

The Territorial Jurisdiction for Transnational Cybercrime: A Reading of French Case Law

Bouzidi Iliyes*

¹ University Centre of Maghnia (Algeria), i.bouzidi@cu-maghnia.dz

Received: 02/06/2026

Accepted: 11/06/2026

Published: 13/06/2026

Abstract:

Solving the issue of territorial jurisdiction in cybercrimes requires reconsidering traditional legal criteria and adopting flexible rules that suit the virtual, cross-border nature of the internet. One of the most prominent legally adopted solutions is expanding the application of the "principle of criminal result." Under this principle, judicial jurisdiction is granted to the state that suffered damage or where the effects of the crime appeared, even if the execution took place outside its geographical borders.

Modern jurisprudence also employs the "server location or digital infrastructure" standard, extending state jurisdiction to any digital media used in perpetrating the crime and located within its territory. The "content availability and accessibility" standard is also adopted, granting national courts jurisdiction over the crime simply by the ability to access the targeted website or platform within the state, thus facilitating the protection of victims and the legal prosecution of perpetrators.

Keywords: cybercrime; principle of territoriality; jurisdiction; globalization; sovereignty.

1. INTRODUCTION

The rapid evolution of communication networks, the widespread use of the internet within companies, and the constant accessibility to sensitive information or data within organizations have led to an increase in cybercrime. Although crime is inherent in societies, it remains a challenge in terms of its evolution: just as it has been linked to economic development across land, sea, and air domains, it has now also become intertwined with development within cyberspace.

In fact, cyberspace—often referred to as a virtual, non-physical environment—has become a theater for various crimes that inflict severe damage on both economic operators

*Bouzidi Iliyes

and civil society. Consequently, cybercrime constitutes a reality that the law cannot afford to ignore.

From this perspective, determining judicial jurisdiction allows for a better understanding of the distinct roles judges play in combating cybercrime. On one hand, this raises questions regarding the specific competencies of the judge based on different potential criminal classifications. On the other hand, it brings up issues concerning territorial jurisdiction, given the transboundary nature of these offenses.

Once territorial jurisdiction is established to penalize the cybercriminal, questions regarding subject-matter jurisdiction inevitably arise. From this angle, multiple jurisdictions intervene as different legal procedures overlap simultaneously. At this stage, it is worth noting the convergence of criminal procedures among European Union member states.

This crime can be domestic, international, or transnational. It is domestic when it occurs entirely within one country's territory. It is international when one party is an international entity. It is transnational when committed within one country, but its effects extend beyond its borders¹.

To analyze how judges handle cybercrime, it is useful to compare the work of judges within European Union member states with how the European Union court addresses digital crimes.

Judges receive jurisdiction based on connectivity criteria set by legal texts or the case's link to a specific area. Thus, statutory jurisdiction usually aligns with judicial jurisdiction.

It frequently occurs that these two jurisdictional criteria do not align; a specific law may govern the merits of a case, yet the underlying facts fall outside the territorial jurisdiction of the court reviewing them. For instance, in its decision dated December 10, 2013, the Grenoble Court of Appeal ruled that the Grenoble court lacked jurisdiction over a case involving comments published on a Belgian blog², even though French law was applicable to the facts in question³.

¹ Arab Maryam, "Jurisdiction in Cybercrimes," *Annals of the Faculty of Law and Political Science, University of Oran 2*, Volume 7, Issue 3, 2015, p. 269.

² The facts leading to the judgment reveal that Mr. B., a police officer in charge of the intelligence department in Lyon, France, and residing in Belgium, was found guilty of disclosing confidential information regarding the organization of a police station during his long-term sick leave. He transmitted confidential information through his blog maintained in Belgium. Consequently, he was questioned by the judges, and the court of first instance sentenced him, based on Article L 226-13 of the Penal Code, to a suspended two-month prison sentence. On appeal, the judges declared that the French courts lacked jurisdiction, given that no procedural document had been sent to Mr. B. in France. All documents were sent to him in Belgium, to his place of residence and his known address with the police.

³ Grenoble Court of Appeal, First Chamber, Judgment of December 10, 2013.

Given the borderless nature of the internet and digital networks, how is the issue of territorial jurisdiction resolved when allocating authority over cybercrimes?

To address this issue, the research employs a descriptive-analytical approach to deconstruct relevant legal texts, supported by a comparative approach through a review of French judicial rulings on the matter. Accordingly, the study is divided into three main sections: the first examines indicators of the international nature of transnational cybercrime; the second discusses the criteria for determining territorial jurisdiction; and the third explores the difficulties of applying the principle of territoriality to this type of crime.

