

Legal Safeguards and Regulatory Controls Governing the Use of Social Media Networks in the Digital Space

الضمانات القانونية وآليات ضبط استخدام شبكات
التواصل الاجتماعي في الفضاء الرقمي

Garanties juridiques et mécanismes de régulation de l'usage des
réseaux sociaux dans l'espace numérique

MEZAACHE ABDERRAHIM

University M'hamed Bougara of Boumerdès

Avenue de l'Indépendance, 35 000 Boumerdès , Algérie

a.mezaache@univ-boumerdes.dz

<https://orcid.org/0009-0007-9309-8092>

Date de réception	Publication numérique	Archivage ASJP
25/03/2026	22/05/2026	19/06/2026

Référence électronique

Mezaache Abderrahim, « Legal Safeguards and Regulatory Controls Governing the Use of Social Media Networks in the Digital Space », Aleph [En ligne], Vol 13 (3) | 2026, mis en ligne le 22 mai 2026, consulté le 08 juillet 2026. URL : <https://aleph.edinum.org/16822>

Référence papier (archivage Asjp)

Mezaache Abderrahim, « Legal Safeguards and Regulatory Controls Governing the Use of Social Media Networks in the Digital Space », Aleph, Vol 13 (3) | 2026, 385-403.

Abstract

This article examines the legal safeguards and regulatory controls governing the use of social media networks in the digital space. The expansion of online platforms has transformed the conditions under which individuals communicate, express opinions, circulate information, form communities and participate in public debate. At the same time, it has increased the risks of privacy violations, misuse of personal data, reputational harm, online harassment, misinformation and unlawful publication. The study adopts a doctrinal and comparative legal method, drawing on international human rights instruments, regional conventions, European data-protection and platform-regulation frameworks, and Algerian legislation. It argues that social media cannot be treated either as a space of unrestricted expression or as a space of uncontrolled surveillance and censorship. The legitimate regulation of digital expression must therefore be based on legality, legitimate aim, necessity, proportionality, transparency and effective remedy. The article concludes that the protection of users requires a balanced framework combining individual awareness, platform accountability, data-protection rules, judicial safeguards and public regulation respectful of fundamental freedoms.

Keywords

social media networks, legal safeguards, platform regulation, privacy, personal data, freedom of expression, cybersecurity

المخلص

يتناول هذا المقال الضمانات القانونية وآليات الضبط المنظمة لاستخدام شبكات التواصل الاجتماعي في الفضاء الرقمي. فقد غيّرت المنصات الرقمية شروط التواصل والتعبير عن الرأي وتداول المعلومات وتشكيل الجماعات والمشاركة في النقاش العام، لكنها في الوقت نفسه ضاعفت مخاطر المساس بالحياة الخاصة، وسوء استعمال المعطيات الشخصية، والإضرار بالسمعة، والتحرش الإلكتروني، والتضليل، والنشر غير المشروع. تعتمد الدراسة منهجاً قانونياً تحليلياً ومقارناً يستند إلى المواثيق الدولية لحقوق الإنسان، والاتفاقيات الإقليمية، والأطر الأوروبية المتعلقة بحماية البيانات وتنظيم المنصات، والتشريع الجزائري. وتذهب الدراسة إلى أن شبكات التواصل الاجتماعي لا يمكن النظر إليها بوصفها فضاءاً للتعبير المطلق، ولا بوصفها مجاًلاً مفتوحاً للرقابة أو التقييد غير المنضبط. لذلك ينبغي أن

تقوم مشروعية تقييد التعبير الرقمي على مبدأ الشرعية، والهدف المشروع، والضرورة، والتناسب، والشفافية، وضمان سبل الانتصاف الفعّالة. وتخلص الدراسة إلى أن حماية المستخدمين تتطلب إطاراً متوازناً يجمع بين الوعي الفردي، ومسؤولية المنصات، وقواعد حماية البيانات، والضمانات القضائية، والتنظيم العام المحترم للحريات الأساسية.

