

SEGMENTED LIABILITY IN ONLINE LEGAL ADVICE: A RECONCEPTUALIZATION OF RESPONSIBILITY TOWARD THE DIGITAL CONSUMER

DOI: 10.26341/issn.2241-4010-2026-1c-7

Ana Maria Cristişor

Moldova State University, Moldova

ann.cristisor@gmail.com

Olesea Plotnic

Moldova State University, Moldova

olesea.plotnic@usm.md

Dorina Cimil

University of Bucharest, Romania

cimil.dorina20@gmail.com

Abstract

The accelerated digitalization of legal services has profoundly reshaped the way legal information is produced, accessed, and perceived by users. Online platforms have become, for an increasing number of individuals, the primary point of access to legal consultancy. Within this emerging ecosystem, users, often positioned as digital consumers lacking critical evaluative resources, are exposed to new forms of legal risk generated by asymmetries of expertise and by the opacity of algorithmic mechanisms that influence content visibility and perceived credibility.

In this context, classical models of civil liability centered on the author–user relationship prove inadequate to explain the emergence of harm in digital environments. This paper advances a segmented liability model grounded in the interaction between the author of legal content, the digital platform, and the algorithmic architecture, each contributing in a distinct manner to the formation of legal risk.

The study adopts a comparative perspective, examining the regulatory frameworks of Romania and the Republic of Moldova. It highlights the transformative role of the Digital Services Act and demonstrates that legal harm may arise not only from human error, but also from algorithmic mechanisms of automated validation and dissemination of information.

The segmented liability model offers an analytical framework capable of integrating civil law principles with European digital governance and of supporting a preventive approach to technological risks. The conclusions emphasize the model’s potential to inform future doctrinal and legislative developments concerning legal responsibility in digital environments, particularly within the Eastern European legal space.

Key words: online legal advice; segmented liability; digital consumer; digital platforms; algorithms; Digital Services Act (DSA); legitimate trust.

Introduction

The accelerated digitalization of legal services has reshaped how legal information is produced, organized, and accessed, with digital platforms becoming, for a growing audience,

the primary point of contact with law. Within this informational ecosystem (Floridi, 2014), the digital consumer faces trust-based risks: difficulty verifying response accuracy and the opacity of technical distribution criteria, which can create an appearance of authority and turn informational errors into legal harm (Pasquale, 2015; Helberger et al., 2022).

These risks are illustrated by recent judicial incidents, such as *Mata v. Avianca* (2023) in the United States, where unacknowledged use of generative algorithms led to fabricated legal authorities being presented as evidence—showing that digital error can translate directly into material and professional harm—and *Moffatt v. Air Canada* (2024), which underscores a platform’s liability for information mediated algorithmically.

The European Union has responded through the Digital Services Act (Regulation (EU) 2022/2065), shifting the discussion from technological neutrality to duties of diligence and transparency regarding content-distribution architecture. In this framework, the Romania–Republic of Moldova comparison is particularly relevant: Romania operates under the DSA (directly applicable), while the Republic of Moldova remains largely *ex post*, yet offers civil-law reference points (especially Article 2018 of the Civil Code) capable—through evolutionary interpretation—of supporting digital-consumer protection.

Practically, a key tension lies in the gap between widespread exposure to such technologies and the scarcity of visible litigation, suggesting difficulties in identifying the pertinent actor and characterizing technological causal chains. Consistent with ECO4ALL’s objectives, the analysis proceeds from the premise that fairness in digital markets depends on an accountability framework capable of preventing the externalization of informational-error costs onto the vulnerable consumer.

Against this background, the paper asks whether classical civil-liability models centered on the author–user relationship can adequately explain harm in online legal advice, or whether a reconceptualization is required for multi-actor digital environments. The working hypothesis is that a focus exclusively on the author’s conduct is insufficient, as platforms and algorithmic mechanisms play a decisive role in shaping user trust and generating legal risk.

The study’s original contribution is a model of segmented liability, grounded in the interaction between the author of legal content, the digital platform, and algorithmic architecture, as an analytical tool integrating civil law with European platform regulation. Through a comparative analysis of Romanian and Moldovan normative frameworks, the paper highlights the model’s potential to provide a coherent approach for protecting the digital consumer and managing legal risks online.

Methodology and theoretical framework

The paper adopts a predominantly normative and doctrinal approach, aiming to formulate an analytical model of legal liability applicable to online legal advice, at the intersection of civil law, consumer protection, and the governance of digital platforms.

Methodologically, the analysis relies on a systematic interpretation of the relevant European Union legal framework—with particular focus on the Digital Services Act (Regulation (EU) 2022/2065)—and on integrating specialized literature on platform governance, informational risk, and digital-consumer vulnerability. The theoretical framework proceeds from the premise that legal harm in the digital environment may result not only from the content provided, but also from how it is organized, amplified, and validated through platformized architectures and algorithmic mechanisms (Floridi, 2014; Busch & De Franceschi, 2021; De Bruyne, Dheu & Ducuing, 2023). The assessment of liability is

structured around the interaction among actors who contribute to the production and circulation of legal information online.

A comparative method is used to highlight structural and functional differences between Romania and the Republic of Moldova. Romania, as an EU Member State, operates within an integrated framework shaped by digital governance (including ex ante platform obligations), whereas the Republic of Moldova—though within the same civil-law tradition—remains in a process of normative convergence, without a fully functional DSA equivalent. The comparison identifies regulatory asymmetries relevant to Eastern Europe and provides a “mirror-effect” analysis: Romania illustrates the integration of the European digital-governance layer, while the Republic of Moldova tests the capacity (and limits) of civil law’s organic adaptation in the absence of an equivalent digital normative apparatus.

As regards scope, the inquiry does not compare administrative enforcement effectiveness, institutional capacity, or domestic judicial practice in volume and trends (quantitative data). Rather, it offers a doctrinal-normative comparison of mechanisms for attributing liability and protecting the digital consumer. The “constant” element is the civil-law matrix, centered on civil liability and legitimate trust; the “EU-specific” element is the DSA’s ex ante layer of obligations, which is not fully transferable outside the Union and is therefore treated, for the Republic of Moldova, as a guiding reference rather than a directly applicable standard.