2. Indicators of the international nature of transnational cybercrime

Criminal liability is primarily based on the principle of the personality of punishment, meaning that an individual is only held accountable for their own personal actions, whether they committed the crime as a principal perpetrator or as an accomplice. This principle extends to cybercrimes, where everyone who contributes to an illicit act online bears the legal consequences of their actions.

However, the digital space introduces unique complexities in applying this principle, particularly regarding the liability of technical intermediaries. On one hand, questions arise about the extent of liability for Internet Service Providers (ISPs) and web hosts (*les habergeons*) regarding illegal content they transmit or host without having created it themselves.

On the other hand, cyberspace raises the dilemma of determining territorial jurisdiction. Due to the absence of digital geographical borders and the fragmentation of data, web hosts can manage their servers from multiple distinct countries and regions, leading to a conflict of national laws applicable to these acts.

Would you like to specify the law of a particular country to see how it regulates the liability of these intermediaries? Or would you prefer to explore the international conventions that govern jurisdiction in cyberspace?

2.1 The criminally liable party in transnational cybercrime

The principle of personal liability in cyberspace requires a precise definition of criminal roles; the law distinguishes between publishers, who bear full liability as content creators and controllers, and internet service providers (ISPs) and hosting providers, who enjoy conditional criminal immunity as mere technical intermediaries for data transmission and storage, and thus cannot be prosecuted unless it is proven that they had actual knowledge of illegal content and deliberately failed to remove it or disable access to it.

2.1.1 The Hosts

They are natural persons or legal entities (companies) that provide – for a fee or free of charge – digital spaces on the Internet to store and preserve various types of data, such as texts, images, sounds, and signals. These entities ensure the provision of the infrastructure and technical means necessary to enable users, whether individuals or institutions, to access and share their stored content around the clock¹.

From a legal perspective, and in application of the principle of personal liability, hosting providers are exempted from criminal and civil liability arising from any illegal content published by users, provided they have no prior knowledge of the existence of these violations or illicit content on their servers².

2.1.2 Internet service providers

The criminal liability of Internet Service Providers (ISPs) is governed by a well-established legal principle known as "personal liability." This principle means that no criminal liability can be established against these entities unless the illegal acts can be personally and directly attributed to them. In essence, the provider lacks criminal intent regarding the content published by users over its network.

Legally and technically, an ISP is defined as any natural or legal person acting as a technical intermediary. They allow the public to access the telecommunications network and ensure the transmission of content, messages, and information related to a specific topic. This content is made available to users either free of charge or for a financial fee, without the provider being the original creator of this data³.

In many cases, technical roles overlap, as an ISP can also play the role of a "host." In this scenario, the law applies a general principle of non-liability for the content stored on their servers. This is due to their lack of actual control over the materials users choose to publish.

To crown this legal protection, service providers and hosts are exempted from any general obligation to monitor the information passing through their networks or stored on their servers. The law does not require them to proactively search for illegal activities, given the technical impossibility of doing so and its conflict with privacy protection. Their liability only arises if they fail to act promptly to remove illegal content after being officially notified.

¹ Ibrahim Sabri Al-Arnaout, The Extent of Civil Liability of Internet Service Intermediaries, A Comparative Study, Algerian Journal of Comparative Law, Abu Bakr Belkaid University of Tlemcen, Volume 3, Issue 5, 2020, p. 8.

² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), OJ L 178, 17.7.2000, p. 1.

³ Ibrahim Sabri Al-Arnaout, op.cit, p. 5.

2.1.3 the publishers

While the author of illegal content is directly liable in criminal matters, the publisher is also responsible because they guarantee editorial control. Consequently, the publication director is held liable when they have the opportunity to access and verify the information before its publication¹.

This distinction between the host's non-liability and the publisher's liability is well understood because the publisher is personally responsible for distributing the content: by exercising editorial selection, they can be held liable for illegal content. The same applies to bloggers, who act as both the authors and publishers of their online articles².

Historically, the technical host was exempt from liability because its role was limited to data storage, while the publisher bore full responsibility because it intervened in the content. However, as platforms evolved, the law granted judges the authority to reclassify a "host" as a "publisher" if its role extended beyond passive storage.

This legal shift occurs when a platform assumes an active editorial role, such as organizing content into sections and topics, using algorithms to manipulate content, or integrating ads into hosted pages to generate revenue. This intervention strips the platform of its legal immunity and makes it directly liable for any infringing content³.

2.2 The website for transnational and regional cybercrime

Determining the location of a cybercrime is a critical step for applying the territorial standard of law and identifying the digital identity of perpetrators. By establishing where the crime occurred, a state can assert its judicial jurisdiction and investigate the incident under its national laws. Furthermore, tracking digital footprints, such as Internet Protocol (IP) addresses, helps uncover the true identities of cybercriminals and trace their locations.