الكلمات المفتاحية

شبكات التواصل الاجتماعي، الضمانات القانونية، تنظيم المنصات، الحياة الخاصة، المعطيات الشخصية، حرية التعبير، الأمن السيبراني

Résumé

Cet article examine les garanties juridiques et les mécanismes de régulation applicables à l'usage des réseaux sociaux dans l'espace numérique. L'extension des plateformes sociales a transformé les conditions de la communication, de l'expression des opinions, de la circulation de l'information, de la formation des communautés et de la participation au débat public. Elle a toutefois renforcé les risques d'atteinte à la vie privée, d'usage abusif des données personnelles, d'atteinte à la réputation, de harcèlement en ligne, de désinformation et de publication illicite. L'étude adopte une méthode juridique doctrinale et comparative, fondée sur les instruments internationaux des droits de l'homme, les conventions régionales, les cadres européens relatifs aux données personnelles et aux plateformes, ainsi que la législation algérienne. Elle montre que les réseaux sociaux ne sauraient être considérés ni comme un espace d'expression illimitée ni comme un espace de surveillance ou de censure sans contrôle. La régulation légitime de l'expression numérique doit ainsi reposer sur la légalité, le but légitime, la nécessité, la proportionnalité, la transparence et l'existence de recours effectifs. L'article conclut que la protection des usagers suppose un cadre équilibré associant vigilance individuelle, responsabilité des plateformes, protection des données, garanties judiciaires et régulation publique respectueuse des libertés fondamentales.

Mots-clés

réseaux sociaux, garanties juridiques, régulation des plateformes, vie privée, données personnelles, liberté d'expression, cybersécurité

Introduction

The development of information and communication technologies has profoundly changed the legal and social conditions under which individuals participate in public life. Social media networks have become ordinary instruments of communication, self-presentation, information exchange, political discussion, cultural participation and professional interaction. They are no longer marginal technical tools ; they constitute, for many users, a daily environment in which private life, social relations and public speech intersect. Facebook, X/Twitter, Instagram, YouTube, TikTok, LinkedIn and other platforms enable users to create profiles, publish opinions, share images and videos, comment on public events, organize communities and interact across geographical borders.

This transformation has undeniably expanded the practical possibilities of freedom of expression. Individuals who previously depended on traditional media institutions to access a public audience can now publish directly, respond immediately and circulate information widely. The digital space has therefore opened new forms of participation and has contributed to the democratization of speech. Yet the same environment also produces serious legal risks. A post, an image, a comment or a forwarded message may affect privacy, reputation, personal data, religious sensibilities, public order or national security. The speed, persistence and transnational circulation of online content mean that harm may be amplified before ordinary legal mechanisms are able to intervene.

The legal question is therefore not whether social media should be free or regulated. The decisive question is how to articulate freedom and responsibility in a digital environment where users, platforms and public authorities all participate in the production, circulation and moderation of content. The right to freedom of expression remains a fundamental right, protected by international and constitutional instruments. However, it is not an absolute right. Under international human rights law, restrictions may be imposed only when they are provided by law, pursue a legitimate aim and are necessary and proportionate in a democratic society. This principle is essential because the regulation of online speech may itself become a source of abuse if it is formulated in vague, excessively broad or discretionary terms.

The present article examines the legal safeguards and regulatory controls governing the use of social media networks in the digital space. It focuses on three safeguards that structure the protection of users : the right to privacy, the protection of personal data and freedom of expression. It then examines three categories of legal controls : respect for the law and the principle of legality, respect for public order and public morality, and respect for the rights, freedoms and religious sentiments of others. The aim is not merely to list legal norms, but to show how they interact and how they must be balanced in order to avoid two symmetrical

dangers : the absence of regulation, which exposes users to abuse, and excessive regulation, which threatens public debate and fundamental freedoms.

The study is based on a doctrinal and comparative legal method. It analyses international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, regional instruments such as the European Convention on Human Rights, the American Convention on Human Rights and the Arab Charter on Human Rights, as well as selected European and Algerian legal frameworks. Particular attention is given to privacy in the digital age, data protection, platform responsibility and the legal standards of necessity and proportionality. The comparative dimension does not aim to transpose one system mechanically into another ; rather, it identifies common principles and points of divergence that can assist in constructing a balanced framework for the regulation of social media.

The article proceeds in two main parts. The first part analyses the legal safeguards protecting users of social media networks in the digital environment. The second part examines the legal controls that limit the exercise of rights on these platforms. The conclusion presents the principal findings and recommendations, with emphasis on the need for a legally precise, rights-based and technologically informed regulatory approach.

The contribution of the study lies in bringing together areas of law that are often treated separately. Studies of freedom of expression sometimes neglect data protection, while studies of privacy sometimes give insufficient attention to the democratic function of online speech. A legal approach to social media must avoid this fragmentation. The user is simultaneously a speaker, a data subject, a potential victim of unlawful content and sometimes a producer of harmful content. Platforms are simultaneously private companies, technical intermediaries, economic actors and quasi-public spaces of visibility. This dual complexity requires an integrated analysis rather than a simple inventory of rights and restrictions.

