International Journal of Science, Technology and Society
2023; 11(5): 175-184
http://www.sciencepublishinggroup.com/j/ijsts
doi: 110.11648/j.ijsts.20231105.11
ISSN: 2330-7412 (Print); ISSN: 2330-7420 (Online)

Smart Contracts & Personal Data Protection: A Legal Perspective on Potential Issues

María Emiliana Flores

Facultad de Ciencias Sociales y Jurídicas, Universidad Nacional del Litoral, Santa Fe, Argentina

Email address:
mariaemilianaflores@gmail.com

To cite this article:
María Emiliana Flores. Smart Contracts & Personal Data Protection: A Legal Perspective on Potential Issues. *International Journal of Science, Technology and Society*. Vol. 11, No. 5, 2023, pp. 175-184. doi: 10.11648/j.ijsts.20231105.11

Received: July 10, 2023; **Accepted**: August 18, 2023; **Published**: September 27, 2023

Abstract: Blockchain is an innovative technology that allows for a more efficient life for people, through a variety of actions, including enabling trustworthy transactions and reducing operating costs. In relation to Blockchain, Smart Contracts have emerged, revolutionizing the field of contracts. There are great expectations surrounding these technological advances for various sectors such as finance or registration. However, despite the obvious benefits, some obstacles are being identified regarding compliance with regulations on personal data protection in the service of smart contracts, specifically in relation to privacy/confidentiality controls and the right to be forgotten due to the governing principles of Blockchain. Throughout the course of this paper, we will analyze the different facets that arise within the presented issue, as well as explore various global scenarios and the regulations, doctrine, and jurisprudence, both from Argentina and internationally, in order to envision potential solutions to the identified problems**.** It is our duty as legal professionals to delve into the revolutionary and disruptive technologies that are currently emerging, so that they can be used as allies both in the daily lives of citizens and in more complex scenarios. Furthermore, we must anticipate potential problems that may arise regarding their use in order to effectively address them.

Keywords: Smart Contracts, Personal Data Protection, Blockchain

1. Introduction

Traditional contractual law has been characterized by involving a series of formalities that affect the formation and execution of contracts. With the advancement of technology and globalization, the contractual world envisioned by Dalmacio Velez Sarsfield began to undergo significant modifications. In the face of this new underlying reality, new contractual concepts and protections for rights have emerged.

Currently, we are facing a disruptive paradigm in technology. Terms like blockchain, cryptocurrencies, smart contracts, tokens, and NFTs have started to appear in our lives. Like any revolution, we find opposing sides - haters and fans - that have ventured into this new digital world where developers have been at the core.

Thus, a new form of contracting arises: smart contracts. The legal sector cannot remain unaffected by this phenomenon, along with the corresponding new legal challenges it will bring. Given the principles upon which blockchain and the rest of the new paradigms are built, it is worth asking: Are they compatible with our current regulations?

It is important to remember that the law must be constantly updated to adapt, reinterpret, and provide certainty to specific situations, as it ultimately seeks to provide fair solutions to problems arising from historical reality.

That is why it is absolutely necessary for all legal practitioners to take part and maintain their rightful position in the technological future of electronic contracting and smart contracts.

A definition of so-called personal data is necessary. Our legal system establishes that it is "Information of any kind related to individuals or legal entities, determined or determinable." It also defines sensitive data as "Personal data that reveals racial or ethnic origin, political opinions, religious, philosophical, or moral beliefs, trade union membership, and information related to health or sexual life." While it is known that the latter have been treated and protected more extensively, the handling of personal data is where individuals' ability to exercise their fundamental right

to privacy and control over their personal information lies. However, for the purposes of this work, everything developed in connection with personal data can also be considered in its application to sensitive data."

2. Problem Statement, General and Specific Objectives

2.1. Problem Statement

The ongoing technological paradigm shift introduces new concepts such as Blockchain and Smart Contracts, which offer security features to their users, including immutability and transparency.

Currently, there is significant global progress in personal data protection, with various organizations working to safeguard this information, resulting in appropriate regulations. Argentina is in the process of enacting a new personal data protection law, but jurisprudence has aligned with the guidelines established by these global organizations, adopting concepts that are not legislated in our legal system, such as the right to be forgotten.

In this context, as is often the case with a new paradigm, we must question whether these new concepts align with our existing regulations.

2.2. General and Specific Objetives

Regarding the objectives, we have established a general objective followed by specific objectives:

1. To analyze the problems related to Smart Contracts and the protection of personal data, understanding the fundamental aspects of both Blockchain and Smart Contracts, while considering the underlying principles they are based on.
2. To investigate different doctrinal positions and opinions from relevant organizations in order to determine if there is a collision of norms.
3. To assess the present and future impact of this paradigm shift on society and the field of law.
4. To determine the extent of the problem and find an acceptable solution.

2.3. Hypothesis

Due to their immutability and transparency characteristics, Smart Contracts jeopardize privacy control and the corresponding protection of personal data.

3. Current State of the Matter

The technological revolution triggered by internet access since 1993, when the United States lifted the ban on internet usage and ceased government administration of the network, has had a significant impact not only on new technologies but also on commerce, electronic contracting, and electronic payment methods.

Currently, a new technology has emerged that has generated contrasting opinions but has also brought new challenges to be addressed. This technology is called Blockchain, which operates on the "distributed ledger technology" mechanism, constructing a digital database with cryptography. The so-called "blockchain" has two classifications: private (permissioned) and public (permissionless). In the words of important doctrine: "(...) a decentralized record of information stored in the form of transactions grouped into blocks." [1]

It can be concluded that "Blockchain can be defined as a set of technologies that, through the use of cryptographic techniques, establish a distributed network registry of information without the need for validation by a central authority.