However, this process faces a complex legal challenge in reconciling the strict geographical limitations of criminal law with the boundless, global nature of digital networks. Traditional laws were designed to protect specific territorial borders, whereas the digital environment is characterized by speed and the ability to cross continents in fractions of a second. This disparity allows criminals to launch attacks from one country, target servers in a second, and cause harm to victims in a third.

As a result of this overlap, the effectiveness of punitive and repressive laws becomes "relative" and limited in cyberspace due to each state's adherence to its national

¹ ECHR, 2nd Section, 30 March 2004, application no. 53984/00, *Radio France and another v. France*.

² The judgment rendered by the Paris Court of Appeal on June 6, 2007 (case of *Google Inc. and Google France v. Axa SA and others*, No. 06/14890).

³ CA Paris, October 29, 2008, *MySpace v. Lafesse*; see Ph. Stoeffel-Munck, column "Responsibility and contracts", *Comm. com. électr.*, 2009, p. 36.

sovereignty. Since law enforcement authority stops at political borders, pursuing criminals or gathering external digital evidence is impossible without clashing with the barrier of sovereignty. This situation creates a pressing need to move beyond local solutions toward crafting flexible international cooperation agreements to combat cybercrime effectively¹.

2.2.1 National sovereignty and overlapping jurisdictions in cybersecurity

States maintain their national sovereignty and regional criminal laws despite the existence of international cooperation and agreements that seek to unify legislation against cybercrimes; states ensure their legal independence by placing reservations on those agreements, which makes penal law a pure expression of the state's authority within its geographical borders.

This traditional principle raises a fundamental question about its effectiveness in dealing with transnational cybercrimes. Under the territoriality standard, jurisdiction lies with the state in whose territory the crime occurred, which is what French criminal law applies, extending its authority to cover all cybercrimes committed or realized on the territory of the French Republic².

The emergence of cross-border cyberspace has driven nations to expand the traditional concept of "territorial jurisdiction." National courts are no longer limited to prosecuting crimes that occur entirely within their physical borders. Instead, they now extend their authority to cover any cybercrime where even a minor part—such as the location of the victim or the server—touches their territory³. This expansion allows local penal laws to automatically apply to acts committed in the digital world, opening the door for multiple judicial authorities to claim jurisdiction over the exact same crime⁴.

Consequently, the international legal system faces a crisis of "conflict of jurisdiction," where multiple countries seek to prosecute the same defendant for the same act. This directly violates the universal legal principle that prohibits trying or punishing a person twice for the same offense (*non bis in idem*). The solution does not lie in unifying or standardizing laws across countries, because the core issue is each nation's insistence on asserting its own sovereignty. As a result, national courts often ignore final judgments issued abroad and insist on re-prosecuting the individual, thereby increasing the risk of

¹ M. Delmas-Marty, *The Imaginative Forces of Law*, vol. 1, *The Relative and the Universal*, Paris, Le Seuil, 2004, p. 336.

² Article 113-2 of the French Penal Code

³ D. Rebut, *International Criminal Law*, 2nd ed., *Précis Dalloz*, Paris, Dalloz, 2014; Cass. crim. 12 February 1979, Bull. crim. no. 60; 1 October 1986, no. 262; 26 September 2007, no. 224.

⁴ Cass. crim., September 11, 2007, No. 07-82018; February 4, 2004, Bull. crim. No. 32, D. 2005, p. 621, note V. Malabat

overlapping and conflicting international legal proceedings¹.

The legal dilemma lies in determining territorial jurisdiction for cybercrimes. Due to the transnational nature of the internet, courts find it difficult to identify the country with jurisdiction to prosecute the perpetrator, leading to conflicting judicial rulings based on two criteria. The first criterion focuses on the "place of issuance or origin" (the location of the message or server), an approach that creates a serious loophole allowing criminals to base their activities in countries with lax laws or "digital safe havens" to evade legal punishment.

The second criterion depends on the "place of reception or accessibility" of the website, which is also facing sharp criticism. Since the internet is available globally, this criterion gives every country in the world the right to declare its jurisdiction simply by being able to browse the site, which causes chaos of "overlapping jurisdictions" and conflict of laws, and creates a state of legal insecurity where website owners find themselves governed by the conflicting laws of several countries at the same time².

The French judiciary has begun addressing cybercrime by adopting flexible and broad criteria for asserting its territorial jurisdiction. French courts have deemed the mere possibility of accessing a website from within France (the accessibility criterion)³ or the ability to download and receive its content on French territory (the message reception criterion) sufficient to establish that a cybercrime occurred in France, thus triggering the jurisdiction of its national courts.

