Personal Data Management against Identity Theft: Analysis of Cases Filed at the Consumers League from Universidad Pontificia Bolivariana Monteria (2019 - 2021)

Received: February 2nd, 2022 • Approved: November 30th, 2022
https://doi.org/10.22395/ojum.v21n46a11

Jaclyn Ximena Carrillo Díaz
Universidad Pontificia Bolivariana, Montería, Colombia
jaclyn.carrillod@upb.edu.co
https://orcid.org/0000-0001-5264-5458

Adriana Isabel Londoño Londoño
Universidad Pontificia Bolivariana, Montería, Colombia
adriana.londono@upb.edu.co
https://orcid.org/0000-0002-5932-9754

Eduardo Alonso Flórez Aristizábal
Universidad Pontificia Bolivariana, Montería, Colombia
eduardo.florez@upb.edu.co
https://orcid.org/0000-0003-4409-1349

ABSTRACT

The main objective of this paper is to build a diagnosis of the current state of the local legal reality (Monteria and the department of Cordoba) regarding consumer law (identification of the most urgent and complex problems and the type of solutions they are currently subject to) in order to define lines of work in strategic litigation. Thus, the methodology used was to observe and analyze the repeated consultations to the Consumers League UPB Monteria of users' victims of impersonation (2019 to 2021), giving rise to this article in which a study is conducted ranging from the conceptual examination of the protection of personal data, the contractual modality used and impersonation, to the analysis of all related rules. The main findings allow identifying situations in which, due to the improper handling of the personal information of the subscribers of a contract that is generally of adhesion, they have been exposed to indiscriminate or improper use by malicious third parties without giving full compliance with the duties of protection and implementation of security protocols by the companies to ensure the proper custody of personal data, which in practice leaves the consumer exposed to various risks regarding the use of their personal information.

K*eywords*: data protection; contract law; identity theft; impersonation; legal liability.

Gestión de datos personales frente al robo de identidad: Análisis de casos radicados en la Liga de Consumidores de la Universidad Pontificia Bolivariana Montería (2019 - 2021)

RESUMEN

El objetivo principal de este trabajo es construir un diagnóstico del estado actual de la realidad jurídica local (Montería y el departamento de Córdoba) en materia de derecho del consumidor (identificación de los problemas más urgentes y complejos y el tipo de soluciones a las que están sometidos actualmente) con el fin de definir líneas de trabajo en litigio estratégico. Así, la metodología utilizada fue observar y analizar las reiteradas consultas a la Liga de Consumidores UPB Montería de usuarios víctimas de suplantación de identidad (2019 a 2021), dando origen al presente artículo en el que se realiza un estudio que va desde el examen conceptual de la protección de datos personales, la modalidad contractual utilizada y la suplantación de identidad, hasta el análisis de todas las normas relacionadas. Los principales hallazgos permiten identificar situaciones en las que, debido al manejo indebido de la información personal de los suscriptores de un contrato que generalmente es de adhesión, se han visto expuestos a un uso indiscriminado o indebido por parte de terceros malintencionados sin dar cabal cumplimiento a los deberes de protección e implementación de protocolos de seguridad por parte de las empresas para garantizar la correcta custodia de los datos personales, lo que en la práctica deja expuesto al consumidor a diversos riesgos respecto del uso de su información personal.

P*alabras clave*: protección de datos; Derecho contractual; usurpación de identidad; suplantación de identidad; responsabilidad jurídica.

Gestão de dados pessoais face o roubo de identidade: Análise de casos radicados na Associação de Consumidores da Universidade Pontifícia Bolivariana Monteria (2019-2021)

RESUMO

O objetivo principal desse trabalho é construir um diagnóstico do estado atual da realidade jurídica local (Monteria e o Estado de Córdoba) em matéria do direito do consumidor (identificação dos problemas mais urgentes e complexos e o tipo de soluções as que estão submetidas atualmente) com o objetivo de definir linhas de trabalho em litigio estratégico. Assim, a metodologia utilizada foi observar e analisar as repetidas consultas na Associação de Consumidores UPB Monteria de usuários vítimas de falsificação de identidade (2019 a 2021), dando origem ao presente artigo no qual se realiza um estudo que vai desde o exame conceitual da proteção de dados pessoais, a modalidade contratual utilizada e a falsificação de identidade, até a análise de todas as normas relacionadas. Os principais resultados permitem identificar situações nas quais que, devido à gestão indevida da informação pessoal dos assinantes de um contrato que geralmente é de adesão, tem sido expostos a um uso indiscriminado ou indevido por parte de terceiro mal-intencionados. Sem dar total cumprimento aos deveres de proteção e implementação de protocolos de seguridade por parte das empresas para garantir a correta proteção dos dados pessoais, o que em prática deixa exposto ao consumidor a diversos riscos respeito ao uso da informação pessoal.

P*alavras-chave*: proteção de dados; direito contratual; roubo de identidade; falsa identidade; responsabilidade jurídica.

Introduction

This paper is the result of the research developed in one of the three lines of the Legal Clinic project called "Strategic Litigation. Construction of a diagnosis" as a challenge to renew and strengthen the elements of legal knowledge to take them to the classroom and society. This research project was financed by the Universidad Pontificia Bolivariana —Monteria Headquarters— and is part of the COEDU research group. This project seeks to create a new scenario in which teaching, research, and social projection converge harmoniously as elements of training conceived by the Universidad Pontificia Bolivariana [UPB], a context in which work in the classroom is linked to the praxis of law (strategic litigation), to carry out the construction of a diagnosis of the current state of the local legal reality (Monteria and the department of Cordoba) concerning consumer law (identification of the most urgent and complex problems and the type of solutions they are currently subject to).

The UPB Monteria Consumer League, created by resolution 0047 from the Office of the Mayor of Monteria (2015), has the primary function to guarantee protection, information, education, and respect for the rights of consumers of goods and services, through advisory work and process assistance carried out by students taking the Legal Clinic course at UPB. This league becomes the environment conducive to finding and identifying the primary input that serves as the basis for this research aiming to determine the most common problems regarding consumer rights in Monteria (user statistics by cases consulted, identifying actors, circumstances, products, and services subject to recurring complaints; events that facilitate user disagreements), counting with the required information in a specific context.

From 2019 to 2021, the Consumers League from UPB Monteria received many requests regarding cases of users who had been victims of identity theft by third parties before different companies. These users stated they were aware of such circumstances because they received calls from collection entities to collect pending payment portfolios. They also found out through calls and messages from the companies before which they had been impersonated, informing them about the delayed payments of products or services they had supposedly acquired. Some users learned about the situation they were being victims of through consultations with databases in which contracts on their behalf were reported, which had not been signed or authorized.

Given these recurring queries within a specific period and the identification of situations with similar characteristics, the need to analyze possible coincidences between accounts of users from the UPB Monteria consumer league was recognized in terms of entities and companies involved, modalities, means, and methods used by active subjects of the behaviors, to establish the findings and suggest corrective and of course, preventive alternatives to protect consumers in Monteria.

Similarly, it is possible to see that all situations are directly related to a lack of personal data protection or inadequate handling and custody of these. This research began with analyzing the regulatory context of treatment and protection of personal data in Colombia to lead the contractual modality study commonly used by companies to provide consumer access to products and services massively. So, it is evident that one of the contractual modalities usually used in current legal traffic is that of adhesion contracts, those prepared by one of the parties before the contract conclusion. The adhering party cannot negotiate and has no choice but to accept or reject them. Therefore, given the negotiation conditions, mainly through e-commerce, several cases have been generated in which users become victims of identity theft when the company selling the product or providing the service does not strictly monitor the unequivocal confirmation of the adherent's identity.

