

---

**INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH**

---

**ISP'S LIABILITY FROM A EUROPEAN PERSPECTIVE**- Adv. Triveni Singal<sup>1</sup>**I. ABSTRACT**

In today's world, technology has become our right hand. One of the areas, in which technology has increased and has now become so synced with our lives is the internet, which is simply the worldwide network of computer programs. It has become ubiquitous. But with great power comes great responsibility. The powerful impact of these service providers in the lives of almost all of the human race, especially regarding electronic communications, needs to be governed and balanced through effective responsibility and liability towards societal interest. Holding them accountable and liable is important for the continuation of freedom and utility of the Internet. This article focuses on the concept of liability of internet service providers under European laws, its interrelation with other classes of rights, and the evolution from the E-Commerce Directive to DSA.

**II. INTRODUCTION**

The OECD (Organisation for Economic Co-operation and Development) provides us with a definition of internet intermediaries. Accordingly, they state that an Internet intermediary facilitates or brings together transactions between people or third parties on the Internet. Their contribution includes hosting, providing access, transmission, etc to products and services originating on the Internet<sup>2</sup>, or providing Internet-based services. After a combined reading of

---

<sup>1</sup> WIPO Joint Masters in IP and New Technologies with Jagiellonian University (Poland)

<sup>2</sup> OECD, The Economic and Social Role of Intermediaries (2010) 9; OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives (2011) 20.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

the E-Commerce Directive<sup>3</sup>, and the Information Society Services Directive<sup>4</sup>, we can understand that an Internet Service Provider (ISP) is any natural or legal entity that provides through electronic means of information society service<sup>5</sup> for remuneration for processing and storage of data relying on any platform of electronic communication. From our understanding, we can divide ISPs into various categories -

- 1) Mere conduits (such as Airtel) - The services of these include transmission of information in a communication network, or access to a communication network<sup>6</sup> (for example- Airtel, T-Mobile)
- 2) Hosting - The services of these include storage of information provided by a recipient of the service<sup>7</sup> (such as Facebook, Amazon, Instagram)
- 3) Caching - The services of these include transmission in a communication network of information provided by a recipient of the service<sup>8</sup> (such as Google, Bing)
- 4) Cloud service providers (such as Dropbox)
- 5) Domain name controllers

### III. LIABILITY OF ISPS UNDER THE E-COMMERCE DIRECTIVE

The E-Commerce Directive of 2000 that sought to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States includes the boundaries for the liability of intermediaries. According to this Directive, the liability of the ISP is dependent on the kind of service they provide. Thus, an ISP can be held liable for illegal content concerning some of its services, while regarding other services, the ISP may be exempted from liability. They are a type of horizontal liability exemption or safe harbors for ISPs.

---

<sup>3</sup>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').

<sup>4</sup>Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

<sup>5</sup> any service provided for a remuneration using electronic equipment, from a distance, for the storage and processing of data, at the individual request of service recipient

<sup>6</sup> Article 12 of E-Commerce Directive (Directive 2000/31/EC)

<sup>7</sup>Article 14 of E- Commerce Directive (Directive 2000/31/EC)

<sup>8</sup>Article 13 of E- Commerce Directive (Directive 2000/31/EC)

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

Important provisions in this regard can be summarized below-

- 1) ISPs that are mere conduits shall not be liable for the information they transmit if that provider did not initiate the transmission, did not select the receiver, and did not select or modify the information contained in it<sup>9</sup>.
- 2) Caching ISPs shall not be liable for the automatic, intermediate, and temporary storage of that information, performed for the sole purpose of efficiency of transmission, if that provider did not modify the information, complies with the conditions on access and update of the information, does not interfere with the lawful use of technology, to obtain data on the use of information, and acts expeditiously to remove or block access of any information ordered by a court having competent jurisdiction or any administrative authority<sup>10</sup>.
- 3) Hosting ISPs shall not be liable for stored information requested by the user of service if the provider did not have actual knowledge of the illegal activity, or upon becoming aware of such illegality, the provider expeditiously removed or disabled access to that information<sup>11</sup>.

