86] *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* (n 13).
[87] ibid para 1. Similarly to the *eDate Advertising* case, the CJEU had the opportunity to examine the application of article 5(3) of the Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJL12/1 in the case Case C-441/13 *Pez Hejduk v EnergieAgentur.NRW GmbH* [2015] ECLI:EU:C:2015:28, which was, however, related to an infringement of copyright as a result of the publication of some pictures online rather than an infringement of personality rights. In that case, the CJEU confirmed the validity of the access-based jurisdictional approach in regard to copyright violations, stating at para 39 that '[a]rticle 5(3) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that, in the event of an allegation of infringement of copyright and rights related to copyright guaranteed by the Member State of the court seized, that court has jurisdiction, on the basis of the place where the damage occurred, to hear an action for damages in respect of an infringement of those rights resulting from the placing of protected photographs online on a website accessible in its territorial jurisdiction. That court has jurisdiction only to rule on the damage caused in the Member State within which the court is situated'.

from using his full name when reporting on the website administered by the company about a crime that X committed in 1990.[88] As to MGN, the company was accused by the French actor Olivier Martinez and his father of having violated their right to private life and the actor's right to his image. These violations had resulted from the posting of an article on the Sunday Mirror website giving details about a meeting between Olivier Martinez and Kylie Minogue and alleging that the actor had resumed his relationship with the singer.[89] Both eDate Advertising and MGN claimed that the German and French courts lacked jurisdiction due to the absence of a sufficient connecting link between the content published online and the damage produced on the German and French territory.[90]

With regard to the interpretation of article 5(3) of the EU Council Regulation on jurisdiction, the CJEU was asked by the Bundesgerichtshof and the TGI to clarify how the expression 'the place where the harmful event occurred or may occur' contained in article 5(3) can be interpreted when content is published online.[91] According to the Regulation, jurisdiction is generally based on the place of domicile of the defendant. However, article 5(3) establishes that in the case of a tort a person domiciled in a given Member State can be sued in another Member State if the harmful event occurs there.[92] The CJEU first clarified that the place where the harmful event occurs can be both the place giving rise to the event, and the place where the damage occurs. Both these criteria constitute 'a significant connecting factor' as far as jurisdiction is concerned.[93] In addition, the Court found that in the case of an infringement of personality rights due to the publication of online content, the place where the harmful event occurs can be interpreted as the place where the victim has his or her centre of interest. This is usually the place where the person resides, however it can also be the place where they conduct professional activities, irrespective of whether they live there. In other words, when defamatory material is published online, the victim might choose to initiate legal proceedings in the Member State where they have their centre of interest. That State, as underlined by the Court, will have jurisdiction in respect to all the damage caused by the publication.[94] According to the CJEU, the criterion of the place where the victim has their centre of interest is respondent to the principles of the 'sound administration of justice' and predictability of jurisdiction.[95] This is because a court in the place where a person has

[88] *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* (n 13) para 17.
[89] ibid para 25.
[90] ibid paras 18, 26.
[91] ibid para 37.
[92] ibid para 6.
[93] ibid para 41.
[94] ibid para 48.
[95] ibid paras 48-50.

their centre of interest is best placed to assess the impact of the online publication of defamatory content on that person's reputation. As to predictability, the CJEU stated that the publisher is or should be in a position to know where the person to whom the online content refers has their centre of interest. In other words, this criterion has the benefit of both being predictable for the defendant and easily allowing the applicant to know where they might be able to initiate legal proceedings.[96]

However, the CJEU added that there is another choice available to victims of online defamation. They can also initiate legal proceedings in the Member States where the content published online can be accessed. In that case, however, the national courts will have jurisdiction only in respect to the damage to reputation that happened locally.[97]

In sum, according to the EU Regulation on jurisdiction, in case of defamation committed trough the publication of content online, jurisdiction can be exercised by the Member State where the publisher is established or the Member State where the victims have their centre of interest in regard to all the damage caused by the publication. Jurisdiction can also be exercised by all the Member States where the online content can be accessed in regard to the damage to reputation that happened within that Member State, provided that the victims have a reputation there.[98]

In October 2017, the CJEU had the opportunity to further clarify the application of the access-based jurisdictional approach to torts committed online in the case *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (the BOÜ case).[99] In this case, the Court was asked to pronounce on the application of article 7(2) of the Regulation (EU) 1215/2012 of the European Parliament and of the Council of the 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.[100] This Regulation entered into force in January 2015 replacing the Council Regulation (EC) No 44/2001 of 22 December 2000. Article 7(2) and article 5(3) mentioned above are however identical in wording.

The applicants in the BOÜ case, the Estonian company BOÜ and a company's employee Ms Ingrid Ilsjan, brought an action against the Swedish company Svensk Handel before the Harju Court of First Instance in Estonia. The applicants asked the Estonian Court to order Svensk Handel to rectify the incorrect and allegedly defamatory

[96] ibid.
[97] ibid para 51.
[98] ibid para 52.
[99] *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (n 14).
[100] 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 [2012] OJ L 351/1 entered into force on 10 January 2015.

information that the Swedish company had published on its website regarding the Estonian company, to delete the related comments published on a discussion forum of the website and to pay compensation for the damages caused to both the applicants.[101] In particular, the applicants argued that the damage to their reputation had happened in in Sweden, since, following the publication of the defamatory information, BOÜ's turnover in Swedish kronor was reduced.[102]

The Estonian Harju Court of First Instance, however, found that article 7(2) of Regulation 1215/2012 was not applicable in this case. Indeed, according to article 7(2) in cases related to tort a party domiciled in a Member State can be sued in the Courts of another Member State if the harmful event occurred there or if it has its centre of interest in that State. However, the Court underlined that the damage to the applicants' reputation had happened in Sweden, rather than in Estonia, as the comments had been published in Swedish, and were therefore incomprehensible to an Estonian audience without translation. In addition, the fact that the loss in turnover was referenced in Swedish kronor rather than Euro supported the finding that the damage had not happened in Estonia.[103] In other words, the Court found that the mere accessibility of the website in Estonia did not justify the initiation of legal proceedings there. For this reason, the Court of First Instance declared that the case was inadmissible.[104] After multiple appeals by the applicants, the case reached the Estonian Supreme Court which decided to refer it to the CJEU. In particular, the CJEU was asked to clarify *inter alia* whether a victim of online defamation can bring requests for rectification of the incorrect information and removal of defamatory comments before the courts of every Member State where that content is accessible in reference to the damage suffered in that Member State.[105]

---

[101] *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (n 14) para 9.
[102] ibid para 10.
[103] ibid para 11.
[104] ibid.
[105] ibid para 21. At para 21 (2) the CJEU was also asked to clarify whether a legal person which claims that its personality rights have been infringed as a result of the publication of content on a website can bring legal proceedings regarding the compensation for the damage to the reputation, rectification of the incorrect information published and removal of the defamatory comments before the courts of the Member State where that legal person has its centre of interest in relation to all the damage suffered. In addition, the Estonian Supreme Court asked the CJEU at para 21(3) which criteria can be used to establish where a legal person has its centre of interests. The CJEU answered the first question in the affirmative, stating at paras 32 and 44 that a legal person can bring an action for compensation of the damage to the reputation suffered, removal of the offensive content and rectification of the incorrect information before the courts of the Member State in which that legal person has its centre of interest. In regard to the latter, the CJEU found at para 41 that this is the place where the legal person carries out the main part of its economic activities. This can be the place where the legal person has its registered office, however the location of the office is not in itself a conclusive criterion. Indeed, the judges found at para 42 that in case the legal person carries out the main part of its economic activities in a Member State other than the one in which it has its registered office, it will be the latter Member State that will be competent to exercise jurisdiction over the legal person's claims.

The CJEU stated that, as far as rectification and removal requests are concerned, the accessibility criterion is not sufficient to establish jurisdiction. Indeed, the judges found that, unlike a request for damages which by its nature can be locally circumscribed to the damages that the victim suffered in each Member State where the illegal content can be accessed, the application for rectification and removal of online content is indivisible. This is due to the ubiquitous nature of online content and to its universal distribution. For this reason, the only court that can exercise jurisdiction on an application for rectification and removal of online content is the court that can rule on the entirety of a request for damage, therefore either the court of the domicile of the defendant or the court of the victim's centre of interest.[106]

Overall, the *eDate Advertising* and the *BOÜ* case show that, although exercising jurisdiction based on access to online content is still legitimate according to EU law, that exercise must be limited to requests for local damages only.

2.3.7 The *Perrin* case

Mr. Perrin, a French national who lived in the United Kingdom, was one of the major shareholders of the US-based Metropole News Group, the company administering the website www.sewersex.com.[107] On 25th October 1999, a police officer of the Obscene Publications Unit in the UK accessed during the course of his duty some pictures of a sexual nature which had been published on the above-mentioned website.[108] More specifically, the pictures were on a preview page available free of charge on the website. The images available on the preview page were deemed to violate section 2(1) of the Obscene Publications Act 1959 which prohibited the publication of obscene material.[109] As a result, Mr. Perrin was arrested. During an interview with the police, he accepted the responsibility for the publication of the pictures.[110] On 16 October 2000 he was convicted by Southwark Crown Court for the publication of an obscene article.[111] On 6 November

---

[106] ibid para 48.
[107] *R v Perrin* (n 7) [4].
[108] The pictures showed 'people covered in faeces, coprophilia or coprophagia, and men involved in fellatio', ibid [2].
[109] 'Prohibition of publication of obscene matter. (1) Subject as hereinafter provided, any person who, whether for gain or not, publishes an obscene article or who has an obscene article for publication for gain (whether gain to himself or gain to another)] shall be liable— (a) on summary conviction to a fine not exceeding one hundred pounds or to imprisonment for a term not exceeding six months; (b)on conviction on indictment to a fine or to imprisonment for a term not exceeding [five years] or both', Obscene Publications Act 1959, pt 2, s(1) (a)(b).
[110] As to Mr. Perrin's formal admission, 'when the case came on for trial at Southwark Crown Court in October 2000 counsel then appearing for the appellant made a formal admission on his behalf – "It is agreed and accepted by the defendant that he was legally responsible for the publication of the articles referred to in counts 1, 2 and 3 on the indictment"', *R v Perrin* (n 7) [5].
[111] ibid [1].

2000 Southwark Crown Court sentenced Mr. Perrin to 30-month imprisonment.[112] Mr. Perrin appealed against his conviction to the Criminal Division of the England and Wales Court of Appeal (EWCA). The Court of Appeal, however, dismissed both Mr. Perrin's appeal against the conviction and his subsequent appeal against the sentence.[113] Mr. Perrin therefore filed an application to the European Court of Human Rights (ECtHR) to bring a case against the United Kingdom. His main claim was that the UK had violated article 10 of the European Convention on Human Rights (ECHR) by convicting and sentencing him for the publication of the pictures on the website www.sewersex.com.[114] The ECtHR, however, dismissed Mr. Perrin's claim and declared the application inadmissible.[115]

Mr. Perrin stated in his application to the ECtHR that due to 'the worldwide nature of the internet, it was unreasonable for publishers to foresee the legal requirements in all the individual states where the material could be accessed'.[116] He therefore suggested that it should only be possible for English courts to convict 'if major steps towards publication had taken place in a location over which they had jurisdiction'.[117] Besides, Mr. Perrin claimed that the publication of the pictures did not happen within the territory of the United Kingdom.[118] In fact, it happened in the United States, where the pictures were legal as the Obscene Publications Act 1959 did not apply.[119] For this reason, section 2 of the 1959 Act was neither sufficiently foreseeable nor sufficiently precise to be considered as "prescribed by law" within the meaning of Article 10 § 2 of the Convention.[120]

As to the approach adopted by the EWCA regarding establishing jurisdiction on the case, the judges found that 'a mere transmission of data constitutes publication'.[121] The

---

[112] ibid.
[113] ibid [52].
[114] *Perrin v the United Kingdom* App no 5446/03 (ECtHR, 18 October 2005) 5.
[115] ibid 10.
[116] ibid 5.
[117] ibid.
[118] ibid. More specifically, in the case before the Court of Appeal, the counsel stated at [32] that the UK courts could not assume that the major steps towards the publications of the pictures had happened within the territory of the UK. Indeed, Mr. Perrin's counsel claimed at [17] that 'the sole evidence of publication adduced at the Crown Court was of one visit by PC Ysart to the relevant web page, the preview page' and at [33] that there was no sufficient evidence as to where the data files where created and posted. It was also equally unclear where the server hosting the data was located, *R v Perrin* (n 7) [17], [32]-[33].
[119] 'In his first ground of appeal the appellant contends that there was no evidence to rebut his statements in interview that the major steps involved in publishing the web page that resulted in his conviction were in a jurisdiction where the material published was lawful', *R v Perrin*, (n 7) [32]. 'The applicant submitted that section 2 of the 1959 Act was not sufficiently foreseeable to satisfy the requirements of law within the meaning of Article 10 § 2 of the Convention because the major steps towards publication took place in the United States, where the 1959 Act did not apply', *Perrin v the United Kingdom* (n 114) 5.
[120] *Perrin v the United Kingdom* (n 114) 5.
[121] *R v Perrin*, (n 7) [18].

Court also added that, as established in the *R v Waddon* case, 'there is publication for the purposes of section 1(3) both when images are uploaded and when they are downloaded'.[122] In addition, the judges rejected the appellant's claim that there should be prosecution against a publisher only when the major steps towards the publication had happened within the territory of the State exercising jurisdiction. The EWCA also rejected Mr. Perrin's claim according to which the Crown should have shown where the major steps towards the publication were taken. In this regard, the Court accepted the respondent's argument that adopting Mr. Perrin's approach would have had the effect of encouraging publishers to publish only in countries where there were less chances of being prosecuted.[123] Overall the Court of Appeal concluded that 'the publication shown by the evidence was sufficient to give jurisdiction to the Court'.[124]

As to the admissibility decision of the ECtHR, the judges of the European Court clarified that section 2 of the Obscene Publications Act 1959 had been already examined by the Court in the cases *Handyside* and *Hoare* and that it had been found in compliance with article 10 of the ECHR.[125] Although those cases did not involve publication on the Internet, the Court stated that section 1(3) of the 1959 Act makes it clear that the law also applies to transmission of data stored electronically.[126] Besides, the Court observed that Mr. Perrin was a UK resident and could therefore not claim that the UK laws were not reasonably accessible to him. Moreover, since he was carrying out a professional activity through his website he should have acted more cautiously than normally expected and should have sought legal advice.[127] In addition, the Court found that the fact that the images available on Mr. Perrin's website were legal in the US did not mean that the UK had exceeded its margin of appreciation by proscribing the circulation of those images within its territory and by prosecuting and convicting the applicant.[128] Finally, in assessing the proportionality of the conviction and sentence by the UK domestic courts, the ECtHR gave particular relevance to the fact that Mr. Perrin was conducting a

---

[122] ibid [18]. In this regard the respondent for the Crown Prosecution Service argued before the EWCA at [51] that 'there was publication when anyone accessed the preview page'.
[123] *R v Perrin*, (n 7) [51]; 'Finally, it [the EWCA] noted, on the jurisdictional point, that the applicant's suggestion, that conviction should only be possible where major steps had been taken towards publication in a place over which the court had jurisdiction, would undermine the aim that the law was intended to protect by encouraging publishers to take the steps towards publication in countries where they were unlikely to be prosecuted', *Perrin v the United Kingdom* (n 114) 3.
[124] *R v Perrin*, (n 7) [52].
[125] *Perrin v the United Kingdom* (n 114) 6. In particular, the ECtHR referred to the cases *Handyside v. the United Kingdom* (judgment of 7 December 1976, Series A no. 24, § 44) (as cited in *Perrin v the United Kingdom* (n 114) 3) and *Hoare v. the United Kingdom* (no. 31211/96, Commission decision of 2 July 1997) (as cited in *Perrin v the United Kingdom* (n 114) 3).
[126] *Perrin v the United Kingdom* (n 114) 6.
[127] ibid.
[128] ibid 7-8.

professional activity whose services were available upon payment. In this regard, the Court concluded that

> 'it would have been possible for the applicant to have avoided the harm and, consequently, the conviction, while still carrying on his business, by ensuring that none of the photographs were available on the free preview page (where there were no age checks). He chose not to do so, no doubt because he hoped to attract more customers by leaving the photographs on the free preview page'.[129]

Ultimately, the ECtHR found that Mr. Perrin's application was inadmissible as manifestly ill-founded since its conviction could be considered as necessary in a democratic society to protect morals and or the rights of others.[130]

2.3.8 The *LICRA and UEJF v Yahoo! Inc. and Yahoo France* case

The *LICRA and UEJF v Yahoo! Inc. and Yahoo France* case (hereafter the *Yahoo!* case) was initiated in France in May 2000 by two French associations combating racism and anti-Semitism, the Ligue Contre la Racisme et l'Antisémitisme (LICRA) and the Union des Etudiants Juifs de France (UEJF). LICRA and UEJF brought a case before the Tribunal de Grande Instance (TGI) of Paris accusing Yahoo! Inc. and Yahoo France of having violated article R.645-1 of the French penal code, according to which the display of Nazi-related items for sale is a criminal offence.[131] More specifically, the two companies were accused of having violated the French penal code because Internet users located in France could access the *Yahoo! Auction* webpages where Nazi memorabilia were displayed for sale. The *Yahoo! Auction* website was maintained by Yahoo! Inc. and could be accessed by all Internet users via the Yahoo.com portal or through a link to Yahoo.com available on Yahoo.fr. The fact that the *Yahoo! Auction* webpage containing the Nazi-related items could be accessed by users located in France was equated by the plaintiffs to having committed a crime within the French territory. Therefore, LICRA and UEJF asked the TGI to issue an order requesting the defendants to prevent Internet users

---

[129] ibid 8.
[130] ibid.
[131] TGI Paris, référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* (n 15); Marc H. Greenberg, 'A Return to Lilliput: The LICRA v Yahoo! Case and the Regulation of Online Content in the World Market' (2003) 18 Berk. Tech L J 1191; Yaman Akdeniz, 'Case analysis of League against Racism and Antisemitism (LICRA), French Union of Jewish Students v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Pairs), Interim Court Order, 20 November, 2000' (*Yaman Akdeniz Academia.edu*) <https://www.academia.edu/943441/Case_Analysis_of_League_Against_Racism_and_Antisemitism_LICRA_French_Union_of_Jewish_Students_v_Yahoo_Inc_USA_Yahoo_France_Tribunale_de_Grande_?auto=download> accessed 09 September 2020. A version of this article was published on (2001) 1(3) EBLR 110.

located within the French territory from accessing the Nazi memorabilia displayed for sale on the Auction website.[132]

The defendants rejected the plaintiffs' claims. Indeed, Yahoo! Inc. stated that the French court lacked jurisdiction since the display and sale of the Nazi items had happened in the United States, where both the company and its servers were based.[133] Moreover, Yahoo! Inc. claimed that any restrictions on the accessibility of the items on sale would have violated the First Amendment of the US constitution in addition to being technically impossible to realize.[134] As to Yahoo France, which was accused of promoting anti-Semitism due to the link to Yahoo.com, it denied liability since the auction was not hosted on Yahoo.fr.[135]

In its order of 22 May 2000, the TGI established that it had jurisdiction over the case pursuant to article 46 of the Code of Civil Procedure. Article 46 establishes that in tort matters a plaintiff may bring a case before 'the court of the place of the event causing liability or the one in whose district the damage was suffered'.[136] Gomez J found that making it possible for users in France to access a website where Nazi memorabilia were displayed for sale equated to committing a wrong within the French territory that produced harm in France.[137] The judge therefore accepted LICRA and UEJF claims and ordered Yahoo! Inc. to '"take all necessary measures to dissuade and render impossible"' from within the French territory '"any access via Yahoo.com to the Nazi artefact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes"'.[138] At the same time, Yahoo France was ordered to issue all the Yahoo.fr Internet users with a warning that if they were to continue their search on Yahoo.com and were provided with search results that included sites that violated French law they should stop their search. Failure to do so would expose them to liability under French law.[139]

Following the 22 May order, Yahoo France modified its terms of use and introduced a banner reproducing the warning issued in the order.[140] On the other hand, Yahoo! Inc.

---

[132] TGI Paris, référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* (n 15).
[133] ibid.
[134] ibid.
[135] ibid.
[136] Art. 46 nouv. C. pr. civ, English translation as reported in Legifrance 'Code Of Civil Procedure' (*Legifrance*) <https://www.legi**france**.gouv.fr/content/download/1962/13735/version/3/.../**Code**_39.pdf> (Accessed: 20 February 2017), 5.
[137] TGI Paris, référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* (n 15). See also Greenberg (131) 1208-1209.
[138] *Yahoo! inc v La Ligue Contre le Racisme et l'Antisemitisme et al*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001), 1185.
[139] TGI Paris, référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* (n 15).
[140] Akdeniz (n 131) 4.

contested the order and stated that applying filtering procedures to block French Internet users from specific websites was technically impossible as well as disproportionately expensive.[141] However, on 20 November 2000 the TGI ordered Yahoo! Inc. to comply with the May order within 3 months from the November order being issued and to pay 100000 Francs per each day of delay once the 3-month compliance period expired.[142]

One important aspect of the November order is related to the TGI's considerations as to the audience targeted by Yahoo!. Indeed, the company claimed that its services were predominantly directed at an American audience. In replying to this argument, Gomez J mentioned a series of factors related to the Auction website, such as the items on sale, the method of payment, the delivery terms, the language and the currency used. He found that these elements validated the claim that the Auction site was mainly directed at an US audience. However, Gomez found that the same could not be said of the sale of Nazi memorabilia, which could have interested anyone.[143] In addition, the judge found that Yahoo! was aware that it was addressing a French audience because the users that accessed Yahoo.com from France were shown advertising banners in French.[144] Therefore, Gomez concluded that a sufficient basis for the exercise of jurisdiction had been established.[145]

2.4 Case analysis

The cases examined in the previous paragraphs outline the difficulties that national and regional courts face when establishing jurisdiction in Internet-related disputes over defendants located outside the domestic forum. As mentioned above, the courts in these cases were faced with the same challenge: establishing when an act committed online by

[141] Tribunal de Grande Instance de Paris Ordonnance de référé du 11 août 2000' (*Legalis.net*) <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-11-aout-2000/> accessed: 20 February 2017.
[142] TGI Paris, référé, 20 Novembre 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*, 20.
[143] ibid 3.
[144] ibid 4.
[145] ibid. A case similar to the *Yahoo! Auction* case is the *Töben* case discussed before the Bundesgerichtshof, the German Federal Court of Justice, Bundesgerichtshof [BGH] [Federal Court of Justice], Urt. v. 12. 12. 2000 – 1 StR 184/00 (LG Mannheim), NJW 54(8), pp. 624–628 (2001) (as cited in Hayashi (n 1) 293-295). In that case, the Federal Court found that it could exercise jurisdiction over Mr. Töben, a German-born Australian citizen who had published from Australia anti-Semitic and revisionist content on his website, based on the fact that that content could be accessed in Germany. In particular, the Court found that section 103(1) and (3) of the German Penal Code could be applied to the online content published by Mr. Töben since the publication of the material online could be considered as an act that happened at least partially on the German territory, as it produced negative effects there. The German Federal Court of Justice found that there was also a special link between the material published online and Germany justifying the exercise of jurisdiction by the domestic courts. Indeed, Mr. Töben's website was focussed on Germany and, due to German history, it affected a German audience in a particular way. For an analysis of the *Töben* case, see also Uta Kohl 'Eggs, Jurisdiction, and the Internet' (2002) 51(3) Int'l & Comp. L.Q. 555, 577-578.

defendants located in another State can be said to have happened within the domestic court's jurisdiction. Overall, four conclusions can be drawn from the analysis of these cases.

First, the domestic courts have used the accessibility of online content within the national territory as a basis to establish jurisdiction over that content.[146] More specifically, the accessibility of online content from within the territory of a given State has been used to justify the application of both the objective territorial principle and the effects doctrine: e.g. online content X is accessible within the territory of State A therefore content X was published in State A (objective territorial principle: the act happened in State A); online content Y is accessible in State B therefore it produced negative effects there (effects doctrine: the act was committed elsewhere but produced negative effects in State B).

The *Perrin* case and the Virginia Western District Court's decision in *Young v New Haven* offer an example of how the objective territorial principle has been applied to online content. Indeed, in the *Perrin* case, the EWCA found that online content is published in the UK both when material is uploaded and when it is downloaded (or merely accessed) from within the territory of the UK.[147] Similarly, Virginia District Court established that the accessibility of an online article from within the territory of Virginia meant that the defendants had acted in Virginia by publishing that article on their website.[148] More specifically, as previously mentioned, the Court found that since content published online is accessible to a worldwide audience, it is 'physically "present" in different locations at one time' and can therefore be subjected to multistate jurisdiction.[149]

On the other hand, an example of how the effects doctrine has been applied to online acts can be found in the *Dow Jones v Gutnick* case and the CJEU cases *eDate Advertising* and *BOÜ*, where the Victoria Supreme Court and the CJEU respectively found that in defamation cases content published online produces adverse effects in the place where the content is accessed.[150] The *Yeung v Google* case offers another example of this point, since the High Court of the Hong Kong Special Administrative Region established that 'an internet publisher who places material on the internet will be responsible for the

[146] The only exception to this point is represented by the Fourth Circuit Court of Appeal in the *Young v New Haven* case. Indeed, the judges openly rejected the accessibility criterion and relied exclusively on a targeting test to establish whether the Court of Appeal had jurisdiction over the article published on the defendants' websites.
[147] *R v Perrin*, (n 7) [18].
[148] *Young v New Haven Advocate et al* W. D. (n 9) 508.
[149] ibid 509.
[150] *Dow Jones and Company Inc v Gutnick* (n 8) [44]; *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* (n 13) para 51; *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (n 14) para 47.

effects of his action whenever the damage occurs'.[151] The emphasis placed by the Court on the negative effects produced by content published online on the territory where that content is accessed seems to confirm that the court relied on the effects doctrine when establishing jurisdiction on it.

The second conclusion that stems from the cases analysed is that the distinction between the objective territorial principle and the effects doctrine is not always clear-cut when these two principles are applied to cyberspace.[152] Indeed, some of the cases examined can be interpreted as an example of the application of both principles. All the defamation cases, for instance, can be interpreted as saying that an act of online defamation happens within a State's territory both because the content published online is found to have been published there (objective territorial principle) and it produces negative effects within that country (effects doctrine). This is because in the legal systems analysed, defamation happens in the place where the damage to reputation occurs. This place is identified with the place where content is published to a third party which, in the case of online content, is the territory from where it can be accessed. Therefore, it does appear that content published online from foreign States is considered as both having been published and capable of exercising negative effects in the States where it is accessible. For this reason, both the effects doctrine and the objective territorial principle appear as an equally plausible basis for exercising jurisdiction. The *Yahoo!* case offers another example of this point. In this case, Gomez J seemed to confirm both the objective territorial principle and the effects doctrine

> '[by] permitting these objects to be viewed in France and allowing surfers located in France to participate in such a display of items for sale, the Company YAHOO! Inc. is therefore committing a wrong in the territory of France […] Whereas, the damage being suffered in France, our jurisdiction is therefore competent to rule on the present dispute under Section 46 of the New Code of Civil Procedure'.[153]

Besides, confirmation of this point can be found in the different interpretation given by some authors of the jurisdictional basis relied upon by the TGI to establish jurisdiction. Indeed, while some commentators found that the TGI had relied on the effects doctrine, others interpreted Gomez J's decision as an example of the application of the objective territorial principle.[154] Overall, this point can be concluded by observing that on the

[151] *Yeung, Sau Shing Albert v Google Inc* (5 August 2014) (n 12) [37].
[152] Hayashi (n 1) 298-301.
[153] Pl.'s Compl. for Decl. Relief, ex. A, at 5 (as cited in Greenberg (n 131) 1208-1209).
[154] See Greenberg (n 131) 1208 for the effects doctrine; Hayashi (n 1) 295-296 for the objective territorial principle.

Internet the distinction between these two principles seems to lose importance, since, as has been pointed out by Hayashi, '[t]he extent of extraterritorial jurisdiction justified by the objective territorial principle seems to be as limitless as the one justified by the effects doctrine'.[155]

The third conclusion is that in addition to the objective territorial principle and the effects doctrine, some national courts carried out a targeting test to reinforce the finding that they had jurisdiction over the defendants.[156] The extent of this targeting test was, however, quite limited. Indeed, the courts established the defendant's intent to target an audience located within the domestic forum based on a very limited number of factors. In the *Young v New Haven* case, for example, Virginia Western District Court referred to the content of the allegedly defamatory article. The judges found that the fact that the article mentioned a Virginia resident and was related to events that had happened in Virginia proved that the exercise of jurisdiction over the defendants respected the due process requirement.[157] Another example of this point can be found in the TGI's reliance in the *Yahoo!* case on the language of the advertising banners shown to the users that accessed Yahoo.com from France. Gomez J found that the fact that Internet users located in France were shown advertising banners in French proved that Yahoo! Inc. was targeting a French audience.[158] Such reliance on the targeting test as an additional basis of jurisdiction could be interpreted as a desire on the Courts' part to justify the application of national laws to foreign defendants by showing a further link, however feeble, between the country exercising jurisdiction and the events happening online.

The last conclusion that can be drawn is related to the limits to the exercise of jurisdiction based on access. The access-based jurisdictional approach seems to give all States where certain content published online can be accessed the power to exercise jurisdiction over it. However, the cases examined show that two limits have emerged. The first is related to defamation cases. This limit is the requirement that national courts establish jurisdiction over a defamation claim only if the claimant has a reputation in the domestic forum.[159] The reputation requirement limits the number of States that can exercise jurisdiction over content published online from a foreign State. Indeed, it is unlikely that a person has a reputation in every country where the allegedly defamatory

[155] Hayashi (n 1) 299.
[156] Uerpmann-Wittzack (n 2) 1255-1256.
[157] *Young v New Haven Advocate et al* W. D. (n 9) 508.
[158] TGI Paris, référé, 20 Novembre 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* (n 142) 4.
[159] *Dow Jones and Company Inc v Gutnick* (n 8) [48]; *Young v New Haven Advocate et al*, 4th Cir. (n 9) 8; *Bredeen v Black* (n 11) [11]; *Yeung, Sau Shing Albert v Google Inc* (5 August 2014) (n 12) [37]; *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* (n 13) paras 42, 51; *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (n 14) paras 31-32.

content can be accessed.[160] In addition, the *BOÜ* case has introduced another limitation to the application of the access-based jurisdictional approach in online defamation cases as far as the EU law on jurisdiction is concerned. In particular, the *BOÜ* case has established that, although exercising jurisdiction based on access is legal according to the Regulation of the European Parliament on jurisdiction, this exercise is limited exclusively to requests for damages caused by the publication of defamatory content online, rather than requests for the removal of that content. Indeed, the CJEU has clarified that access alone is not a sufficient basis for any State where the online content can be accessed to order the removal of that content. Given the ubiquitous and international nature of content online, the only State competent to adjudicate on a removal request is the Member State where the victims have their centre of interest.[161]

The second limit to the application of the access-based jurisdictional approach is related to the proof of actual access to the content published online within the domestic forum. More specifically, in the cases examined, the national courts have established jurisdiction over online content that could be accessed from within their territory when the party making this argument proved that that was the case.[162] In other words, proof of actual access to content published online is required, while the presumption that content published online can and was accessed within the domestic forum is not deemed enough to exercise jurisdiction.[163] The *Coleman v MGN Limited* case illustrates this point particularly well. Indeed, in that case the Supreme Court of Ireland established that it did not have jurisdiction over the content published by MGN because no evidence had been produced showing that that content or the newspaper where it appeared had been published online in 2003. In addition, there was no evidence that the defamatory material had been accessed from within the territory of Ireland.[164] Due to the worldwide nature of the Internet, the actual access requirement does not limit significantly the exercise of State jurisdiction based on access. Indeed, it appears relatively easy to prove that a website can be accessed within a given national territory, especially if the website does not filter users based on their geographical location. Nonetheless, the actual access requirement constitutes an important characteristic of the access-based approach and it contributes to shedding light on this jurisdictional criterion.

---

[160] Maier (n 19) 151.
[161] *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (n 14) para 48.
[162] *R v Perrin* (n 7) [2]; *Young v New Haven Advocate et al*, 4th Cir. (n 9) 5; *Yeung, Sau Shing Albert v Google Inc* (5 August 2014) (n 12) [4], [42]; *Bredeen v Black* (n 11) [20]; *Dow Jones v Gutnick* (n 8) [1]-[2]; *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* (n 13) paras 16, 25; *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* (n 14) paras 9-10.
[163] Maier (n 19) 154.
[164] *Coleman v MGN Limited* (n 10) [14].

2.5 The implications of the access-based jurisdictional approach on the fulfilment of freedom of expression online

The access-based jurisdictional approach has attracted many critiques. The first critique that has been made of this approach is that it impacts negatively on the freedom of expression of Internet users located in foreign States and subjected to foreign jurisdictions.[165] Indeed, if all the countries followed the same approach and claimed that the application of their national laws extended globally, the principle of freedom of expression and the right to access information, as well as the principle of certain and predictable laws could be compromised. Yahoo!'s decision following the TGI's proceedings to amend its terms and conditions and ban the sale of Nazi-related items is particularly useful to illustrate this point. Indeed, as observed by Korff,

> 'whereas it was always completely out of the question that a US court would impose such a ban, Yahoo! was put in a position by the ruling of a foreign court in a foreign jurisdiction that led it to decide "voluntarily" to impose a ban on US citizens using its US-based services to buy and/or sell Nazi memorabilia, a ban that US courts could most probably not have imposed'.[166]

Another example of the implications of the access-based jurisdiction on the rights of foreign citizens is represented by the *Perrin* case. In that case, the EWCA made it clear that the content published on Mr. Perrin's website was illegal in the UK.[167] Therefore, as observed by some commentators, if the person who manages a website hosting similar content from a foreign country were to enter the territory of the UK, he would be liable for prosecution there.[168] As stated above, this would happen regardless of whether the content displayed on the website is legal in the country where the website is hosted.

Freedom of expression concerns have also been raised regarding the use of the access-based approach in defamation cases. On the one hand, as observed by Maier, some commentators have pointed out that this approach encourages forum shopping and exposes publishers to liability in virtually all the countries where the online content can be accessed.[169] On the other hand, other authors and some of the courts that adopted the access-based approach have underlined that the requirement that the claimant has a

---

[165] Korff (n 4) 60-62.
[166] ibid 59-60.
[167] ibid 59.
[168] Alisdair A. Gillespie, 'Jurisdictional issues concerning online child pornography' (2012) 20 Int J Law Info Tech 151, 170.
[169] Smith, G, 'Here, there or everywhere? Cross-border liability on the internet' (2007) 13(2) CTLR 41-51, p. 43 (as cited in Maier (n 19) 151).

reputation in the forum exercising jurisdiction effectively limits the number of countries where the publishers are liable.[170] Another limitation to the risk of forum shopping has been identified in the fact that the claimants might be inclined to pursue a defamation case only in those forums where the damage to their reputation has been substantial, in the hope of receiving a significant compensation.[171] However, both the above-mentioned points are controversial. Indeed, as observed in the Geneva Internet Disputes Resolution Policy 'practical evidence in the field of online defamation has shown that forum shoppers are not actually concerned with the quantum of damages as they rely on the mere threat of a lawsuit made abroad to pressure websites into settlement or into compliance'.[172] Therefore, it can be observed that the mere threat of legal action on multiple jurisdictions can have a negative impact on freedom of expression.

Another critique made of the access-based approach is related to the lack of a thorough analysis of the link between the perpetrator of the unlawful act, the illegal content published online and the State that exercises jurisdiction, as observed by Korff.[173] This analysis could have helped the national courts to limit the exercise of their jurisdiction only to cases that have a close nexus with their country. The targeting test applied by the Fourth Circuit Court of Appeal in the *Young v New Haven* case offers an example of this point. Indeed, in that case the Court stated that 'an intent to target and focus' on the audience located in a given State is necessary for that State to establish jurisdiction over the person responsible for the publication of that content online.

In relation to the necessity of conducting such an analysis there are, however, contrasting opinions. Indeed, in the *R v Perrin* case, Mr. Perrin's counsel accepted that there was no European or English authority that supported the theory that only the country where the major steps for publication had been taken had jurisdiction.[174] However, this statement was related to the position of European or English authorities as interpreted by Mr. Perrin's counsel and the EWCA up to 2002, which is when the *R v Perrin* case was held. There is, however, a 2011 document that outlines a more recent position on the criteria according to which a State can exercise jurisdiction over content published online. This is the Joint Declaration on Freedom of Expression and the Internet issued by the Special Representatives for freedom of information and freedom of the media of the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE),

---

[170] Maier (n 19) 151; *Dow Jones v Gutnick* (n 8) [152]-[155].
[171] Geneva Internet Disputes Resolution Policies 1.0. (n 16) 4. In particular, the Geneva Internet Disputes Policies refers to the approach of the European Court of Justice in *inter alia* the *eDate Advertising* case.
[172] ibid.
[173] Korff (n 4) 61-62.
[174] *R v Perrin*, (n 7) [33].

the Organisation of American States (OAS) and the African Commission on Human and Peoples' Rights (ACHPR).[175] According to the Joint Declaration

> '[j]urisdiction in legal cases relating to Internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State'.[176]

A similar opinion has been expressed by the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights (IACHR). Indeed, in the document Freedom of Expression and the Internet published in 2013 the Office of the Special Rapporteur stated that

> In order to prevent the existence of indirect barriers that disproportionately discourage or directly limit the right to freedom of expression on the Internet, jurisdiction over cases connected to Internet expression should correspond exclusively to States to which the cases are most closely associated, normally because the perpetrator resides there, the expression was published from there, or the expression is aimed directly at a public located in the State in question.[177]

These two documents define the criteria for establishing jurisdiction in Internet related cases in a slightly different way. More specifically, while the Joint Declaration explicitly refers to the place from where 'the content is uploaded'[178], the document produced by the Office of the Special Rapporteur of the IACHR refers more generically to the State from where 'the expression was published'.[179] The latter is more generic than the former because it does not explain what publication consists of and whether it encompasses downloading content in addition to uploading it, as stated in the *Perrin* case.[180] This point is particularly relevant. Indeed, defining the act of publishing content online in a way that encompasses only the uploading of content has the effect of reducing the number of national courts that could legitimately exercise jurisdiction over that content. On the other hand, if the place of publication is the place where the content is

---

[175] The United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet' (1 June 2011).
[176] ibid [4](a).
[177] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (31 December 2013), [66].
[178] Joint Declaration on Freedom of Expression and the Internet (n 175) [4] (a).
[179] Freedom of Expression and the Internet (n 177), [66].
[180] *R v Perrin* (n 7) [18].

uploaded or downloaded, then potentially all the countries in the world where that content can be accessed could have jurisdiction, which is the core of the reasoning in *Perrin*.

Overall, following the 2011 Joint Declaration and the 2013 IACHR document some conclusions can be drawn. First, some consensus at the international level exists - at least among some international authorities in the field of freedom of expression - on limiting State jurisdiction only to cases were a close nexus can be found between the State establishing jurisdiction and the content published online/person publishing it. Second, some criteria for establishing which State has the right to exercise jurisdiction online in a way that is compatible with freedom of expression have been identified by the international authorities.[181] These are: the place where the author/perpetrator is established, the place where the content has been uploaded/published and the place/people targeted by the content published/uploaded on the Internet. The third conclusion stems from observing that the first two of these criteria refer to the territorial principle of jurisdiction, while the last one is related to a targeting test. It can therefore be argued that even in a borderless environment such as the Internet, territory is seen as a central element in establishing jurisdiction. On the other hand, however, the territorial principle will be not very useful in all those cases where the place where the content has been uploaded, or even who uploaded it, cannot be established. Therefore, the targeting test seems better suited to establish which State has jurisdiction in a non-physical environment such as the cyberspace. Indeed, the targeting test permits to by-pass the obstacles represented by the unknown location of the person who uploaded some content online or the place where the content was uploaded from. This is because for the targeting test to be satisfied it is sufficient to establish that the content published online was targeting an audience located within a given State, regardless of where the content was originally uploaded from or who uploaded it. However, the difficulty associated with the targeting test is that so far there is no consensus as to the criteria upon which this test should be based.[182] In other words, it is unclear which factors must be considered when establishing whether content published online from a given State targets an audience located in a foreign country. The debate regarding this issue is currently ongoing within the scholarly community investigating State jurisdiction online and is likely to continue in the forthcoming years.

[181] See Chapter 5 sections 5.2 and 5.3 for a discussion of the international law principles applicable to acts committed online.
[182] Geneva Internet Disputes Resolution Policies 1.0. (n 16) 6-7. See also Chapter 5 section 5.3 for a discussion of this point.

2.6 Conclusion

In this chapter, the main characteristics of the access-based jurisdictional approach have been examined through the analysis of some key cases discussed in various jurisdictions. Notwithstanding the heterogeneous nature of the cases examined, several conclusions can be drawn regarding the access-based jurisdictional approach.

First, the accessibility of online content from within the territory of a given State has been used to justify the application of both the objective territorial principle and the effects doctrine.

Moreover, in addition to these two jurisdictional principles, some national courts carried out a targeting test to reinforce the finding that they had jurisdiction over the defendants. The extent of this targeting test was, however, quite limited, since the courts established the defendant's intent to target the domestic forum based on a small number of factors. Such reliance on the targeting test could be interpreted as the courts' desire to justify the application of national laws to foreign defendants by showing a further link, however feeble, between the country exercising jurisdiction and the events happening online.

Furthermore, the cases examined show that the distinction between the objective territorial principle and the effects doctrine is not always clear-cut when these two principles are applied to cyberspace. Indeed, some courts' decisions can be interpreted as an example of the simultaneous application of both principles. Some authors have observed that a consequence of this point is that the scope of the exercise of extraterritorial jurisdiction justified by these two principles becomes limitless.[183]

Another conclusion that can be drawn from the analysis conducted in this chapter is that there seems to be two limits to the exercise of jurisdiction based on access: the reputation requirement, which is related to defamation cases, and the actual access requirement. However, the efficacy of these requirements on limiting the exercise of jurisdiction based on access is debated. This is especially true regarding the reputation requirement, since the threat of lawsuits in multiple legal systems is still a possibility and constitutes a phenomenon that can negatively impact freedom of expression online.

The curtailing effect of the access-based approach on freedom of expression is one of the main critiques that have made of this jurisdictional criterion. Indeed, the cases analysed in this chapter could be interpreted as having the same overall effect: imposing restrictions on Internet users located in foreign countries and subjected to foreign

[183] Hayashi (n 1) 299.

jurisdictions. This is because if other countries followed the same approach and claimed that the application of their national laws extended globally, the principle of freedom of expression, the right to access information, and the principle of certain and predictable laws could be compromised. Indeed, following the court's decision in the *Yahoo!* case, Yahoo! introduced a ban on the sale of Nazi-related items among its terms and conditions. Therefore, Internet users in the US could not view, buy or sell material that was perfectly legal there according to US law. In addition, following the logic of the *Perrin* case, if a person living outside the UK and managing a website hosted in a foreign country published on that website content illegal in the UK, he could be prosecuted there if he were ever to enter British territory.

Another criticism of establishing jurisdiction based on access is that no thorough analysis of the link between the perpetrator of the unlawful act, the illegal content published online and the State that exercises jurisdiction has been conducted by the courts adopting this approach. This analysis could have helped the national courts to limit the exercise of their jurisdiction only to cases that have a close nexus with their country. In relation to the necessity of conducting such an analysis there are, however, contrasting opinions. Nevertheless, there seems to be some consensus among international authorities in the field of freedom of expression on limiting State jurisdiction only to cases where a close nexus can be established. Besides, some criteria for determining which State has the right to exercise jurisdiction online have been identified by the above-mentioned authorities. These are: the place where the author/perpetrator is established, the place where the content has been uploaded/published and the place/people targeted by the content published/uploaded on the Internet. There are, however, some difficulties associated with these criteria. Indeed, the territorial principle is not useful in all those cases where the place where the content has been uploaded or even who uploaded it cannot be established. On the other hand, while the targeting test permits to by-pass these obstacles, there is no consensus as to the criteria upon which this test should be based. The debate regarding this issue is currently ongoing within the scholarly community investigating State jurisdiction online and is likely to continue in the forthcoming years.

3. The extraterritorial application of national laws in Internet-related cases

3.1 Introduction

This chapter deals with the extraterritorial application of national laws to regulate content published online. The purpose of this analysis is to highlight the negative implications that the extraterritorial exercise of State jurisdiction over online content has on both the respect for foreign States' sovereignty and for freedom of expression of foreign Internet users.

This chapter argues that, while the domestic courts in the cases analysed had jurisdiction over the defendants, these courts had no authority to impose measures with extraterritorial effects, such as global de-listing. Overall, the main problem represented by the jurisdictional approach adopted in these cases is that it equates to applying universal jurisdiction over acts that are not international crimes.

This claim will be developed through three main steps. Section two will introduce the domestic cases examined and will provide an outline of the main jurisdictional issues discussed before the national courts. Section three will critically analyse these cases with a focus on highlighting the problems that the extraterritorial exercise of State jurisdiction poses to the principle of international comity and freedom of expression online. Finally, section four will summarize the main conclusions of the analysis.

3.2 Case selection

This chapter focuses of four main Internet jurisdiction cases: *Google Inc. v CNIL*,[1] *Google Inc. v Equustek Solutions Inc.*,[2] *A.T. v Globe24H.com*[3] and *Microsoft v. the United States*.[4] These cases deal with two areas of law: data protection and access to data in a criminal investigation. These two fields have been selected because the way in which

[1] Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772; Decision no. 2016-054 of March 10, 2016 of the Restricted Committee of the French Data Protection Authority issuing Google Inc. with a financial penalty < https://sites.les.univr.it/cybercrime/wp-content/uploads/2017/08/2016-google.pdf> accessed 8 September 2020.
[2] *Equustek Solutions Inc. v. Jack* 2014 BCSC 1063; *Google Inc. v Equustek Solutions Inc.* 2017 SCC 34.
[3] *A.T. v Globe24H.com* 2017 FC 114.
[4] *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. 2016).

States exercise jurisdiction over online content in these sensitive areas highlights the difficulties faced by national courts in reconciling domestic interests with the respect for other States' sovereignty and for foreign Internet users' rights. In particular, the national courts in the cases examined in this chapter have all been presented with the same problem: establishing whether they can apply domestic laws extraterritorially to regulate the online activities of foreign defendants or to access data stored in foreign countries.

The cases examined in this analysis belong to different jurisdictions in two main geographic regions: Europe and North America. These cases are quite controversial and have received widespread international coverage attracting the opinions of many scholars.[5] International NGOs in the field of freedom of expression as well as many ISPs and technology companies have taken part in the proceedings in these cases and have submitted their observations to the Courts as *amicus curiae*.[6] This shows how topical these cases are in connection with clarifying the expectations of different stakeholders regarding the rules regulating the exercise for State jurisdiction online.