1. Legal Safeguards for the Use of Social Media in the Digital Environment

Social media networks have become one of the most visible manifestations of the digital transformation of public and private life. They facilitate dialogue, mobilization, access to information and the expression of individual identity. In many contexts, they have also played an important role in political debate, social protest, professional networking, cultural circulation and civic participation. These functions explain why their legal regulation cannot be reduced to a purely technical matter. The regulation of social media directly concerns fundamental rights.

The legal safeguards applicable to social media users must be understood as protective mechanisms designed to preserve the dignity, autonomy and freedom

of individuals in a technologically mediated environment. Three safeguards are particularly important : privacy, personal data protection and freedom of expression. Each safeguard has its own legal foundation, but none of them operates in isolation. Privacy is affected by the collection and publication of personal data ; personal data protection is linked to user consent and platform responsibility ; freedom of expression is conditioned by the rights and reputations of others. A coherent legal framework must therefore treat these rights as mutually connected.

The notion of safeguard must also be distinguished from the notion of control. A safeguard protects the user against arbitrary interference, unlawful exposure or abusive processing of data. A control organizes the conditions under which the user may exercise freedom without harming others or undermining legally protected interests. The two dimensions must remain connected : if controls are adopted without safeguards, regulation becomes repressive ; if safeguards are affirmed without controls, legal protection becomes purely declaratory and ineffective.

1.1. The Right to Privacy

The right to privacy is one of the fundamental rights recognized by international and national legal instruments. Article 12 of the Universal Declaration of Human Rights protects individuals against arbitrary interference with privacy, family, home or correspondence, and against attacks on honour and reputation. Article 17 of the International Covenant on Civil and Political Rights confirms this protection by prohibiting arbitrary or unlawful interference and requiring legal protection against such interference. Regional instruments, including the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the American Convention on Human Rights and the Arab Charter on Human Rights, also establish privacy as an essential component of human dignity.

In the digital environment, privacy takes on renewed significance. Social media platforms encourage users to publish personal information, photographs, opinions, locations, affiliations and relational data. Even when this publication is voluntary, the user does not always understand the technical and legal consequences of disclosure. Content initially shared with a limited audience may be copied, forwarded, archived, indexed, screenshot, reused or transferred to another platform. The distinction between private and public communication becomes unstable, particularly when the user has a large network of contacts or does not adequately control privacy settings.

Privacy violations on social media may arise from the conduct of other users, from the policies of platforms or from the practices of public and private actors that collect and analyse digital traces. Insults, defamation, cyberstalking, harassment, unauthorized publication of images, disclosure of intimate information, identity theft and reputational attacks are forms of harm that may occur

through social media. Their digital character does not remove them from the scope of ordinary legal responsibility. On the contrary, the online environment often increases the extent of harm because content can be reproduced rapidly and remain accessible for long periods.

The legal treatment of privacy on social media must therefore combine traditional civil and criminal protections with specific digital safeguards. Existing rules on defamation, insult, invasion of privacy, unauthorized recording, disclosure of secrets and damage to reputation may apply when the legislature does not require a specific technological means. However, general legal provisions are not always sufficient, because platform architecture, algorithmic visibility, data retention and cross-border circulation create forms of exposure that traditional law did not fully anticipate.

A purely contractual or self-regulatory approach is also insufficient. Platforms generally provide privacy settings and terms of service, but users often lack the time, knowledge or bargaining power necessary to understand and control these mechanisms effectively. Moreover, platform operators may have commercial incentives to maximize engagement and data circulation. Legal regulation must therefore require transparency, effective consent, clear user controls, rapid remedies and accountability for failures to act against unlawful content once properly notified.

At the same time, privacy cannot be used to suppress legitimate public-interest speech. The protection of private life must be balanced with freedom of expression, particularly when the information concerns public debate, official conduct or matters of collective importance. The legal challenge is not to make all personal information untouchable, but to distinguish between legitimate disclosure, voluntary public communication and harmful or unlawful intrusion into private life.

The legal protection of privacy must also consider the contextual nature of disclosure. A user may share a photograph within a family group, express a political opinion to a limited circle or publish professional information for networking purposes. These acts do not necessarily imply consent to unlimited circulation. Digital law should therefore avoid the simplistic assumption that once information appears online it is entirely public. A more nuanced approach is required, taking account of audience, purpose, platform settings, reasonable expectations and the subsequent use of the information.

1.2. Protection of Personal Data

Personal data includes any information relating to an identified or identifiable natural person. In the context of social media, such information may include name, age, date of birth, images, videos, contact details, geolocation, political opinions, religious beliefs, professional information, educational status, preferences, browsing behaviour, device identifiers, IP addresses and other digital traces.