The study remains predominantly normative and does not pursue empirical validation or quantitative analysis of litigation involving AI or online legal advice. Complementarily, it selectively refers to a limited number of recent jurisprudential reference points and factual incidents, used solely for illustrative purposes: to exemplify risk typologies associated with the three tiers (author–platform–algorithm) and to make the model’s application intelligible in concrete situations. These examples are not invoked as empirical validation and do not support generalizations; they serve to conceptually anchor the normative argument on allocating responsibility within a technological causal chain.

The analysis is limited to civil liability and the consumer-protection dimension regarding legal information provided or mediated digitally. It does not aim to exhaustively address all potentially relevant legal regimes (e.g., criminal law, professional/disciplinary liability, public-law enforcement mechanisms/regulatory sanctions), but rather to construct an analytical framework for the civil-law characterization of risks.

The Transformation of Legal Advice in the Online Environment and the New Status of the Digital Consumer

The digitalization of legal services has not only changed the channels through which legal information reaches the public, but also the nature of that information and the way it is perceived. Within the environment of digital platforms, online legal advice no longer appears exclusively as a clearly delimited professional service, but rather as a heterogeneous set of answers, opinions, and recommendations, delivered across diverse technical and communicative contexts. This transformation places online legal advice at the intersection of public information, legal counselling, and digital architecture, raising new issues regarding legal qualification and the attribution of liability.

Before examining the legal regime applicable to platforms, it is necessary to clarify the nature of online legal advice as an informational practice: what type of content it is, what expectations it generates, and through which technical mechanisms it comes to be perceived as influential.

This section successively highlights the hybrid character of such advice, the role of algorithms in amplifying risk, the function of platforms as active informational actors, and the position of the digital consumer as a vulnerable subject within this ecosystem.

Online Legal Advice: Conceptual Definition and Methodological Framework

In a broad sense, online legal advice denotes the set of legal information, opinions, and recommendations provided through digital platforms. It is distinct both from general legal information and from traditional professional legal advice; instead, it occupies an intermediate zone, marked by a variable degree of personalization and a significant impact on users' decisions.

This intermediate positioning gives online legal advice a hybrid character that is relevant for liability analysis. A user may rely on a legal response without a contractual relationship or professional guarantees as to accuracy, thereby increasing the likelihood of harm.

Accordingly, a piece of content's legal relevance depends not only on what it conveys, but also on the function it performs in the digital context, its degree of adaptation to the user's situation, and the likelihood that the user will treat it as a basis for a legal decision. As responses are perceived as signaling authority or expertise, the associated legal risk increases proportionally.

To capture these differences in impact, the analysis proposes an operational typology of the main forms of online legal advice, summarized in Table 1. The typology maps a progression from general information—with low legal impact—to tailored or automated counselling, where both the risk of harm and the complexity of liability increase significantly.

The typological criteria draw on the literature on platform governance, informational risk, and trust dynamics in digital environments, adapted to the specificities of legal content—where the consumer occupies a structurally vulnerable position in cognitive terms.

Table 1. Typology of Online Legal Advice

Type of Legal Content	Core Feature	Degree of Personalization	Risk Level for User	Liability Potential
General Information (articles, FAQs)	Explains general legal concepts	Low	Low	Minimal
Informal Opinion or Guidance	Generic, non-tailored responses	Low–Medium	Variable	Moderate
Contextualized Recommendation	Partially adapted to a specific situation	Medium	Significant	High
Individualized legal advice	Case-specific analysis	High	High	High
AI-generated content	Automated responses without human oversight	Variable	High (unpredictable)	Complex, Shared

The typology highlights the increasing degree of personalization and, correlatively, the intensification of risk for the user and the growing complexity of potential liability.

Algorithms and the Visibility of Legal Information: Digital Distribution and Legal Impact

The hybrid character of online legal advice is decisively amplified by the way platforms structure and distribute information. Legal content does not reach the user at random; rather, it is filtered through algorithmic mechanisms that take into account browsing history, the

aggregated behavior of other users, personal data, and technical parameters specific to each platform.

In this context, algorithms function as invisible intermediaries (Pasquale, 2015): although they do not, as a rule, “create” legal content, they determine its visibility and its appearance of relevance - establishing which answer appears first, which opinions are reinforced through repetition, and which content is signaled as “trustworthy.” As a result, incomplete or erroneous information may acquire an aura of authority, while accurate information may remain marginal.

The main legal consequence is that algorithms do not merely mediate content; they contribute to shaping user trust and, implicitly, to the configuration and redistribution of legal risk in the digital environment (Floridi, 2014; Busch & De Franceschi, 2021).

Digital Platforms as Informational Actors

In the context of online legal advice, the platform does not operate as a neutral infrastructure (Balkin, 2021), but as an informational actor that configures visibility, ranking, and the reception context of the message. The legal relevance follows from the fact that these design choices can generate reasonable expectations of authority and can transform questionable information into effective harm. Consequently, the platform must be treated distinctly in the liability analysis, alongside the author and the recommendation mechanisms (developed in Section 2).

The Asymmetry of Legal Protection for the Digital Consumer: Romania vs. Republic of Moldova

The transformations of online legal advice must be examined in light of the normative differences between Romania and the Republic of Moldova.

Romania applies the Digital Services Act (DSA) directly, operating within a European framework focused on prevention, transparency, and the mitigation of systemic risks generated by platforms. This model promotes a proactive vision of digital responsibility and of the protection of the vulnerable user.

The Republic of Moldova, although outside the DSA regime, has at its disposal a modern normative instrument - Article 2018 of the Civil Code - which governs liability for harm caused through legitimate reliance on erroneous information. This solution provides a solid conceptual basis for addressing digital risks, centered on informational asymmetry and on protecting the user who is situated in a position of cognitive inferiority.

Moldovan legal scholarship, notably through the works of Olesia Plotnic and Dorin Cimil, offers important reference points for understanding the imbalance between provider and recipient, unfair terms, and the formation of trust in the context of online information. Although formulated within a pre-algorithmic framework, these contributions support the conceptualization of informational liability within the logic of protecting the digital consumer.

Towards a Model of Segmented Liability in the Digital Environment

In light of the elements outlined above, the traditional author–recipient scheme becomes insufficient to explain the mechanisms through which harm is produced in the digital environment.