3.2.1 The *Google LLC. v CNIL* case

In May 2016, the US-based Google Inc. (now Google LLC) filed a complaint against the French Data Protection Authority (DPA), the Commission Nationale de l'Informatique et des Libertés (CNIL), before the Conseil d'Etat. The complaint was

[5] Michael Geist 'Global Internet Takedown Orders Come to Canada: Supreme Court Upholds International Removal of Google Search Results' (*Michael Geist*, 28 June 2017) <http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results/> accessed: 08 September 2020; Internet & Jurisdiction Policy Network 'US Court issues preliminary injunction to block enforcement in the US of Google de-indexation ordered by Canadian Supreme Court' (*Internet & Jurisdiction Retrospect Database*, November 2017) <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiZXF1dXN0ZWsiLCJmcm9tIjoiMjAxMi0wMiIsInRvIjoiMjAxOC0wMSJ9> accessed 08 September 2020; Daphne Keller 'Global Right to Be Forgotten. Delisting: Why CNIL is Wrong' (*Stanford Center for Internet and Society*, 18 November 2016 <http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong> accessed 12 March 2018; Internet & Jurisdiction Policy Network 'Canada's Federal Court applies national data protection law against Romanian website' (*Internet & Jurisdiction Retrospect Database*, February 2017) <https://www.internetjurisdiction.net/publications/retrospect#eyJmcm9tIjoiMjAxNy0wMSIsInRvIjoiMjAxNy0xMiJ9> accessed 12 March 2018; Teresa Scassa 'Federal Court Orders Romanian Website Operator to Take Down Canadian Court Decisions Under Privacy Statute' (*Teresa Scassa*, 21 February 2017) <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=242:federal-court-orders-romanian-website-operator-to-take-down-canadian-court-decisions-under-privacy-statute&Itemid=80> accessed 12 March 2018; Jennifer Daskal 'Three Key Takeaways: The 2d Circuit Ruling in The Microsoft Warrant Case' (*Just Security*, 14 July 2016) <https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case/> accessed 12 March 2018.

[6] As an example, see the amicus curiae briefs submitted in the *Microsoft* case, Microsoft 'Resources: Microsoft's Search Warrant Case' (2014) (*Microsoft*, December 2014) < https://blogs.microsoft.com/datalaw/resource/initiative/microsofts-search-warrant-case/page/3/> accessed: 12 March 2018; Written Observations of Article 19 and Others, 29 November 2017, case C-507/17 *Google Inc. v Commission Nationale de l'Informatique et des Libertés (CNIL)*.

related to a €100000 financial penalty that the CNIL had issued against Google in March 2016. In particular, the CNIL had found the company in violation of articles 38 and 40 of the French Data Protection Act for not granting the de-listing requests that it had received from some French Internet users.[7] Articles 38 and 40 of the French Data Protection Act establish the data subjects' right to object to the processing of personal data and the right to erasure of incomplete or inaccurate data (right to de-listing) respectively.[8] The duty to de-list for search engine operators was established by the Court of Justice of the European Union (CJEU) in the 2014 *Google Spain* case.[9] De-listing is an operation carried out by search engine operators, such as Google, and consists of the removal from the list of search results associated to a person's name linking to a webpage containing private information about that person. De-listing does not involve the removal of the undesired information itself. Indeed, the information remains online and is accessible when other search terms are used other than the requestor's name.[10]

The dispute between the CNIL and Google is related to the number of domain names which should be affected by de-listing and the geographical scope of the de-listing operations. Indeed, the CNIL's position is that de-listing is effective only when carried out in regard to all the geographical extensions of a search engine and all the search queries that are made worldwide using a person's name. In other words, according to the

[7] Decision no. 2016-054 (n 1) 9.

[8] The Loi Informatique et Libertes Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties is the French Data Protection Act. It incorporates the provisions contained in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (the Data Protection Directive). This Directive was repealed by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJL 119/1 (see n 24). An English translation of the Loi Informatique et Libertes can be found at https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf accessed 12 March 2018.

[9] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317.

[10] The grounds on which delisting can be requested are currently listed in article 17.1 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJL 119/1: 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)'.

French authority, following the request of a French Internet user, Google should remove the unwanted search result from all Google Search geographical extensions and in respect to all the search queries that are made globally. The consequence of this position is that the undesired link is no longer accessible worldwide when searching for the requestor's name. The French DPA justified the extraterritorial application of de-listing with the need to ensure that European data subjects' rights to object and to erasure are applied 'without circumvention'.[11]

Google's position, on the other hand, is that de-listing should be carried out only in regard to the European extensions of its search engine and only when search queries are made from Europe.[12]

The debate between Google and the CNIL regarding the lawfulness of global de-listing is particularly relevant to this analysis. In opposing to the CNIL's request for global de-listing, Google claimed that the French DPA was acting outside the scope of its powers by trying to impose the extraterritorial application of the French Data Protection Act. This Act, according to Google, does not apply to search queries that are made outside the French territory because these queries neither target French Internet users nor are linked to the activities of Google France.[13] Indeed, the company stated that Google Search geographical extensions are to be considered as separate entities, each of which targets users located in different countries. Google also claimed that, due to its extraterritorial effects, applying de-listing to the entirety of its search engine extensions is a violation of the sovereignty of the other States as well as a violation of the right to freedom of expression and information.[14]

The CNIL responded to Google's claims with three main counterarguments. First, the French Data Protection Law applies to all of Google's geographical extensions because Google France contributes in the French territory to the activities of the US-based Google Inc.[15] According to the CNIL, Google Search geographical extensions can be considered as mere technical paths that refer to the same processing system - Google Search available through www.google.com - rather than being single processing systems separated from one another. Second, in regard to the alleged violation of other States' sovereignty, the

[11] Decision no. 2016-054 (n 1) 8.
[12] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (n 1) para 31.
[13] Decision no. 2016-054 (n 1) 6.
[14] ibid 7-8.
[15] Decision no. 2016-054 (n 1) 6-7. Article 5-I-2 of the French Data Protection Act states that the law applies only to the data controller who 'although not established on French territory or in any other Member State of the European Union, uses means of processing located on French territory, with the exception of processing used only for the purposes of transit through this territory or that of any other member State of the European Union', Loi Informatique et Libertes (n 8) art 5-I-2.

French authority affirmed that its decision is related exclusively to Internet users located in France. In particular, such a decision is necessary to ensure that French Internet users' right to complete protection is effective 'without restrictions for all processing, even if it conflicts with foreign rights'.[16] Finally, as to the infringement of the right to freedom of expression and information, the CNIL stated that the right to erasure and to object are only granted when specific conditions are met, such as proof of a legitimate interest and the existence of obsolete, incomplete or erroneous information.[17] In other words, the CNIL grants de-listing requests only if it finds that 'a tight balance between the respect for the right to privacy and personal data protection of individuals and the benefit to the public of accessing information' can be retained.[18]

The dispute between the CNIL and Google before the Conseil d'Etat was put on hold on 21 August 2017, when the French Court decided to stay the proceedings and presented its request for a preliminary ruling to the CJEU.[19] The French Court asked three questions to the EU judges. The first is whether search engine operators should carry out de-listing on all the domain names of a search engine, and in respect to all the search queries that are made using a person's name.[20] This equates to asking whether de-listing should be applied globally, as stated by the CNIL. Alternatively, the Conseil d'Etat has asked whether de-listing should be limited to the domain name corresponding to the State from where the de-listing request is made or, more generally, domain names corresponding to EU member States.[21] The French Court's last question is whether de-listing should be applied to search queries made from the country of residence of the person requesting de-listing or more generally from EU member States irrespective of the domain name used by Internet users.[22] In other words, the Conseil d'Etat has asked whether de-listing should be applied to search queries made from within the EU even when the queries are made on non-European versions of the search engine, such as google.com.

Following the request for a preliminary ruling, however, Google changed the way in which the national versions of its search engine operate. In particular, the domain name entered by Internet users is not the factor that determines which national version of

[16] Decision no. 2016-054 (n 1) 7.
[17] ibid 8.
[18] ibid.
[19] Internet & Jurisdiction Policy Network 'France's highest administrative court refers Google right to be de-indexed case to CJEU' (*Internet & Jurisdiction Retrospect Database*, December 2017) <https://www.internetjurisdiction.net/publications/retrospect#eyJjYXRlZ29yaWVzIjpbIjE2NiJdLCJ0byI6IjIwMTctMTIiLCJmcm9tIjoiMjAxMi0wMiJ9> accessed 17 January 2018.
[20] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (n 1) para 39 (1).
[21] ibid para 39 (2).
[22] ibid para 39 (3).

Google Search engine can be accessed by the user. Indeed, Google now uses geo-location technology to identify the location of the Internet user and automatically redirects the user to the national version of its search engine corresponding to that location.[23] The CJEU has therefore reinterpreted the questions presented by the Conseil d'Etat as asking whether articles 12(b) and 14(a) of the Directive 96/45 and article 17(1) of the General Data Protection Regulation (GDPR)[24] establish that, when granting a de-listing request, Google should remove the unwanted search result from all the versions of its search engine, only from the versions of the search engine that correspond to EU Member States or only from the national version of the search engine that corresponds to the Member State from where the request has been made. The CJEU was also asked to establish whether Google should use geo-blocking techniques to prevent that search queries made from the country of residence of the person requesting delisting or from any EU Member State access the unwanted search result regardless of the national version of the search engine used.[25]

The CJEU found that both the Directive 96/45 and the GDPR apply to Google since the processing of personal data on Google's part is carried out on the French territory. This is because Google France is linked to the other national versions of Google and it conducts advertising activities in France which are linked to the processing of personal data operated by Google.[26] As to the geographical scope of the right to delisting, the CJEU found that a search engine operator is only required to carry out delisting in regard to the national versions of its search engines corresponding to the Member States of the EU.[27] However, the search engine operator is required to apply the relevant techniques to prevent or seriously discourage Internet users located in the EU Member States from accessing the delisted search result when searching for the name of the person who requested delisting.[28] As to global delisting, the CJEU found that while the right to delisting is recognised in EU law, it cannot be said the same for other States which might not recognize this right or have a different approach to it.[29] In addition, the judges

[23] ibid para 42.
[24] On 25 May 2018 Directive 96/45 was repealed by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJL 119/1. However, since the Directive 96/45 was still in force when the request for a preliminary ruling was presented before the CJEU, the Court at para 41 specified that it would have answered the questions in light of both the directive and the regulation.
[25] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (n 1) para 43.
[26] ibid para 52.
[27] ibid para 66.
[28] ibid para 70.
[29] ibid 59.

underlined that the right to delisting is not absolute and it must be applied in a way that is compatible with the proportionality principle. Besides, a balance must be struck between this right and the right to freedom of information of Internet users.[30] While, however, this balance has been found in EU law, other parts of the world might find a different balance between these two rights.[31] For this reason, the Court found that EU law does not require delisting to be carried out in regard to all the various versions of a search engine.[32] Interestingly, however, the CJEU did not exclude that global delisting might still be ordered. Indeed, the judges found that, based on the effects doctrine, since global access to an undesired search result regarding a person located in the EU will have an immediate and substantial effect on that person, there is a competence in the EU legislature to order global delisting.[33] In particular, the CJEU found that, while EU law does not currently require global delisting, it does not prohibit it either. It will therefore be up to the domestic courts and supervisory authorities of the EU Member States to strike a balance on a case by cases basis between the right to privacy of the data subject and the right of access to information. Based on that assessment, the national authorities will still be competent to order global delisting if they deem it necessary.[34]

Overall, as will be shown in the case analysis section, the CNIL's exercise of jurisdiction over Google Inc. does not seem particularly problematic, since the company was operating on French territory. The extraterritorial exercise of State jurisdiction and the imposition of global de-listing, on the other hand, which have not been excluded by the CJEU, pose problems with regard to the respect for comity between States and freedom of expression online. These points will be discussed further below.

3.2.1.1 The territorial scope of de-listing according to the European Data Protection Authorities and the wide jurisdictional reach of the GDPR

The French DPA's interpretation of the extraterritorial application of the right to de-listing is *prima facie* in line with the guidelines issued by Article 29 Working Party (WP), the data protection working party established by article 29 of the Directive 96/45. The Working Party, which included representatives of EU member States' DPAs, was an independent advisory body providing the Commission with advice in the field of data

[30] ibid para 60.
[31] ibid.
[32] ibid para 64.
[33] ibid paras 57-58.
[34] ibid para 72.

protection.[35] In May 2018, when the GDPR entered into force repealing the Directive 96/45, the Working Party was replaced by the European Data Protection Board (EDPB). As the dispute between Google and the CNIL started in 2016 and the request for a preliminary ruling was presented before the CJEU in 2017, the guidelines issued by the Working Party on delisting could be considered as a relevant authority at the time. According to the guidelines issued by Article 29 WP on November 2014, to be effective de-listing should be carried out by search engine operators on all their domain names, as opposed to the European versions only.[36] However, unlike the CNIL, the Article 29 WP did not specify the territorial scope of application of de-listing. In particular, the advisory body did not clarify whether search engine operators should remove the unwanted search result from all their domain names in relation to all the search queries that are made globally. In other words, it is unclear whether, according to the EU working party, Internet users outside the EU should have been prevented from accessing a search result that could be legal in their countries. However, Article 29 WP's guidelines were issued in 2014, soon after the *Google Spain* judgement and before the *Google v CNIL* dispute started. Therefore, the lack of further elaboration by the EU data protection authority on the territorial scope of de-listing could be linked to the fact that the guidelines were issued at the beginning of the de-listing era. Following the *Google v CNIL* judgement of September 2019, the EDPB which replaced Article 29 WP, published an updated version of the Guidelines on the right to delisting. However, the territorial scope of delisting is not mentioned in these new Guidelines.[37]

Before the CJEU issued its judgement in the *Google v CNIL* case, other DPAs in Europe followed Article 29 WP's approach to global de-listing as far as applying it to all the domain names of a search engine is concerned. However, some differences have emerged regarding the territorial scope of this operation. The UK DPA, the Information Commissioner's Office (ICO), for example, on 2 November 2015, announced that it had amended a de-listing notice issued against Google where the company was originally asked to remove certain search results from Google.uk only. Indeed, in November 2015

[35] European Data Protection Supervisor 'Glossary - Article 29 Working Party' (European data Protection Supervisor) <https://edps.europa.eu/data-protection/data-protection/glossary/a_en> accessed 20 January 2018.

[36] Article 29 Working Party 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment On "Google Spain and Inc. v Agencia Española De Protección De Datos (Aepd) and Mario Costeja González"' C-131/12 26 November 2014, 3.

[37] European Data Protection Board 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' 2 December 2019 ,https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en> accessed 7 August 2020.

ICO asked the company to carry out de-listing on all its domain names when the search query appeared to have come from within the UK.[38] ICO's position is therefore different from CNIL's, since ICO did specify that de-listing, although to be applied to non-EU domain names as well as European, was to be limited to searches conducted from within the UK.

Global de-listing, however, received the approval of another data protection authority, the Swedish Datainspektionen. In May 2017 the Swedish DPA published the results of an investigation that it had conducted on how de-listing should be applied. The Swedish authority claimed that, in principle, search engine operators should remove unwanted search results only when the search queries are made from Sweden. However, the DPA found that there are certain circumstances that require the de-listing to be applied to queries made from foreign countries as well. This is so when there is a 'specific connection to Sweden and to the data subject'.[39] According to the Swedish DPA, this special connection exists if the search result to be de-listed is linked to information 'written in Swedish, addressed to a Swedish audience, contains information about a person that is in Sweden or if the information has been published on the Swedish domain .se'.[40] The Swedish approach to exercising jurisdiction extraterritorially with regard to de-listing is therefore a qualified approach. Indeed, the exercise of State jurisdiction is justified only if there are certain connecting factors linking the search result to be de-listed to Sweden. Overall, the Swedish approach seems preferable to the French, because it reflects the country's need to limit the extraterritorial exercise of State jurisdiction only to cases that are closely linked to Sweden.

As mentioned above, the right to delisting is contained in Article 17 of the GDPR. Having examined the territorial scope of delisting, it is also worth mentioning the wide jurisdictional reach of the GDPR itself. Article 3 of the GDPR defines its territorial scope and it establishes that the Regulation applies to the processing or personal data within the establishment of a controller or processor in the EU, regardless of where the data processing happens.[41] The Regulation also covers the processing of personal data of data subjects who are in the Union by a controller that is not established in the Union if the processing activities are related to the offering of goods or services to the data subjects in

[38] David Smith 'Has the search result ruling stopped the internet working?' (*Information Commissioner's Office*, 2 November 2015) <https://www.wired-gov.net/wg/news.nsf/articles/Has+the+search+result+ruling+stopped+the+internet+working+031120151520 00?open> (Accessed: 20 January 2018).
[39] Datainspektionen 'The right to be forgotten may apply all over the world' (Datainspektionen, 4 May 2017) <https://perma.cc/NT8D-42Z3> accessed: 20 January 2018.
[40] ibid.
[41] General Data Protection Regulation (n 10) art 3(1).

the Union or to the monitoring of the behaviour of the data subjects as long as their behaviour takes place within the Union.[42] Finally, Article 3 establishes that the Regulation applies to the processing of personal data by controllers not established in the Union but established in places where the law of the Member States applies according to public international law.[43] As will be explored in section 3.3, article 48 of the GDPR also introduces significant limitations to the disclosure of personal data to non-EU states, which impacts on the possibility that foreign States access data stored in the EU.[44] Besides, article 27 of the GDPR establishes that a controller that is outside the EU but that nonetheless falls within the scope of the GDPR must designate a representative in the EU.[45]

Some commentators have highlighted the wide extraterritorial jurisdictional reach of the GDPR, which imposes obligations on data processors and controllers not just within the EU but also outside, since it poses restrictions on data transfers and the obligation for processors not established in the EU but falling within the scope of the GDRP to nominate a representative there.[46] Overall, according to these commentators, the GDPR is increasingly seen as standard setting, as it is influencing the way in which countries and multinational companies outside the EU approach and structure data privacy laws.[47] Among these countries figure Thailand that in its Personal Data Protection Act B.E. 2562 (2019) (PDPA) adopted a jurisdictional approach similar to that of article 3 of the GDPR.[48] For this reason, it has been argued that the biggest impact of the GDPR might be that it might encourage other States to carry out progressively broad exercises of jurisdiction in the field of data privacy.[49]

---

[42] ibid art 3(2).
[43] ibid article 3(3).
[44] See section 3.3 for an analysis of this point.
[45] General Data Protection Regulation (n 10) art 27.
[46] Internet & Jurisdiction Policy Network 'Global Status Report 2019' (*Internet & Jurisdiction*, 2019) <https://form.jotformeu.com/93222419949364> accessed: 28 November 2019, 95.
[47] ibid.
[48] 'The PDPA applies to the collection, usage and disclosure by a data controller or a data processor located in Thailand, even if the collection, usage and disclosure of the Personal Data is undertaken outside of Thailand. The PDPA also applies to data controllers and data processors located outside Thailand, but only in the following cases: When goods or services are offered to data subjects in Thailand, regardless of whether there is payment or not; or When monitoring of data subjects' behaviour is taken place in Thailand' Tassanai Kiratisountorn, Pimchanok Eianleng, Anna Gamvros and Ruby Kwok 'Thailand Personal Data Protection Law' (*The Norton Rose Fulbright Data Protection Report*, 28 February 2020) <https://www.dataprotectionreport.com/2020/02/thailand-personal-data-protection-law/> accessed 11 August 2020. The PDPA was due to enter into force on 27 May 2020, however, there are reports that Thailand's government decided to postpone the entry into force of the Act to May 2021 due to the difficulties caused by the Covid-19 pandemic, see Dhiraphol Suwanprateep 'Postponement of Thailand's Personal Data Protection Act (PDPA)' (Lexology, 12 May 2020) <https://www.lexology.com/library/detail.aspx?g=c628a738-f929-4987-b6db-b0ee00e69b30> accessed 11 August 2020. See also Internet & Jurisdiction Policy Network 'Global Status Report 2019' (n 46) 96.
[49] Internet & Jurisdiction Policy Network 'Global Status Report 2019' (n 46) 96.

3.2.2 The *Google Inc. v Equustek Solutions Inc.* case

The dispute between the Canadian company Equustek Solutions and the US-based Google Inc. commenced following Google's refusal to de-list all the websites of Equustek's former distributor, the Canada-based Datalink. Equustek had obtained an order and an injunction by the Supreme Court of British Columbia against Datalink due to the latter's unlawful sale and distribution of Equustek's intellectual property. As a result, Datalink had been prohibited from selling Equsteek's products and, on 13 December 2012, the company had been ordered to cease operating or carrying out business through any website.[50] Datalink, however, had not complied with the order and, after having abandoned the legal proceedings, it left British Columbia and moved to an unknown location from where it continued to sell the plaintiff's products through its websites.[51]

Following the December 2012 injunction, Equustek asked Google, which was not a party to the legal proceedings, to de-list all of Datalink's websites. Google, however, carried out de-listing only on Google.ca, rather than on the entirety of its search engine's geographical extensions, and only in relation to 345 webpages associated with Datalink, rather than all of the company's websites.[52] For this reason, Equustek asked the British Columbia court to issue an interlocutory injunction ordering Google not to display any part of Datalink's websites on any of Google Search results worldwide. Fenlon J granted the interlocutory injunction. The judge found that by displaying Datalink's websites among Google search results worldwide, Google was involuntarily facilitating Datalink in carrying out irreparable harm to Equustek.[53] Fenlon J's order was upheld by both the Court of Appeal of British Columbia and Canada Supreme Court.

The question presented before Canada Supreme Court was whether British Columbia courts could issue an interlocutory injunction ordering Google to de-list all Datalink's websites on the entirety of the geographical extensions of its search engine. More specifically, the Court had to determine whether granting an interlocutory injunction was "just and equitable".[54] Interlocutory injunctions are equitable remedies with a temporary validity: they are usually enforceable until trial or until the final determination of the case is reached. Their purpose is to 'ensure that the subject matter of the litigation will be "preserved" so that effective relief will be available when the case is ultimately heard on

[50] *Google Inc. v. Equustek Solutions Inc.* 2017 SCC (n 2) [14].
[51] ibid [7].
[52] ibid [16].
[53] ibid [18]-[19].
[54] ibid [25].

the merits'.[55] The Supreme Court found with a majority of seven to two that all the criteria that determine whether interlocutory injunctions can be granted were met. Indeed, the judges affirmed that there was a serious issue to be tried, that Equustek was suffering irreversible harm due to Datalink's continuing sale of its products online, and that the balance of convenience was in favour of granting the injunction. In particular, the Court found that Google was 'a determinative player' in allowing Datalink to sell Equustek's products and therefore causing the harm to Equustek to continue.[56]

Google's objections to the extraterritorial character of the interlocutory injunction are particularly relevant to the scope of this analysis. The Supreme Court found that the British Columbia courts had both personal and territorial jurisdiction over Google Inc. since the company carried out business in British Columbia through its advertising and search operations.[57] Google accepted that British Columbia courts had jurisdiction. However, the company claimed that the extraterritorial reach of the injunction was improper and unnecessary and that Canadian courts should limit the territorial reach of the injunction to Canada and Google.ca only.[58] The Supreme Court dismissed this claim and found that Canadian courts can issue injunctions with extraterritorial effects when they have *in personam* jurisdiction and when the extraterritoriality is essential to ensure the injunction's effectiveness. The Court also mentioned a number of Internet-related cases from foreign countries, including the CJEU *Google Spain* case, as an example of the international support towards issuing orders that have extraterritorial effects in relation to Internet abuses.[59] According to the Supreme Court, the extraterritorial reach of the injunction was necessary because the majority of Datalink's sales happened outside Canada.[60] Therefore, the injunction was only going to be effective if it had extraterritorial effects.[61] Indeed, an injunction limited to Canada or Google.ca would have allowed consumers outside Canada and Canadian Internet users using any other Google geographical extension to access Datalink's products. The Supreme Court also found that the balance of convenience was not in Google's favour, because '[t]here is […] no harm

[55] ibid [23]-[24].
[56] ibid [53].
[57] ibid [37].
[58] ibid.
[59] ibid [39]. More specifically, at [39] the Court referred to the judgment of the Court of Appeal of British Columbia, *Equustek Solutions Inc. v. Google Inc*., 2015 BCCA 265, where at [95] Groberman J. made reference to a series of cases where domestic courts issued orders with extraterritorial effects. Among these cases figure: '*APC v. Auchan Telecom*, 11/60013, Judgment (28 November 2013) (Tribunal de Grand Instance de Paris; *McKeogh v. Doe* (Irish High Court, case no. 20121254P); […] and *ECJ Google Spain SL, Google Inc. v. Agencia Española de Protecciób de Datos, Mario Costeja González*, C-131/12 [2014], CURIA', *Equustek Solutions Inc. v. Google Inc*., 2015 BCCA [95].
[60] *Google Inc. v. Equustek Solutions Inc.* 2017 SCC (n 2) [40].
[61] ibid [41].

to Google which can be placed on its "inconvenience" scale arising from the global reach of the order'.[62] This is because, as admitted by Google, it is relatively easy for the company to carry out global de-listing. This operation can be done in one location, in the place where the search engine is controlled, and does not require Google to take steps in multiple countries.[63]

Google also raised the argument that a global injunction violated international comity. Indeed, according to Google, a global injunction could not have been obtained in a foreign country. Alternatively, the company claimed that complying with the injunction would have led Google to violate the laws of another country.[64] The Court, however, found this claim to be theoretical, since, as observed by the judge of first instance, in most countries the sale of other companies' intellectual property is considered illegal as well.[65]

Finally, Google stated that the injunction raised freedom of expression concerns which should have led the Courts to refrain from granting it.[66] The Supreme Court dismissed this claim as it found that the injunction had been issued due to an infringement of intellectual property rights. Therefore, it was quite unrealistic that the injunction could have offended the core values of another country.[67] Indeed, in the judges' opinion, protecting freedom of expression does not require condoning the facilitation of the illegal sale of other companies' intellectual property.[68] However, the judges stated that in case Google had evidence of foreign laws that it would have been required to violate in order to comply with the injunction, it could have applied to the British Columbia courts to modify the order accordingly.[69]

On 24 July 2017, Google started legal proceedings against Equustek before US courts. The company asked the US District Court for the Northern District of California to declare that the order of the Canadian Supreme Court is not enforceable in the United States. Google argued that the Canadian order violates the First Amendment, contrasts with the immunity for interactive service providers established by the Communication Decency Act and infringes the principle of comity.[70]

On 2 November 2017, the Californian Court granted Google's motion for preliminary injunctive relief, which was subsequently confirmed in a final ruling on 14 December

[62] ibid [43].
[63] ibid.
[64] ibid [44].
[65] ibid.
[66] ibid [27].
[67] ibid [45].
[68] ibid [48].
[69] ibid [46].
[70] *Google LLC v Equustek Solutions Inc., et al.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017), 3.

2017.[71] The US Court found that the Canadian order is not enforceable in the United States because it would cause irreparable harm to Google by depriving it of the benefit of US federal law. Indeed, according to Section 230 of the Communications Decency Act '"[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"'.[72] In addition, the Canadian order was found to be contrary to US public interest, since Congress had established that freedom of speech in the US would be impaired if ISPs were liable for content published by a third party.[73] The Court concluded that '[b]y forcing intermediaries to remove links to third-party material, the Canadian order undermines the policy goals of Section 230 and threatens free speech on the global internet'.[74]

Based on the favourable ruling obtained before the US courts, Google applied to the Supreme Court of British Columbia asking to set aside or change the injunction regarding global delisting.[75] The company argued *inter alia* that the ruling from the Californian court showed that the injunction issued by the Canadian courts violated the core values of another jurisdiction.[76] On 16 April 2018, however, the Supreme Court of British Columbia dismissed Google's application. The British Columbia Court found that, as affirmed by the Canadian Supreme Court, the injunction could only be reconsidered if it required Google to violate the laws of another country.[77] However, Smith J found that the US decision did not establish that Google carrying out global delisting would constitute a violation of US law. Indeed, the judge found that the injunction simply restricts Google's freedom to decide whether to list the websites in question. Restricting a party's freedom, however, is not the same as requiring that party to violate the law.[78] In addition, Smith J found that Google had not shown that the injunction violates core American values. Indeed, the judge underlined that the Californian decision did not examine Google's submission that the injunction violated the First Amendment of the American Constitution, which can be considered in Smith J's opinion as an expression of American core values.[79] Ultimately, according to the Supreme Court of British Columbia

> '[t]he effect of the U.S. order is that no action can be taken against Google to enforce the injunction in U.S. courts. That does not restrict the ability of this Court to protect

[71] *Equustek Solutions Inc. v Jack,* 2018 BCSC 610, [10].
[72] *Google LLC v Equustek Solutions Inc., et al.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017) (n 70) 3.
[73] ibid 5.
[74] ibid 6.
[75] *Equustek Solutions Inc. v Jack,* 2018 BCSC (n 71), [2].
[76] ibid [12].
[77] ibid [19].
[78] ibid [20].
[79] ibid [21].

the integrity of its own process through orders directed to parties over whom it has personal jurisdiction'.[80]

Google's request to set aside or modify the injunction was therefore dismissed by the British Columbia Court. Similarly to the *CNIL* case, in the *Equustek* case as well the exercise of State jurisdiction over Google Inc. is justified by the objective territorial principle. Indeed, as observed by the British Columbia Courts, Google Inc. was carrying out business activities in Canada through its advertising and search activities.[81] However, the global de-listing order imposed by Canadian courts violates both the sovereignty of foreign States and freedom of expression online, as discussed below.

3.2.3 The *A.T. v Globe24H.com* case

The case *A.T. v Globe24H.com* was decided by the Ontario Federal Court on 30 January 2017. It concerns a dispute between A.T., a Romanian citizen living in Canada, and Sebastian Radulescu, a Romanian citizen who lived in Romania, from where he administered the website Globe24H.com. The website, which was hosted on severs located in Romania, republished decisions from various national courts, including Canada.[82] The Canadian decisions available on Globe24H.com were also publicly available on legal websites such as the Canadian CanLII.org. However, unlike the Canadian legal websites, Mr. Radulescu had allowed for the decisions republished on Globe24H.com to be indexed by third party search engines, such as Google.[83] As a result, those decisions appeared among the list of search results associated to the parties' names.[84] Consequently, personal details related to those parties could be easily accessed by Internet users who searched for the litigants' names on Internet search engines.

The applicant, A.T., initiated legal proceedings against Mr. Radulescu pursuant to section 14 of the Personal Information Protection and Electronic Documents Act (PIPEDA).[85] In particular, A.T. sought relief for the damages caused by the publication of personal information and asked the Court to order, inter alia, the removal of the Canadian decisions from the respondent's website.

---

[80] ibid [22].
[81] *Equustek Solutions Inc. v. Jack* 2014 BCSC (n 2) [26]-[28].
[82] *A.T. v Globe24H.com* (n 3).
[83] ibid [8].
[84] 'Notably, the content of the Canadian legal websites is generally not indexed and a person seeking such information must go directly to each site and conduct a search with the names of the parties, the style of cause and/or the citation for the decision to obtain the content' ibid [9].
[85] ibid [1].

A.T. had originally filed a complaint against Mr. Radulescu to the Office of the Privacy Commissioner of Canada (OPCC) since a Canadian decision concerning a labour case that he was a party to had been republished through Globe24H.com. The applicant was concerned that the personal details accessible through Google and other search engines would affect his possibility to find a job in the future.[86] The OPCC, who was also a party in the present case, conducted an investigation into A.T's and another twenty-six complaints received against Globe24H.com. The investigation concluded that Mr. Radulescu's website constituted an organisation whose purpose was to collect, use and disclose personal information for commercial purposes within the meaning of PIPEDA.[87] Indeed, Mr. Radulescu had a system in place asking the interested parties to pay a certain sum in exchange for the removal of their personal information from Globe24H.com.[88]

One of the questions presented by the parties to the Ontario Federal Court was whether PIPEDA has extraterritorial application and can therefore regulate the activities of a foreign organisation, such as Globe24H.com, that have an impact on people residing in Canada.[89] The Court first noted that notwithstanding the absence of any reference in the Act to its extraterritorial scope, there was no express provision restricting its application to Canada.[90] For this reason, the judge found that the Statute could be applied to all those cases that had a '"real and substantial link"' to Canada, as stated by the Supreme Court of Canada in the case *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers* (SOCAN).[91] In the SOCAN case, which dealt with the extraterritorial application of the *Canadian Copyright Act*, Binnie J affirmed that relevant connecting factors for acts committed on the Internet included: 'the situs of the content provider, the host server, the intermediaries and the end user'.[92] Ultimately, the Supreme Court concluded that a sufficient connection for exercising jurisdiction is verified both when Canada is the country of transmission of a communication and the country of receipt.[93]

In conducting the real and substantial connection test related to the extraterritorial application of PIPEDA, the judge in the present case referred to four connecting factors.

---

[86] ibid [18].
[87] ibid [39].
[88] ibid [31].
[89] ibid [44]-[47].
[90] ibid [48].
[91] ibid. *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers, 2004 SCC 427, [2004]* 2 SCR 427 at paras 54-63 [SOCAN] (as cited in *A.T. v Globe24H.com* (n 34) [48]).
[92] SOCAN [61] (as cited in *A.T. v Globe24H.com* (n 3) [49]).
[93] SOCAN [63] (as cited in *A.T. v Globe24H.com* (n 3) [49]).

These are: the location of the target audience of the website, the source of the content on the website, the location of the website operator and that of the host server.[94] The judge found that while the last two criteria pointed at Romania rather than Canada, since both Mr. Radulescu and the website server were located there, this fact was not decisive in dismissing Canada's jurisdiction.[95] This is because 'when an organization's activities take place exclusively through a website […] telecommunications occur "both here and there"'.[96] Ultimately, in establishing jurisdiction over Globe24H.com the judge relied on the first two connecting factors mentioned above, the audience targeted by the website and the content of the website, as well as on the fact that the website produced negative effects on the Canadian public. The content of the website constituted a connecting factor in the judge's opinion since Globe24H.com contained Canadian case-law. In addition, the judge found that the website directly targeted a Canadian audience since it explicitly advertised that it provided access to domestic case-law. To prove this point, the Court referred to the fact that the website was mostly accessed by Canadian visitors. Finally, the judge found that the website had a negative impact on the Canadian public due to the number of complaints received by the OPCC from people in Canada.[97]

The final point examined by the Court regarding the extraterritorial application of PIPEDA was whether exercising jurisdiction over the defendant was compliant with the principle of comity.[98] Indeed, the respondent had been fined by the Romanian National Supervisory Authority for Personal Data Processing (RNSAPDP) for violating local data protection laws following a complaint that the applicant A.T. had initiated in Romania as well.[99] Mr. Radulescu had appealed against the fine and the proceedings before the RNSAPDP were ongoing when the present case was discussed by the Ontario Federal Court. The Court, however, found that the fine issued by the RNSAPDP and the fact that the latter had participated in the investigation carried out by the OPCC in Canada was not a sufficient reason for the Canadian court to decline the exercise of jurisdiction over the defendant.[100] This is because, given the participation of the RNSAPDP in the OPCC's investigation, the Federal Court's findings complemented rather than offended any action

[94] *A.T. v Globe24H.com* (n 3) [51].
[95] ibid [52].
[96] ibid. The judges referred to *Libman v The Queen*, [1985] 2 SCR 178 at p 208 [*Libman*] (as cited in *A.T. v Globe24H.com* (n 3) [52]). The case was related to a fraudulent stock scheme whereby American purchasers were contacted via phone calls from Canada, where the profits from the scheme were ultimately collected.
[97] *A.T. v Globe24H.com* (n 3) [53].
[98] ibid [54]-[62].
[99] ibid [22].
[100] ibid [54].

taken against the defendant in Romania.[101] Finally, the Court dismissed Mr. Radulescu's argument that following the *Club Resorts v Van Breda* decision a Canadian Court cannot establish jurisdiction over a foreign defendant if the latter did not have an actual presence in the jurisdiction, such as maintaining an office there, as opposed to a merely virtual presence.[102] Indeed, the judge stated that *Van Breda* did not deal with e-trade but with tort claims, and that in fact the Supreme Court was concerned about avoiding the exercise of 'what would amount to forms of universal jurisdiction in respect of tort claims arising out of certain categories of business or commercial activity'.[103] For this reason, the Ontario Federal Court found that the *Van Breda* reasoning was not relevant to the present case.[104] Ultimately, the judge ordered Mr Radulescu to pay for the damage caused to the claimant and to remove all Canadian decisions containing personal information from Globe24h.com.[105]

Similarly to the two previous cases examined, the exercise of State jurisdiction by the Canadian Courts in this case is justified by the fact that the defendant targeted a Canadian audience. This is evidenced by the fact that Mr. Radulescu published Canadian Court's decisions and received payments from Canadian Internet users in exchange for the de-listing of their personal information. In other words, Mr. Radulescu had put himself within Canadian jurisdiction. However, as will be examined below, this case poses problems regarding the exercise of freedom of expression online. This is because the domestic court, instead of ordering the de-listing of the personal information, ordered the removal of the content published on Mr. Radulescu's website, which was perfectly legal in Canada.

3.2.4 The *Microsoft v. the United States* case

On December 2013, a United States Magistrate Judge from the US District Court for the Southern District of New York issued a "Search and Seizure Warrant" directed at Microsoft at the request of the US government.[106] The warrant was issued pursuant to section 2703 of the Stored Communications Act (SCA) and was related to an Outlook email account maintained by Microsoft.[107] The account was believed to be used in

[101] ibid [58].
[102] ibid [60]. *Club Resorts Ltd v Van Breda*, 2012 SCC 17, [2012] 1 SCR 572 [*Van Breda*] (as cited in *A.T. v Globe24H.com* (n 3) [59]).
[103] *A.T. v Globe24H.com* (n 3) [62].
[104] ibid.
[105] ibid 'Judgement' [2]-[3].
[106] *Microsoft Corp. v. United States* (n 4) 9.
[107] Section 2703 of the SCA establishes 'conditions under which the government may require a service provider to disclose the content of stored communications', *Microsoft Corp. v. United States* (n 4) 16. In particular, section 2703 states that in order to access stored communications the government must obtain a

conjunction with illegal drug trafficking. The nationality and the location of the user who set up the account were unknown.[108] Microsoft was asked to seize the email account and to disclose its content to the US government.[109] However, the company found that most of the account content was stored outside the US, in its Dublin datacentre. Therefore, after having provided the authorities with the data that were stored in the United States, the company asked the Magistrate Judge to quash the warrant in respect to the content stored in Dublin.[110] The Magistrate Judge denied the motion to quash the warrant and the District Court subsequently held Microsoft in contempt for its failure to fully comply with it.[111] Microsoft applied to the US Court of Appeals for the Second Circuit. On 14 July 2016, the Court granted Microsoft's appeal, and reversed the Magistrate Judge's decision. The US government appealed against the Court of Appeals' decision, however the appeal was rejected and the decision was upheld on January 2017.

Microsoft argued that a warrant issued under section 2703 of the Stored Communications Act (SCA) does not have extraterritorial effect and therefore does not apply to material that is stored in a foreign country.[112] According to Microsoft's argument, disclosing data that are stored abroad would amount to an unlawful invasion of its clients' privacy.[113] On the other hand, the US government maintained that an SCA warrant is to be equated to a subpoena, rather than a warrant. For this reason, just like a *subpoena duces tecum*, an SCA warrant requires that the service provider disclose the data stored on its facilities, regardless of the location of the latter.[114] In particular, the US government stated that, as acknowledged by Microsoft, the company could retrieve the data contained in its Dublin servers directly from the United States by using a database management programme.[115] This fact showed that the warrant did not require Microsoft to act outside the territory of the United States.

The Court of Appeal rejected the US government's arguments. Indeed, the Court stated that in the SCA the geographical scope of the Act and that of the search warrants was not specified.[116] However, the judges did underline that there are strong and binding

warrant issued according to the Federal Rules of Criminal Procedure. Rule 41 of the Federal Rules of Criminal Procedure, which is related to federal warrants, allows magistrates to issue warrants whose geographical scope is limited to the United States territory.

[108] *Microsoft Corp. v. United States* (n 4) 20-21.
[109] ibid 4.
[110] ibid 11.
[111] ibid 5.
[112] ibid 20.
[113] ibid.
[114] ibid 5.
[115] ibid 9.
[116] ibid 21.

precedents in US case law against the extraterritorial application of US Statutes.[117] Besides, the Court found that the warrant provisions of the SCA did not foresee nor permit the extraterritorial application of the Act and that when the Congress approved the SCA it did not intend for it to apply extraterritorially.[118] Moreover, the Court stated that the SCA's plain meaning, text, framework, procedural aspects and legislative history showed that the primary focus of the Act was to protect the privacy of the stored electronic communications of Internet users.[119] Finally, the Court of Appeal found that compelling Microsoft to execute the warrant would amount to unlawfully applying the SCA extraterritorially. Indeed, the content to be disclosed was located in Dublin and was therefore subjected to the jurisdiction of a foreign State. This was true notwithstanding the fact that the data could be accessed by Microsoft from the US through a data management programme. In other words, the act of accessing data equated to an extraterritorial act because it implied an interaction between Microsoft and the data stored in Dublin that were subjected to Irish jurisdiction.[120] For this reason, the disclosure of the data would have taken place outside the United States, irrespective of the location of the person who set up the email account or the fact that Microsoft is based in the United States.

The Court of Appeal acknowledged that there are some practical difficulties associated with not granting the extraterritorial effect of the SCA, as stated by the Magistrate Judge. Indeed, offenders could easily mislead service providers into storing their data outside the US. In Microsoft's case, for example, data are stored near the location that the users indicate as their own when they subscribe to the service.[121] In addition, the process for obtaining foreign-stored data is cumbersome. This is regulated by the Mutual Legal Assistance Treaties (MLAT) between the US and other countries. Although Ireland is a party to the treaty, there is no formal way of obtaining assistance from those countries which have not signed it.[122] However, the Court found that these considerations do not override its findings against the extraterritorial application of the SCA. In particular, the judges highlighted the importance of respecting the principle of comity in cross-boundary criminal investigation.[123] Specifically, the Court dismissed the theory that foreign States' interests are unaffected by extraterritorial orders that allow the

[117] ibid.
[118] ibid 22, 32.
[119] ibid 33.
[120] ibid 40.
[121] ibid 8, 41.
[122] ibid 41.
[123] ibid 41-42.

US to access data stored abroad and 'import' them in the US just because the service provider has a base there.[124]

On 23 June 2017, the US Department of Justice (DOJ) filed a petition asking the Supreme Court to review the July 2016 decision.[125] In October 2017, the Supreme Court granted the US DOJ's petition and in February 2018 it heard oral arguments from the parties.[126] However, a major legal development led the Supreme Court to declare the case moot on 17 April 2018.[127] Indeed, in March 2018, while the case was still pending before the Court, President Trump signed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amended the SCA requiring email providers to grant US authorities in the course of a criminal investigation access to electronic communication or remote computing data in the email providers' possession, custody or control regardless of where the data are stored.[128] The CLOUD Act also allows the providers of email and remote computing data services to file a motion to quash or modify the legal process if they believe that the costumer whose communication the government is trying to get access to is not a US person and does not reside in the US and if complying with the disclosure request would require them to violate the laws of a qualifying foreign government.[129] In particular, a qualifying foreign government according to the CLOUD Act is a government with which the US have established an executive agreement pursuant to the Act and that provides electronic communication service providers and remote service providers with procedural and substantive opportunities similar to those guaranteed in the CLOUD Act. Based on this Act, the US government presented Microsoft with a new warrant regarding the disclosure of the requested information and this warrant replaced the one issued

[124] ibid 42.
[125] David Kravetz 'Does US have right to data on overseas servers? We're about to find out' (*ArsTechnica*, 24 June 2017) https://arstechnica.com/tech-policy/2017/06/supreme-court-asked-to-decide-if-us-has-right-to-data-on-foreign-servers/ accessed: 1 December 2017.
[126] SCOTUS blog 'United States v. Microsoft Corp.' (*SCOTUS blog*) <https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/> accessed 09 August 2020.
[127] Oyez 'United States v. Microsoft Corporation' (*Oyez*) <https://www.oyez.org/cases/2017/17-2> accessed 09 August 2020.
[128] 'A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States' H.R.4943 CLOUD Act § 2713 <https://www.congress.gov/bill/115th-congress/house-bill/4943/text> accessed: 09 August 2020.
[129] '(A) A provider of electronic communication service to the public or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—"(i) that the customer or subscriber is not a United States person and does not reside in the United States; and "(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government', ibid § 2713 (2) Motions to Quash or Modify— (A).

previously.[130] The US Supreme Court, therefore, declared the case moot since there was no longer a live dispute between the parties.[131]

Overall, the *Microsoft* case differs from the cases examined so far since, notwithstanding their territorial competence over Microsoft, the domestic courts found that they did not have jurisdiction to order the extraction of the data. The judges in this case did recognize the extraterritorial implications of an act, such as the extraction of data from a database, that would at least partially happen from within the national territory. Notwithstanding the fact that the CLOUD Act subsequently rendered it possible for US authorities to access data in possession of a US company regardless of where in the world the data are located, this point represents a difference with the other cases examined in this chapter and will be discussed in the next section.

3.3 Case analysis

The cases examined in this chapter deal with the extraterritorial exercise of State jurisdiction to regulate content published online. In three out of four cases, the *CNIL*, *Equustek* and *Radulescu* cases, the domestic courts have found that the respective national laws can be applied to regulate the online activities committed by foreign defendants. In these cases, the exercise of State jurisdiction over the foreign defendants does not seem particularly problematic as it is justified by the fact that the foreign defendants were operating in those States or targeted an audience located there. It is the extraterritorial reach of the measures imposed by these domestic courts that poses problems regarding the respect for comity between States and the rights of foreign Internet users. This point is illustrated particularly well in the fourth case examined in this chapter, the *Microsoft* case. In that case the US Court of Appeals for the Second Circuit clearly stated that access from the United States to data stored in Ireland without the latter's consent would negatively impact on Ireland's sovereignty.

In regard to the justification for the exercise of jurisdiction, in the *CNIL*, *Equustek* and *Radulescu* cases the exercise of jurisdiction over the US-based Google and the Romania-based Mr. Radulescu is justified by the fact that the defendants were operating or targeting an audience located in France and Canada. In particular, in the *Google v CNIL* case, the CNIL found that the French Data Protection Act is applicable to the US-based Google Inc. due to the presence on the French territory of a Google subsidiary and the fact that

[130] Oyez 'United States v. Microsoft Corporation' (n 127).
[131] ibid.

the data processing happened, at least partially, on the French territory.[132] Indeed, the CNIL found that Google France is not an independent processing system separated from the one operated by Google but rather a mere pathway to the main processing system operated by the US company. The French authority therefore relied on the objective territorial principle when establishing the application of the French Data Protection Law to Google. In particular, the CNIL's finding regarding the interconnection between the activities of Google France and Google Inc. echoed the CJEU's finding in the *Google Spain* case. In that case, the Court stated that the activities of Google Inc. and its European subsidiaries are

> 'inextricably linked since the activities relating to the advertising space [*carried out by Google's subsidiaries*] constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed'.[133]

These findings were also confirmed by the CJEU in its 2019 pronouncement on the *Google v CNIL* case, where the Court found that both the Directive 96/45 and the GDPR apply to Google since the processing of personal data carried out by Google LLC happens on the French territory.[134]

Similarly, in the *Equustek* case the Canadian courts found that Google Inc. conducted business activities in Canada both because it sold advertising space to Canadian consumers and because Goole Search activities happened in Canada.[135] In this regard, the court of first instance stated that Google Search could not be considered as a merely passive information website, as claimed by Google. Indeed, its auto-complete function generated a list of search suggestions designed to help Canadian Internet users with their search queries. In particular, the company collected a wide range of data related to the search history of its Canadian Internet users and drew on the data collected to make its auto-complete function more responsive to each user's preferences.[136] It can therefore be

---

[132] Decision no. 2016-054 (n 1) 6-7. Article 5-I-1 of the French Data Protection Act states that the law applies only to the data controller who 'although not established on French territory or in any other Member State of the European Union, uses means of processing located on French territory, with the exception of processing used only for the purposes of transit through this territory or that of any other member State of the European Union'. Article 48 of the Data Protection Act establishes that '[t]he powers provided under Article 44 (on-site investigations), as well as in Section I, in Section II Paragraph 1° and in Section III of Article 45 shall be applicable as regards any processing operations carried out, whether fully or partially, on the national territory, including where the data controller is established in another Member State of the European Union' Loi Informatique et Libertes (n 8) art 5-I-1 and 48.

