Digital Transformation and Human Rights Responsibilities: Strategies and Challenges for Multinational Corporations in Developing Countries

Linhua Hao

Southwest University of Political Science & Law, Chongqing, 401120, China

2021021125@stu.swupl.edu.cn

Abstract. While digital transformation promotes global economic development, it also poses new challenges for MNEs in terms of their responsibilities and human rights protection in developing countries. This article focuses on how MNEs should protect the privacy and data rights of users in developing countries in the context of rapid digitalization. The main challenges faced include the digital divide in developing countries, inadequate regulatory systems, lack of awareness among users about privacy protection, pressure on MNEs in terms of legal compliance, social responsibility, and corporate reputation, as well as differences in international and local legal environments. Through analyzing both positive and negative cases, this article proposes several coping strategies: establishing a sound internal governance mechanism, utilizing technological innovations to enhance user privacy protection, and building bridges of cooperation among multiple stakeholders. These measures will help MNEs better fulfill their responsibilities for human rights protection during digital transformation, achieving harmonious progress in both digital advancement and human rights protection.

Keywords: MNEs, Human Rights, Digital Transformation, Privacy, Developing Countries.

1 INTRODUCTION

With the rapid development of science and technology, digital transformation has become an irreversible trend worldwide. From the Internet to the Internet of Things, from big data to artificial intelligence, every technological advancement is profoundly changing the way human society produces and lives. As important participants and beneficiaries of this process, developing countries are facing unprecedented opportunities and challenges. How to securely protect users' privacy and data rights in developing countries while multinational enterprises (Henceforth MNEs) are promoting digital transformation has become an urgent issue to be studied and solved. The acceleration of digitalization has not only changed the way people live but also changed the business model of enterprises. MNEs have become an important force [1] driving

A. Bhunia et al. (eds.), *Proceedings of the 2024 2nd International Conference on Finance, Trade and Business Management (FTBM 2024)*, Advances in Economics, Business and Management Research 304,
https://doi.org/10.2991/978-94-6463-546-1_5

global digital transformation by virtue of their advantages in technology, capital, and market. However, while MNEs enjoy the benefits of digitalization, developing countries are often faced with problems such as technology gaps, insufficient infrastructure, and imperfect laws and regulations, which leave users in a weak position in terms of privacy and data rights protection. The actions of MNEs in this context directly impact the rights and interests of users in developing countries.

The core issue of this paper is how MNEs protect the privacy and data rights of users in developing countries during digital transformation. Specifically, under the premise that developing countries are host countries, in a practical sense, the digital technology of developing countries is relatively backward, the regulatory system and framework are imperfect [2], and the privacy and information protection awareness of users in developing countries is relatively insufficient. In this context, this paper aims to discuss how to strengthen MNEs' internal management, innovate technology to protect user privacy, and cooperate with the host government to jointly promote the formulation and improvement of laws and policies.

The purpose of this paper is to reveal the impact and responsibility of MNEs in terms of human rights through an in-depth analysis of their strategies and challenges through digital transformation in developing countries. This paper provides practical guidance for MNEs, theoretical support for relevant policy-making, and promotes the balanced development of the global economy. Theoretically, digital transformation and the human rights responsibility of MNEs are two hot topics. Yet, integrating these two, particularly in the context of developing countries, presents a significant research gap. This study aids in understanding the intersection between these areas. In addition, traditional research mainly focuses on the domestic perspective, while research on MNEs is rare. In the context of digital transformation, the operation, supply chain management, data flow and other aspects of MNEs have become more complex, and the understanding and application of human rights responsibility also needs to be updated. Therefore, it is of great theoretical significance to paper the human rights responsibilities of MNES in the process of digital transformation in developing countries, as well as their coping strategies and challenges. Practically, on the one hand, it can provide suggestions for MNEs to balance economic interests and human rights responsibilities [3] in developing countries, and help MNEs protect users' human rights on the premise of realizing business interests. On the other hand, governments in developing countries need to consider how to protect the basic rights of their citizens while attracting foreign investment and promoting digital transformation. This paper can provide suggestions for the specific practice of policy-making so that policy-making can meet the needs of economic development and safeguard human rights.

