

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

**Cyber Risks in Algerian Society: A Sociological Analysis of the Transformations
of Social Action in Digital Space.**

Akhal nafissa*

Ziane Achour University of Djelfa (Algeria), nafissa.akhal@univ-djelfa.dz

Date of send: 01 / 06 / 2026	date of acceptance: 01 / 07 /2026	Date of Publication: 01/09/2026
------------------------------	-----------------------------------	---------------------------------

***Corresponding author**

Abstract :

This article examines cyber risks in Algerian society through a sociological approach that seeks to analyze the transformations of social action within digital space. With the growing reliance on modern technologies and the widespread use of social media platforms, various cyber risks have emerged, including privacy violations, misinformation, and cyber extortion, as reflections of profound social and cultural transformations. The article is based on a theoretical analysis of the concepts of risk, digital deviance, and social control, highlighting that these threats are no longer merely technical issues but have become complex social phenomena that require a sociological understanding capable of addressing the challenges of the digital society. Furthermore, the article explores the role played by institutions and society in confronting these risks, while raising critical questions related to digital awareness and social culture within a rapidly evolving and constantly changing digital environment.

Keywords: Digital Society ; Digital Deviance ; Social Action ;Social Control; Digital Culture; Algerian Society.

Introduction:

In recent years Algerian society has undergone profound social and cultural transformations driven by the rapid development of digital technologies and the widespread expansion of the Internet and social media platforms. Digital space has become a central arena for social interaction, where online activities increasingly constitute an essential part of both individual and institutional life. This transformation has generated a range of cyber risks that extend beyond their purely technical dimension to become social phenomena influencing behaviors, patterns of interaction, and forms of social action.

The significance of studying these risks lies in their reflection of society's ongoing transition toward digitalization. Such risks manifest in multiple forms, including privacy violations, cyber extortion, misinformation, and digital breaches, all of which reveal emerging challenges related to social control and collective cultural norms. From a sociological perspective, these cyber risks may be understood as indicators of profound transformations affecting social relations, digital identities, and the mechanisms through which individuals communicate and interact within digital environments.

This article adopts a descriptive and analytical theoretical approach in order to examine the key concepts associated with cyber risks and social action, while highlighting the relationship between digital transformations and social phenomena in Algerian society. Furthermore, the study seeks to provide a comprehensive understanding of digital space as a social phenomenon by focusing on the ways in which cyber risks influence both individual and collective behaviors, as well as the role of digital transformations in reshaping patterns of social interaction.

Research Problem:

The accelerated digital transformations characterizing contemporary societies have generated new forms of social interaction that have profoundly reshaped human relationships within networked environments. These transformations have contributed to the emergence of multiple cyber risks that extend beyond their technical dimension to become complex social and cultural phenomena. In this context, digital space has evolved into a domain for the reproduction of new forms of deviance, surveillance, and symbolic domination, reflecting the profound transformations affecting the structure of social action in the digital society.

In the Algerian context, the widespread expansion of the Internet and social media platforms has coincided with a relative weakness in digital awareness and socio-cultural regulation, contributing to the spread of deviant digital practices such as cyber extortion, misinformation, cyberbullying, and privacy violations.

These phenomena reveal significant transformations in mechanisms of social control and patterns of interaction within digital space, particularly with the increasing role of algorithms and digital platforms as emerging actors in the production of power and social norms.

Accordingly, the central research problem of this study can be formulated as follows:

To what extent do cyber risks reflect the transformations affecting social action and mechanisms of social control within digital space in Algerian society?

Conceptual and Analytical Framework:

This section outlines the main concepts underlying the study and links them to the sociological analysis of digital transformations in Algerian society. It focuses on the concepts of cyber risks, social action, digital deviance, social control, and digital culture in order to provide a theoretical understanding of the relationship between digital technology and contemporary social change.

Cyber Risks:

Cyber risks refer to digital threats affecting individuals and societies within online environments, including cyber extortion, privacy violations, cyberbullying, and misinformation. These risks are not merely technical issues but also social phenomena reflecting transformations in values, behaviors, and patterns of interaction within digital society¹.