Due to the above, a situation assessment raised by users in their queries is carried out, beginning with a detailed conceptual and legal analysis of personal data protection (Law 1581, 2012), using contractual modality (adhesion contracts) and identity theft in Colombia, to establish the relationship among these issues and determine their scope by Law 1480 of 2011, 'Consumer Statute'. Finally, procedures and protocols to be followed by the Consumer League from UPB Monteria and other entities related to identity theft cases were reviewed to assess them and present the pertinent recommendations that allow achieving the adequate protection of consumer rights in the city of Monteria and the Department of Cordoba.

1. General Treatment of Personal Data

Personal data refers to information about an identified or identifiable living physical person. Thus, any information that allows individualization to a specific person constitutes personal data (European Commission, 2021).

> Within the prerogatives or minimum contents detached from the right to habeas data, we find at least the following: (i) The people's right to know or access information collected on databases, entailing access to databases where said information is. (ii) The right to include new data to provide a complete owner image. (iii) Right to update the information, i.e., to update the content of said databases. (iv) Right to which the information contained in databases is rectified or corrected in such a way that it agrees with the reality. (v) Right to exclude information from a database, either because of improper use or because of a simple willingness of the owner -without the exceptions foreseen in the regulations. (Judgment C-748, 2011) (translated by the authors)

Article 15 from the Political Constitution of Colombia (1991) raised to Constitutional Rank states the right that all persons have to "know, update, and rectify information collected on them in data banks and files of public and private entities". Thus, regarding the collection, treatment, and data circulation, this right should be procured by

freedom, respect, and other guarantees enshrined in the Constitution, attributing to the State the obligation to serve as the guarantor of compliance with these provisions.

Therefore, Statutory Law 1266 (2008) was issued at its time, whose purpose was to develop this constitutional postulate, in addition to that enshrined in article 20, also from the Political Constitution (1991), referring to truthful and impartial information against data of a financial and credit type, commercial, services, and that come from third countries. Subsequently, it became necessary to issue a law broadening the spectrum of personal data protection in general. Law 1581 (2011) was enacted to regulate personal data recorded in any database and subject to treatment by entities of a public or private nature.

Statutory Law 1581 of 2012 defines personal data as "any information linked, or that can be associated with one or several determined or determinable natural people." This definition allows the complete and unequivocal identification of the owner of said information from their individualization (Resolution 15339, 2016). So, when talking about these data, Law 1266 (2008) categorizes them into public, semi-private, and private data, and Law 1581 (2012) includes two more categories, such as sensitive data and the rights of children and adolescents.

Nowadays, the categorization of personal data arises from the Special Law of Habeas Data (Law 1266 of 2008) and the General Law of Personal Data Protection (Law 1581 of 2012), which classify these data into five groups depending on treatment requirements.

It should be clear that before the previous classification, when reference is made to reserved information, it is indicated that it is of interest only to its owner, closely linked to the protection of rights to privacy, freedom, and human dignity. Here are the political, ideological, religious, and sexual preference cases. In a jurisprudential manner, these types of data were grouped under the category of sensitive information, not susceptible to access by third parties, but in an exceptional situation, in which the reserved data constitutes a relevant and conducive evidence element within a criminal investigation and that, in its time, is directly related to the investigation object. Due to its nature, this information is subject to the reserve of the said criminal process when it comes to this type of data. The statutory legislator has included private and reserved information categories in private data. (Judgment C-1011, 2008).

Figure 1. Classification of Personal Data

Public Data

Data is not subject to a reservation so that others can know it, e.g., people's marital status, those contained in public documents, duly executed judicial decisions that third parties can understand, and others; clarifying that personal data is not made public for the simple fact of being able to access it on a public access platform such as social networks, telephone directories, and so on. (Resolution No. 15339 of 2016)

Semi-private Data

That is not naturally public, reserved, or intimate. Its knowledge is relevant to its owner and a particular group of people, sector, or society in general (Statutory Law 1266 of 2008). Information of a semi-private nature, even when it is not considered public, requires a specific limitation for its access, inclusion in a database, and disclosure. Therefore, a court or administrative order is needed to access it. Among these data are those such as "financial, commercial, and credit behavior, and data on social security other than those that have to do with the users' medical conditions" (JudgmentC 1011 of 2008).

Private Data.

This is only relevant for its owner because of its intimate or reserved nature (Statutory Law 1266 of 2008). When access to this type of personal data is necessary, an order from a court authority, competent and in the exercise of its functions, is previously required, e.g., those contained in documents of a private nature, clinical histories, merchant books, and others, (Judgment C 1011, 2008).

Sensitive Data

Those whose improper use may lead to cause discrimination against its owner. The legislator seeks to safeguard habeas data and the privacy right enshrined in the Political Constitution by protecting this right. Therefore, when access to said sensitive data is required, those in charge of carrying out said treatment, by the principle of habeas data, of access and restricted circulation, are entrusted with a reinforced responsibility, for which their non-compliance makes them subject to sanction in administrative and criminal matters, (Judgment C 748 of 2011).

Data of children and adolescents

Their treatment is aimed at ensuring prevailing respect for their rights, the reason why, except for data of public nature, other types of data (sensitive, private, semi-private) are subject to their treatment "as long as the prevalence of their fundamental rights is not to put at risk, and it unequivocally responds to the realization of the principle of their best interests, whose specific application will come from the analysis of each particular case" (Judgment C 748, 2011).

Source.Own elaboration. It is adapted from Law 1581 (2012) and Law 1266 (2008).

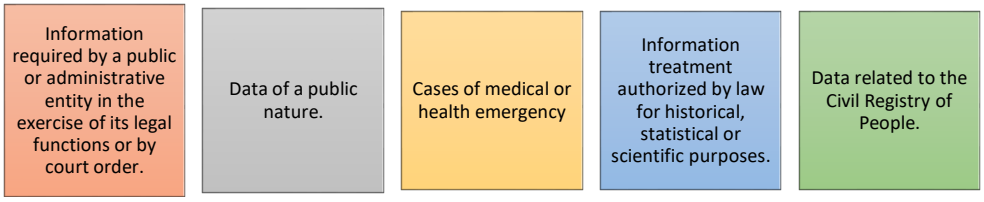
To summarize and to consider that in a certain way, private data can be confused with sensitive data, it is possible to affirm that personal data is that which, due to its reserved or intimate nature, is relevant only for the information's owner, while sensitive data is that whose improper use can lead to the owner to be discriminated against or that which affects the owner's privacy.

When any operation or set of processes is going to be carried out aimed at "*collection*, *storage*, *use*, *circulation*, or *deletion*," it faces what is known as "*treatment*." It is necessary to analyze the concepts presented by the norm (Statutory Law 1581, 2012) to understand each participating party's role when accessing personal data. The "*holder*" is the information's owner that is going to be treated by the '*liable for the treatment*' who is a natural or legal, public or private person who decides on the database, and in turn, on the treatment, and that at the same time can designate another natural or legal person, public or private, to be "in charge" of the treatment on behalf of the "*liable for the treatment*"' However, to be able to do all this, it is required that the "*owner*"

issue their "*authorization*" which is the consent that has previously, expressly, and knowingly issued of their "personal data" so that it becomes part of a database (Statutory Law 1581, 2012).