The importance of personal data lies in the fact that it allows individuals to be profiled, targeted, evaluated, monitored or manipulated.

The protection of personal data therefore differs from, while remaining connected to, privacy. Privacy concerns the sphere of personal life protected against intrusion. Data protection concerns the rules governing the collection, processing, storage, transfer and use of information about individuals. In social media environments, the two rights often overlap. A photograph posted without consent may violate both privacy and the right to control one's image ; the extraction of user behaviour for profiling may affect both autonomy and informational self-determination.

A sound data-protection framework must be based on a set of principles : lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. Users must be informed about the purposes for which their data are processed, the categories of data concerned, the duration of storage, the recipients of the data, the existence of automated decision-making and the rights available to them. Consent, when used as a legal basis, must be free, specific, informed and unambiguous. It cannot be reduced to a formal click on obscure terms drafted in technical language.

European law has played a major role in strengthening the global vocabulary of data protection. Regulation (EU) 2016/679, known as the General Data Protection Regulation, treats personal data protection as a fundamental right and grants individuals several rights, including access, rectification, erasure, restriction of processing, portability and objection. Article 21 establishes the right to object, including in cases of direct marketing and profiling. Although the Regulation is European, its practical influence extends beyond the European Union because many digital services operate transnationally and may process the data of users located in different jurisdictions.

In Algeria, the legal framework on personal data is structured notably around Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data, as modified and complemented by Law No. 25-11 of 24 July 2025. This framework affirms that the processing of personal data must respect human dignity, private life and public freedoms, and it establishes the role of the competent authority in supervising compliance. For a study devoted to social media, this Algerian legal framework must be placed at the centre of the analysis, especially when the article addresses the national protection of users and the obligations of controllers.

Images constitute one of the most sensitive forms of personal data circulated on social media. The unauthorized publication or transfer of a person's image may violate personality rights and private life. Consent should specify the purpose, scope, duration and medium of publication. In the absence of valid authorization, legal liability may arise under civil rules of fault and, where applicable,

criminal rules protecting private life and reputation. The right to one's image cannot be treated as a mere courtesy ; it is a legal expression of personal autonomy and dignity.

Personal data is also exposed to cybersecurity threats. Malware, phishing, unauthorized access, ransomware, account hijacking and data breaches may compromise confidentiality, integrity and availability. Cybersecurity is therefore not an external technical issue ; it is an essential condition for the effective protection of personal data. Legal regulation must require appropriate security measures, breach notification mechanisms, accountability of controllers and processors, and cooperation between public authorities, platforms and users.

Nevertheless, data protection should not be reduced to formal compliance. In practice, many websites and platforms provide broad and vague privacy policies, reserve the right to modify processing purposes and use complex interfaces that make refusal difficult. Effective protection requires readable information, privacy by design, privacy by default, independent supervision and accessible remedies. Without these guarantees, the user's formal consent may conceal a situation of practical dependence and informational asymmetry.

A further difficulty concerns the relationship between personal data protection and algorithmic profiling. Social media platforms do not merely store information provided by the user ; they infer preferences, habits, ideological orientations, vulnerabilities and behavioural patterns. These inferences may be used for advertising, recommendation, content ranking or political targeting. Consequently, the protection of data should include not only the data voluntarily declared by the user, but also inferred data and behavioural profiles generated through platform analytics.

1.3. Freedom of Expression

Freedom of expression is a foundational right in democratic societies and a central condition of public debate. Article 19 of the Universal Declaration of Human Rights protects the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Article 19 of the International Covenant on Civil and Political Rights reinforces this protection and expressly recognizes that expression may take place through different media. This wording is broad enough to include the internet and social media networks.

The digital environment has expanded the practical reach of freedom of expression. Social media allows individuals to react immediately to public events, circulate information, criticize authorities, defend causes, produce cultural content and participate in transnational debates. It can give visibility to groups that are underrepresented in traditional media and can contribute to pluralism. These democratic functions explain why restrictions on online expression must be examined with particular care.

However, freedom of expression does not mean freedom from all legal responsibility. International law permits restrictions when they are provided by law and necessary for respect of the rights or reputations of others, or for the protection of national security, public order, public health or morals. The Human Rights Committee has emphasized that restrictions must not jeopardize the right itself. They must be precise, necessary and proportionate. Vague prohibitions, excessive sanctions or broad administrative discretion may transform legitimate regulation into censorship.