[133] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (n 9) para 56.

[134] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (n 1) para 52.

[135] *Equustek Solutions Inc. v. Jack* 2014 BCSC (n 2) [51].

[136] ibid [48]-[49].

argued that the courts in the *Equustek* case exercised jurisdiction over the defendant based on the objective territorial principle: Google Inc.'s sale of advertising space and Google Search's processing of personal data happened, at least partially, on Canadian territory.

The *A.T. v Radulescu* case is slightly different from the two cases discussed above since the Ontario Federal Court exercised jurisdiction over Mr. Radulescu based on a qualified access-based jurisdictional approach. Indeed, the judge found that the content hosted on Globe24H.com had been published in Canada since it was accessible there. However, the Court also conducted a targeting test and found that the website expressly targeted Canadian audience because it advertised that it contained decisions from Canadian Courts and because the majority of the website's visitors were Canadian. However, the extent of this targeting test appears quite limited. The Court did not mention other possible targeting factors that would have helped the judge to substantiate the finding of a close connection between the Romanian defendant and Canada. Examples of these factors are: the website's top-level domain name, its language, its search engine ranking and visibility when searched from Canada and whether the website contained any advertisement that targeted a Canadian audience.[137] Moreover, it would have been particularly useful to know which currency was adopted by Mr Radulescu when he asked for payments to remove the personal information of Canadian Internet users. However, the limited extent of the targeting test conducted by the Ontario Federal Court is not surprising. Indeed, there is no international agreement on the factors on which each Court should rely in order to establish the existence of a close connection between a foreign website and the domestic forum.[138] This subject is perceived by many Courts as an internal affair or a matter of private international law, rather than the subject of public international law with direct repercussions on the relationship between States and the freedom of expression of foreign Internet users.

Notwithstanding the limited extent of the targeting test conducted by the Ontario Federal Court, the existence of a close connection between Mr. Radulescu and Canada is reinforced by the fact that the defendant was conducting business activities in Canada, as stated by the OPCC.[139] Indeed, he was receiving payments from Canadian Internet users in exchange for the removal of their personal details from the website. This fact suggests that the defendant was aware that he was targeting Canadian Internet users, since he

[137] University of Geneva 'Geneva Internet Disputes Resolution Policies 1.0' (*Geneva Internet Disputes Resolution Policies 1.0*) <https://geneva-internet-disputes.ch/> accessed: July 2017), 7.
[138] See Chapter 5 section 5.3 for an analysis of the targeting test and of the criteria being used to determine when a website is targeting an audience located in a given State.
[139] *A.T. v Globe24H.com* (n 3), [81].

consciously entered into a transaction with them and was obtaining money from them as a result of the de-indexing of their personal information.

However, the fact that the domestic courts in the above mentioned three cases had personal jurisdiction over the defendants does not mean that those courts had the authority to impose measures with extraterritorial effects. The fourth case examined in this chapter, the *Microsoft* case, illustrates this point particularly well. Unlike the other cases examined, in the *Microsoft* case the transnational character of the dispute is not due to the location of the parties - Microsoft is an American corporation and the US sovereignty over the company is undisputed - but rather due to the location of the data, which were stored in Microsoft's Irish data centre. However, notwithstanding their territorial competence over Microsoft, the domestic courts stated that they did not have jurisdiction to order the extraction of the data. Interestingly, the judges found that although the act of extraction itself could be conducted via computer from the United States and did not require the US authorities' physical presence in Ireland, it still equated to an unlawful extraterritorial act. In other words, in this case the judges recognized that an act committed online had the potential to violate the sovereignty of other States even if that act could be initiated by a domestic company from within the national territory and would therefore at least partially happen within the domestic jurisdiction. However, as mentioned above, the finding of the US Court of Appeals for the Second Circuit have been rendered void by the passing of the CLOUD Act, which makes it possible for US authorities to access data stored abroad and for foreign States to access data stored by US service providers if they meet specific conditions set out in the Act. Interestingly, the CLOUD Act has introduced some guarantees to address concerns that accessing data stored abroad could violate the rights of foreign Internet users, by allowing the company to apply to quash the access request if it believes that the data are related to a non-US person not residing in the US and if by granting access to the data the company would be required to violate the laws of a qualifying foreign government.[140] In addition, the CLOUD Act provides for a comity analysis that US Courts must conduct in case the communications service provider argues that it cannot comply with the request for disclosure of data as it would require it to violate the laws of a qualifying foreign government. In that instance, among the factors that should be taken into account by the Courts when deciding whether to order access to the data figure *inter alia* the interest of the US to access the data, the interest of the relevant foreign government to prevent the

[140] Jennifer Daskal 'Unpacking the Cloud Act' (2018) 4 EUCRIM 220, 221-222.

disclosure and the likelihood and the extent of the penalty that could be imposed on the service provider.[141] Overall, the CLOUD Act has been defined by some commentators as a positive development which could incentivise foreign governments to raise the standards of protection of the data stored abroad to comply with the security requirements imposed by the Act.[142] However, some issues remain open, such as the conflict between the CLOUD Act and the GDPR, article 48 of which states that any judgement or decision from a third country requiring a data controller or processor to transfer or disclose personal data can only be recognised or enforced 'if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State'.[143] In this regard in July 2019, the European Data Protection Board and the European Data Protection Supervisor conducted a preliminary assessment regarding the implications of the CLOUD Act on the GDPR concluding that

> 'unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, the lawfulness of such transfers of personal data cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject'.[144]

It will therefore be interesting to see how this issue will develop in the future.

In any case, the findings of the US Court of Appeals for the Second Circuit differ significantly from those of the *CNIL* and *Equuste*k cases. Indeed, in those cases the opposite has happened: the existence of a link between the activities of a foreign defendant and a given forum was used as a basis to order measures with extraterritorial effects. As stated above, these measures violate the sovereignty of foreign States as well as the freedom of expression of Internet users located in foreign countries. Indeed, in the *CNIL* and *Equuestek* cases, the domestic authorities argued that the de-listing is effective only if it is carried out globally. Therefore, according to these cases, in order to guarantee the effective enjoyment of the right to de-listing and intellectual property, citizens of other countries must be prevented from accessing content that might be legal in those countries. This, however, equates to unlawfully limiting the freedom of expression of foreign Internet users, who, according to international law, should primarily be regulated by the laws of the country where they are located.

---

[141] CLOUD Act (n 128) § 2713 (3).
[142] Daskal (n 140) 220.
[143] General Data Protection Regulation (n 10) art 48. See also Daskal (n 140) 223.
[144] Juan Fernando López Aguilar, LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data, protection' 10 July 2019 <https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_coverletter_en.pdf> accessed: 10 August 2020.

In addition, this approach violates the sovereignty of foreign States. The CNIL, for instance, stated that de-listing that only applies to Google European domain names is not effective because French Internet users could still access the unwanted search result if they were outside the EU. This point is problematic because, although international law does allow for concurring exercises of jurisdiction,[145] CNIL's claim equates to imposing the laws of one country on all the other countries, which, as observed by the CJEU, might not recognise the right to delisting or have a different approach to it.[146] The *Equustek* case is a perfect example of this point. Indeed, the Canadian Supreme Court rejected the argument that global de-listing violated the core values of foreign countries. The judges found that it was likely that in foreign countries the sale of other companies' intellectual property was illegal as well. This finding, however, has been directly contradicted by the US District Court for the Northern District of California which declared that the order of the Canadian Supreme Court is unenforceable in the United States. In particular, the judges found that the Canadian order was contrary to US public interest, since Congress had established that freedom of speech in the US would be impaired if ISPs were liable for content published by a third party.[147] The Court also stated that the order undermines global freedom of speech online.[148] As mentioned above, the disagreement between the Canadian and the US courts continued when the British Columbia Court refused to interpret the Californian District Court's decision as showing that the delisting ordered in Canada violated foreign law.[149] This disagreement is concrete proof of the many implications on both international comity and freedom of expression of extraterritorial measures with worldwide effect. Indeed, notwithstanding the different interpretation of the order given by the British Columbia Court, the US Court's order shows that a sovereign State's interests are affected when a foreign State exercises jurisdiction extraterritorially on the Internet.

Overall, the problem posed by CNIL and the Canadian Supreme Court's jurisdictional approach is that it equates to exercising jurisdiction over an act, such as the indexing of personal information, that is not internationally unlawful.[150] Indeed, imposing the worldwide erasure of a search result is a measure with extraterritorial effect that makes it impossible for anyone in the world to access that information through a given search

[145] See Chapter 4 section 4.2 for an analysis of this point.
[146] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (n 1) para 59.
[147] *Google LLC v Equustek Solutions Inc., et al.*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017) (n 70) 5.
[148] ibid 6.
[149] *Equustek Solutions Inc. v Jack,* 2018 BCSC (n 71), [20]-[22].
[150] Douwe Korff, The rule of law on the Internet and in the wider digital world, Council of Europe Commissioner for Human Rights, 2014, 61.

engine when searching for the name of the person who requested delisting. The worldwide implications of such extraterritorial exercise of jurisdiction would be justified if the indexing of personal information was considered as a *delicta iuris gentium*, for example, a particularly grave crime constituting a concern for the whole international community. In that case, the international community would have a vested interest in allowing every State to order global de-indexing. However, this is not the case since the right to de-listing has only recently been recognised and is mainly a European right, although other countries are increasingly following the CJEU's approach and are recognising a right to delisting in their jurisdictions.[151] In Canada, for example, the Office of the Privacy Commissioner of Canada (OPC) has stated that the Personal Information Protection and Electronic Documents Act (PIPEDA) already provides for a right to deindexing.[152] Due to uncertainties in the interpretation of the law, however, in October 2018 the OPC asked the Federal Court to examine this issue,[153] which is currently pending before the Court.[154] However, a proof of the controversial nature of a global approach to delisting can be found in the critique moved to it by the Office of the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights. In the report Standards for a Free, Open and Inclusive Internet, the Office of the Special Rapporteur stated in regard to the issuing of global delisting orders by domestic courts that these global orders can lead to the extraterritorial application of domestic laws and that they 'raise complex questions regarding the future of jurisdiction on the Internet and its interplay with national sovereignty'.[155] In particular, in the report, which was issued

[151] Internet & Jurisdiction Policy Network 'Global Status Report 2019' (n 46) 97. According to this Report, among the countries that have recognised a right to delisting in their domestic law figure Argentina, India, South Korea and Canada.

[152] 'Following public consultations, the OPC took the view that PIPEDA provides for a right to de-indexing – which removes links from search results without deleting the content itself – on request in certain cases. This would generally refer to web pages that contain inaccurate, incomplete or outdated information.' Office of the Privacy Commissioner of Canada 'Privacy Commissioner seeks Federal Court determination on key issue for Canadians' online reputation' (*Office of the Privacy Commissioner of Canada*, 10 October 2018) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181010/ accessed: 09 August 2020).

[153] ibid.

[154] This information is accurate as of 10 December 2019, when the OPC published its 2018-1029 Annual Report stating *inter alia*: 'Our Office has also brought a reference to the Federal Court to seek clarity on whether PIPEDA applies to Google's search engine service, which is an issue that arose in the context of a complaint to our Office against Google requesting that certain web pages be de-indexed from results for searches of the complainant's name. Though this preliminary jurisdictional issue is currently before the courts, we believe that it is incumbent on Parliament to consider the right to be forgotten and other proposed remedies for protecting online reputation, and that it would be inappropriate to wait to act on such fundamental issues', Office of the Privacy Commissioner of Canada 'Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy' (*Office of the Privacy Commissioner of Canada*, 10 December 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/> accessed 09 August 2020.

[155] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (15 March 2017), [120].

in 2017 and therefore before the 2019 *CNIL* judgement of the CJEU clarifying the scope of delisting, the Special Rapporteur underlined that international human rights law does not recognise the right to delisting in the terms expressed by the CJEU. On the contrary, if the system that leaves to private parties the decision on how to implement delisting were to be applied to the Americas, it would lead to serious problems in regard to the protection of freedom of expression guaranteed by Article 13 of the American Convention on Human Rights.[156] Besides, the Commission stated that

> '[i]n the Americas, after many years of conflict and authoritarian regimes, individuals and human rights groups have maintained a legitimate claim to access to information regarding governmental and military activity of the past and gross human rights violations. *People want to remember and not to forget. In this sense, it is important to recognize the particular context of the region and how a legal mechanism such as the so-called "right to be forgotten" and its incentive for de-indexation might impact the right to truth and memory*' [emphasis added].[157]

This shows that, as observed by the CJEU in the *CNIL* case, the global reach of a delisting order is problematic as it does not take into account the fact that the right to delisting is not globally protected. Therefore, the fact that the CJEU has left the door partially open to global delisting orders can be seen as questionable. In this regard, the qualified approach to global delisting followed by the Swedish DPA seems a preferable alternative. This approach, as mentioned in section 3.2.1.1, consists in granting global delisting only when there is a specific connection to the country ordering delisting, in particular if the search result to be de-listed is linked to information written in the language of that country, is addressed to an audience located there, contains details about a person that is in that country or if it has been published on a website containing that country code top level domain.[158]

As to the *Radulescu* case, as stated above, this case is slightly different from the *CNIL* and *Equustek* cases. Indeed, while Ontario Federal Court's decision does impose restrictions on freedom of expression, the order to remove the content published on Globe24H.com does not represent an unlawful extraterritorial act. Indeed, as stated above, the exercise of State jurisdiction over the foreign defendant was justified by the fact that Mr. Radulescu was targeting Canadian Internet users and was conducting business in Canada. In other words, because of his actions, Mr Radulescu had put himself within Canadian jurisdiction. For this reason, the Ontario Federal Court was competent

[156] ibid [132].
[157] ibid [134].
[158] Datainspektionen 'The right to be forgotten may apply all over the world' (n 39).

to order that the defendant de-indexed the personal information of Canadian Internet users. However, the problem represented by the *Radulescu* decision is that the Court did not limit itself to order the de-indexing of personal information, but rather it ordered the removal of the Canadian decisions themselves. This fact is problematic because those decisions were in compliance with Canadian law. Indeed, they were available on Canadian legal websites, the only difference being that on those websites the decisions were not indexed. Therefore, the Court should have ordered Mr Radulescu to remove the indexing of the decisions published on Globe24H.com and to cease requesting money in exchange for the de-indexing, rather than to remove the decisions themselves. This is all the more so considering the final nature of the act of removal, as the *BOÜ* case discussed before the CJEU and examined in Chapter 2 shows. Ordering the removal of content from a website is a definitive act since it is not territorially quantifiable: once removed from the Internet, the information disappears worldwide.[159] In Mr. Radulescu's case, however, the decisions published on his website remained accessible on Canadian legal websites. Notwithstanding this, because the information contained on Globe24H.com was legal in Canada, the Ontario Federal Court should have refrained from ordering its removal.

3.4 Conclusion

This chapter has dealt with the extraterritorial exercise of State jurisdiction in transnational Internet-related cases. The argument brought forward in this analysis is that the extraterritorial application of national laws and the adoption of measures with worldwide implications, such as global de-listing, violate the sovereignty of foreign States and the freedom of expression of foreign Internet users.

In the first two cases examined, the *CNIL* and *Equustek* cases, the exercise of State jurisdiction over the US-based Google was justified by the fact that Google was operating in France and Canada respectively. The national authorities in these cases relied on the objective territorial principle to establish jurisdiction over the US-based Google. Indeed, the domestic authorities found that Google Search activities, which are conducted in the US by Google, happen at least partially on French and Canadian territory as well. This, according to the CNIL, the CJEU and the Supreme Court of Canada, is due to a combination of factors, including the presence of Google subsidiaries in France and Canada respectively and the fact that those subsidiaries are inextricably linked to the search activities conducted by Google.

[159] For an analysis of the *BOÜ* case, see Chapter 2 section 2.3.6.

However, notwithstanding the fact that the national authorities in these cases had jurisdiction over the defendant, these authorities violated the sovereignty of foreign States and affected freedom of expression online when they ordered global de-listing. Indeed, as stated in the *Microsoft* case, the fact that a State can exercise jurisdiction over a given subject does not justify that State's adoption of extraterritorial orders.

Ordering global de-listing infringes the freedom of expression of foreign Internet users because such a worldwide measure prevents them from accessing content that might be legal in their countries. This global measure is therefore contrary to the international law principle that citizens of foreign States should primarily be subjected to the laws in force in those States.

Further important proof of the implications on State sovereignty of global de-listing is represented by the order issued by the US District Court for the Northern District of California declaring the *Equustek* order unenforceable in the United States. Interestingly, the US judges found the Canadian order to be contrary to US public interest and a threat for global freedom of speech online. This fact shows that, as stated in the *Microsoft* case, foreign States' interests are deeply affected when a State exercises jurisdiction extraterritorially on the Internet.

Ultimately, the problem posed by CNIL and the Canadian Supreme Court's jurisdictional approach is that it equates to exercising universal jurisdiction over an act, such as the indexing of personal information, that is not unlawful according to international law. As mentioned above, the worldwide implications of such extraterritorial exercise of jurisdiction would be justified if for instance the international community recognized the indexing of personal information as a crime of exceptional gravity and therefore allowed every State to order global de-indexing. This, however, is not the case since the right to de-listing has only recently been recognised and is mainly a European right (although other States are increasingly recognising a right to delisting in their legal systems). The criticism of the right to delisting by the Office of the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights proves this point particularly well. As observed by the Special Rapporteur, in the Americas, where a right to delisting could clash with the right to truth and memory, people want to remember, rather than forget. This underlines how different legal systems have different approaches towards delisting and how therefore a global approach to delisting orders is problematic.

As to the *Radulescu* case, this case is slightly different from the *CNIL* and *Equustek* cases since the Ontario Federal Court's order against Mr. Radulescu has not an unlawful

worldwide effect. This is because, as a consequence of the targeting of Canadian Internet users, Mr. Radulescu was, or should have been, aware that he had put himself within Canadian jurisdiction. For this reason, the domestic Court was competent to order that the defendant de-indexed the personal information of Canadian Internet users. However, the problem represented by the *Radulescu* decision is that the domestic Court not only ordered the de-indexing of personal information, but also the removal of the content published on Globe24H.com. That content, however, was perfectly legal according to Canadian law. Therefore, by ordering its removal, the domestic Court violated Radulescu's freedom of expression.

Finally, the analysis of the cases examined in this chapter highlights a further important point: national courts have so far approached the subject of establishing State jurisdiction online as either a purely domestic matter or a matter that should be regulated by existing rules of private international law. However, as discussed above, the way in which States exercise jurisdiction online has direct implications on the principle of State sovereignty and international comity as well as the rights of foreign Internet users. Therefore, the study concludes that, when establishing State jurisdiction online, national courts should apply domestic laws in compliance with public international law. In particular, the courts should bear in mind that, due to the apparently borderless nature of the Internet, their decisions have the potential to affect the sovereignty of foreign States and freedom of expression rights of foreign Internet users. Ultimately, an international agreement on how to balance and reconcile the diverse and apparently conflicting domestic and international needs in the jurisdictional field is needed.

4. The Rules Regulating the Exercise of State Jurisdiction according to Public International Law and Human Rights Law

4.1 Introduction

This chapter deals with the rules regulating the exercise of State jurisdiction according to international law and human rights law. This analysis will highlight the uncertainties as to the rules governing State jurisdiction in these two regimes as well as the fundamentally different meaning that State jurisdiction has in these two areas of law. This will be achieved by first illustrating the meaning of State jurisdiction in public international law in section two, where the rules governing territorial and extraterritorial State jurisdiction will be presented. Section three will then turn to human rights law, highlighting the personal and the spatial model of jurisdiction developed by human rights courts. Finally, section four will summarize the main conclusions of the analysis conducted in the previous sections.

4.2 The concept of State jurisdiction according to public international law

The concept of State jurisdiction in public international law is primarily related to the legality of State action. The public international law rules of jurisdiction define the criteria according to which a State is entitled to regulate a given matter without infringing the sovereignty of other States.[1]

State jurisdiction is usually divided into prescriptive, adjudicative and enforcement jurisdiction. As stated in Chapter 1, this study focuses on the exercise of prescriptive jurisdiction, which is related to the right of a State to apply its own laws to regulate certain matters. Adjudicative jurisdiction illustrates the right of the domestic courts of one State

[1] Cedric Ryngaert, *Jurisdiction in International Law* (1st, Oxford University Press 2008) 5-6; Ralph Wilde 'The "Jurisdiction" Test in the Main Human Rights Treaties on Civil and Political Rights' (2007) 40 Isr L Rev 505, 513; Alex Mills 'Rethinking jurisdiction in international law' (2014) 84 BYIL 187, 194; Marko Milanović, 'From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties' (2008) 8 Hum. Rts. L. Rev. 411, 423; Marko Milanović, *Extraterritorial Application of Human Rights Treaties* (1st, Oxford University Press 2011) 128.

to hear cases that are brought before them, whereas enforcement jurisdiction indicates the right of the authorities of a State to compel other parties to comply with the laws and regulations of that State.

The division of State jurisdiction into these three categories however has been contested in literature due to the lack of agreement as to whether this division in fact reflects customary international law.[2] In addition, some commentators have underlined how the division between these three categories of jurisdiction is not always clear-cut, as some of the categories tend to merge in certain cases. In particular, some authors have claimed that adjudicative jurisdiction tends to merge with prescriptive jurisdiction in all those cases where the reach of a domestic statute is not clear and the courts are therefore said to exercise prescriptive rather than adjudicative jurisdiction.[3] Despite the disagreement, however, the three categories of jurisdiction are widely accepted internationally. Indeed, both scholars and judges refer to these three categories when describing the international law rules of jurisdiction.

Another difference between the categories of jurisdiction is related to the different scope of application of prescriptive and enforcement jurisdiction. According to customary international law, jurisdiction is primarily territorial, meaning that a State can exercise jurisdiction first and foremost within its national borders.[4] However, according to the *Lotus* judgement of the Permanent Court of International Justice (PCIJ), while States cannot exercise enforcement jurisdiction outside their national territory, they are free to exercise prescriptive jurisdiction regarding events and people located in other States. According to this view, the exercise of prescriptive jurisdiction outside the national territory is limited only if there is a specific prohibitive rule of international law that prevents States from doing so.[5] The view expressed in the *Lotus* judgement has received

[2] Mills (n 1) 194-195.
[3] Ryngaert (n 1) 10; Mills (n 1) 195.
[4] The concept according to which jurisdiction in international law is primarily territorial has, however, been criticised by various authors, according to whom, apart from the territorial principle of jurisdiction, the other international law jurisdictional principles deal with exceptions to territoriality. For a discussion of this point, see Chapter 5 Section 5.3.
[5] 'Now the first and foremost restriction imposed by international law upon a State is that-failing the existence of a permissive rule to the contrary-it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention. It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts 'outside their territory, and if, as an exception to this general prohibition, it allowed States to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their

many critiques. Some commentators consider it outdated and an expression of the theory of international positivism that was dominant in the early 20th century, while others contest its nature of valid precedent as far as extraterritorial jurisdiction is concerned.[6] The main critique of the *Lotus* rule, however, is that it is not deemed to reflect customary international law anymore.[7] International Court of Justice (ICJ) President Bedjaoui in his Declaration in the *Case Concerning the Legality of the Threat or Use of Nuclear Weapons* for example, underlined that the ICJ did not interpret the absence of a specific provision regarding the use of nuclear weapons as an automatic authorization to use nuclear weapons.[8] Instead, the theory that some consider as an expression of customary international law is that a State can only exercise extraterritorial prescriptive jurisdiction if a permissive rule of international law establishes so.[9] In other words, according to this view the exercise of extraterritorial prescriptive jurisdiction is limited by positive international law rules.

Finally, there are three principles of international law that, according to some commentators, might underly the rules of jurisdiction: the requirement of a genuine connection between the State and the subject or act upon which jurisdiction is exercised, the principle of non-intervention and the principle of reasonableness.[10] The requirement of a genuine connection establishes that in order for a State to exercise jurisdiction over given acts there must be a genuine connection between the State and the act. The principle of non-intervention establishes that States should balance their contacts with the situation over which they exercise jurisdiction and their interests in exercising jurisdiction with other States' contacts and interests. However, the criteria that States should take into account when conducting such a balance remain unclear. Finally, the rule of reasonableness establishes that States should not interfere with other States' sovereignty. This rule is part of the US Restatement of the Law (Third), although its status under international law is unclear.[11] Overall, as observed by Mills, international law does allow for concurring exercises of jurisdiction by States, as evidenced, for example, by the fact

territory, it leaves them in this respect a wide measure of discretion which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable', *The Case of S.S Lotus* [1927] PCIJ Series A N.10 18-19.

[6] Mills (n 1) 191; Ryngaert (n 1) 26.

[7] Mills (n 1) 193-194; Ryngaert (n 1) 27.

[8] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion), Declaration of President Bedjaoui [1996] ICJ Rep 95 [14]-[15]; See also R Rabinovitch 'Universal Jurisdiction in Absentia' (2005) 28 Fordham Int'l L.J. 500, 505-506.

[9] Ryngaert (n 1) 27; Mills (n 1) 193-194.

[10] Ryngaert (n 1) 35-36; R Uerpmann-Wittzack, 'Principles of International Internet Law' (2010) 11 German L. J. 1245, 1253.

[11] Ryngaert (n 1) 36; Mills (n 1) 200.

that the same offence can be regulated by the laws of the State where the offence started but also by the laws of the State where it produced its effects, according to the subjective and objective territorial jurisdiction principles which will be examined below.[12] Although concurring exercises of jurisdiction are accepted in international law, these might become problematic especially in the online environment, as Chapters 2 and 3 have shown.[13] In this regard, for example, the Group of International Experts who produced the Tallinn Manual 2.0 on the international law rules applicable to cyber operations in peacetime recognised that

> 'cyber activities pose a number of challenges to the rational and equitable exercise of jurisdiction. […] These factors could lead any number of States to attempt to assert different types of jurisdiction over particular cyber activities, thereby generating confusion and friction between States. […] Hence, with regard to cyber activities, international cooperation in law enforcement is especially important'.[14]

Having dealt with some general considerations regarding the concept of State jurisdiction in public international law, the following section proceeds to look at specific international law rules regarding territorial and extraterritorial State jurisdiction.

4.2.1 Territorial Jurisdiction

In the *Lotus* case, one of the most quoted cases regarding international law jurisdictional norms, the judges of the Permanent Court of International Justice (PCIJ) stated that "jurisdiction is certainly territorial".[15] As this statement suggests, the territorial principle is one of the main jurisdictional principles according to international law.[16] In regard to prescriptive jurisdiction, the territorial principle establishes that in order for a State to apply its laws to acts or subjects there must be a territorial connection between that State and the acts or subjects.[17] It follows that according to the territorial principle a

---

[12] Mills (n 1) 199-200.
[13] See Chapters 2 and 3 for an analysis of the freedom of expression implications of the access-based jurisdictional approach and of the extraterritorial application of domestic laws to regulate online content.
[14] Michael N. Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 54, [15]. See Chapter 5 Section 5.2 for a discussion of the Tallinn Manual 2.0 and the international law rules applicable to cyber operations in peacetime.
[15] *The Case of S.S Lotus* (n 5) 18.
[16] Mills (n 1) 197; Uerpmann-Wittzack (n 10) p. 1253-1254; Pardis Moslemzadeh Therani and Nazura Abdul Manap 'A rational jurisdiction for cyberterrorism' (2013) 29 Com. L & S Rev 689, 690; Joanna Kulesza, 'Internet Governance and the Jurisdiction of States. Justifications for the need of an international regulation of cyberspace' (2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1445452> accessed 07 October 2019, 7.
[17] Mills (n 1) 196-197; Uerpmann-Wittzack (n 10) 1253-1254; Therani and Manap (n 16) 690; Kulesza (n 16) 7; Rabinovitch (n 8) 504; Kenneth C. Randall 'Universal Jurisdiction Under International Law' (1988) 66 Tex L Rev 785, 787.

State can exercise prescriptive jurisdiction primarily on its territory and on people located within its borders.

The existence of a territorial connection between a State and a given matter can however be interpreted more or less loosely. For example, there are acts that present a territorial connection with more than one State, such as cross-border acts. In the field of international criminal law, in order for a State to exercise jurisdiction over a cross-border offence, it is sufficient that at least one of the constitutive elements of that offence takes place within the State's territory.[18] The constitutive elements approach to establishing jurisdiction is linked to two jurisdictional heads which are considered to be extensions of the territorial principle. In particular, according to the objective territorial principle a State can exercise jurisdiction over offences that started abroad but were completed within its territory. Conversely, according to the subjective territorial principle, a State can exercise jurisdiction if the offence started on its territory but was completed abroad.[19]

One of the critiques that have been moved to the constitutive elements approach of international criminal law is that it is problematic for public international law because the constitutive elements of an offence are defined by domestic rather than international law.[20] However, both the objective and subjective territorial jurisdictional principles are part of conventional international law, since they are contained in two conventions, the Convention for the Suppression of Counterfeited Currency and the Convention for the Suppression of the Illicit Traffic of Drugs.[21] Notwithstanding this, Ryngaert observes that while these two jurisdictional approaches are undoubtedly valid in the field of international criminal law, 'international law seems […] to have satisfied itself with requiring that either the criminal act or its effects have taken place within a State's territory for the State to legitimately exercise territorial jurisdiction'.[22]

The requirement that the effects of an act take place within a State's territory in order for that State to exercise jurisdiction over the act is a defining characteristic of the effects doctrine. This doctrine was developed and applied by US Courts in the application of US anti-trust regulations and was mainly concerned with adverse economic effects felt within US territory.[23] More specifically, according to this doctrine, the US can exercise jurisdiction over cartel arrangements that did not happen on its territory but whose adverse

[18] Cedric Ryngaert, *Jurisdiction in International Law* (2nd, Oxford University Press 2015) 78.
[19] Ryngaert 2015 (n 18) 78-79; Mills (n 1) 196; Therani and Manap (n 16) 690; Rabinovitch (n 8) 504.
[20] Ryngaert 2015 (n 18) 78.
[21] ibid.
[22] ibid.
[23] Mika Hayashi, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace' (2006) 6 In.Law 284, 288.

economic effects were felt there. The difference between the objective territorial principle and the effects doctrine is that the first requires a territorial connection between the act and the State whereas the second does not require this connection at all, since this principle is based purely on adverse effects being felt within the State exercising jurisdiction.[24]

The effects doctrine can be described as 'a further extension of the territorial principle', and, according to the Tallinn Manual 2.0 on the rules of international law applicable to cyberoperations, this doctrine is part of customary international law.[25] However, the application of this theory poses some problems.[26] The main difficulty associated with it is that the definition of what constitutes an adverse effect is left to each State that claims jurisdiction. In other words, there is no international agreement on what constitutes an adverse effect and on how to ascertain when an act produces adverse effects within a given State if those effects are non-physical. The same Tallinn Manual 2.0, for example, has recognised that the conditions according to which this doctrine could be applied are not fully settled in international law, and that therefore this doctrine remains in some ways controversial. Besides, according to the Manual, the unqualified application of the effects doctrine has been a cause of controversy among States.[27] Arguably, the unqualified use of the effects doctrine equates to exercising universal jurisdiction. This is because it allows States to exercise jurisdiction over an act that has no connection with those States other than its non-physical harmful effects. However, unlike universal jurisdiction, in the effects doctrine's case the acts over which States exercise jurisdiction are not international crimes. This means that, unlike international crimes, those acts are not deemed by the international community as so egregious to justify an exercise of jurisdiction in absence of any of the other recognised jurisdictional heads. Ultimately, as observed by some commentators, the effects doctrine removes the limits to the exercise of extraterritorial jurisdiction that were introduced thanks to the objective territorial principle.[28]

Both the objective territorial principle and the effects doctrine are strictly linked to extraterritorial jurisdiction, which is examined below.

---

[24] Hayashi (n 23) 288-289; Thomas Schultz, 'Carving up the Internet: jurisdiction, legal orders, and the private/public international law interface' (2008) 19(4) EJIL 75, 812.
[25] See respectively Hayashi (n 23) 288 and Schmitt (n 14) 57-58, [11]. The Tallinn Manual 2.0 explicitly refers to the application of the effects doctrine to cyber operations. See Chapter 5 section 5.2 for a discussion of the international law rules related to cyberoperations.
[26] Hayashi (n 23) 288; Schultz (n 24) 812-813.
[27] Schmitt (n 14) 57, [11].
[28] Hayashi (n 23) 289.

4.2.2 Extraterritorial Jurisdiction

The term extraterritorial jurisdiction indicates jurisdiction exercised by a State over acts that happen outside the territory of that State and that therefore do not present a territorial connection with it. The term extraterritorial is, however, controversial. Some authors have observed that this term often has a negative connotation, since it is used as a synonym for unlawful exercise of jurisdiction or is often not accurate.[29] Indeed, the term has sometimes been associated to acts that do have a territorial connection with the State, although not an exclusive one, such as acts that happened abroad but produced negative effects within the territory of another State and could therefore in principle be justified by the objective territorial criterion.[30] It is therefore preferable to use the term extraterritorial jurisdiction to refer to acts that are '"not exclusively territorial"' or to assertions of jurisdiction over acts that happened abroad.[31]

The principles of extraterritorial jurisdiction are the personality, protective and universal jurisdiction principles.

Jurisdiction based on the personality principle is centred on nationality and therefore on the personal relation between the State and the individual over which jurisdiction is exercised.[32] According to the personality principle, a State can exercise jurisdiction over its nationals regardless of where in the world they are located.[33] In this regard, it has been observed that 'state authority does not end at the national border but attaches to people and effectively travels with them'.[34] This is a further example of the fact that, as mentioned above, international law does accept concurring exercises of jurisdiction.[35]

The personality principle is divided into active and passive personality. The active personality principle is a well-established international law jurisdictional principle that is especially relevant in the field of international criminal law. This principle gives States the authority to exercise jurisdiction over their nationals if they have committed a crime, regardless of where the crime was committed.[36] The active personality principle is also used in international family law as well as in the domestic tax law of some States.[37]

As to the passive personality principle, it establishes that States have jurisdiction over their nationals if they are victims of crimes, irrespective of where the crimes were

[29] Ryngaert 2015 (n 18) 7-8.
[30] ibid.
[31] ibid 8.
[32] Mills (n 1) 198; Ryngaert 2015 (n 18) 104.
[33] Ryngaert 2015 (n 18) 104; Mills (n 1) 198; Randall (n 17) 787.
[34] Mills (n 1) 198.
[35] ibid 199-200.
[36] Ryngaert 2015 (n 18) 104-105; Rabinovitch (n 8) 504.
[37] Ryngaert 2015 (n 18) 106-107; Kulesza (n 16) 8.

committed.[38] Unlike the active personality principle, the status of passive personality under international law is controversial. While the principle is accepted with regard to acts of terrorism or crimes committed against foreign officials, the absence of an international convention makes it difficult to establish whether the principle is legal according to international law.[39] As observed by some authors, however, State practice and the absence of international protest against the application of the principle seem to suggest that it might in fact be legal, although its use should be limited to the most serious crimes only.[40]

Another basis for the exercise of extraterritorial jurisdiction is the protective principle. According to the Restatement of the Law (Third) The Foreign Relations of the United States, the protective principle establishes that States can exercise jurisdiction over acts committed abroad by perpetrators that are not their nationals if these acts are directed against the State security or a limited class of State interests, such as the State's right to political independence.[41] The rationale behind the existence of this principle is that the acts in question might be perfectly legal in the State where they are carried out. Therefore, the protective principle would allow to fill a jurisdictional gap by allowing the State whose sovereignty or independence is threatened to exercise jurisdiction over the foreign acts.[42]

Jurisdiction based on the protective principle can be exercised even if there is no actual harm suffered by the targeted State, for example if people conspire to commit a crime against the security of a foreign State, but their plan is stopped before its effects are felt within the targeted State.[43] This point distinguishes the protective principle from the

[38] Ryngaert 2015 (n 18) 110; Mills (n 1) 198; Rabinovitch (n 8) 504; Randall (n 17) 787.
[39] Mills (n 1) 199; Ryngaert 2015 (n 18) 110-111; Kulesza (n 16) 9.
[40] Ryngaert 2015 (n 18) 112.
[41] 'Subject to § 403, a state has jurisdiction to prescribe law with respect to (1) (a) conduct that, wholly or in substantial part, takes place within its territory; (b) the status of persons, or interests in things, present within its territory; (c) conduct outside its territory that has or is intended to have substantial effect within its territory; (2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and (3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests', Sarah H Cleveland and Paul B Stephan (ed), *Restatement of the Law (Third) The Foreign Relations Law of the United States* (1st edn, American Law Institute Publishers 1987), section 402. See also Kulesza (n 16) 9-10; Rabinovitch (n 8) 505; Randall (n 17) 787-788.
[42] Ryngaert 2015 (n 18) 114; MR Garcia Mora, 'Criminal Jurisdiction over Foreigners for Treason and Offences Against the Safety of the State Committed Upon Foreign Territory' (1958) 19 U Pitt L Rev 576, 587 (as cited in C Ryngaert, *Jurisdiction in International Law* (2nd, Oxford University Press 2015) 114).
[43] 'Two principles of extraterritorial jurisdiction recognized under international law are applicable here: the effects or "objective territoriality" principle and the "protective" principle […] Furthermore, although cases are rare, international law permits jurisdiction under these theories even if the act or conspiracy at issue is thwarted before ill effects are actually felt in the target state […] For that matter, jurisdiction may be proper even if no acts were committed in that state, especially where the statute does not require proof of an overt act' *United States v Evans et all* 1987 SDNY 974, 980-981. See also Ryngaert 2015 (n 18) 114.

objective territorial principle and the effects doctrine, which conversely presuppose the presence of adverse effects being felt within the targeted State.[44]

As to the status of the protective principle under international law, its legality seems uncontested, and many affirm that this is indeed a well-established international law principle.[45] However, there are controversies regarding the justification for the principle being States' self-defence, since unlike self-defence, the protective principle can be applied after an act has occurred and even in the absence of an armed attack.[46] In addition, due to the lack of an international convention regarding the protective principle, there is no international agreement regarding which crimes justify its adoption. This could be problematic since States could abuse the principle as they are free to determine what constitutes an act against their sovereignty or political independence. However, the lack of international protests following the adoption of the protective principle and the fact that it has been used rarely (usually in regard to offenses such as drug trafficking or forgery of foreign currency) support its uncontroversial nature.[47]

Universal jurisdiction is the last international law principle related to the exercise of extraterritorial jurisdiction. Universal jurisdiction is usually exercised in the field of international criminal law in regard to the most serious international crimes, such as piracy, crimes against humanity and genocide.[48] The key characteristic of this principle is the absence of a nexus connecting the State exercising jurisdiction and the act upon which jurisdiction is exercised.[49] Indeed, the universal jurisdiction principle allows States to exercise jurisdiction over acts that did not happen within their territory and whose perpetrators or victims are not their nationals. The most quoted rationale for the exercise of the universal jurisdiction principle is the nature of the crimes to which this principle applies that is so egregious that their perpetrators are considered as *hostis humani generis* who have violated *erga omnes* obligations. Therefore, every State in the international community has the right to prosecute those crimes.[50]

---

[44] Ryngaert 2015 (n 18) 114.

[45] Ryngaert 2015 (n 18) 114; Kulesza (n 16) 10; Eric Talbot Jensen, 'The Tallinn Manual 2.0: Insights and Highlights' (2017), 48 Geo J Int'l L 735, 748**.** Talbot Jensen refers to the international law jurisdictional principles that apply to cyber activities committed in other States and includes the protective principle as a legitimate basis for the exercise of jurisdiction under international law.

[46] Ryngaert 2015 (n 18) 115. Ryngaert refers to Article 51 of the UN Charter, which establishes that States' right of individual or collective self-defence is indeed linked to the occurrence of an armed attack.

[47] ibid 116-117.

[48] Therani and Manap (n 16) 694; Kulesza (n 16) 10; Ryngaert 2015 (n 18) 127; Rabinovitch (n 8) 505.

[49] Ryngaert 2015 (n 18) 126; Rabinovitch (n 8) 505; Kulesza (n 16) 10; Therani and Manap (n 16) 695.

[50] Ryngaert 2015 (n 18) 127. Ryngaert at 126-127 also mentions two other rationales for the exercise of universal jurisdiction, namely that the crimes committed pose a danger to all States and therefore all States have a common interest in prosecuting those crimes and that the mere presence of the perpetrator on the territory of a State is a threat to that State since the perpetrator could reoffend; Ademola Abass *International Law* (1st, Oxford University Press 2012) 539; Vaughan Lowe 'Jurisdiction' in Malcom D. Evans (ed)

The only condition for a State to exercise universal jurisdiction is that the perpetrator of the act is within its territory. However, this point is controversial, as there is an ongoing debate regarding whether international law allows for universal jurisdiction to be exercised even without the perpetrator of the act being present on the territory of the State exercising jurisdiction i.e. universal jurisdiction *in absentia*.[51] The ICJ had an opportunity to clarify this issue in 2000 in the *Case Concerning the Arrest Warrant of 11 April 2000* where Belgium issued an arrest warrant *in absentia* against the Minister of Foreign Affairs of the Democratic Republic of Congo (DRC) for grave breaches of the Geneva Conventions 1949 and crimes against humanity committed in Congo.[52] However, in its final submission the DRC dropped the claim according to which international law does not allow for the exercise of universal jurisdiction *in absentia*. Therefore, the ICJ did not examine this issue in its decision, unlike some judges who did so in their dissenting or separate opinions. However, there was no uniformity of views on this point. Judge Van den Wyngaert found that international law does allow for the exercise of universal jurisdiction *in absentia*, while judges Higgins, Kooijmans and Buergenthal agreed but submitted the exercise of jurisdiction *in absentia* to specific conditions.[53] Finally, judges Guillaume, Ranjeva, Rezek and Bula-Bula found that customary international law does require the presence of the perpetrator within the territory of the State for that State to exercise universal jurisdiction.[54] Notwithstanding the variety of views expressed, it does not appear that there is enough uniformity of State practice to conclude that in fact a norm of customary international law exists either prohibiting or allowing the exercise of universal jurisdiction *in absentia*. The majority of the States that have exercised universal jurisdiction according to international conventions in the form of the *aut dedere aut judicare principle* or translated it into their domestic laws have done so provided that the perpetrator was on their territory. However, there is not enough data showing that this State practice is accompanied by the related *opinio juris*.[55] Therefore, this issue remains

International Law (1st, Oxford University Press 2003) 343. As a rationale for the exercise of universal jurisdiction, Lowe also mentions that fact that there are some crimes that, although not egregious, are committed in a location that cannot be linked to any State, such as piracy which happens on the high seas. Therefore, universal jurisdiction is needed because otherwise those crimes would go unpunished.

[51] Ryngaert 2015 (n 18) 133-135; Rabinovitch (n 8).

[52] Rabinovitch (n 8) 502-504.

[53] '(1) all applicable immunities are respected; (2) the national State of the accused person is first given the opportunity to act upon the charges alleged; (3) the charges are laid by a prosecutor or *juge d'instruction* who acts in full independence, without links to or control by the government of the State; and (4) it is reserved for only the most heinous international crimes' Arrest Warrant, [2002] I.C.J. at 80-81, [20021 41 I.L.M. at 586 (joint separate opinion of Higgins, J. Kooijmans, J. & Buergenthal, J.) (as cited in Rabinovitch (n 8) 504).

[54] Rabinovitch (n 8) 504.

[55] Rabinovitch (n 8) 507; Ryngaert 2015 (n 18) 134.

open and will be clarified once a more uniform State practice emerges in one direction or the other.

As to the status of universal jurisdiction under international law, some authors believe that it is a norm of customary international law.[56] However, this status is controversial, since State practice regarding the exercise of universal jurisdiction is not uniform.[57] Even more relevantly, the modality of application of universal jurisdiction is unclear. For example, it is uncertain what crimes are subjected to universal jurisdiction and whether there are any restrictions that limit the application of this principle to reduce international conflict.[58]

Universal jurisdiction in criminal law can be differentiated from other exercises of jurisdiction such as vicarious jurisdiction and the *aut dedere aut judicare* principle. Vicarious or representational jurisdiction allows States to act as representatives of the State where the unlawful act was committed and therefore to exercise jurisdiction over crimes committed abroad by foreign perpetrators. Vicarious jurisdiction has rarely been exercised and is usually applied to crimes that are less serious than international crimes.[59] This jurisdictional principle is different from universal jurisdiction also because specific conditions apply in order for it to be carried out: that the perpetrator is on the territory of the State exercising jurisdiction, that the unlawful act is an offence both in the territorial State and in the forum State and that extradition is not possible for reasons that are not related to the nature of the crime.[60] In addition, the rationale of vicarious jurisdiction is different from that of universal jurisdiction, since, as some authors have pointed out, the forum State exercises jurisdiction to protect the interests of the territorial State rather than those of the international community.[61] However, this point is controversial as, rather than an autonomous jurisdictional head, vicarious jurisdiction has also been interpreted as an extension of universal jurisdiction or of the *aut dedere aut judicare* principle.[62]

The *aut dedere aut judicare* principle is a norm of conventional international law. It establishes that States under whose jurisdiction the perpetrators of the offences defined in the conventions are found have the obligation to either extradite or prosecute them.[63] More specifically, as clarified by the ICJ with regard to the crime of torture, the obligation

[56] Therani and Manap (n 16) 695.
[57] Ryngaert 2015 (n 18) 132.
[58] Ryngaert 2015 (n 18) 133; Abass (n 50) 542.
[59] Ryngaert 2015 (n 18) 121. In particular, Ryngaert refers to § 7(2), 2° of the German StGB (as cited in Ryngaert 2015 (n 18) 122) and to Article 113-8-1, § 1 French CP (as cited in Ryngaert 2015 (n 18) 123).
[60] ibid 121.
[61] ibid 122.
[62] ibid 122-123.
[63] Ryngaert 2015 (n 18) 123; Lowe (n 50) 344.

for the States party to the UN Torture Convention is to prosecute the perpetrator of the crime, whereas extradition is to be considered as an option rather than an obligation.[64] The *aut dedere aut judicare* principle is different from universal jurisdiction since it applies only between the States that are party to the conventions rather than to all the States in the international community.[65] However, especially in regard to terrorism there have been cases where States have applied the *aut dedere aut judicare* principle to nationals of States that were not party to the related anti-terrorism conventions.[66] Interestingly, these assertions of jurisdiction have not raised international protest on the part of the States not party to the conventions.[67] Therefore, some have argued that if the absence of protest continues, in time the *aut dedere aut judicare* principle with regard to terrorism could develop into a norm of customary international law.[68]

Finally, the last form of universal jurisdiction that should be discussed is universal tort jurisdiction. This is related to universal jurisdiction that is exercised by States in civil rather than criminal proceedings. In particular, domestic courts exercise universal tort jurisdiction when they hear claims for damages related to gross violations of international law that have no jurisdictional link with the State exercising jurisdiction.[69] This form of jurisdiction is usually applied with regard to human rights violations and, similarly to universal criminal jurisdiction, the rationale for its application is the egregious nature of the unlawful act.[70]

Universal civil jurisdiction has been applied mainly in the US where domestic courts have heard various civil cases with no jurisdictional connection to the US based on the Alien Tort Statute.[71] However, whether a pure form of universal civil jurisdiction currently exists – jurisdiction over 'foreign cubed' cases, i.e. cases where the violation happened abroad, and both the claimant and the defendant are foreign - is debatable. Indeed, the US Supreme Court in the 2013 *Kiobel* case did place limits on the application of the Alien Tort Statute to 'foreign cubed' cases, saying that a case needs to 'touch and

---

[64] ICJ, *Questions Concerning the Obligation to Prosecute or Extradite (Belgium v Senegal)*, Judgement of 20 July 2012, §§ 92-5 (as cited in Ryngaert 2015 (n 18) 125).
[65] Ryngaert 2015 (n 18) 124; Lowe (n 50) 344.
[66] Ryngaert 2015 (n 18) 124-125. In particular, Ryngaert refers to federal courts in the United States that have extended the application of the International Convention Against the Taking of Hostages and the Convention for the Suppression of Unlawful Seizure of Aircraft to citizens of non-State parties to those Conventions.
[67] Ryngaert 2015 (n 18) 125; Lowe (n 50) 344.
[68] Ryngaert 2015 (n 18) 125.
[69] ibid 135.
[70] ibid.
[71] Legal Information Institute 'Alien Tort Statute' *Cornell Law School* <https://www.law.cornell.edu/wex/alien_tort_statute> accessed 11 August 2020; See also Paul David Mora 'The Alien Tort Statute after Kiobel: the Possibility for Unlawful Assertions of Universal Civil Jurisdiciton Still Remains' (2014) 63 ICLQ 699, 699-700.

concern' the US to be tried there.[72] In other words, it does appear that in order for US courts to exercise jurisdiction based on the Alien Tort Statute a strong connection with the United States is needed.