Therefore, for this treatment to be within the principle of legality, it is required that the authorization to treat said data has been carried out by means that may be subject to subsequent consultation by the holder. When this personal data is accessed without prior authorization, the law provisions must be complied with for the respective data processing. However, this authorization is not necessary when it is expressly:

Figure 2. Exceptions in the personal data processing



Source. Own elaboration. It is adapted from Law 1581 of 2012.

In short, in Colombia, when referring to personal data protection, there are two types of rules with their respective regulations, those of Financial Habeas Data (Law 1266, 2008; Law 2157, 2021) and General Law of Personal Data (Law 1581, 2012), each with its respective protection scope, but with the same guaranteed purpose.

Statutory Law 1266 (2008) was Colombia's first protectionist norm for personal data. This is a law of an exceptional nature since it focuses on the information regulation found in personal databases, but especially information of a financial, credit, commercial, services nature and third countries. This norm ensures that the personal data stored in these databases meet specific prerequisites that safeguard the good name and access to different credit modalities from the information perspective on economic and financial behavior. However, due to the health emergency in 2020, to recover the country's economy, Law 2157 (2021), commonly known as the Clean Slate law, is given effect, modifying and adding Law 1266 (2008).

After the issuance of the particular financial *habeas data* law and given that there was an increase in the use of different digital platforms in which data was delivered and captured for other databases, a general regulation of personal data was made necessary. Consequently, Statutory Law 1581 (2012), known as 'the general law of habeas data,' was issued. This is the framework for personal data protection in Colombia, with the purpose of "developing the constitutional right that all persons have to know, update, and rectify information that has been collected about them

in databases or files, and the other rights, freedoms, and constitutional guarantees" (Law 1581, 2012) (translated by the authors).

Similarly, with this law, the National Registry of databases was regulated as a public directory of databases subject to treatment, which are operating in the country, granting the administration of the same to the Superintendence of Industry and Commerce to be of free consultation for citizens. So, those in charge of carrying out this registry must deliver the information treatment policies to the entity, which must be subject to the regulation of the general norm of personal data protection (Law 1581, 2012).

Because of the different technological advances, presence of new technologies in terms of applications, and in general daily use of technological tools, people are forced to provide detailed data that by their nature may have sensitive or private status, such as data related to their name, surname, addresses, telephone numbers, emails, photographs, fingerprints, geographic locations, among others. (Aguilar Castañeda, 2018).

2. Impersonation of Personal Data in Colombia

The impersonation act has been defined in a general way as "taking the place of someone with evil arts, defrauding them of the right, employment or favor they enjoyed" (Spanish Royal Academy [RAE], n/d). When referring to impersonation, it is possible to affirm that it relates to the conduct in which an individual displays acts tending to alter or impose aspects of the person's identity. This action involves impersonating someone in any possible physical, digital, or virtual[1] areas.

Regarding the impersonation concept, the meaning, and the scope that it projects in Colombian legislation regarding the protection of identity and personal data, it is essential to glimpse the problem that arises with the circumstances in which the personal falsehood (impersonation) is the trigger for situations that are harmful to consumers. Consequently, there is a close relationship between the concepts of impersonation and that of identity since the act of "impersonating" has an impact on the latter, since the purpose of substituting or altering the information or data of a person is specified in circumstances that they allow to take the place of someone, to derive from this situation an illegitimate benefit that is evidenced in what is commonly known as *identity theft* It is necessary to establish that identity is understood as the "set of data or information that officially defines a person and allows them to be distinguished from another" (Spanish Royal Academy [RAE], n/d). Its etymological root comes from the Latin word *identïtas* or *idem*, meaning "the same." It is also represented in the expression "over and over again" since identity allows people to differ from others (EcuRed contributors, n/d).

[1] Digital is understood as "said of a device or system: that creates, presents, transports or stores information through bits' combination," while virtual is understood as that which 'is located or takes place online, usually through the internet, virtual store, campus, course, or meeting' (Spanish Royal Academy [RAE], n/d) (translated by the authors)

Nonetheless, depending on the context within which its conception is analyzed, identity will have a social, cultural, or legal scope, from which perspective identity is conceived as a fundamental right recognized by international instruments such as the Universal Declaration of Human Rights (1948) and the Convention on the Rights of the Child (1989), consisting in that all people without distinction have data that individualize them to achieve their full and free development within society. Its importance since it develops through social interaction in the environment and context in which it operates, making a person identifiable, unrepeatable, and with a sense of individuality.

On the other hand, the identity conception has varied. It has expanded thanks considerably to scientific advances and new information and communication technologies [ICT] so that personal identity can include more actual data than those before the developments of the technological era from which we begin to talk about digital identity or identity 2.0[2], which allows the individual to participate and interact on different digital platforms with other purposes (e-commerce, social networks, e-learning). In this sense, information digitation is making the development of applications based on creating consumer profiles, making it attractive for companies to continue contributing to the evolution of people's digital identity, to be able to view their reputation and privacy on social networks and Internet applications (Aguilar Barrera, 2019).

Due to the above, at this time, private data and sensitive data can be identified on the internet that accounts for exact and detailed information about a person, which is part of the particularities that identify someone and, therefore, determine to a great extent the construction of their identity 2.0. This information which is possible to access through databases of a private nature can be used illegitimately when there is no authorization from the holder. Therefore, there is a complete regulation aimed at the protection of personal data and, consequently, the identity and identity 2.0[3] of people through the fundamental right of Habeas Data enshrined in the political Constitution of 1991, Law 1266 of 2008, and Law 1581 of 2012, regulations alluded to regarding the analysis of the subject of personal data protection.

On the other hand, the Criminal Code of 2000 (Law 599) in article 296 establishes the crime of personal falsehood. It describes it in the following way:

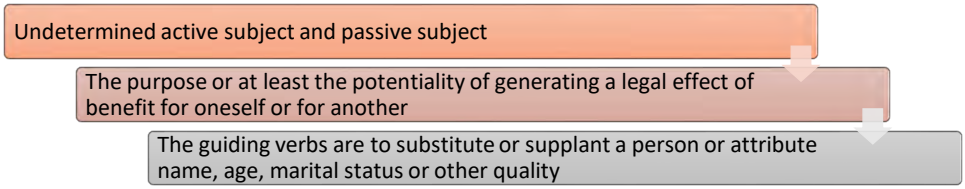
> The one that to obtain a benefit for itself or another, or causes damage, substitutes, or impersonates a person or assigns a name, age, marital status, or quality that may have legal effects will incur a fine, provided that the conduct does not constitute another crime. (Law 599, 2000) (Translated by the authors)

[2] It is understood by identity 2.0 or digital identity everything that "we manifest in cyberspace and includes both our actions and how others perceive us on the network" (Aparicio & Osua Ocedo, 2013)

[3] Identity is data that identifies the person in the physical world. Identity 2.0 is individualizing information but is located in digital or virtual spaces.

In this sense, said criminal type refers to what is commonly known as "*impersonation or identity theft*" and that within this set of regulations is located within the articles whose protected legal interest is public faith, which can be specified in the trust of the community in the correct identification of people, which represents an essential instrument of social life, legal traffic, and public economic order.