This expansive judicial approach quickly extended to other legal areas of social and economic sensitivity. The courts applied the same standard to crimes committed through digital media, such as libel and defamation, asserting their jurisdiction as soon as the article appeared in France⁴. This pattern was repeated to protect public health and the market economy in cases of defamation of pharmaceutical products⁵, as well as in cases regulating the financial market and online betting to block unlicensed foreign websites operating within the French market⁶.

Nevertheless, the French judiciary has undergone a radical shift in intellectual property and copyright cases, moving away from the "accessibility" standard, which had become criticized for its excessive broadness. The courts now require, as a fundamental

¹ Council of Europe, Evaluation Report: the provisions of the Budapest Convention on Cybercrime concerning mutual legal assistance, adopted by the T-CY, Cybercrime Convention Committee, Strasbourg, 3 December 2014, 216 p.

² M. Vivant, "Cyberworld: law and network rights", JCP, 1996, 1, 3969.

³ Paris High Court, summary proceedings, May 22 and November 20, 2000, Comm. com. électr. 2000, comm. no. 92; Paris High Court, 17th Chamber, February 26, 2002, Comm. com. électr. 2002, no. 77.

⁴ Paris High Court, November 13, 1998, Gazette du Palais, 2000, 1, legal doctrine, p. 697.

⁵ Criminal Chamber of the French Court of Cassation, 15 January 2008, Criminal Bulletin, Judgment number 5.

⁶ Nanterre Criminal Court, 15th Chamber, March 15, 2007, Review of Criminal Sciences, 2008, p. 101, obs. J. Francillon.

condition for considering a crime to have been committed in France, the application of the "concentration standard." This means proving that the infringing foreign website did not simply appear in France by chance, but rather deliberately and intentionally directed its activity and content toward the French consumer audience¹.

2.2.2 National sovereignty and overlapping jurisdictions in cybersecurity

The European Court of Justice based its rulings on the interpretation of Article 5.3 of the Brussels Regulation I, which concerns the determination of the competent court to adjudicate tort cases². According to this text, any person residing in a member state within the European Union can be prosecuted in the courts of another member state, specifically in the place where the harmful act occurred or is expected to occur.

The Court of Justice of the European Union has issued a ruling on the issue of the location of cybercrimes, particularly in matters relating to personal and trademark rights³. This jurisprudence has also evolved through the acceptance of the accessibility criterion and then the focus criterion. However, the development of European jurisprudence remains either "selective" or "pluralistic"⁴.

Thus, in matters of trademark infringement, the Court of Justice of the European Union, in its ruling in the Wintersteiger case, held that recourse may be made to the courts of the Member State in which the advertiser is located, such as the courts of the place where the causative event took place; or the judges of the Member State in which the trademark is registered⁵.

When considering online trademark infringement cases, the traditional standards of private international law are transcended. In the digital environment, the judge does not simply examine the "accessibility" of a website to users in a particular country, or the extent to which the website "targets" an audience in that country. Instead, the jurisdiction and national law of the country where the trademark is registered and enjoys legal protection are considered.

This approach stems from the "unique nature of counterfeiting," a blatant violation of intellectual property rights with negative repercussions for the national economy and consumer protection against deception. This specific nature of the crime necessitates that courts disregard technical formalities, such as server location or domain name, to ensure effective legal deterrence and combat piracy, preventing counterfeiters from exploiting

¹ Crim. Chamber of the French Supreme Court, 14 December 2010, Appeal No. 10-80.088, Dalloz Collection, 2011, p. 1055, commentary by E. Dreyer.

² Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Article 5(3), OJ L 12, 16.1.2001, p. 1

³ Court of Justice of the European Union (CJEU), 12 July 2011, L'Oréal SA and Others v eBay International AG and Others, Case C-324/09.

⁴ F. Pollaud-Dulian, "Jurisdiction. Online infringement. Internet-Accessibility", RTD com., 2013, p. 733.

⁵ CJEU, April 19, 2012, Wintersteiger, Case C-523/10, D. 2012, p. 1926, note by T. Azzi.

cross-border digital vulnerabilities to evade punishment.

3. Determining territorial jurisdiction for transnational cybercrime

In terms of territorial jurisdiction, Article 22(1) of the 2001 Budapest Convention on Cybercrime adopts broad and comprehensive criteria for determining jurisdictional options. This article mandates each State Party to adopt the necessary legislative and other measures to establish jurisdiction over the cybercrimes specified in the Convention. This jurisdiction extends to offenses committed within the state's territory, onboard a ship flying its flag, or inside an aircraft registered under its laws. Furthermore, jurisdiction encompasses offenses committed by a state's nationals abroad, provided that the act is punishable under the penal law of the country where it occurred, or if the offense falls outside the territorial jurisdiction of any other state.