Lastly, Article 15 of the directive lays down the principle that there shall be no general obligation on these providers to monitor the information or to actively seek facts indicating illegal activity.

The interpretation of this Article in various cases has provided us with a more clear view regarding the balance between human rights, IPR, reputation, and privacy rights of users or the public versus the extent of liability of the ISP.

- 1) Defamation - In the landmark Glawischnig-Piesczek case<sup>12</sup>, the question regarding the obligation of ISP to monitor identically worded and/or equivalent content to that which

---

<sup>9</sup>Article 12 of E- Commerce Directive (Directive 2000/31/EC)

<sup>10</sup>Article 13 of E- Commerce Directive (Directive 2000/31/EC)

<sup>11</sup>Article 14 of E- Commerce Directive (Directive 2000/31/EC)

<sup>12</sup>Eva Glawischnig-Piesczek v Facebook Ireland Limited [2019], CJEU C-18/18

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

has already been declared illegal by a court having competent jurisdiction was answered, and furthermore, the territorial scope of such limitation. The CJEU stated that firstly, the safe harbor provided to hosting ISPs shall not be exercised here by Facebook as it did not satisfy the given conditions. Secondly, Article 15 isn't violated when a court orders the hosting ISP to cover identical content (as the one declared illegal) as this would not be a “general obligation”, but rather a “specific obligation”. This assessment by the CJEU does not give a basic interpretation of Article 15, but rather a “basic interpretation minus injunctions<sup>13</sup>”. Thirdly, Article 15 also does not prevent a court to order an obligation to monitor “equivalent content” (as to one previously declared unlawful) as long as such monitoring is limited to content whose message remains essentially unchanged and there is no need for independent assessment of all content by the hosting ISP. Fourthly, the obligation to monitor in such cases is not limited by territory and can take place globally as long as it is in conformity with international laws. This case showed how the interests of the public can be balanced with the interests of the ISP by adopting the reasonableness rule. That is, in other words, the “reasonable duty to review” before ordering an obligation to monitor to identify content identical in its “core” to the content previously declared unlawful. However, it is unclear as to whether this interpretation would be applicable in the context of IPR because, primarily different users may copy and post the same protected content online for unconnected reasons which may be lawful for some of them to post (due to licenses or other authorizations) but not for others. Similarly, using AI technology to avoid problematic overblocking is severely exacerbated in the area of intellectual property. Lastly, this judgment does not harm the freedom of expression of the users but only affects the ability to post illegal content.

- 2) Balance of rights - Maintaining the balance between the protection of IP rights and other fundamental rights, including the freedom to conduct business, the CJEU in the SABAM case<sup>14</sup> stated that courts can not order any ISP to preventively, indefinitely, and at their own expense install a filtering and blocking system applicable to all electronic

---

<sup>13</sup>The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market (2020), pg 8.

<sup>14</sup>Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), CJEU, C-70/10 (2011).

communication between customers. This type of system also violates individuals' right to privacy, freedom of communication, and information. A contested filtering systems that require monitoring of all the data in order to prevent further IP infringements are incompatible with Article 15.