Figure 3. Elements of the crime of personal falsehood, impersonation, or identity theft

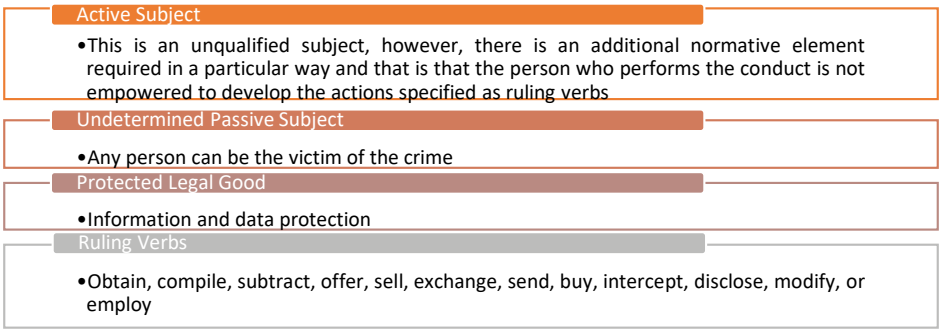


Source. Own elaboration. It is adapted from the Penal Code (Law 599, 2000, Art. 296).

In turn, the Penal Code includes a provision in which personal data is directly protected in article 269F, which was added by Law 1273 (2009) in which it is established:

> Anyone who, without being empowered to do so, for their benefit or that of a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies, or uses personal codes, personal data contained in files, archives, databases, or similar means will incur sentenced to prison for forty-eight (48) to ninety-six (96) months and a fine of 100 to 1,000 current monthly legal minimum wages. (Law 599, 2000; Law 1273, 2009) (Translated by the authors)

Figure 4. Elements of the criminal type: personal data violation



Source. Own elaboration. It is adapted from the Penal Code of 2000, Article 269F.

So, it is possible to verify that Colombian legislation has a system made up of provisions that tend to avoid situations that generate impersonation of people, aimed at protecting identity —identity 2.0 is implicitly guaranteed— and of the elements that make up what personal data is like. These norms are established in order and hierarchy

typical of a Kelsenian system[4], which goes from Article 15 of the Political Constitution, passing through the legal developments protecting the information contained in databases in general, with Law 1581 of 2012 and the handling of personal data, primarily financial, credit, commercial, services, and information from third countries with Law 1266 of 2008, until reaching the last ratio of sanctioning law, criminal law, in articles 269F and 296 of the Penal Code of 2000.

Currently, on October 29th, 2021, Law 2157 of 2021 was issued, named by its authors in colloquial language as the 'Law of a Clean Slate,' which makes an express reference to the situations in which identity impersonation occurs in article 7 that add numerals 7 and 8 in numeral 11 from article 16 from Law 1266 of 2008. In short, this article provides that if the information owner declares to be a victim of a crime of identity theft and that as a result of this, the payment of obligations is demanded, they must present a request for correction before the entity that acts as the information source (central risk), attaching the corresponding supports so that the entity, once it compares the obligation documents with those of the petition's owner, proceed to report the crime and include a legend in the personal record that says: '*victim of impersonation*'.

Thus, with this new provision, there is the possibility that the information holder, with the simple presentation of the request for correction before the entity (central risk), is allowed to expeditiously modify the harmful data created through the crime of identity theft (impersonation) protecting their data and keeping their credit history clean.

In conclusion, most databases in which all people's information is stored and rests are digital files. Precisely, by the technology use and unscrupulous handling given to these databases, the occurrence of identity theft situation has taken on the greater force since it is a more promising and advantageous means for cybercriminals to access their victim's personal information in an unlawful manner and without express authorization from the holder of the personal data.

At this point, it is necessary to establish, based on the current legislation, the way to prevent unscrupulous people from making improper use of information and personal data lying in databases of all public and private entities to be able to analyze this problem that arises with situations in which identity theft (impersonation) is the trigger for conditions harmful to consumers, mainly on the occasion of signing adhesion contracts in which information and personal data of the adhering contracting parties are often used without their authorization.

[4] It is a legal system graphed in a pyramid form, used to represent law hierarchy, one above the other, divided into three levels, the fundamental level in which the constitution is founded, as the supreme norm of a state and from which the foundation of the validity of all norms is derived (Ugarte Godoy, 1995).

3. Adhesion Contracts and their Relationship with Personal Data Protection.

In Colombian legislation, contracts are the maximum manifestation form of the disposition and faculty of man to be bound to comply with a benefit, based on a joint agreement between equals to reciprocally benefit, since through these, it is that transactions or exchanges that allow the society to function are made.

In this sense, one of the essential principles of contract law is private autonomy prevalence, consisting of the parties' possibility to determine and regulate their legally relevant relationships by themselves, granting it —in principle—- as the only limitation for its exercise, respect, and compliance with the rules of public order, as well as those related to morality and good customs. (Álvarez Estrada, 2014).

To this end, the Civil Code (1873) defined in its article 1494 the sources of obligations, pointing out, among others, those coming from "a contest of wills between two or more people," which would be the basis to lay the foundations of a contract defined in article 1495 as an "act by which one party binds himself to another to give, do, or not do something" (translated by the authors); concept reaffirmed in turn by the Commerce Code (1971) which defines it in its article 864 by providing that the contract is an agreement of two or more parties to establish, regulate, or extinguish between them a legal patrimonial relationship. Unless otherwise stipulated, on the contrary, it will be understood to be celebrated in the proponent's residence and at the moment in which the latter receives the proposal acceptance.

Nonetheless, consistent with society's economic and demographic growth, there were situations where a considerable number of individuals wanted access to a specific object or service from the same supplier; however, individually agreeing on each contract's conditions would become a tedious unmanageable task for the offeror. So, standardized agreements began to be created in which the interested party only had to subscribe to the needs pre-established by the offeror. It is from this that they begin to present what has been called "mass contracts," a form of contracting that meets the demands of economic traffic, manifesting itself for this through pre-written papers that allow the serial contracting of goods and services, whose contents have been set in advance of their execution by one of the parties (Rodríguez Chávez, 2010, p. 201).

However, it became evident that this contracting did not fit with the legal premise of the agreement. The parties settle on the circumstances in which the contract is going to be executed since, as observed in the definitions coined by the norm, the possibility of presenting agreements typically made through predisposed structures, which have been in everyday use among individuals, such as the transport or insurance contract, is omitted (Álvarez Estrada, 2014).

With the entry into force of the 1991 Constitution, the first contribution was made towards the regulation of these types of contracts by enshrining consumer protection

in article 78 as a principle, which led to an effort to regulate the contents of the standard clauses of mass contracts, which, although they had been presented, had not been regulated. This is how Law 142 (1994), dealing with the legal regime of residential public services in Colombia, speaks of "adhesion contracts" when referring in its article 128 to these as a uniform and consensual contract, applying criteria of compared law in which:

> The inter-parties negotiation of a few contract conditions does not constitute enough reason to exclude its adhesive character since, in reality, most of its clauses continue to be imposed *en bloc* by the predisposing party, and there is no possibility of negotiation on them. (Álvarez Estrada, 2014) (Translated by the authors)

After that, it would be the Constitutional Court (Judgment C-1162, 2000) that would enter into the matter through its jurisprudence by ruling on it and concluding that adhesion contracts, to introduce a balance in them, must be intervened by the State since two parties are immersed in them, one strong and one weak[5].