On the other hand, the Convention does not preclude any criminal jurisdiction exercised by a State Party in accordance with its domestic law. In the event of a positive conflict of jurisdiction, where more than one State Party claims jurisdiction over the same alleged offense, the Convention requires the concerned states to consult and coordinate with one another. The objective of these consultations is to determine which country is best positioned to initiate prosecution and handle the judicial proceedings.

Consequently, it is evident that Article 22 primarily aims to prevent legal vacuums by ensuring that at least one competent judge is available to hear the case. However, implementing this multiplicity of jurisdictional criteria faces complex practical challenges in real-world application. This difficulty is clearly demonstrated by various judicial decisions and rulings issued by different courts in this regard.

A judge establishes territorial jurisdiction based on either the "accessibility theory" or the "targeting theory" (focus theory), both of which have been clarified through various judicial rulings. Regarding the accessibility theory, the territorial jurisdiction of the judge is determined by the mere fact that the content is publicly accessible online via the website.

3.1 accessibility theory

The accessibility theory is a legal criterion used by courts to determine a judge's territorial jurisdiction in internet disputes (defamation, trademark infringement, copyright violation). According to this theory, a court has jurisdiction as long as the website in question is technically accessible from the territory of the country where that court is located.

3.1.1 Yahoo's decision issued by the High Court of Claims in Paris on May 22, 2000

The facts leading to this judicial ruling center on "Yahoo!" broadcasting

The Territorial Jurisdiction for Transnational Cybercrime: A Reading of French Case Law

advertisements on its website that offered Nazi items and memorabilia for sale via public auction. As these advertisements reached internet users within France, a key legal question arose regarding the jurisdiction of French judges to adjudicate a dispute involving online commercial activities conducted by a foreign company, which nevertheless directly impacted the values of French society and its penal legislation prohibiting the trade of Nazi symbols¹.

In this context, French jurisprudence recognized the jurisdiction of local courts under the landmark ruling issued by the Tribunal de Grande Instance de Paris (Paris Grand Instance Court) on May 22, 2000. The court based its judgment on the criterion of "accessibility." It ruled that because the website in question was accessible on French territory and could be reached by users residing in France, the effects of this action and the resulting damage occurred directly within France.

The legal solution adopted by the judge affirmed the jurisdiction of the French court on the grounds that permitting the viewing of these prohibited items in France, along with the potential participation of a French-resident internet user in such an offer and sale, rendered Yahoo! an entity that committed a legal fault extending onto French territory. Consequently, the judge took into account not only that the offense had a local impact but also that the moral and social damage was sustained in France. This justified the issuance of an interim injunction ordering the company to cease broadcasting these auctions to French users.

The impact of this interim decision was not limited to this case alone; it deeply influenced the broader issue of international jurisdiction in cyberspace across subsequent, similar cases. This legal evolution culminated in the definitive establishment of this theory by the Civil Chamber of the French Court of Cassation in its ruling on the famous Cristal case in 2003. As a result, the criterion of accessibility, combined with the presence of fault and damage within national territory, became an established principle in French private international law.

3.1.2 The French Court of Cassation's decision known as the Cristal decision, issued on December 9, 2003

This is a landmark judicial decision issued by the First Civil Chamber of the French Court of Cassation on December 9, 2003, known as the "Cristal" case. This decision addresses a complex legal issue that arose with the advent of the internet age: how to determine the jurisdiction of national courts (in this case, French courts) to hear claims for damages resulting from the infringement of intellectual property rights by foreign

¹ Paris High Court, Interim Order of August 11, 2000, "Union of Jewish Students of France" Association, "League against Racism and Anti-Semitism" v. Yahoo! Inc. and Yahoo France.

websites¹.

The dispute stems from a lawsuit filed by the French winery Louis Roederer, owner of the trademark "Cristal" (a trademark protecting a distinctive champagne bottle design), against a Spanish company called Castellbajac. The Spanish company had displayed and marketed a bottle with a similar design on its website without authorization, prompting the French company to consider this online display an infringement on its territory and commercial rights.

In response, the Spanish company argued, based on the nature of the digital space, that its website was intended solely for consumers within Spain. It faced sharp criticism of the French courts for disregarding the global and transnational nature of the internet, as the French judiciary at the time considered the mere "accessibility" of the site from within France sufficient to establish its jurisdiction.