As to the status of universal civil jurisdiction under international law, it is unclear whether this form of jurisdiction reflects customary international law. Indeed, while only few States have exercised this form of jurisdiction, there is no sufficient State practice that shows that this is due to other States opposing to universal civil jurisdiction on legal grounds.[73]

The doctrine of *forum necessitatis* is similar to universal civil jurisdiction, although this doctrine is part of private international law.[74] It establishes that a State can exercise jurisdiction over a foreign case if it is legally or practically impossible or unreasonable to bring the case before the forum which has stronger connections with it.[75] The *forum necessitatis* doctrine has been applied in some countries in Europe (including Switzerland, Holland, Belgium and Netherlands) and Canada, whereas it does not exist as a separate basis for the exercise of jurisdiction in the United States.[76] Similarly to universal civil jurisdiction, the status of the *forum necessitatis* doctrine under international law is unclear. The courts that recur to this approach believe that this is in line with customary international law. However, due to scarcity of state practice it is not possible to conclude that this is the case.

Having examined the international law regime related to State jurisdiction, the next section will look into how this concept has been defined in human rights law.

4.3 The concept of State jurisdiction in human rights law

In human rights law, the jurisdictional clauses contained in human rights conventions refer to the jurisdiction of the States parties to the conventions rather than the Courts whereby established. However, these two concepts are strictly related, since a Court will only have jurisdiction over a given act if that act was committed within the jurisdiction of the States parties or can be attributable to them. This also means that a State will only be bound to the provisions of human rights conventions if an act falls within its jurisdiction. Therefore, State jurisdiction in human rights law can be seen as a *sine qua*

[72] 'even where the claims touch and concern the territory of the United States, they must do so with sufficient force to displace the presumption against extraterritorial application' *Kiobel v Royal Dutch Petroleum Co.* 569 U.S. 108 (2013) Opinion of the Court, 14; see also Ryngaert 2015 (n 18) 136, 139.
[73] Ryngaert 2015 (n 18) 136-137.
[74] ibid 139-140.
[75] ibid 139.
[76] ibid 139-140.

non condition for the application of the conventions.[77] It follows that, although the jurisdictional issues are mostly dealt with at the admissibility stage of a proceeding, jurisdiction in human rights law is not a mere rule of procedure of the Courts established by the treaties since it impacts on the substantive rights contained in the human rights conventions.[78]

The meaning of jurisdiction in human rights law is different from the meaning of jurisdiction in public international law. While in public international law jurisdiction is related to the legality of State action, in human rights law it can be seen as a factual test or power.[79] The public international law rules of jurisdiction define the criteria according to which a State is entitled to regulate a given matter without infringing the sovereignty of other States. In contrast, according to human rights law a State has jurisdiction over a territory or a person when it exercises effective overall control over that territory or authority over that person, regardless of whether that exercise of jurisdiction is legal according to international law.[80] The *Loizidou* case before the ECtHR provides an example of this point. In that case, the Court found that Turkey exercised jurisdiction over the Cypriot territory because Turkish troops had occupied that territory and therefore had effective overall control over it, regardless of whether the Turkish military occupation was legal according to international law.[81] In this regard, as Wilde observes, 'the notion that human rights obligations do not apply if the action in question is not itself lawful is perverse'.[82] Indeed, it would be a paradox if human rights treaties would not apply because their violation was committed as a result of an act that is considered unlawful according to international law. As Milanović notes, not all the acts committed by States are an expression of States' legal authority, as States can, for example, kill or torture without passing any domestic law that authorizes them to do so, in other words, without exercising prescriptive jurisdiction.[83] Therefore, equating jurisdiction in human rights law to jurisdiction in international law would lead to the absurd result that acts such as State

[77] Directorate of the Jurisconsult, Guide on Article 1 of the Convention – Obligation to respect human rights – Concepts of "jurisdiction" and Imputability, 31 December 2019, [1]. See also Milanović, 'From Compromise to Principle' (n 1) 416.
[78] Milanović 'From Compromise to Principle' (n 1) 416-417.
[79] ibid 417; Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 39-41; R Wilde The "Jurisdiction" Test (n 1) 508.
[80] Milanović 'From Compromise to Principle' (n 1) 417-429; Wilde 'The "Jurisdiction" Test' (n 1) 507-508.
[81] *Loizidou v. Turkey* App no 15318/89 (ECHR, 18 December 1996) para 52.
[82] Wilde 'The "Jurisdiction" Test' (n 1) 514; Milanović, 'From Compromise to Principle' (n 1) 422-426.
[83] Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 29.

torture would not be considered as an exercise of State jurisdiction even when committed on the domestic territory unless there is a domestic law that authorizes torture.[84]

Notwithstanding the difference between the meaning of jurisdiction in public international law and the meaning of jurisdiction in human rights law, the ECtHR affirmed in *Banković* that these two concepts coincide. More specifically, the Court implied that the meaning of jurisdiction according to the ECHR reflects that of public international law.[85] This view has attracted many critiques, since it contrasts with previous case-law from the ECtHR itself and with the interpretation of jurisdiction of other human rights bodies. Indeed, before *Banković* the European Commission or the European Court of Human Rights had never based the interpretation of Article 1 of the Convention on the international law rules on jurisdiction.[86] In addition, the UN Human Rights Committee (HRC) in its General Comment No.31 did clarify that the obligations contained in the ICCPR apply to anyone within the power or effective control of a State party to the Covenant, regardless of the legality of that exercise of power.[87]

Finally, while the rules regulating the exercise of State jurisdiction outside States' domestic territory are controversial and still evolving, there is no doubt that in human rights law as well as in public international law, States exercise jurisdiction when they act within their territory. Some human rights courts such as the ECtHR and the Inter-American Court of Human Rights (IACtHR), for example, stated on numerous occasions that jurisdiction according to Article 1 of the ECHR and to Article 1.1. of the American Convention on Human Rights (ACHR) is primarily territorial, while extraterritorial jurisdiction is exceptional.[88] It is necessary then to examine the debate related to the nature of extraterritorial jurisdiction in human rights law together with the concept of legal space of human rights conventions.

---

[84] ibid 29-30.

[85] *Banković and Others v. Belgium and Others* App no 52207/99 (ECtHR, 12 December 2001) paras 59-61.

[86] Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 27.

[87] HRC General Comment No. 31 (26 May 2004) CCPR/C/21/Rev.1/Add. 13, [10]. See also Wilde 'The "Jurisdiction" Test' (n 1) 513-514; Milanović, 'From Compromise to Principle' (n 1) 417-419, 422-426.

[88] Guide on Article 1 of the Convention 31 December 2019 (n 77) [2], [11]. The focus on the territorial aspect of jurisdiction in the ECHR is also reflected on the draft of article 1 of the ECHR prepared by the Committee on Legal and Administrative Affairs of the Consultative Assembly of the Council of Europe. The initial draft of the article stated that the contracting parties were bound by the obligations contained in the Convention with regard to anyone residing on their territory. However, the word 'residing' was later replaced by the expression 'within their jurisdiction' to include all those who were on the territory of the contracting parties, regardless of whether their presence could legally amount to residence. See also *Banković* (n 85) para 61; *Soering v. The United Kingdom* App no 14038/88 (ECtHR, 7 July 1989) para 86; *Ilaşcu and Others v. Moldova and Russia* App no 48787/99 (ECtHR, 8 July 2004) para 312; *Al-Skeini and Others V. The United Kingdom* App no 55721/07 (ECtHR, 7 July 2011) para 131; *Medio Ambiente y Derechos Humanos*, Advisory Opinion OC-23/17 Inter-American Court of Human Rights (15 November 2017), [104 (d)].

4.3.1 Extraterritorial Jurisdiction in Human Rights Law

Human rights conventions apply extraterritorially as well as within the territory of the Member states, as stated on various occasions by the ICJ and by many human rights courts and bodies with regard to the ECHR, the ICCPR, the ACHR, the Convention Against Torture (CAT), the Convention on the Rights of the Child (CRC), and the African Charter on Human and Peoples' Rights (ACHPR).[89] Therefore, as a matter of principle, States are liable for violations of the human rights conventions to which they are a party even when these violations happen outside their domestic borders. In this regard, some human rights bodies have affirmed that extraterritorial jurisdiction in human rights law is exceptional and its exercise must be interpreted restrictively[90] and requires special justifications.[91] The ECtHR in *Catan and Others v. The Republic of Moldova and Russia*, for example, stated that

> '[j]urisdiction is presumed to be exercised normally throughout the State's territory […]. Conversely, acts of the Contracting States performed, or producing effects, outside their territories can constitute an exercise of jurisdiction within the meaning of Article 1 only in exceptional cases'.[92]

However, it is not clear whether the exceptional nature of extraterritorial jurisdiction in human rights law is an inherent and defining characteristic of this concept in this area of law, as the ECtHR and the IACtHR have stated, or whether it could simply be a matter of

---

[89] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Reports 136, [109]; *Loizidou v. Turkey* (n 81) para 52; *Cyprus v Turkey* App no 25781/94 (ECtHR, 10 May 2001) para 77; *Issa and Others v. Turkey* App no 31821/96 (ECtHR, 30 March 2005) para 71; *Banković and Others v. Belgium and Others* (n 85) paras 70-71; *Solomou and Others v Turkey* App no 36832/97 (ECtHR, 24 September 2008) paras 44–45; *Andreou v Turkey* Merits App no 45653/99 (ECtHR, 27 January 2010), para 25; *Coard at al v US*, Inter-American Commission on Human Rights Report N. 109/99 - Case 10.951, [37]; Committee Against Torture Consideration of Reports Submitted by States Parties under Article 19 of the Convention, Conclusions and Recommendations: United States of America (25 July 2006) UN Doc. CAT/C/USA/CO/2, [15]; Committee Against Torture General Comment No. 2 Implementation of Article 2 by States Parties (24 January 2008) UN doc. CAT/C/GC/2, [16]; Committee On The Rights Of The Child Thirty-first session Consideration of Reports Submitted by States Parties under Article 44 of the Convention Concluding observations: Israel (9 October 2002) CRC/C/15/Ad 195, [2]; *Democratic Republic of the Congo v. Burundi, Rwanda and Uganda* African Commission on Human and Peoples' Rights, Communication 227/99 (May 2003), [76], [79]-[81], [83]-[84]. See also M Milanović, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv Int'l L J 81, 99-101 with reference to the ICCPR and the ECHR and R Wilde 'Human Rights Beyond Borders at the World Court: the Significance of the International Court of Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties' (2013) 12(3) CJIL 639, 664-667.

[90] *Medio Ambiente y Derechos Humanos* (n 88) [104 (d)].

[91] *Banković and Others v. Belgium and Others* (n 85) para 61; *Issa and Others v. Turkey* (n 89) para 68.

[92] *Catan and Others v. The Republic of Moldova and Russia* App no 43370/04, 8252/05 and 18454/06 (ECtHR, 19 October 2012) para 104. See also *Banković and Others v. Belgium and Others* (n 85) para 67; and *Al-Skeini and Others v. The United Kingdom* (n 88) para 131.

fact.[93] The ICJ, for example, explained the exceptional nature of extraterritorial jurisdiction according to the ICCPR by referring to the fact that States act less frequently outside their national borders than they do domestically.[94] The difference between these two interpretations is that the view of ECtHR and of the IACtHR promotes a more restrictive approach to the definition of extraterritorial jurisdiction in human rights law. According to this view, even if a State acts outside its territory as a matter of fact, that action could still not be considered as an exercise of extraterritorial jurisdiction as a matter of law since extraterritorial jurisdiction according to the ECHR and the ACHR is exceptional and only happens in a limited number of circumstances.[95] For some time, the ECtHR was the only human rights Court to maintain the '*de jure* exceptionalism' of extraterritorial jurisdiction in human rights law.[96] Other courts and bodies, such as the HRC and the Inter-American Commission of Human Rights had never mentioned this theory. This changed recently, when, as mentioned above, the IACtHR issued its advisory opinion on the meaning of extraterritorial jurisdiction with regard to the right to life and personal integrity. The Court statement that '[e]l ejercicio de la jurisdicción bajo el artículo 1.1 de la Convención Americana, fuera del territorio de un Estado, es una situación excepcional que debe analizarse en cada caso concreto y de manera restrictiva' confirms the 'de jure exceptionalism'[97] interpretation of the ECtHR.[98] It remains to be seen whether other human rights courts will follow this approach in the future.

Finally, strictly linked to the theme of the exceptional nature of extraterritorial jurisdiction is the concept of legal space of human rights conventions. This concept was introduced with regard to the ECHR by the ECtHR in the *Bankovic* case, when the Court stated that

> 'the Convention is a multi-lateral treaty operating […] in an essentially regional context and notably in the legal space (*espace juridique*) of the Contracting States. […] The Convention was not designed to be applied throughout the world, even in respect of the conduct of Contracting States. Accordingly, the desirability of avoiding a gap or vacuum in human rights' protection has so far been relied on by the Court in

[93] Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 669-670; Wilde 'The "Jurisdiction" Test' (n 1) 514-515.
[94] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (n 89) [109]. See also Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 669-670; Wilde 'The "Jurisdiction" Test' (n 1) 514-515.
[95] Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 669-670; Wilde 'The "Jurisdiction" Test' (n 1) 514-515.
[96] Wilde 'The "Jurisdiction" Test' (n 1) 514; Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 670.
[97] Wilde 'The "Jurisdiction" Test' (n 1) 514.
[98] 'the exercise of jurisdiction outside of the territory of the State under Article 1.1 of the American Convention is an exceptional situation that must be analysed in each specific case and in a restrictive manner' (author's translation) *Medio Ambiente y Derechos Humanos* (n 88) [104 (d)].

favour of establishing jurisdiction only when the territory in question was one that, but for the specific circumstances, would normally be covered by the Convention'.[99]

This statement affirms the regional nature of the ECHR which applies primarily within the territory of its Member States. However, it could also be interpreted as saying that, although a State might meet the criteria for the exercise of extraterritorial jurisdiction under the ECHR, the ECHR would not apply if that exercise of jurisdiction was committed outside the territory of its Member States.[100] If this idea were to be extended to all the human rights conventions, the exercise of extraterritorial jurisdiction in this area of law would be severely restricted to include only extraterritorial exercises of jurisdiction that involve States that are party to the same convention, thus leaving States free to commit human rights violations in the rest of the world.[101] However, the ECtHR itself abandoned the 'espace juridique' concept in the *Al Skeini* case, where it found that the UK had exercised jurisdiction over the Iraqi applicants notwithstanding the fact that the violation of Article 2 of the ECHR had happened in Iraq, and therefore outside the legal space of the Convention.[102] The legal space concept of jurisdiction has also been discarded by the ICJ in the *Wall* advisory opinion, where it found that Israel's obligations under the ICCPR and the CRC apply to the Palestinian Territories, which are not party to these treaties.[103]

The next section will look into the two main models of extraterritorial State jurisdiction that have been developed throughout the years by human rights courts.

4.3.2 Models of Extraterritorial Jurisdiction in Human Rights Law

As stated above, the concept of State jurisdiction in human rights law is linked to a factual exercise of power or authority by the State. More specifically, two main models of extraterritorial jurisdiction have been developed by the human rights courts: the spatial model and the personal model.

According to the spatial model, a State exercises extraterritorial jurisdiction when it exercises effective overall control over a territory located outside its domestic borders.

---

[99] *Banković and Others v. Belgium and Others* (n 85) [80].

[100] Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 671-672; C Ryngaert 'Clarifying the extraterritorial application of the European Convention on Human Rights' 2012 28(74) UJIEL 57, 58-59.

[101] Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 672.

[102] See paragraph 4.4.2 for an expanded analysis of this point. See also Ryngaert 'Clarifying the extraterritorial application of the European Convention on Human Rights' (n 100) 59.

[103] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (n 89) [109]-[113]. Wilde 'Human Rights Beyond Borders at the World Court' (n 89) 673.

This model of jurisdiction is the most supported by both the text of some human rights treaties and the jurisprudence of the related courts.[104] Indeed, some treaties such as the Convention Against Torture (CAT) explicitly refer to jurisdiction as control over territories.[105] Besides, the jurisprudence of the ECtHR, the HRC, the African Commission on Human and Peoples' Rights (AComHPR), the Inter-American Commission on Human Rights (IACommHR), the ICJ, the Committee on Economic, Social and Cultural Rights, the Committee Against Torture and the Committee on the Rights of the Child shows that this model has consistently been applied by human rights courts.[106]

The threshold for the application of the effective overall control test is high, however the level of control exercised by the States on the relevant territory does not need to equate that exercised on their domestic territory to trigger jurisdiction.[107] The acts that might be classified as effective overall control cover a wide range of activities which include, among other things, military occupying all or part of a territory, supporting an insurrection or civil war in another country and favouring or assisting the installation of a separatist regime.[108] As to the criteria that are taken into account to determine whether effective overall control exists, the ECtHR, for example, refers mainly to the number of soldiers employed by the occupying State on the territory in question and to the extent of that State's control and influence over the region exercised through its political, military or economic support for the subordinate local administration.[109]

A factor that, according to some, should have a bearing on the level of control required to trigger State jurisdiction is whether the State exercising control over a territory is required to fulfil both its positive and negative human rights obligations with respect to

---

[104] Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 128.

[105] 'Each State Party shall take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction' Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) UNTS 1465 85, art 2.1. See also Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 128.

[106] *Loizidou v. Turkey* (n 81) para 62; *Banković and Others v. Belgium and Others* (n 85) para 71; HRC Concluding observations of the Human Rights Committee Israel (18 August 1998) CCPR/C/79/Add.93 [10]; *Democratic Republic of the Congo v. Burundi, Rwanda and Uganda* (n 89) [76], [79]-[81], [83]-[84]; *Coard et al v US* (n 89), [37]; Committee on Economic, Social and Cultural Rights Concluding Observations: Israel (4 December 1998) E/C.12/1/Add.27, [8]; Committee Against Torture Conclusions and Recommendations, United Kingdom of Great Britain and Northern Ireland, Crown Dependencies and Overseas Territories (10 December 2004) CAT/C/CR/33/3, [4(b)]; Consideration of Reports Submitted by States Parties under Article 44 of the Convention Concluding observations: Israel (n 89), [2]; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (n 89) [109]-[113]; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ Report 168, [179], [216]-[217]; See also Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1), 128.

[107] Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1), 141.

[108] Directorate of the Jurisconsult, Guide on Article 1 of the Convention – Obligation to respect human rights – Concepts of "jurisdiction" and Imputability, 30 April 2019 [42].

[109] ibid [47].

that territory.[110] The ECtHR in the *Banković* case stated that the obligations contained in the ECHR could not be 'divided and tailored in accordance with the particular circumstances of the extra-territorial act in question'.[111] Therefore, according to the Court, both these obligations apply, which is an argument in favour of setting a stringent level of control to trigger State jurisdiction. However, some authors have questioned a too high threshold, since States need different levels of control to fulfil their positive and negative obligations. While States do not need a high standard of control over a territory to comply with their negative obligations not to violate human rights in that territory, they do need a higher level of control to fulfil the more demanding positive obligations to ensure or secure human rights there.[112] Nevertheless, this theory has little support from the text of the human rights treaties and the related jurisprudence.[113]

At a first glance, the application of the spatial model of jurisdiction appears straightforward as it triggers jurisdiction every time that a State exercises control over a territory. Besides, some commentators have remarked on its capacity of combining the need for universality that is at the core of the normative aspect of human rights treaties with ensuring that these can be effectively applied.[114] This is because on the one hand, this model ensures that States are bound to their human rights obligations every time that they exercise control over a territory, thus promoting the uniform application of the human rights norms. On the other, since States are in a better position to ensure the fulfilment of their human rights obligations when they have control over a territory, this model promotes the effective application of the human rights norms.

Notwithstanding its positive aspects, there are various difficulties associated with the spatial model. The main shortcoming of this model is its uncertainty with regard to how big an area must be for this model to apply. While it is clear that an extended territory qualifies as an area, such as Northern Cyprus in the *Loizidou* case, the spatial model becomes less stable and more arbitrary the more the dimensions of the area shrink. It is not clear, for example, whether a building controlled by a State in a foreign territory or a room within that building could be considered as an area for the purposes of this model.[115]

The main critique that has been moved to the spatial model is the fact that are no

[110] Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 141.
[111] *Banković and Others v. Belgium and Others* (n 85) para 75. The ECtHR was specifically referring to the positive obligations under the ECHR.
[112] Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1) 141.
[113] ibid 209-212.
[114] ibid 128, 170.
[115] ibid 128-129.

legitimate grounds for extending its application to increasingly smaller places.[116] Interestingly, when the ECtHR dealt with cases where States acted within smaller places such as military prisons in a foreign State, embassies and consulates abroad, or ships and aircrafts registered or flying the flag of that State the Court relied on the personal model of jurisdiction, i.e. jurisdiction as authority or control over individuals, rather than on the spatial model of control over a place.[117] There are, however, some exceptions, such as the cases *Medvedyev and others v. France* and *Al Saadoon and Mufdhi v the United Kingdom* where the ECtHR found that the respondent States had jurisdiction based on both power exercised by their agents over the applicants and effective control over the premises, respectively a foreign ship and a military prison in Iraq.[118] In addition, the application of the spatial model to places rather than areas was endorsed by the ECtHR in *Al Skeini*, where the Court, referring inter alia to *Medvedyev* and *Al Saadoon* stated:

'The Court does not consider that jurisdiction in the above cases arose solely from the control exercised by the Contracting State over the buildings, aircraft or ship in which the individuals were held. What is decisive in such cases is the exercise of physical power and control over the person in question'.[119]

---

[116] Milanović, for example, examined whether the spatial model as control over places can be extended to cover smaller places such as embassies and consulates abroad by virtue of the supposed special status of these places under international law. The author says that the fact that international law recognizes the exercise of extraterritorial jurisdiction in these places means that according to international law States can extend the application of their laws to these places. This fact, however, is not due to the special status of embassies and consulates under international law, as the reason why States can exercise their jurisdiction there is the consent of the territorial States. More importantly, according to Milanovic, the recognition of extraterritorial State jurisdiction in embassies and consulates abroad under international law does not provide a justification for the extension of the spatial model to smaller places in human rights law. Indeed, what matters in human rights law is whether a State exercises a factual power over areas or individuals, rather than whether it is able to apply its laws to given places, Milanović *Extraterritorial Application of Human Rights Treaties* (n 1), 156-160.

[117] Directorate of the Jurisconsult, Guide on Article 1 of the Convention – Obligation to respect human rights – Concepts of "jurisdiction" and Imputability, 31 August 2019 [30]-[32], [38]-[40]. See also Milanović *Extraterritorial Application of Human Rights Treaties* (n 1), 164-166 with regard to the cases of *Freda v Italy* App no 28780/95 (ECtHR, 24 June 1996); *Illich Sanchez Ramirez v France* App no 28780/95 (ECtHR, 24 June 1996) and *Öcalan v Turkey* App no 46221/99 (ECtHR, 12 May 2005).

[118] *Medvedyev and others v. France* App no 3394/03 (ECtHR, 29 March 2010), para 67: 'the Court considers that, as this was a case of France having exercised full and exclusive control over the Winner and its crew, at least de facto, from the time of its interception, in a continuous and uninterrupted manner until they were tried in France, the applicants were effectively within France's jurisdiction for the purposes of Article 1 of the Convention'. A*l Saadoon and Mufdhi v the United Kingdom* Admissibility Decision App no 61498/08 (ECtHR, 30 June 2009) para 88: 'The Court considers that, given the total and exclusive de facto, and subsequently also de jure, control exercised by the United Kingdom authorities over the premises in question, the individuals detained there, including the applicants, were within the United Kingdom's jurisdiction'. However, it is indicative that the Directorate of the Jurisconsult in the above-mentioned Guide on Article 1 of 31 August 2019 classifies *Medvedyev* and *Al Saadoon* as an expression of the personal model of jurisdiction rather than the spatial one. Although the Guide does not bind the Court, it is an authoritative summary of the Court's jurisprudence and reflects the Court's interpretation of the latter. See also Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1) 162-164.

[119] *Al-Skeini and others v. The United Kingdom* (n 88) para 136.

This statement and, more specifically, the use of the word solely allows room for the application of the spatial model to places.[120] Similarly to the ECtHR, the Committee Against Torture did openly endorse the spatial model as control over places and objects; however, in its jurisprudence related to acts committed by a State on a foreign ship, it adopted the personal model of jurisdiction instead.[121] Ultimately, therefore, because there are no clear grounds for applying the spatial model to places rather than territories, either this model fails to address human rights violations when applied rigidly or it collapses into the personal model of jurisdiction.[122] This is because according to a rigid application of the spatial model smaller places such as buildings in a foreign State are within the jurisdiction of that State, therefore if another State were to control the building and commit human rights violations there, that State could not be considered as exercising jurisdiction. On the other hand, to avoid this, the spatial model could be substituted by the personal one and the criterion of control over a place would be replaced by that of control over individuals, causing the spatial model to collapse into the personal model.[123] The personal model of jurisdiction is the second model developed by human rights courts. Its main characteristic is the focus on the relationship between the State and the individual, rather than the place where a human rights violation occurs.[124] The notion that a State exercises jurisdiction when it has power or control over an individual, although in contrast with the text of some human rights treaties,[125] has been endorsed in the jurisprudence of the Human Rights Committee, the Committee Against Torture, both the Inter-American Commission and the Inter-American Court of Human Rights, and the European Commission and Court of Human Rights.[126] The acts that have been classified

[120] M Milanović 'Al-Skeini and Al-Jedda in Strasbourg' (2012) 23(1) EJIL 121, 128.
[121] *J.H.A. v. Spain* (2008) CAT/C/41/D/323/2007 [8.2]. See also Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1) 167-168.
[122] For an in-depth analysis on the grounds justifying the application of the spatial model to places rather than areas see Milanović *Extraterritorial Application of Human Rights Treaties* (n 1), 151-173.
[123] ibid 171-172.
[124] *Lopez Burgos v Uruguay* (1981) U.N. Doc.CCPR/C/OP/1 at 88, [12.2]; *Celiberti de Casariego v. Uruguay* (1981) CCPR/C/13/D/56/1979 [10.2]; *Coard et al v US* (n 89) [37]. See also Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1) 176.
[125] See above note n 105.
[126] *Lopez Burgos v Uruguay* (n 124) [12.1]-[12.3]; *Celiberti de Casariego v Uruguay* (n 124) [10.1]-[10.3]; HRC General Comment No. 31 (26 May 2004) CCPR/C/21/Rev.1/Add.13 [10]; UN Committee Against Torture General Comment No. 2: Implementation of Article 2 by States Parties 24 January 2008 CAT/C/GC/2 [16]; Inter-American Commission of Human Rights, *Saldaño v Argentina*, Inter-American Commission on Human Rights Report N. 38/99, [17], [21]-[22], *Coard et al v US* (n 89) [37]; *Medio Ambiente y Derechos Humanos* (n 88) [104 (e)]; *Cyprus v Turkey* App no 6780/74 and 6950/75 (European Commission of Human Rights, 10 July 1976) paras 83, 201, 203-204, 233, 307, 525; *Issa v United Kingdom* (n 89) para 71; *Pad and Others v Turkey* App no 60167/00 (ECtHR, 28 June 2007) para 53; *Isaak and Others v Turkey*, App no 44587/98 Admissibility Decision (ECtHR, 28 September 2006) 20-21; *Solomou and Others v Turkey* (n 89) paras 45, 51; *Andreou v Turkey* Admissibility Decision (ECtHR, 03 June 2008) 9-10; *Al Skeini and Others v The United Kingdom* (n 88) paras 133-137. See also Milanović *Extraterritorial Application of Human Rights Treaties* (n 1) 175-187.

as exercise of power over an individual comprise *inter alia* acts committed by diplomatic or consular agents, the exercise of public powers on the territory of another State with the latter's consent and the use of force by State agents operating outside the related State's territory.[127]

The main objection that has been moved to the personal model of jurisdiction is that the criteria determining what constitutes an exercise of power or control are not clearly defined.[128] For this reason, it is not clear how to limit the personal model of jurisdiction, which, if applied in its broadest sense, could mean that a State exercises jurisdiction every time that it violates the human rights of an individual, regardless of where in the world the violation happens. This in turn would equate to depriving the jurisdictional threshold embedded in human rights treaties of any meaning, as a broad application of the personal model ultimately translates into having no jurisdictional threshold at all.[129] On the other hand, however, since the criteria defining what constitutes an exercise of power are not clear, limiting the application of this model to specific circumstances is challenging and could become arbitrary.[130]

A general indication on how to limit the personal model of jurisdiction could be found in the *Medvedyev* case, where the ECtHR expressed some considerations on the kind of extraterritorial acts that are not included in the definition of jurisdiction according to Article 1 of the ECHR. In *Medvedyev* the ECtHR affirmed *Banković* and stated that an 'instantaneous extraterritorial act' such as the bombing of the RTS Radio Station in Belgrade could not be considered as an exercise of jurisdiction as Article 1 does not support a '"cause and effect"' notion of jurisdiction.[131] Therefore, following *Medvedyev* and *Banković*, instantaneous acts such as killings caused by bombs dropped by the air force of foreign States cannot be characterized as exercising control over the victims of the bombing nor as exercising control over the territory targeted by the bombing. However, instantaneous acts such as killings committed by State agents have been

[127] Guide on Article 1 of the European Convention on Human Rights April 2019 (n 108) [29], [31]-[32], [37].
[128] Milanović *Extraterritorial Application of Human Rights Treaties* (n 1), 173-174.
[129] ibid 173-174, 207-208.
[130] For an analysis on various ways of limiting the personal model of jurisdiction see ibid 187-205.
[131] *Medvedyev and others v. France* (n 118) para 64. The ECtHR in *Medvedyev* was referring to the spatial model of jurisdiction, rather than the personal one. However, its considerations can be extended to the overall meaning of jurisdiction according to Article 1, and consequently, to the personal model of jurisdiction. This is because the Court justified the finding that an instantaneous extraterritorial act does not give rise to effective overall control over a territory by saying that Article 1 as a whole does not admit a cause and effect notion of jurisdiction. Therefore, it is worthwhile to examine whether, in an attempt of limiting the personal model of jurisdiction, only non-instantaneous acts can be considered as exercising power over an individual, as instantaneous acts give rise to a cause and effect notion of jurisdiction that is not contemplated in Article 1. See also Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1), 186-187, 191.

classified by the ECtHR as exercising power or control over the victims even when the victims were not in custody of the State agents, which explains why these killings can be considered as instantaneous. Indeed, the *Pad*, *Isaak*, *Solomou* and *Andreou* cases, for example, are all related to killings committed by State agents who did not have custody of the victims.[132] This fact shows that the personal model cannot be limited to non-instantaneous acts, since the Court's jurisprudence proves that instantaneous acts such as killings outside custody have in fact been considered as an exercise of power over an individual. In addition, and perhaps more importantly, limiting the personal model only to non-instantaneous acts such as killings committed while the person is in custody of State agents does not meet the universal rationale at the basis of human rights conventions and it might result in the absurd outcome of incentivising States to kill people rather than take them into custody.[133]

A difference that can, however, be traced between the *Pad*, *Isaak*, *Solomou* and *Andreou* cases and *Banković* is that the first four cases, unlike *Bankovic*, happened within the legal space of the Convention, with the exception perhaps of the *Pad* case. One might therefore wonder if the location of the violation and whether it happened within the legal space of the ECHR could be used to limit the application of the spatial model. As mentioned above, *Isaak*, *Solomou* and *Andreou* are all related to killings committed in Cyprus, and therefore ultimately within the legal space of the ECHR, which is a factor in favour of considering the legal space of the Convention as a relevant criterion. The *Pad* case, however, seems to directly contradict this even though the location of the violation in *Pad* was never determined due to disagreements between the parties as to where the victims were killed.[134] Ultimately, however, notwithstanding the unknown location, *Pad* can still be considered as disproving *Banković* regarding the legal space of the ECHR because in *Pad* the ECtHR found it irrelevant to determine where the violation had occurred to establish jurisdiction even if it was possible that the killings had happened outside the legal space

---

[132] Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1), 185-186, 191.

[133] ibid 191.

[134] *Pad and Others v Turkey* (n 126) paras 48, 51, 54-55. The applicants stated at para 48 that the killings had happened on Iranian territory and that therefore Turkey had acted extraterritorially, while the Turkish government affirmed at para 51 that these had happened on their territory which the victims illegally entered. The Court found at paras 54-55 that, since neither of the parties contested Turkey's jurisdiction, it did not matter where the act had ultimately happened in order to establish jurisdiction. According to the Court, what brought the applicants within Turkey's jurisdiction was the fact that Turkish agents had shoot them. While it is clear that the ECtHR in the *Pad* case interpreted jurisdiction as power or control over individuals, it is not clear whether this case is in fact about extraterritorial jurisdiction at all, since the location of the act has not been determined. If we take the Government's position, then the case becomes about Turkey exercising jurisdiction on its own territory which renders the case irrelevant as far as the rules on extraterritorial jurisdiction are concerned. If, on the other hand, we take the applicants' position, this becomes a case about extraterritorial jurisdiction in a place, Iran, that is not within the legal space of the ECHR.

of the Convention.[135] The same goes for the *Issa* case, where the ECtHR openly admitted that both the personal and the spatial model of jurisdiction could be applied to alleged violations that happened in Iraq, and therefore outside the legal space of the ECHR.[136] In any case, as mentioned above, the ECtHR abandoned the concept of legal space of the ECHR in *Al Skeini* where it stated that

> 'where the territory of one Convention State is occupied by the armed forces of another, the occupying State should in principle be held accountable under the Convention for breaches of human rights within the occupied territory, because to hold otherwise would be to deprive the population of that territory of the rights and freedoms hitherto enjoyed and would result in a "vacuum" of protection within the "legal space of the Convention". However, the importance of establishing the occupying State's jurisdiction in such cases does not imply, a contrario, that jurisdiction under Article 1 of the Convention can never exist outside the territory covered by the Council of Europe member States. The Court has not in its case-law applied any such restriction'.[137]

It can therefore be said that, just like the instantaneous nature of the act, the legal space of the ECHR has no bearing on whether or not an act constitutes an exercise of power according to the personal model.

However, the *Al Skeini* case introduced a new version of the personal model of jurisdiction linking the exercise of power over individuals by State agents with the exercise of public powers by the related State on the territory where the violation happens. In *Al* Skeini, the applicants were Iraqi citizens, five of whom were allegedly killed by UK troops during a patrolling operation in South East Iraq while the sixth was killed while in a detention facility controlled by the UK. The Court found that the UK had jurisdiction not simply because UK armed forces exercised power or authority over the victims, but also because the UK was exercising in that part of Iraq public powers, such as the maintenance of security, normally reserved to a sovereign government.[138] Therefore, according to *Al Skeini* a factor that could limit the application of the personal model is the exercise of public powers by the State on the territory where the violation occurs. This is, however, in contrast with previous jurisprudence of the ECtHR, more specifically with *Issa* and *Pad*, where no reference was made to the respondent State's exercise of public powers.[139] For this reason, it can be concluded that the main objection moved to the

---

[135] Milanović, *Extraterritorial Application of Human Rights Treaties* (n 1) 185.
[136] *Issa v Turkey* (n 89) paras 69, 71, 74-81. See also Milanović 'Al-Skeini and Al-Jedda in Strasbourg' (n 120) 124, 126.
[137] *Al-Skeini and others v. The United Kingdom* (n 88) para 142. See also Milanović 'Al-Skeini and Al-Jedda in Strasbourg' (n 120) 129.
[138] *Al-Skeini and others v. The United Kingdom* (n 88) para 149. See also Milanović 'Al-Skeini and Al-Jedda in Strasbourg' (n 120) 130-131.
[139] M Milanović 'Al-Skeini and Al-Jedda in Strasbourg' (n 120) 130-131.

personal model, the fact that it cannot be effectively limited and that it therefore renders the jurisdictional threshold meaningless, remains valid. It will be interesting to see how the human rights courts will deal with the personal model in the future and how the law develops in this area.

4.4 Conclusion

This chapter examined the rules regulating the exercise of State jurisdiction according to public international law and human rights law. One point that has emerged from this analysis is that both these regimes present some uncertainties as to the rules defining the exercise of State jurisdiction. In particular, in international law the uncertainties surrounding the effects doctrine and the protective principle leave room for the potential abuse of these principles by States. This is because in both cases the definition of what constitutes an adverse effect or an act against the sovereignty of a State is left to each State that claims jurisdiction. Therefore, in the absence of an international agreement, this could translate to States abusing the discretion that is left to them and exercising jurisdiction over acts that present a feeble connection with their territory. However, in regard to the protective principle, the lack of international protest following its application and the fact that it has been used in a reduced number of cases seems to vouch for its unproblematic nature according to international law. The effects doctrine, on the other hand, seems to be more frequently applied, especially when it comes to acts that happen online and that have no physical connection with the State exercising jurisdiction, as we have seen in the two previous chapters. The problem posed by this doctrine is that when it is taken to the extreme it can equate to exercising universal jurisdiction in relation to acts that are not an international crime. This means that, unlike international crimes, those acts are not deemed by the international community as so egregious to justify an exercise of jurisdiction in absence of any of the other recognised jurisdictional heads. Ultimately, as observed by some commentators, the effects doctrine removes the limits to the exercise of extraterritorial jurisdiction that were introduced thanks to the objective territorial principle. As far as the human rights law regime is concerned, the uncertainties surrounding this regime are related to the two jurisdictional models that have been created by the human rights courts to establish extraterritorial jurisdiction. In particular, both the spatial and personal model of jurisdiction have been critiqued for the difficulty to limit their application and the consequent arbitrariness of their application by the courts, especially with regard to the ECtHR.

Finally, the most important observation that stems from the analysis conducted in this chapter is that the international law and the human rights regimes are fundamentally different when it comes to the meaning of State jurisdiction. Indeed, the public international law rules of jurisdiction define the criteria according to which a State is entitled to regulate a given matter without infringing the sovereignty of other States. In contrast, according to human rights law a State has jurisdiction over a territory or a person when it exercises effective overall control over that territory or authority over that person, regardless of whether that exercise of jurisdiction is legal according to international law. This fundamental difference has a bearing on the meaning of State jurisdiction online, which is the theme that will be explored in the next chapter.

5. The Application of the Human Rights Conventions to Online Acts

5.1 Introduction

This chapter aims at answering the first research question: when and under what conditions acts that happen online can be considered to have happened within a State's jurisdiction according to the human rights conventions? In other words, what does online State jurisdiction mean in human rights law? This question will be answered by first analysing in sections two and three how international law has so far dealt with the concept of online State jurisdiction, highlighting the challenges and criticalities that the Internet poses to the jurisdictional rules. Section four will then proceed by illustrating the case law of the human rights courts regarding online State jurisdiction in order to highlight how the Courts have so far dealt with jurisdictional issues in Internet-related cases. Section five will focus on the application of the personal and spatial models of jurisdiction to the online environment and with an analysis of the extraterritorial effects model of jurisdiction. Finally, section 6 will summarize the main conclusions reached.

5.2. The International Law Rules Applicable to Cyber Operations: The Tallinn Manual 2.0 approach

A useful starting point in the discussion of the jurisdictional rules applicable to online acts according to international law is the Tallinn Manual 2.0, which is a guide for policy advisors and legal experts on how existing international law applies to cyber operations. The Tallinn Manual 2.0 defines cyber operations as cyber activities conducted during peacetime.[1] According to the Tallinn Manual 2.0, States can exercise both territorial and extraterritorial prescriptive jurisdiction over cyber activities as, in principle, these activities are subjected to the same jurisdictional rules as their offline counterparts.[2] However, the International Group of Experts who produced the Manual did recognise that

[1] M Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 1.
[2] ibid 51, [1]-[2].

the global nature of cyber activities and their ability to travel and produce effects in various States simultaneously could lead to multiple exercises of jurisdiction. Although these are allowed under international law, the Experts underlined that they could still lead to confusion and disputes between States.[3] Therefore, according to the Experts, international cooperation, especially in the law enforcement field, is particularly important.[4]

As to the jurisdictional rules governing cyber operations, the Tallinn Manual 2.0 has confirmed that States can exercise jurisdiction over cyber activities based on the objective and subjective territorial principles and on the effects doctrine.[5] There was disagreement among the Group of Experts on whether the territorial jurisdiction principle allows States to exercise jurisdiction if the territorial connection between the State and the cyber operation is minimal, for example if the data merely transits in that State's cyber infrastructure while it travels to reach the final destination.[6] In regard to the objective territorial principle, the Group of Experts clarified that the exercise of jurisdiction based on this principle is legal if the cyber operation in question, which originated in a different State, was intended to culminate in the State exercising jurisdiction or was directed against people located there.[7] Since, however, it might be difficult to determine when or where a given cyber operation starts or ends, the Tallinn Manual affirmed that jurisdictional rules have moved towards the effects doctrine.[8] Based on this doctrine, a State has jurisdiction over a cyber activity if this produces effects within that State.[9] Although, according to the Tallinn Manual 2.0 the effects doctrine can be considered as part of customary international law, it remains a controversial basis for the exercise of jurisdiction due to the fact that the criteria regulating its application are not fully settled in international law.[10] Indeed, its unqualified use has caused disputes between States.[11] In this regard, the Tallinn Manual has listed a series of conditions that render the exercise of jurisdiction over cyber operations based on the effects doctrine acceptable according to international law. These include the fact that the State exercising jurisdiction has a clear and internationally acceptable interest in doing so, the effects of the cyber operations must be direct, intended, foreseeable, and substantial and the exercise of jurisdiction does not

[3] ibid 54, [15].
[4] ibid.
[5] ibid 55, Rule 9.
[6] ibid 55, [3]-[4].
[7] ibid 56, [5].
[8] ibid 57, [9].
[9] ibid 57, [10].
[10] ibid 57-58, [11], [13].
[11] ibid 57, [11].

unjustifiably violate the interests of foreign States or nationals without a significant connection with the State exercising jurisdiction.[12] Ultimately, the exercise of jurisdiction over cyber activities based on the effects doctrine must be reasonable so that the sovereignty of foreign States and the comity principle can be respected.[13] As an example of a legitimate exercise of jurisdiction based on the effects doctrine the Tallin Manual 2.0 mentions cyber operations conducted abroad that have a substantial effect upon a State's territory, financial and economic activity and stability and legal order.[14] In contrast, exercising jurisdiction over a website located abroad and operated by foreign nationals is not permitted if that website does not target persons or objects in the State exercising jurisdiction.[15] In particular, a State cannot apply the effects doctrine to criminalise cyber operations conducted abroad and that are legal in that country, as that would lead to the violation of the foreign State's sovereignty and legitimate interests. On the other hand, it would be legitimate for a State to exercise jurisdiction over cyber operations taking place abroad but resulting in violence against its government even if these cyber activities are legal in the country where they originate.[16]

As to the international law rules regulating the exercise of prescriptive extraterritorial jurisdiction over cyber activities, the International Group of Experts recognised the validity of the active and passive nationality principle, of the protective principle and of the universal jurisdiction principle.[17] Similarly to the exercise of the effects doctrine, the Tallin Manual underlined that the exercise of extraterritorial prescriptive jurisdiction must be reasonable and must consider the interests and sovereignty of foreign States.[18] The Experts also distinguished between the protective principle and the effects doctrine, underlying that States exercising extraterritorial jurisdiction over cyber activities based on the protective principle can do so in a very limited number of instances, for example when the cyber operation in question compromises their national security, financial stability and other vital national interests.[19] In addition, States can apply the protective principle even in the absence of any effect within their territory, unlike the effects

[12] ibid 58, [13].
[13] ibid 58, [14].
[14] ibid 59, [15].
[15] ibid 59, [17].
[16] ibid 60, [19].
[17] ibid.
[18] ibid 61, [2].
[19] 'Acts that are generally accepted as falling within this category include: attempts upon the life or physical safety of key State officials; acts that are directed at forcibly overthrowing a State's government or seriously interfering with key State functions or national security, such as terrorism; and acts that are aimed at seriously compromising a State's financial solvency and stability, such as counterfeiting its currency or seriously compromising its banking system. Since cyber activities can facilitate each of these activities, they are in principle subject to protective principle jurisdiction', ibid 63, [11].

doctrine, which requires such effect and which is not limited to a specific range of offences.[20]

This section has provided an overview of the international law jurisdictional principles applicable to acts committed online as defined by the Tallinn Manual 2.0. The next section will focus on the current debate among the academic and the Internet community regarding online State jurisdiction and on some of the difficulties that exercising jurisdiction online poses.

5.3 The concept of State jurisdiction online: territoriality, effects doctrine and targeting test

The concept of State jurisdiction online has been the subject of multiple studies, many of which aimed at answering one fundamental question: how can the law, both domestic and international, deal with the transnational nature of the Internet? The answer to this question is, of course, not immediate nor simple, as evidenced by the contrasting and conflicting ways in which each State establishes jurisdiction online in various fields of the law. The current debate regarding tackling the online transnational legal challenges has moved away from whether regulation of the Internet is necessary to focus on how regulation might be possible. Indeed, while in the 1990s part of the academic debate was centred on whether existing laws applied to the Internet or whether Internet self-regulation was a preferable alternative, the main concern today is how to overcome the multiple challenges associated with developing a global harmonized approach to Internet jurisdiction.[21] The inadequacy of the existing jurisdictional concepts, regulatory fragmentation, and States' aggressive assertions of jurisdiction online are among the challenges that have been identified in this regard.[22] More specifically, Internet experts from various sectors (government, academia, civil society, Internet companies, technical operators and international organisations) have expressed concerns that the existing jurisdictional concepts are ill-equipped to deal with cross-border jurisdictional challenges online.[23] Some believe that this is because these concepts have been developed for the

[20] ibid 64, [12].