With Law 1328 (2009), the Financial Consumer Protection regime was established, complementing the concept of adhesion contracts themselves in Colombian legislation, defining them as "those prepared unilaterally by the supervised entity and whose clauses and/or conditions cannot be discussed freely and previously by the clients, limiting these to express their acceptance or rejection in their entirety"; the antecedent of what would be Law 1480 of 2011, Consumer Statute, which regulated matters related to the effectiveness and free exercise of the consumer's rights, mainly their economic interests.

In this sense, since it is typical of mass commercial activities that there is a dominant position, represented by the producer or supplier and another weak party (consumer as a subject of special protection)[6], the Legislator materializes the general principle[7] of the Consumer Statute of 2011 (Law 1480) regarding the security of this particular subject (consumer), in its article 5 defines the adhesion contract as "one

[5] 'The basis for elevating these contracts to an autonomous form different from those traditionally recognized is the following justification: given that in the contracts concluded between producers and consumers, the latter face a unilateral imposition involving a severe impairment of their will, severely violating the normative principles that in terms of contracts have been consigned in the legislations on private law; a reaction is mandatory on the legislator's part, who, to guarantee that the contracts continue to be useful according to the reason for which they were conceived, must regulate the contractual contents based on strict compliance rules that impose on the contracting parties the observance of the requirements outlined in the Law'. (Álvarez Estrada & Herrera Tapias, 2016) (Translated by the authors)

[6] Consequently, all contracts (whether by adhesion or not) entered into between consumers and producers or suppliers would be included in the category of legal consumer relations and, as a consequence, are subject to the rules of Law 1480 of 2011 because, as the Law does not refer specifically to consumer contracts, it can be logically inferred that any legal relationship involving the subjects described must be regulated by the rules of the consumption right, which, as already mentioned, are mandatory and inalienable norms (Álvarez Estrada & Herrera Tapias, 2016) (Translated by the authors)

[7] Article 1°. General principles. This law aims to protect, promote, and guarantee the effectiveness and free exercise of consumer rights and respect for their dignity and economic interests (...) (Law 1480, 2011).

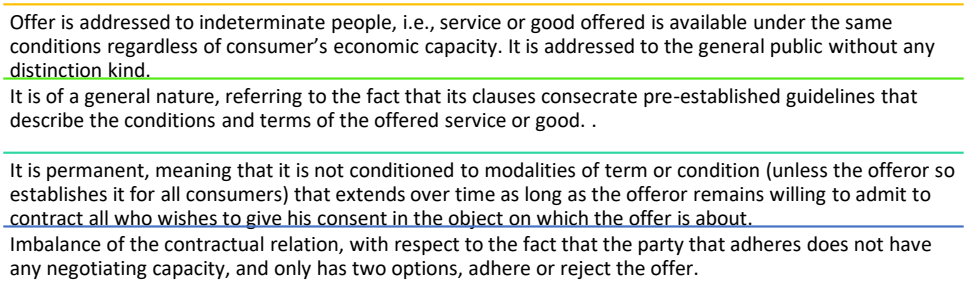
in which the producer or supplier arranges the clauses, so that the consumer cannot modify them, nor can do nothing but accept or reject them" and in turn, devotes an entire title to develop contractual protection.

In short, the adhesion contract can be understood as a model contract written only by one of the parties that signs it in such a way that the other party can only accept or reject the agreement in its entirety, which allows the offeror to make its own legal rules to govern its transactions if the other party (the consumer) expresses its general consent on the contractual form. It will be executed and valid regardless of whether they fully understand the content, agree with the terms provided and even read them. This means that the offeror's capacity is much more favored since they can impose adhesive terms on the other. The latter can only abide by the contract provisions.

> The doctrine has defined an adhesion contract as an agreement of wills employing which one of the contracting parties, called predisposing, imposes on the other, called adherent, the content of the contract without any possibility of discussing or modifying it, counting only on the power to freely decide whether or not to contract under the offered clause, within a 'take it or leave it' scheme. In Colombian law, neither the Civil Code nor Commercial Code defines the concept of an adhesion contract. However, we can find a definition in the Consumer Statute in which the producer or supplier arranges the clauses so that the consumer cannot modify them, nor can they do anything other than accept or reject them. (Posada Torres, 2015 p.143) (Translated by the authors)

Presently, regarding their characteristics, Garcés Bejarano (1966) concludes that the main particularities of this contract type are as follows:

Figure 5. Characteristics of the adhesion contract



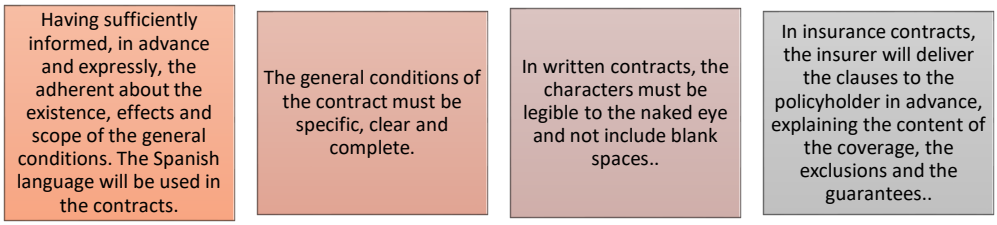
Source. Own elaboration, adapted from Garcés Bejarano (1966).

Regarding the imbalance of the contractual relation, it is of special care since the disadvantageous position that this contracting modality causes towards one of the parties is evident because it has no possibility of negotiating or modifying the clauses, and the other party may tend to abuse such circumstance for their benefit. Consequently, the asymmetric nature of adhesion contracts predominates, which

materializes in the inequality between the parties concerning their contractual power that is manifested. On the one hand, in the specific knowledge that the predisposing party has acquired as a result of the exercise of its commercial operation, and of which the adherent does not have; and, on the other, in the power that the predisposing person has due to his economic position in the market (Posada Torres, 2015).

Thus, to avoid possible abusive situations that may arise on the occasion of adhesion contracts, the consumer statute requires that the negotiable conditions surrounding the contract comply with special requirements indicated in article 37 of the law above:

Figure 6. Requirements of the adhesion contract



Source. Own elaboration, adapted from Law 1480 (2011, Art. 37).

Regarding the first point, the Superintendence of Industry and Commerce has ruled on several occasions, concluding that in the case of these contracts, any sale of products or services obliges the producer or supplier to provide the consumer with clear andeEnough information on the marketed well implies that the information provided about the offered properties of the goods and services must be truthful, complete, and not misleading. (Radicado 17- 30407 – 1, 2017).

In this sense, providing complete, detailed, timely, and transparent information on the conditions of the offered service or good is constituted as a provider's obligation in such a way that consumers have the corresponding elements that allow them to determine whether or not to purchase a particular service or product, considering that generally many of the contracts are not set out in detail at the time they are signed by the adhering party, implying that this does not fully know the agreement content, leaving the opportunity for bidders to include clauses that, although they are not directly harmful, can lead to damages for the subscriber.