On social media, the main difficulty lies in the interaction between user responsibility and platform responsibility. A user may be liable for unlawful content, such as defamation, harassment, threats, incitement to violence, violation of privacy or unauthorized disclosure of protected data. Platforms, for their part, may become responsible when they fail to implement adequate notice, moderation, transparency or removal mechanisms, especially after receiving legally valid notification of manifestly unlawful content. The responsibility of platforms should be graduated and proportionate : they should not be required to monitor all speech in a manner that suppresses legitimate expression, but they must not ignore harmful or illegal content when the law requires action.

Recent regulatory developments, especially in the European Union, reflect this search for balance. The Digital Services Act establishes due-diligence obligations for intermediary services and online platforms, including transparency, complaint mechanisms and measures against illegal content. While it is not directly a universal model, it shows that contemporary platform regulation increasingly combines user rights, procedural safeguards, transparency obligations and institutional oversight. Such developments are relevant for comparative reflection because social media platforms operate across borders and influence regulatory debates beyond the European Union.

Freedom of expression on social media must therefore be protected against two risks : private abuse and public overreach. Private abuse occurs when digital tools are used to destroy reputation, harass individuals, expose intimate data or manipulate information. Public overreach occurs when states invoke broad concepts such as public order, morality or national security to restrict criticism or dissent. A rights-based legal framework must address both risks simultaneously.

The quality of online public debate also depends on procedural guarantees. When content is removed, accounts are suspended or visibility is reduced, users should be informed of the reasons and have access to an effective appeal mechanism. This does not mean that platforms must tolerate unlawful content, but that moderation decisions must be explainable, contestable and consistent. Freedom of expression in the digital space is therefore not limited to the right to publish ; it also includes the right not to be subjected to arbitrary or opaque restrictions by either public authorities or private platforms.

2. Legal Controls for the Use of Social Media in the Digital Space

Legal controls are not the negation of freedom ; they are the conditions under which freedom can coexist with the rights of others and with the requirements of social life. In the digital space, the absence of control may expose users to harm, while excessive control may suppress legitimate expression. The question is therefore one of legal balance. Controls must be precise enough to prevent abuse, flexible enough to respond to technological change and constrained enough to protect fundamental rights.

Three types of controls are particularly important : respect for the law and the principle of legality, respect for public order and public morality, and respect for the rights, freedoms and religious sentiments of others. These categories are often invoked in national and international legal instruments. Yet they must be interpreted carefully, because their breadth can lead to disproportionate restrictions if not accompanied by safeguards.

The legal response must therefore operate at several levels. First, it must define the responsibilities of users who publish content. Second, it must determine the obligations of platforms that host, rank or recommend that content. Third, it must delimit the powers of public authorities that order removal, blocking, investigation or prosecution. Fourth, it must provide independent review so that the protection of public interests does not become a pretext for disproportionate interference with rights.

2.1. The Legal Obligation to Respect the Law

The digital space is not a legal vacuum. The fact that communication takes place through a platform, a profile or a pseudonymous account does not remove it from the scope of law. Social media users are subject to rules concerning defamation, insult, threats, harassment, privacy, intellectual property, personal data, hate speech, fraud, public security and other legal fields. The same principle applies to platforms, which must comply with applicable obligations concerning hosting, data processing, transparency, moderation and cooperation with competent authorities.

The principle of legality is the first guarantee against arbitrary restriction. A limitation on freedom of expression must be clearly established by law. The law must be accessible, foreseeable and formulated with sufficient precision to allow individuals to regulate their conduct. If a rule is vague, unpredictable or excessively broad, it may produce self-censorship and arbitrary enforcement. This requirement is particularly important online, where users may be exposed to criminal, administrative or civil liability for rapid and informal acts of communication.

Article 19(3) of the International Covenant on Civil and Political Rights provides a useful analytical framework. Restrictions must be provided by law and must pursue one of the recognized legitimate aims, such as respect for the rights or reputations of others, national security, public order, public health or morals. They must also be necessary and proportionate. Necessity requires that the restriction respond to a pressing need ; proportionality requires that the measure be appropriate and not excessive in relation to the aim pursued.

This framework applies to social media because international instruments protect expression through any media and regardless of frontiers. Online speech does not receive less protection simply because it is digital. At the same time, its digital character may justify specific regulatory measures when the speed, scale or persistence of content creates particular risks. For example, mechanisms for reporting unlawful content, judicial orders for removal, data-protection obligations and cybersecurity duties may be legitimate when they are based on clear law and accompanied by procedural safeguards.