Social Action:

According to Max Weber, social action refers to behavior oriented toward others and shaped by subjective meaning. In digital contexts, social action extends to virtual interactions, digital identity construction, and participation in online social networks².

Digital Deviance:

Digital deviance refers to behaviors that violate social or legal norms within digital space, such as hacking, online harassment, and the spread of harmful content. It represents a modern form of deviance characterized by anonymity, rapid dissemination, and the influence of networked communication technologies³.

Social Control:

Social control refers to the mechanisms used by society and institutions to regulate behavior and maintain social order. In digital environments, social control includes legal regulation, self-monitoring, technological surveillance, and platform governance⁴.

Digital Culture:

Digital culture refers to the values, practices, and forms of interaction that emerge within digital environments. It includes technological practices, online communication, digital identity management, and participation in social media networks, all of which shape social behavior within contemporary digital society⁵.

Cyber Risks and Social Transformations in Digital Space:

Cyber risks can be understood as social and behavioral threats emerging within digital environments as a result of the interaction between human practices and digital technologies. These risks include privacy violations, cyber extortion, misinformation, and digital harassment. From a sociological perspective, cyber risks are not merely technical issues but social phenomena that reflect transformations in social relations, cultural values, and patterns of interaction within digital society⁶.

The expansion of the Internet and social media platforms has significantly transformed the nature of social action by shifting interaction from physical environments to networked digital spaces characterized by speed, interactivity, and continuous connectivity. According to Max Weber, social action is oriented toward others and shaped by subjective meaning; in digital contexts, this action increasingly takes place through virtual communication, digital identities, and online participation⁷.

Digital environments have also contributed to the emergence of new forms of digital deviance, including cyberbullying, hacking, and the dissemination of misleading content. These practices reveal the weakening of traditional forms of social control and the rise of new mechanisms of algorithmic governance and digital surveillance⁸.

Furthermore digital culture has redefined social interaction, identity formation and symbolic recognition within networked societies. As Pierre Bourdieu suggests, symbolic capital is increasingly reproduced through digital visibility, online influence, and social media presence.

Consequently digital space should be understood not merely as a technological environment, but as a social structure that reshapes identities, behaviors, and forms of social interaction within contemporary society.

Digital Deviance and Social Threats:

1. Digital Deviance as an Extension of Traditional Deviance:

Digital deviance represents one of the most significant social transformations associated with the expansion of cyberspace. Deviant behavior is no longer limited to physical environments but increasingly extends into virtual spaces through practices such as hacking, cyber fraud, digital extortion, and online hate speech. From a sociological perspective, digital deviance can be understood as an extension of traditional deviance, which classical sociology—particularly Émile Durkheim—associated with the violation of social norms and collective values. However, digital deviance differs in that it operates within a virtual environment characterized by anonymity, speed, and weak direct regulation⁹.

Similarly, Howard S. Becker, through labeling theory, argues that deviance is not inherent in an act itself but results from social definitions and reactions. This perspective also applies to digital deviance, whose meanings and boundaries are continuously reshaped by technological, cultural, and legal transformations.

2. Cyber Risks in Individual and Collective Behaviors:

Digital environments have generated new forms of cyber risks that appear in both individual and collective behaviors. At the individual level, these risks include identity theft, cyberbullying, digital addiction, and online extortion. At the collective level, they manifest through organized cybercrime, transnational digital attacks, and the exploitation of online networks for political or extremist purposes¹⁰.

According to Manuel Castells, the network society has created new spaces of social conflict in which power and risk are increasingly exercised through the control and circulation of information within digital networks. Consequently, cyber risks should be understood as complex social phenomena embedded in the political, economic, and cultural structures of digital society.

3. Cyber Risks and Transformations in Social Control:

Cyber risks have profoundly transformed mechanisms of social control, as traditional institutions such as the family, schools, and legal authorities are no longer solely capable of regulating deviant behavior within digital environments.

