Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 18(67) Special Issue – 2025
https://doi.org/10.31926/but.ssl.2025.18.67.3.43

LEGAL MEANS OF PROTECTING HUMAN DIGNITY IN THE DIGITAL ERA

C.-N. IACHIM [1] E. MĂDULĂRESCU [2]

Abstract: *This paper aims to present how to adapt social relations, through law, to the digital age, focusing on how to share legal liability, especially tort liability, between content providers and hosting service providers. Human dignity continues to be protected, both through the application of traditional means of law and through detailed regulations at European level, such as the Digital Services Act.*

Key words: *Digital Services Act, protection of dignity, civil liability of the service provider.*

1. Introduction

One of the fundamental concepts of law is that of dignity. Without going into details on the content of this particularly complex notion already analyzed in the literature (Sava-Mirea, 2019, p.22; Sâmboan, A. U. D. 2012), I shall consider the legally relevant meaning, which requires the defense of the person primarily because of his or her status as a person, as a subject of law (Sava–Mirea, 2019, p. 27).

The dignity of man has the value of an international principle, affirmed as such in a number of documents. Thus, in the Fundamental Declaration of Human Rights of 1948, dignity was mentioned, along with freedom, as a value - the foundation for these rights. References to this notion include the preambles of the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. Although such a right is not enshrined in the text of the European Convention on Human Rights, so that its existence in its own right cannot be retained, the notion of 'human dignity' plays a key role in the interpretation and application of the protection afforded by the other rights of the Convention. On the other hand, at European level, Article 1 of the Charter of Fundamental Rights of the European Union expressly states that 'Human dignity shall be inviolable. It must be respected and protected". The constitutions of several Member States expressly refer to the right to dignity, either merely as a supreme value or in relation to other rights, such as the rights of personality.

[1] *Transilvania* University of Braşov, cristina.iachim@unitbv.ro, corresponding author
[2] *Dimitrie Cantemir Christian* University, Bucharest.

Obviously, however, at the constitutional level we find principles, foundations that determine the subsequent activity through which they are integrated and articulated in the specific legislative systems. However, we are currently going through a period globally that is often referred to as the 'digital age' or the information age, characterised by the ability to access and transmit information without the classical limitations of time and space. Since the primary function of law is to regulate social relations, it is natural that the constant concern is to analyze how it evolves in concrete terms and, more precisely, what are the legal instruments through which the principle of human dignity, enshrined at constitutional and international level, takes on a form directly applicable to legal relationships.

Thus, we would point out that the term 'digital rights' is already used in the literature, which are usually seen extensively in several aspects, such as an extension, an extension of human rights to the use of new technologies, a framework for evaluating initiatives and policies on new technologies, or as a basis for preventing cases of 'injustice' caused by the use of new information technologies (Robert, 2025), whether it includes new rights, such as the right to be forgotten, the right to a secure digital environment (Custers, B.H.M. 2022).

There is, however, agreement that already recognised rights can serve as the current basis for ensuring a level of protection applicable also to the digital sphere in which we live.

What are the means by which such protection can be achieved and what are the challenges posed by the new extended limits of communication? Who is responsible for any damage caused?

As far as the Internet is concerned, the classic variant is that of incurring civil liability in tort for the damages caused, by awarding damages and/or by removing defamatory posts or by other means, such as the publication of the court decision. Thus, this is not an action for a declaration (of an unlawful act), but an action for enforcement, an action for civil liability in tort seeking to remove non-material damage by ordering the defendant to cease the infringement of rights and/or compensation for non-material damage caused by the defendant by infringements of the applicant's rights (pecuniary liability).

2. Determination of Jurisdiction

A first challenge is to determine whether we can speak of the existence of a jurisdiction, consisting of the jurisdiction of a court to hear a case and give a decision.

Generally, disputes relating to the Internet involve an international element, which raises the question of whether or not there is territorial jurisdiction, which will have to be decided by the domestic courts in the light of one of the principles of private international law applicable to jurisdiction. However, the ECtHR holds that it cannot be ruled out that situations in which the act complained of is outside national territory may fall within the 'extraterritorial jurisdiction' of the State in the light of the Convention.