[21] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 1996) < https://www.eff.org/cyberspace-independence> accessed 18 November 2019; Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (*Internet & Jurisdiction*, 2019) <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf> accessed: 16 October 2019, 42-43.

[22] Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 26-28, 32-33.

[23] ibid 26. The Global Status Report Key Findings was published in May 2019 by the Internet & Jurisdiction Policy Network (I&J). The Report highlights some key challenges presented by online transnational

offline environment or are so vague and their application by States is so non-uniform that it is difficult to even identify what these concepts are.[24] In contrast, others believe that while the current jurisdictional rules are sound, it is their application to the online environment that is problematic.[25] Overall, a view held among many Internet experts is that there is a clear need for a new and simplified regulatory regime for Internet jurisdiction.[26]

Another challenge to the harmonization of the jurisdictional rules applicable online is represented by regulatory fragmentation and 'jurisdictional hyperregulation'.[27] These two phenomena are interlinked and can be reconducted to the fact that there are multiple laws that simultaneously apply to the same acts/parties performed/operating online, which however makes compliance with all the laws impossible.[28] At the same time, the increasingly aggressive exercises of jurisdiction by States have resulted in the imposition of heavy fines against parties located abroad but operating online to ensure compliance with local laws.[29] These facts have led to an increasing fragmentation of the Internet, since companies and individuals rely more and more on technical and non-technical measures (such as geolocation and disclaimers/terms of service respectively) to avoid specific countries.[30] This is why regulatory fragmentation and jurisdictional hyperregulation are seen as threats to the cross-border nature of the Internet as well as to the development of a globally harmonized regulatory regime.[31]

---

jurisdictional issues and contains surveys conducted among more than 100 of the I&J stakeholders regarding various online regulatory trends. The I&J stakeholders are Internet experts representing States, Internet companies, technical operators, civil society, academia and international organizations. The list of all the experts interviewed can be found at pages 7-9 of the Report. When asked whether the right legal concepts are already applied to deal with online cross-border legal challenges, the majority (40.2%) of the I&J experts interviewed disagreed, however a consistent 36% could neither agree or disagree and only 18% strongly agreed. Looking at the breakdown of votes by category of interviewees, it is possible to see that while the majority of academics (43.8%), representatives of international organisations (66.6%), and technical operators (50%) believed that the right legal concepts are not being applied, the majority of State representatives (40.7%) and civil society (50%) could neither agree nor disagree. Internet companies were split on this point as the same percentage of interviewees (38.9%) disagreed with the statement and neither agreed nor disagreed. Overall, however, only a minority across all the categories of interviewees believed that the right legal jurisdictional concepts are already being applied, which shows that there is consensus on the inadequacy of the current jurisdictional framework.

[24] ibid 26-27. The Report refers to various reasons given by the interviewees regarding whether or not the right legal concepts are already being applied to tackle cross-border legal challenges. In regard to vagueness of some of the current concepts, the example provided in the Report is comity, which has a precise meaning within the US legal system, while it is quite a vague principle in international law.

[25] ibid 26.

[26] ibid 27-28.

[27] ibid 43. On regulatory fragmentation see also T Schultz, 'Carving up the Internet: jurisdiction, legal orders, and the private/public international law interface' (2008) 19(4) EJIL 759.

[28] Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 43-44.

[29] ibid 33.

[30] ibid.

[31] ibid 33.

A crucial point that is at the heart of the ongoing online jurisdictional debate is the issue of territoriality. The territorial principle of jurisdiction is one of the main jurisdictional principles adopted by States. However, while this principle has a relatively clear application offline, the same cannot be said for the online environment. The primary role played by the principle of territoriality in establishing jurisdiction has, however, been contested by academics even with regard to the offline environment. Indeed, some have criticised the assumption that jurisdiction in international law is primarily territorial and have contested the effectiveness of the distinction between territorial and extraterritorial assertions of jurisdiction.[32] In particular, with regard to the primacy of territorial jurisdiction in international law, some authors have observed that while enforcement jurisdiction is certainly primarily territorial, prescriptive jurisdiction is not, since many rules of prescriptive jurisdiction, such as the nationality, passive personality, protective and universal jurisdiction principles, are related to extraterritorial exercises of jurisdiction.[33] Therefore, it cannot be argued that jurisdiction in international law is *tout court* primarily territorial. For this reason, in regard to the effectiveness of the distinction between territorial and extraterritorial, some have pointed out that 'to speak of extraterritoriality is akin to describing cars as "'horseless carriages'" – both descriptions are founded in a mistaken notion of what is "'normal'".[34] Besides, the relevance of the territorial principle in the current jurisdictional landscape has been questioned, as some commentators believe that this principle is eroding in favour of other factors, such as the criterion of the centre of interests adopted by the CJEU in the *eDate* case.[35] This point is, however, controversial, since the territorial principle, especially in its objective territorial version, is among the jurisdictional principles that States consistently apply not only offline but also online, as Chapters 2 and 3 have shown.[36] The territorial principle is also regularly listed in international agreements among the jurisdictional rules that apply on the Internet. As mentioned in the previous section, for example, the Tallinn Manual 2.0 includes this principle – in the form of subjective and objective territoriality and the

[32] Marko Milanović, *Extraterritorial Application of Human Rights Treaties* (1st, Oxford University Press 2011) 22, 24-25; Dan Jenker B Svantesson 'Nostradamus Lite – Selected Speculations as to the Future of Internet Jurisdiction' (2016) 10 Masaryk UJL & Tech 47, 63-64; Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49.
[33] Milanović (n 32) 22, 24-25; Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49.
[34] Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49. For a critique of the term extraterritorial, see also Cedric Ryngaert, *Jurisdiction in International Law* (1st, Oxford University Press 2008) 7-9.
[35] Svantesson (n 32) 61-65. For a discussion of the *eDate* case, see Chapter 2.
[36] See Chapters 2 and 3 for an analysis of Internet-related cases where States refer to the territorial principle to establish jurisdiction online.

effects doctrine - among those that are applicable to cyber-operations.[37] The same view is held by the International Association of Penal Law, which stated that 'the principle of territoriality remains the primary principle of jurisdiction also in cyberspace'.[38] Besides, Article 22 of the Convention on Cybercrime lists the territorial principle among those that can be used by States to establish jurisdiction over cybercrimes.[39]

However, despite the fact that the territorial principle is both found to apply in the online environment and is in fact frequently adopted by States, this principle poses more than one problem when it is employed in Internet-related cases.[40] Indeed, applying the territorial principle online allows multiple States to exercise jurisdiction in a universal-like manner, since, as the access-based jurisdictional chapter showed, it is particularly easy to establish a territorial connection with content that is accessible simultaneously worldwide. This gives rise to unpredictable exercises of jurisdiction which prevent individuals and parties operating online from reasonably anticipating which domestic laws apply to them.[41] Moreover, due to the ease with which territorial connections can be established with online content, the territorial principle fails in one of its main aims, that of identifying which State has a reasonable right to exercise jurisdiction.[42] Besides, the online application of the territorial principle makes it difficult to differentiate between territorial and extraterritorial exercises of jurisdiction. For example, with regard to the *Microsoft Ireland* case, some have observed that strictly applying the territorial principle leads to the impossible situation whereby the claims of both the parties to the case were plausible. This is because on the one hand it is technically true that accessing data stored in another country from computers located in the US does not require US enforcement

---

[37] Schmitt (n 1) 55, Rule 9; E Talbot Jensen, 'The Tallin Manual 2.0: Insights and Highlights' (2017) 48 Geo J Intl L 735, 747.

[38] International Association of Penal Law, 'Nineteenth International Congress of Penal Law Topic: "Information society and penal law"' (AIDP) < http://www.penal.org/en/resolutions-last-congress> accessed 20 November 2019. In regard to the application of the territorial principle to cybercrimes, see also C Ryngaert *Jurisdiction in International Law* (2nd, Oxford University Press 2015), 79 who lists objective territoriality and the constitutive elements approach as the jurisdictional principles related to Internet-based offences.

[39] Convention on Cybercrime (adopted 23 November 2011, entered into force 1 July 2004) ETS No.185, art 22. See also Ryngaert 2015 (n 38) 79.

[40] International Association of Penal Law (n 38); Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49. For a critic of the term extraterritorial, see also Ryngaert 2008 (n 34) 7-9; Dan Jenker B Svantesson 'A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft' (2015) 109 AJIL Unbound 69, 69-70.

[41] 'While the principle of territoriality remains the primary principle of jurisdiction also in cyberspace, it produces adverse effects when applied to offences in cyberspace, in that it de facto allows states to localise offences on their territory almost on a universality basis and leaves individuals in doubt as to which states may claim jurisdiction. States should exercise restraint in exercising jurisdiction in situations in which the effect is not "pushed" by a perpetrator into the state, but "pulled" into it by an individual in that state' International Association of Penal Law (n 38).

[42] Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49.

authorities to physically act on the territory of that country. On the other, as Microsoft stated, since the sought-after data were stored in its Dublin datacentre that access could be seen as an extraterritorial exercise of jurisdiction.[43]

Ultimately, one of the main reasons why the territorial principle is not suited for the online environment is represented by what has been described as 'the un-territoriality of data', a collection of data's distinctive characteristics which set them apart from their physical counterparts rendering territorial-based jurisdictional criteria meaningless.[44]. More specifically, data are extremely mobile, therefore when an email is sent from a given State the data have the potential to travel across many States at incredibly high speed and in an unpredictable way. This means that the Internet user who sent the email has more often than not no way of knowing where the data are at any given time or which country the data travelled to before reaching the recipient of the email.[45] Similarly, data available in the cloud are highly divisible, meaning that they can be copied and stored in multiple locations at a speed which allows for several jurisdictions to have a territorial connection with their storage.[46] Another key characteristic of data is that their location is independent from that of the users. This not only means that the data users do not know where their data are most of the time, but also poses serious problems to governments seeking to access the data. Indeed, even if the enforcement authorities knew the location of the data user, that information would have no bearing in identifying the location of the data and therefore the country that the enforcement authorities would need to contact in order to access them.[47] Besides, data are often owned by more than one user, such as data in a group chat, and even if it is possible to determine the identity and location of each user, it is difficult to establish which location should count in order to select the domestic law that applies.[48] Finally, users' data are controlled by third parties, such as Internet companies, who have the potential to determine both where the data are stored and the legal regime that applies to them, which is usually the location of the Internet company. This highlights the fact that data are different from their tangible counterparts as sometimes it is the location of the Internet company rather than that of the data that counts as far as the domestic laws that apply are concerned.[49]

[43] Svantesson 'A New Jurisprudential Framework for Jurisdiction' (n 40) 69-70.
[44] Jennifer Daskal 'The Un-Territoriality of Data' (2015) 125(2) YLJ 326.
[45] ibid 366-368.
[46] ibid 368-369.
[47] ibid 373-375.
[48] ibid 375-376.
[49] ibid 377-378.

All these points show that there is a clear need to "disentangle" Internet jurisdiction from territoriality.[50] Yet, due to the role played by territoriality in domestic and international law, this task appears herculean with domestic Courts struggling to adapt to the fluid nature of the online environment. Indeed, throughout the years domestic Courts, especially in Europe and North America, have switched between various ways of establishing jurisdiction online, moving from those based purely on the accessibility of a website to those involving an analysis of the activities conducted on the website, albeit a rudimentary one. Each of these jurisdictional approaches has, however, specific downsides, which render them less than ideal for the online environment. Indeed, as we have seen in Chapter 2, the accessibility of a website within the country exercising jurisdiction has been one of the main criteria through which domestic Courts have established jurisdiction in Internet-related cases. On some occasions, Courts have interpreted the fact that a given website was accessible within the domestic forum as proof that the online act complained of had in fact happened there, thus establishing jurisdiction based on the objective territorial principle. In the United States and Canada, for example, Courts in the 1990s interpreted the existence of a website as a clear proof that the out of State/foreign defendants had engaged in activities directed at the domestic forum, therefore satisfying the minimum contacts and the real and substantial connection doctrines.[51] Other times, the accessibility of a website was considered as evidence that

[50] 'It is well established and beyond intelligent dispute that international law's focus on territoriality is a bad fit with the fluidity of the online environment, which is characterized by constant and substantial cross-border interaction. Yet until recently, little had been done, and even less achieved, in the pursuit of disentangling internet jurisdiction from territoriality', Internet & Jurisdiction Policy Network (2019) Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49.

[51] 'In the present case, Instruction has directed its advertising activities via the Internet and its toll-free number toward not only the state of Connecticut, but to all states. The Internet as well as toll-free numbers are designed to communicate with people and their businesses in every state […] Further, once posted on the Internet, unlike television and radio advertising, the advertisement is available continuously to any Internet user. ISI has therefore, purposefully availed itself of the privilege of doing business within Connecticut. The court concludes that since ISI purposefully directed its advertising activities toward this state on a continuing basis since March, 1995, it could reasonably anticipate the possibility of being hailed into court here' *Inset Systems Inc. v. Instruction Set Inc.* 937 F. Supp. 161 (D. Conn. 1996), 165; 'Through its website, CyberGold has consciously decided to transmit advertising information to all internet users, knowing that such information will be transmitted globally. Thus, CyberGold's contacts are of such a quality and nature, albeit a very new quality and nature for personal jurisdiction jurisprudence, that they favor the exercise of personal jurisdiction over defendant' *Maritz, Inc. v. Cybergold, Inc*., 947 F. Supp. 1328 (E.D. Mo. 1996) 1333. 'The Plaintiffs allege that the investing public were misled by the Defendant's financial performance in that the means by which the Defendant communicated its financial performances were through internationally accessible mediums. Public documents such as SEC filings, securities analysts' reports, and advisories about the company, press releases issued by the company, and media reports about the company, were all available to the Plaintiffs as a means of determining the financial future of this company. When the Defendant made these research tools available to the investing public, and, in particular, Newfoundland investors, they ran the risk of having legal action initiated against them should any of these financial performance claims be shown to have been made negligently or in such a manner as to be intentionally misleading. As to the Defendant's claim that it never made or issued any public statements to the Canadian financial or business press, the Plaintiffs state that any information disseminated

the online act complained of produced negative effects in the domestic forum, giving rise to the application of the effects doctrine.[52] However, in some of the cases involving the effects doctrine the accessibility of a website within the domestic forum was used in conjunction with other factors to establish jurisdiction, such as the possibility for those located in that forum to order goods from the website.[53] The main problem with the access-based approach, be it based on the objective territorial principle or the effects doctrine, is that when it is the only factor used to establish jurisdiction, it gives rise to limitless assertions of jurisdiction. Indeed, every online act can be said to have happened within every domestic forum where it is accessible or can be found to produce adverse effects there. Therefore, this jurisdictional test is problematic, especially from the standpoint of the freedom of expression of Internet users and the predictability of the exercise of jurisdiction.[54] However, in some late 1990s cases a different approach to Internet jurisdiction started to develop in the United States which was based on the nature and quality of the commercial activity conducted through a website. In particular, the active vs passive test of jurisdiction was introduced by Pennsylvania District Court in the *Zippo* case.[55] According to this test, Courts could exercise jurisdiction over out of State

---

by the various news wires and through the Internet are often picked up in news stories by the Canadian financial or business press' *Alteen v. Informix Corp* (1998) N.J. No. 122 1997 No. C.B. 439, [13]. See also Michael A Geist 'Is There a There There - Toward Greater Certainty for Internet Jurisdiction' (2001) 16(3) Berkeley Tech LJ 1345, 1361-1364.

[52] 'It is clear from the Court's case-law that […] Article 5(3) does not require, in particular, that the activity concerned be 'directed to' the Member State in which the court seised is situated (see judgment in Pinckney, EU:C:2013:635, paragraph 42). Therefore, for the purposes of determining the place where the damage occurred with a view to attributing jurisdiction on the basis of Article 5(3) of Regulation No 44/2001, it is irrelevant that the website at issue in the main proceedings is not directed at the Member State in which the court seised is situated. In circumstances such as those at issue in the main proceedings, it must thus be held that the occurrence of damage and/or the likelihood of its occurrence arise from the accessibility in the Member State of the referring court, via the website of EnergieAgentur, of the photographs to which the rights relied on by Ms Hejduk pertain', Case C-441/13 *Pez Hejduk v EnergieAgentur.NRW GmbH* [2015] ECLI:EU:C:2015:28, paras 30-34; See also Edouard Treppoz 'Jurisdiction in the Cyberspace' (2016) 26 Swiss Rev Int'l & Eur L 273, 277.

[53] For example, in the case *Euromarket Designs Inc. v. Crate & Barrel Ltd* the Court found that 'Limited's Internet activities were directed toward Crate & Barrel and Illinois. Limited allegedly registered an Illinois company's mark as its domain name and deliberately designed an Internet website using an Illinois company's mark with the knowledge that this conduct would likely injure Plaintiff in Illinois, its place of incorporation and principal place of business. In addition, Limited intentionally designed the website to be interactive, inducing Illinois and United States residents to order goods over the Internet with an order format specifically designed for United States "ship to" and "bill to" addresses, and providing for credit card usage for ease of billing' *Euromarket Designs Inc. v. Crate & Barrel Ltd.* 96 F. Supp. 2d 824 (N.D. Ill. 2000), 836. See also Geist (n 51) 1373-1374 and generally 1371-1380 for a discussion of the effects doctrine.

[54] See Chapter 2, section 2.5 for a detailed analysis of the negative implications of the access-based jurisdictional approach. See also Treppoz (n 52) 279: 'In other words, after the Hedjuk case, any European court has jurisdiction for any cyber copyright infringement, even if the website is written in Japanese, offers the streaming of Japanese music with advertisements for local Japanese shops. Such a solution gives jurisdiction to Court having not clear proximity with the tort. What is more, such solution creates unpredictability for the defendant. No one could predict where he will be sued, since all court may have jurisdiction based on the Internet universality'.

[55] *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).

defendants if they maintained an active website through which they stipulated contracts with those living in the domestic forum and therefore conducted business there.[56] On the other hand, according to this test, passive websites of a purely informative nature were immune from the exercise of jurisdiction, regardless of the fact that they were accessible within the domestic forum. The middle ground in this test was represented by interactive websites which involve the exchange of information with the user's computer. In this case, domestic courts were encouraged to establish jurisdiction on a case by case basis depending on 'the level of interactivity and commercial nature of the exchange of information' occurring on the website.[57] Similarly to the access-based jurisdictional criterion, however, the active versus passive jurisdictional test poses problems due to its lack of predictability, notwithstanding the fact that it does involve a limited analysis of the activity conducted through a website. This is because, since not many websites are entirely active or passive, Courts needed more often than not to use their discretion in determining which category a website could be ascribed to, making it difficult for website owners to anticipate to which jurisdiction their website could be exposed.[58] More importantly, with the evolution of technology, today the majority of websites can be considered to be highly interactive. Therefore, even if the *Zippo* test represents a more nuanced alternative compared to the access-based jurisdictional approach, it appears outdated with Courts increasingly resorting to either the effects doctrine or the targeting test instead.[59]

The targeting test has been consistently used by the Courts of various countries, especially in Europe and North America, to establish jurisdiction in Internet-related cases.[60] According to this test, a given domestic Court can exercise jurisdiction over an online act

---

[56] 'This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. E.g. CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir.1996). At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. E.g. Bensusan Restaurant Corp., v. King, 937 F. Supp. 295 (S.D.N.Y.1996). The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. E.g. Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D.Mo.1996)' ibid 1124. See also Geist (n 51) 1365-1367; G Heissl, 'Jurisdiction for human rights violations on the Internet' (2011) 2(1) EJLT, 4-5.

[57] *Zippo* (n 55) 1124. For a discussion of US and Canadian cases affirming *Zippo* see Geist (n 51) 1367-1371.

[58] Geist (n 51) 1379. Geist at also criticizes the *Zippo* test because it provides inconsistent results and it does not differentiate between actual and potential sales conducted on active websites.

[59] ibid 1380.

[60] Internet & Jurisdiction Policy Network 'Global Status Report 2019' (*Internet & Jurisdiction*, 2019) <https://form.jotformeu.com/93222419949364> accessed: 28 November 2019, 149.

that has territorial connections with more than one State if that act is targeting the domestic forum. The targeting test is often associated to the effects doctrine, as Courts tend to consider a series of targeting factors to substantiate the finding that a given online act produced effects on the domestic forum. The targeting test has been used in various areas of the law, including defamation, trademark infringement and consumer contracts, with some commentators suggesting that this test is due to expand to other legal fields and systems.[61] A positive aspect of the targeting test compared to other jurisdictional criteria adopted online is that it gives rise to more predictable exercises of jurisdiction. This is because this test bases the exercise of jurisdiction over the identification of specific steps taken by a foreign actor to target a given forum, making it easier for the foreign actor to anticipate the exercise of jurisdiction by the targeted State.[62] However, one of the major problems of this jurisdictional criterion is that there is no agreement as to what amounts to targeting. This question was at the heart of the 2010 consumer contract joint case *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller* (the *Hotel Alpenhof* case) before the CJEU. In the *Hotel Alpenhof* case, the Court was asked to clarify what factors could be used to establish that a trader advertising its services on a website was directing its activities towards the Member States of the domicile of the consumer, pursuant to article 15(1)(c) of the Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.[63] The Court found that the trader's clear intention to establish commercial relations with consumers in the relevant member State was central to the answer.[64] Interestingly, however, the Court excluded that the mere existence of a website could be considered as proof of such an intention, in contrast with the assumption on which the access-based jurisdictional approach rests.[65] Overall, the judges found that a series of

[61] For example, according to the Internet & Jurisdiction Global Status Report, the targeting test has been adopted in data protection proposals in Argentina and Thailand, ibid 149. In regard to cases where the targeting test has been adopted see *Young v New Haven Advocate et al*, 315 F.3d 256 (4th Cir. 2002) discussed in Chapter 2 Section 2.3.2 in the field of defamation, *Ward Group Pty Ltd v Brodie & Stone Plc* [2005] FCA 471, [37] and *American Information Corp. v. American Infometrics, Inc*., 139 F. Supp. 2d 696 (D. Md. 2001), [700] in regard to trademark infringement, and Joined Cases C-585/08 *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)* [2010] 2010 I-12527 in regard to consumer contracts. See also: Treppoz (n 52) 280-281 for a discussion of the European approach to the regulation of consumer contracts; Geist (n 51) 1381-1382 and Heissl (n 56) 5-7 for a discussion of cases in the United States where the targeting approach has been used.

[62] Geist (n 51) 1381.

[63] *Hotel Alpenhof* (n 61) para 47.

[64] ibid para 75.

[65] 'Whilst seeking to confer further protection on consumers, the European Union legislature did not go as far as to lay down that mere use of a website, which has become a customary means of engaging in trade, whatever the territory targeted, amounts to an activity 'directed to' other Member States which triggers application of the protective rule of jurisdiction referred to in Article 15(1)(c) of Regulation No 44/2001' ibid para 72.

factors should together be taken into account to ascertain whether a trader is targeting a particular State, including: mentions that the services offered are available for consumers located in that State designated by name, the use of Internet referencing services offered by search engine operators to facilitate the access to the trader's website to consumers located in that State[66], 'the international nature of the activity at issue, such as certain tourist activities; mention of telephone numbers with the international code; use of a top-level domain name other than that of the Member State in which the trader is established, for example '.de', or use of neutral top-level domain names such as '.com' or '.eu'; the description of itineraries from one or more other Member States to the place where the service is provided; and mention of an international clientele composed of customers domiciled in various Member States, in particular by presentation of accounts written by such customers'.[67] With regard to language and currency, the Court concluded that these factors are only relevant if the website gives the consumers the possibility to select different languages and currencies[68], whereas the mere presence on the website of the trader's contact details, (such as email address, physical address and phone number without an international code), and the possibility to conclude a contract through the website do not count as proof of targeting.[69] This approach to targeting has also been adopted in other EU instruments, such as the General Data Protection Regulation.[70] The reliance on factors such as use of language, currency and availability of service in a given country is also reflected in the criminal law field, where it received approval from the International Association of Penal Law.[71]

---

[66] ibid para 81.
[67] ibid para 83.
[68] ibid para 84.
[69] ibid paras 77-79.
[70] 'In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union', Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJL 119/1, Recital 23; see also Internet & Jurisdiction Policy Network 'Global Status Report 2019' (n 60) 149.
[71] 'In determining effects, states shall consider the existence of a particular nexus with the offence, such as the intent of the perpetrator as it may appear from the use of a given language, the provision of domestic payment facilities, a service offer in specific cities, etc. When a state localizes the effects of an offence

However, notwithstanding the fact that there seems to be greater consensus towards the adoption of the targeting test or some of the factors that this should be based on, there is still no international consensus on how to conduct this test whose application is controversial according to international law, as underlined by the Tallinn Manual 2.0.[72] It certainly seems that some progress has been made towards greater clarity in this regard, as the *Hotel Alpenhof* case shows. However, international harmonization in this field still seems far off. One of the main downsides associated to the use of the targeting test is that it could lead to Internet fragmentation, with companies increasingly relying on filtering measures to exclude specific jurisdictions from the reach of their websites.[73] Another disadvantage of the targeting test is that it does still require a certain degree of Courts' discretion in its application, which could lead to arbitrary and unpredictable assertions of jurisdiction.[74] In addition, there are various uncertainties associated with the targeting test. For example, it is not clear how this test would work in regard to intangible activities, activities that do not require a payment or the stipulation of contracts and that do not have a place of delivery, such as streaming services offered on a free basis.[75] Another uncertainty is represented by websites that do not rely on geolocation technologies to filter out specific audiences. It is not clear whether these websites might be considered as targeting a worldwide audience, especially if they use the English language and present advertisements from global rather than local companies.[76] However, as mentioned above, notwithstanding its negative aspects and uncertainties, the targeting test appears as a preferable alternative to establishing jurisdiction online from a predictability point of view. Indeed, unlike the other tests examined so far, this test does contain clearer factors that online actors could rely on to predict which jurisdiction they are going to attract.

Overall, it seems unrealistic that the various jurisdictional issues that arise online examined in this section can be resolved through an all-encompassing international agreement. Instead, some commentators believe that a more realistic possibility is gradual harmonisation, which might be easier to achieve in specific sectors such as data privacy.[77]

---

within its borders, the principle of legality requires that the perpetrator could have had a reasonable expectation that his or her conduct would cause effects in that country' International Association of Penal Law (n 38).

[72] Schmitt (n 1) 57-58, [11], [13].

[73] Geist (n 51) 1381, 1405; Treppoz (n 52) 281.

[74] Internet & Jurisdiction Policy Network 'Global Status Report 2019' (n 60) 149-150. See also Schultz (n 27) 818-819 on the indeterminacy of the meaning of targeting.

[75] Treppoz (n 52) 282-283.

[76] ibid.

[77] Svantesson 'Nostradamus Lite' (n 32) 60; Internet & Jurisdiction Policy Network 'Global Status Report 2019' (n 60) 55.

Having examined the issues surrounding the general international law rules regulating State jurisdiction online, the next section will focus on the issues surrounding the human rights jurisdictional rules regarding Internet jurisdiction.

5.4 The concept of extraterritorial online jurisdiction according to human rights conventions

A starting point in the analysis of the meaning of online State jurisdiction according to human rights conventions is that these conventions apply to online acts as well as to their physical counterparts. As stated by the Human Rights Council (HRC) in 2012 in the resolution *The promotion, protection and enjoyment of human rights on the Internet* 'the same rights that people have offline must also be protected online'.[78] While the HRC was expressly referring to the fact that two particular human rights conventions, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), apply to online acts, the same principle can be extended to other human rights treaties. In particular, the European Convention on Human Rights (ECHR), the African Charter on Human and Peoples' Rights (ACHPR) and the American Convention on Human Rights (ACHR) have all been found to apply both offline and online.[79]

What, however, needs to be clarified is the exact scope of the various human rights online together with the rules that define the jurisdictional threshold for their application to

[78] HRC, The promotion, protection and enjoyment of human rights on the Internet (29 June 2012) A/HRC/20/L.13.

[79] For the application of the ECHR to online acts see *inter alia* generally Research Division of the European Court of Human Rights, Internet: Case Law of the European Court of Human Rights, Council of Europe/European Court of Human Rights, 2015; Council of Europe Committee of Ministers, Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, [1]-[2], [5]; Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, Strasbourg: Council of Europe Publishing, 2013. ISBN 978-92-871-7702-5, 19. In regard to the online application of the American Convention on Human Rights see *inter alia* Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (31 December 2013), [2], [36]; see also generally Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (15 March 2017). As to the application of the African Charter on Human and Peoples' Rights to online acts, see *inter alia* The African Commission on Human and Peoples' Rights 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa' (Banjul 2019); African Commission on Human and Peoples' Rights 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa' (Banjul 2016) ACHPR/Res.362(LIX)2016; The African Commission on Human and Peoples' Rights 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the situation of freedom of expression and access to information in the Republic of Zimbabwe' (Banjul 2019). See also generally The United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet' (1 June 2011).

online acts. While the first point is dependent on the circumstances of each case and can therefore be clarified by the human rights courts at the merits stage of the case, the second issue is a threshold one which affects who is entitled to the protection offered by the human rights conventions. In particular, as noted by the Research Division of the European Court of Human Rights (ECtHR) in regard to the ECHR, it is unclear under what circumstances a State can exercise jurisdiction over a defendant located outside its domestic borders in relation to an alleged violation of the Convention committed online.[80] The Research Division noted that this question needs to be answered primarily by domestic courts and through the application of the relevant principles of private international law on jurisdiction. In other words, according to the Research Division, the ECtHR is not directly concerned with this issue and will assume that the Member States have jurisdiction if the jurisdictional issue is not contested by the parties to an Internet-related case.[81] However, while this is true, a question that the ECtHR is certainly concerned with is when a violation of the Convention that has happened online or that is the result of an act committed online can be said to have happened within the Member States' jurisdiction or is attributable to them.[82] Unfortunately, the criteria according to which such a determination can be made are still unclear. In particular, it is not clear how to deal with those online cases that present a cross-border element. Indeed, while the Internet crosses the borders of multiple countries simultaneously, not all Internet-related cases raise extraterritorial jurisdictional issues. For example, it is relatively uncontested that a State can exercise jurisdiction over data uploaded from its territory by individuals living there and managed by Internet service providers established in that State. In these cases, there is no cross-border element and therefore from a jurisdictional point of view the cases do not differ from those that happen in the physical environment. This is true for most of the Internet-related proceedings brought before the ECtHR and the HRC, where the Internet-element of the cases is so clearly linked to the Member States exercising jurisdiction that neither party raised jurisdictional concerns.[83] However, jurisdictional uncertainties remain for those online cases that are linked to more than one State because the online action at the centre of the case has been committed in foreign States or affects people located there. In these cases, it is not clear whether the human rights conventions apply to the extraterritorial online activities because the criteria

[80] Internet: Case Law of the European Court of Human Rights (n 79) 4.
[81] ibid 4-5.
[82] ibid 5.
[83] See for example the case of *Premininy v Russia* App no 44973/04 (ECtHR, 26 June 2011) or *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013).

regulating the exercise of State jurisdiction online according to these conventions are uncertain.

The ECtHR has been presented with the opportunity to clarify this jurisdictional point in a limited number of occasions, as observed by the Research Division of the ECtHR which quoted the *Perrin v the UK* case as the only Internet-related case that raised jurisdictional issues.[84] However, notwithstanding the fact that *Perrin* does present a clear cross-border element, as the pictures for whose publication Mr Perrin had been arrested were uploaded from the US by his company, the case is not directly concerned with establishing whether the Convention applies to extraterritorial online acts.[85] This is because in this case the ECHR applied based on the principle of territorial jurisdiction because Mr Perrin lived in the UK and was *ipso facto* in an area controlled by that State. Therefore, the *Perrin* case illustrates territorial jurisdiction, rather than the extraterritorial application of the ECHR to a foreign party, in this case Mr Perrin's company, which did not present any links with the UK except for the fact that the pictures that it had uploaded online were accessible worldwide and therefore within the British territory as well. However, *Perrin* still provides an interesting precedent as far as clarifying whether certain extraterritorial exercises of jurisdiction by States over online content are compliant with the Convention. Indeed, in this case the applicant argued that in exercising jurisdiction based on access to online content the UK had violated his right to freedom of expression. More specifically, Mr Perrin claimed that the Obscene Publications Act 1959 was not sufficiently foreseeable nor precise to satisfy the law requirement of article 10(2) because the major steps towards the online publication of the pictures had happened in the US and not in the UK.[86] In other words, in *Perrin* the ECtHR was asked to establish whether an exercise of jurisdiction based on access to online content is compliant with the clarity and foreseeability requirements of the freedom of expression obligations of the ECHR. Interestingly, the ECtHR found in the affirmative, as it stated that the Obscene Publications Act 1959 was reasonably accessible to Mr Perrin as he lived in the UK and was also sufficiently precise because it did make it clear that it applied to electronic data as well.[87] The ECtHR judgement in the *Perrin* case has attracted many critiques and poses more than one problem as far as the concept of predictability of the law is concerned.

[84] '[R]esearch reveals that there are very few Internet-related cases concerning "jurisdictional issues" at present. In particular, Perrin v. the United Kingdom (dec.) (no. 5446/03, ECHR 2005-XI) may be mentioned', Internet: Case Law of the European Court of Human Rights (n 79) 6.
[85] The *Perrin* case, both before the UK courts and the ECtHR, is examined in detail in Chapter 2. Therefore, this section will focus on some selected findings of the ECtHR only.
[86] *Perrin v the United Kingdom* App no 5446/03 (ECtHR, 18 October 2005), 5-6.
[87] ibid 6.

These points have been discussed in Chapter 2 and will also be examined in more detail in the next chapter, which looks into the compliance of some exterritorial exercises of jurisdiction online with the freedom of expression provisions of the human rights conventions. As far as the present discussion is concerned, it suffices to say that the *Perrin* case shows that according to the ECtHR establishing jurisdiction over cross-border online content based on access does not violate the freedom of expression provisions of the ECHR.

A case that might provide more answers in regard to the application of the Convention to cross-border online acts is *Tamiz v the UK*. In this case the applicant, Mr Tamiz, a British national living in the UK brought a complaint related to some defamatory comments that had been published about him by anonymous third parties under a blog post. The blog post was hosted via the platform Blogger.com managed by the US-based Google Inc. Mr Tamiz argued before the ECtHR that the UK had violated the positive obligation to protect his reputation under Article 8 of the Convention since the domestic courts had not granted him remedy against Google Inc. notwithstanding the fact that the company could be considered responsible for the publication of those comments according to common law.[88] The applicant had initially successfully obtained permission to serve the claim in libel against Google Inc. outside the UK jurisdiction by the domestic courts.[89] However, this permission was subsequently set aside as the courts found that they had no jurisdiction to hear the case since no real and substantial tort had been committed within the domestic forum.[90] More specifically, the Courts found that it was highly unlikely that the defamatory comments had been accessed by a significant number of readers within the timeframe that Google was responsible for their publication according to common law.[91] Therefore, the damage to the reputation of the applicant was so trivial that it could not amount to a real and substantial tort.[92] The ECtHR agreed with the domestic courts and found in favour of the UK. As far as jurisdiction is concerned, just like in *Perrin*, in *Tamiz* it is immediately apparent that the ECHR applies to the British applicant based on the principle of territorial jurisdiction, as he was a citizen and resident of the UK. However, the part of the *Tamiz* judgment that makes this case relevant to this discussion is that related to the ECtHR's finding that the Convention applies to the US-based Google

[88] *Tamiz v UK* App no 3877/14 (ECtHR, 19 September 2017), para 57.
[89] ibid para 22.
[90] ibid para 39.
[91] The Court of Appeal found that the principles of the case *Byrne v Deane* [1937] 1 KB 818 (as cited in *Tamiz v Google Inc.* [2013] EWCA Civ 68, [27]) applied to this case, *Tamiz v Google Inc.* [2013] EWCA Civ 68, [30], [34], [36].
[92] ibid [50].

Inc. and to its users as well. Indeed, the ECtHR found that the domestic courts had exercised 'a fair balance between the applicant's right to respect for his private life under Article 8 of the Convention and the right to freedom of expression guaranteed by Article 10 of the Convention and enjoyed by both Google Inc. and its end users'.[93] In particular, the Strasbourg judges found that in applying the test of a real and substantial tort 'the national courts were, in fact, ensuring that there would be no interference with Google Inc.'s right to freedom of expression in a case where the interference with the applicant's reputation was "trivial"'.[94] This point is particularly significant because Google Inc. is a foreign company located outside the UK territory with users all over the world and yet the ECtHR had not hesitation in recognising that both Google Inc. and its users had freedom of expression rights under the Convention. Therefore, according to the *Tamiz* case the ECHR applies to a party that has no territorial connection with the State exercising jurisdiction apart from the fact that it manages online activities that can be accessed by Internet users located in that country. While, however, all the parties to this case took it for granted that the ECHR applied to Google Inc., it is not clear which jurisdictional model justifies this application. This point will be discussed in detail in the next section, which examines the application of the spatial and personal model of jurisdiction to cross-border Internet cases. What is worth highlighting here is that in the *Tamiz* case the ECtHR took it for granted that the Convention applies to Google Inc. and its users without examining the issue in more detail.

This observation can be extended to another recent high-profile Internet-related case brought before the ECtHR that clearly showed an extraterritorial element. This is the case of *Big Brother Watch and Others v the UK*. The 16 applicants in this case were several individuals and organisations campaigning for civil liberties.[95] They brought a complaint against the UK following the Snowden revelations regarding surveillance and interception programmes operated by the UK and the US intelligence agencies. The applicants believed that, due to the nature of their work, their electronic communications

[93] *Tamiz v UK* (n 88) para 90.
[94] ibid para 87.
[95] This case joins three different applications lodged before the ECtHR: *Big Brother Watch and Others v. the United Kingdom*, *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* and *10 Human Rights Organisations and Others v. the United Kingdom*. The 16 applicants were: Human Rights Watch, Access Now, Bureau Brandeis, Center For Democracy & Technology, European Network of National Human Rights Institutions and the Equality and Human Rights Commission, the Helsinki Foundation For Human Rights, the International Commission of Jurists, Open Society Justice Initiative, The Law Society of England and Wales and Project Moore, the Center For Democracy & Technology, the Helsinki Foundation For Human Rights, the International Commission of Jurists, the National Union of Journalists and the Media Lawyers' Association, Article 19, the Electronic Privacy Information Center and the Equality and Human Rights Commission, *Big Brother Watch and Others v. the United Kingdom* Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018), para 4.

had been intercepted by the UK or obtained by the UK from the US or from communications service providers.[96] In particular, the applicants challenged the legality of three surveillance regimes: the bulk interception regime and the regime allowing the UK to obtain communications data from communications service providers – both of which were carried out according to the Regulation of Investigatory Powers Act (RIPA)[97] – and the intelligence sharing regime which allowed the UK to receive material intercepted by the US National Security Agency (NSA) under the PRISM and Upstream programmes.[98] The applicants argued that all three surveillance regimes violated their rights to privacy and freedom of expression according to Articles 8 and 10 of the Convention.[99] The ECtHR found in favour of the applicants as it did establish that there had been a violation of the right to privacy and freedom of expression in relation to two of the surveillance regimes, the bulk interception regime and the regime related to obtaining communications data from communications service providers.[100] The ECtHR however found no violation of the ECHR in regard to the regime of sharing intelligence with foreign governments.[101] The *Big Brother Watch* case is particularly relevant as far as the extraterritorial application of the ECHR to online acts is concerned. This is because

---

[96] ibid paras 7-8.

[97] Both the bulk surveillance regime and the regime related to obtaining communications data from communications service providers have undergone a significant number of changes introduced by the Investigatory Powers Act 2016 which received the royal assent on 29 November 2016. For more details on the Investigatory Powers Act 2016 as summarised by the ECtHR see *Big Brother Watch and Others v. the United Kingdom* (n 95) paras 195-201.

[98] ibid paras 10-18.

[99] ibid paras 270, 389, 450, 469. The third set of applicants also claimed at 501 that the domestic procedure for challenging surveillance actions violated Article 6 of the Convention. In addition, the applicants stated at 514 that Article 14 of the Convention read in combination with Articles 8 and 10 had been violated, because the bulk interception of communications discriminated against people outside the United Kingdom who were disproportionately more likely to have their communications intercepted.

[100] The Court found at 314 that, although conducting a bulk interception regime does not *a priori* violate the Convention, in this case the right to privacy was violated since there was no independent oversight under the RIPA regime in regard to the selectors and search criteria that were used to filter the communications to be intercepted, paras 340-347. In addition, the judges found a violation of Article 8 in the regime regarding obtaining data from communications service providers because this regime was not in accordance with the law, paras 467-468. As far as Article 10 is concerned, the ECtHR found that both the bulk interception and the obtaining communications regimes under RIPA violated freedom of expression because the safeguards in place for protecting access to confidential journalistic material were inadequate, paras 493, 495, 499-500.

[101] The judges found that the fact the UK had received material intercepted by the NSA did not violate Articles 8 and 10 of the Convention as the regime of sharing intelligence with foreign governments was sufficiently foreseeable and it could be considered as necessary in a democratic society. In particular, in regard to the proportionality of the sharing of intelligence regime, the Court stated at 446 that as States were facing the threat of international terrorism it was 'legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts […]. Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this "information flow" was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was "necessary in a democratic society"', *Big Brother Watch and Others v. the United Kingdom* (n 95) paras 428-448.

the case focuses on the interception of external communications, which section 20 of RIPA defines as communication that is sent or received outside the British Islands.[102] Accordingly, this case covers interception by the UK of electronic communication of both UK residents and people outside the UK.[103] In addition, some of the applicants were located outside the UK, such as The American Civil Liberties Union, The Canadian Civil Liberties Association, The Egyptian Initiative For Personal Rights, The Hungarian Civil Liberties Union and The Irish Council For Civil Liberties Limited. This means that in *Big Brother Watch* the ECtHR was called to examine the application of the ECHR to the extraterritorial surveillance of electronic communications of individuals located outside the territory of a Member State. However, the question of whether and according to which model the ECHR applies to individuals outside the UK was not asked to the Court. As the judges observed:

> '[t]he Government […] did not […] raise any objection under Article 1 of the Convention; nor did they suggest that the interception of communications under the section 8(4) regime was taking place outside the United Kingdom's territorial jurisdiction. The Court will therefore proceed on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom'.[104]

Therefore, it is fair to conclude that according to the *Big Brother Watch* case the ECHR applies to individuals located outside the territory of a Member State due to the online surveillance activities conducted by that Member State on its territory. This case highlights two main points: that the electronic surveillance activities have been considered as happening in the UK, and that the Convention applies based on the location of the interference with the applicants' rights rather than the location of the applicants.[105] This is, however, a departure from the jurisprudence of the ECtHR regarding the extraterritorial application of the Convention. Indeed, a key factor in applying the spatial model of jurisdiction is that the individual is within an area controlled by the State, while according to the personal model of jurisdiction the location of the individual is irrelevant

---

[102] ibid para 69.

[103] The only communications that could not be subjected to interception according to RIPA were communications between two individuals both located in the UK (ex. two people emailing each other while both were in the UK, regardless of the location of server hosting the communication). In contrast, according to RIPA all those communications where at least one of the recipients, either the sender or the receiver, was located outside the UK were considered as external communications. Similarly, communications from people in the UK who used a search engine overseas or who posted a public message on social media were considered as external communications according to RIPA, *Big Brother Watch and Others v. the United Kingdom* (n 95) paras 70-71.

[104] ibid para 271.

[105] Marko Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK' (*EJIL: Talk!*, 17 September 2018) <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> accessed: 02 March 2020.

as what matters is the exercise of power or authority by the State over the victim.[106] In other words, although it seems natural that the Convention would apply to acts that happen on the territory of a Member State, it is unclear the conceptual model upon which this application is based. This point will however be examined in more details in the next section. A final point worth mentioning here in regard to *Big Brother Watch* is that the Court made another significant assumption concerning the extraterritorial application of the ECHR.[107] Indeed, when examining the regime allowing the UK to receive intelligence data collected by foreign governments, the Court stated that the applicants could 'claim to be victims of the alleged violation of Article 8 of the Convention occasioned by the existence of an intelligence sharing regime'.[108] This means that, as some commentators have observed, the Court assumed that individuals outside the UK whose communications were intercepted outside the UK by another country 'have Convention rights vis a vis the UK'.[109] The *Big Brother Watch* case is ongoing as it is currently being examined before the Grand Chamber of ECtHR after having been referred to it in February 2019.[110] It will be interesting to see how the Grand Chamber will deal with all the complex issues raised by this case.

The question of the application of the Convention to individuals located outside a Member State due to the surveillance of their communications operated by that State had however been presented to the ECtHR even before the *Big Brother Watch* case. More specifically, in the 2006 case *Weber and Saravia v Germany* two applicants who lived in Uruguay, one of whom was a German citizen, claimed that their rights under the Convention had been violated due to the interception of their telecommunications by Germany.[111] The German government argued that the application was incompatible *ratione personae* because the applicants lived in Uruguay and the alleged violation of their Convention rights had happened in Uruguay, and therefore outside the German jurisdiction.[112] The ECtHR, however, avoided addressing the jurisdictional issue altogether as it found that the application was inadmissible as 'manifestly ill-founded' on the merits.[113] While in

[106] M Milanović, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv Int'l L J 81, 124-126.
[107] Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK' (n 105).
[108] *Big Brother Watch and Others v. the United Kingdom* (n 95) para [419]. The Court however subsequently found no violation of the Convention in regard to the intelligence sharing regime, see note 101.
[109] Marko Milanovic, 'ECtHR Judgment in Big Brother Watch v. UK' (n 105). See also *Big Brother Watch and Others v. the United Kingdom* (n 95) paras 419-421.
[110] This information is accurate as of 03 September 2020.
[111] *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 29 June 2006), paras 63-65.
[112] ibid para 66.
[113] ibid [156]. 'The Court does not consider it necessary in the present case to rule on the objections made by the Government since, even assuming that the application is compatible ratione personae with the

Weber and Saravia the ECtHR had been explicitly presented with the objection by a Member State that individuals located in foreign States could not be found within that Member State's jurisdiction due to surveillance operations allegedly conducted by that State, in *Liberty and Others v the UK* this objection was never raised. In that case, the applicants were one British and two Irish organisations established in London and Dublin respectively operating in the civil liberties field.[114] They claimed that their right to privacy under the Convention had been violated by the UK due to the interception of their telephone and electronic communications conducted by UK officials within the domestic territory.[115] The ECtHR found that the UK had indeed violated the applicants' Article 8 rights under the Convention. Therefore it can be said that, since the jurisdictional point was never raised by any of the parties, the Court assumed that the ECHR applied to Irish residents whose privacy had been violated by the UK due surveillance operations conducted there.[116] Therefore, *Liberty* can be seen as another example of those cases that show that a State exercises jurisdiction according to the ECHR when it commits an act within its territory that affects the rights of people located abroad.

Finally, the ECtHR was asked to examine the jurisdictional issues that arise in regard to extraterritorial online surveillance in the case *Privacy International and Others v the United Kingdom*. The case was communicated to the UK in November 2018 and was declared inadmissible by the ECtHR on 7 July 2020. In this case, the 6 applicants were NGOs, privacy activists, and Internet and communications service providers from the UK, Germany, United States and South Korea.[117] They claimed that the UK violated their rights to privacy and freedom of expression since the UK Government Communications Headquarter (GCHQ) committed equipment interference, i.e. hacked their equipment pursuant to section 7 of the Intelligence Services Act 1994 (ISA).[118] Section 7(1) of ISA

Convention, that domestic remedies have been exhausted and that both applicants can claim to be victims of Convention violations, it considers that the application is in any event inadmissible' ibid para 72.