This unstable judicial standard has raised concerns among legal scholars, who have criticized its adoption because it opens the door to what is known as "forum shopping." This phenomenon refers to litigants selecting and extending the jurisdiction of the court most biased in their favor to protect their own interests (such as a French company resorting to the French courts, which are more protective of local trademarks). This is a legal loophole that allows parties to evade the application of their home country's national laws and submit the dispute to a foreign jurisdiction².

In conclusion, the importance of this decision lies in the fact that it constituted a turning point that prompted the French and European judiciary to later abandon the standard of "mere accessibility of the site" and move towards a more precise standard known as the "targeting standard"; which requires proving that the foreign site directs its activity and offers specifically and deliberately towards the public within the French territory in order for jurisdiction to be established for the French courts.

3.1.3 Case of Sociétés Google Inc. et Google France c/ Axa et autres dated November 23, 2010.

This decision demonstrates the French judiciary's adaptation to digital developments in online disputes. French courts have updated their standards for international jurisdiction, particularly in trademark infringement cases.

This represents a radical shift in the approach of the French Court of Cassation. It has abandoned the unrestricted "accessibility" standard and replaced it with the more

¹ Judgment of the First Civil Chamber of the Court of Cassation of December 9, 2003, published in Bulletin 2003, I, No. 245, p. 195.

² Rafaa Ahmed Belabidi, Al-Sadiq Abdelkader, the effectiveness of the optional submission clause as a mechanism for determining international judicial jurisdiction in e-commerce contract disputes, International Journal of Legal and Political Research, University of El Oued, Volume 5, Issue 3, 2021, p. 298.

The Territorial Jurisdiction for Transnational Cybercrime: A Reading of French Case Law

realistic "targeting and evidence" standard, which requires proof that a website's activity is directed toward a French audience.

The case began when the renowned insurance group (AXA) and its subsidiaries (Avansur and Direct Assurances) noticed that competing companies were exploiting their legally protected trademarks. It was revealed that these competitors had purchased AXA's trademark names as keywords through Google's advertising system. As a result, advertisements for competing companies appeared to users as soon as they typed terms like AXA or AGIPI into the search engine, which the group considered a flagrant infringement on its intellectual property and unfair competition.

In response to this action, AXA filed a lawsuit directly against Google Inc (the US entity) and Google France before the French court of first instance (Tribunal de Grande Instance), accusing them of trademark infringement and complicity. For its part, Google attempted to evade liability by challenging the legitimacy of the trial, arguing that French courts lacked both territorial and subject-matter jurisdiction over the lawsuit. This defense was based on the technical and global nature of the internet and the fact that the parent company is located outside France. However, the lower court judge rejected Google's arguments, affirmed the court's jurisdiction, and issued a legal order against it, prompting Google to appeal the ruling on August 8, 2006.

This initial ruling sparked a broad legal and jurisprudential debate among trial judges in France regarding the precise legal criteria for determining jurisdiction in internet-related disputes. This controversy culminated on June 6, 2007, when the Paris Court of Appeal launched a judicial opposition movement against previous expansionist rulings. The court adopted a new, narrower approach to the jurisdiction of French courts. It required proof of a close and direct link between the advertising activity and the target audience within French territory, rather than merely relying on the accessibility of the website from France¹.

The Court of Appeal excluded the jurisdiction of French judges based on a purely physical criterion: the fact that the disputed websites were hosted on servers located abroad. Consequently, it ruled that the Paris High Court lacked territorial jurisdiction to hear the case.

The Commercial Chamber of the French Court of Cassation rejected this reasoning. In its landmark ruling, the court overturned and quashed the Court of Appeal's decision. It referred the parties back to a different court of appeal for a judgment on the merits, while firmly asserting that French courts do hold jurisdiction over the dispute, regardless of where the website is hosted².

¹ Paris Court of Appeal, 4th Chamber, Section A, June 6, 2007, Google Inc. and Google France v. Axa and others.

² Commercial Chamber of the Court of Cassation. November 23, 2010, appeal no.: 07-19543.

The Court of Cassation refused to rely on the criterion of "mere accessibility" (the simple fact that a website can be opened and viewed from within France) to grant jurisdiction. The court considered this criterion insufficient, noting that it creates a state of "legal uncertainty" by exposing any website owner in the world to lawsuits in France simply because their website is accessible there.

Instead, the court upheld the theory based on the analysis of evidence and presumptions. Under this approach, French courts only hold jurisdiction if there is proof of an activity specifically "directed at" or "targeting" the French public. This targeting is established through concrete indicators, such as the use of the French language, the option to pay in Euros, or the availability of shipping delivery to France.