This paper is structured into five parts. The first part is the introduction, which mainly introduces the research background, research problem, research purpose, and significance, as well as the structure of the paper. The second part analyzes the current situation of the dilemma, starting from three perspectives: the challenges of privacy and data rights, the responsibilities and challenges faced by MNEs, and the differences between international and local laws. The third part will deeply analyze the strategic choices and implementation effects of multinational enterprises in digital transformation in developing countries through case studies and empirical analysis.

The fourth part will put forward targeted strategies and suggestions for existing problems. Finally, based on the research results, this paper puts forward policy suggestions and practical implications to promote MNEs to better fulfill their human rights responsibilities in developing countries.

2 CURRENT DILEMMAS

2.1 Challenges of Privacy Rights and Data Rights

In the context of digital transformation, MNEs face multiple strategic challenges and complex dilemmas when operating in developing countries. Due to the influence of various factors such as technology, economy, and culture in developing countries, the regulatory framework for digital information is inadequate, and users' awareness of privacy protection is relatively weak. Consequently, the risks of data leakage and abuse have increased significantly. When dealing with user data, MNEs must face the complex issue of how to collect, store, and use data in compliance with regulations.

With the in-depth development of globalization and informatization, the issue of the digital divide has gradually become prominent, posing a significant challenge to developing countries and reflecting the vast disparities in digital capabilities both between and within nations [4]. According to the United Nations Conference on Trade and Development's report "Cross-border Data Flows and Development: For Whom the Data Flow, 2021", internet usage in the least developed countries hovers around a mere 20%. These countries also struggle with slow download speeds and high internet access costs, compounding their inability to transform data into digital intelligence. Due to their limited access to digital resources and lack of advanced technology and infrastructure, developing countries often only contribute raw data without the capability for high-value data processing and analysis. This creates a disparity where developing countries provide raw data, and developed countries use this data for innovation, gaining significant economic benefits.

The complexities of modern technologies like big data and cloud computing have made cross-border data flows more intricate and varied, raising the bar for regulatory challenges. Both British Airways and a leading hotel chain have faced heavy fines due to data breaches. British Airways was fined £20 million for a customer data leak caused by a hacker attack, while the hotel chain incurred a €110 million fine due to a long-standing vulnerability in its customer information system that led to the theft of data from 339 million customers. A similar incident involved Facebook, which was investigated by the US Federal Trade Commission for a data leak and reached a $5 billion settlement. These incidents underscore the need for stricter data protection and improved regulation, especially in developing countries where limited resources compromise data security. Inadequate regulations leave data exposed to unauthorized exploitation.

Amidst the era of big data, which brings a wealth of information resources and services, the potential for privacy violations has notably increased. Information leaks can occur unbeknownst to consumers, as illustrated by the example of predictive advertising, which can reveal private information through data mining techniques. Consider

the case of "predicting teenage pregnancy and disclosing it to businesses" published in the New York Times [5]. Despite these advancements, consumer awareness remains low, often leading to passive acceptance of predictive advertisements for the sake of enhanced user experiences [6]. With the endless emergence of technological means in the information age, it is necessary to raise awareness among users to better protect personal privacy information.

2.2 Responsibilities and Challenges Faced by Multinational Corporations

The home country of a multinational corporation is generally a developed country, while the host country is usually a developing country. During the investment process, MNEs need to consider the legal compliance of both their home and host countries. However, typically, there are differences in legal regulations for MNEs between the home and host countries, creating legal compliance challenges for these corporations. When operating in developing countries, MNEs must not only pursue economic benefits but also undertake corresponding social responsibilities. Nevertheless, in practical operations, companies often face the difficult task of balancing economic benefits and social responsibilities. How to meet user needs while ensuring the compliance and ethical standards of corporate behavior has become an unavoidable challenge for MNEs.