In this context, Michel Foucault argues that modern forms of power are based on surveillance and discipline. Within digital society, these mechanisms have become more complex through the rise of algorithmic monitoring and platform governance. In addition, digital environments encourage forms of self-regulation, as individuals increasingly adjust their behavior according to norms of online acceptance and fears of exclusion or digital exposure¹¹.

Thus cyber risks reflect a broader crisis in traditional social control and highlight the need for new legal, cultural, and ethical frameworks adapted to digital environments.

4. Cultural and Psychological Impacts of Cyber Risks

Cyber risks extend beyond technical and legal concerns to produce significant cultural and psychological consequences. Culturally, digital threats have reshaped values and social norms by weakening privacy, intensifying fears of surveillance and exposure, and expanding forms of symbolic violence within online platforms.

Psychologically, cyber risks are associated with increasing levels of anxiety, depression, and feelings of digital insecurity, particularly among youth and adolescents. Sherry Turkle argues that digital technologies, despite facilitating communication, may simultaneously generate social isolation, as individuals become "constantly connected yet emotionally alone"¹².

Moreover digital societies have contributed to new forms of psychological distress linked to cyberbullying, online harassment, and the loss of control over digital identity.

Sociological Analysis of Cyber Risks:

Cyber risks should be understood not merely as technical or legal issues, but as social phenomena closely linked to digital culture, social behavior, and transformations in contemporary society. From a sociological perspective, cyber risks represent new forms of digital deviance emerging within virtual environments characterized by anonymity, rapid interaction, and weak direct

regulation. Émile Durkheim argues that deviance reflects broader social transformations and changes in collective norms, while Howard S. Becker explains that deviance is socially constructed through cultural and institutional definitions¹³.

Cyber risks have also transformed mechanisms of social control. According to Michel Foucault, modern societies increasingly rely on surveillance and disciplinary systems, which in digital contexts operate through algorithms, platform governance, and technological monitoring. At the same time, digital culture has reshaped values, communication patterns, and symbolic interactions within networked societies.

Addressing cyber risks therefore requires more than technical security measures. Institutions such as families, schools, and state agencies must contribute to the development of digital awareness and responsible online behavior. Anthony Giddens emphasizes that modern institutions continuously adapt to technological and social transformations, while Manuel Castells argues that power within the network society is increasingly distributed through digital networks rather than traditional institutions alone¹⁴.

Furthermore, cyber risks can be interpreted as a product of broader digital and social transformations associated with globalization and technological change. Ulrich Beck describes contemporary society as a “risk society” shaped by new technological threats, whereas Pierre Bourdieu highlights how inequalities and symbolic power are reproduced within digital environments through unequal access to information and technological resources.

Digital Space and the Social Future:

1. Future Challenges of Digital Society in Algeria:

Algerian society, like many contemporary societies, is experiencing a rapid expansion in the use of the Internet and social media platforms, making digital space a central component of everyday life. However, this transformation raises complex social, cultural, and security challenges that extend beyond the technical dimension of digitalization.

One of the most significant challenges is the expansion of digital deviance and cybercrime, including cyber fraud, online extortion, and attacks on personal data. David Wall argues that crime in the digital age has evolved into a new structural form that requires reconsideration of traditional mechanisms of regulation and control. In addition, Algeria faces challenges related to limited digital awareness and the gap between technological development and socio-legal regulation, making society more vulnerable to unsafe digital practices¹⁵.

According to Manuel Castells, contemporary societies increasingly operate within a “network society” in which power, conflict, and risk are shaped through the

control of information flows. This transformation highlights the importance of integrating sociological perspectives into future digital policies in Algeria.

2. Strengthening Digital Culture and Risk Awareness:

Promoting digital culture represents a fundamental strategy for addressing cyber risks. Developing cybersecurity infrastructures alone is insufficient without building social and cultural awareness capable of preventing digital deviance and unsafe online behavior.

Digital culture involves values and norms related to responsible technological use, including privacy protection, awareness of cybercrime, and ethical online interaction. Henry Jenkins emphasizes that participatory digital culture creates new opportunities for interaction while simultaneously generating new forms of vulnerability in the absence of digital education¹⁶.