- 3) Trademarks - In the 2011 eBay case<sup>15</sup>, it was held that a trademark proprietor is entitled to prevent the operator of an online marketplace from advertising its goods without consent which was targeted at consumers in the EU and Article 14 exemption is not applicable when the ISP plays an active role in the sale of infringing goods. In the recent Louboutin joined cases<sup>16</sup>, it was held that Article 9(2)(a) of Regulation (EU) 2017/1001<sup>17</sup> must be interpreted as meaning that the operator of an online sales website itself using a sign which is identical to an EU trade mark of another person for identical goods. If a third party offers for sale on that online marketplace, without consent of the trademark owner, a well-informed user may have an impression that the operator itself is marketing the goods bearing that sign. Thus, advertisements must be presented in such a way that the user can easily distinguish the offers of the market operator from the offers of third-party sellers.
- 4) Personal data- in the landmark Promusicae judgement<sup>18</sup>, the CJEU reaffirmed the necessity of protecting the right to the protection of personal data. It held that the e-commerce Directive and some other Directives, don't bear the Member States to lay down an obligation to communicate personal data in order to ensure adequate protection of the brand in the environment of civil proceedings.
- 5) Freedom of expression - In the SABAM v. Netlog NV<sup>19</sup> case, the ECJ reaffirmed the necessity of guarding the right to freedom of expression and the right to protection of one's personal data when it decided that a specific type of measure couldn't be assessed

---

<sup>15</sup>L'Oréal SA v. eBay International AG (C-324/09)

<sup>16</sup>Christian Louboutin v Amazon Europe Core Sàrl and Other, Joined Cases C-148/21 and C-184/21 (2022)

<sup>17</sup> Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trademark

<sup>18</sup>Promusicae v. Telefónica de España SAU, Case C-275/06 (2008)

<sup>19</sup> Case C-360/10 (2012)

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

upon an internet social network service provider in order to help and cease the violation of the rights of third parties, specifically IP rights.

#### IV. CDSM DIRECTIVE

Article 17 of the Directive on Copyright and related rights in the Digital Single Market<sup>20</sup> lays down provisions regarding the use of protected content by online content-sharing service providers and has amended the existing Infosoc Directive<sup>21</sup> and Legal Protection of Databases Directive<sup>22</sup>. This Article recognizes that when an online content-sharing service provider gives access to copyright-protected (or other related rights-protected) works, it performs the act of “communication to the public or making available to the public” as understood under the copyright laws. Thus, now that the service provider is obligated to obtain proper authorization from the right holder before giving its users access to the work. Further, such a service provider is beyond the scope of applicability of Article 14 of the E-Commerce Directive.

There is no general obligation to monitor the information under this Article also. Liability is exempted if-

1. best efforts were made to obtain authorization and ensure the unavailability of specific works for which the rightsholders have provided the service providers with the relevant and necessary information, and
2. It acted expeditiously to disable access to, or to remove the content after being informed by the right holder.

In a recent case, Poland<sup>23</sup> challenged that this Article violates principles of the right to freedom of expression and information and sought annulment of certain parts of the Article that provide rules for content-sharing platforms. The CJEU dismissed the action stating that firstly, this Article can not be partially annulled since it forms a new liability regime. Secondly, the freedom of expression is not absolute and can be restricted in some cases following the principle of proportionality. Thirdly, the obligation to take measures to ensure copyright is complied with

---

<sup>20</sup> Directive (EU) 2019/790

<sup>21</sup> Directive 2001/29/EC

<sup>22</sup> Directive 96/9/EC

<sup>23</sup> Republic of Poland v European Parliament and Council of the European Union (C-401/19)

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

when services are used is necessary to respect the freedom of those service providers to conduct a business<sup>24</sup>, and to respect the fair balance between that freedom, the right to freedom of expression, and information of the users of their services<sup>25</sup>, and the IP rights of the rightsholders to let those service providers determine the specific measures to be taken to achieve the result sought.

## V. DIGITAL SERVICES ACT (DSA)

The DSA<sup>26</sup> is one of the key pillars that will shape the EU's digital economy. It amends the E-Commerce Directive and provides better protection to consumers online and their fundamental rights. The Act aims to provide harmonization regarding online intermediaries, promote transparency, establish a level playing field to foster innovation, growth, and competitiveness, and provide safer digital spaces by preventing the dissemination of illegal content. It follows the principle of "what is illegal offline should be illegal online". The Regulation employs a broad definition of "illegal content" to effectively ensure the presence of a safe, predictable, and trustworthy online environment. It shall include information concerning illegal content, products, activities, and services, that is, any information in whatever form it may be which is illegal as per the applicable laws (such as hate speech, terrorist content, discriminatory content, copyright infringement, etc.). It has expressly been clarified that an eyewitness video of potential crime will not be included under the umbrella of "illegal content" merely because it shows an illegal act provided that dissemination of such a video to the public is not illegal under the applicable laws.