It is a peer-to-peer (P2P) digital system that allows verified transactions to take place without intermediaries. Through consensus among participants, the network itself guarantees that the information has not been altered in any way." [2]

Within the algorithms of Blockchain, we find Smart Contracts, a term coined by Nick Szabo. Currently, there is no uniformity regarding their legal status as contracts, with some denying their contractual nature while others recognize them as true contracts. Considering that the purpose of this work is not to determine it, this author adheres to the affirmative stance.

"Smart Contracts are nothing more than algorithms stored on the Blockchain that execute automated decisions. They are programs designed to execute predetermined obligations automatically and without the need for human intervention in many cases." [3]

Through what is called an oracle, a tool agreed upon by the parties beforehand, compliance with the conditions stipulated in the contract is verified, and the obligations are automatically executed through computer code.

Smart Contracts have two inherent characteristics due to their use of Blockchain: immutability and transparency. These characteristics make them secure and reliable, as the risk of manipulation and falsification is low. “For example, in Ethereum, contracts store the executable code of the program, the associated data, and the contract's balance on the Blockchain. Just like users accounts have an address, contracts also have an address and can execute functions or transfer funds. Therefore, it is argued that transactions or operations carried out on the Blockchain are not confidential, as anyone with access to the blockchain can access and view all the information sent and stored in a contract. Although transparency is one of the advantages of this revolutionary technology, it can be a disadvantage in these cases.” [4]

3.1. Issues with Personal Data Protection

The main challenges regarding personal data protection that arise with the emergence of Smart Contracts and require legal responses, in the view of this author, are, on one hand, the concealment of personal identity, and on the other hand, the protection of personal data. Additionally, there is a tension surrounding legislation regarding the Right to be Forgotten. We can note that the first two issues have been

partially addressed through data encryption and accompanied by data protection regulations (such as GDPR in Europe).

Based on GDPR, which we will delve into later, there is a broad debate regarding its possible incompatibilities with the use of Blockchain technology, which extends to Smart Contracts. Among the controversial issues raised are:

Identification of actors: GDPR imposes obligations and responsibilities on the various actors involved in the processing of personal data, necessitating the identification of the legal position of each of them. However, this can be challenging in Blockchain technology, where each participant in the network has access to personal data, making it difficult to determine who is the data controller and data processor. This issue is subject to debate among data protection authorities and specialized working groups in Europe. One possible solution is to operate on a private Blockchain network, where owners decide who can participate and better identify the role of each actor in data protection.

Exercise of rights, rectification, or erasure: The right to erasure and the right to rectification raise concerns regarding their application in immutable Blockchain technology. One possible solution is to apply irreversible anonymization processes, making the data so inaccessible that it could be considered equivalent to erasure. Regarding rectification, a new record could be introduced that modifies the previous one, with the latest record being considered valid.

Automated decision-making with legal effects: The use of smart contracts involves automated decision-making, which may conflict with GDPR requirements. However, the versatility of Blockchain technology allows these smart contracts to be configured and adapted to comply with the requirement of human intervention.

Other aspects to consider: The applicable legal basis for each case and the relationship between different actors in the Blockchain network must be carefully analyzed. The participation of actors from different parts of the world in a Blockchain-based system could involve international data transfers that may need regulation. Additionally, personal data incorporated into Blockchain should be anonymized to minimize the impact on the rights and freedoms of individuals.

3.2. Confidentiality / Privacy

This conflict arises due to the inherent transparency feature, which, while positive for preventing fraudulent acts, manipulation, falsification, or generating trust and security, can be seen as negative if the parties, for example, seek the confidentiality of the existence of the contract or the privacy of its clauses – even with the presence of confidentiality clauses.

Confidentiality can be achieved when using a private server, but "in the case of using public DLT platforms, the information can potentially be accessible to different participants/users of the platform or its operator, albeit subject to the terms and conditions of use. Maintaining confidentiality would require restricting access to information or, at the very least, attempting to ensure the anonymity of relevant information through encryption techniques, for example. In any case, there will always be a certain level of tension and uncertainty when using open platforms, given the uncertainties and potential vulnerabilities to which users are exposed." [5]

3.3. Right to Be Forgotten

Another aspect, and a more controversial one, is the claim that the technology underlying Smart Contracts, Blockchain, is in conflict with Data Protection regulations.

"Among the rights recognized by our regulations is the obligation of the data controller to delete or rectify personal data when requested by a data subject. Well, it is this possibility of modifying or deleting data that can create major problems between data protection regulations and Blockchain. The reason is that there is a direct clash between the right to modify or delete data and the immutability and unchangeability of data in Blockchain." [6]

It should be noted that the right to be forgotten is not explicitly legislated, but Argentine doctrine and jurisprudence have defined it, understanding that after a certain period of time, certain information must be erased to prevent individuals from being imprisoned by their past. In Europe, debates were also heated prior to the enactment of GDPR.

The right to be forgotten is closely related to the habeas data principle, and it was Law 25,326 that allowed jurisprudence to shape the right to be forgotten in the Catania and Napoli cases, relying on Articles 16 and 26 of that law. Therefore, national doctrine has affirmed that our country is "on the path to harmonizing regulations and standards with the European Union." [7]

4. Factual and Socio-Economic Framework

After the aforementioned clarifications, it is essential to establish the existing implementations of Smart Contracts in general terms and their consequent factual and socio-economic impact, as follows:

Smart Contracts are highly useful for keeping records during the stages of product development. If the parties determine that payments are to be made upon completion of a phase, for example, the contract triggers the transfer.