The adaptation of traditional legal principles to social media must avoid mechanical transposition. A newspaper, a private message, a viral post and an algorithmically recommended video do not have the same conditions of circulation. The law must therefore account for the role of platform design, amplification, visibility and data processing. The responsibility of the user who produces content is not identical to the responsibility of the platform that organizes its circulation. A refined legal analysis must distinguish between author, publisher, host, intermediary and algorithmic amplifier.

Legal certainty is particularly important for journalists, researchers, activists, students and ordinary users who rely on social media to participate in public discussion. If users cannot foresee the legal consequences of a post, they may refrain from legitimate expression. Conversely, if unlawful behaviour is not clearly identified, victims may be left without protection. A balanced statute must therefore be precise enough to guide users and broad enough to cover technological developments without producing arbitrary interpretation.

2.2. Respect for Public Order and Public Morality

Public order and public morality are traditional grounds for limiting certain freedoms. They refer to the basic conditions that allow social life, public security, institutional stability and collective values to be preserved. In many legal systems, public order includes the prevention of violence, disorder, serious crime and threats to essential social interests. Public morality is more difficult to define because it is connected to ethical, cultural and sometimes religious values that vary across societies and historical periods.

In relation to social media, public order may justify measures against content that incites violence, organizes criminal activity, threatens public security, spreads dangerous instructions in contexts of imminent harm or contributes to

serious disorder. It may also justify certain obligations imposed on platforms, such as cooperation with judicial authorities or mechanisms for rapid response to manifestly illegal content. However, the invocation of public order must remain controlled. It cannot become a general formula used to suppress criticism, satire, political opposition or unpopular opinions.

Public morality presents an even greater risk of vague application. Because moral standards differ among societies, legal restrictions based on morality must be carefully formulated and interpreted in light of human rights. International law does not allow morality to be invoked in an unlimited manner. Restrictions must still satisfy legality, necessity and proportionality. They must not be discriminatory, and they must not destroy the essence of freedom of expression.

The digital environment intensifies these questions because content circulates across borders and may be received by audiences with different legal, cultural and religious standards. A publication that is acceptable in one society may be considered offensive in another. This does not mean that every offense must be prohibited. Democratic societies must tolerate disagreement, criticism and even shocking or disturbing expression. The law should intervene when expression causes legally recognized harm, such as incitement to discrimination, hostility or violence, serious defamation, harassment or violation of privacy.

A balanced approach to public order and morality therefore requires precision. Legislators should define the protected interests, courts should apply proportionality, administrative authorities should be subject to judicial control, and users should have access to remedies. Platforms should also be transparent when removing or limiting content on the basis of legal or policy grounds. Without transparency, moderation may become arbitrary ; without moderation, digital harm may become widespread.

Public order must also be understood in a rights-compatible manner. In a constitutional state, public order is not the silence of disagreement ; it is the legal condition that allows disagreements to be expressed without violence and without destruction of the rights of others. A conception of public order that suppresses pluralism would contradict the very foundations of democratic legality. The regulation of social media must therefore protect the public sphere rather than reduce it to a space of compliance.

2.3. Respect for the Rights, Freedoms and Religious Sentiments of Others

The exercise of freedom on social media must respect the rights and freedoms of others. This principle is central to international human rights law and applies with particular force in the digital environment. The rights most often affected by social media use include privacy, reputation, image, dignity, equality, intellectual property and personal security. The fact that a platform enables rapid publication does not authorize users to violate these rights.

Defamation, insult, harassment, cyberstalking, threats, doxing, unauthorized disclosure of intimate information and manipulation of images are examples of conduct that may require legal response. The protection of reputation is not contrary to freedom of expression ; it is one of the legitimate aims recognized by international law. However, the protection of reputation must not be used to shield public authorities or public figures from legitimate criticism. The distinction between private individuals, public figures and matters of public interest remains essential.

Religious sentiments constitute a sensitive legal issue. Religion is a central dimension of personal and collective identity for many societies. International instruments protect freedom of thought, conscience and religion, including the right to adopt a religion or belief and the right to manifest it, subject to lawful and necessary limitations. Individuals and groups must be protected against discrimination, hostility and violence on the basis of religion or belief. Online incitement to hatred, threats against religious communities or calls for violence must therefore be addressed by law.

At the same time, legal protection of religion must not be confused with the prohibition of all criticism, debate, academic analysis, artistic representation or satire. The law should protect persons and communities from hatred and violence, not place ideas beyond discussion. This distinction is essential if regulation is to remain compatible with freedom of expression. The protection of religious sentiments must therefore be formulated in terms of human dignity, non-discrimination and public peace, rather than as an open-ended power to suppress critical speech.