A conceptual framework is needed that distinguishes the roles and contributions of the actors involved. To this end, the paper proposes the model of segmented liability, in line with the literature on algorithmic regulation and normative personalization in digital ecosystems (Busch & De Franceschi, 2021).

The next section presents the framework established by the Digital Services Act and the way it reconfigures legal responsibility in the digital environment, assigning platforms an active role in managing the risks associated with the distribution of legal content.

The Digital Consumer: A Vulnerable Subject of Online Legal Advice

The vulnerability of the digital consumer stems from structural features of the digital informational ecosystem—information asymmetry, algorithmic opacity, and the ambiguous legal status of online-distributed content—which expose users to misinterpretation or unjustified reliance on answers that carry a professional appearance (Helberger et al., 2022).

Online legal advice is no longer addressed to an abstract user but to a digital consumer: a person interacting with legal information delivered in opaque technical environments, without clear benchmarks for professional validation and, often, without the capacity for critical evaluation. Under these conditions, harm may arise not only from erroneous content, but also from the mechanisms through which information is framed as credible and relevant.

This position of cognitive inferiority echoes the classical consumer who acts on trust rather than expertise. Yet, unlike traditional goods or services, the digital consumer confronts a trust-based (*credence*) service whose correctness cannot be autonomously verified before or after use. Accordingly, trust is not professionally built, but can be technologically induced through visibility, positioning, and algorithmic repetition (Sax, Helberger, & Bol, 2018).

Perceived relevance or authority does not necessarily track intrinsic quality; it may be produced by the platform via distribution and signaling mechanisms. This generates a climate of apparently legitimate, yet structurally fragile, trust that amplifies legal risks.

Within this framework, liability analysis must extend beyond the classical author–recipient relationship to reflect a multi-actor reality: not only the content author matters, but also the platform that shapes the informational context and the algorithmic mechanisms that may artificially consolidate credibility. The segmented liability model captures this distribution of responsibility without conflating roles.

Legal responsibility in the digital environment should therefore be understood not only as a post-factum remedy, but also as an instrument for protecting the consumer’s legitimate trust within an informational environment marked by systemic imbalances.

The Digital Services Act and the Reconfiguration of Digital Platforms’ Responsibility

The Digital Services Act (Regulation (EU) 2022/2065) marks a turning point in the legal regulation of digital platforms in the European Union. While the eCommerce Directive entrenched, for more than two decades, the paradigm of the passive intermediary and technological neutrality, the DSA introduces a different normative architecture in which platforms acquire duties of diligence connected to the way they organize, distribute, and amplify information.

In the context of online legal advice, the DSA is relevant because it introduces duties of diligence concerning the architecture of content distribution and reaction mechanisms, with a direct impact on informational risks and on user protection.

From Passive Intermediary” to „Responsible Actor”: The New DSA Paradigm

The model established by the eCommerce Directive was built on the premise that platforms exercise limited control over transmitted or stored content. The DSA reconfigures this paradigm through a structural shift: platforms acquire duties of diligence and legal responsibility for the informational architecture they administer, and technical decisions such

as moderation, recommendation, and ranking are treated as having legally relevant effects (Kuczerawy, 2021; Husovec, 2022).

Consequently, distribution and recommendation become legally relevant as part of the platform’s duties of diligence, rather than merely serving as the technical “backdrop” of content.

Platforms’ Obligations in the Context of Online Legal Advice

Recent scholarship (Douek, 2021; Van Hoboken & Ó Fathaigh, 2022; Schulz & Dankert, 2023; Peguera, 2023) emphasizes that the DSA introduces a set of obligations that directly affect how information is perceived and used online. In the case of online legal advice, these obligations are all the more salient insofar as errors may have concrete consequences for the exercise of rights.

In essence, platforms must ensure meaningful transparency regarding recommendation and ranking criteria, so that the user can distinguish between algorithmic visibility and professional validation; in parallel, notice-and-action mechanisms require proportionate reactions to content reported as harmful, and for very large platforms the obligations extend to the assessment and mitigation of systemic risks, including through audits and governance measures. Complementarily, the DSA strengthens user control over recommendations (including alternative/non-personalized options), limiting the effects of overexposure and “validation through repetition.” Although the DSA does not directly regulate AI, the use of automated tools in delivering or amplifying information may be treated as a risk factor within the logic of duties of control and prevention, particularly where content affects the exercise of rights (Frosio, 2021).

Romania and the Republic of Moldova in Relation to the DSA: A Comparative Regulatory Overview

Regulatory differences that matter for online legal advice become more visible through a comparison between Romania (an EU Member State, with the DSA directly applicable), the Republic of Moldova (outside the DSA regime), and the EU framework as the normative matrix. In Romania, the DSA and national implementation mechanisms shape a framework oriented toward prevention and accountability, with obligations concerning transparency, risk management, and compliance oversight. In the Republic of Moldova, in the absence of a DSA-equivalent framework, the analysis remains anchored predominantly in civil law (especially Article 2018 of the Civil Code), emphasizing ex post compensation for harm and lacking specific instruments of algorithmic governance.

To illustrate these differences comparatively, Table 2 provides a synthesis of the regime applicable to online legal advice in the two states and at EU level, from the perspective of platform responsibility, user protection, and the treatment of algorithmic risks.

Table 2. Comparative Table: Legal Frameworks Governing Online Legal Advice

Regulatory Element	Romania (DSA + Law 50/2024)	Republic of Moldova	EU / DSA Framework
Applicable legal framework	Direct DSA application; Law 50/2024 operationalizes it; ANCOM designated as supervisory authority; layered governance combining DSA with civil law	No specific digital regulation; relies on general civil liability under Article 2018	Comprehensive DSA framework; coordinated oversight; shared standards.
Platform liability	Due diligence, notice-and-action, risk assessment, audits; liability also under national civil law	No specific platform duties; liability assessed through classical tort law	Multi-level obligations: moderation, risk audits, algorithmic accountability.
Transparency and information	Mandatory algorithmic transparency, explanations for automated decisions, option for non-personalized content display	No regulation on transparency or algorithmic logic	„Meaningful transparency” concept: clarity on algorithmic processes.
User protection	Strong procedural and preventive protections via DSA; supplemented by traditional remedies under civil law	Civil protections via interpretation of various laws; lacks digital-specific procedural tools.	Comprehensive procedural rights and risk-prevention mechanisms
Algorithmic governance	Explicit obligations: algorithmic risk audits, mitigation, non-personalized options	No recognition of algorithmic risks in legislation	Central to DSA: periodic audits, prohibition of manipulative algorithms for VLOPs
Online legal advice	Treated as high-risk content; platforms must manage visibility and categorization responsibly	Viewed as general information; protection depends on Article 2018 and fault analysis	Framed as systemic risk content with potential rights implications
AI-generated content	Indirectly regulated via technological risk obligations and transparency	Entirely unregulated from a digital perspective	Treated as high-risk content; special oversight for VLOPs