The decisive factor is the exercise of effective power and control by the Member State outside its national territory. Thus, in Perrin v. the United Kingdom (ECHR, 2005), the applicant, a French national residing in the United Kingdom, was convicted of having published an obscene article on a website. This site was operated and controlled by a

company based in the United States of America, which complied with all local laws and in which the interested party was the majority shareholder. The ECtHR accepted the reasoning of the UK court that limiting the jurisdiction of the UK courts in the matter to cases where the place of publication was within their area incited publishers to publish in countries where they would have little chance of being prosecuted. The Court also ruled that, as a British resident, the interested party could not argue that the laws of the United Kingdom were not reasonably accessible to him. In addition, he pursued a professional activity with his website and could therefore reasonably consider that it was for him to exercise great caution in that context and to obtain the necessary legal advice. Although the dissemination of the images in question might not have been unlawful in other States, including States not party to the Convention, such as the United States of America, that did not mean that by prohibiting such dissemination in its territory and prosecuting and convicting the interested party, the respondent State exceeded its discretion. Thus, the Court declared the application manifestly unfounded within the meaning of Article 35 § 3 of the Convention.

Furthermore, the ECtHR has stated that, where a case falls within the jurisdiction of the courts of the State concerned by the request, the Court cannot take the place of the domestic courts of that State. The Court did not grant the request of an applicant who claimed before it that the courts should have applied to the facts of the case other texts, in particular the provisions of European Union law relating to Internet service providers. The position of the European Court of Human Rights is clear: it is not for it to rule 'on the appropriateness of the techniques chosen by the legislature of the defendant State to regulate a particular field; its role is limited to verifying that the methods adopted and their effects comply with the Convention' (Delfi AS v. Estonia (MC), Application No. 64569/09, para. 127, 16 June 2015).

As regards territorial jurisdiction at national level, between national courts, in matters relating to civil liability in tort, the legislature may establish an alternative territorial jurisdiction, as is the case under Romanian law, under which the applicant may bring the action either at the defendant's domicile/registered office, pursuant to Article 107(1) of the Code of Civil Procedure, or at the court in whose jurisdiction the tort/delict was committed or the damage occurred, in accordance with Article 113(1)(9) of the Code of Civil Procedure. In the case of alternative territorial jurisdiction, under Romanian law, the applicant has the choice between several courts equally competent (Article 116 C. civ.proc).

Given that dissemination via the Internet presupposes that the information can be accessed by any person with access to it, we consider that the criterion relating to the 'place where the act was committed' remains of no legal relevance. As regards, however, the criterion relating to the 'place where the damage occurred', it has been stated in domestic case-law that it has jurisdiction to hear the case of the court in whose jurisdiction the damage to the protected social value occurred, that is to say, the direct damage, which, in the particular circumstances of the case, in which damage is claimed to have been caused by the dissemination in a virtual environment of defamatory images of the applicant, is represented by the court of the applicant's domicile (I.C.C.J., First Civil Division, Decision No 1541 of 24 June 2021).

3. Civil (delictual) Liability of the Author of the Post/repost

In the case of civil liability in tort, the 'classical' offence consists in making a defamatory post or defamatory statements on the Internet or on a social network. In this situation we find, for example, posts made on a blog, on an Internet site, on Facebook, Instagram, Tik-tok, etc.

As a rule, the responsibility belongs to the author of the post, and in this category, we include all posts, both those made on a site (or blog) owned by him, as well as posts made through hosting service providers. In this situation, the wrongful act consists in posting content that infringes the legitimate rights of a person, with the possibility of accessing it through online means.

Therefore, for example, if we find denigrating images/videos faked with the help of another person, and the latter did not know the illicit purpose for which the result of the computer intervention was to be used, the responsibility lies with the person who disseminated the fake images/videos in the public space.