Taking China and the United States as examples, we see a dynamic interplay between the world's largest developing market and a major developed economy. China's market, known for its vast potential and rapid growth, is continuously opening up, attracting significant foreign investment. However, when U.S.-based MNEs operate in China, they encounter complex legal challenges. The U.S. may apply sanctions or domestic legal measures affecting these MNEs' operations in China, which in turn might respond with its own counter-policies. Amid such a backdrop, the uncertainty surrounding international trade has increased, affecting the operations of MNEs. Which party's laws should MNEs abide by? How should they navigate legal compliance challenges? These are questions MNEs must face in their compliance journey.

Classical economists, such as Adam Smith, proposed that enterprises should be orientated towards economic efficiency to meet the needs of society through the market. Although they did not explicitly mention social responsibility, this view laid the foundation for corporation social responsibility (CSR), which states that enterprises should provide products and services needed by society through the efficient use of resources. The damages caused by MNEs to human rights and the environment in recent years have attracted the attention of the international community, such as the Shell oil case and the Bhopal case in India. Given MNEs' profit-driven nature, enforcing social responsibility remains challenging. While international law lacks direct mechanisms to mandate CSR, it's crucial for MNEs to voluntarily embrace social responsibilities [7], with sovereign states enhancing regulatory frameworks to support this commitment.

Corporate reputation and trust risk play a crucial role in the field of data compliance. With the rapid development of the digital era, data has become a core asset of business operations. Taking user privacy data as an example, 339 million customers'

information was stolen due to a vulnerability in the customer information system of a hotel chain, which was hacked into the guest booking system and copied and encrypted the information. Upon investigation, the hotel chain group of companies failed to process user information in accordance with the General Data Protection Regulation (GDPR) requirements and was eventually fined 110 million euros. This kind of incident may lead to the loss of user trust, which in turn affects the reputation and market position of enterprises.

2.3 Differences between International and Local Laws

The regulation of the cross-border flow of data [8] involves a number of legal areas, including international trade law, data protection law, cybersecurity law, and so on. The intersection and conflict between these legal fields make the regulation of the cross-border flow of data complex and difficult, and the regulation of the cross-border flow of data also involves differences in the legal systems of different countries and regions. As the legal provisions on data protection, privacy rights, etc. vary across countries and regions, it makes it difficult to form uniform standards and rules in the regulation of the cross-border flow of data. Such differences in legal systems not only increase the legal risks of cross-border data flows but also impede the smooth conduct of international trade.

A poignant illustration of international legal conflicts is the case brought by Austrian citizen Schrems against Facebook Inc. in the United States for data protection [9]. Schrems argued that Facebook failed to adequately protect the privacy of European users' data when transferring it to the United States, violating European data protection laws such as the 1995 EU Data Protection Directive (DPD). Directive (DPD) in 1995 and GDPR in 2018. As a result of the U.S. Foreign Intelligence Surveillance Act 1978 (FISA), U.S. intelligence agencies may have accessed these European user data transfers to the U.S., thereby violating the privacy rights of European citizens. The Court found that U.S. surveillance laws fundamentally clashed with EU data protection standards, leading to the invalidation of the Safe Harbor Agreement. Despite a subsequent EU-US Privacy Shield Agreement in 2016, it was invalidated by the Court of Justice of the European Union (CJEU) in July 2020 [10]. Through this case, it can be observed that the conflicting interests of different countries are reflected in legislation as a conflict of laws, which in turn affects judicial practice. In this context, data compliance of MNEs needs to develop appropriate responses to conflict of laws.