The table highlights the functional asymmetry between the two systems: in Romania, the emphasis falls on ex ante obligations (transparency, diligence, risk assessment), whereas in the Republic of Moldova protection is achieved predominantly ex post, through civil-law instruments. In this context, it becomes necessary to articulate a conceptual framework capable of integrating civil law with platform governance and the role of algorithms in shaping legal risk.

Conceptual Implications and the Shift Toward a Segmented Liability Model

The DSA shifts the focus from the isolated speaker to the distribution infrastructure, recognizing the role of digital architecture in generating risk. Against this background, an analytical instrument for the differentiated allocation of responsibility becomes useful.

The next section develops the segmented liability model and its operational utility.

The Segmented Liability Model: A Legal Architecture Centered on the Digital Consumer

Within platformized ecosystems, online legal advice generates legal risk that cannot be reduced to the author–user dyad.

Harm typically takes shape through a combination of factors: the content provided; the manner in which it is presented and distributed within the platform; and the amplifying effects of algorithmic mechanisms on the visibility and perceived credibility of information—vis-à-vis a consumer situated in a position of cognitive vulnerability and not reasonably able to autonomously verify the accuracy of the response (a *credence service*).

Against this background, the paper proposes the segmented liability model as an analytical tool for the differentiated allocation of responsibility within a multi-actor informational chain, compatible both with the European regulation of platforms and with the logic of civil liability in the legal systems under analysis (Busch & De Franceschi, 2021; Floridi, 2014).

The illustrative anchoring of these distinctions through jurisprudential reference points and factual incidents is developed subsequently in Section 5.

The Foundation of the Model: The Interaction Between Author, Platform, and Algorithm

The factual and conceptual premises concerning the platformized distribution of legal information and the role of recommendation mechanisms were established in Section 1.

Accordingly, liability analysis can no longer remain confined to the author–user axis, because harm is often formed through the interaction between the legal content provided, the delivery architecture, and the credibility signals produced by the platform, as well as the opaque amplification/validation through recommendation and ranking (Husovec, 2022; Kuczerawy, 2021; Douek, 2021).

The segmented liability model therefore proposes an analytical separation of these causal contributions, in order to identify the pertinent actor and the legally significant conduct within technological causal chains, avoiding both automatic mono-causal attribution and the dilution of responsibility through the conflation of roles.

The Three Tiers of Liability in the Segmented Model

The segmented liability model operates with three analytical tiers, corresponding to distinct causal contributions in the formation of legal risk and legal harm. The delimitation seeks to separate elements of content, informational architecture, and algorithmic amplification, so that the attribution of responsibility can be assessed in a differentiated manner.

The Operational Structure of the Segmented Model

In digital environments, attributing liability to a single actor is often inappropriate, since harm frequently results from the interdependence between content, informational architecture, and algorithmic amplification.

Operationally, the model separates the relevant causal contributions and correlates them with the forms of liability applicable under Romanian law, Moldovan law, and within the EU framework.

Table 3 synthesizes, for each tier, its role in generating risk, the typologies of contribution to harm, and the potentially applicable liability regimes.

Table 3. The Structure of Segmented Liability in Online Legal Advice

Actor	Role in Risk Generation	Contribution to Harm	Potential Form of Liability
Author of legal content	Produces the initial legal information; determines accuracy, clarity, and completeness	Direct legal error; omission of essential information; ambiguous legal formulations; creation of unjustified trust	Civil liability (tort or contract-based, depending on whether a contractual relationship exists)
Platform	Creates and manages the informational architecture; ranks, promotes, and contextualizes content	Amplification of erroneous content; lack of algorithmic transparency; inadequate response to notices; creation of unwarranted professional authority	Independent civil liability; technological and procedural obligations under the DSA (risk assessment, audits, etc.)
Algorithm	Selects, ranks, and prioritizes legal information	Distortion of accurate information; unintentional amplification of incorrect content; false validation through placement; excessive homogenization of information flows	Not a legal subject per se; indirect liability through the platform, based on obligations for audit, control, and transparency

On the basis of this structure, the following section highlights the model’s analytical advantages.

The Analytical Advantages of the Segmented Liability Model

The segmented liability model has three main advantages.

First, it enables a differentiated identification of the source of legal harm in the digital environment, avoiding the reduction of the phenomenon to a “single author” and delineating the relevant contributions of the author, the platform, and algorithmic mechanisms.

Second, it coherently integrates civil-liability principles with the preventive layer of digital governance: it does not replace traditional rules, but renders them operational within a framework in which, in Romania, DSA obligations (transparency, procedures, risk assessment) operate complementarily to civil remedies.

Third, it treats algorithmic risks as autonomous vectors of amplification, which is useful for explaining situations where harm does not derive from an isolated error, but from effects of ranking, repetition, and technical validation.

Through this structure, the model also provides a conceptual basis for discussing generative AI, where the boundaries between author, platform, and technical instrument tend to blur.

The next section develops the model’s comparative application in Romania and the Republic of Moldova, while Section 5 anchors it illustratively in jurisprudential reference points and factual incidents in order to clarify diligence expectations at each tier.

The Application of the Segmented Liability Model in Romania and the Republic of Moldova

The comparative analysis of how the segmented liability model operates in Romania and the Republic of Moldova highlights two distinct ways of integrating the technological dimension into the assessment of legal risk associated with online legal advice.

The difference is not exclusively legislative; it also concerns how mechanisms of prevention, proof, and redress function within a multi-actor digital ecosystem.

Against this background, the section aims to delineate the contribution of each tier and to highlight their implications for the protection of the digital consumer.