Social media governance should encourage responsible expression without imposing uniformity. Educational measures, digital literacy, counter-speech, moderation policies, judicial remedies and platform transparency may all contribute to a healthier public sphere. Family, community and institutional awareness can play a role, but governmental regulation must remain bounded by law and judicial oversight. The objective is not to produce a controlled digital space, but a lawful and responsible one.

This distinction is also important in multicultural and multilingual societies. Social media can intensify religious or cultural tensions because messages are detached from their context and circulated to heterogeneous audiences. Legal protection should therefore be accompanied by educational and dialogical mechanisms. Counter-speech, mediation, public explanation and digital citizenship may sometimes be more appropriate than criminalization, particularly when the content is offensive but does not amount to incitement, threat or unlawful discrimination.

Conclusion

Social media networks have become indispensable instruments of contemporary communication. They allow users to build relationships, express opinions, exchange information, participate in public debate, share cultural content and organize collective action. Their importance explains why they must be protected as spaces of freedom. Yet their risks also explain why they cannot be left without legal safeguards and regulatory controls.

The analysis has shown that privacy, personal data protection and freedom of expression are the central safeguards governing the use of social media in the digital space. Privacy protects individuals against arbitrary or unlawful intrusion. Personal data protection gives users control over information that identifies, profiles or exposes them. Freedom of expression guarantees participation in public debate and the circulation of information through any media. These rights are interconnected and must be interpreted together.

The analysis has also shown that legal controls are legitimate only when they satisfy the requirements of legality, legitimate aim, necessity and proportionality. Respect for the law, public order, public morality and the rights of others may justify restrictions, but only within a framework that prevents arbitrariness. Vague concepts must not be used to suppress dissent or critical debate. Platform responsibility must be strengthened without imposing generalized surveillance or excessive content removal.

The main finding of this study is that social media regulation must be neither libertarian nor authoritarian. It must be rights-based, transparent, technologically informed and institutionally accountable. The protection of users depends on the combined responsibility of individuals, platforms, regulators and courts. Users must understand privacy settings and digital risks ; platforms must adopt transparent and effective mechanisms ; legislators must produce precise laws ; courts must ensure proportionality ; and public authorities must protect both security and freedom.

Several recommendations follow from this analysis. First, national legal frameworks should clearly define unlawful online conduct while preserving the legitimate exercise of freedom of expression. Second, data-protection law should be effectively implemented through independent supervision and accessible remedies. Third, platforms should be required to provide clear privacy controls, transparent moderation and effective complaint mechanisms. Fourth, digital literacy should be strengthened so that users understand the legal and technical consequences of online publication. Fifth, international and regional cooperation should be encouraged because social media platforms and cyber risks operate across borders. Finally, academic research should continue to examine the relationship between law, technology and fundamental rights, particularly

in societies where digital transformation is rapidly changing the forms of public communication.

In this perspective, the legal governance of social media is not simply a matter of prohibition or permission. It is an effort to preserve the conditions of a digital public sphere in which freedom remains meaningful, privacy remains protected and responsibility remains legally grounded.

Ultimately, the central legal issue is institutional trust. Users will accept regulation more readily when rules are clear, authorities are accountable, platforms are transparent and remedies are effective. Conversely, unclear laws, opaque moderation and selective enforcement undermine both freedom and security. The legitimacy of social media regulation therefore depends not only on the content of legal norms, but also on the procedures through which they are applied.

Key Findings

- Social media networks are legally significant spaces because they combine private communication, public expression, commercial data processing and platform-mediated visibility.
- Freedom of expression applies to digital media, but its restrictions must remain grounded in legality, legitimate aim, necessity and proportionality.
- Privacy protection is weakened by the architecture of platforms, the size of user networks and the technical possibility of copying, forwarding and archiving content.
- Personal data protection requires more than formal consent ; it requires transparency, purpose limitation, security, accountability and effective remedies.
- Platform responsibility must be developed without imposing generalized surveillance or creating incentives for excessive removal of lawful content.
- Public order, morality and religious sentiments may justify legal controls only when they are precisely defined and applied under judicial or procedural safeguards.

Recommendations

- Adopt clear national provisions on unlawful online conduct while protecting legitimate expression and public-interest criticism.
- Strengthen the implementation of personal data protection law, including independent supervision and accessible complaint mechanisms.
- Require platforms to provide transparent moderation, effective notification mechanisms, appeal procedures and readable privacy settings.
- Promote digital literacy among users, particularly regarding privacy settings, image rights, data sharing and legal responsibility for online publication.