In judicial practice, cases involving transnational corporations will always involve multiple countries at the same time, thus potentially involving different jurisdictions, leading to judicial cooperation and enforcement difficulties. When there are cases of infringement by MNEs, due to the different laws and penalty standards of different countries, this leads to the judicial dilemma of having to face different legal liabilities in different countries on the substantive side, and different standards of collecting and examining evidence on the procedural side, which leads to difficulties in the identification of evidence and inconsistent conflicting judgment results. In terms of enforce-

ment, differences in legal provisions on asset seizure, freezing and confiscation between different countries may make it difficult to enforce judgements in practice.

The challenge of global coherence stems mainly from inconsistencies in human rights laws, differences in cultural values and differences in levels of socio-economic development. The quest for global coherence in human rights standards faces significant hurdles due to the inconsistencies in human rights laws across countries, influenced by each nation's unique historical, legal, and political context. Additionally, cultural values greatly affect the understanding and implementation of human rights, leading to divergent practices in labor, privacy, and freedom of expression. Socio-economic development levels further complicate this landscape, as countries at different stages of development prioritize economic growth, which can sometimes come at the expense of stringent human rights protections. This complex scenario challenges multinational enterprises to adapt their operations to a tapestry of legal systems, cultural norms, and development priorities, making the uniform application of human rights standards a daunting task.

3 REAL-WORLD INSIGHTS: MNES' DATA PRIVACY PRACTICES AND CHALLENGES

MNEs, as major players in global business, are particularly concerned about their practices and challenges in data privacy. Based on the aforementioned real-life dilemmas, the following section will analyze in detail the latest practices of MNEs in data privacy with several real-life cases, explaining the successful experiences and challenging cases of MNEs' data compliance and human rights responsibilities in the context of digital transformation, respectively.

3.1 Exemplary Practices in Data Privacy

Apple has always made user privacy protection one of its core values. According to data published on Apple's official website, the company has taken a number of measures to protect the security and privacy of user data. iCloud is a cloud storage and synchronization service provided by Apple. Apple has taken a number of measures to protect the privacy of user data stored in iCloud. For example, Apple uses end-to-end encryption to protect certain user data (e.g., health data and passwords), even though Apple cannot decrypt such data. In addition, Apple provides security features such as dual identity verification to enhance the security of iCloud accounts. Moreover, Apple's adoption of Differential Privacy [11] technology exemplifies its innovative approach to privacy, ensuring user data remains anonymous and secure. Expanding its focus on privacy to meet regional needs, Apple partnered with Guizhou-Cloud Big Data Group Co., Ltd (Guizhou-Cloud) to establish a data center in Guizhou, China, for iCloud services. This initiative not only meets the Chinese government's requirements for data localization but also helps to improve data security and privacy protection. At the same time, as a local company, Guizhou-Cloud has a

better understanding of the needs and characteristics of the Chinese market and is better able to provide customized services to users.

Similarly, Google, one of the world's largest search engines and advertising platforms, has adjusted its data privacy policy and taken measures to comply with the GDPR and protect the data privacy rights of its European users. Firstly, Google updated its privacy policy to comply with the GDPR and added the option of user data control; secondly, Google strengthened its internal data security management to ensure the security of user data; and lastly, Google is committed to developing new encryption technologies and anonymization methods to further protect the privacy and security of user data. These efforts have enabled Google to achieve significant results in complying with the GDPR and set an example for other MNEs. Google has been an industry leader in technological innovation. For example, Google first proposed a technology called Federated Learning [12], which allows machine learning models to be trained on local devices without having to send user data to a cloud server. This technique not only improves the security of user data but also reduces the cost of data transmission and provides new ideas for the application of machine learning in privacy protection.

3.2 Challenges in Upholding Data Privacy

Facebook (now renamed Meta) is one of the world's largest social media platforms with billions of users. However, in recent years Facebook has suffered major blows to its data privacy. The most notable of these was the Cambridge Analytica data breach in 2018. The incident exposed vulnerabilities in Facebook's data privacy protection, which led to tens of millions of users' personal information being leaked to third-party organizations for inappropriate purposes. Cambridge Analytica collected the personal data of millions of Facebook users through an app called "This is your digital life". The data collection activities were reportedly not authorized by enough users and the data was also used for political campaigning and election influencing without users' consent.