Traditional institutions such as families and schools therefore play a crucial role in promoting safe Internet use, particularly among youth who are the most exposed to digital risks. Anthony Giddens argues that modern institutions continuously transform their functions in response to technological and global changes.

3. Future Sociological Perspectives on Cyber Risks:

Cyber risks open important avenues for future sociological research, as they increasingly shape social action within digital society. Ulrich Beck describes contemporary society as a “risk society” characterized by technologically produced threats that transcend national boundaries, a framework highly relevant to cyber risks.

At the same time, digital environments reshape social interaction through surveillance, algorithmic regulation, and new forms of social control. Michel Foucault explains that modern power increasingly operates through systems of monitoring and discipline, dynamics that are highly visible in digital environments¹⁷.

Similarly, Pierre Bourdieu highlights how social inequalities and symbolic domination are reproduced through unequal access to technological and informational resources. Consequently, cyber risks constitute a critical field for analyzing future social transformations in Algeria, particularly in relation to deviance, digital culture, and mechanisms of social control.

Recommendations:

Based on the sociological analysis of cyber risks in Algerian society, the study proposes the following recommendations:

1. **Strengthening Digital Culture and Risk Awareness**

- ✚ Integrating digital education into school and university curricula in order to raise awareness of cyber risks and preventive strategies.
- ✚ Launching continuous media and awareness campaigns targeting families, youth, and civil society to encourage safe and responsible Internet use.

2. **Developing Mechanisms of Digital Social Control**

- ✚ Reinforcing the role of official institutions, including cybersecurity agencies and cybercrime units, in protecting society from digital deviance and cybercrime.
- ✚ Encouraging local communities and youth organizations to participate in promoting collective digital responsibility and self-regulation within online environments.

3. **Enhancing Digital Responsibility and Regulation**

- ✚ Encouraging digital platforms to improve monitoring systems aimed at reducing harmful content, misinformation, and online abuse while respecting freedom of expression.
- ✚ Promoting individual responsibility among users to limit participation in harmful or deviant online behaviors.

4. **Supporting Scientific Research and Field Studies**

Encouraging universities and research centers to conduct interdisciplinary studies on cyber risks, digital deviance, and the impact of digital technologies on social interaction.

Establishing national databases for monitoring cybercrime and digital threats in order to support evidence-based policymaking.

5. **Integrating Psychological and Social Dimensions**

- ✚ Providing psychological and social support programs for victims of cyberbullying, online harassment, and digital extortion.
- ✚ Prioritizing preventive educational approaches over purely punitive measures in digital governance strategies.

6. Promoting Technological Innovation and Cybersecurity

- ✚ Developing advanced national cybersecurity technologies and digital protection systems to secure personal and institutional data.
- ✚ Investing in artificial intelligence and algorithmic systems capable of detecting harmful digital behaviors at early stages.

7. Strengthening Regional and International Cooperation

- ✚ Expanding cooperation with international organizations specialized in cybersecurity in order to exchange expertise and best practices.
- ✚ Supporting regional agreements and collaborative strategies to combat transnational cybercrime and enhance digital security.

Conclusion:

Cyber risks in Algerian society can no longer be understood merely as technical threats or isolated individual acts; rather, they have evolved into complex social phenomena reflecting profound transformations in the structure of social action within digital environments. The widespread expansion of the Internet and social media platforms has reshaped patterns of social interaction, generated new forms of virtual relationships, and contributed to the construction of multidimensional digital identities. Consequently, digital deviance has emerged as one of the most significant manifestations of social and cultural transformations in contemporary society.

From a sociological perspective, cyber risks reveal important changes in traditional mechanisms of social control. Institutions such as the family, schools, and formal authorities are no longer solely capable of regulating behavior within digital environments. Instead, digital space has introduced new forms of surveillance and regulation operating through platforms, algorithms, and technologically mediated systems of monitoring. At the same time, individuals increasingly engage in forms of self-regulation shaped by fears of digital exposure, online exclusion, or symbolic loss of social recognition.