3.2 Focusing Theory

The theory of targeting or directing activity is a modern legal mechanism developed by scholars and courts within the framework of private international law. This theory aims to regulate the rules of international jurisdiction and the applicable law in the online environment. Specifically, it seeks to protect digital actors from the risk of unexpected prosecution in the courts of any country in the world simply because their websites are technically accessible there.

The essence of this theory lies in replacing the "technical accessibility of the website" criterion with the "actual and intentional targeting" criterion. Accordingly, jurisdiction is only established for the courts of a particular country if the plaintiff proves that the foreign website directly and explicitly targets its audience in that country. The courts infer this targeting through a range of indicators, such as the use of the country's language, the availability of payment in its local currency, or the provision of shipping options to its territory.

The theory of focus originated from the practices of American courts since the Supreme Court decision in the case of *International Shoe Company v. Washington* on December 3, 1945. Here, a judge's jurisdiction is determined based on a set of evidence¹.

3.2.1 Decision of the French Court of Cassation in the case of the newspaper "Le Monde" dated September 9, 2008

Italian writer Antonio Z. wrote an exclusive article for the French newspaper *Le Monde*. Later, Italian journalist Giuliano X. republished the article in its entirety in the Italian newspaper *Il Foglio* (both print and online) without permission, prompting the affected parties to sue him in French courts for copyright infringement.

The French Court of Appeal upheld the conviction of the Italian journalist and ordered him to pay €10,000. The court based its jurisdiction on the French nationality of

¹ Supreme Court, *International Shoe Co v. Washington*, Dec. 3, 1945, 326 U.S. 310.

the newspaper "Le Monde," the distribution of a few print editions of the Italian newspaper in France, and the accessibility of its website from within French territory.

The Court of Cassation overturned this ruling and declared that the French courts lacked jurisdiction. The court affirmed that mere "accessibility" to a foreign website from France was insufficient to establish jurisdiction; rather, it must be proven that the website deliberately targets and focuses on a French audience (through language, advertising, or the nature of the content), which was not the case with the Italian newspaper¹.

The Court of Cassation ruled to overturn the Court of Appeal's decision on the grounds that it did not provide sufficient reasons for its decision and did not respond to the defendant's memoranda.

3.2.2 Decision of the French Court of Cassation regarding the case of the website "www.universal.music.de" dated December 14, 2010.

This case addresses the issue of territorial jurisdiction of French criminal courts in dealing with transnational digital crimes. It focuses on establishing the legal criteria that would allow for the prosecution of foreign websites for piracy of artistic works within France.

The case began when the German website Universal Music DE published musical excerpts by a French artist known as "Z" without his permission. Although the website is hosted in Germany and operated by a German company, French copyright authorities detected the infringement and deemed it a case of plagiarism.

The French artist filed a lawsuit against the director of the German company (Mr. X) in French courts. The defendant argued that the French courts lacked jurisdiction, asserting that the website was German, targeted at a German audience, and that the alleged act did not occur on French soil.

The Court of Appeal rejected the defendant's plea and convicted him, considering that the site targeted the French public based on four pieces of evidence: the violation was observed within France, the artist's French nationality, the song titles remaining in French, and the site's reliance on gray playback icons that do not require knowledge of the German language.

The Court of Cassation overturned the conviction, confirming that the Court of Appeal's evidence was insufficient to prove that the French public was targeted. The court ruled that the mere ability to access a German website from within France was not enough to establish French jurisdiction, meaning that the material element of the crime was absent

¹ The judgment of the Court of Cassation (Criminal Chamber) of September 9, 2008 (appeal no. 07-87.281).

in France¹.

4- Conclusion

Contemporary criminal law faces a genuine dilemma in reconciling the sovereignty of territorial states with the transnational nature of cybercrime. Despite international efforts to harmonize legislation, the risk of overlapping prosecutions and jurisdictional conflicts remains significant. Strict reliance on territoriality alone is no longer sufficient to govern a borderless digital space, necessitating a flexible legal framework that transcends the physical concept of territory to protect the security of digital communities without compromising the rights of the accused.

Overcoming jurisdictional conflicts in cyberspace requires a comprehensive update of traditional legal concepts. This begins with developing the territoriality standard itself to include broader, virtual dimensions that link jurisdiction to the location of the crime or the victim's residence, not just the location where the crime originated. The international community must also establish sophisticated coordination mechanisms to determine the "most appropriate jurisdiction" for adjudicating digital disputes, ensuring a clear division of responsibilities among states and preventing double jeopardy for the same offense.