This incident has sparked a widespread privacy controversy. Many Facebook users are angry and upset about the unauthorized collection and misuse of their personal data. They have serious questions about the social media platform's ability to protect user data, and it has sparked a major global debate about the protection of personal privacy. Facebook has been accused of failing to effectively regulate and control Cambridge Analytica's access to and use of user data in this incident. Despite having various data protection policies and security protocols in place, they proved inadequate in preventing the breach. This exposed Facebook's failures in data protection and compliance and raised questions among regulators and the public about its management and oversight capabilities. The incident had profound implications for Facebook's social responsibility, damaging its reputation, causing its share price to tumble, and significantly eroding trust among investors and users. In addition, Facebook faced investigations and penalties from regulators in several countries, and was ultimately forced to pay billions of dollars in fines.

3.3 Summary of Cases

In the digital age, the performance of multinational technology companies in terms of privacy protection is influenced by a number of factors. Successful companies typically view privacy protection as a core value and solidify user trust and loyalty by publicly demonstrating respect for user privacy. Technological innovations such as differential privacy and federated learning enable companies to make efficient use of data while protecting privacy. Close collaboration with partners and quick response to security breaches are also key to success. Conversely, instances of failure in safeguarding privacy often stem from a lackadaisical attitude towards privacy concerns, deficient data management practices, opacity in operations, and a tendency to underestimate the gravity of potential threats. Such lapses not only compromise user privacy but also tarnish the company's reputation.

Drawing lessons from both the successes and failures, MNEs should view privacy and data protection as the cornerstone of their business operations, not only as a legal requirement but also as the key to winning users' trust. Companies should convey respect for user privacy through clear actions and policies while building user relationships through transparency. Technological innovation should drive the development of corporate privacy protection and the adoption of cutting-edge technologies to balance business interests with social responsibility. Collaboration with stakeholders is also essential to build a solid data protection system. In addition, internal regulatory mechanisms and auditing procedures are important safeguards for self-improvement of privacy protection. In the digital age, MNEs must fully implement these concepts and actions in order to gain an advantage in the field of user privacy protection and to contribute to the long-term development of their businesses and the protection of human rights globally.

4 STRENGTHENING DATA PROTECTION AND COMPLIANCE: STRATEGIES FOR MNEs

4.1 Strengthening Internal Policies and Management: Building a Good Internal Governance Mechanism

In addressing the challenges of human rights responsibilities faced by MNEs in developing countries, the establishment of sound internal governance mechanisms is crucial. Among them, the establishment of a sound data protection regime is a key component. For example, the Law of the People's Republic of China on the Protection of Personal Information requires MNEs to comply with relevant laws and regulations when collecting and using personal information within China, and to establish stringent data handling systems and processes to safeguard the personal data of their employees and users. This not only helps companies to comply with the law, but also helps to enhance their corporate image and reputation and increase their sense of social responsibility in developing countries.

Moreover, it is crucial to enhance employees' awareness of privacy and data protection. MNEs can raise the level of employees' awareness of personal privacy and

data protection by holding trainings, issuing notices and organizing seminars. For example, Google emphasizes the importance of data protection in its employee handbook and provides relevant training and educational resources to help employees better understand and respond to data security issues.

In addition, conducting regular compliance and risk assessments is an important step in ensuring the robustness of a multinational company's internal governance mechanisms. Compliance assessments aim to verify that company behavior is in line with applicable laws, regulations and industry standards, while risk assessments aim to identify potential risks and vulnerabilities and take appropriate measures to address them. When conducting a compliance assessment, a multinational company needs to collect, analyze and interpret relevant laws and regulations, especially those involving personal data protection, to ensure that the company's data processing practices are in line with the regulations. This may involve regulations on cross-border data transfers, data security protection measures, user rights protection, etc., which the company needs to adjust and improve according to the actual situation. In terms of risk assessment, MNEs should adopt a systematic approach, including regular security audits, vulnerability scanning, use of risk assessment tools, etc., in order to identify and assess potential risks and take timely measures to address them.