[114] *Liberty and Others v the United Kingdom* App no 58243/00 (ECtHR, 01 October 2008), para 1.

[115] ibid para 42. The applicants at 71 also claimed that there had been a violation of Article 13 of the ECHR, however having found a violation of Article 8, the Court decided that there was no need to examine this complaint separately.

[116] ibid paras 69-70.

[117] The applicants are the NGO Privacy International registered in London, the internet service providers GreenNet Limited registered in London, Media Jumpstart Inc. registered in the United States and Korean Progressive Network Jinbonet registered in South Korea, the communications service provider Riseup Networks Inc. registered in the United States and the "'hactivists'" association Chaos Computer Club E.V. registered in Germany, *Privacy International and Others v the United Kingdom* App no 46259/16 Statement of Facts and Questions (ECtHR, 19 November 2018) para 1.

[118] 'The applicants complain under Articles 8 and 10 of the Convention that the power under section 7 of the Intelligence Services Act 1994 is not in accordance with the law in the absence of a code of practice governing its use. Moreover, they complain that that section contains no requirement for judicial authorisation; there is no information in the public domain about how it might be used to authorise Equipment Interference; and there is no requirement for filtering to exclude irrelevant material. The

provides that if a person 'would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State'.[119] In the domestic proceedings, the Investigatory Powers Tribunal (IPT) considered the jurisdictional issue of whether Articles 8 and 10 of the ECHR apply to equipment interference committed outside the UK.[120] The IPT found that, since the equipment interference under discussion is an act committed outside the UK, that act would not normally fall within the meaning of jurisdiction according to the ECHR, which in IPT's opinion is primarily territorial. Accordingly, persons living abroad who find themselves subjected to hacking committed by GCHQ abroad pursuant to section 7 ISA could not normally be found to be within the territorial scope of the ECHR.[121] However, the IPT did not exclude that there could be some exceptional circumstances bringing those individuals within the scope of the Convention. The claimants, for example, argued that such circumstances would arise if the victim of the interference was in the UK while the computer or the information was abroad or if the equipment interfered with was brought back to the UK.[122] However, the applicants also conceded before the IPT that

> 'in most cases where someone who is the subject of an authorisation granted under s.7 is abroad it was difficult to argue that such person is within the territorial scope of the Convention, and in any event that there would be a "very limited number of circumstances" in which there was going to be a breach of the Convention'.[123]

On the jurisdictional point, the UK Tribunal concluded that, due to the various difficulties raised by jurisdiction, there was an insufficient factual basis in the present case to reach a specific conclusion on this point.[124] The question '[d]id the facts of which the applicants complain in the present case occur within the jurisdiction of the United Kingdom?' was asked by the ECtHR to the parties to the case and it was at the centre of the Court's July 2020 admissibility decision.[125] However, the Court did not examine this issue as it found the application to be inadmissible since the applicants had not exhausted the domestic

---

applicants also argued under Article 13 that the IPT did not provide an effective remedy as it did not rule on the Section 7 regime in the domestic litigation' ibid paras 31-32.

[119] Intelligence Services Act 1994, s 7(1).

[120] *Privacy International and Greennet & Others v.s (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters* [2016] UKIP Trib 14_85-CH, [48].

[121] ibid [49]-[51].

[122] ibid [52].

[123] ibid.

[124] ibid [53].

[125] *Privacy International and Others v the United Kingdom* Statement of Facts and Questions (n 117) 10.

remedies available to them in violation of article 35(1) of the ECHR.[126] In particular, the ECtHR found that, as claimed by the Government, the applicants had conceded before the IPT that, as Section 7 of ISA was related to acts that occurred outside the UK, there was no jurisdiction under the ECHR.[127] Therefore, the European judges found that the applicants had not exhausted the domestic remedies since they had not argued the jurisdictional point before the IPT.[128] In this regard, the Court refused the applicants' argument that they had not pursued the jurisdictional point before the UK Tribunal because they wanted the ECtHR to examine this issue. Indeed, the judges found that such an argument violates the Court's case-law on the exhaustion of domestic remedies as well as the principle of subsidiarity of the Court.[129] The ECtHR also found that the domestic remedies had not been exhausted since the applicants could have applied for judicial review of the IPT's decision.[130] Ultimately, the judges found that the applicants had not provided the domestic courts with the opportunity of addressing, preventing or rectifying the alleged violation of Article 8 and 10.[131]

Overall, the analysis of the jurisprudence of the ECtHR examined so far shows that there is a tendency on the Court's part to base the application of the Convention on the location of the interference with people's rights rather than on the location of the individuals whose rights have been violated. In particular, the ECtHR has been more likely to find that the ECHR applies to individuals located in foreign States whose rights have been interfered with as a result of an act committed online if that act is considered to have happened on the territory of a contracting State. This fact represents a departure from the

---

[126] *Privacy International and Others v the United Kingdom* App no 46259/16 Admissibility Decision (ECtHR, 7 July 2020), paras 43, 46-48.

[127] 'In the context of the present case there is no doubt that addressing the question of jurisdiction called for an assessment of a number of highly complex legal and practical issues. However, the applicants appear to have conceded before the IPT that there was no jurisdiction and the IPT indicated in its "no determination" letter that it "has not been required to consider, and has not considered" the question of jurisdiction', ibid para 42.

[128] 'Taking into account the Court's subsidiary role, the nature of the common law system, the role of the IPT and the novelty of the issue before it, the Court considers that there can be no question that the applicants needed to argue the question of jurisdiction before the IPT in order to exhaust their domestic remedies', ibid para 43.

[129] ibid.

[130] 'As to the necessity of seeking judicial review in the circumstances the Court recalls that extraordinary remedies cannot, as a general rule, be taken into account for the purposes of applying Article 35 § 1 […] It also considers that it was not fully clear at the time the applicants made their application to this Court that pursuing a judicial review of the IPT decision was possible. However, it cannot overlook the fact that the first applicant did attempt such proceedings, was successful and that as a result judicial review proceedings concerning the complaint under section 5 of the Investigatory Powers Act 2016 are currently pending (see paragraph 21 above). As those developments concern the same case and one of the applicants as in the present application, in the circumstances the Court does not regard that attempt at judicial review as an extraordinary remedy and concludes it was therefore a remedy to be exhausted by the applicants' ibid para 46.

[131] ibid para 47.

jurisprudence of the Court on extraterritorial jurisdiction, as will be explained in the next section.

The ECtHR is, however, not alone in finding that the related human rights convention applies to individuals located in foreign States due to cross-border online activities. Indeed, the HRC issued declarations to a similar extent in its 2014 and 2015 Concluding Observations in relation to State surveillance operations conducted by the US, UK and France. In these Concluding Observations, the HRC stated that the ICCPR applies to surveillance operations conducted through the Internet by domestic security agencies both inside and outside the domestic territory of its Member States.[132] This statement could indicate that people located in foreign countries whose data have been subjected to surveillance operations committed by Member States of the ICCPR inside their territory or abroad might have ICCPR rights *vis a vis* those States.[133] Therefore, according to this view, a Member State could exercise jurisdiction according to article 2(1) of the ICCPR when it conducts online surveillance activities of foreign people's data both from within its domestic territory and outside. If this view is confirmed in the future practice of the HCR, it could be considered as an expansion of the concept of jurisdiction according to the ICCPR, which so far adhered to the spatial and personal model of jurisdiction. It might also be considered as an expansion of the meaning of jurisdiction compared to the ECtHR,

---

[132] 'The Committee is concerned about the surveillance of communications in the interest of protecting national security, conducted by the National Security Agency (NSA) both within and outside the United States […] through PRISM (collection of communications content from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic) and the adverse impact on individuals' right to privacy. […] While welcoming the recent Presidential Policy Directive/PPD-28, which now extends some safeguards to non-United States citizens "to the maximum extent feasible consistent with the national security", the Committee remains concerned that such persons enjoy only limited protection against excessive surveillance. Finally, the Committee is concerned that the persons affected have no access to effective remedies in case of abuse (arts. 2, 5 (1) and 17). […] The State party should: (a) Take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17' HRC Concluding observations on the fourth periodic report of the United States of America (23 April 2014) CCPR/C/USA/CO/4, [22]; 'The Committee is concerned: (a) that the Regulation of Investigatory Powers Act 2000 (RIPA), that makes a distinction between "internal" and "external" communications, provides for untargeted warrants for the interception of external private communication and communication data which are sent or received outside the United Kingdom without affording the same safeguards as in the case of interception of internal communications […] The State party should: (a) Review the regime regulating the interception of personal communications and retention of communication data […] with a view to ensuring that such activities, both within and outside the State party, conform to its obligations under the Covenant, including article 17', HRC Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland (17 August 2015) CCPR/C/GBR/CO/7 [24]; 'The Committee is concerned about the powers granted to the intelligence services for digital surveillance both within and outside France […] The State party should take all necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular article 17' HRC Concluding observations on the fifth periodic report of France (21 July 2015) CCPR/C/FRA/CO/5, [12].

[133] Gerald L. Neuman 'Has the Human Rights Committee Extended its Reach?' (*Just Security*, 29 July 2015) <https://www.justsecurity.org/25022/human-rights-committee-extended-reach/> accessed 26 March 2020.

which as observed above, appears keener to find an exercise of jurisdiction when the online surveillance operation happens within the territory of a Member State rather than abroad. Similarly to what has been observed in regard to the ECtHR, it remains to be seen which jurisdictional model might accommodate this new meaning of jurisdiction.[134] It is worth highlighting, however, that the HRC Concluding Observations do not equate to a finding of a violation of the ICCPR, nor do they represent the ultimate legal conclusions of the HRC.[135] Indeed, in the Follow Up on Concluding Observations on State Party Reports, a member of the HRC, Ms. Seibert Fohr, stated in relation to the Concluding Observations with regard to the United States that the Committee should limit 'its subsequent evaluation to measures taken with regard to surveillance activities within the United States'.[136] This might indicate a disagreement within the Committee as to the implications of applying the ICCPR to surveillance activities conducted outside the territory of a Member State.[137] Overall, as has been observed by some commentators, the Concluding Observations examined so far 'do not definitely establish that the committee has adopted a new definition of "jurisdiction" for purposes of article 2(1). They do suggest, however, that the committee might need to modify either its definition or its practice'.[138] As to the case-law of the HCR on cross-border Internet cases, unlike the ECtHR, there are no cases that deal directly with this issue. The case of *Griffiths vs Australia*, for example, had at its centre an act committed over the Internet, and in particular the production by an Australian resident, Mr Griffiths, of 'copies of software and computer games made available to download' for the members of an Internet group of which Mr. Griffiths was part.[139] Notwithstanding the fact that Mr Griffiths had operated from Australia, he was indicted with criminal copyright infringement and conspiracy to violate copyright laws by the US District Court for the Eastern District of Virginia. Indeed, the US Court found that the copyright infringement had happened in the United States based on the access-based jurisdictional criterion, as the material was downloaded by Internet users located there.[140] The jurisdictional issue of where the alleged copyright infringement had happened was debated before the Australian Courts as well and, notwithstanding an early determination by the New South Wales Court that the facts complained of had in fact happened in Australia, Mr Griffiths was subsequently

[134] ibid.
[129] ibid.
[136] HRC Follow-up on concluding observations on State party reports (22 July 2015) CCPR/C/SR.3183, [72].
[137] Neuman (n 133).
[138] ibid.
[139] *Griffiths vs Australia* (2014) U.N. Doc. CCPR/C/112/D/1973/2010, [2.1].
[140] ibid [2.2].

extradited to the United States.[141] This was following the finding by the Federal Court of Australia that the acts had happened within the US jurisdiction regardless of Mr Griffiths' physical presence in Australia.[142] The jurisdictional issue was however not debated before the HRC, as the applicant's complaint focused on a violation on Australia's part of articles 9, 13 and 14 of the ICCPR in relation to his detention in Australia before extradition and the lack of fairness in the extradition proceedings.[143] Therefore, it is possible to conclude that this case shows that the ICCPR is applied based on the spatial model of jurisdiction, as Mr Griffiths resided in Australia, rather than providing any insight on the meaning of online jurisdiction according to the ICCPR.

Finally, as far as the jurisprudence of the Inter-American Court and Commission on Human Rights and the African Court and Commission on Human and Peoples' Rights are concerned, there are no Internet-related cases to date that have been presented before the Courts. There are also no cases where the exercise of State jurisdiction in regard to cross-border online acts has been discussed. As far as the Inter-American system is concerned, some experts[144] have affirmed that the Inter-American Court on Human Rights has not yet had the opportunity to examine cases related to the impact of technology on human rights, while others have underlined, however, that Internet-related cases are being examined before the domestic courts of Latin America and that these cases will inevitably be brought before the Inter-American Court in the future.[145] In any case, both the Inter-American and the African human rights institutions have, however, recognised that the ACHR and the ACHPR apply offline as well as online and have issued various reports and declarations that deal with the protection of human rights online.[146] These documents will be discussed in the next Chapter.

5.5 Applying the spatial model and the personal model of jurisdiction to online acts

There are many difficulties associated with applying the spatial and personal model of jurisdiction contained in the human rights conventions to online acts. Some of these

[141] ibid [2.4]-[2.9].
[142] ibid [2.5]-[2.6].
[143] ibid [3.1]-[3.7].
[144] Maria Paz Canales, 'Repaso a la Jurisprudencia de la Corte Europea y las Altas Cortes de la region en materia de Internet', (03 May 2019) <https://vimeo.com/334638074> (accessed 12 August 2020).
[145] Guilherme Canela, 'Panel El Articulo 13 de la Convencion Inter-Americana y la protection de la libertad de expression en Internet', (03 May 2019) <https://vimeo.com/334638074> accessed 12 August 2020.
[146] See, for example, African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (OAU Banjul 2019), and Standards for a Free, Open and Inclusive Internet (n 79).

challenges pertain to the cross-border nature of the Internet, whereas others are linked to the uncertainties surrounding extraterritorial jurisdiction in human rights law. As observed in section 5.3, the Internet poses multiple challenges when it comes to establishing jurisdiction, one of the most difficult of which is related to the application of the territorial principle to un-territorial data[147] and the consequent need to "disentangle" Internet jurisdiction from territoriality.[148] While a jurisdictional principle that is ideal for the online environment has not been agreed upon, this is especially true for human rights law, where only recently some human rights courts have been confronted with complex cross-border online jurisdictional issues.[149] In particular, the cases presented before the ECtHR and the HCR show that online acts such as the publication of comments on websites managed by foreign companies or surveillance of Internet communications of foreign citizens are considered to have happened within the territory of the Member State exercising jurisdiction notwithstanding their non-physical, cross-border nature. This indicates that, similarly to domestic law, online acts are presented as territorial acts before human rights courts as well. The rationale for the application of the territorial principle to online acts, however, varies according to the specificities of each case. In particular, in *Liberty*, the interception of the Irish applicant's electronic communications operated by the UK Ministry of Defence had happened within the territory of the UK, and specifically from the Electronic Test Facility in Cheshire, using two British Telecommunications Radio Stations.[150] In this case, therefore, the non-physical act complained of had clear ties with the UK territory since the interception had been conducted from and using infrastructure located in the UK. The *Big Brother Watch* case is, in this respect, slightly different because in this case it is unclear where the bulk surveillance operations carried out by GCHQ took place. Indeed, the location of the Internet cable bearers accessed by GCHQ as well as the place from where GCHQ had accessed the bearers are not mentioned in the case. In regard to this last point, one could assume that CGHQ had operated from within the UK territory as the UK government never contested this point, however

[147] Daskal (n 44). See section 5.3 for a detailed analysis of the application of the territorial principle to Internet-related cases.
[148] Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (n 21) 49.
[149] See section 5.3 on the debate on whether an Internet-specific jurisdictional principle is desirable and also for a critical analysis of some of the most common ways that States have established jurisdiction online, including the access-based jurisdictional approach, the *Zippo* test and the targeting test.
[150] *Liberty and Others v the United Kingdom* (n 114) para 5. As to the Government's official position in relation to the location of the surveillance operations, at 47 the ECtHR stated that '[f]or security reasons, the Government adopted a general policy of neither confirming nor denying allegations made in respect of surveillance activities. For the purposes of this application, however, they were content for the Court to proceed on the hypothetical basis that the applicants could rightly claim that communications sent to or from their offices were intercepted at the Capenhurst ETF during the relevant period'.

whether that is the case for sure does not emerge from the proceedings before the ECtHR. On the other hand, in the *Griffiths*, *Perrin* and *Tamiz* cases, the territorial principle took the form of the access-based jurisdictional approach according to which the online content at the centre of the cases was considered to have been published within the territory of the US in the *Griffiths* case and UK in the *Perrin* and *Tamiz* cases, because it could be downloaded or viewed on computer screens located there. However, the access-based approach applied in the *Tamiz* case is a qualified one because the criteria used to establish whether the defamatory comments had been published in the UK relied on the number of readers that had accessed those comments in the domestic forum.[151] Finally, in *Weber and Saravia* the act complained of was the interception by German authorities of the applicants' telecommunications while they were located in Uruguay. There is no information in the case presented before the ECtHR regarding where the interception took place. The German government argued that since the applicants resided in Uruguay, the act had happened outside its territorial jurisdiction. As mentioned above, the ECtHR never pronounced on the issue as it found that the case was ill-founded on the merits.

From the analysis conducted above it emerges that the online acts at the centre of the cases brought before the ECtHR and the HRC have been characterized as acts that happened on the territory of the Member States exercising jurisdiction regardless of their non-physical cross-border nature. In some cases, such as *Liberty*, this characterization is furthered by the presence of clear links between the interception of foreign communication and the territory of the UK. In other cases, such as *Big Brother Watch* the online act is considered to have happened within the territorial jurisdiction of the UK notwithstanding the absence of information as to whether such physical links with the domestic territory existed. In this regard, the *Big Brother Watch* case is particularly useful as it clearly shows the difficulties associated with establishing where online acts take place. Indeed, as explained in the case, each single Internet communication is divided into packets of data which travel on many occasions separately within multiple Internet bearers via a combination of the cheapest and quickest route depending also on the location of the server.[152] Therefore, a communication between two individuals may cross the borders of multiple countries simultaneously. In any case, understanding how each Internet-related act that is at the centre of the cases has been presented before the ECtHR and the HCR is useful because it has an impact on how the Courts interpret these online acts. It is certainly true that, as the Research Division of the ECtHR stated, it is first and

[151] *Tamiz v UK* (n 88) para 39.
[152] *Big Brother Watch and Others v. the United Kingdom* (n 95) para 9.

foremost up to the Member States to establish when an act falls within their jurisdiction, and that therefore the Court will assume that a State has jurisdiction if this point is not contested by the parties.[153] However, whether an online act is considered to have happened on the territory of the Member States will have a direct impact on how the human rights Courts will interpret the jurisdictional issue and therefore on the meaning of State jurisdiction according to the related human rights conventions. This is especially true considering, as observed in section 5.4, that there is a tendency on the ECtHR's part on basing the application of the ECHR on the location of the interference rather than the location of the victim. In other words, the ECtHR has been more likely to find that the ECHR applies to individuals located in foreign States whose rights have been violated as a result of an act committed online if that act is considered to have happened on the territory of a Member State. Establishing jurisdiction based on the location of the interference, however, rather than that of the victim is a departure from both the personal and spatial models of jurisdiction of the human rights conventions.[154] This is because both models apply to individuals who are either in a territory controlled by a State Party to the human rights conventions or are subjected to the power or authority of that State. However, as will be shown below, this way of establishing jurisdiction is not new to the case-law of the human rights Courts. Before examining this point, however, it is important to highlight that, as stated in Chapter 4, unlike international law, jurisdiction in human rights law is related to the exercise of a factual power or authority by a State rather than to the legality of the use of power by that State. Therefore, the challenge of applying the human rights law models of jurisdiction to Internet-related cases is how to define when a State exercises a factual power or authority over individuals in the absence of physical power.

As far as applying the personal model of jurisdiction is concerned, this model could become particularly useful to deal with all those Internet-related cases where both the victim of an online violation and the violation itself are located outside the territory of the Member State, as happened in the *Privacy International* case.[155] This is because the personal model allows the bypass of the problem of the physical location of the victim to focus on the relationship between the latter and the State. This characteristic also renders the personal model *prima facie* better suited than the territorial model to deal with acts that happen on the Internet. However, as stated above, the main problem posed by the

[153] Internet: Case Law of the European Court of Human Rights (n 79) 4-5.
[154] Milanović, 'Human Rights Treaties and Foreign Surveillance' (n 106) 124-126.
[155] ibid 127-128.

personal model of jurisdiction is how to define power or control over an individual when the alleged violation is non-physical. Indeed, so far the acts that have been considered as an expression of the personal model of jurisdiction are mainly physical acts, such as arrest, detention and the use of force by the authorities of a State Party to the human rights conventions.[156] In order to apply the personal model of jurisdiction to online acts, such as, for example, surveillance of electronic communications of foreign citizens, it could be useful to focus on the effects of those non-physical acts over the victims and to equate their ability to affect the targeted individuals to the ability that a comparable physical action might have on them, such as search and seizures of communications.[157] In this regard, some have argued that the effective control test should be replaced by a virtual control test.[158] This would allow the inclusion of online State actions in the personal model of jurisdiction, such as the remote control of communications of foreign nationals, based on the fact that these acts render States' presence in certain contexts even more persistent than the corresponding control that States are able to exercise through physical actions.[159] The problem with translating the application of the personal model of jurisdiction to the cyberspace is that there is no non-arbitrary way of limiting the application of this model and therefore distinguishing what amounts to virtual control and what does not.[160] Indeed, it is not even clear which actions define the exercise of virtual control over individuals. Consequently, similarly to what happens for physical acts, the personal model of jurisdiction collapses because, in the absence of a non-arbitrary way of limiting its application, potentially all the virtual acts exercised by a State could be included in the meaning of jurisdiction with the result of not having a jurisdictional threshold at all.[161]

In regard to the application of the spatial model of jurisdiction to online acts, if both the victim of a human rights violation committed over the Internet and the violation itself happen in a territory controlled by a State, that State would certainly have jurisdiction according to the related human rights conventions.[162] This represents the most straightforward scenario for the application of the human rights conventions to online acts, such as for example a violation of the privacy of individuals who are subjected to

[156] See Chapter 4 section 4.4.2 for an in-depth discussion of the case-law related to the personal model of jurisdiction.
[157] Milanović, 'Human Rights Treaties and Foreign Surveillance' (n 106) 129.
[158] Peter Margulies 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2014) 82 Fordham L.Rev. 2137, 2151-2152.
[159] ibid.
[160] Milanović, 'Human Rights Treaties and Foreign Surveillance' (n 106) 128-129.
[161] ibid 129.
[162] ibid 122-124.

surveillance operations of their electronic communications while they are located in a territory controlled by the State and the surveillance is performed from within that territory. However, as mentioned above, there are difficulties associated with determining where an online act takes places since in many cases its location is unknown and the act itself by its nature is linked to multiple State simultaneously. In any case, if the State has control over the territory where an online human rights violation occurs, then it has the duty to both respect the human rights of the individuals who are in that territory and to secure those rights.[163] This means that both positive and negative human rights obligations apply, which implies that the State must adopt domestic laws to secure the protection of those rights within its territory. The State would also need to act in due diligence to prevent third parties located in that territory committing human rights violations.[164]

However, a more complicated scenario for the application of the spatial model of jurisdiction to online acts arises if the online human rights violation happens in a territory controlled by a State whereas the victim of the violation is in another country. As mentioned above, this is the scenario that the ECtHR has been confronted with more often with regard to online acts and in relation to which the Court found that the ECHR applied. Interestingly, this way of exercising jurisdiction is not new in the jurisprudence of the human rights courts, as there are various cases brought before the ECtHR and the HRC where the Courts found that their respective conventions applied to acts that happened within the domestic territory while the alleged victims were abroad.[165] Indeed, the cases *Gueye et al v France*, *Varela Nunez v Uruguay*, *Samuel Lichtensztejn v Uruguay*, *Mabel Pereira Montero v. Uruguay* and *Sophie Vidal Martins v. Uruguay* of the HCR and the cases *Sejdovic v. Italy*, *Mullai and Others v. Albania*, *Vrbica v Croatia* and *Markovic v. Italy* of the ECtHR are all related to the exercise by the States Parties of some form of legal power towards people located in foreign States. In particular, in *Gueye v France* the HRC found that the ICCPR applied to retired Senegalese members of the French armed forces residing in Senegal who claimed that they had been discriminated against as French legislation provided a different treatment in regard to their pension rights compared to retired French soldiers.[166] In *Varela Nunez v Uruguay*, *Samuel Lichtensztejn v Uruguay*,

[163] ibid 123.
[164] ibid.
[165] ibid 125.
[166] In regard to the jurisdictional point, the HCR observed that the Senegalese nationals 'are not generally subject to French jurisdiction, except that they rely on French legislation in relation to the amount of their pension rights'. This shows that the Committee found that France was indeed exercising jurisdiction over the Senegalese nationals via the domestic legislation that regulated their pensions *Gueye et al v France* (1989) U.N. Doc. CCPR/C/35/D/196/1985 (1989), [9.4].

Mabel Pereira Montero v. Uruguay and *Sophie Vidal Martins v. Uruguay* the HCR found that Uruguay was responsible for the exercise of jurisdiction over Uruguayan nationals that were living abroad due to its refusal to issue its citizens with a new passport. In all these cases, Uruguay claimed that the authors of the communications could not be considered to be within its jurisdiction as they resided abroad.[167] However, the HCR consistently dismissed this point since it stated that issuing a passport is clearly an exercise of State jurisdiction regardless of where in the world the recipient of the passport is located.[168] As to the ECtHR, the case *Vrbica v Croatia* is related to Croatia's failure to enforce a judgment that had been issued by Montenegrin courts against two Croatian companies in favour of the applicants which lived in Montenegro.[169] Conversely, the legal proceedings at the centre of the cases *Mullai and Others v. Albania*, *Sejdovic v. Italy* and *Markovic v Italy* took place in Albania and Italy respectively, while the applicants resided abroad. In *Mullai and Others v. Albania* the ECHR was found to apply to the refusal by Albanian authorities to enforce a court judgement which recognized the validity of a building permit in favour of the Albanian applicants notwithstanding the fact that some of them resided in Italy and in the US.[170] Similarly, in *Sejdovic v. Italy* the ECHR was found to apply to a trial of the applicant held *in absentia* by Italian courts while the applicant was in Germany.[171] Finally, the *Markovic v Italy* case shows that applicants located in the former Serbia and Montenegro had fair trial rights against Italy regarding legal proceedings before Italian Courts.[172] Overall, all the cases discussed show that the ECHR and the ICCPR apply to acts that happened within the territory of the Member States whose victims were abroad. What is unclear is which jurisdictional model justifies this application. A possible solution for the application of the spatial model in these cases might be interpreting the act that has happened within the territory of a Member State as having extraterritorial effects and therefore negatively affecting victims located abroad.[173] Some authors, however, have criticised this justification for the application of the spatial model of jurisdiction because they find it not conceptually sound, since any act that

---

[167] *Varela Nunez v Uruguay* (1983) U.N. Doc. CCPR/C/19/D/108/1981, [4.1]; *Samuel Lichtensztejn v Uruguay* (1983) U.N. Doc. CCPR/C/OP/2 at 102 (1990), [4.1]; *Mabel Pereira Montero v. Uruguay* (1983) U.N. Doc.CCPR/C/OP/2 at 136 (1990), [7.1]. In the case of *Sophie Vidal Martins v. Uruguay* (1980) U.N. Doc. Supp. No. 40 (A/37/40) (1982), Uruguay did not raise the jurisdictional point as the State never presented any submissions before the HRC [6.1]. Therefore, at [7] the HRC examined the jurisdictional point ex officio.

[168] *Varela Nunez v Uruguay* (n 167) [6.1]; *Mabel Pereira Montero v. Uruguay* (n 167) [5]; *Sophie Vidal Martins v. Uruguay* (n 167) [7].

[169] *Vrbica v Croatia* App no 32540/05/2010 (ECtHR, 1 April 2010).

[170] *Mullai and Others v. Albania* App no 9074/07 (ECtHR, 18 January 2012).

[171] *Sejdovic v. Italy* App no 56581/00 (ECtHR, 1 March 2006).

[172] *Markovic v Italy* App no 1398/03 (ECtHR, 14 December 2006).

[173] Milanović, 'Human Rights Treaties and Foreign Surveillance' (n 106) 126.

happens within the territory of a State can be said to have some extraterritorial consequences.[174] Interestingly, however, this theory is supported by the *Drozd and Janousek v. France and Spain* case of the ECtHR, where the Court stated that States exercise jurisdiction according to the Convention due to acts of their authorities that have extraterritorial effects.[175] Therefore, it does appear that the extraterritorial effects of acts committed within the domestic territory are relevant as far as determining whether a State exercises jurisdiction according to the ECHR. However, it is important to underline that in *Drozd and Janousek* the ECtHR was referring to the personal model of jurisdiction, rather than to the application of the territorial one.[176] This means that, following *Drozd and Janousek*, a State exercises jurisdiction when its authorities produce acts within the domestic territory that have effects abroad. The extraterritorial effects model of jurisdiction could be particularly useful when it comes to justifying the application of the personal model of jurisdiction to online acts. This is because according to the extraterritorial effects model, online acts could be interpreted as acts of the authorities of a State, such as State surveillance, that have extraterritorial effects and that therefore equate to the exercise of power over individuals located abroad. In other words, by interpreting online acts as acts that have extraterritorial effects it could be possible to bypass the impasse of the absence of physical power in the personal model of jurisdiction. The model of State jurisdiction based on extraterritorial effects of domestic acts however, seems to have been confirmed as a new stand-alone basis for the exercise of State jurisdiction in a relatively recent pronouncement of the IACtHR, the Advisory Opinion on Environment and Human Rights of the IACtHR. In particular, the Advisory Opinion of the Inter-American Court covers the meaning of extraterritorial jurisdiction with regard to the right to life and personal integrity. The Opinion was requested by Colombia with regard to States' obligations under the ACHR for infrastructure work that could significantly damage the marine environment in the Wider Caribbean Region. More specifically, the opinion is related to States' environmental obligations that derive from the duty to respect and ensure the rights to life and personal integrity under the ACHR.[177] In the Advisory Opinion, the Court recognized the exceptional nature of extraterritorial

[174] ibid.
[175] 'The term "jurisdiction" is not limited to the national territory of the High Contracting Parties; their responsibility can be involved because of acts of their authorities producing effects outside their own territory' *Drozd and Janousek v. France and Spain* App no 12747/87 (ECtHR, 26 June 1992), para 91; see also Marko Milanović, 'Human Rights Treaties and Foreign Surveillance' (n 106) 126.
[176] Milanović, 'Human Rights Treaties and Foreign Surveillance' (n 106) 126.
[177] *Medio Ambiente y Derechos Humanos*, Advisory Opinion OC-23/17 Inter-American Court of Human Rights (15 November 2017), [35], [38].

jurisdiction according to the ACHR.[178] It also found that States exercise extraterritorial jurisdiction when they exercise authority or effective control over people who are located either inside or outside their domestic borders, thus reinstating the spatial and personal models of jurisdiction.[179] However, the Court added an additional jurisdictional criterion, that of having effective control over acts carried out within the State's territory but that cause the violation of the rights of those who are located outside that State. In other words, according to article 1(1) of the ACHR, a State exercises extraterritorial jurisdiction over the people whose rights have been violated outside that State's borders if it had effective control over the actions carried out within its territory that caused the extraterritorial violation of those rights.[180] The difference between this new jurisdictional criterion and the effective control over people or territory is that in this case a State exercises jurisdiction even when it does not have any effective control over the territory or people whose rights are violated. Indeed, this jurisdictional link is based on having effective control over the actions carried out within the State's territory but that have extraterritorial effects. However, according to some commentators, although this new jurisdictional criterion broadens the concept of extraterritorial jurisdiction, it does not equate to the cause and effect jurisdiction that ECtHR dismissed in *Banković* according to which everyone who is adversely affected by an action of a State is within that State's jurisdiction, no matter where in the world they are located.[181] Indeed, according to this theory, the difference between the extraterritorial effects criterion and the cause and effect jurisdiction is that under the first a State is only responsible if it failed to prevent the action that caused the violation within its territory.[182] Some commentators believe that this principle broadens the due diligence principle and its main novelty is that it imposes

[178] See Chapter 4 section 4.3 for a discussion of this point.
[179] 'The concept of jurisdiction under Article 1(1) of the American Convention encompasses any situation in which a State exercises effective control or authority over a person or persons, either within or outside its territory' *Medio Ambiente y Derechos Humanos* (n 177) [104 e].
[180] 'The exercise of jurisdiction arises when the State of origin exercises effective control over the activities that caused the damage and the consequent human rights violation', ibid [104 h].
[181] 'In the first place, the applicants suggest a specific application of the "effective control" criteria developed in the Northern Cyprus cases. They claim that the positive obligation under Article 1 extends to securing the Convention rights in a manner proportionate to the level of control exercised in any given extra-territorial situation. The Governments contend that this amounts to a "cause-and-effect" notion of jurisdiction not contemplated by or appropriate to Article 1 of the Convention. The Court considers that the applicants' submission is tantamount to arguing that anyone adversely affected by an act imputable to a Contracting State, wherever in the world that act may have been committed or its consequences felt, is thereby brought within the jurisdiction of that State for the purpose of Article 1 of the Convention' *Banković and others v Belgium and others* App no 52207/99 (ECtHR, 12 December 2001), para 75; Antal Berkes 'A New Extraterritorial Jurisdictional Link Recognised by the IACtHR' (*EJIL: Talk!*, 28 March 2018) <https://www.ejiltalk.org/a-new-extraterritorial-jurisdictional-link-recognised-by-the-iacthr/> accessed 15 April 2020.
[182] Berkes (n 182).

both positive and negative obligations on States with regard to extraterritorial effects. This is because not only States need to refrain from violating the rights of those who are abroad, but they have to take reasonable steps to protect those rights, by for example preventing that companies within their territory violate them.[183] The main problem of this new jurisdictional criterion, is the absence of clear limits regarding its application. Indeed, the ACtHR failed to clarify how serious the adverse impact of the act with extraterritorial effects need to be for the State's jurisdiction to apply. Other points that need clarification are also whether this jurisdictional criterion applies to all the rights under the ACHR or only to the right to life and how to determine that a causal link exists between the domestic act and the extraterritorial consequences.[184] This points will need to be clarified by the ACHR in the immediate future for this jurisdictional link to apply.

Overall, the extraterritorial effects jurisdictional principle seems the best equipped to deal with online jurisdiction, because it is the principle that best adapts to the non-physical nature of the online environment. Whether this principle will receive enough traction in the jurisprudence of the human rights Courts for it to be applied consistently to online acts remains, however, to be seen.

5.6 Conclusions

The analysis conducted in this chapter shows that there are multiple challenges associated with establishing jurisdiction online. The territorial principle is one of the jurisdictional principles that are applied more often in domestic law with regard to Internet-related cases. However, the un-territoriality of data shows that there is a clear need to disentangle Internet jurisdiction from territoriality. The jurisprudence of the human rights courts shows that there are very few Internet-related cases where the jurisdictional issue has been examined by the Courts, with the ECtHR as the only human rights court that has been presented with these issues more frequently. Notwithstanding the small number of cases, a tendency has emerged in the jurisprudence of the ECtHR to establish that States have jurisdiction in Internet-related cases based on the location of the violation rather than that of the victim. Although this represents a departure from both the personal and spatial models of jurisdiction, establishing jurisdiction based on the location of a violation is supported from the jurisprudence of both the HRC and the ECtHR. Since the application of both the personal and spatial models of jurisdiction to online acts presents difficulties

[183] ibid.
[184] ibid.

related mainly to establish how States exercise power or control over individuals in the absence of physical power, the extraterritorial effects model of jurisdiction seems more promising. Indeed, this model, which can be seen as both an adaptation of the personal model of jurisdiction or as a new jurisdictional head, is better suited for the online environment. This is because by interpreting online acts as acts that have extraterritorial effects this model allows to reflect the ability of non-physical acts to negatively impact on the rights of people located in foreign States. This model, however, is not immune from criticalities, such as the fact that it is not clear how to limit its application and how to define when an online act is able to have extraterritorial effects abroad.

6. Compliance of the Extraterritorial Application of Domestic Laws with Freedom of Expression Provisions in International Human Rights Law

6.1 Introduction

This chapter aims to answer the second research question: are the extraterritorial exercises of State jurisdiction over online content examined in Chapters 2 and 3 compliant with the freedom of expression provisions contained in the human rights Conventions? In particular, this chapter aims to understand whether these exercises of jurisdiction are compliant with the accessibility and foreseeability requirements that laws restricting freedom of expression must respect so that they can be considered as prescribed by law according to the European Convention of Human Rights (ECHR), the International Covenant on Civil and Political Rights (ICCPR), the American Convention of Human Rights (ACHR) and the African Charter of Human and Peoples' Rights (ACHPR). To answer this question, section two will illustrate the framework for the protection of freedom of expression both offline and online, while section three will investigate the permissible restrictions to freedom of expression according to the human rights Conventions, with a focus on the meaning of 'prescribed by law' according to the Courts' jurisprudence. Section four will investigate the claim that the extraterritorial exercises of jurisdiction over online content illustrated in Chapters 2 and 3 cannot be considered compliant with the accessibility and foreseeability requirements of the freedom of expression provisions. The analysis will highlight the necessity to adapt the interpretation of these requirements in a way that takes into account the global nature of content published online. Finally, section five will summarise the main conclusions reached.

6.2 The right to freedom of expression offline and online according to the ECHR, the ICCPR, the ACHPR and the ACHR

Freedom of expression is one of the fundamental human rights protected by human rights conventions.[1] The protection of freedom of expression is considered to be paramount to

[1] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 19; Convention for the Protection of Human Rights and Fundamental Freedom (adopted 4 November 1950,

the functioning of any democratic society, as well as to the enjoyment of other human rights.[2] This is especially true considering the dual dimension of this right, which is an individual as well as a collective right, as it enables not only individuals but also social groups to express their views and beliefs.[3] In this regard, freedom of expression is considered as a 'multiplier or meta right' because the fulfilment of freedom of expression facilitates the enjoyment of many other human rights.[4] The articles related to freedom of expression in the European Convention on Human Rights (ECHR), the International Covenant on Civil and Political Rights (ICCPR), the American Convention on Human Rights (ACHR) and the African Charter on Human and Peoples' Rights (ACHPR) follow

---

entered into force 03 September 1953) 213 UNTS 221 (European Convention on Human Rights) art 10; International Convention on the Elimination of All Forms of Racial Discrimination (adopted 7 March 1966, entered into force 12 March 1969) UNTS 660 195 art 5; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 19; American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 (Pact of San José) art 13; African Charter on Human and Peoples' Rights (entered into force 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217 (African Charter) art 9; Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC) art 12 and 13.

[2] HRC General Comment No. 34 (12 September 2011) CCPR/C/GC/34, [2]; *Law Offices of Ghazi Suleiman v. Sudan*, Comm. 220/98, 15th ACHPR AAR Annex V (2001-2002), [40]; *Media Rights Agenda v. Nig.*, Comm. 105/93, 128/94, 130/94, 152/96, 12th ACHPR AAR Annex V (1998-1999), [54]; *Monim Elgak, Osman Hummeida and Amir Suliman v Sudan*, Comm. 379/09, https://www.achpr.org/public/Document/file/English/achpr15eos_decision_379_09_eng.pdf accessed: 4 September 2020, [114]; *Open Society Justice Initiative v. Cameroon*, Comm. 290/2004, 20th ACHPR AAR Annex IV (2006-2007), [126]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (OAU Banjul 2019), Principle 1; Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, Strasbourg: Council of Europe Publishing, 2013. ISBN 978-92-871-7702-5, 24; Dominika Bychawska-Siniarska, Protecting the Right to Freedom of Expression under the European Convention on Human Rights, Strasbourg: Council of Europe, 2017, 11; *Handyside v UK* App no 5493/72 (ECtHR, 7 December 1976), para 49; *Hertel v. Switzerland* App no 25181/94 (ECtHR, 25 August 1998) para 46; *Steel and Morris v. the United Kingdom* App no 68416/01 (ECtHR 15 May 2005) para 87; *Stoll v Switzerland* App no 69698/01 (ECtHR, 10 December 2007) para 101; The United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet' (1 June 2011), Preamble; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (31 December 2013), [1]; *Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism*, Advisory Opinion OC-5/85 Inter-American Court of Human Rights Series A No. 5 (13 November 1985), [70]; *Claude-Reyes et al. v. Chile*, Inter-American Court of Human Rights Series C No 151 (19 September 2006), [85]; *Herrera-Ulloa v. Costa Rica*, Inter-American Court of Human Rights Series C No 107 (2 July 2004), [112]; *Ricardo Canese v. Paraguay*, Inter-American Court of Human Rights Series C No 111 (31 August 2004), [82]; *Ríos et al. v. Venezuela*, Inter-American Court of Human Rights Series C No 194 (29 January 2009), [105]; *Perozo et al. v. Venezuela*, Inter-American Court of Human Rights Series C No 195 (28 January 2009) [116].

[3] HRC, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Mr. Frank La Rue (20 April 2010) A/HRC/14/23, [29]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (15 March 2017), [71].

[4] Michael O'Flaherty, 'Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No 34' (2012) 12(4) HRLRev 627, 632.

roughly the same scheme. They first illustrate the scope of the right and then list the circumstances under which it is permissible to limit the enjoyment of freedom of expression.[5]

As to the scope of the right to freedom of expression, this right includes freedom of opinion, also defined as freedom of thought, freedom to express one's opinion, i.e. freedom of expression, and freedom of information.[6] Unlike the other freedoms associated with freedom of expression, freedom of opinion enjoys absolute protection. Indeed, article 19(1) of the ICCPR expressly mentions that freedom of opinion cannot be subjected to limitations.[7] This also applies to the ECHR and to the ACHPR.[8] As to the American Convention on Human Rights, Article 13 does not expressly mention that freedom of thought cannot be subjected to restrictions. However, article 13(1) states that the right to freedom of thought and expression includes the right to seek, receive and impart information and ideas, whereas article 13(2) states that the exercise of the right listed in 13(1) can be subjected to restrictions. The right to seek, receive and impart information and ideas, however, is different from freedom of thought, because freedom of thought is the freedom to have an opinion rather than to seek, receive and impart one. It can therefore be assumed that when article 13(2) states that the rights listed in 13(1) can be subjected to restrictions, the rights affected by these restrictions are the rights to seek, receive and impart information rather than the right to freedom of thought. This assumption finds confirmation in a document published by the Office for the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights. Indeed, the report, The Inter-American Legal Framework Regarding the Right to Freedom of Expression states that

[5] In this regard, however, the African Charter on Human and Peoples Rights represents an exception, since Article 9 introduces the right for every individual to receive information and express and disseminate their opinions without referencing any permitted restrictions of this right. However, a list of justifiable limitations to the right of freedom of expression according to Article 9 is contained in Principle 9 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (n 2).

[6] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 10; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [68]; HRC General Comment No. 34 (n 2), [11]; Benedek and Kettemann (n 2) 23-24; Bychawska-Siniarska (n 2) 13-15.

[7] ICCPR (n 1) art 19(1); HRC General Comment No. 34 (n 2), [9]-[10]. As to the African Charter on Human and Peoples' Rights, article 8 does not expressly mention freedom of opinion, as the article refers to freedom of conscience. However, the Declaration of Principles on Freedom of Expression and Access to Information in Africa (n 2) affirms in Principle 2 that freedom of opinion is indispensable to the exercise of freedom of expression and that this freedom cannot be subjected to any restrictions.

[8] Benedek and Kettemann (n 2) 27; Bychawska-Siniarska (n 2) 13; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 2.

'[t]he legal framework of the Inter-American system for the protection of human rights is probably the international framework that provides the greatest scope and the broadest guarantees of protection to the right to freedom of thought and expression […] From a comparative perspective, when the texts of Article 13 of the American Convention, Article IV of the American Declaration, and Article 4 of the Inter-American Democratic Charter are contrasted with the relevant provisions of other international human rights treaties–specifically with Article 19 of the International Covenant on Civil and Political Rights or with Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms—it is clear that the Inter-American framework was designed by the American States to be more generous and to reduce to a minimum the restrictions to the free circulation of information, opinions and ideas'.[9]

It therefore follows that if the ECHR, the ICCPR and the ACHPR grant absolute protection to the right of freedom of thought, it is reasonable to assume that the ACHR does the same.

As to freedom of information, this can be defined as the right to impart and also receive information and ideas. Given the crucial role played by the media in a democratic society, freedom of information is usually associated with the right of the media to provide the public with information and with the corresponding right of the public to receive it.[10] In regard to freedom of expression, this right is considered to have horizontal effects in that not only States but also third parties, such as private companies, media owners and intermediaries should refrain from violating people's freedom of expression rights.[11] It follows that States have a positive obligation to protect individuals from freedom of expression violations perpetrated by third parties.[12]

The protection of the right to freedom of expression extends to both the content of the expression and the means by which this is communicated. Indeed, many forms of expression such as political discourse, commentary, canvassing, discussions on human rights, journalism, cultural expression, teaching and religious discourse are included in the protection.[13] Artistic expression is also protected[14], together with information that is

[9] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (30 December 2009), [3]-[4].

[10] 'Not only does the press have the task of imparting such information and ideas: the public also has a right to receive them', *Lingens v Austria* App no 9815/82 (ECtHR, 8 July 1986) para 41; Bychawska-Siniarska (n 2) 14.

[11] Benedek and Kettemann (n 2) 24.

[12] *Fuentes Bobo v Spain* App no 39293/98 (ECtHR, 29 February 2000) para 38; *Dink v Turkey* App no 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09 (ECtHR, 14 September 2010) para 106; Benedek and Kettemann (n 2) 24-25; HRC General Comment No. 34 (n 2), [7].

[13] HRC General Comment No. 34 (n 2), [11].

[14] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 10; American Convention on Human Rights (n 1) art 13(1); ICCPR (n 1) art 19(2); HRC General Comment No. 34 (n 2), [11]; Benedek and Kettemann (n 2) 33; Bychawska-Siniarska (n 2) 14.

false, or offends, shocks or disturbs.[15] A special degree of protection is reserved for political speech and speech related to questions of public interest, speech regarding candidates for public office and the way in which public officials perform their duties, and speech associated to the identity and dignity of the person.[16] It follows that States should be particularly mindful of any restriction that they impose on this type of speech, given the special role played by it in a democratic society. Commercial speech is also included in the category of protected expression,[17] although to a lesser extent than political speech. The ECtHR, for example, grants States a wider margin of appreciation when it comes to restricting commercial speech compared to political expression.[18] As to the means by which information and ideas are expressed, oral, written and printed expression are protected, together with any other form of communication.[19] However, in regard to the ICCPR, some commentators have observed that while it is clear that article 19 covers all forms of verbal and artistic expression, it is unclear whether it covers non-verbal forms as well. More specifically, while some forms of non-verbal expression such as raising a banner have been considered by the HRC as protected expression, others such as the defacement of road signs have been excluded from the scope of article 19.[20] It is

[15] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 23(3); *Ríos et al. v. Venezuela* (n 2), [105]; *Perozo et al. v. Venezuela* (n 2), [116]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [72]; HRC General Comment No. 34 (n 2), [11]; *Handyside v UK* (n 2), para 49; Benedek and Kettemann, (n 2) 23-24; Bychawska-Siniarska (n 2) 75-77.