Romania – The Effective Functioning of Segmented Liability within an Integrated Regulatory Framework

In Romania, the application of the DSA, read together with Law no. 50/2024, renders segmented analysis operational by introducing an ex ante layer of obligations concerning transparency, reaction procedures, and risk management, which operates complementarily to civil-law remedies. From the civil-law perspective, the author remains the natural target of liability for the accuracy and completeness of content; from the perspective of the platform’s own conduct, design and governance choices become relevant insofar as they shape users’ reasonable expectations and the conditions of distribution/amplification.

Within this configuration, algorithmic mechanisms are not treated as subjects of law, but as objects of the operator’s organizational control (auditability, traceability, functional safeguards). By reducing informational asymmetries (particularly through transparency duties and procedural obligations), the Romanian framework increases the prospects of differentiated causal attribution and reduces the tendency for the dispute to “collapse” exclusively onto the most visible actor.

The Republic of Moldova – Doctrinal Application of the Model within Civil Law

The Republic of Moldova does not currently have a digital framework equivalent to the Digital Services Act. Nonetheless, a systematic analysis of domestic legislation reveals a normative core that can support—through evolutionary interpretation—the application of the segmented liability model.

Article 2018 of the Civil Code provides a foundation for liability based on legitimate reliance on incorrect information or recommendations, while rules on advice and tort liability allow liability to be engaged even in the absence of a formal contractual relationship. Related legislation on e-commerce, personal data protection, and access to information complements this framework, offering anchoring points for analysing platform responsibility and algorithmic personalization; however, the role of the platform and of algorithmic mechanisms is not yet structured through explicit duties of transparency, audit, or preventive risk management.

Applying the segmented model in the Republic of Moldova is therefore possible, but it remains conditioned on extensive doctrinal interpretation and on leveraging existing civil-law institutions, particularly liability grounded in legitimate trust. Functional differences vis-à-vis Romania are comparatively synthesized in Section 4.3 and analysed in Section 4.4.

Comparative Synthesis of the Segmented Liability Model in Romania and the Republic of Moldova

Table 4 synthesizes how the segmented liability model is reflected in each legal order, from the perspective of regulation, the structure of responsibility, and user protection

Table 4 – Application of the Segmented Liability Model in Romania and the Republic of Moldova

Criterion	Romania	Republic of Moldova
Primary regulation	Harmonized digital European framework: DSA directly applicable, supplemented by Law No. 50/2024 as the national mechanism for implementation and oversight, in correlation with the general tort liability rules in the Civil Code.	Classical civil law framework: Civil Code (Art. 2018, Art. 1415–1418, Art. 1979–1982) and related laws (Law No. 284/2004 on e-commerce, Law No. 133/2011 on personal data, Law No. 241/2007 on electronic communications, Law No. 148/2023 on access to information).
Structure of liability	Distributed across distinct layers: author – platform – algorithm, under a cumulative regime combining traditional civil liability with preventive digital obligations.	Predominantly linear: author – user; the author remains the central pivot of liability.
Platform responsibility	Expressly regulated through the DSA: obligations of transparency, algorithmic auditing, risk management, and notice-and-action mechanisms, without excluding civil liability for own actions.	Not specifically regulated; liability possible only through extensive doctrinal interpretation, relying on the theory of legitimate reliance.
Role of algorithms	Recognized as legal risk vectors; subject to evaluation, audit, and control obligations as part of platform responsibility.	Absent as an autonomous legal concept; may be conceptually integrated through interpretation of Article 2018 of the Civil Code.
User protection	Strengthened protection: procedural and preventive mechanisms established under the DSA, supplemented by classical civil remedies (tort liability).	Predominantly post-factum protection; user bears the burden of proving the harm.
Liability for amplification of error	Directly regulable through platform obligations concerning information architecture and algorithmic amplification.	Difficult to prove in practice; lacks technological instruments for prevention.
Compatibility with segmented model	High – the model integrates naturally into a layered normative framework (civil + digital).	Medium – dependent on doctrinal developments and potential legislative reforms.
Level of digital maturity	Advanced – functionally integrated within the EU’s digital regulatory architecture.	Emerging – requires adaptation of civil law norms to digital realities.
Evolutionary direction	Consolidation of the existing framework and expansion toward legal AI regulation.	Digital reform and gradual convergence with European standards.

The synthesis highlights differences that are not only normative but also functional: in Romania, there is a framework that facilitates integrating the technological dimension into risk analysis, whereas in the Republic of Moldova civil-law instruments of subsequent compensation predominantly prevail.

The Preventive–Reactive Gap and Convergence Scenarios

Based on the analysis in Sections 4.1–4.3, the central difference between the two systems may be described as a preventive–reactive gap: in Romania, the DSA-related ex ante layer internalizes risks linked to distribution and recommendation, while in the Republic of Moldova ex post civil-law instruments predominate, with a heavier evidentiary burden on the user.

In the Republic of Moldova, conceptual convergence is possible along three complementary tiers. A first tier is doctrinal, by leveraging existing civil-law institutions—fault, advice, and legitimate trust—to extend the analysis beyond content as such toward the infrastructure that confers visibility and authority on information in the digital environment. A second tier is normative and gradual, which could introduce minimal transparency duties and functional notice-and-action procedures for potentially harmful content, without fully replicating the DSA apparatus. A third tier concerns evidentiary convergence and risk governance, by clarifying diligence standards and establishing mechanisms for access to relevant information (for example, recommendation criteria, logs, traceability), so that liability attribution becomes operational within technological causal chains. Overall, the differences between the two systems primarily reflect Romania’s membership in the Union framework and the existence of an *ex ante* layer of digital governance, whereas the Republic of Moldova remains a space for civil-law adaptation with potential for gradual evolution.

Illustrative Validation of the Segmented Liability Model: Jurisprudential Reference Points, Factual Vignettes, and the Sustainability of Digital Governance

The Role of Illustrative Validation and Selection Criteria

In order for the segmented liability model to be usable beyond the purely conceptual level, this section selectively draws on a small number of publicly visible jurisprudential reference points and factual vignettes. They are not treated as generalizable empirical “evidence” and do not aim to provide a quantitative mapping of litigation; rather, they function as plausibility tests. They help identify the legally relevant conduct, the pertinent actor, and the way in which an informational risk can translate into harm in digital contexts.