Moreover, cyber risks reflect broader processes of power redistribution and symbolic domination within digital society. Technological power increasingly belongs to actors capable of controlling information flows, digital communication, and technological resources, thereby creating new inequalities between digitally empowered groups and those lacking digital access or literacy. This transformation highlights the complexity of digital space as a social field in which economic, political, and cultural dimensions intersect and continuously interact.

The study also demonstrates that digital culture and social awareness constitute essential factors in reducing cyber risks and promoting safer digital practices. The absence of digital education and critical awareness contributes to the spread of digital deviance, whereas strengthening digital literacy enhances society's capacity to confront online threats and foster a more secure and socially balanced digital environment.

In conclusion, cyber risks in Algeria represent a direct outcome of intertwined digital and social transformations. They are not simply consequences of technological progress, but also manifestations of changing social values, norms, identities, and forms of interaction within contemporary digital society.

Understanding these phenomena therefore requires a comprehensive sociological approach that combines the analysis of digital deviance, digital culture, and mechanisms of social control with the examination of their practical impact on social action. Like other contemporary societies, Algerian digital society exists within a dynamic and continuously evolving environment that requires flexible analytical approaches capable of interpreting ongoing transformations in digital space and their implications for social and cultural life.

Bibliography List :

- ¹ Hijazi Abdel Fattah Bayoumi. *Cybercrime and Information Protection*. Dar Al-Fikr Al-Jami'i, 2018, p. 73.
- ² Giddens, Anthony. *Sociology*. Translated by Fayez Al-Sayyagh, Arab Organization for Translation, 2005, p. 121.
- ³ Al-Badayneh, Diyab Mousa. *Digital Sociology*. Dar Al-Yazouri Scientific Publishing and Distribution, 2018, pp. 141.
- ⁴ Abdel Hamid, Mohamed. *Media Theories and Trends of Influence in the Digital Age*. Alam Al-Kotob, 2021, pp. 83
- ⁵ Ali, Nabil. *Arab Culture and the Age of Information*. National Council for Culture, Arts and Letters, 2019, p. 121.
- ⁶ Abdel Hamid, Mohamed. *Media Theories and Trends of Influence in the Digital Age*. Alam Al-Kotob, 2021, p. 83
- ⁷ Qasim, Hussein Saleh. *Cyberbullying and Digital Deviance among Youth*. Dar Al-Ayyam for Publishing and Distribution, 2023, p. 66.
- ⁸ Barah Samir. "Cyber Security in Algeria: Policies and Institutions." *The Algerian Journal of Human Security*, vol. 4, no. 31, 2017, p. 255.
- ⁹ Durkheim, Émile. *The Rules of Sociological Method*. Translated by Mahmoud Qasim, Egyptian General Book Organization, 2006, p. 83.
- ¹⁰ Castells, Manuel. *The Information Age: Economy, Society, and Culture*. Translated by Faleh Abdul Jabbar, Arab Organization for Translation, 2005, p. 95.
- ¹¹ Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Ali Muqallid, Markaz Al-Inma' Al-Qawmi, 1990, p. 195.
- ¹² Turkle, Sherry. *Life on the Screen: Identity in the Age of the Internet*. Translated by Hossam El-Din Khaddour, Dar Al-Hiwar, 2015, p. 133.
- ¹³ Durkheim, Émile. *The Rules of Sociological Method*. Translated by Mahmoud Qasim, Egyptian General Book Organization, 2006, p. 83.
- ¹⁴ Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Ali Muqallid, Markaz Al-Inma' Al-Qawmi, 1990, p. 195.
- ¹⁵ Al-Saadi, Khaled Abdullah. *Cybersecurity and the Protection of Digital Society*. Dar Al-Khaleej Publishing and Distribution, 2022, p. 55.
- ¹⁶ Ben Yahia, Chaimaa. *The Impact of Cybercrime on Cybersecurity in Algeria*. Master's Thesis, Abdelhafid Boussouf University Center of Mila, 2025, p. 92.
- ¹⁷ Bouriah, Mohamed. "Algerian Public Policies in Cybersecurity: Reality and Challenges." *Algerian Journal of Public Policies*, vol. 2, no. 1, 2023, p. 33.