By contrast, the taking of messages, regardless of their content, from the social page of another "unidentified" person is not such as to exonerate the person who merely retransmits, in this manner, the messages because they are "about the opinion of the original author of the post".

In reality, the person who takes the messages and perpetuates them, multiplies them, by relaying them in the online space, is responsible for their content and for any negative, denigrating consequences that could be passed on to other people, on an equal basis with the original author of the post.

This is because, by assumption, the person who takes over the messages of another post acts with discernment, adhering to their content, which he considers, for various reasons, to be relevant, capable of being passed on and of reaching as many recipients as possible.

Therefore, a person who merely retransmits messages on social networks, considered to be a public space, cannot invoke an exemption from liability for his actions, if they would infringe the rights of someone else, since the liability is personal and he also commits himself to the original author of the post and to those who, appreciating and endorsing the content of those messages, retransmit them in such a way as to reach as many recipients as possible (see ICCJ Decision No 2509/6 December 2023 Civil Section I).

4. Obligations and Liability of the Hosting Service Provider

If we find content generated by users of a hosting service (including a platform), beyond the incurring of tortious liability of the author of the post, can we also find the incurring of liability of the hosting service?

As a general rule, the hosting service provider shall not be liable for user-generated content unless it becomes aware of the illegality and does not act expeditiously to withdraw or disable access to it as soon as it becomes aware of the illegality of the posting.

In regulatory terms, that rule was laid down in Article 14(1) of 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, which provided, in essence, that the provider of the storage service was not responsible for the information stored at the request of a recipient of the service, provided that: a) the supplier is not aware of the illegal activity or information and, as regards actions for damages, is not aware of facts or circumstances from which it appears that the illegal activity or information is manifestly illegal or b) the supplier, from the moment it becomes aware of them, acts promptly to remove the information or to block access to it.

Similarly, the prerequisite for prior notice and conduct of the hosting service provider is clear from the CJEU judgment C-18/18. In that case, the applicant was a former Member of Parliament, chairman of the Greens Parliamentary Group and spokesperson for that party. A Facebook user shared on his personal page an article from an Austrian online information magazine entitled 'Greens in favour of maintaining a minimum income for refugees', which had the effect of generating on that page a 'miniature image' of the website of origin, including the title of the article, a short summary of the article and the photograph of the applicant. That user also published, in connection with the article, a denigrating comment against the applicant. The post was public.

The applicant requested Facebook Ireland to delete that article, which it did not do. Subsequently, the applicant brought proceedings against Facebook Ireland before the Austrian courts and the court of first instance, by an interim order, ordered Facebook Ireland to cease, immediately and pending the final outcome of the injunction proceedings, the publication and/or dissemination of photographs of the applicant in the main proceedings, if the accompanying message contains the same statements or information with a content equivalent to the impugned comment. Facebook Ireland (which manages the Facebook platform for users outside the US and Canada) has blocked access to the information originally published in Austria. The appellate court upheld the decision of the court of first instance, but held that the dissemination of information of an equivalent nature was to cease only in respect of information brought to Facebook Ireland by the applicant, third parties or otherwise. On appeal, the court asked the CJEU about the interpretation of Article 15(1) of Directive 2000/31.

In response, the CJEU stated that Directive 2000/31/EC allows a court of a Member State to order a hosting service provider to remove information which it stores and the content of which is identical to that of information previously declared unlawful or to disable access to it, irrespective of the author of the request to store that information. Similarly, that directive allows a court of a Member State to order a storage provider to remove information which it stores and the content of which is identical to that of information previously declared unlawful or to disable access to it, in so far as the monitoring and search for the information generated by such an injunction is limited to information conveying a message the content of which remains essentially unchanged from that which led to the finding of unlawfulness and which contains the elements specified in the injunction, provided that the differences between the initial and subsequent message are not such as to compel the provider to carry out an independent assessment of the content. Nor does the Directive preclude a national court from

requiring the supplier to remove the information to which the injunction relates or to disable access to it worldwide under the relevant international law.