The selection of examples follows three benchmarks: first, the possibility of associating each example predominantly with one of the model’s tiers (author–platform–algorithmic mechanism), without artificially conflating roles; second, the clarity of the causal chain, from the production or uptake of information to the harmful consequence; third, their relevance for outlining the expected conduct at each tier (diligence and verification; design and warning; control, audit, and traceability).

Intentionally, these reference points are treated as analytical units: they allow a legal “cut-out” of the pertinent conduct in *credence service* situations, where autonomous verification of informational accuracy is, realistically, impracticable.

The “Author” Tier: the Standard of Diligence and the Duty to Verify When Using Generative Tools

At the author tier, legal risk arises at the level of the conduct of the person who produces, selects, or reuses legal information and presents it as a basis for a decision. The use of a generative tool does not “transfer” responsibility; it changes the diligence context: it increases the importance of source verification, final control over assertions, and filtering of plausible errors precisely because of their persuasive form.

A useful reference point, even if it does not concern online legal advice *stricto sensu*, is *Mata v. Avianca* (S.D.N.Y., 2023), which became emblematic for the risk of fictitious citations generated by generative tools and then introduced into professional circulation without verification.

The analytical stake, for the model, is a clear delimitation of the relevant conduct: not the technical “hallucination” as such, but the author’s conduct in validating and transmitting as

true content that could have been verified by reasonable means, thereby increasing the likelihood of harm (material, professional, or procedural).

Operationally, the author tier activates classic criteria (fault/diligence, foreseeability, causation), but within a framework in which the message’s “technologically credible” form may induce disproportionate reliance. This explains why the duty to verify becomes the pivotal criterion at this tier.

The “Platform” Tier: the Architecture of Trust and Responsibility for the Delivery Interface

At platform level, the focus is not on content *per se*, but on how content is delivered as a “service”: the official interface, credibility signals, functional warnings, and the capacity to correct problematic information once it appears. At this tier, the typical risk is misleading the user through “contextualization” (how the message is presented and what reasonable expectations it generates).

Moffatt v. Air Canada (B.C. Civil Resolution Tribunal, 2024) is useful precisely because it treats information provided through a chatbot as part of the service communication, and the entity operating the tool cannot dissociate itself from its own official channel by arguing that the user “should have verified elsewhere.”

For the segmented model, the case is relevant because it delineates the platform tier: choosing to provide information through an official conversational interface triggers requirements of accuracy, warning, and corrective remedies, independently of the automated character of generation.

The “Algorithm” Tier: Opaque Amplification, Design Defects, and Risk Governance

At the tier of algorithmic mechanisms, the risk is no longer a punctual error, but a systemic effect: selection, ordering, and personalization can produce false validation (through positioning/repetition), overexposure, and persistence, while opacity impedes both user self-correction and causal attribution in litigation. Since the algorithm is not a subject of law, legal analysis shifts toward the governance duties of the actor who operates it: control, monitoring, functional safeguards, auditability, and traceability.

The episode of the “Tessa” chatbot, launched by the National Eating Disorders Association, is relevant as a risk-governance vignette: a conversational tool presented with the appearance of specialized support was withdrawn in 2023 following public reactions concerning responses considered inappropriate for the target audience. This highlights the importance of *safety-by-design* guarantees (delimitations, functional warnings, escalation to human support, monitoring, and rapid intervention).

Finally, the litigation *Garcia v. Character Technologies Inc.* (M.D. Fla., 2024, pending) is useful as a “test” for the register of design defects and foreseeable risks of conversational interaction (anthropomorphization, engagement strategies, emotional validation).

Even as a pending case, it is methodologically relevant: it shifts the discussion from an isolated exchange (“what was said”) to the control framework (“what limits, monitoring, and intervention mechanisms were instituted”)—precisely the zone in which the algorithmic tier becomes legally intelligible through the operator’s obligations.

In model terms, the stake of the algorithmic tier is not the identification of an “author” of the error, but the delimitation of foreseeable risk generated by design and operation, and of the control obligations incumbent on the platform in relation to amplification effects, opaque validation, and repeated exposure.

Implications for the Model: Confirmations, Tensions, and Limits of Segmentation

Taken together, the examples discussed support a central intuition of the paper: in digital ecosystems, harm associated with online legal advice is generally not mono-causal. It arises from a combination of contributions: error, omission, or ambiguity at the level of content (author); the conversion of that content into harm through the trust-and-delivery context created by the platform interface (platform); and opaque amplification or validation through recommendation mechanisms and conversational design (algorithm, as an object of platform governance). Accordingly, a strictly author–user analysis risks overlooking what, in platformized environments, often makes the difference between questionable information and effective harm: the infrastructure that confers visibility, authority, and persistence on content.

Practically, this explains the value of the segmented liability model as an orienting grid. The tiered distinction remains productive because it separates roles without conflating them, helping identify the pertinent defendant and the legally significant conduct within a technological causal chain—without forcing a “single culprit” narrative or diluting the distinct contributions of the author, the platform, and algorithmic-risk governance.

The tensions, however, remain structural. Segmentation is difficult to operationalize without access to recommendation criteria, logs, and traceability, and these evidentiary constraints tend to re-concentrate litigation on the “visible” actor (the author), even where distribution mechanisms made a material contribution. This is where an *ex ante* governance layer (where it exists) shows its value: it does not replace civil remedies, but it can reduce the informational asymmetries that hinder liability attribution in technological causal chains.

In ECO4ALL terms, the stake is to avoid externalizing technological risks onto consumers and to shape sustainable digital markets through accountability and risk governance. The reference points analyzed indicate the need to treat recommendation systems and conversational design as objects of the platform’s organizational diligence: proportionate risk assessment and mitigation, meaningful transparency, effective control and audit mechanisms, and operational procedures for intervention and correction.

Finally, this section should be read in an illustrative key: the examples neither ground generalizations nor substitute an empirical litigation analysis; they provide controlled reference points showing how the model applies when risk is generated through the interaction between content, interface, and recommendation mechanisms.