Furthermore, companies should establish effective internal reporting and response mechanisms to encourage employees to report security breaches and data leakage incidents in a timely manner so that remedial measures can be taken in a timely manner to minimize losses. Through these compliance and risk assessment measures, MNEs can identify and address potential problems in a timely manner, safeguard the rights and interests of their employees and users, effectively respond to the challenges of human rights responsibilities in developing countries, and make greater contributions to sustainable development [13].

4.2 Technological Solutions: Using Technological Innovation to Protect User Privacy

In developing countries, MNEs face important challenges in protecting user privacy and fulfilling their human rights responsibilities. Through technological innovations, such as data encryption, anonymization and other advanced technologies, companies can significantly improve data security and comprehensively protect user privacy, thereby achieving their social responsibility and sustainable development goals.

Data encryption is the cornerstone of user privacy protection. Employing state-of-the-art encryption algorithms like AES-256 or RSA ensures that user data is encrypted end-to-end – from the user's device to the server, throughout its storage and processing. Access to the data is strictly limited to authorized personnel, who can decrypt it with the proper keys, substantially mitigating the risk of data breaches.

To further protect user privacy, data anonymization techniques should be deployed. By obscuring or substituting sensitive information within user data, such as transforming identifiable personal details into anonymized formats, data utility can be preserved while personal privacy exposure is minimized. In addition, a comprehensive user data management system should be established to ensure that the collection,

storage, use and disposal of data comply with relevant laws and regulations and privacy policies.

By combining advanced technologies such as differential privacy and federated learning, MNEs can better protect user privacy. Differential privacy technology effectively protects personal privacy information by introducing controllable noise or perturbation in the data processing process, thus achieving a balance between privacy and data availability in data sharing and analysis in MNEs. In data management in MNEs, differential privacy techniques can be used to protect users' personal data, such as customer account information and user preferences, while ensuring data usability. It is achieved to improve the accuracy of personalized recommendations while protecting user privacy. Similarly, federated learning techniques have an important role in privacy protection for MNEs. For example, a multinational bank can use federated learning technology to collaborate on customer credit assessment and fraud detection to improve the quality and efficiency of financial services while protecting customer privacy. In addition, a multinational e-commerce platform can use federated learning technologies to analyze user behavior and make personalized recommendations without directly accessing users' personal data, thus providing users with a safer and more private shopping experience. These practical applications illustrate the value and advantages of federated learning technologies in privacy protection for MNEs.

4.3 Cooperation and Dialogue: Building a Cooperation Platform for Multiple Stakeholders

To tackle the challenges of human rights responsibilities faced by MNEs in developing countries, it is imperative to build a multi-stakeholder platform for cooperation. The establishment of such a platform not only helps to improve communication and cooperation between businesses and governments, and to facilitate policy formulation and improvement but also promotes the development of international norms and standards, in particular the harmonization of global data protection standards. MNEs often face complex political, social, and legal environments in their operations in developing countries, so it is crucial to establish good cooperation with local governments and policy-making bodies. Through communication and co-operation with governments, MNEs can better understand and comply with local laws and regulations to ensure that their operations are conducted on a legally compliant basis. At the same time, enterprises can also play a more active role in protecting human rights and promoting sustainable development by participating in the formulation and improvement of legal policies.