Also, in the light also of that decision, I consider that it is possible that storage service provider be required to remove the information it stores whose content has been declared unlawful, or to disable access to it, not only within the national territory but also on a large scale. At the same time, it may be obliged to remove/block access to similar information if it is reported by the injured party, by third parties, or by its own means, without, however, entailing a general obligation of supervision on the part of the provider.

From a procedural point of view, the action based on civil liability in tort may be brought simultaneously against the content creator (*lato sensu*) and against the hosting service provider, for the removal of illegal content or the disabling of access to it, as a remedy for the non-material damage caused. In this regard, we would also refer to Civil Section I of the HCCJ Decision No 679/19.03.2025, noting that, by court order, the 'principal' defendant was ordered to pay compensation for non-material damage both by paying non-material damages and by ordering him to remove the material containing the allegations found to be unlawful, published on the channel held on the network, as well as any references and references thereto, and that the 'secondary' defendant, as the holder of an audiovisual licence and owner of a news portal, was ordered to remove denigrating material from the public space.

The liability of the supplier may be incurred, including in the form of monetary compensation, if the measures taken by the latter following notification prove insufficient to protect the rights of the injured party. In support of that assertion, I refer to Delfi vs. Estonia, handed down by the ECHR, in which the European Court of Human Rights held that Delfi being ordered to pay compensation of approx. EUR 320 to the injured party complied with the requirements of compatibility with Article 10 of the ECHR.

Delfi was one of the largest news portals in Estonia, also operating in Latvia and Lithuania. One of the published articles received 185 comments, about 20 of which contained threats and insults to the injured party. By notification, the injured party requested the applicant company to remove the defamatory comments and to pay the amount of approx. 32,000 euros by way of compensation for non-material damage. Delfi deleted the insulting comments on the same day, six weeks after they were written. The injured party sued Delfi for compensation for non-material damage and, at first instance, the claim was dismissed, the court considering that there was a need to differentiate between the commentary field in the applicant company's news portal and the journalistic field of the portal; the applicant company's management of the first domain was mainly mechanical and passive; the applicant company could not be regarded as the publisher of the comments, nor was it under an obligation to monitor them.

On appeal, the judgment was set aside with a retrial, taking the view that Delfi could be held liable. In the retrial, the court of first instance upheld the injured party's claim, but awarded compensation in the amount of approximately EUR 320.

The High Court ruled on the appeal and classified Delfi in the light of the provisions of national law transposing Directive 2000/31/EC and the content of the Directive. It considered that Delfi's activities at the time the comments were posted were not of a purely technical, automatic and passive nature. Delfi's objective is not simply to provide

an intermediary service. It integrated the comments section into the news portal, inviting website visitors to add their own [hinnangud] judgments and opinions (comments) to the news. In this section, Delfi actively invites readers to comment on the news that appears on the portal.

The number of hits it records depends on the number of comments; the revenue from the advertisements displayed on the portal also depends on the number of hits. Thus, the publication of comments is of economic interest to Delfi. The fact that they do not write them themselves does not mean that they have no control over the comments section. They set the rules for this section and make changes to it (deleting certain comments) if the rules are broken. Users, on the contrary, cannot modify or delete the comments they have written. They can only report inappropriate comments. Thus, Delfi can select which comments will be published and those that will not be published. In other words, Delfi, which manages the data stored in the comments section, **provides a content service,** which is why the circumstances removing liability referred to in Articles 12 to 15 of the Directive (transposed into national law) are not applicable in the present case.

The European Court of Human Rights has held in situations such as that examined in the present case, where comments by third parties appear to be hate speech and direct threats to the physical integrity of an individual, **that, in order to protect the rights and interests of individuals and of society** as a whole, contracting States may be entitled to hold internet news portals liable, without this constituting a breach of Article 10 of the Convention, if the portals fail to take measures to remove manifestly illegal comments immediately after their publication, **even in the absence of a referral from the alleged victim or third parties.**

The above distinction is particularly relevant. It should also be noted, however, that in the above case, the comments had as mandatory fields the text of the comment and the name of the author (chosen by him), filling in the email address being optional. In those circumstances, identifying the authors of the denigrating comments was an almost impossible task for the injured party. We believe that in the opposite situation, where a field containing identification data of those who post comments is mandatory, we can also retain the possibility of an individual civil response.