SDG12 and the Circular Economy of Legal Information: From Informational Risk to Sustainable Governance

In the digital economy, legal information circulates in a quasi-circular regime: it is produced, taken up, repackaged, recommended, and recirculated at scale, while its utility for users is decisively shaped by distribution architectures and the credibility signals attached to content. Absent minimal guarantees of traceability and control, the same error can be replicated and amplified into a systemic externality: the costs of being misled fall predominantly on the vulnerable consumer, while the economic benefits of content circulation and attention monetization accrue to the platformized infrastructure. In this sense, SDG12 (Responsible Consumption and Production), as a goal of the UN 2030 Agenda, can be translated juridically into a requirement of responsible production and distribution of legal information online, including by limiting the persistence and recirculation of erroneous or misleading content.

The segmented liability model provides an operational bridge between fairness, accountability, and sustainability. Fairness follows from reducing structural asymmetries: the model separates causal contributions and explains why the consumer, situated in a *credence*

service, cannot be treated as the final validator of accuracy. Accountability results from the differentiated allocation of obligations: the author bears responsibility for diligent verification of content; the platform for the delivery architecture and the trust signals it produces; and algorithmic risk is treated as an object of platform governance (control, audit, traceability). Sustainability is understood as internalizing risks in design and operation so that errors are not scaled and recirculated as informational externalities; where an *ex ante* layer exists (such as the DSA), this logic is reinforced through meaningful transparency, functional corrective procedures, and risk-management mechanisms capable of reducing the social costs of digital harm and preventing their externalization onto consumers.

Conclusions, Limitations, and Future Directions: Legal Responsibility in Online Legal Advice and the Protection of the Digital Consumer

Conclusions

The paper began by asking whether classical civil-liability models, centered on the author–user relationship, can adequately explain harm produced in online legal advice. The analysis confirms the working hypothesis: in multi-actor digital ecosystems, harm typically results not only from the content provided, but from the interaction between content, delivery architecture, and distribution and recommendation mechanisms. In this framework, online legal advice often functions as a *credence service*, and the digital consumer cannot realistically be treated as the final validator of accuracy.

On this basis, the study’s central contribution is the formulation and operationalization of the segmented liability model (author–platform–algorithmic mechanism). The model provides an analytical tool for legally “carving out” relevant conduct and for avoiding both mono-causal simplification (automatic attribution of harm to the author) and the dilution of responsibility through conflated roles. Practically, segmentation operates as an orienting grid, enabling the identification of the pertinent actor and legally significant conduct within a technological causal chain, without reducing the phenomenon to a “single culprit.”

The comparative analysis reveals a relevant functional difference between Romania and the Republic of Moldova. Romania operates within a layered framework in which civil-law remedies are complemented by an *ex ante* layer of digital governance under the DSA (and domestic implementation mechanisms), rendering the platform’s contribution and algorithmic risk more legally intelligible through transparency, risk assessments, procedures, and notice responses. The Republic of Moldova, lacking a functional DSA equivalent, remains predominantly *ex post*, but it retains relevant civil-law anchors—especially legitimate trust (Article 2018 of the Civil Code)—which can, through evolutionary interpretation, extend analysis beyond content to delivery and validation infrastructure.

The illustrative validation section (jurisprudential reference points and factual vignettes) reinforces the model’s methodological plausibility: the author tier foregrounds diligence and the duty to verify, including when generative tools are used; the platform tier shows how interfaces and credibility signals can convert problematic information into effective harm; and the algorithmic tier clarifies why risk becomes legally intelligible through operator governance (control, audit, traceability, and functional “brakes”), rather than by attributing legal subjectivity to the algorithm.

Finally, integrating the SDG12 perspective and the “quasi-circular economy” of legal information completes the argument coherently: absent traceability and control, errors are recirculated and amplified, and costs are externalized onto the vulnerable consumer. The segmented model supports a fairer allocation of risk by reducing structural asymmetries

(fairness), differentiating duties (accountability), and internalizing risks in design and operation (sustainability), with stronger potential where an ex ante governance layer exists.

Practical and Normative Implications

The analysis yields three main implications for the civil-law characterization of harm produced through online legal advice.

At the author tier, the diligence standard remains the anchor of liability, but it must be calibrated to the risks of “technologically credible” content. The duty to verify becomes decisive, alongside avoiding the presentation of unverified content as certain and explicitly delimiting the level of personalization (general guidance versus a recommendation applied to a concrete situation).

At the platform tier, responsibility becomes legally relevant whenever the platform constructs a context of trust: delivering information through an official interface, attaching signals of authority, omitting functional warnings, or responding inadequately to content with harmful potential. Relevance does not turn on automated generation, but on how the platform shapes users’ reasonable expectations and the conditions under which they rely on information.

At the level of algorithmic risk governance, expected operator conduct includes meaningful transparency on recommendation criteria, auditability, traceability (relevant logs), intervention and correction mechanisms, and functional limits in sensitive contexts. Without these safeguards, causal attribution becomes difficult in litigation, and disputes tend to re-concentrate on the “visible” actor (the author), even when distribution or amplification materially contributed to the harm.

Limitations

The paper acknowledges several limitations that flow directly from its methodological choices.

The inquiry is predominantly normative and doctrinal. It does not seek empirical validation of litigation frequency, nor a quantitative measurement of how online legal advice affects user behavior or legal decisions adopted on its basis.

The jurisprudential reference points and factual vignettes serve an illustrative function, as plausibility tests for the causal chain and for delineating tiers (author–platform–algorithm). They are not a representative sample and cannot support statistical generalizations.

The Romania–Republic of Moldova comparison is deliberately focused on mechanisms for attributing liability and on conceptualizing the contribution of platforms and algorithmic distribution. It is not an assessment of enforcement effectiveness, institutional capacity, or a systematic mapping of domestic judicial practice.

The analysis remains centered on civil liability and consumer protection, without exhaustively addressing intersections with professional/disciplinary liability, criminal liability, or the full range of public-law sanctioning mechanisms.

Finally, the rapid evolution of AI tools and platformized architectures may quickly change technical risk profiles and design practices. Accordingly, the model’s concrete applications realistically require periodic updates, even if the conceptual structure remains useful as an analytical grid.

Future Research Directions

Based on the findings and limitations, several avenues for further research emerge.

Empirically, it becomes relevant to validate the model by mapping litigation—and the phenomenon of “non-litigation”—in online legal advice, including an analysis of barriers to

access to justice and of the difficulties in identifying the pertinent actor and characterizing technological causal chains.