Smart Contracts have been used in Initial Coin Offerings (ICOs) and have gained significant relevance due to their implications. ICOs are governed by a Smart Contract that establishes the rules for acquiring the new cryptocurrency and manages the automatic issuance and purchase of the tokens.

The financial sector is particularly compatible with technological and digital innovations since its assets are generally already digitized, making it easier for them to adapt to changes.

Following this line of thought, "the main actors that could

benefit from Blockchain technology are (among others) banks and financial markets, as they could reduce costs while remaining secure and more efficient. With Ethereum, decentralized applications could be created that use Smart Contracts to carry out their functions." [8]

As an example, in Spain, if there is a flight delay attributable to the airline beyond the scheduled departure time stated on the ticket, the passenger is entitled to a refund of 7% of the ticket value. If the purchase is made through a smart contract, verification of the delay by air traffic control is sufficient for the money to be deposited in the passenger's account in real-time. Another example is Toyota, which is testing the implementation of smart contracts in installment car sales. If the payment for the recently purchased vehicle installment is not made on time, an instant order is executed from a remote location worldwide, resulting in the immediate immobilization of the vehicle until the outstanding payments are verified.

General examples of Smart Contract implementation include online product sales, patent registration, food traceability, insurance, product sales, rentals, and their use in virtual realities, where Descentraland is a clear example.

It is correct to state that Blockchain has introduced a new way of conducting transactions, improving the distribution of global capital and providing greater opportunities. This represents a change in the global financial system, given the revolution of the current economic model. Blockchain is a technology that has definitely arrived and cannot be ignored.

"Currently, we live in the digital era, where innovation represents a revolution for everyone. Moreover, the world needs to produce, manage, and store a huge amount of certified information at all times, which until now has been done by humans. Through technological advances, we have changed the way things are done, which used to be routine." [9]

To use a Smart Contract, the first thing to consider is whether the contract clauses can be translated into code. If that is possible, various smart contracts can be configured, such as rentals and sales contracts. In rentals, one of the benefits is that it prevents the parties from modifying the contract. In sales contracts, the latent advantage is the reduction in notarial costs, as the change of ownership can be verified through digital signatures. Smart Contracts can also be applied, as the Carlos III University and UNIR in Spain do, to prevent document forgeries, such as university diplomas. All of this is made possible by a crucial characteristic of Blockchain: immutability, meaning that the data entered into the blockchain cannot be modified. It should not be forgotten that another attractive feature of Smart Contracts is the elimination of intermediaries and third parties. Consequently, the possibility of a third party modifying the document to their advantage would also be eliminated. Therefore, due to the properties of immutability and transparency inherent in the network, smart contracts represent a revolution.

In the words of Valenti: "With the use of smart contracts, increasingly complex tasks can be performed, simplifying and automating all kinds of procedures. Thus, Blockchain could be more than just a registry and begin to be considered for use in processes such as product traceability systems, document issuance, and even to configure automated administrative actions, public procurement and contracting procedures, bid evaluation (automatically applying the regulated and parameterized criteria established in the specifications), subsidies, grants, and payment processing, amog others." [10]

Valentini exemplifies different initiatives that highlight the benefits of using Blockchain and smart contracts. For instance, Maersk Line and IBM in the transport and logistics sector aim to achieve end-to-end real-time supply chain traceability, transparency, and security. Wal-Mart also required its suppliers to use software developed by IBM before September 2019 for the same purpose. In Russia, particularly in the mining sector, Blockchain technology is used to ensure the authenticity of the supply chain, tracing natural diamonds from extraction and polishing to the end consumer. Other countries exploring the use of blockchain include Brazil, the United Arab Emirates, and China, with the aim of implementing a domestic solid waste management system. Furthermore, as previously mentioned, some universities use Blockchain to prevent diploma counterfeiting. [10].

5. Doctrine Study

National and international doctrine has sought to define smart contracts, analyze their legal nature and elements, but very few have addressed the issue of personal data protection and smart contracts.

However, it is necessary to discuss the problems that doctrine has addressed in order to reason the problem presented in this paper.

Cristina Poncibo explains when a smart contract can be considered a contract in the legal sense, as certain circumstances must be present. She adds that European and American scholars debate the validity of smart contracts, with common law scholars appearing more inclined to admit the possibility that such a program can constitute a proper contract, as the parties' consent can be expressed without special formalities when negotiating the contract using digital means. European continental scholars (e g., Germany, France, Italy, and Spain), on the other hand, are more cautious and consider that a smart contract cannot become a true contract but only represents a mere executive fact of a contract.[11]

Nicolás Negri presents Eliza Mik's perspective, who discusses programs that run on the blockchain rather than contracts in the legal sense, and even criticizes Szabo's precedent of vending machines as precursors to smart contracts. Negri also presents another less critical view, such as Arcari's, who defines smart contracts as the code of a computer program that automates the verification, execution, and fulfillment of certain terms and conditions of a contract. According to Arcari, smart contracts are automated agreements that depend on the occurrence or non-occurrence of certain predetermined objective conditions, as stipulated in

a contract. [12]

It also brings forth the definition that, according to this author, is the most accurate and adhered to by other scholars. This is the definition by Tur Fernandez: “contracts entered into through a web page accessible to the parties, the form of which is constituted by the user interface of the external application and one or more self-executable programs (smart contracts) residing on the blockchain with the ability to interact reciprocally and with said interface.” [13]

Negri also introduces the categories proposed by the European Union's Blockchain Observatory and Forum: 1) Smart Legal Contracts, and 2) Smart Contracts with legal implications. Another proposed classification is 1) Soft and 2) Pure.