On the other hand, states must strive to reduce their reservations to international agreements to ensure the harmonious and equitable application of legal rules globally. This must be accompanied by streamlining international judicial cooperation procedures and the cross-border exchange of digital evidence to ensure swift prosecution, while strictly adhering to the principle of double jeopardy to protect the fundamental rights of defendants in the digital environment.

Litigants are advised to digitally document the harm immediately upon its occurrence through official inspection reports that prove the appearance of the offensive content locally, while searching for any evidence that confirms the site targeted the national audience to ensure the acceptance of the lawsuit and avoid arguments of lack of regional jurisdiction.

On the other hand, companies and website developers must strengthen their legal position by including an explicit clause specifying the competent court and applicable law within the terms of use, or by resorting to geo-blocking technologies to prevent content from reaching countries whose laws may raise unwanted legal disputes.

Finally, modern legal thought is moving towards the necessity of the judiciary adopting a flexible standard that integrates the two theories; so that the accessibility theory is sufficient to protect rights inherent to the person, such as slander and defamation,

¹ the Criminal Chamber of the Court of Cassation on December 14, 2010 (appeal no.: 10-80.088), commented on by Professor Emmanuel Dreyer in the Dalloz Collection (2011, p. 1055).

while the strict concentration theory is applied in commercial disputes and consumer protection to ensure the stability of electronic transactions.

Bibliography List :

I. Books

- 1) Delmas-Marty, M. (2004). *The Imaginative Forces of Law*, Vol. 1: The Relative and the Universal. Paris: Le Seuil.
- 2) Rebut, D. (2014). *International Criminal Law* (2nd ed.). Paris: Précis Dalloz.

II. Journal Articles

- 1) Arab, Maryam (2015). "Jurisdiction in Cybercrimes". *Annals of the Faculty of Law and Political Science, University of Oran 2*, Volume 7, Issue 3.
- 2) Ibrahim Sabri Al-Arnaout (2020). "The Extent of Civil Liability of Internet Service Intermediaries, A Comparative Study". *Algerian Journal of Comparative Law*, Abu Bakr Belkaid University of Tlemcen, Volume 3, Issue 5.
- 3) Pollaud-Dulian, F. (2013). "Jurisdiction. Online infringement. Internet-Accessibility". *RTD com*.
- 4) Rafaa Ahmed Belabidi, & Al-Sadiq Abdelkader (2021). "The effectiveness of the optional submission clause as a mechanism for determining international judicial jurisdiction in e-commerce contract disputes". *International Journal of Legal and Political Research*, University of El Oued, Volume 5, Issue 3.
- 5) Vivant, M. (1996). "Cyberworld: law and network rights". *JCP*.

III. Judicial Rulings and Legislative Texts

A. European Legislation

- 1) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000.

B. International and European Case Law

- 1) ECHR, 2nd Section, March 30, 2004, application no. 53984/00, *Radio France and another v. France*.
- 2) CJEU, April 19, 2012, *Wintersteiger*, Case C-523/10, D. 2012, p. 1926, commentary by T. Azzi.

C. French Case Law (Court of Cassation)

- 1) Cass. 1^{ère} civ. (First Civil Chamber), December 9, 2003, Bull. 2003, I, No. 245.
- 2) Cass. crim. (Criminal Chamber), February 4, 2004, Bull. crim. No. 32, D. 2005, p. 621, commentary by V. Malabat.
- 3) Cass. crim. (Criminal Chamber), September 11, 2007, No. 07-82018.

- 4) Cass. crim. (Criminal Chamber), January 15, 2008, Criminal Bulletin, Judgment No. 5.
- 5) Cass. crim. (Criminal Chamber), September 9, 2008, appeal no. 07-87.281.
- 6) Cass. com. (Commercial Chamber), November 23, 2010, appeal no. 07-19543.
- 7) Cass. crim. (Criminal Chamber), December 14, 2010, appeal no. 10-80.088, Dalloz Collection 2011, p. 1055, commentary by E. Dreyer.

D. French Case Law (Courts of Appeal and Lower Courts)

- 1) Paris High Court, summary proceedings, May 22 and November 20, 2000.
- 2) Paris High Court, Interim Order of August 11, 2000, "Union of Jewish Students of France" Association, "League against Racism and Anti-Semitism" v. Yahoo! Inc. and Yahoo France.
- 3) Paris Court of Appeal, June 6, 2007, Google Inc. and Google France v. Axa SA and others, No. 06/14890.
- 4) Paris Court of Appeal, October 29, 2008, MySpace v. Lafesse; see Ph. Stoeffel-Munck, column "Responsibility and contracts", Comm. com. électr., 2009.
- 5) Grenoble Court of Appeal, First Chamber, Judgment of December 10, 2013.