From an evidentiary and access-to-information perspective, it is necessary to develop a traceability framework (relevant logs, recommendation criteria, auditability) and to assess legal instruments capable of reducing informational asymmetries in disputes involving algorithmic distribution, amplification, and validation.

At the level of normative intersections, the model could be more explicitly integrated with developments in AI regulation and governance (transparency duties, technical and organizational standards) and with the modernization of liability regimes for digital products, to clarify complementarities and potential tensions between frameworks (De Bruyne, Dheu & Ducuing, 2023; Hacker, 2023).

Applicatively, the model merits testing across distinct platform types (service marketplaces, social networks, search engines, conversational applications) and content forms (from FAQs to contextualized or automated recommendations), with a view to refining tier-specific diligence standards and more precisely delineating risk thresholds.

For the Republic of Moldova, a practically significant direction is doctrinal and legislative-policy analysis of the gradual introduction of minimal functional mechanisms (basic transparency, notice-and-action, access to relevant data), compatible with the civil-law matrix and existing instruments, without presupposing full transplantation of the DSA apparatus.

References

- Balkin J. M. (2021). How to regulate (and not regulate) social media. “Journal of Free Speech Law”, Vol. 1, pp. 71–96.
- Busch C., De Franceschi A. (Eds.) (2021). Algorithmic Regulation and Personalized Law: A Handbook. Baden-Baden: Nomos.
- Cimil D. (2013). Calificarea raporturilor contractuale. Chişinău: Grafema Libris.
- De Bruyne J., Dheu O., Ducuing C. (2023). The European Commission’s approach to extra-contractual liability and AI: An evaluation of the AI Liability Directive and the revised Product Liability Directive. “Computer Law & Security Review”, Vol. 51.
- Douek E. (2021). Governing Online Speech: From Posts-as-Trumps to Proportionality and Probability. “Columbia Law Review”, Vol. 121, pp. 759–840.
- European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act). “Official Journal of the European Union”, L 277, 27 October 2022.
- Floridi L. (2014). The Fourth Revolution. Oxford: Oxford University Press.
- Frosio G. (2021). From Horizontal to Systemic Liability: Re-thinking Intermediary Liability in the Platform Economy. “Journal of Intellectual Property, Information Technology and Electronic Commerce Law”, Vol. 12, No. 3, pp. 193–210.
- Garcia v. Character.ai, Case No. 24-cv-05123 (M.D. Fla. 2024), available at: <https://www.courtlistener.com/docket/69300919/garcia-v-character-technologies-inc/>, accessed 28 January 2026.
- Hacker P. (2023). The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future. “Computer Law & Security Review”, Vol. 51.
- Helberger N., Sax M., Strycharz J., Micklitz H.-W. (2022). Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. “Journal of Consumer Policy”, Vol. 45, No. 2, pp. 175–200.

- Husovec M. (2022). *Injunctions Against Intermediaries in the European Union*. Cambridge: Cambridge University Press. DOI: 10.1017/9781108895470.
- Kuczerawy A. (2021). *The Digital Services Act: Towards a More Responsible Internet*. “Computer Law & Security Review”, Vol. 41, Article 105561. DOI: 10.1016/j.clsr.2021.105561.
- Mata v. Avianca, U.S. District Court (S.D.N.Y.), 2023, available at: <https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2022cv01461/575368/54/>, accessed 28 January 2026.
- Moffatt v. Air Canada, 2024 BCCRT 149, available at: <https://www.canlii.org/en/commentary/doc/2025CanLIIDocs1963>, accessed 28 January 2026.
- Pasquale F. (2015). *The Black Box Society*. Cambridge, MA: Harvard University Press.
- Peguera M. (2023). *The Notice-and-Action Mechanisms in the Digital Services Act*. “European Law Review”, Vol. 48, No. 2, pp. 257–276.
- Plotnic O. (2011). *Protecția consumatorului în raporturile juridice civile*. Chișinău: CEP USM, Universitatea de Stat din Moldova.
- Republic of Moldova. (2002). *Civil Code of the Republic of Moldova*, adopted by Law No. 1107-XV of 6 June 2002. “Official Gazette of the Republic of Moldova”, Nos. 82–86, 22 June 2002, Arts. 2018, 1415–1418, 1979–1982.
- Republic of Moldova. (2004). *Law No. 284/2004 on Electronic Commerce*. “Official Gazette of the Republic of Moldova”, Nos. 138–146, 13 August 2004.
- Republic of Moldova. (2007). *Law No. 241/2007 on Electronic Communications*. “Official Gazette of the Republic of Moldova”, Nos. 51–54, 11 March 2008.
- Republic of Moldova. (2011). *Law No. 133/2011 on Personal Data Protection*. “Official Gazette of the Republic of Moldova”, Nos. 170–175, 14 October 2011.
- Republic of Moldova. (2016). *Law No. 8/2016 on Access to Information*. “Official Gazette of the Republic of Moldova”, Nos. 75–81, 18 March 2016.
- Romania. (2009). *Civil Code*, adopted through Law No. 287/2009. “Official Gazette of Romania”, No. 505, 2009, Arts. 1349–1395.
- Romania. (2024). *Law No. 50/2024 on Measures for the Implementation of 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), and on Amending and Supplementing Law No. 365/2002 on Electronic Commerce*. “Official Gazette of Romania”, No. 232, 19 March 2024.
- Sax M., Helberger N., Bol N. (2018). *Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices*. “Journal of Consumer Policy”, Vol. 41, No. 2, pp. 103–134.
- Schulz W., Dankert K. (2023). *Regulating Recommender Systems: Transparency, Choice and Accountability under the DSA*. “Journal of European Consumer and Market Law”, Vol. 12, No. 1, pp. 1–10.
- Van Hoboken J., Ó Fathaigh R. (2022). *Regulating Systemic Risks in the Digital Services Act*. “European Law Journal”, Vol. 28, Nos. 3–4, pp. 255–279. DOI: 10.1111/eulj.12413.
- National Eating Disorders Association (NEDA). (2023). *Tessa chatbot: reports on its withdrawal following feedback*, available at: <https://www.yahoo.com/lifestyle/eating-disorder-chatbot-shut-down-224806659.html>, accessed 28 January 2026.