Santiago Mora mentions the issue raised in this paper when he warns that "privacy and confidentiality issues may arise, particularly regarding access rights, deletion, updating, and modification." [14]

Following Arcari's line of thought, smart contracts share the concept of privacy with traditional contracts under the general principle of contract relative effect. However, they expand the concept of privacy to include the privacy of the parties' identity and transactions. [15]

Sebastián Heredia Querro understands that these aspects are intrinsically linked to control and confidentiality but also to the special forms of identity -anonymous and pseudonymous- allowed by the blockchain. [7]

Continuing with this author, it is explained that regarding contract privacy, although the parties control the contract, the problem lies in the fact that the contract code is publicly visible -in the case of a public blockchain- and therefore, the contract is not and will not be confidential. [7]

All blockchains allow for the recording and association of transactions with public keys between the parties involved -these keys are not necessarily known by everyone. Therefore, it is technically more accurate to speak of pseudonymity. Asymmetric encryption developments are not new and are an essential feature of all public blockchains. This technology protects the real identity of a blockchain user, just as credit card numbers are protected when making an online purchase through an insecure connection.

In blockchain, privacy is achieved in three ways: operating anonymously, encrypting information, and not hosting sensitive information on the blockchain but on off-chain parallel channels. It is crucial to keep this idea in mind for the possibility of establishing a solution to our problem.

Currently, various companies have emerged that offer the possibility to hinder the linkage of identity to a public key, as well as those that seek to associate identity with the corresponding public key. Another resource involves creating a new public key for each transaction, making it difficult to track the user's identity. Finally, it is necessary to mention On-Chain Analysis, an emerging method in which public transaction data recorded on the blockchain is observed, and if the Smart Contracts used for those transactions are added, patterns of who, how, and when cryptocurrencies are used can be extracted.

Marcelino Tamargo argues that the CNIL (French National Commission on Informatics and Liberty), the French authority for the protection of personal data, is the first European authority to address the compatibility of this technology with the protection of personal data as regulated in existing legislation. The reality is that both the regulations and the blockchain seek the same purpose: giving individuals more control over the processing of their personal data, but with different approaches, and it is precisely in this dichotomy that the potential conflict arises. On one hand, European regulations are based on a centralized system, focusing on the data controller of the organization, who has full control over the data and can access, modify, or delete it. On the other hand, blockchain is based on decentralized management, where data cannot be altered without affecting the blockchain. [16]

Based on Article 25 of the GDPR, the CNIL recommends that blockchain be used only when necessary. It proposes reducing personal data to only the public key, and if additional personal data needs to be entered into the data chain, additional measures must be taken to ensure maximum confidentiality. Finally, it believes that more specific regulations are urgently needed to facilitate data processing on the blockchain.

Elvira Sebastià Puig points out that the collision between the nature of the technology used in smart contracts and the current regulation on personal data protection, particularly the GDPR, is the reason for the conflict between data protection and smart contracts. The GDPR represents a genuine declaration of fundamental rights regarding data protection in the digital sphere, but the new technology has opposing precepts. Some of the problems arise because the GDPR defines personal data as "any information relating to an identified or identifiable natural person," and since IP addresses can identify the device that accessed the internet, the Spanish Data Protection Agency and the Supreme Court have declared that IP addresses are personal data. Consequently, when smart contracts use blockchain, although personal data is not used each time the chain is accessed, the entries and exits in each transaction are recorded. Thus, there is a possibility of identifying the connection's owner. [17]

Another problem is that data protection regulations establish the figure of a data controller, who is responsible for ensuring the effectiveness of data protection regulations and who can be held accountable for non-compliance. Users can exercise their rights with the data controller. However, in the blockchain, all participants have control over each transaction since it is a peer-to-peer network, and its nature is decentralized, so there is no data controller.

Another issue is that the GDPR includes a series of rights conferred to users whose data is being processed, which are contrary to the principles of the blockchain. For example, Article 17 of the GDPR states that data subjects have the right to request the erasure of their data in certain situations specified in the text. However, the use of the blockchain implies, on one hand, the absence of a data controller, as mentioned earlier. On the other hand, one of the fundamental

purposes of using the blockchain is immutability, which contradicts the GDPR.

Finally, there is the right to restriction of processing. In this case, the data subject can request the data controller to apply various measures to their data to prevent its modification, deletion, or erasure. Again, this right is incompatible with the immutability of data within the blockchain, as this technology is based on creating an immutable database.

6. Regulatory Framework

6.1. Argentine Legislation

Considering the existing regulations, it is important to highlight two aspects: data protection and smart contracts. Regarding data protection, we refer first to our Constitution, as in 1994, the habeas data action was incorporated in Article 43, third paragraph, guaranteeing the right to "obtain access to the data about themselves and their purpose, contained in public data registries or private databases intended to provide reports. In case of falsehood or discrimination, they may demand the suppression, rectification, confidentiality, or updating of said data. The secrecy of journalistic sources shall not be impaired." [18]

"This regulatory milestone involved the inclusion of the right to personal data protection in our fundamental legal text, both substantively and procedurally, which led to subsequent specific legislative reception." [19]

In 2000, Law No. 25,326 on Personal Data Protection was enacted, which is a public law that regulates the principles applicable to the matter, as well as the habeas data procedure, coming into force the following year.