It should be pointed out that the above-mentioned Directive 2000/31/EC was amended by the Digital Services Act 2022/2065 (DSA), which is directly applicable. It repealed the provisions of the Directive on the limited liability of the service provider, replacing them with much more detailed provisions that also take into account the scale of the provider.

The Regulation also defines ‘illegal content’ in Article 3(h) as ‘any information which, in itself or in relation to an act, including the sale of products or the provision of services, does not comply with Union law or with the law of any Member State which complies with Union law, irrespective of the precise subject matter or nature of that law’.

Although the court is in principle competent to declare content illegal, institutions such as ANCOM, CNCD or ANSPDCP are responsible for determining whether content is illegal, but only for a specific regulated area (e.g. ANCOM for video audio content, CNCD for discriminatory content, ANSPSPC for unlawfully processed personal data).

The Regulation qualifies online platforms as a sub-category of hosting service providers, and defines them, by not only storing the information provided by the recipients of the service at their request, but also disseminating that information to the public at the request of the recipients of the service.

Interpersonal communications services as defined in Directive (EU) 2018/1972 of the European Parliament and of the Council, such as emails or private messaging services, fall outside the scope of the definition of online platforms, as they are used for interpersonal communication between a finite number of persons determined by the sender of the communication.

However, the obligations laid down in the Regulation for providers of online platforms may apply to services that allow information to be made available to a potentially unlimited number of recipients, not determined by the sender of the communication, for example through public groups or open channels. Information should be considered to be disseminated to the public for the purposes of this Regulation only where such dissemination takes place at the direct request of the recipient of the service that provided the information.

Thus, the Regulation sets out several avenues for the notification of illegal content. The first way is to notify the hosting service provider of the existence of information considered to be illegal content, and the hosting service provider is required to put in place mechanisms to take up such referrals. Those mechanisms shall be easy to access and use, allow, but not require, the identification of the natural person or entity submitting a notification, and allow for the submission of notifications exclusively by electronic means.

In the case of online platforms, it is also possible for trusted flaggers to inform them. A trusted flagger can be any entity (public or private) that demonstrates that it has specific expertise and competence in detecting, identifying and notifying illegal content is independent from any online platform providers and carries out its activities in such a way as to submit notices with diligence, accuracy and objectivity.

This status is granted by the Digital Services Coordinator of each Member State (in Romania, by ANCOM). Currently, the National Institute for the Study of the Holocaust in Romania 'Elie Wiesel', 'Save the Children' Organisation and the Foundation for Social Services are authorised as trusted notifiers in Romania.

Therefore, in the light of the foregoing, the question arises as to whether the prior notification of the host provider can be regarded as similar to a procedure prior to the application of the court, even if it is not enshrined in law at the level of the Member State of the European Union. In my view, the answer must be in the affirmative. At the same time, compared to the provisions of the Regulation, the prior notification can also be made by a trusted notifier (although, practically, they are less likely to have the physical capacity to report violations of the dignity of a private person). On the other hand, if the injured party has previously applied to another authority, such as the CNA, and the latter declares that content to infringe the applicant's rights and notifies the service provider, I consider that the respective requirement is satisfied.

In conclusion, the protection of the rights of individuals has clearly been extended, with alternative ways of referring the matter to the service provider to be regulated. It

follows from the text of Article 3(h) in conjunction with Article 52 of the Preamble to the Regulation that the protection and mechanisms established by the Regulation also extend to human dignity rights, including the right to image. The person thus becomes better protected, both as an individual and as a member of a particular race, nationality, etc.