Similar to the GDPR, this Act will also have an extra-territorial effect. The principle of substantial connection<sup>27</sup> has been provided in the DSA according to which all the online intermediaries that are providing services in the European single market will be required to comply with the DSA rules notwithstanding the location of their headquarters.

---

<sup>24</sup> Article 16 of the EU Charter of Fundamental Rights

<sup>25</sup> Article 11 of the EU Charter of Fundamental Rights

<sup>26</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

<sup>27</sup> Article 3(e) of the DSA (Regulation (EU) 2022/2065)

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>

The Act has also recognized a list of “very large online platforms” and “very large online search engines” that have additional obligations on them having a cumulative effect. In other words, the DSA sets rules proportional to the size, impact, and role of the service provider. It has a broader scope of application.

Chapter two of the Regulation lays down the liability of intermediary service providers which is very similar to the provisions of the E-Commerce Directive, including the prohibition on general monitoring obligation. However, Recital 30 expressly states that the prohibition will not extend in specific cases as decided by the national legislation.

The DSA additionally introduces the “Good Samaritan” principle<sup>28</sup> in the European Union which is already a well-established principle in the United States<sup>29</sup>. According to this principle, an online intermediary shall not be held liable for any voluntary actions taken in good faith against certain objectionable content. Thus, the intermediaries will not automatically lose the conditional exemption from liability on the ground that they had engaged in voluntary investigations or other initiatives for the detention, identification, removal, or disabling access to illegal content.

Lastly, the concept of trusted flaggers<sup>30</sup> has been introduced by the DSA to harmonize the ‘notice and action<sup>31</sup>’ regime, which till now was fragmented under the E-Commerce Directive. These trusted flaggers are essentially certified independent entities that have particular expertise and competence in dealing with illegal content and send notices concerning objectionable activities diligently, accurately, and objectively. Hosting services, including online platforms, are required to set up a notice and action mechanism through which any individual or entity could notify them of the presence of illegal content, including content infringing copyrights, patents, trademarks, or other IP rights.

---

<sup>28</sup> Article 7

<sup>29</sup> 47 U.S.C. § 230

<sup>30</sup> Article 22

<sup>31</sup> Article 16



## VI. CONCLUSION

The concept of ISP liability has come a long way from the 2000 E-Commerce Directive to the upcoming 2024 Digital Services Act. All through these years, the E-Commerce Directive had provided the users and the public a balance between their rights and the ISP rights but with the growth in AI and modernization, the implementation of DSA was definitely needed. Furthermore, with the rapid development of the online environment where new digital technologies and digital services are increasingly being utilized, the requirement for a new set of rules was inevitable. In some cases, the development has been statutory, while in others it has grown due to legal precedents.

Furthermore, the DSA is a general law (*lex generalis*) that provides general rules and regulations for the online intermediaries to follow, while on the other hand, the CDSM is a specific law (*lex specialis*) that focuses only on the dissemination of copyright-infringing content. Thereby, by the principle of '*lex specialis derogat legi generali*<sup>32</sup>', the DSA is not applicable to the cases where the CDSM is applied. It shall be applicable where Article 17 of the CDSM does not apply.

The central role played by the online service providers makes their liability a subject of considerable interest as we have seen above. There is no doubt that this evolution of the liability of online service providers will provide a safer online environment, but with the everyday progress in machine learning and artificial intelligence, will the DSA be enough is a question for the future.

---

<sup>32</sup>More specific rules will prevail over more general rules.

For general queries or to submit your research for publication, kindly email us at [editorial@ijalr.in](mailto:editorial@ijalr.in)

<https://www.ijalr.in/>