However, it is undeniable that the scenario in which Law No. 25,326 was enacted has changed drastically in the past twenty-two years due to technological advancements. These advancements have had a significant impact on data protection, generating new legal questions and challenges in the field of rights exercise. As with any new technological reality, the benefits are celebrated enthusiastically, especially when paradigm shifts occur. However, we must not forget to identify, analyze, and investigate the potential new privacy vulnerabilities in order to find solutions.

Under the program "Justicia 2020," the then National Directorate for Personal Data Protection (DNPDP), under the Ministry of Justice and Human Rights, took the initiative to draft a bill on personal data protection to reform the current legislation and introduce new institutes, definitions, and innovative and highly debated rules in the field.

Following the message of 147/2018, the new regulation aims not to be an impediment to innovation and technological development while complying with international standards aimed at protecting personal data and privacy. Throughout its provisions, this bill "adequately guarantees the rights of data subjects, clarifies the legal bases for data processing (including legitimate interest of the data controller as one of the legal bases, moving away from the current law, which only contemplates the consent of the data subject), and imposes obligations on data controllers consistent with the intended purpose of the proposed regulation: comprehensive protection of personal data to ensure the full exercise of the rights of data subjects."[20] This bill generated expectations but has numerous deficiencies in its wording.

In addition, on May 25, 2018, the General Data Protection Regulation (GDPR) came into effect, establishing a new international regulatory context in this field, which Argentina must consider as part of the international community.

Regarding the novelties introduced by the bill and relevant to this work, we can mention the following: Article 2 defines personal data, including specific definitions for an identified person, an identifiable person, biometric data, and genetic data, as well as sensitive data. Article 16 discusses exceptions to the processing of sensitive data. Articles 5 to 10 establish the following principles: loyalty and transparency, proactive responsibility, purpose limitation, data minimization, accuracy, and retention period. Article 11 deals with the lawfulness of data processing, Article 12 with consent, and Article 14 with exceptions to prior consent. Article 15 outlines the information to be provided to data subjects. Article 19 establishes another principle, data security, which is reinforced by Article 20 on security breach notification. Article 21 establishes the duty of confidentiality. Articles 23 to 25 address the international transfer of personal data. From Articles 27 to 33, the rights of data subjects are established. The obligations of data controllers and data processors are outlined from Articles 37 to 45.

Having mentioned the aforementioned articles related to data protection, concerning this work, we need to analyze how smart contracts would be integrated into the national legislation on personal data protection contained in Laws No. 25,326, 27,275, 27,483, and in resolutions issued by the regulatory authority, such as Resolution 4/2019. We understand that there are certain scenarios where smart contracts collide with data protection legislation, leaving as alternatives either adapting smart contracts to our legislation or adapting our legislation to the immutability of the blockchain.

The right to be forgotten is intimately related to habeas data, representing a new legal institution "to effectively achieve, in a rule of law, the justified protection, security, accuracy or rectification, preservation, or destruction of secrecy or privacy regarding the citizen's data, which the State or other public or private entities have about them for the purpose of their authorized knowledge and dissemination, whether they are stored or kept in electronic or similar media since they constitute evidence or projections of the person, life, identity, cultural thought or instruction, social, economic, religious activities, as well as those related to genetics, health, sexual orientation, political thought, whether they are already registered or to be registered, in accordance with the protection and safeguards established by the Constitution and respective laws." [7]

As mentioned earlier, the right to be forgotten is not

legislated in our legal system. However, both doctrine and jurisprudence in our country have defined it.

The right to be forgotten is closely related to habeas data, and Law No. 25,326 allowed jurisprudence to extend the right to be forgotten in the Catania and Napoli judgments. In both cases, through a habeas data action, the erasure of information on bank debts was sought, relying on Articles 16 (right to rectification, updating, or erasure) and 26 (provision of credit information services) of that law. Therefore, national doctrine has asserted that our country is "moving towards harmonization of regulations and standards with the European Union." [7]

An example of this is the Argentine ruling "Denegri, Natalia Ruth c/ Google Inc. s/ Personal Rights: Related Actions" from 2020, where the right to be forgotten was expressly recognized, based on the Spanish Costeja case, where the Court ordered Google to comply with the right to be forgotten, which is in force in Europe. This ruling is of vital importance since, although we can discuss the correct application of the institute, it is the first Argentine ruling to expressly recognize the right to be forgotten.

It is worth mentioning that the draft new data protection law also regulates it as the right to erasure. In the message presenting the proposed regulation, it is noted that the right to be forgotten "has sparked many theoretical discussions and criticisms about its application in practice, as a deficient implementation could lead to violations of other fundamental rights, such as freedom of expression or access to information. Hence, in the proposed regulation, although this right is recognized, it is explicitly stated that the right to erasure does not apply when data processing serves a public interest or is necessary to exercise the right to freedom of expression and information." [7]

On the other hand, Law No. 27,275 deals with access to public information, recognized as a fundamental right. Article 19 establishes the Agency of Access to Public Information as an autonomous entity operating within the scope of the Chief of Cabinet of Ministers. This agency was designated as the supervisory authority for Law No. 25,326 on personal data protection.

Law No. 27,483 approved the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, dated 1981, and includes an additional protocol to the aforementioned Convention, addressing supervisory authorities and the cross-border flow of data, signed in 2001.

To conclude with Argentine legislation, it is important to mention Criterion 2 of Resolution 4/2019, which contains guiding criteria and indicators of best practices in the application of the Personal Data Protection Law. "Criterion 2. Automated data processing. In the event that the data controller makes decisions based solely on automated data processing that produce adverse legal effects or significantly affect the data subject, the data subject shall have the right to request an explanation from the data controller regarding the logic applied in that decision, in accordance with Article 15, paragraph 1 of Law No. 25,326." [21] The nature of smart contracts lies in making automatic decisions based on data, which w/ill always be the case when a smart contract exists. Therefore, it is not coherent for the data subject to have the right to receive an explanation about the logic of the smart contract's decision since they would have been properly informed before initiating the smart contract.