5. Responsibility for comments posted in the online environment

If we are talking about the provision of hosting services or online platforms, the above considerations regarding the possibility of obliging them to delete/block access to those elements, which fall under the notion of 'illegal content', are applicable. We do not believe, however, that the hosting service provider or the online platform for comments posted by users can be held liable for pecuniary damages, which fall under the category of 'hosted content'.

Separately, however, the author of the post may be held liable in tort (including in the form of damages) if identified, including for comments made by third parties in response to the author's posts or comments. In this regard, we refer to the ECHR decision Pătrașcu v. Romania, in which, although a violation of Article 10 of the CEDH on freedom of expression was found, it was determined by the fact that the national authorities did not carry out a real balancing exercise to demonstrate that the civil judgment handed down against the applicant for the statements posted on his Facebook page (including by third parties) corresponded to an imperative social need and was proportionate to the legitimate aim pursued. It should be noted that an element held to be important by the ECHR in its reasoning in the judgment in Pătrașcu v. Romania was the behaviour of the injured parties, who did not inform the complainant in advance of their dissatisfaction before taking legal action. The facts of Pătrașcu v. Romania differ substantially from those of another ECtHR case, the judgment of 16 June 2015 in Delfi AS v. Estonia, in which the ECtHR found that Article 10 ECHR had been complied with, but there was prior notification of the person responsible.

Therefore, we can conclude that even if individual liability is requested, **it is necessary to notify in advance** the person who has the control over the content of the page. This becomes a substantive condition in the analysis of maintaining the balance between the competing rights provided for in Articles 8 and 10 of the ECHR.

6. Conclusions

The protection of dignity in the online environment is achieved by extending the already established reasoning and rules on finding a fair balance between the right to privacy and the right to free expression. In the European area, by adopting the DSA Regulation, we can speak of an extension of the protection granted to the rights of individuals by establishing clearer mechanisms for the removal of illegal content as soon as possible and establishing additional obligations on service providers, also taking into account their scale.

Apparently, there is a higher protection offered by means of the provisions of the CEDH as compared to the detailed provisions of EU "law", as the main issue is whether the measures taken to remove manifestly illegal comments, immediately after their

publication, are effective and are able to provide a real protection for the rights and interests of individuals and of society as a whole. Yet, we can notice a tendency to a congruent approach, through the adoption of the DSA Regulation.

References

Custers, B. (2021). New digital rights: Imagining additional fundamental rights for the digital era, *Computer Law & Security Review*, 44, 105636, https://doi.org/10.1016/j.clsr.2021.105636.

CJEU judgment C-18/18, 2019. Glawischnig-Piesczek. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0018

Decision of I.C.C.J., Civil Section I, No 1541 of 24 June 2021. Retrieved from https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=185606#highlight=##

Decision of I.C.C.J., Civil Section I, No 2509 of 6 December 2023. Retrieved from https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=212387#highlight=##%20interes

Decision of I.C.C.J., Civil Section I, No 679 of 19 March 2025. Retrieved from https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=229753#highlight=##

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,* ~~pp. 1–16~~*,* Retrieved from https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

ECHR, Case of PERRIN v. UNITED KINGDOM, Application no. 5446/03. Retrieved from Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-70899%22]}

ECHR, Case of DELFI AS v. ESTONIA, Application no. 64569/09. Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-176293%22]}

ECHR, Case of ALEXANDRU PĂTRAŞCU v. ROMANIA (Application no. 1847/21). Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-238635%22]}

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). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Robert, T. (2025). *Understanding Digital Rights: definitions, Conceptions, an Myths*. Brighton: Institute of Development Studies. DOI:10. 19088/IDS.2025.014, retrieved from https://www.ids.ac.uk.

Sâmboan, C. (2012). Cum a intrat demnitatea în drept şi ce a adus demnitatea dreptului [How dignity was introduced into the law and what dignity contributed to the law], *Juridical Tribune*, 2(1), 155–161. Retrieved from https://tribunajuridica.eu/arhiva/An2v1/nr1/art5.pdf

Sava Mirea, A. L. (*2019*). *Dreptul la demnitate* [The right to dignity]. Craiova: Aius.