[16] *Tristán Donoso vs. Panama*, Inter-American Court of Human Rights Series C No 193 (27 January 2009), [115]; *Palamara-Iribarne v. Chile*, Inter-American Court of Human Rights Series C No 135 (22 November 2005), [83]; *Herrera-Ulloa v. Costa Rica* (n 2) [82]; *Kimel v. Argentina*, Inter-American Court of Human Rights Series C No 177 (2 May 2008) [87]-[88]; *Usón Ramírez v. Venezuela*, Inter-American Court of Human Rights Series C No 207 (20 November 2009), [83]; *López-Álvarez v. Honduras*, Inter-American Court of Human Rights Series C No 141 (1 February 2006), [169]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [32]-[56]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 21 (1)(b); *Bodrožić v. Serbia and Montenegro* (2005) U.N. Doc. CCPR/C/85/D/1180/2003, [7.2]; HRC General Comment No. 34 (n 2), [34]; O'Flaherty (n 4) 637; Benedek and Kettemann (n 2) 49; *Wingrove v. the United Kingdom* App no 17419/90 (ECtHR, 25 November 1996) para 58; *Mouvement Raëlien Suisse v Switzerland* App no 16354/06 (ECtHR, 13 July 2012) para 61; *Ceylan v Turkey* App no 23556/94 (ECtHR, 8 July 1999) para 34; Research Division of the European Court of Human Rights, Internet: Case Law of the European Court of Human Rights, Council of Europe/European Court of Human Rights, 2015, 32.

[17] HRC General Comment No. 34 (n 2), [11]; *Ballantyne, Davidson, McIntyre v. Canada* (1993) U.N. Doc. CCPR/C/47/D/359/1989 and 385/1989/Rev.1 (1993), [11.3].

[18] Bychawska-Siniarska (n 2) 14.

[19] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 10; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [19]-[29]; Bychawska-Siniarska (n 2) 17-18; HRC General Comment No. 34 (n 2), [12].

[20] O'Flaherty (n 4) 638. Regarding raising a banner as a form of protected expression see *Kivenmaa v Finland* (1994) U.N. Doc. CCPR/C/50/D/412/1990 (1994), [9.3]. As to the defacement of road signs see *S.G. v France* (1991) U.N. Doc. CCPR/C/43/D/347/1988 at 8 (1991), [5.2].

also unclear whether hunger strikes and expression through clothes as well as forms of expression of gender identity are included in the protection offered by article 19.[21]

A right that is also associated with the right to freedom of expression is the right of access to information. This right is included in the protection of freedom of expression guaranteed by article 13 of the ACHR, article 19 of the ICCPR, article 9 of the ACHPR and article 10 of the ECHR.[22] However, in regard to the latter, the recognition of the right of access to information as part of article 10 is a relatively recent development. Indeed, the original position of the ECtHR was that the right to receive information, from which the right of access to information derives, included only a negative obligation for States not to interfere with people's freedom to receive information rather than a positive one to grant people access to documents held by public authorities.[23] For this reason, the right of access to information was first associated with the right to respect for private and family life granted by article 8 of the ECHR, especially in the Court's case-law on environmental and health-related issues.[24] However, in more recent case-law the ECtHR broadened its interpretation of the freedom to receive information recognising that the public authorities' refusal to grant access to information that they held constituted a violation of article 10 of the ECHR.[25] As to the scope of the right of access to information, this right shares with freedom of expression the dual nature of individual and collective right as well as the central role in facilitating the enjoyment of other human rights.[26] The right of access to information gives people the right to access information held by public

---

[21] O'Flaherty (n 4) 638-639. In regard to the possibility of considering hunger strike as a form of protected expression, the Human Rights Committee in *Baban v Australia* (2003) U.N. Doc. CCPR/C/78/D/1014/2001 (2003) was asked to examine the issue. However, at [6.7] it declared the application inadmissible as it was not sufficiently substantiated. As to clothes, in the case *Hudoyberganova v. Uzbekistan* (2004) U.N. Doc. CCPR/C/82/D/931/2000 (2004) the Human Rights Committee found that the State's refusal to allow a student to wear hijab was a violation of her right to freedom of religion. As to whether the refusal was also a violation of article 19, the HCR found at [5.3] that the author of the communication had failed to substantiate the claim. For this reason, the application was considered inadmissible in this regard.

[22] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 26; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [163]; HRC General Comment No. 34 (n 2), [18]; Bychawska-Siniarska (n 2) 15; *Társaság a Szabadságjogokért v. Hungary* App no 37374/05 (ECtHR, 14 July 2009) para 35; *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria* App no 39534/07 (ECtHR, 28 February 2014) para 41.

[23] Internet: Case Law of the European Court of Human Rights (n 16), 41.

[24] Internet: Case Law of the European Court of Human Rights (n 16), 42-43; *Guerra and Others v. Italy* App no 14967/89 (ECtHR, 19 February 1998) para 60; *McGinley and Egan v. the United Kingdom* App no 21825/93 23414/94 (ECtHR, 9 June 1998) para 101.

[25] Internet: Case Law of the European Court of Human Rights (n 16), 41; *Guerra and Others v. Italy* (n 24) para 60; *Társaság a Szabadságjogokért v. Hungary* (n 22) para 35; *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria* (n 22) para 41; *Youth Initiative for Human Rights v. Serbia* App no 48135/06 (ECtHR, 25 September 2013) para 20.

[26] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [163]-[164].

authorities in a timely and inexpensive manner and following the principles of maximum and proactive disclosure.[27] The principle of maximum disclosure establishes that all information held by public authorities must be subject to disclosure and that restrictions on access should be the exception rather than the norm. Besides, these restrictions should be narrowly defined, provided by law and should also comply with human rights law.[28] At the same time, according to the principle of proactive disclosure, public and relevant private bodies should make information of public interest available even without a specific request from the public.[29] Similarly to freedom of expression, the right of access to information is not absolute as it can be subjected to restrictions. These, however, must follow the three-part test developed by human rights Courts regarding legitimate limitations to freedom of expression which will be examined in more detail in the next section. In addition, any exception to the right of access to information can only apply when there is a risk of substantial harm to the protected interest and the harm is greater than the public interest in accessing the information.[30]

Lastly, as mentioned in the previous chapter, the protection of freedom of expression is of paramount importance not only offline but also in the online environment. In this regard, various commentators and authorities in the field of freedom of expression have underlined how the norms regarding freedom of expression of the human rights conventions apply to the Internet as well.[31] Similarly to freedom of expression offline, freedom of expression on the Internet is considered as a facilitator for the fulfilment of

---

[27] Organisation of American States, 'Model Inter-American Law on Access to Public Information' General Assembly Res AG/RES. 2607 (XL-O/10) (8 June 2010), [2]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 26 (1) (a), Principle 26 (1) (b), Principle 28, Principle 29; HRC General Comment No. 34 (n 2), [19]; UNGA, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (4 September 2013) A/68/362, [76].

[28] Organisation of American States, 'Model Inter-American Law on Access to Public Information' (n 27), [2]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [168]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 28; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (n 27), [76].

[29] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 29.

[30] African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 33; Organisation of American States, 'Model Inter-American Law on Access to Public Information' (n 27), [41]; HRC General Comment No. 34 (n 2), [19]; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (n 27), [75]-[76]; Bychawska-Siniarska (n 2) 17; Internet: Case Law of the European Court of Human Rights (n 16), 43.

[31] Yaman Akdeniz, Freedom of Expression on the Internet, Vienna: The Representative on Freedom of the Media, 2012. ISBN 978-92-9234-638-6, 50; Joint Declaration on Freedom of Expression and the Internet (n 2), [1] (a); Benedek and Kettemann (n 2) 24, 29; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [97].

other human rights.[32] In this regard, the ECtHR affirmed in the *Times Newspapers Ltd (nos. 1 and 2) v. The United Kingdom* case that '[i]n light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally'.[33] These concepts have been echoed by the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights, who affirmed that the Internet has democratised freedom of expression.[34] By making it possible for a greater number of people to express their opinion, the Internet has made public debate more accessible and less controlled by professional journalists who used to act as gatekeepers.[35] At the same time, however, various commentators and human rights courts have underlined how the Internet has the potential of amplifying the negative impact of problematic speech.[36] The ECtHR, for example, in the case *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* affirmed that online content poses a greater risk to the enjoyment of human rights compared to that posed by the press and that this justifies a different regulation of content posted on the two media.[37] In addition, the special characteristics of the Internet, more specifically its impact, accessibility, durability and asynchronicity must be taken into account when protecting and promoting freedom of expression online.[38]

An argument that is usually discussed in relation to freedom of expression on the Internet is the right of access to the Internet. The Special Rapporteurs on Freedom of Expression of the Organisation for Security and Cooperation in Europe (OSCE), the United Nations

---

[32] Wolfgang Benedek and Kettemann, (n 2) 18; M Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 187; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [2]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [2], [5]; African Commission on Human and Peoples' Rights 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa' (Banjul 2016) ACHPR/Res.362(LIX)2016.

[33] *Times Newspapers Ltd (nos. 1 and 2) v. The United Kingdom* App no 3002/03 23676/03 (ECtHR, 10 June 2009) para 27.

[34] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [80]-[81]; The African Commission on Human and Peoples' Rights 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa' (Banjul 2019).

[35] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [81].

[36] Akdeniz (n 31) 19; Benedek and Kettemann (n 2) 25.

[37] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* App no 33014/05 (ECtHR, 5 August 2011) para 63.

[38] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* (n 37) para 63; Benedek and Kettemann (n 2) 25, 27.

(UN), the Organisation of American States (OAS) and the African Commission on Human and Peoples' Rights have affirmed that in order to fulfil freedom of expression States have an obligation to promote universal access to the Internet.[39] This seems to suggest that access to the Internet can be considered a human right because, as stated by the Special Rapporteurs, due to the centrality of the Internet in everyday life, Internet access is fundamental to the realisation of other human rights, such as the right to education, assembly and free elections.[40] However, there are contrasting opinions regarding whether access to the Internet can be considered as a human right. The International Group of Experts who produced the Tallinn Manual 2.0, for example, have argued that access to the Internet is not a human right according to customary international law since technology is an enabler of rights, rather than a right in and of itself.[41] However, one point where there is consensus is the necessity for States to respect the guarantees contained in human rights conventions when restricting access to the Internet.[42] In particular, as showed by the *Yildirim v Turkey* and the *Kalda v Estonia* case of the ECtHR, States need to respect the limits contained in article 10(2) ECHR when imposing restrictions on access to the Internet or specific websites.[43]

After having examined the contextual framework regarding the protection of freedom of expression both offline and online, the next section will explore the conditions under which it is possible to limit the enjoyment of this right, with a special focus on the meaning of the expression 'prescribed by law'.

---

[39] Joint Declaration on Freedom of Expression and the Internet (n 2), 6(a). See also The African Commission on Human and Peoples' Rights 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa' (n 34); Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [84].

[40] Joint Declaration on Freedom of Expression and the Internet (n 2), 6(a); Benedek and Kettemann (n 2) 42.

[41] Schmitt (n 32) 195; Benedek and Kettemann (n 2) 42.

[42] Schmitt (n 32) 195; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (n 3), [86]-[90]; The African Commission on Human and Peoples' Rights 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa' (n 34); African Commission on Human and Peoples' Rights 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa' (n 32); The African Commission on Human and Peoples' Rights 'Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the situation of freedom of expression and access to information in the Republic of Zimbabwe' (Banjul 2019); African Commission on Human and Peoples' Rights' Press Release on the growing trend of stringent regulation of the internet in East African States' (Banjul 2018); Council of Europe Committee of Ministers, Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, Appendix to Recommendation CM/Rec(2016)5, [2.1.6].

[43] *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013); *Kalda v Estonia* App no 17429/10 (ECtHR, 6 June 2016); *Cengiz et al. v. Turkey* App no 48226/10 14027/11 (ECtHR, 1 March 2016).

6.3 Restrictions to freedom of expression and the meaning of 'prescribed by law'

As mentioned in the previous section, the right to freedom of expression, both offline and online, is not absolute since it can be subjected to restrictions. These restrictions, however, need to respect specific conditions set in the ECHR, the ICCPR, the ACHR and the ACHPR so that they can be justified according to these conventions. In particular, restrictions on freedom of expression must be prescribed by law, pursue one of the legitimate aims listed in the human rights conventions and be necessary and proportionate to the legitimate aim pursued.[44] All these conditions, which are also known as legality, legitimacy and proportionality respectively, must be met simultaneously so that a restriction can be justified according to the human rights conventions and the burden of proof of the conformity of a restriction with the Conventions is with the State.[45] Out of these three conditions, legality and legitimacy have a particular importance. Indeed, if, for example, a restriction pursues a legitimate aim but is not prescribed by law nor proportionate to the aim pursued, the restriction is found to be in violation of the human rights conventions.[46]

The first condition that a restriction on freedom of expression must fulfil to be justified according to the ECHR, the ICCPR, the ACHR and the ACHPR is legality, which means that the restriction must be prescribed by law. The expression 'prescribed by law' indicates that the restriction must have some basis in the domestic law. [47] As to a

---

[44] Douwe Korff and Ian Brown, 'Social Media and Human Rights' in Human Rights in a Changing Media Landscape, Strasbourg: Council of Europe Publishing, 2011. ISBN 978-92-871-7198-6, 185; Douwe Korff, The rule of law on the Internet and in the wider digital world, Council of Europe Commissioner for Human Rights, 2014, 10; Council of Europe Committee of Ministers, Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, [3]; Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom (n 42), [2.4.1]; Information Society Department Directorate General Human Rights and Rule of Law, Freedom of Expression in 2018, Council of Europe, 2019, 17; Council of the European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, Brussels, 2014, [20]; Bychawska-Siniarska (n 2) 33; HRC General Comment No. 34 (n 2), [21]-[22]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [52], [55]; *Herrera-Ulloa v. Costa Rica* (n 2), [120]; *Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism* (n 2) [35]; *Francisco Martorell v Chile*, Inter-American Court of Human Rights Series L V II.95 (3 May 1996), [55]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [61], [68]; *Kimel v. Argentina* (n 16) [54]; *Palamara-Iribarne v. Chile* (n 16) [79]; *Tristán Donoso vs. Panama* (n 16), [110]; *Ríos et al. v. Venezuela* (n 2), [106]; *Perozo et al. v. Venezuela* (n 2), [117]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9.

[45] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [68]; Bychawska-Siniarska (n 2) 33; HRC General Comment No. 34 (n 2), [27].

[46] Benedek and Kettemann (n 2) 47.

[47] *Yildirim v Turkey* (n 43) para 57; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [58].

definition of law, the Inter-American Court of Human Rights has explained that law is 'a general legal norm […] passed by democratically elected legislative bodies established by the Constitution, and formulated according to the procedures set forth by the constitutions of the States Parties'.[48] Although the term law certainly includes written rules adopted by Parliament, restrictions to freedom of expression can also be based on unwritten rules, such as the common law of contempt of court, on the rules of public international law and on the law of parliamentary privilege.[49] Conversely, restrictions based on administrative orders[50], or traditional, religious and other similar customary law are not admitted within the definition of prescribed by law.[51] The expression prescribed by law, however, does not refer only to the necessity that a law exists that foresees a given restriction. It also refers to specific qualities that the law must possess to be considered as such. In particular, the law imposing a restriction on freedom of expression must be sufficiently accessible to the individuals concerned, foreseeable, compatible with the rule of law and applied by an independent body in a non-arbitrary and non-discriminatory way.[52] In order to comply with the accessibility requirement it is sufficient that the law is made public, which means that it is published[53] or, in the case of international law, it is

---

[48] *The Word 'Laws' in Article 30 of the American Convention on Human Rights*, Advisory Opinion OC-6/86 Inter-American Court of Human Rights Series A No. 6 (9 May 1986), [38]. This definition of law applies specifically to article 30 of the American Convention of Human Rights. However, at [17] the Inter-American Court clarified that 'the criteria of Article 30 are applicable to all those situations where the word "laws" or comparable expressions are used in the Convention in referring to the restrictions that the Convention itself authorizes with respect to each of the protected rights'.

[49] Bychawska-Siniarska (n 2) 39; *The Sunday Times v. the United Kingdom (no. 1)* App no 6538/74 (ECtHR, 26 April 1979) paras 46-53 where the ECtHR found that the law of contempt of court can be considered as law within the meaning of article 10(2) of the ECHR; *Groppera Radio Ag and Others v. Switzerland* App no 10890/84 (ECtHR, 28 March 1990) para 68 in regard to the compliance of international telecommunications law with the requirement of prescribed by law of article 10(2) of the ECHR; HRC General Comment No. 34 (n 2), [24]; *Robert W. Gauthier v. Canada* (1999) UN Doc CCPR/C/65/D/633/1995 (1999), [13.5] regarding the compliance of the law of parliamentary privilege with the prescribed by law requirement of article 19(3).

[50] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [58].

[51] HRC General Comment No. 34 (n 2), [24].

[52] Bychawska-Siniarska (n 2) 39-43; HRC General Comment No. 34 (n 2), [25]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [58]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [69]; Benedek and Kettemann (n 2) 45; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [56]; *Yildirim v Turkey* (n 43) para 57.

[53] *The Sunday Times v. the United Kingdom (no. 1)* (n 49) para 49; *Kokkinakis v. Greece* App no 14307/88 (ECtHR, 25 May 1993) para 40; *G. V. France* App no 15312/89 (ECtHR, 27 September 1995) para 25; *Müller and Others v. Switzerland* App no 10737/84 (ECtHR, 24 May 1988) para 29; *Custers, Deveaux and Turk v. Denmark* App no 11843/03, 11847/03 and 11849/03 (ECtHR, 3 August 2008) paras 82-83; Directorate of the Jurisconsult, Guide on Article 7 of the European Convention on Human Rights, 2020, [26]. Although this guide examines *inter alia* the meaning of prescribed by law according to article 7 of the ECHR, the Guide states at [8] that '[t]he concept of "law" […] as used in Article 7 corresponds to that set out in other Convention articles, covering both domestic legislation and case-law, and comprises qualitative requirements, notably those of accessibility and foreseeability'. Therefore, the analysis conducted in the

incorporated into domestic law and therefore appears in an official publication.[54] In contrast, unpublished norms cannot not be considered accessible because the person concerned cannot not be aware of their existence.[55] As to the foreseeability requirement, this indicates that the law must be clear and predictable, sufficiently unambiguous, transparent and precise so as to allow the individuals concerned to regulate their conduct and foresee the consequences of the law.[56] In other words, the individual concerned must be able to understand from the wording of the law, if necessary resorting to legal advice or aided by the courts' interpretation of the law, which actions will give rise to liability and what the related penalty is.[57] However, due to the necessity to avoid excessive rigidity and to cover the ever evolving nature of human affairs, the wording of the law does not need to be absolutely precise for the law to respect the requirement of foreseeability.[58] Therefore, laws that are to a certain extent vague and whose interpretation and application depend on practice will still likely be considered as foreseeable, provided that they are found to be sufficiently clear in the majority of cases.[59] It follows that if a person needs to resort to legal advice for the interpretation of a norm, that norm will still be considered foreseeable, especially if that person is carrying out a professional activity, as in that case they are expected to proceed more cautiously than normal and take special care in assessing the risks of carrying out their profession.[60] As explained by the ECtHR, there

guide regarding the accessibility and foreseeability requirements of article 7 can be extended to those of article 10 of the ECHR.

[54] *Korbely v. Hungary* App no 9174/02 (ECtHR, 19 September 2008) paras 74-75; Directorate of the Jurisconsult, Guide on Article 7 of the European Convention on Human Rights (n 53), [26].

[55] Bychawska-Siniarska (n 2) 42.

[56] *Gaweda v Poland* App no 26229/95 (ECtHR, 14 March 2002) para [40]; *Yildirim v Turkey* (n 43) para 57; *RTBF v. Belgium* App no 50084/06 (ECtHR, 15 September 2011) para 103; *Altuğ Taner Akçam v Turkey* App no 27520/07 (ECtHR 25 January 2012) para 87; HRC General Comment No. 34 (n 2), [25]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [58]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [69].

[57] Directorate of the Jurisconsult, Guide on Article 7 of the European Convention on Human Rights, (n 53), [27].

[58] ibid [29].

[59] 'When the legislative technique of categorisation is used, there will often be grey areas at the fringes of the definition. This penumbra of doubt in relation to borderline facts does not in itself make a provision incompatible with Article 7 (art. 7), provided that it proves to be sufficiently clear in the large majority of cases. The role of adjudication vested in the courts is precisely to dissipate such interpretational doubts as remain, taking into account the changes in everyday practice' *Cantoni v. France* App no 17862/91 (ECtHR, 11 November 1996) para 32. The *Cantoni v France* case is related to article 7 of the ECHR rather than article 10. See above note 53 on the fact that the meaning of law contained in article 7 corresponds to that of other Convention articles; *RTBF v. Belgium* (n 56) para 104; *Altuğ Taner Akçam v Turkey* (n 56) para 87; Directorate of the Jurisconsult, Guide on Article 7 of the European Convention on Human Rights (n 53) [29].

[60] Directorate of the Jurisconsult, Guide on Article 7 of the European Convention on Human Rights (n 53), [30]; *Kononov v. Latvia* App no 36376/04 (ECtHR, 17 May 2010) para 235; *Cantoni v. France* (n 59) para 35.

are some factors that the Court takes into account to establish foreseeability. These are the content of the law, the field that that law covers and the number and status of those to whom the law applies.[61] In this regard, examples of restrictions that have been found to be in violation of the foreseeability requirement are *inter alia* those at the centre of the *Rotaru v. Romania*, *Petra v. Romania*, *Gawęda v. Poland* and *Yildirim v Turkey* cases of the ECtHR and the *Usón Ramirez v Venezuela* case of the IACtHR.[62] In these cases, the Courts have clarified that any law containing a restriction of a Convention right must also contain some guarantees against the arbitrary interference of the authorities to be considered foreseeable. This means that the law must indicate clearly the scope of any discretionary power left to the authorities, and how this discretion will be exercised.[63] In the *Usón Ramirez v Venezuela* case, for example, the Inter-American Court of Human Rights found that the terms in which the domestic law defined the crime of slander against the armed forces could not be considered compliant with the legality requirement because they failed to define accurately the key elements of the crime, thus leaving an unfettered margin of discretion to the authorities.[64] Similarly, in *Rotaru v. Romania* case the ECtHR stated that secret surveillance laws must illustrate with sufficient precision the circumstances under which the State can store and make use of personal information.[65] Therefore, surveillance laws that contain no indication as to the limits of the exercise of power by the authorities, no definition of the information that can be recorded and of the category of people that can be subjected to surveillance, no indications regarding when surveillance can be applied and which procedure will be followed and that contain no supervisory mechanisms regarding how surveillance will be conducted cannot be considered as foreseeable.[66] The same applies to the law regarding the monitoring of prisoners' correspondence at the centre of the *Petra v. Romania* case. In this case, the domestic law was found to be in violation of the foreseeability requirement because it was formulated in such vague terms that it rendered the monitoring process 'automatic,

---

[61] Directorate of the Jurisconsult, Guide on Article 7 of the European Convention on Human Rights (n 53), [30]; *Kononov v. Latvia* (n 60) para 235; *Cantoni v. France* (n 59) para 35.
[62] The *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) case and *Petra v Romania* App no 27273/95 (ECtHR, 23 September 1998) case are related to the meaning of prescribed by law of article 8 of the ECHR, rather than article 10. However, the Court's observations can be extended to article 10 as well.
[63] On the necessity not to grant unlimited discretionary power to the authorities, see also HRC General Comment No. 34 (n 2), [25].
[64] *Usón Ramírez v. Venezuela* (n 16), [56]. 'Article 505 of the Organic Code of Military Justice whereby "whoever slanders, offends, or disparages the National Armed Forces or any of its units shall be subject to three to eight years in prison"' *Usón Ramírez v. Venezuela* (n 16), [38]. See also Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [73].
[65] *Rotaru v Romania* (n 62) para 56. See also Bychawska-Siniarska, (n 2) 40.
[66] *Rotaru v Romania* (n 62) paras 57-59.

independent of any decision by a judicial authority and unappealable'.[67] Similarly, in the *Yildirim v Turkey* case, the ECtHR found that the domestic law regulating Internet publications could not be considered foreseeable since it granted extensive powers to the domestic administrative body in the implementation of a blocking order issued in relation to a website.[68] In addition, the law did not impose any obligation for the domestic courts to examine whether it was necessary under article 10 of the ECHR to block all Google Sites, nor did it provide any safeguards to avoid that a blocking order directed against a particular website being used as a way of blocking access in general.[69] In contrast, the reason why the ECtHR found that Poland had violated the foreseeability requirement under article 10 of the ECHR in the *Gawęda v. Poland* case had to do not with the domestic law in itself, but rather with the domestic court's interpretation of the law. Indeed, although the ECtHR found that the domestic law regulating the registration of newspapers was to a certain extent vague as it stated that a request for registration could be refused if '"inconsistent with the real state of affairs"', the real problem was represented by the way in which the domestic court interpreted this last requirement.[70] In particular, the domestic court found that registration could be refused if the title of the newspaper 'conveyed an essentially false picture'.[71] However, the ECtHR stated that the expression 'inconsistent with the real state of affairs' meant that registration could be refused if the request for registration did not respect the technical requirements indicated in the domestic law, rather than imposing an additional requirement, that according to which the title had to correspond to truthful information.[72] The ECtHR therefore concluded that 'the interpretation given by the courts introduced new criteria, which could not be foreseen on the basis of the text specifying situations in which the registration of a title could be refused'.[73]

---

[67] *Petra v Romania* (n 62) para 37. See also Bychawska-Siniarska (n 2) 40.
[68] *Yildirim v Turkey* (n 43) para 63.
[69] ibid paras 66, 68.
[70] *Gaweda v Poland* (n 56) paras 42-43. The expression '"inconsistent with the real state of affairs'" was contained in Section 5 of the Ordinance of the Minister of Justice on the registration of periodicals. See also Bychawska-Siniarska (n 2) 40.
[71] *Gaweda v Poland* (n 56) para 43. The title of the applicant newspaper was The Social and Political Monthly – A European Moral Tribunal. The Bielsko-Biała Regional Court dismissed the applicant's request for registration because '[t]he court considered that in accordance with the Press Act and the Ordinance of the Minister of Justice on the registration of periodicals, the name of a periodical should be relevant to its contents. The name as proposed by the applicant would suggest that a European institution had been established in Kęty, which was untrue and would be misleading to prospective buyers. Moreover, the proposed title would be disproportionate to the periodical's actual importance and readership as it was hardly conceivable that a periodical of a European dimension could be published in Kęty', *Gaweda v Poland* (n 56) para 6.
[72] *Gaweda v Poland* (n 56) para 43.
[73] ibid.

The second condition with which a restriction on freedom of expression must comply to be justified according to the ECHR, the ICCPR, the ACHR and the ACHPR is legitimacy. A restriction is legitimate if it pursues one of the legitimate aims listed in these human rights conventions.[74] In regard to the legitimate aims, there is a difference between the ECHR and the other three Conventions as the list of legitimate aims contained in the ECHR is longer and more detailed than those of the ICCPR, the ACHR and the ACHPR.[75] Indeed, while the last three Conventions admit mainly two categories of legitimate aims, namely the protection of the rights and reputations of others and the protection of national security, public order, public health and morals, the ECHR also admits restrictions that pursue territorial integrity, the prevention of disorder or crime, the prevention of disclosure of information received in confidence, or restrictions that protect the authority and impartiality of the judiciary.[76] In any case, according to all four Conventions the list of the legitimate aims is exhaustive and no new aims can be added by the States. States are not free to interpret the legitimate aims in any way that they might see fit, since there are specific criteria that they must respect when interpreting these aims. For example, the legitimate aims must always be interpreted in light of the principles of a democratic society.[77] Therefore, as explained by the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights, restrictions on freedom of expression in the name of national security cannot consist of intercepting or using private communications of dissidents.[78] However, in assessing the existence of a pressing social

[74] ICCPR (n 1) art 19(3); American Convention on Human Rights (n 1) art 13(2); African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9(3); European Convention on Human Rights (n 1) article 10(2).

[75] The African Charter on Human and Peoples' Rights does not list the aims that a restriction on freedom of expression must pursue to be justified. However, this list is contained in Principle 9(3) of the Declaration of Principles on Freedom of Expression and Access to Information in Africa issued by the African Commission on Human and Peoples' Rights (n 2).

[76] ICCPR (n 1) art 19(3); American Convention on Human Rights (n 1) art 13(2); African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9(3); European Convention on Human Rights (n 1) article 10(2); Benedek and Kettemann (n 2) 46; HRC General Comment No. 34 (n 2), [28]-[32]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [59]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [74]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9(3); O'Flaherty (n 4) 640-641.

[77] Bychawska-Siniarska (n 2) 43; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [59]-[60]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [66]; O'Flaherty (n 4) 640-641; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9(1).

[78] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [59]-[60].

need, some human rights Courts grant the States a margin of appreciation. More specifically, the doctrine of the margin of appreciation is applied by the ECtHR and it consists of leaving Member States of the ECHR a margin of discretion in assessing the existence of a pressing social need that justifies the restriction.[79] Nevertheless, the ECtHR does retain a supervisory role in the application of the margin of appreciation by the States. Indeed, as explained by the Court in the *Ovchinnikov* case

'[t]he Court's task in exercising its supervisory function is not to take the place of the national authorities, but rather to review under Article 10, in the light of the case as a whole, the decisions they have taken pursuant to their margin of appreciation. In so doing, the Court has to satisfy itself that the national authorities applied standards which were in conformity with the principles embodied in Article 10 and, moreover, that they based their decisions on an acceptable assessment of the relevant facts'.[80]

The margin of appreciation, which has occasionally been applied also by the Inter-American Court of Human Rights[81], however, has been openly rejected by the HRC which in General Comment No 34 stated that the scope of freedom of expression is not to be assessed by reference to a margin of appreciation and that it will be for the Committee itself to determine whether there might have been circumstances which made the restriction of freedom of expression necessary.[82]

Finally, so that a restriction can be justified according to the human rights Conventions mentioned above, it must be proportional and necessary in a democratic society to achieve the legitimate aim pursued.[83] This criterion, also known as proportionality or necessity,

---

[79] Benedek and Kettemann (n 2), 48.

[80] *Aleksey Ovchinnikov v. Russia* App no 24061/04 (ECtHR, 16 March 2011) para 46.

[81] Marie Ghantous 'Freedom of Expression and the "Margin of Appreciation" or "Margin of Discretion" Doctrine' (2018) 31 RQDI 221, 228-229. For a discussion on the application of the margin of appreciation by the Inter-American Court see also Andreas Follesdal 'Exporting the Margin of Appreciation: Lessons for the Inter-American Court of Human Rights' (2017) 15 ICON 359.

[82] HRC General Comment No. 34 (n 2), [36]; see also *Ilmari Länsman et al. v. Findland* (1992) UN Doc. CCPR / C / 52D / 511 / 1992, [9.4] in regard to the scope of the margin of appreciation with reference to article 27 of the ICCPR. However, O'Flaherty (n 4) observes at p. 650 that when the HRC in the General Comment No 34 stated that the scope of the right to freedom of expression is not to be assessed by reference to a margin of appreciation, the Committee officially departed from its previous case-law. Indeed, in *Hertzberg v Finland* (1985) U.N. Doc. CCPR/C/OP/1, which is the only case where the HRC openly invoked the margin of appreciation, the Committee found at [10.3] that since public morals differ widely as there is no common understanding of morals, a certain margin of appreciation must be left to the State in this regard. This doctrine was, however, subsequently reversed by the HRC in *Kyu Sohn v Republic of Korea* (1995) U.N. Doc. CCPR/C/54/D/518/1992 at [10.4] when it stated that it will be the Committee itself to evaluate whether the restriction was necessary to achieve the legitimate purpose invoked by the State.

[83] European Convention on Human Rights (n 1) article 10(2); Bychawska-Siniarska (n 2) 44; Benedek and Kettemann (n 2) 45; HRC General Comment No. 34 (n 2), [33]-[34]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [61]-[64]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [83]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9 (1) (c). In

means that States imposing restrictions to freedom of expression must show that there is a pressing social need that requires for that specific restriction to be introduced.[84] In other words, States must show that there is a verifiable, sure and credible threat to the basic conditions for the operation of democratic institutions and that the imposed restriction on freedom of expression is the least restrictive means to achieve the legitimate aim pursued.[85] In this regard, the HRC has clarified that the State Parties must 'demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat'.[86] This requirement sets a high threshold for restrictions thus furthering the protection of freedom of expression.[87] In order to assess proportionality, the Courts will take into account a series of factors, such as the circumstances of the publication, their content and context, the existence of public interest, and the severity of the sanction.[88] For example, in case of restrictions on freedom of expression that are necessary to protect the rights and reputations of others, the Inter-American Court of Human Rights has explained that the factors that it considers to establish proportionality are: the severity of the violation of the competing right, the importance of fulfilling this right, and whether fulfilling this right justifies the restriction on freedom of expression.[89] Besides, in cases of restrictions on the operation of websites, various human rights Courts and bodies have underlined how restrictions should be content specific and limited only to content that is illegal according to international law. Therefore, generic bans on websites are generally not in line with the freedom of

---

relation to the American Convention of Human Rights, Article 13(3) states that restrictions to freedom of expression must not be introduced by indirect means, such as the abuse of government controls over media. In addition, Article 13(4) specifies that restrictions on freedom of expression in regard to public entertainment must not amount to prior censorship, unless this is necessary for the moral protection of childhood and adolescence.

[84] Bychawska-Siniarska (n 2) 44; *Observer and Guardian v. the United Kingdom* App no 13585/88 (ECtHR, 26 November 1991) para 59(c); *Başkaya And Okçuoglu v. Turkey* App no 23536/94 and 24408/94 (ECtHR, 8 July 1999) para 61; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9 (4) (a).

[85] Benedek and Kettemann (n 2) 45; HRC General Comment No. 34 (n 2), [34]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [83]-[86]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [61]-[62]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 9 (4).

[86] HRC General Comment No. 34 (n 2), [35]; see also *Shin v. Republic of Korea* (2004) U.N. Doc. CCPR/C/80/D/926/2000, [7.3].

[87] O'Flaherty (n 4) 649-650.

[88] Bychawska-Siniarska (n 2) 45; *Başkaya And Okçuoglu v. Turkey* (n 84) para 61(iii).

[89] *Kimel v. Argentina* (n 16), [84]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'The Inter-American Legal Framework regarding the Right to Freedom of Expression' (n 9), [88]-[89].

expression provisions of the human rights Conventions.[90] In particular, as observed by the Special Rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights, when evaluating the proportionality of a freedom of expression restriction on the Internet, it is important to take into account not only the impact that that restriction could have on the private parties affected by it, but also the repercussions of that restriction on the functioning of the Internet and the freedom of expression of all users.[91]

6.4 Compliance of the extraterritorial application of domestic laws with the freedom of expression provisions of the human rights Conventions

Chapters 2 and 3 have explored two particular ways in which States have exercised jurisdiction in Internet-related cases. These are the access-based jurisdictional approach and the extraterritorial application of domestic laws to regulate content published online. The access-based jurisdictional approach is characterised by the exercise of jurisdiction over content published online but uploaded and hosted in foreign countries by foreign parties based on the fact that that content can be accessed on the territory of the State exercising jurisdiction. As to the cases illustrating the extraterritorial application of domestic laws such as those discussed in Chapter 3, these cases are characterised by the imposition by domestic courts of measures that have extraterritorial reach, such as global de-listing rather than de-listing applied only to the local domain names of a search engine. Both these approaches have been criticised because they impact negatively on the freedom of expression of Internet users located in foreign States and subjected to foreign jurisdictions.[92] The key objection that can be moved to both approaches is that they extend the application of domestic laws beyond the national borders to regulate online content that is linked to foreign jurisdictions and that is not illegal according to international law. In regard to the access-based jurisdictional approach, all this also happens in the absence of a clear nexus linking the acts over which jurisdiction is exercised to the country exercising jurisdiction.

---

[90] Joint Declaration on Freedom of Expression and the Internet (n 2), [3]; HRC General Comment No. 34 (n 2), [43]; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [84]-[85]; African Commission on Human and Peoples' Rights 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' (n 2), Principle 38 [1].

[91] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (n 2), [53].

[92] For an in-depth analysis of these two approaches and the critiques that have been moved to them see Chapter 2 on the access-based jurisdictional approach and Chapter 3 on the extraterritorial application of domestic laws in Internet-related cases.

As mentioned in Chapter 2, the Special Representatives on Freedom of Expression of the Organisation for Security and Cooperation in Europe (OSCE), the United Nations (UN), the Organisation of American States (OAS) and the African Commission on Human and Peoples' Rights (ACHPR) stated in the 2011 Joint Declaration on Freedom of Expression that in order to protect freedom of expression online, '[j]urisdiction in legal cases relating to Internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State'.[93] Therefore, according to the Special Representatives on Freedom of Expression, so that an exercise of jurisdiction over online content is compliant with freedom of expression it must be justified by clear links between the content and the State exercising jurisdiction. These clear links, however, are absent in the access-based jurisdictional approach while, although they might be present in the case of global de-listing[94], they cannot justify the global reach of domestic laws.[95]

A question that is worth considering is whether these exercises of jurisdiction could be considered illegal according to the freedom of expression provisions of the human rights Conventions. In particular, this analysis aims to understand whether the extraterritorial application of domestic laws examined in Chapters 2 and 3 can be considered as prescribed by law according to the human rights conventions, and therefore compliant with the accessibility and foreseeability requirements that restrictions to freedom of expression should respect. In other words, the research hypothesis that needs to be verified is whether the foreign parties who are at the receiving end of these exercises of jurisdiction can reasonably be expected to have accessed or even predicted such an application of domestic laws. For example, following the *Perrin* case and the finding that the Obscene Publications Act 1959 applies both when material is uploaded in the UK but also when it is downloaded there, how foreseeable is it for a foreign party operating in a foreign jurisdiction to predict that the UK domestic law applies to them because the content that they published online is accessible worldwide and therefore in the UK as well? The same question can be extended to the *Yahoo! Auction* case as well as all the defamation cases[96] discussed in Chapter 2: is expecting that foreign publishers comply

[93] Joint Declaration on Freedom of Expression and the Internet (n 2), [4] (a).

[94] As stated in Chapter 3 section 3.3, in the *CNIL* and *Equustek* cases the exercise of State jurisdiction over the foreign defendants was justified by the fact that the foreign defendants were operating in the States exercising jurisdiction or targeted an audience located there.

[95] See Chapter 3 section 3.3 for an analysis of this point.

[96] As to the defamation cases discussed in Chapter 2, a limit to the exercise of jurisdiction in these cases is the requirement that the victim of defamation has a reputation in the forum State. For an analysis of this point, see Chapter 2 Section 2.4.

with the laws of all the countries where the online content can be accessed a predictable restriction to their freedom of expression? As to the de-listing cases, is the fact that Google is expected to carry out delisting globally based on the application of a domestic law compliant with the requirement that freedom of expression restrictions are predictable and accessible?[97]

So far, *Perrin v the United Kingdom* is the only case presented before a human rights court expressly dealing with the question of whether the exercise of jurisdiction by a Member State over content published online from abroad, based on the accessibility of that content within the Member State, could be considered as 'prescribed by law' according to the freedom of expression provision of the Convention. In that case, the ECtHR found that the Obscene Publications Act 1959 under which Mr Perrin was convicted was sufficiently clear to satisfy the prescribed by law requirement of article 10(2) of the ECHR because it did make it clear that its provisions covered electronic as well as more traditional publications.[98] The Obscene Publications Act 1959 was also considered sufficiently accessible to Mr Perrin since he was a UK resident. Indeed, in this regard the ECtHR concluded that since Mr Perrin was carrying out a professional activity in the UK, as he was the owner of the company responsible for uploading the pictures, he should have sought legal advice to clarify the local norms regulating his activity.[99] A point that the ECtHR failed to appropriately take into account, however, is the unique and ubiquitous nature of online content which is instantly available worldwide. Surely, Mr Perrin lived in the UK and therefore could have expected that UK laws were applicable to him. However, due to the uncertainties surrounding the exercise of State jurisdiction online and the immediate global accessibility of online content, it is certainly more difficult for the owner of a company established abroad and which uploaded content online that was legal in the country of upload, to anticipate that that content was going to be subjected to the jurisdiction of the UK. This complexity was completely glossed over by the Court, which relied on its classic interpretation of accessibility and foreseeability of the law as if Internet content could be assimilated to printed content. In fact, as observed by Korff, the Court referred to the case *Chauvy and Others v France* to underline the point that as Mr Perrin was carrying out a professional activity in the UK as the owner of a company, he should have sought legal advice to clarify which laws were

[97] These questions assume that the human rights conventions are applicable to the online acts attributed to the foreign parties responsible for the acts. However, see Chapter 5 for a discussion of this point and of the application of the personal, spatial and extraterritorial effects models of jurisdiction to online acts.
[98] *Perrin v the United Kingdom* App no 5446/03 (ECtHR, 18 October 2005) 6.
[99] ibid.

applicable to him.[100] The *Chauvy and Others v France* case, however, is related to defamation proceedings brought against French citizens who authored and published a printed book in France.[101] In other words, there was no transnational, cross-border element in the case referred to by the Court to justify the point made in *Perrin*.[102]

Ultimately, the analysis regarding the meaning of prescribed by law according to the ECHR, the ICCPR, the ACHR and the ACHPR conducted in section 6.3 shows that the accessibility requirement is satisfied if the law introducing the restriction is published, whereas the foreseeability requirement is satisfied if the law is sufficiently clear so as to allow the individuals affected to regulate their conduct, if necessary resorting to legal advice or courts' interpretation. However, the problem of laws that regulate content published online by foreign parties and linked to foreign jurisdictions is that, although domestic laws might technically be found to be compliant with the prescribed by law requirements of the human rights Conventions, often these requirements do not take into account the special difficulties associated with content that is accessible globally, as the *Perrin v the UK* case shows. In particular, as observed by Khol, there are some extra-legal factors that influence the accessibility of the law that cannot be as easily applied in the global context. These are: common knowledge and intermediaries.[103] Indeed, in a given country, common knowledge is more likely to alert individuals of the presence of a law regulating a certain conduct rather than the official publication of the norm, even though common knowledge does not necessarily provide people with the details of the regulation.[104] At the same time, similarly to common knowledge, intermediaries facilitate the compliance of people's behaviour with the law because often intermediaries are the direct subject of the law and therefore if they comply with it the general public will as well.[105] An example provided by Khol in this regard is that of the laws that regulate the sale of firearms. These laws are primarily directed at shops that sell firearms, therefore people who want to buy firearms do not need to know the details of the law regulating the purchase so that they can complete it. Indeed, it will be the shops selling the firearms that will likely be required by law to inform those who buy them of their rights and duties ultimately facilitating people's compliance with the law.[106] However, as mentioned above, common knowledge and intermediaries do not work well when applied to the

[100] *Perrin v the United Kingdom* (n 98) 6; Korff and Brown (n 44) 196.
[101] *Chauvy and Others v France* App no 64915/01 (ECtHR, 29 July 2004).
[102] Korff and Brown (n 44) 196.
[103] Uta Kohl, 'Ignorance is no Defence, but is Inaccessibility? On the Accessibility of National Laws to Foreign Online Publishers' (2005) 14 Info&CommTechL 25, 31-34.
[104] ibid 31.
[105] ibid.
[106] ibid.

global context. This is because global common knowledge does not go further than a generic assumption that certain acts, such as theft for example, are likely to be prohibited abroad as well.[107] However, different States have different standards, and therefore common knowledge might not be particularly helpful in this regard. Besides, even admitting that online publishers knew through some form of global common knowledge that different countries have different rules, they might interpret the law of a foreign country in a way that is similar to the law that applies in their country, and this might prevent them from realising that in certain respects the foreign law might be different.[108] In addition, especially individual or small publishers that do not have access to special legal counsel might not even be aware that there is a foreign law that is applicable to them.[109] In other words, as Khol observes 'the global village lacks key notice mechanisms, such as the common knowledge and knowledge hotspots, which in the domestic context play a critical role either in bringing rules to the attention of their subjects or in relieving them of knowing them'.[110] These considerations which impact on the accessibility and foreseeability of foreign laws should be taken into account together with the complexities of the online environment by human rights Courts when assessing the exercise of jurisdiction by a Member State over online content published by foreign parties. However, as Kohl concludes '[w]hether […] it can really be expected of a judge to take these concerns into account […] is doubtful. It would seem that, in the name of certainty, the judiciary is likely to view accessibility as requiring no more than the formal publication of the law.'[111]

6.5 Conclusions

The analysis conducted in this chapter has illustrated the framework for the protection of the right to freedom of expression online and offline together with the conditions under which freedom of expression can be restricted according to the ECHR, the ICCPR, the ACHR and the ACHPR. In particular, it has shown that the human rights Courts have recognised the dual nature of the Internet as a catalyst for the fulfilment of human rights online but also as a multiplier of the negative impact caused by the publication of harmful content in the cyberspace. In addition, the study of the permissible restrictions to freedom

[107] ibid 32.
[108] ibid.
[109] ibid.
[110] ibid 33.
[111] ibid.

of expression according to article 13 of the ACHR, article 19 of the ICCPR, article 9 of the ACHPR and article 10 of the ECHR has clarified the conditions under which Member States can restrict freedom of expression in a way that is justified under the Conventions. More specifically, the analysis of the meaning of 'prescribed by law' has shown that the accessibility requirement is satisfied if the law restricting freedom of expression is published, whereas the predictability requirement is satisfied if the law allows those who are affected by it to regulate their conduct with sufficient clarity, if necessary resorting to legal advice. However, the research into whether the extraterritorial exercises of jurisdiction such as those illustrated in Chapters 2 and 3 are compliant with the prescribed by law requirements of the human rights Conventions has shown that although domestic laws might technically be found to be compliant with the accessibility and foreseeability requirements, often these requirements do not take into account the special difficulties associated with content that is accessible globally. Indeed, as shown by the *Perrin* case, the ECtHR judges approached the case by interpreting the accessibility and foreseeability requirements as if the publication at the centre of the case were a printed publication rather than an online one assimilating it to a case where no transnational cross-border elements were present. In addition, the research has shown that there are some extra-legal factors, namely common knowledge and intermediaries, that influence the accessibility of the law in the domestic context. These factors do not work well when translated into the global context, which makes it even more difficult for foreign parties to access domestic laws and predict that these laws apply to them.

7. Conclusions

This thesis focussed on the rules regulating the exercise of State jurisdiction online according to human rights law. In particular, it aimed at answering two main research questions: what does online State jurisdiction mean in human rights law and are specific instances of extraterritorial jurisdiction by States over content published online compliant with the freedom of expression provisions of the human rights Conventions?