It is essential to note that our legal system does not have specific regulations on smart contracts, and the majority of doctrine believes that general contract rules can be applied. However, this should not be limited to that, as numerous situations may arise where rules related to adhesion contracts, personal data protection, computer crimes, and consumer protection legislation may also be applicable.

Smart contracts should not be confused with electronic contracts, regulated in Article 1105 of the Civil and Commercial Code.

Electronic contracts are those carried out through electronic means where consent or assent is exclusively expressed electronically, and the execution of their clauses depends on the impulse of each party.

On the other hand, smart contracts, through the use of blockchain technology, enable automatic execution without the intervention of a third party to trigger their consequences.

According to Gianfelici, the absence of specific regulations on smart contracts does not prevent an analog application of the regime applicable to traditional contracts regarding the necessity of consent, object, and cause. [22]

Looking ahead, it is necessary to anticipate and follow the guidelines provided by the European Observatory and Forum on Blockchain regarding the possibility of future specific regulation in this field. These guidelines highlight three relevant characteristics: cooperation between regulators and the private sector, identifying cases where smart contracts are used extensively, and establishing minimum criteria to determine applicable legislation and jurisdiction.

6.2. Comparative Legislation

When analyzing comparative law, it is necessary to differentiate between the regulation of Smart Contracts on one hand and the protection of personal data on the other.

Given that Smart Contracts are highly innovative globally, their legal validity is uncertain, and specific regulations on the subject are limited to a few countries, even though multiple blockchain-based platforms offering the use of Smart Contracts have been developed.

It is important to understand that Smart Contracts cannot operate without the blockchain, which is why many jurisdictions that have addressed their regulation have incorporated the blockchain in their legal definition and treatment.

The main interest in comparative law starts with countries that have the Common Law system, as they have been the first to tackle the regulation, especially the United States, seeking legal solutions due to the lack of existing regulations that fit Smart Contracts. Arizona and Vermont are two pioneering states in this regard.

Arizona was the first state in the world to adopt blockchain

technology in its legislation in 2017 when House Bill 2417 was approved in the House of Representatives. This law provides a legal definition of the blockchain and Smart Contracts. In relation to Smart Contracts, the law considers them legal, effective, and valid since they exist in commerce. The law specifies that a signature, record, or contract secured through blockchain must be legally recognized in its electronic form, just like digital signatures or records.

Vermont was the first state to regulate blockchain technology in 2015, and in May 2018, through Act 269, it included the definition of a smart contract, which was very similar to that of Arizona. The novelty was the introduction of the BBLLC, which stands for Blockchain-Based Limited Liability Company. This designation is specifically for companies that operate a business using blockchain in all or part of their activities. This established the first law that proposes a model without intermediaries in the decision-making of the company. Another novel aspect of the law is that existing digital records in the blockchain are admissible as evidence in court, provided there is an affidavit from an authorized person responsible for entering the data into the blockchain.

Delaware, known as the "birthplace" of corporate law and where over two-thirds of Fortune 500 companies are incorporated, introduced Senate Bill 69, which allows private companies incorporated in the state to issue and track shares, shareholders, and other corporate aspects using blockchain. In this case, Smart Contracts are used for legal purposes and are a source of legal facts since financial transactions are coded and recorded on the blockchain, allowing them to be converted into written form for legal actions, as established by the law.

In the case of the United Kingdom, which has been a precursor in this matter and followed by many other countries, there is no legally binding regulation. However, there is a legal statement from the UK Jurisdiction Taskforce in 2019, composed of experts with government support. In this statement, the UKJT addressed the legal nature of Smart Contracts and considered them contracts with legal effects as long as they meet the legal requirements to establish a legally binding relationship between the parties. This declaration provides confidence that crypto assets and Smart Contracts have a solid foundation in English law. The UK Law Commission stated that "they do not require statutory law reform for legal smart contracts in the digital asset space...(they) are permissible within the current legal framework of England and Wales. The Law Commission recommended only "incremental development of the common law," as needed for existing frameworks, but also encouraged parties to Smart Contracts to explain the risks associated with "the execution of code" and any other necessary terms." [23]

Italy is another country worth mentioning. While it did not have a legal definition of Smart Contracts, it had various regulations related to cryptocurrency exchanges and ICOs, as well as guidelines from the Italian Tax Agency on the taxation of holding cryptocurrencies. However, the absence of specific regulations for Smart Contracts, which made these operations possible, created a serious lack of legal certainty. This was addressed through the Decree Semplificazioni, which incorporated the definitions of blockchain and Smart Contracts into the legal text. A Smart Contract is defined as "an informational program that operates through distributed ledger technology and whose execution automatically binds two or more parties based on predefined effects. Furthermore, Smart Contracts are not considered to meet the requirement of written form until the computer identification of the parties takes place." [24] This way, the code language used in Smart Contracts is recognized as a new way to enter into agreements between parties.

Lastly, in terms of Smart Contract regulation, Estonia should be highlighted. Estonia is a country that has consistently been interested in innovation and the adoption of new technologies. In fact, it began exploring blockchain technology in 2008. In 2012, it became the first country in the world to implement blockchain as a register for government data. Therefore, it is not surprising that the adoption of this technology and the use of Smart Contracts are a reality in Estonia. Its legislation establishes that a recognized and qualified electronic signature has the same legal effect as any handwritten signature, stamp, or physical seal, making Smart Contracts a legally valid method for contracting in Estonia.