One of the most common cases is the inclusion of a data management clause, which allows the service producer to create databases with the information of their contractors[8]. In principle, having this information relationship does not cause signifi-

[8] The terms and conditions with which providers intend to govern the contracting of goods and services they offer online, without fail, include clauses on using and treating personal data. The purpose of such clauses goes far beyond the legitimate need to individualize the contracting party: the collection of user data

cant inconvenience since it is a form of organization that companies use to perform their functions more efficiently; however, this can be a factor that causes transgressions to consumers if it does not perform adequate information management or if effective security mechanisms are not established. In this vein, there have been situations in which, due to improper management of the personal information of contract subscribers, they have been exposed to indiscriminate or inappropriate use by malicious third parties, violating the rights of consumers since there is no full compliance with the duties of protection and implementation of security protocols to guarantee the proper custody of personal data, which in practice leaves the consumer exposed to several risks regarding the use of their personal information.

4. Analysis and Management of Identity Theft Cases Identified by the Consumers League from UPB Monteria.

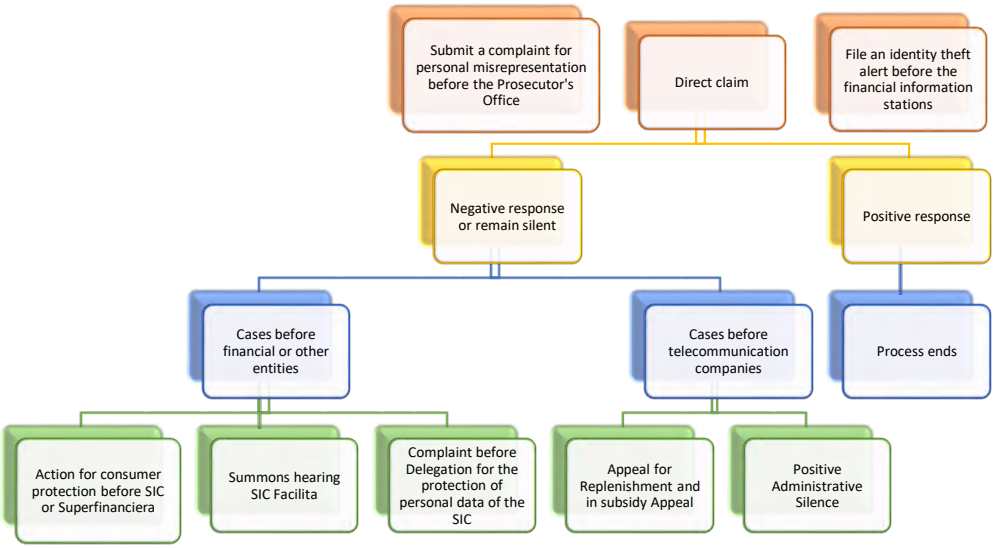
The Law Program from UPB Monteria, opting for the research and social projection stage, establishes the challenge of renewing and strengthening the elements of legal knowledge to bring them to the classroom and society, generating a connection between theory and practice, teaching the legal phenomenon towards the context realities. This is why the UPB Monteria Consumer League serves as an input for the project called 'Legal Research Clinic,' which serves as a laboratory for strategic litigation.

The primary function of the UPB Monteria consumer league is to guarantee protection, information, education, and respect for the rights of consumers of goods and services, as well as any similar, related, or complementary activity that facilitates or develops consumer protection in the community (Alcaldía de Montería, 2015). From 2019 to 2021, this organization provides advisory services and process monitoring to pursue consumer protection by its purpose.

Per the protocol established by the UPB Monteria consumer league, the complaint is made in the first instance before the Attorney General's Office for the crime of identity theft and the respective direct claim before the company that requires payment for the obligations allegedly contracted, following the provisions of article 56 from Law 1480 of 2011.

has become an extremely lucrative business, through its treatment and marketing, in what is known as the model of big data business. (Momberg Uribe & Morales Ortiz, 2019).

Figure 7. Procedure standardized by the Consumers League for cases of impersonation and violation of personal data



Source. Own elaboration. It is adapted from UPB Monteria Consumers League Protocol.

Likewise, an identity theft alert should be filed with the financial information centers (CIFIN, Datacredito, Procredito) to verify before these centers have consulted their credit history and inform those companies or people that the user possibly has been impersonated. Suppose after 15 business days, a response is not received or there is no agreement with it. In that case, the next step is to file a complaint with the Superintendence of Industry and Commerce regarding the direct violation of personal data. At the same time that the previous procedure is carried out, it is verified if the supplier with whom the conflict arises is registered in the SIC F*acilita*[9] program to convene a facilitation hearing before them[10].

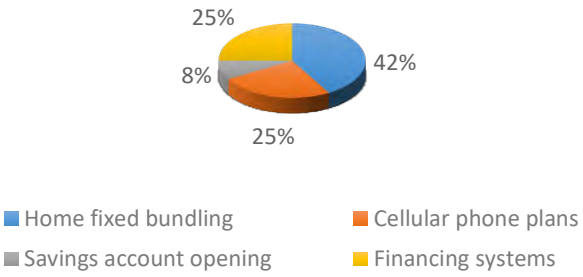
In the cases in which the claims are filed with telecommunications companies, when the answer is negative, one must proceed with the resources for replacement and subsidy of appeal, a help using which it is possible to go before the Superintendence of Industry and Commerce if the company does not replace its decision, or directly when positive administrative silence is filed as a result of not having answered the company within the legally established time.

[9] Virtual tool in which the Superintendence of Industry and Commerce [SIC], as a facilitator, seeks agreements between consumers and suppliers in search of the protection of the consumers' rights which come before the entity (Superintendency of Industry and Commerce of Colombia, n/d).

[10] Transaction agreement achieved as an alternative dispute resolution mechanism through the SIC FACILITA platform.

Following this procedure, those cases of '*identity theft*' identified in the UPB Monteria Consumers League, whose users, at the time of requesting services from this organization, have the following characteristics, are taken as a sample for developing this research: i) received calls from some collection entities for recovering pending portfolios, ii) received calls or messages from companies informing them about the delay in payments for current services and, iii) in the exercise of their right to consult the databases, had knowledge that there were reported contracts in their name.

Figure 8. Products are subject to impersonation



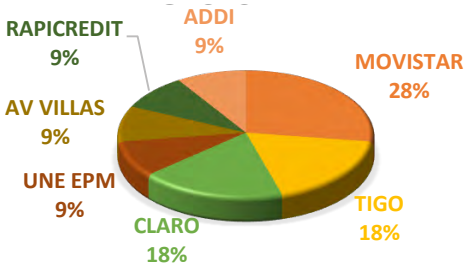
Source. Own elaboration. It is adapted from Cases Handled by the UPB Monteria Consumers League from 2019 to 2021.

Similarly, another analysis variable is the product subject to impersonation, resulting in 42 % bundling[11], 25 % referring to cell phone plans, 25 % mentioning financing systems, and 8 % opening savings accounts.

On the other hand, Figure 9 refers to the companies before which the cases referring to 'impersonation' were presented:

Graph 2. Companies before which the cases of impersonation were filed.

Figure 9. Companies before which the cases of impersonation were filed



Source. Own elaboration. It is adapted from Cases treated at the UPB Monteria Consumers League from 2019 to 2021.

[11] The Communications Regulatory Commission (2015) defines bundling as the sale of two or more products in a package at a price that is more attractive than the price for the parts that constitute said package

Therefore, as a result of this research, it is determined that the companies in which the cases of impersonation are filed are Movistar with 28 %, followed by TIGO and Claro, both with 18 %, and ending with ADDI, AV-Villas, UNE EPM, RAPPICREDIT, each represented with 9 %.