In order to answer these two research questions, Chapters 2 and 3 have identified specific instances of extraterritorial exercise of State jurisdiction over online content through the analysis of some key Internet-related domestic cases. The analysis of the access-based jurisdictional approach conducted in Chapter 2 has allowed to highlight the distinctive characteristics of this approach, i.e. the fact that the domestic courts in the cases analysed have exercised jurisdiction over content published online but uploaded and hosted in foreign States based on the fact that, having been published online, the content was accessible from within the territory of the State exercising jurisdiction. This analysis has allowed to highlight two main points. The first is related to application of the objective territorial principle and the effects doctrine to content published online. In particular, the cases analysed have shown that, when applied to online content, the objective territorial principle and the effects doctrine tend to conflate into each other. This is because it is not always possible to distinguish whether domestic courts establishing jurisdiction over online acts have done so based on the fact that some components of those acts physically happened within the domestic territory or whether the exercise of jurisdiction was justified by the fact that, although the online acts happened abroad, they produced negative effects within the domestic territory. In other words, due to the global, non-physical and worldwide accessible nature of online content, it is difficult to distinguish which country is physically affected by that content and which is affected only by its negative effects. The result is that the application of the objective territorial principle to online acts leads to exercises of jurisdiction that are as limitless as those associated with the effects doctrine. The second point that has emerged from the analysis conducted in Chapter 2 is related to the negative consequences of the application of the access-based jurisdictional approach. In particular, the analysis has highlighted that if all the countries claimed that the application of their national laws extended globally based on the fact that online content is accessible worldwide, the principle of freedom of expression and the

right to access information, as well as the principle of certain and predictable laws could be compromised. Overall, the main critique that can be moved to establishing jurisdiction based on access to online content is the absence of any analysis on whether factors other than the accessibility of the content within the domestic territory existed linking the country exercising jurisdiction to the online content. That analysis could have helped the domestic Courts to limit the exercise of jurisdiction only to those online cases that presented a clear and close nexus with the country exercising jurisdiction, as indicated by the Special Representatives on Freedom of Expression of the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE), the American Commission on Human Rights and the African Commission on Human and Peoples' Rights.[1]

The objective territorial principle has also been at the heart of the domestic cases analysed in Chapter 3. These cases provide an outline of other instances of the extraterritorial application of domestic laws to regulate content published online, in particular in the field of data protection and access to data. In the cases analysed in this chapter, there was no doubt that the domestic courts had jurisdiction over the defendants, many of whom were established abroad, based on the objective territorial principle as those defendants were conducting business within those States. However, the controversial element of the exercises of jurisdiction examined in this chapter is represented by the global nature of the measures imposed by the domestic courts. In particular, ordering global delisting based on the application of the domestic law on data protection and copyright, as happened in the *CNIL* and *Equustek* cases respectively, is problematic because it violates the principle of comity between States and the freedom of expression of foreign Internet users. Indeed, the disagreement between the Canadian and the American Courts in the *Equustek* case is a direct proof that foreign States' interests are affected by a measure with global jurisdictional reach. Ordering a measure with worldwide effect based on domestic rather than international law and in the absence of specific connecting factors linking the content over which jurisdiction is exercised to the country exercising jurisdiction equates to imposing the laws of one country to other States and has the effect of preventing Internet users located in those States from accessing content that might be perfectly legal there. Different countries have different laws and each country conducts a balance

[1] The United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet' (1 June 2011), 4(a); Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Freedom of Expression and the Internet' (31 December 2013), [66].

between competing rights that is tailored to the values and legal system of that country. Therefore, ordering global delisting equates to imposing a very specific balance between the right to privacy and freedom of expression which might be right for the country that ordered the global measure, but that does not necessarily reflect the values of other countries. As outlined by the Inter-American Commission on Human Rights in regard to the so-called right to be forgotten, for example, in the Americas

> '[p]eople want to remember and not to forget. In this sense, it is important to recognize the particular context of the region and how a legal mechanism such as the so-called "right to be forgotten" and its incentive for de-indexation might impact the right to truth and memory'.[2]

Ultimately, exercising jurisdiction through the imposition of measures with a global effect and without a close connection between the online act and the country exercising jurisdiction equates to exercising universal jurisdiction over acts that are not international crimes.

Having examined the main pitfalls of exercising extraterritorial jurisdiction over online content, Chapter 4 analysed the rules regulating the exercise of State jurisdiction according to both international law and human rights law. This analysis set the ground for answering the research questions at the centre of this research as it clarified the jurisdictional rules applicable in these two fields. It also highlighted the uncertainties surrounding the exercise of State jurisdiction according to both these regimes. The effects doctrine and the protective principle represent some of the most uncertain subjects as far as the international law jurisdictional rules are concerned. The main criticalities associated to these two jurisdictional principles are that the definition of what constitutes an adverse effect or an act against the sovereignty of a State is left to each State that claims jurisdiction. This leads to States potentially abusing these principles and establishing jurisdiction over acts that are not closely related to them. The uncertainties surrounding the use of these principles have led to disagreements between States, especially due to an unqualified use of the effects doctrine in association to online acts. As to the jurisdictional rules governing the exercise of State jurisdiction according to human rights law, the analysis has highlighted the problems associated with the spatial and the personal model of jurisdiction, which have been criticised due to the difficulty of limiting their application and the consequently arbitrary way in which Courts apply them,

[2] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet' (15 March 2017), [134].

with particular reference to the European Court of Human Rights (ECtHR). Overall, Chapter 4 has allowed to highlight the differences between the international law and the human rights law jurisdictional rules, underlining the fundamentally different meaning of State jurisdiction according to these two regimes. Indeed, while in international law State jurisdiction is related to the legality of the use of power by States, in human rights law this term indicates a factual exercise of power by States, regardless of whether that exercise of power is legal according to international law.

The association of State jurisdiction with the exercise of a factual power that is central in human rights law influences the meaning of online State jurisdiction according to this regime. This theme was explored in Chapter 5, whose primary aim was indeed to answer the first research question by clarifying the rules regulating the exercise of State jurisdiction online according to regional and international human rights conventions. Chapter 5 answered this question by first highlighting some of the main difficulties associated with exercising jurisdiction online according to international law. In particular, this analysis confirmed that, although international law allows for multiple exercises of State jurisdiction, it also requires States to refrain from the unqualified application of the effects doctrine to online acts and to limit the exercise of State jurisdiction only to those acts whose adverse effects on the State are direct, intended, foreseeable and substantial.[3] The analysis also highlighted the difficulties related to the application of the territorial principle of jurisdiction online and evidenced the need to move away from territoriality as the main jurisdictional principle applicable to online acts. At the same time, however, Chapter 5 also explored the problems associated with establishing jurisdiction online based on alternative criteria such as the targeting test, whose parameters regulating its functioning are still left to each domestic Court to set. As to the meaning of State jurisdiction online in human rights law, the analysis of the jurisprudence of the European Court of Human Rights (ECtHR), the Human Rights Committee (HRC), the African Court and Commission on Human and Peoples' Rights and the Inter-American Court and Commission on Human Rights revealed that there are very few Internet-related cases presented before the Courts where these were asked to clarify the meaning of online State jurisdiction according to the related Conventions. The ECtHR and the HRC, however, have had more opportunities to examine Internet-related cases compared to the Courts of the Inter-American and African system. More specifically, the analysis of the Internet-related jurisprudence of the ECtHR and the HCR allowed to highlight an important point.

[3] M Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 58, [13].

There is a tendency on the ECtHR's part, also confirmed in the some opinions issued by the HCR, to find that the ECHR applies to individuals located abroad whose rights have been violated due to an act committed online if that act is found to have happened on the territory of a Contracting State. This fact highlights that online acts such as the publication of comments on websites managed by foreign companies or surveillance of Internet communications of foreign citizens are found to have happened within the territory of the Member State exercising jurisdiction regardless of their transborder and non-physical nature. This indicates that, just like domestic courts, human rights courts tend to interpret online acts mainly as territorial acts. However, the tendency of the ECtHR to establish that Member States have jurisdiction over foreign people based on the location of the online act represents a departure from both the personal and spatial models of jurisdiction of the human rights conventions. This is because both models apply to individuals who are either in a territory controlled by a State Party to the human rights conventions or are subjected to the power or authority of that State. Notwithstanding this apparent departure from the application of the spatial and personal model of jurisdiction, establishing jurisdiction based on the location of the violation is supported by the case-law of both the HCR and ECtHR. What is, however, unclear is which jurisdictional model justifies the application of the human rights Conventions in this case. This point is directly linked to the application of the spatial and personal models of jurisdiction to Internet-related cases. Both models present more than one problem when applied to online acts. The main difficulty that arises in both cases is related to how to establish when a State is exercising power or control over a territory or a person in the absence of physical power. The analysis conducted in Chapter 5 therefore focussed on an alternative jurisdictional model, that of the extraterritorial effects, according to which an online act that is considered to have happened on the territory of a Member State could be interpreted as a domestic act with negative extraterritorial effects on people located abroad. The extraterritorial effects model of jurisdiction could be particularly useful to deal with online acts as it could be used to reinterpret the personal model of jurisdiction as involving an exercise of power over individuals located abroad through the commission of online acts that, although happened within the domestic territory, have extraterritorial effects and thus violate the rights of foreign people. Although this model seems to have found confirmation in recent jurisprudence of the Inter-American Court of Human Rights in regard to the right to life, it is not immune from criticisms, especially with regard to the fact that the rules regulating how to define when an online non-physical act is capable of producing extraterritorial effects are not clear. Notwithstanding this, Chapter 5 concluded that the extraterritorial

model represents a better alternative than the personal and spatial models to interpret online State jurisdiction in human rights law.

Finally, Chapter 6 answered the second research question by conducting an analysis into whether the extraterritorial exercises of jurisdiction analysed in Chapters 2 and 3 are compliant with the freedom of expression norms of the human rights Conventions. The claim at the centre of this chapter was that the application of domestic laws to foreign parties due to the publication of online content, typical of the access-based jurisdiction and of global delisting measures, is not accessible nor predictable and cannot therefore be considered as prescribed by law according to the human rights Conventions. This is because it does not seem particularly predictable for foreign parties who publish content online that is lawful according to both their domestic law and international law to anticipate that they could be subjected to an exercise of jurisdiction by other countries in the absence of specific links between the content published online and the foreign country exercising jurisdiction. At the same time, it does not seem that domestic laws that apply globally can be considered as accessible to all the foreign parties that these laws purport to regulate. However, the analysis of the permissible restrictions to freedom of expression contained in the European Convention on Human Rights (ECHR), the International Covenant on Civil and Political Rights (ICCPR), the American Convention on Human Rights (ACHR) and the African Charter on Human and Peoples' Rights (ACHPR) showed that in order to satisfy the accessibility requirement the domestic laws introducing the restriction to freedom of expression must simply have been published, whereas the foreseeability requirement is met if the law is sufficiently clear so as to allow the individuals affected to regulate their conduct, by recurring to legal advice or courts' interpretation if necessary. In addition, the analysis of the *Perrin* case, which is so far the only case discussed before a human rights court where the "prescribed by law" requirement of the domestic law establishing jurisdiction over online content published from abroad has been discussed, showed that the ECtHR interpreted the accessibility and foreseeability requirements by assimilating the online publication at the centre of the case to a printed one with no transnational elements. In other words, the Court glossed over the complexities that are typical of worldwide accessible Internet content, sticking to an interpretation of the accessibility and foreseeability requirements that is appropriate for printed publications. Therefore, it can be concluded that, according to the jurisprudence of the human rights courts, domestic laws such as those examined in Chapters 2 and 3 are in fact compliant with the prescribed by law requirement of the human rights Conventions. Nonetheless, the research conducted in this Chapter observed that the

accessibility and foreseeability requirements should be adapted to Internet-related cases so as to reflect the complex nature of online content. This is especially so considering that there are some extra-legal factors, such as common knowledge and intermediaries, that contribute to making a domestic law accessible to the public. While however, these factors alert the public to the existence of a new law in the country where the law is adopted, they do not work well in the global context. For this reason, in the absence of these two extra-legal factors, it seems particularly difficult for a foreign party, especially a small company or a private individual rather than an international corporation, to anticipate that the laws of another country might be applicable to them. The accessibility and foreseeability requirements of the human rights conventions should reflect this complexity. It seems, however, difficult, that the human rights courts might take extra-legal factors into account in their future evaluations of Internet-related cases. It will certainly be interesting to see how the law develops in this regard.

Bibliography and References

Secondary sources

Abass A, *International Law* (1st, Oxford University Press 2012).

Charlesworth H, 'Feminist method in international law', (1999) 93 AJIL 379.

Chynoweth P, 'Legal Research' in Andrew Knight and Les Ruddock (ed), *Advanced Research Methods in the Built Environment* (Wiley-Blackwell 2008).

Cleveland SH and Stephan PB (ed), *Restatement of the Law (Third) The Foreign Relations Law of the United States* (1st edn, American Law Institute Publishers 1987).

Daskal J, 'The Un-Territoriality of Data' (2015) 125(2) YLJ 326.

– – 'Unpacking the Cloud Act' (2018) 4 EUCRIM 220.

Follesdal A, 'Exporting the Margin of Appreciation: Lessons for the Inter-American Court of Human Rights' (2017) 15 ICON 359.

Geist MA, 'Is There a There There - Toward Greater Certainty for Internet Jurisdiction' (2001) 16(3) Berkeley Tech LJ 1345.

Ghantous M, 'Freedom of Expression and the "Margin of Appreciation" or "Margin of Discretion" Doctrine' (2018) 31 RQDI 221.

Gillespie A, 'Jurisdictional issues concerning online child pornography' (2012) 20 Int J Law Info Tech 151.

Gondek M, 'Extraterritorial application of the European Convention on Human Rights: territorial focus in the age of globalization' (2005) 52 Netherl I L Rev 349.

Greenberg MH, 'A Return to Lilliput: The LICRA v Yahoo! Case and the Regulation of Online Content in the World Market' (2003) 18 Berk. Tech L J 1191.

Hayashi M, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace' (2006) 6 In.L. 284.

Heissl G, 'Jurisdiction for human rights violations on the Internet' (2011) 2(1) EJLT.

Hutchinson T and Duncan N, 'Defining and describing what we do: doctrinal legal research' (2012) 17 Deakin LR 83.

Kohl U, 'Eggs, Jurisdiction, and the Internet' (2002) 51(3) Int'l & Comp. L.Q. 555.

– – 'Ignorance is no Defence, but is Inaccessibility? On the Accessibility of National Laws to Foreign Online Publishers' (2005) 14 Info.& Comm.Tech.L. 25.

Lowe V, 'Jurisdiction' in Malcom D. Evans (ed) International Law (1st, Oxford University Press 2003).

Koskenniemi M, 'Letter to the editors of the symposium', (1999) 93 AJIL 351.

Kulesza J, *International Internet Law* (1st edn, Routledge 2012).

– – and Balleste R, 'Signs and Portents in Cyberspace: the Rise of a Jus Internet as New Order in International Law' (2013) 23 Fordham Intell. Prop. Media & Ent. L.J. 1311.

Maier B, 'How has the law attempted to tackle the borderless nature of the internet?' (2010) 18 Int J Law Info Tech 142.

Margulies P, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2014) 82 Fordham L.Rev. 2137.

Milanović M, 'From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties' (2008) 8 Hum. Rts. L. Rev. 411.

– – ‘Al-Skeini and Al-Jedda in Strasbourg’ (2012) 23(1) EJIL 121.

– – *Extraterritorial Application of Human Rights Treaties* (1st, Oxford University Press 2011).

– – ‘Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age’ (2015) 56 Harv Int'l L J 81.

Mills A, ‘Rethinking jurisdiction in international law’ (2014) 84 BYIL 187.

Mora PD, ‘The Alien Tort Statute after Kiobel: the Possibility for Unlawful Assertions of Universal Civil Jurisdiciton Still Remains’ (2014) 63 ICLQ 699.

Mowbray A, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights* (1st edn, Hart Publishing 2004).

Mueller ML and Badiei F, ‘Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country-Code Top Level Domains’ (2017) 18 Colum Sci & Tech L Rev 435.

O’Connell ME, ‘New International Legal Process’, (1999) 93 AJIL, 334.

Oddis DI, ‘Combating Child Pornography on the Internet: The Council of Europe Convention on Cybercrime’ (2002) 16 Temp. Int’l & Comp. L. J. 477.

O'Flaherty M, ‘Freedom of Expression: Article 19 of the International Covenant on Civil and Political Rights and the Human Rights Committee's General Comment No 34’ (2012) 12(4) HRLRev 627.

Rabinovitch R, ‘Universal Jurisdiction in Absentia’ (2005) 28 Fordham Int'l L.J. 500.

Rahman MM and others, ‘Cyberspace claiming new dynamism in the jurisprudential philosophy’ (2009) IJLMA, 51, 274.

Randall KC, ‘Universal Jurisdiction Under International Law’ (1988) 66 Tex L Rev 785.

Ryngaert C, *Jurisdiction in International Law* (1st, Oxford University Press 2008).

– – ‘Clarifying the extraterritorial application of the European Convention on Human Rights’ 2012 28(74) UJIEL 57.

– – *Jurisdiction in International Law* (2nd, Oxford University Press 2015).

Schmitt M (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017).

Schultz T, ‘Carving up the Internet: jurisdiction, legal orders, and the private/public international law interface’ (2008) 19(4) EJIL 75, 812.

Simma B and Paulus AL, ‘The responsibility of individuals for human rights abuses in internal conflicts: a positivist view’ (1999) 93 AJIL 302.

Slaughter AM and Ratner SR, ‘The method is the message’ (1999) 93 AJIL 410.

Smith SA, ‘Taking law seriously’ (2000) 50 U. Toronto L.J. 241.

Svantesson DJB, ‘A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft’ (2015) 109 AJIL Unbound 69.

– – ‘Nostradamus Lite – Selected Speculations as to the Future of Internet Jurisdiction’ (2016) 10 Masaryk UJL & Tech 47.

Uerpmann-Wittzack R, ‘Principles of International Internet Law’ (2010) 11 German L. J. 1245.

Talbot Jensen E, ‘The Tallinn Manual 2.0: Insights and Highlights’ (2017), 48 Geo J Int'l L 735.

Therani PM and Manap NA, ‘A rational jurisdiction for cyberterrorism’ (2013) 29 Com. L & S Rev 689.

Treppoz E, ‘Jurisdiction in the Cyberspace’ (2016) 26 Swiss Rev Int'l & Eur L 273.

Wiessner S and Willard AR, ‘Policy-oriented jurisprudence and human rights abuses in internal conflict: toward a world of public order of human dignity’, (1999) 93 AJIL 316.

Wilde R, ‘The “Jurisdiction” Test in the Main Human Rights Treaties on Civil and Political Rights’ (2007) 40 Isr L Rev 505.

– – ‘Human Rights Beyond Borders at the World Court: the Significance of the International Court of Justice’s Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties’ (2013) 12(3) CJIL 639.

Regional and international cases

Al Saadoon and Mufdhi v the United Kingdom Admissibility Decision App no 61498/08 (ECtHR, 30 June 2009).

Al-Skeini and Others V. The United Kingdom App no 55721/07 (ECtHR, 7 July 2011).
Altuğ Taner Akçam v Turkey App no 27520/07 (ECtHR 25 January 2012).

Andreou v Turkey Admissibility Decision (ECtHR, 03 June 2008).

Andreou v Turkey Merits App no 45653/99 (ECtHR, 27 January 2010).

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) [2005] ICJ Report 168.

Baban v Australia (2003) U.N. Doc. CCPR/C/78/D/1014/2001 (2003)

Ballantyne, Davidson, McIntyre v. Canada (1993) U.N. Doc. CCPR/C/47/D/359/1989 and 385/1989/Rev.1 (1993).

Banković and Others v. Belgium and Others App no 52207/99 (ECtHR, 12 December 2001).

Başkaya And Okçuoglu v. Turkey App no 23536/94 and 24408/94 (ECtHR, 8 July 1999).

Big Brother Watch and Others v. the United Kingdom Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).

Bodrožić v. Serbia and Montenegro (2005) U.N. Doc. CCPR/C/85/D/1180/2003.

Case C-194/16 *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* [2017] ECLI:EU:C:2017:766.

Ricardo Canese v. Paraguay, Inter-American Court of Human Rights Series C No 111 (31 August 2004).

Cantoni v. France App no 17862/91 (ECtHR, 11 November 1996).

Catan and Others v. The Republic of Moldova and Russia App no 43370/04, 8252/05 and 18454/06 (ECtHR, 19 October 2012).

Celiberti de Casariego v. Uruguay (1981) CCPR/C/13/D/56/1979.

Cengiz et al. v. Turkey App no 48226/10 14027/11 (ECtHR, 1 March 2016).

Ceylan v Turkey App no 23556/94 (ECtHR, 8 July 1999).

Chauvy and Others v France App no 64915/01 (ECtHR, 29 July 2004).

Claude-Reyes et al. v. Chile, Inter-American Court of Human Rights Series C No 151 (19 September 2006).

Coard at al v US, Inter-American Commission on Human Rights Report N. 109/99 - Case 10.951.

Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism, Advisory Opinion OC-5/85 Inter-American Court of Human Rights Series A No. 5 (13 November 1985).

Custers, Deveaux and Turk v. Denmark App no 11843/03, 11847/03 and 11849/03 (ECtHR, 3 August 2008).

Cyprus v Turkey App no 6780/74 and 6950/75 (European Commission of Human Rights, 10 July 1976).

Cyprus v Turkey App no 25781/94 (ECtHR, 10 May 2001).

Democratic Republic of the Congo v. Burundi, Rwanda and Uganda African Commission on Human and Peoples' Rights, Communication 227/99 (May 2003).

Dink v Turkey App no 2668/07, 6102/08, 30079/08, 7072/09 et 7124/09 (ECtHR, 14 September 2010).

Tristán Donoso vs. Panama, Inter-American Court of Human Rights Series C No 193 (27 January 2009).

Drozd and Janousek v. France and Spain App no 12747/87 (ECtHR, 26 June 1992).

Joined Cases C–509/09 and C-161/10 *eDate Advertising GmbH v X and Olivier Martinez Robert Martinez v MGN Limited* [2011] ECR I–10269.

Editorial Board of Pravoye Delo and Shtekel v. Ukraine App no 33014/05 (ECtHR, 5 August 2011).

Monim Elgak, Osman Hummeida and Amir Suliman v Sudan, Comm. 379/09.

Fuentes Bobo v Spain App no 39293/98 (ECtHR, 29 February 2000).

Robert W. Gauthier v. Canada (1999) UN Doc CCPR/C/65/D/633/1995 (1999).

Gaweda v Poland App no 26229/95 (ECtHR, 14 March 2002).

Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772.

Written Observations of Article 19 and Others, 29 November 2017, case C-507/17 *Google Inc. v Commission Nationale de l'Informatique et des Libertés (CNIL)*.

Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317.

Griffiths vs Australia (2014) U.N. Doc. CCPR/C/112/D/1973/2010.

Groppera Radio Ag and Others v. Switzerland App no 10890/84 (ECtHR, 28 March 1990).
Guerra and Others v. Italy App no 14967/89 (ECtHR, 19 February 1998).

Gueye et al v France (1989) U.N. Doc. CCPR/C/35/D/196/1985 (1989).

G. V. France App no 15312/89 (ECtHR, 27 September 1995).

Handyside v the United Kingdom App no 5493/72 (ECtHR, 7 December 1976).

Case C-441/13 *Hejduk v EnergieAgentur.NRW GmbH* [2015] ECLI:EU:C:2015:28.

Herrera-Ulloa v. Costa Rica, Inter-American Court of Human Rights Series C No 107 (2 July 2004).

Hertel v. Switzerland App no 25181/94 (ECtHR, 25 August 1998).

Hertzberg v Finland (1985) U.N. Doc. CCPR/C/OP/1;

Hudoyberganova v. Uzbekistan (2004) U.N. Doc. CCPR/C/82/D/931/2000 (2004).

Ilaşcu and Others v. Moldova and Russia App no 48787/99 (ECtHR, 8 July 2004).

Isaak and Others v Turkey, App no 44587/98 Admissibility Decision (ECtHR, 28 September 2006).

Issa and Others v. Turkey App no 31821/96 (ECtHR, 30 March 2005).
J.H.A. v. Spain (2008) CAT/C/41/D/323/2007.

Kalda v Estonia App no 17429/10 (ECtHR, 6 June 2016).

Kimel v. Argentina, Inter-American Court of Human Rights Series C No 177 (2 May 2008).

Kivenmaa v Finland (1994) U.N. Doc. CCPR/C/50/D/412/1990 (1994).

Kokkinakis v. Greece App no 14307/88 (ECtHR, 25 May 1993).

Kononov v. Latvia App no 36376/04 (ECtHR, 17 May 2010) para 235;

Korbely v. Hungary App no 9174/02 (ECtHR, 19 September 2008).

Kyu Sohn v Republic of Korea (1995) U.N. Doc. CCPR/C/54/D/518/1992.

Ilmari Länsman et al. v. Findland (1992) UN Doc. CCPR / C / 52D / 511 / 1992.

Law Offices of Ghazi Suleiman v. Sudan, Comm. 220/98, 15th ACHPR AAR Annex V (2001-2002).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Reports 136.

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), Declaration of President Bedjaoui [1996] ICJ Rep 95.

Liberty and Others v the United Kingdom App no 58243/00 (ECtHR, 01 October 2008).

Samuel Lichtensztejn v Uruguay (1983) U.N. Doc. CCPR/C/OP/2 at 102 (1990).

Lingens v Austria App no 9815/82 (ECtHR, 8 July 1986).

Loizidou v. Turkey App no 15318/89 Preliminary objections (ECHR, 23 March 1995).

Loizidou v. Turkey App no 15318/89 (ECHR, 18 December 1996).

López-Álvarez v. Honduras, Inter-American Court of Human Rights Series C No 141 (1 February 2006).

Lopez Burgos v Uruguay (1981) U.N. Doc.CCPR/C/OP/1 at 88.

The Case of S.S Lotus [1927] PCIJ Series A N.10 18-19.

Markovic v Italy App no 1398/03 (ECtHR, 14 December 2006).

Francisco Martorell v Chile, Inter-American Court of Human Rights Series L V II.95 (3 May 1996).

McGinley and Egan v. the United Kingdom App no 21825/93 23414/94 (ECtHR, 9 June 1998).

Media Rights Agenda v. Nig., Comm. 105/93, 128/94, 130/94, 152/96, 12th ACHPR AAR Annex V (1998-1999).

Medio Ambiente y Derechos Humanos, Advisory Opinion OC-23/17 Inter-American Court of Human Rights (15 November 2017).

Medvedyev and others v. France App no 3394/03 (ECtHR, 29 March 2010).

Mouvement Raëlien Suisse v Switzerland App no 16354/06 (ECtHR, 13 July 2012).

Müller and Others v. Switzerland App no 10737/84 (ECtHR, 24 May 1988).

Mullai and Others v. Albania App no 9074/07 (ECtHR, 18 January 2012).

Varela Nunez v Uruguay (1983) U.N. Doc. CCPR/C/19/D/108/1981.

Observer and Guardian v. the United Kingdom App no 13585/88 (ECtHR, 26 November 1991).

Open Society Justice Initiative v. Cameroon, Comm. 290/2004, 20th ACHPR AAR Annex IV (2006-2007).

Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria App no 39534/07 (ECtHR, 28 February 2014)

Aleksey Ovchinnikov v. Russia App no 24061/04 (ECtHR, 16 March 2011).

Pad and Others v Turkey App no 60167/00 (ECtHR, 28 June 2007).

Palamara-Iribarne v. Chile, Inter-American Court of Human Rights Series C No 135 (22 November 2005).

Joined Cases C-585/08 *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)* [2010] 2010 I-12527.

Mabel Pereira Montero v. Uruguay (1983) U.N. Doc.CCPR/C/OP/2 at 136 (1990).

Perozo et al. v. Venezuela, Inter-American Court of Human Rights Series C No 195 (28 January 2009).

Perrin v the United Kingdom App no 5446/03 (ECtHR, 18 October 2005).

Petra v Romania App no 27273/95 (ECtHR, 23 September 1998).

Premininy v Russia App no 44973/04 (ECtHR, 26 June 2011).

Privacy International and Others v the United Kingdom App no 46259/16 Statement of Facts and Questions (ECtHR, 19 November 2018).

Privacy International and Others v the United Kingdom App no 46259/16 Admissibility Decision (ECtHR, 7 July 2020).

Ríos et al. v. Venezuela, Inter-American Court of Human Rights Series C No 194 (29 January 2009).

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000).

RTBF v. Belgium App no 50084/06 (ECtHR, 15 September 2011).

Inter-American Commission of Human Rights, *Saldaño v Argentina*, Inter-American Commission on Human Rights Report N. 38/99.

Sejdovic v. Italy App no 56581/00 (ECtHR, 1 March 2006).

S.G. v France (1991) U.N. Doc. CCPR/C/43/D/347/1988 at 8 (1991).

Shin v. Republic of Korea (2004) U.N. Doc. CCPR/C/80/D/926/2000.

Soering v. The United Kingdom App no 14038/88 (ECtHR, 7 July 1989).

Solomou and Others v Turkey App no 36832/97 (ECtHR, 24 September 2008).

Steel and Morris v. the United Kingdom App no 68416/01 (ECtHR 15 May 2005).

Stoll v Switzerland App no 69698/01 (ECtHR, 10 December 2007).

Tamiz v UK App no 3877/14 (ECtHR, 19 September 2017).

Társaság a Szabadságjogokért v. Hungary App no 37374/05 (ECtHR, 14 July 2009).

The Sunday Times v. the United Kingdom (no. 1) App no 6538/74 (ECtHR, 26 April 1979).

The Word 'Laws' in Article 30 of the American Convention on Human Rights, Advisory Opinion OC-6/86 Inter-American Court of Human Rights Series A No. 6 (9 May 1986).

Times Newspapers Ltd (nos. 1 and 2) v. The United Kingdom App no 3002/03 23676/03 (ECtHR, 10 June 2009).

Usón Ramírez v. Venezuela, Inter-American Court of Human Rights Series C No 207 (20 November 2009).

Sophie Vidal Martins v. Uruguay (1980) U.N. Doc. Supp. No. 40 (A/37/40) (1982).

Vrbica v Croatia App no 32540/05/2010 (ECtHR, 1 April 2010).

Weber and Saravia v Germany App no 54934/00 (ECtHR, 29 June 2006).

Wingrove v. the United Kingdom App no 17419/90 (ECtHR, 25 November 1996).

Yildirim v Turkey App no 3111/10 (ECtHR, 18 March 2013).

Youth Initiative for Human Rights v. Serbia App no 48135/06 (ECtHR, 25 September 2013).

Domestic cases

Alteen v. Informix Corp (1998) N.J. No. 122 1997 No. C.B. 439.

American Information Corp. v. American Infometrics, Inc., 139 F. Supp. 2d 696 (D. Md. 2001).

A.T. v Globe24H.com 2017 FC 114.

Breeden v Black 2012 SCC 19 666.

Coleman v MGN Limited [2012] IESC 20 [4] (Denham CJ).

Decision no. 2016-054 of March 10, 2016 of the Restricted Committee of the French Data Protection Authority issuing Google Inc. with a financial penalty < https://sites.les.univr.it/cybercrime/wp-content/uploads/2017/08/2016-google.pdf>

Dow Jones and Company Inc v Gutnick (2002) 210 CLR 575.

Equustek Solutions Inc. v. Jack 2014 BCSC 1063.

Equustek Solutions Inc. v. Google Inc., 2015 BCCA 265.

Equustek Solutions Inc. v Jack, 2018 BCSC 610.

Euromarket Designs Inc. v. Crate & Barrel Ltd. 96 F. Supp. 2d 824 (N.D. Ill. 2000).

Google Inc. v Equustek Solutions Inc. 2017 SCC 34.

Google LLC v Equustek Solutions Inc., et al., 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

Inset Systems Inc. v. Instruction Set Inc. 937 F. Supp. 161 (D. Conn. 1996).

Kiobel v Royal Dutch Petroleum Co. 569 U.S. 108 (2013).

Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996).

Microsoft Corp. v. United States, No. 14-2985 (2d Cir. 2016).

Privacy International and Greennet & Others v.s (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters [2016] UKIP Trib 14_85-CH.

R v Perrin [2002] EWCA Crim 747.

Tamiz v Google Inc. [2013] EWCA Civ 68.

TGI Paris, référé, 22 mai 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* as reported in Juriscom.net 'TGI Paris, référé, 22 mai 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France' (*Juriscom.net*) < http://juriscom.net/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/>

TGI Paris, référé, 11 août 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France* as reported in Legalis.net 'Tribunal de Grande Instance de Paris Ordonnance de référé du 11 août 2000' (*Legalis.net*) <https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-11-aout-2000/>

TGI Paris, référé, 20 Novembre 2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*.

United States v Evans et all 1987 SDNY 974.

Ward Group Pty Ltd v Brodie & Stone Plc [2005] FCA 471.

Yahoo! inc v La Ligue Contre le Racisme et l'Antisemitisme et al, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

Yeung, Sau Shing Albert v Google Inc. HCA 1383/2012 (5 August 2014).

Young v New Haven Advocate et al, 184 F. Supp. 2d 498 (W.D. Va. 2001).

Young v New Haven Advocate et al, 315 F.3d 256 (4th Cir. 2002).

Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

Reports

African Commission on Human and Peoples' Rights 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa' (Banjul 2016) ACHPR/Res.362(LIX)2016.

– – ‘Press Release on the growing trend of stringent regulation of the internet in East African States’ (Banjul 2018).

– – ‘Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the Continuing Trend of Internet and Social Media Shutdowns in Africa’ (Banjul 2019).

– – ‘Press Release by the Special Rapporteur on Freedom of Expression and Access to Information in Africa on the situation of freedom of expression and access to information in the Republic of Zimbabwe’ (Banjul 2019).

– – ‘Declaration of Principles on Freedom of Expression and Access to Information in Africa’ (OAU Banjul 2019).

Akdeniz Y, Freedom of Expression on the Internet, Vienna: The Representative on Freedom of the Media, 2012. ISBN 978-92-9234-638-6.

Article 29 Working Party ‘Guidelines on the Implementation of the Court of Justice of the European Union Judgment On “Google Spain and Inc. v Agencia Española De Protección De Datos (Aepd) and Mario Costeja González”’ C-131/12 26 November 2014.

Benedek W and Kettemann MC, Freedom of Expression and the Internet, Strasbourg: Council of Europe Publishing, 2013. ISBN 978-92-871-7702-5.

Bychawska-Siniarska D, Protecting the Right to Freedom of Expression under the European Convention on Human Rights, Strasbourg: Council of Europe, 2017.

Committee Against Torture Consideration of Reports Submitted by States Parties under Article 19 of the Convention, Conclusions and Recommendations: United States of America (25 July 2006) UN Doc. CAT/C/USA/CO/2.

Committee Against Torture Conclusions and Recommendations, United Kingdom of Great Britain and Northern Ireland, Crown Dependencies and Overseas Territories (10 December 2004) CAT/C/CR/33/3.

Committee Against Torture General Comment No. 2 Implementation of Article 2 by States Parties (24 January 2008) UN doc. CAT/C/GC/2.

Committee on Economic, Social and Cultural Rights Concluding Observations: Israel (4 December 1998) E/C.12/1/Add.27.

Committee on the Rights of the Child Thirty-first session Consideration of Reports Submitted by States Parties under Article 44 of the Convention Concluding observations: Israel (9 October 2002) CRC/C/15/Ad 195.

Council of Europe Committee of Ministers, Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom.

– – Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, Appendix to Recommendation CM/Rec(2016)5.

Council of the European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, Brussels, 2014.

Datainspektionen 'The right to be forgotten may apply all over the world' (Datainspektionen, 4 May 2017) <https://perma.cc/NT8D-42Z3>

Directorate of the Jurisconsult, Guide on Article 1 of the Convention – Obligation to respect human rights – Concepts of "jurisdiction" and Imputability, 30 April 2019.

– – Guide on Article 1 of the Convention – Obligation to respect human rights – Concepts of "jurisdiction" and Imputability, 31 August 2019.

– – Guide on Article 1 of the Convention – Obligation to respect human rights – Concepts of "jurisdiction" and Imputability, 31 December 2019.

– – Guide on Article 7 of the European Convention on Human Rights, 2020.

European Data Protection Board 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' 2 December 2019 <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en>

Governmental Advisory Committee 'Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains' (ICANN Archives, 5 April 2005) <https://archive.icann.org/en/committees/gac/gac-cctld-principles.htm>

HRC, Concluding observations of the Human Rights Committee Israel (18 August 1998) CCPR/C/79/Add.93.

– – General Comment No. 31 (26 May 2004) CCPR/C/21/Rev.1/Add. 13.

– – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Mr. Frank La Rue (20 April 2010) A/HRC/14/23.

– – General Comment No. 34 (12 September 2011) CCPR/C/GC/34.

– – The promotion, protection and enjoyment of human rights on the Internet (29 June 2012) A/HRC/20/L.13.

– – Concluding observations on the fourth periodic report of the United States of America (23 April 2014) CCPR/C/USA/CO/4.

– – Concluding observations on the fifth periodic report of France (21 July 2015) CCPR/C/FRA/CO/5.

– – Follow-up on concluding observations on State party reports (22 July 2015) CCPR/C/SR.3183.

– – Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland (17 August 2015) CCPR/C/GBR/CO/7.

Information Society Department Directorate General Human Rights and Rule of Law, Freedom of Expression in 2018, Council of Europe, 2019.

International Association of Penal Law, 'Nineteenth International Congress of Penal Law Topic: "Information society and penal law"' (AIDP) < http://www.penal.org/en/resolutions-last-congress>

Internet & Jurisdiction Policy Network 'Global Status Report 2019 Key Findings' (*Internet & Jurisdiction*, 2019) <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf>

– – 'Global Status Report 2019' (*Internet & Jurisdiction*, 2019) <https://form.jotformeu.com/93222419949364>

Korff D, The rule of law on the Internet and in the wider digital world, Council of Europe Commissioner for Human Rights, 2014.

– – and Brown I, 'Social Media and Human Rights' in Human Rights in a Changing Media Landscape, Strasbourg: Council of Europe Publishing, 2011. ISBN 978-92-871-7198-6.

López Aguilar JF, LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data, protection' 10 July 2019 <https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_coverletter_en.pdf>

Office of the Privacy Commissioner of Canada, 'Privacy Commissioner seeks Federal Court determination on key issue for Canadians' online reputation' (*Office of the Privacy Commissioner of Canada*, 10 October 2018) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181010/>

– – ‘Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy’ (*Office of the Privacy Commissioner of Canada*, 10 December 2019) <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/>

Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, ‘The Inter-American Legal Framework regarding the Right to Freedom of Expression’ (30 December 2009).

– – ‘Freedom of Expression and the Internet’ (31 December 2013).

– – ‘Standards for a Free, Open and Inclusive Internet’ (15 March 2017).

Organisation of American States, ‘Model Inter-American Law on Access to Public Information’ General Assembly Res AG/RES. 2607 (XL-O/10) (8 June 2010).

Research Division of the European Court of Human Rights, Internet: Case Law of the European Court of Human Rights, Council of Europe/European Court of Human Rights, 2015.

UN Committee Against Torture General Comment No. 2: Implementation of Article 2 by States Parties 24 January 2008 CAT/C/GC/2.

UNGA, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (4 September 2013) A/68/362.

UN Secretary-General and UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General, (22 July 2015) A/70/174.

UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the

Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet' (1 June 2011).

University of Geneva 'Geneva Internet Disputes Resolution Policies 1.0' (*Geneva Internet Disputes Resolution Policies 1.0*) <https://geneva-internet-disputes.ch/>

World Summit on the Information Society, Tunis Agenda for the Information Society (18 November 2005) WSIS-05/TUNIS/DOC/6(Rev.1)-E.

Internet sources

Art. 46 nouv. C. pr. civ, English translation as reported in Legifrance 'Code Of Civil Procedure' (*Legifrance*) <https://www.legi**france**.gouv.fr/content/download/1962/13735/version/3/.../**Code**_39.pdf>

Barlow JP, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 1996) < https://www.eff.org/cyberspace-independence>

Berkes A, 'A New Extraterritorial Jurisdictional Link Recognised by the IACtHR' (*EJIL: Talk!*, 28 March 2018) <https://www.ejiltalk.org/a-new-extraterritorial-jurisdictional-link-recognised-by-the-iacthr/>

Cambridge Dictionary 'Triad' (Cambridge Dictionary) <https://dictionary.cambridge.org/dictionary/english/triad>

Canales MP, 'Repaso a la Jurisprudencia de la Corte Europea y las Altas Cortes de la region en materia de Internet', (03 May 2019) <https://vimeo.com/334638074> (accessed 12 August 2020).

Canela G, 'Panel El Articulo 13 de la Convencion Inter-Americana y la protection de la libertad de expression en Internet', (03 May 2019) <https://vimeo.com/334638074> accessed 12 August 2020.

Columbia University Global Freedom of Expression, 'Dr. Yeung, Sau Shing Albert v. Google Inc.' (*Columbia University Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/dr-yeung-sau-shing-albert-v-google-inc/>

Corn G, 'Tallinn Manual 2.0 – Advancing the Conversation' (*Just Security*, 15 February 2017) <https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/#more-37812>

Daskal J, 'Three Key Takeaways: The 2d Circuit Ruling in The Microsoft Warrant Case' (*Just Security*, 14 July 2016) <https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case/>

European Data Protection Supervisor 'Glossary - Article 29 Working Party' (European data Protection Supervisor) <https://edps.europa.eu/data-protection/data-protection/glossary/a_en>

Geist M, 'Courts adopt aggressive approach in cross-border Internet jurisdiction cases' (*The Star.com*, 5 January 2013). <https://www.thestar.com/business/2013/01/05/courts_adopt_aggressive_approach_in_crossborder_internet_jurisdiction_cases.html#.UOrJtuIHp7w.twitter>

– – 'Global Internet Takedown Orders Come to Canada: Supreme Court Upholds International Removal of Google Search Results' (*Michael Geist*, 28 June 2017) <http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results/>

Internet & Jurisdiction Policy Network, 'I&J Observatory Members' (*Internet & Jurisdiction*) <https://www.internetjurisdiction.net/work/observatory/members>

– – 'I&J Observatory' (*Internet & Jurisdiction*) <https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMjAtMDcifQ==>

– – ‘US Court issues preliminary injunction to block enforcement in the US of Google de-indexation ordered by Canadian Supreme Court’ (*Internet & Jurisdiction Retrospect Database*, November 2017) <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiZXF1dXN0ZWsiLCJmcm9tIjoiMjAxMi0wMiIsInRvIjoiMjAxOC0wMSJ9>

– – ‘Canada’s Federal Court applies national data protection law against Romanian website’ (*Internet & Jurisdiction Retrospect Database*, February 2017) <https://www.internetjurisdiction.net/publications/retrospect#eyJmcm9tIjoiMjAxNy0wMSIsInRvIjoiMjAxNy0xMiJ9>

– – ‘France’s highest administrative court refers Google right to be de-indexed case to CJEU’ (*Internet & Jurisdiction Retrospect Database*, December 2017) <https://www.internetjurisdiction.net/publications/retrospect#eyJjYXRlZ29yaWVzIjpbIjE2NiJdLCJ0byI6IjIwMTctMTIiLCJmcm9tIjoiMjAxMi0wMiJ9>

Keller D, ‘Global Right to Be Forgotten. Delisting: Why CNIL is Wrong’ (*Stanford Center for Internet and Society*, 18 November 2016 <http://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong>

Kiratisountorn T and others, ‘Thailand Personal Data Protection Law’ (*The Norton Rose Fulbright Data Protection Report*, 28 February 2020) <https://www.dataprotectionreport.com/2020/02/thailand-personal-data-protection-law/>

Kravetz D, 'Does US have right to data on overseas servers? We’re about to find out' (*ArsTechnica*, 24 June 2017) <https://arstechnica.com/tech-policy/2017/06/supreme-court-asked-to-decide-if-us-has-right-to-data-on-foreign-servers/>

Kulesza J, ‘Internet Governance and the Jurisdiction of States. Justifications for the need of an international regulation of cyberspace’ (2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1445452>

Legal Information Institute 'Alien Tort Statute' *Cornell Law School* <https://www.law.cornell.edu/wex/alien_tort_statute>

Microsoft 'Resources: Microsoft's Search Warrant Case' (2014) (*Microsoft*, December 2014) < https://blogs.microsoft.com/datalaw/resource/initiative/microsofts-search-warrant-case/page/3/>

Milanovic M, 'ECtHR Judgment in Big Brother Watch v. UK' (*EJIL: Talk!*, 17 September 2018) <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/>

Neuman GL, 'Has the Human Rights Committee Extended its Reach?' (*Just Security*, 29 July 2015) <https://www.justsecurity.org/25022/human-rights-committee-extended-reach/>

Oyez 'United States v. Microsoft Corporation' (*Oyez*) <https://www.oyez.org/cases/2017/17-2>

Scassa T, 'Federal Court Orders Romanian Website Operator to Take Down Canadian Court Decisions Under Privacy Statute' (*Teresa Scassa*, 21 February 2017) <http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=242:federal-court-orders-romanian-website-operator-to-take-down-canadian-court-decisions-under-privacy-statute&Itemid=80>

Schmitt M, 'US Transparency Regarding International Law in Cyberspace' (*Just Security*, 15 November 2016) <https://www.justsecurity.org/34465/transparency-international-law-cyberspace/>

SCOTUS blog 'United States v. Microsoft Corp.' (*SCOTUS blog*) <https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/>

Smith D, 'Has the search result ruling stopped the internet working?' (*Information Commissioner's Office*, 2 November 2015) <https://www.wired-gov.net/wg/news.nsf/articles/Has+the+search+result+ruling+stopped+the+internet+working+03112015152000?open>

Solmone S, ‘Establishing Jurisdiction Online: the Problem of the Access-based Jurisdictional Principle’ (RIPE Labs, 16 October 2017) <https://labs.ripe.net/Members/sara_solmone/establishing-jurisdiction-online>

Suwanprateep D, ‘Postponement of Thailand's Personal Data Protection Act (PDPA)’ (Lexology, 12 May 2020) <https://www.lexology.com/library/detail.aspx?g=c628a738-f929-4987-b6db-b0ee00e69b30>

Wildy & Sons Ltd ‘Leading Internet Case Law’ (*Wildy & Sons Ltd*) <https://www.wildy.com/isbn/2399-0015/e-commerce-law-reports-print-online-law-reports-online-cecile-park-publishing>

Yaman Akdeniz, ‘Case analysis of League against Racism and Antisemitism (LICRA), French Union of Jewish Students v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Pairs), Interim Court Order, 20 November, 2000’ (*Yaman Akdeniz Academia.edu*) <https://www.academia.edu/943441/Case_Analysis_of_League_Against_Racism_and_Antisemitism_LICRA_French_Union_of_Jewish_Students_v_Yahoo_Inc_USA_Yahoo_France_Tribunale_de_Grande_?auto=download>

International treaties, directives and regulations

African Charter on Human and Peoples' Rights (entered into force 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217 (African Charter)

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 (Pact of San José).

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) 1465 UNTS 85.

Convention for the Protection of Human Rights and Fundamental Freedom (adopted 4 November 1950, entered into force 03 September 1953) 213 UNTS 221 (European Convention on Human Rights).

Convention on Cybercrime (adopted 23 November 2011, entered into force 1 July 2004) ETS No.185.

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJL12/1.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

International Convention on the Elimination of All Forms of Racial Discrimination (adopted 7 March 1966, entered into force 12 March 1969) 660 UNTS 195.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

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 [2012] OJ L 351/1 entered into force on 10 January 2015.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJL 119/1.

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

Domestic laws

H.R.4943 CLOUD Act.

Intelligence Services Act 1994.

Loi Informatique et Libertes Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties.

Obscene Publications Act 1959.

Va.Code Ann. § 8.01-328.1(A) (3).