Regarding the protection of personal data, the focus is mainly on the General Data Protection Regulation (GDPR), not only because of its significance in Europe but also because of its implications for countries like Argentina, which seeks to harmonize its regulations and standards with the European Union. It is important to note that the purpose of the GDPR is to give control to individuals and residents over their personal data and to simplify the regulatory environment for international businesses by unifying regulations within the EU, i e., centralized data. Therefore, since the blockchain is decentralized by definition, at least in the case of public blockchains, many authors have argued that there is a total incompatibility with the GDPR because encrypted data still qualifies as personal data under the directive. However, this is not a uniform view. Michèle Fink explains this issue by stating that "one of the functions offered by the blockchain is the maintenance of records that eliminates the need for intermediaries, allowing for the decentralization of data collection, storage, and processing. This way of working with data is very different from the current system, which, on the contrary, centralizes data in the form of "platform power." Google, Amazon, Apple, and Facebook are giant intermediaries who control how individuals search, buy, and connect. They collect, store, process, and monetize our data traces autonomously. This allows them to increase their market power using the collected data to their benefit, with new algorithms, for example. Such market power has raised concerns from a competition policy perspective, as it hinders market entry...(the) blockchain offers the promise of decentralized data handling and data sovereignty, a concept that focuses on

giving individuals control over their personal data and allowing them to share that information only with trusted parties. The GDPR shares the goal of data sovereignty, as it aims to grant individuals 'control over their own personal data.'" [25]

One of the areas where the GDPR and Smart Contracts collide is the determination of the parties involved in granting obligations and/or rights since it goes against the essence of the blockchain, where each participant is on an equal footing, making it difficult to determine the roles of data controller and data processor. It has been recommended to use a private network to enable compliance with GDPR requirements. In this context, it is advisable to operate on a private blockchain network where the network owners can determine the participating parties, making it easier to identify the roles.

Another issue arises with the right to erasure and the right to rectification, as they operate within a network that is, by nature, immutable. The GDPR establishes that the data subject can request human intervention when an automated decision produces legal effects. This goes against the nature of Smart Contracts, which function automatically without human intervention.

Despite the various challenges arising from the collision between the GDPR and Smart Contracts, data protection authorities and specialized working groups are seeking reconciliation between the two.

7. Case Law

In the field of case law, no national or international precedents have been found regarding the issue at hand, unlike the case of personal data protection. Both nationally and internationally, case law harmoniously grants protection to the affected individuals.

This lack of case law is consistent with the new paradigm. It is important to note that our personal data protection law has not yet been modified, and globally, there is still doctrinal debate regarding the legal nature and even the definition of Smart Contracts.

8. Hypothesis Verification

After considering the most important points related to the protection of personal data and its relationship with Smart Contracts, it can be concluded that the use of Smart Contracts in our country will lead to different scenarios, namely:

Regarding privacy, it will depend on the type of blockchain used, whether public or private, and how the safeguards for personal data are implemented, considering the immutability existing in the network. As mentioned earlier, through Smart Contracts, access to data that may be considered personal under our law, such as public keys, could be possible, and in some cases, it could even involve sensitive data.

Since Argentina is part of the European community and seeks to comply with high standards of personal data protection, discussions arise regarding the immutable nature of the blockchain.

This author believes that the mere use of blockchain does not constitute a violation of data protection regulations. The main problem arises from how the technology is configured and used, which could potentially lead to non-compliance. However, these regulatory non-compliances occur because the law was designed for a different technological scenario.

9. Proposal

One of the solutions proposed regarding privacy, which is considered at risk with blockchain, is to use the so-called Zero-Knowledge Proof (ZKP). This cryptographic method enhances the security, privacy, and anonymity of the blockchain. One of the most innovative and appealing premises of the blockchain was to propose a safer and more private space for its users. By combining it with a secure authentication method like ZKP, the blockchain gains even greater privacy capabilities. With Zero-Knowledge Proof, both the blockchain and its services have authentication methods without the need to reveal sensitive information. This new protocol is one of the most famous products in cryptography. After all, security, anonymity, and privacy can be achieved by combining these features in the blockchain industry.

This author believes that using ZKP in the blockchain would be a fundamental tool to counteract the privacy issues discussed in this work.

On the other hand, when it comes to immutability and the right to be forgotten, the solution is not as straightforward. After the analysis conducted in this study, this author believes, without excluding the possibility of some unknown technical solution, that in pursuit of technological development and the benefits found within the blockchain and its implications, it will be the legislators who will need to adapt data protection regulations, taking into account the immutability characteristic and finding an alternative to protect personal and sensitive data.

10. Conclusion and Final Thoughts

In conclusion, the revolution in the digital age is undeniable, and the new paradigms present an encouraging outlook for society and the market as they simplify processes and reduce costs. Although there are legal gaps and contradictions between the nature of the blockchain and the legal system, we should not remain stagnant.

It is important to recognize that the law must adapt to new realities, regulating them in the fairest way possible. Therefore, many legal experts have stated that law is a social construct, and thus, we need to understand these new realities and find new solutions.

In this case, an integrative effort among experts from different fields will be necessary to provide a proper legal approach to the new paradigm and integrate it into our legal system. Smart Contracts should be seen as an additional set

of digital tools that can accelerate and simplify processes, promote development, and establish greater web security and transparency.