Similarly, the contractual modality usually used in case studies is adhesion or adhesion contracts. There is a written contract corresponding to the formats that each company has stipulated (preprinted and/or printed or digital). Likewise, during the research, it was established that some of these contracts (physical and/or digital) did not have the adherent's signature. In contrast, in other cases, the signature did not correspond to the users. Finally, situations were found where no evidence of the contract existed. A related circumstance was that, at the time of obtaining a response to the claim from the companies, they indicated that said adhesion contract was made verbally (recorded and/or monitored telephone call) and after the adherent answered the questions. However, since there was no physical presence of the user, it is inferred that these companies possibly did not fully identify the owner to enter into contracts.

For the company to be sure of the possible user's identity, it is necessary to comply with the provisions of Statutory Law 1581 of 2012, which establishes the management that must be given in Colombia to the personal data recorded in any database that makes them susceptible to treatment by entities of a public or private nature or; when the 'liable for the treatment is not established in the national territory, Colombian legislation is applicable by international norms and treaties.

Likewise, Statutory Law 1581 of 2012, in its article 4, stipulates that in its development, interpretation, and application, certain guiding principles of personal data processing must be given in a 'harmonious and comprehensive manner, to prevent the inappropriate use of the information contained in the physical, digital, or virtual databases.

In the cases under investigation, it was possible to corroborate that in light of these guiding principles, those in charge and liable for carrying out the treatments failed to comply with the obligations that the norm imposes on them since when upon a request of the record of the authorization from the holder for the processing of their personal data, (copy of the physical/digital contract or recording of the verbal contract), some of the required companies refused to deliver the requested documentation, while others proceeded to issue favorable responses but did not deliver any documentation. Finally, others kept absolute silence and provided the required information.

Figure 10. Guiding principles of treatment

Principle of legality regarding data processing	The obligation that companies have at the time of carrying out said treatment to adjust their actions to the provisions of the law
Principle of purpose	The treatment must be carried out under a legitimate purpose as regulated by the Constitution and the Law, and that must be informed to the holder.
Principle of freedom	Information cannot be obtained or disclosed without prior authorization by the owner or that that consent has been judicially or legally relieved
Principle of veracity or quality	It strictly forbids the data to be treated to mislead due to a lack of integrity or inaccurate, incomplete, and incomprehensible data.
Principle of transparency	It aims to guarantee that the liable or in-charge person of the treatment guarantees the owner the right to obtain information regarding their data at any time.
Principle of access and restricted circulation	Subject to the treatment to the provisions of the Law and Constitution, limiting it exclusively to the people authorized by the owner or those provided by law
Principle of confidentiality	All people who participate in the processing of personal data that do not enjoy being of a public nature have the obligation to guarantee that the information will be reserved even when the relationship has been terminated
Security principle	Seeks that the information subject to treatment is handled with all technical, human, and administrative measures to prevent these data from being degraded, lost, or fraudulently accessed or without authorization

Source. Own elaboration. It is adapted from Statutory Law 1581 (2012, Art. 4).

Some companies continue to claim payment for their services regarding the claims presented. Their responses argue that their actions were framed within the principle of good faith and legitimate expectations[12], leading the user to comply with his obligation to settle the pending debts. Given this, these arguments are refutable because, by the principles of demonstrated responsibility[13] and integrity, the companies must show that they were diligent in implementing effective measures to prevent the rights of their users from being violated.

Finally, it is established that the companies also violate the principles of security and restricted circulation by not having kept their users' information under the required

[12] The Principle of Legitimate Trust is derived from article 83 of the Political Constitution of 1991 by establishing that "the actions of individuals and public authorities must adhere to the postulates of good faith, which will be presumed in all steps that those take before them."

[13] Principle of Demonstrated Responsibility consists that both those liable and in charge of the treatment must implement measures in addition effective, appropriate, and verifiable to allow evidence that their actions were done under strict legal parameters so that when they are subject to evaluation and review, permanently done, it is denoted that it was done under a whole effectiveness level, just as it covers much more than the adoption of policies and issuance of documents. Therefore, it is required to verify that it was done accurately and effectively when putting these functions into practice (Superintendency of Industry and Commerce of Colombia, 2020).

conditions of due custody and, in this way, having allowed the impersonator to consult, use, or have unauthorized or fraudulent access to the personal data of the person who impersonated and is the owner of the data, since these personal data unless they are public information, cannot be available in any means of dissemination, mass communication, or the Internet unless their access is to provide restricted knowledge and is technically controllable as established by Statutory Law 1581 of 2012 in paragraph (f) of article 4.

Furthermore, Law 1480 of 2011, in article 50, provides that when suppliers and vendors in the national territory offer products using electronic means, they must maintain lasting support mechanisms for the proof of the commercial relationship, especially the consumer's entire identity. This guarantees the information's integrity and authenticity and is verifiable by the competent authority (Law 1480, 2011).

It is necessary to mention that according to information provided on July 10, 2019, by the Superintendence of Industry and Commerce, complaints about identity theft grew by 122 % after analyzing the 1,705 complaints that reached the Delegation for the Protection of Personal Data between January 1st and June 26th of that year compared to the same period of 2018 in which 767 complaints were received. Similarly, it indicated that the sectors with the highest complaints about impersonation are telecommunications companies at 69.6 %, followed by the catalog sales sector at 30.4 % (Superintendency of Industry and Commerce of Colombia, 2019).

Conclusions

In short, reference is made to the constitutional postulate enshrined in article 15 (1991) when referring to personal data protection in Colombia. Nonetheless, there are two types of norms within the legal system with their respective regulations. The first is a general provision, General Personal Data Law (Law 1581, 2012), and the second is a special regulation represented in the Financial Habeas Data Law (Statutory Law 1266, 2008) (Law 2157, 2021). These legal bodies have a respective protection scope but a guaranteed purpose. Nonetheless, on the occasion of the different technical and scientific advances, the presence of new technologies in terms of applications and in general, and the daily use of digital and technological tools, individuals are forced to provide particular data that by their nature may have the condition of being sensitive or private, which is why personal data protection that largely determines the identity and individuality of people becomes more important every day.

Given the fact that most of the databases in which all people's information is stored and rests are contained in digital files, it is precisely by using technology and the unscrupulous handling of these databases that the occurrence of identity theft situations has taken on the greater force since it is a more propitious and advantageous means for cybercriminals to access personal information of their victims illegitimately and

without express authorization of the personal data owner. In that vein, there have been situations in which, due to improper handling of personal data from companies before which the cases were filed, the subscribers of a contract (general adhesion) have been exposed to indiscriminate or inappropriate use by malicious third parties, violating consumers' rights, since there is no full compliance with the duties of protection and implementation of security protocols by companies to guarantee proper custody of personal data; which in practice leaves the consumer exposed to various risks regarding the use of their personal data.

It is for all this that through the UPB Monteria Consumers League, it has been possible to implement protocols aimed at the effective care of cases that require an appropriate legal defense against identity theft, to achieve a comprehensive conflict resolution in which, in addition, of being intended to eliminate the unjustified charging of a service not authorized or used to the 'user,' proper and adequate protection of their personal data is sought, aimed at preventing these circumstances from being repetitive while setting off alarms before the companies which show that their security protocols are presenting flaws that allow all these violations to occur.