- Encourage cooperation between data-protection authorities, cybersecurity institutions, judicial bodies and academic researchers.
- Develop comparative research on social media regulation in the Maghreb, the Arab world, Europe and international human rights law.

Bibliography

- Al-Hajjar, W. S. (2017). *Social media legal system*. Arab Center for Legal and Judicial Research, League of Arab States.
- Algerian Constitution. (2020). *Constitution of the People's Democratic Republic of Algeria*.
- Arab League. (2004). *Arab Charter on Human Rights*.
- Ayad, M., & Lahmar, N. (2022). *Legal and ethical controls of electronic publishing in the digital environment*. *Journal of Media and Society*, 6(1), 101–118.
- Ben Aichouche, O. (2019). *Islamic and legal controls for the use of social networking sites*. *The Voice of the Law Journal*, 6(2), 445–467.
- Boudjefdjouf, Z. (2024). *Social media as a public space for expressing opinions*. *Al Moufaker Journal*, 19(2), 55–72.
- Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*.
- Dawla, Y. (2013). *Criminal protection from moral crimes through media and communication in light of Islamic criminal jurisprudence and positive criminal law* [Master's thesis, Emir Abdelkader University of Islamic Sciences].
- Derieux, E., & Granchet, A. (2013). *Réseaux sociaux en ligne : Aspects juridiques et déontologiques*. Lamy.
- Dliouah, M. (2013). *Public order as a restriction on freedom of opinion and expression*. *Al-Mieyar Journal*, 4(8), 183–198.
- El Mihoub, N., & Terbah, M. (2024). *Freedom of expression through social networking sites and its repercussions on users*. *Journal of Legal and Economic Research*, 7(1), 115–130.
- El-Najjar, S. A. M. M. (2019). *Freedom of expression in the age of information technology in light of the rules of international law*. *Journal of Jurisprudential and Legal Research*, 31(34), 899–925.
- European Court of Human Rights. (2009, July 23). *Hachette Filipacchi Associés (Ici Paris) v. France* (No. 12268/03).
- European Union. (2000). *Charter of Fundamental Rights of the European Union*.
- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*.
- European Union. (2022). *Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)*.

- Florimond, G. (2016). *Law and the internet: From internationalist logic to realistic logic*. Mare & Martin.
- Guettaf, S., & Bougrine, A. (2023). *Objective legal mechanisms to combat cybercrime under the Budapest Convention and Algerian legislation*. *Governance and Economic Law*, 3(2), 80–98.
- Human Rights Committee. (2011). *General comment No. 34: Article 19: Freedoms of opinion and expression*(CCPR/C/GC/34). United Nations.
- Khelaifia, H. (2023). *Circulating personal data on social media: Risks and legal protection*. *Academic Journal of Legal Research*, 14(1), 287–305.
- La Rue, F. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/23/40). United Nations.
- Miloudi, Z. (2016). *Freedom of expression and the requirements of public security in exceptional circumstances*. *El-Hakika Journal for Social and Human Sciences*, 15(4), 82–101.
- Ordinance No. 66-156 of June 8, 1966. *Concerning the Penal Code, as amended and supplemented*.
- Ordinance No. 75-58 of September 26, 1975. *Concerning the Civil Code, as amended and supplemented*.
- Paillier, L. (2012). *Social networks on the internet and the right to privacy*. Larcier.
- Polymenopoulou, E. (2011). *Freedom of art in the face of the protection of religious beliefs* [Doctoral dissertation, University of Grenoble].
- Qarah, I., & Ben Abdelkader, Z. (2018). *Guarantees and controls for the exercise of the right to freedom of opinion and expression: Analytical study in international human rights law*. *Charia and Economics Journal*, 7(2), 137–158.
- Ramal, S. A. (2017). *The right to privacy in the digital age*. Al-Halabi Legal Publications.
- Republic of Algeria. (2018). *Law No. 18-07 of June 10, 2018, on the protection of natural persons in the processing of personal data*.
- Republic of Algeria. (2025). *Law No. 25-11 of July 24, 2025, modifying and supplementing Law No. 18-07 on the protection of natural persons in the processing of personal data*.
- Rouabeh, S. (2021–2022). *Public order as a restriction on freedom of opinion and expression between international human rights law and Algerian legislation* [Doctoral dissertation, University of Ouargla].
- Spinelli, C. F. (2010). *Social media: No friend of personal privacy*. *The Elon Journal of Undergraduate Research in Communications*, 1(2), 64–69.
- United Nations General Assembly. (1948). *Universal Declaration of Human Rights*.
- United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*.