References

[1] Allende Lopez, Marcos y Colinda Unda, Vanesa (2018) "Aprende los tres elementos clave de blockchain con este ejemplo práctico." Conocimiento abierto. https://blogs.iadb.org/conocimiento-abierto/es/elementos-clave-de-blockchain/

[2] Ibañez Jimenez, Javier (2020) "Concepto y límites del legal smart contracts." https://repositorio.comillas.edu/rest/bitstreams/408683/retrieve

[3] Extremera Maestro, Enrique (2022) "La protección de datos en la Blockchain y los Smart Contracts ¿es posible?" https://www.legalarmy.net/la-proteccion-de-datos-en-la-blockchain-y-los-smart-contracts-es-posible/

[4] Salas, Alvaro Roco (2019) "Estudio sobre Smart contracts en Ethereum." https://core.ac.uk/download/pdf/288502094.pdf

[5] Torrenti-Visiedo, Andrés (2020) "Estudio de los aspectos legales, retos y limitaciones de la implementación de tecnologías DLT y Smart contracts en la sindicación de préstamos corporativos." http://openaccess.uoc.edu/webapps/o2/bitstream/10609/108706/6/atorrentiTFM0120memoria.pdf

[6] Signe, Thomas (2019) "Aspectos Juridicos del Blockchain." https://www.thomas-signe.com/blog/aspectos-juridicos-del-blockchain

[7] Heredia Querro, Sebastián (2020) "Smart contracts: qué son, para qué sirven y para qué no servirán." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875645

[8] Santos Garcia, Alvaro (2019) "Caracterizacion de Smart Contracts en Ethereum." https://e-archivo.uc3m.es/bitstream/handle/10016/30195/TFG_Alvaro_Santos_Garcia_2019.pdf?sequence=1&isAllowed=y

[9] Romero Solis, José (2019) "Aplicaciones de contratos en Ethereum." https://e-archivo.uc3m.es/bitstream/handle/10016/29653/TFG_Jose_Romero_Solis.pdf?sequence=1

[10] Valentini, Daniela B. (2019) "Adopción de tecnologías disruptivas en la contratación pública." https://www.austral.edu.ar/derecho/2019/04/01/adopcion-de-tecnologias-disruptivas-en-la-contratacion-publica-blockchain-como-herramienta-de-eficiencia-transparencia-y-aliado-contra-la-corrupcion/

[11] Poncibo, Cristina (2022) "Smart contracts: moldeando los patrones futuros del consumo." Publicado: EBOOK-TR 2022 (Errico), 04/03/2022, 320. Cita: TR LALEY AR/DOC/2664/2021

[12] Negri, Nicolas Jorge (2022) "Smart Contracts". Publicado en: EBOOK-TR 2022 (Errico), 04/03/2022, 166. Cita TR LALEY AR/DOC/2493/2021

[13] Tur Faundez, Carlos, "Smart contracts. Análisis jurídico", Ed. Reus, Madrid, 2018, ps. 51-59. BIELLI, Gastón E. — ORDÓÑEZ, Carlos J., "Contratos electrónicos", ob. cit., t. II, cap. XXIII.

[14] Mora, Santiago J.(2019) "La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso" Publicado en: La ley 01/04/2019, 01/04/2019, 1 - laley2019-B, 786. Cita: TR LALEY AR/DOC/537/2019

[15] Arcari, Jared (2019) "Decoding Smart Contracts: Technology, Legitimacy & Legislative Uniformity" https://ir.lawnet.fordham.edu/jcfl/vol24/iss2/3/

[16] Tamargo, Marcelino (2020) "Conflicto entre la tecnología Blockchain y la normativa de protección de datos" https://www.economistjurist.es/premium/derecho-inteligente/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos/

[17] Sebastia Puig, Elvira (2022) "Blockchain y normativa de protección de datos: una relación tensa". https://www.loyra.com/blockchain-y-normativa-de-proteccion-de-datos-una-relacion-tensa/

[18] Constitución Argentina, articulo 43 tercer párrafo.

[19] Faliero, Johanna Caterina (2017) "La protección de los datos personales del consumidor y su importancia cardinal en nuestro sistema juridico argentino" https://www.fuerzas-armadas.mil.ar/Instituto-Ciberdefensa-FFAA/archivos/06%20FALIERO%20La%20proteccion%20datos%20personales.pdf

[20] Agencia de acceso a la información pública, cuadro comparativo ley 25.326 y mensaje 147/2018. https://www.argentina.gob.ar/sites/default/files/comparativo_ley_datos.pdf

[21] Resolución 4/2019, Anexo I.

[22] Gianfelici, Florencia (2020) "Smart contracts. ¿Crónica de un cumplimiento anunciado?" Publicado: La Ley 07/01/2019, 07/01/2019, 1 - La ley 2020-A, 547. Cita: TR LALEY AR/DOC/3266/2019

[23] Wright, Turner (2021) "La comisión de derecho del Reino Unido afirma que las leyes inglesas y galesas aplican a los contratos inteligentes". https://es.cointelegraph.com/news/uk-law-commission-affirms-english-and-welsh-laws-apply-to-smart-contracts

[24] Castellano Garcia, Adoración (2021) "Conceptualización de los contratos inteligentes o autoejecutables basados en la tecnología blockchain y si encuadre en el ordenamiento jurídico español". DOI: https://doi.org/10.17561/rej.n21.6756 https://revistaselectronicas.ujaen.es/public/journalslia/rej2021_21/151568764003/index.html

[25] Fink, Michèle (2018) "Blockchains and Data Protection in the European Union" DOI https://doi.org/10.21552/edpl/2018/1/6 https://edpl.lexxion.eu/article/edpl/2018/1/6