References

Aguilar Barrera, E. (2019). *Suplantación de la identidad digital con fines de trata de personas en Facebook*. [Master thesis, INFOTEC – Center for Research and Innovation in Information and Communication Technologies (CONACYT)]. https://infotec.repositorioinstitucional.mx/jspui/handle/1027/363

Aguilar Castañeda, M. A. (2018). La ley de protección de datos en Colombia: sus inicios y exámen de sus principales postulados [undergraduate thesis, Universidad Católica de Colombia]. Institutional Repository. https://repository.ucatolica.edu.co/handle/10983/23060?locale=es

Álvarez Estrada, J. (2014). El contrato de adhesión en la legislación colombiana y en la nueva ley de protección al consumidor. *Advocatus*, (23), 101-116. https://www.unilibrebaq.edu.co/ojsinvestigacion/index.php/advocatus/article/view/292/0

Álvarez Estrada, J., & Herrera Tapias, B. (2016). Contrato por adhesión y relación de consumo en el Estatuto del Consumidor Colombiano. *Revista de Ciencias Sociales*, *22*(1), 166-178. https://produccioncientificaluz.org/index.php/rcs/article/view/24904

Aparicio, R. & Osua Ocedo, S. (2013). La Cultura de la Participación. *Revista Mediterránea de Comunicación*, *4*(2), 137-148. https://doi.org/10.14198/MEDCOM2013.4.2.07

Communications Regulatory Commission of Colombia. (2015, December 11th). *Análisis de Ofertas Empaquetadas en Colombia. Documento soporte propuesta*. https://crcom.gov.co/system/files/Proyectos%20Comentarios/2000-3-3/Propuestas/documento_soporte_ofertas_empaquetadas.pdf

Congress of the Republic of Colombia. (2008, December 31st). *Ley Estatutaria* 1266. *Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Diario Oficial n.° 47.219. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congress of the Republic of Colombia. (1873, May 26th). L*ey 84. Código Civil*. Diario Oficial n.° 2.867. http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html

Congress of the Republic of Colombia. (1994, July 11th). L*ey* 142. P*or la cual se establece el régimen de los servicios públicos domiciliarios y se dictan otras disposiciones*. Diario Oficial n.° 41.433. http://www.secretariasenado.gov.co/senado/basedoc/ley_0142_1994.html

Congress of the Republic of Colombia (2000, July 24th). L*ey* 599. P*or la cual se expide el Código Penal*. Diario Oficial n.° 44.097. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congress of the Republic of Colombia. (2009, January 5th). L*ey 1273. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Diario Oficial n.° 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congress of the Republic of Colombia (2009, July 15th). L*ey 1328. Por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones*. Diario Oficial n.° 47.411. http://www.secretariasenado.gov.co/senado/basedoc/ley_1328_2009.html

Congress of the Republic of Colombia. (2011, April 12nd). L*ey 1480. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones*. Diario Oficial n.° 48.220. http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

Congress of the Republic of Colombia. (2012, October 17th). L*ey Estatutaria* 1581. P*or la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial n.° 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congress of the Republic of Colombia. (2021, October 29th). L*ey 2157. Por medio de la cual se modifica y adiciona la Ley Estatutaria* 1266 *de* 2008, *y se dictan disposiciones generales del Hábeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Diario Oficial n.° 51.842. http://www.secretariasenado.gov.co/senado/basedoc/ley_2157_2021.html

Constitutional Court of the Republic of Colombia. (2000, September 6th). Judgment C-1162 (José Gregorio Hernández Galido, M. P.). https://www.corteconstitucional.gov.co/relatoria/2000/C-1162-00.htm

Constitutional Court of the Republic of Colombia. (2008, October 16th). Judgment C-1011 (Jaime Córdoba Triviño, M. P.). https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Constitutional Court of the Republic of Colombia. (2011, October 6th). Judgment C-748 (Jorge Ignacio Pretelt Chaljub, M. P.). https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

EcuRed contributors. (n/d). I*dentidad*. EcuRed. Consulted on November 28th, 2019. https://www.ecured.cu/Identidad

European Commission. (2021, December 21st). E*uropean Commission*. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

Garcés Bejarano, A. (1966). Del contrato por adhesión en general. *Revista Facultad de Derecho y Ciencias Políticas*, (40), 16-20. https://revistas.upb.edu.co/index.php/derecho/article/view/5851

Mayor's Office of Monteria. (2015, July 12nd). *Resolución No.* 0047. P*or medio del cual se hace reconocimiento a la Liga de Consumidores* UPB M*ontería*.

Momberg Uribe, R. & Morales Ortiz, M. E. (2019). Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos de los Consumidores. *Revista Chilena de Derecho y Tecnología*, *8*(2), 157-180. https://doi.org/10.5354/0719-2584.2019.54441

National Constituent Assembly of the Republic of Colombia. (1991, June 13th). *Constitución Política de Colombia*. Gaceta Constitucional N° 116 de 20 de julio de 1991. https://bit.ly/3kPmJPO

Posada Torres, C. (2015). Las cláusulas abusivas en los contratos de adhesión en el derecho colombiano. *Revista de Derecho Privado, Universidad Externado de Colombia*, (29), 141-182. https://doi.org/10.18601/01234366.n29.07

Presidency of the Republic of Colombia. (1971, June 16th). *Decreto 410. Por el cual se expide el Código de Comercio*. Diario Oficial No. 33.339. http://www.secretariasenado.gov.co/senado/basedoc/codigo_comercio.html

Rodríguez Chávez, R. Y. (2010). La función económica de la contratación masiva. *Revista Oficial del Poder Judicial*, *6*(6/7), 189-228. https://doi.org/10.35292/ropj.v6i6/7.201

Spanish Royal Academy [RAE]. (n/d). *Diccionario de la Lengua Española*. Consulted on December 7th, 2021. https://dle.rae.es

Superintendency of Industry and Commerce of Colombia. (2016, March 31st). *Resolution No. 15339. Por la cual se impone una sanción y se dispone la suspensión de las actividades relacionadas con el tratamiento de información personal*. https://acortar.link/jYvnMd

Superintendency of Industry and Commerce of Colombia. (2017, April). *Radicado* 17- 30407 - 1. https://acortar.link/TiZPz2

Superintendency of Industry and Commerce of Colombia. (2019, July 10th). *Quejas por suplantación de identidad ante la Superindustria crecieron 122%*. https://www.sic.gov.co/Quejas-por-suplantacion-de-identidad-ante-la-Superindustria-crecieron-122

Superintendency of Industry and Commerce of Colombia. (2020, December 14th). *Resolución No. 79845. Radicación No. 20-80545*. https://www.sic.gov.co/sites/default/files/files/2020/Res%2079845%20de%202020%20Cr%C3%A9ditos%20R%C3%A1pidos%20S_A%20VP%20F.pdf

Superintendency of Industry and Commerce of Colombia. (n/d). *SIC Facilita*. Consulted on December 14th, 2021. https://sicfacilita.sic.gov.co/SICFacilita/index.xhtml

Ugarte Godoy, J. J. (1995). El Sistema Jurídico de Kelsen. Sintesis y Critica. *Revista Chilena de Derecho*, *22*(1), 109-118. https://repositorio.uc.cl/handle/11534/14644

United Nations (UN). (1948, December 10th). *Universal Declaration of Human Rights. Resolution 217 A (III)*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations (UN). (1989, November 20th). *Convention on the Rights of the Child. Resolution 44/25*. https://acortar.link/Z9jGyp