Beyond cooperation with governments, MNEs should also actively participate in the activities of international organizations and standard-setting bodies to promote the development and improvement of international norms and standards. Particularly in the area of data protection, the issues of data security and privacy protection are becoming increasingly prominent with the development of the digital era. Therefore, MNEs should be committed to promoting the unification of global data protection standards and ensuring that their business complies with uniform standards and norms globally, so as to improve data security and privacy protection. In addition, MNEs

should actively participate in cross-border cooperation and knowledge sharing, discuss best practices with other enterprises and organizations, and jointly address human rights responsibility challenges. Through cooperation with other enterprises, MNEs can learn from their successful experiences, continuously improve their own management and operation methods, and enhance the level of human rights protection.

5 CONCLUSION

Under the wave of globalization, MNEs are actively embracing digital transformation as an important way to enhance their competitiveness, optimize business processes and expand their markets. However, this transformation process is not a straight path, especially in developing countries, and it is often accompanied by a series of complex human rights challenges, including but not limited to the protection of data privacy, the digital divide, and potential human rights abuses brought about by the application of technology. These issues not only test the ethical bottom line and social responsibility of enterprises but also have a direct bearing on the long-term interests of enterprises in global sustainable development.

In the face of these challenges, MNEs cannot and should not shy away from their human rights responsibilities. Enterprises need to strategically recognize that digital transformation and human rights responsibilities are not either/or issues, but two important aspects that must go hand in hand and develop in a coordinated manner. Only by internalizing human rights responsibilities as the core of their corporate culture, and by integrating them throughout the entire process of digital transformation, will they be able to move forward steadily in the face of fierce market competition, and win the widespread recognition and sustained support of all sectors of society.

The road of digital transformation for MNEs in developing countries is still full of challenges, but also pregnant with infinite possibilities and opportunities. By enhancing their awareness of human rights responsibilities, strengthening internal policies, using technological innovation to protect user privacy, building a multi-stakeholder cooperation platform, and actively exploring new modes and paths to combine digital transformation and human rights protection, enterprises can not only inject new vitality into their own development, but also contribute to the sustainable development of the global economy and social progress.

REFERENCES

1. Kalyanpur, Nikhil and Abraham L. Newman. “The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation.” Cybersecurity (2019): n. pag.
2. Zalnieriute, Monika. “From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Example of Internet Governance and ICANN.” SSRN Electronic Journal (2019): n. pag.

3. Wettstein, Florian, Elisa Giuliani, Grazia D. Santangelo and Günter K. Stahl. "International business and human rights: A research agenda." Journal of World Business (2019): n. pag.
4. UNCTAD, DIGITAL ECONOMY REPORT 2021-Cross-border Data Flows and Development: For Whom the Data Flow, 29 September 2021.
5. Duhigg, Charles and Andrew Pole. "How Companies Learn Your Secrets." (2012).
6. Karas, Stan. "Privacy, Identity, Databases." The American University law review 52 (2002): 1.
7. Jamali, Dima and Charlotte M. Karam. "Corporate Social Responsibility in Developing Countries as an Emerging Field of Study." International Strategy & Policy eJournal (2018): n. pag.
8. Sauvant, Karl P.. "Transborder data flows and the developing countries." International Organization 37 (1983): 359 - 371.
9. See Case C - 362/14, Maximillian Schrems v Data Protection Commissioner and Digital Rights Ireland Ltd, ECLI: EU: C: 2015: 650
10. See Case C - 311 /18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI: EU: C: 2020: 559
11. Abadi, Martín, Andy Chu, Ian J. Goodfellow, H. B. McMahan, Ilya Mironov, Kunal Talwar and Li Zhang. "Deep Learning with Differential Privacy." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (2016): n. pag.
12. McMahan, H. B., Eider Moore, Daniel Ramage, Seth Hampson and Blaise Agüera y Arcas. "Communication-Efficient Learning of Deep Networks from Decentralized Data." International Conference on Artificial Intelligence and Statistics (2016).
13. Li, Shaomin, Marc Fetscherin, Ilan Alon, Christoph Lattemann and Kuang S. Yeh. "Corporate Social Responsibility in Emerging Markets." Management International Review 50 (2010): 635-654.