



Critical legal analysis of identity theft by electronic means as an independent criminal offense in the Organic Integral Penal Code

Análisis crítico jurídico sobre la Suplantación de identidad por medios electrónicos como un tipo penal independiente en el Código Orgánico Integral Penal

Diana Recalde

Msc. Instituto Superior Tecnológico Universitario Corporativo Edwards

Deming

d.recalde@deming.edu.ec

ORCID: 0000-0002-9758-1870

ABSTRACT

This paper addresses a legal review on the crime of impersonation of tangible identity and the lack of independent typification within the criminal legislation for the impersonation of identity by electronic means; also, a critical analysis of objective tendency on the Ecuadorian legislation on this subject is framed. It is argued with related law studies, which exhibit a criminal review on computer crimes, from a general perspective and without estimating at macro, meso and micro level the scope reflected of an intangible reality of social justice. The constitutional postulates are cited sequentially, in criminal matters and according to the legal procedure the state of this legal problem is visualized; with the purpose of diagnosing the best answers to counteract the effects in the Latin American information society. From the cognitive point of view, other mishaps are compared according to the central theme by way of inspection; giving guidelines, where the potentialities of preparing against cybercrimes with the technological

and socioeconomic adequacy for both public and private entities are evidenced.

RESUMEN

Este trabajo aborda una revisión jurídica sobre el delito de suplantación de identidad tangible y la falta de tipificación independiente dentro de la normativa penal para la suplantación de identidad por medios electrónicos; también, se enmarca un análisis crítico de tendencia objetiva sobre la legislación ecuatoriana entorno a esta temática. Se argumenta con estudios de derecho afines, que exhiben una revisión penal sobre delitos informáticos, desde una perspectiva general y sin estimar a nivel macro, meso y micro el alcance reflejado de una realidad intangible de justicia social. Se cita secuencialmente los postulados constitucionales, en materia penal y conforme al procedimiento legal se visualiza el estado de esta problemática jurídica; con la finalidad de diagnosticar las mejores respuestas para contrarrestar los efectos en la sociedad de la información latinoamericana. Desde el punto de vista cognitivo se compara otros percances acordes al tema central a modo de inspección; dando pautas, donde se evidencia las potencialidades de prepararse contra cibercrimes con la adecuación tecnológica y socioeconómica tanto para entidades públicas y como privadas.

Keywords / Palabras clave

identity, legal security, privacy, cybercrime, legislation, impersonation, social networks, social networks

identidad, seguridad jurídica, privacidad, delitos informáticos, legislación, suplantación, redes sociales

Introduction

The advance of computer technology and its influence in almost all areas of social life, has become a necessary and invaluable value, a value that grows by leaps and bounds, without Latin American legislations being able to criminalize cybercrimes that have arisen from unlawful behaviors that violate constitutionally protected rights in Ecuador and Latin America.

Consequently, the phenomenon of cybercrime, without a clear, precise and complete typification in our legislation specifically, gives room to a

variety of crimes; which, committed in a geolocalized scenario, obtain impunity and as a result we evidence a disproportionate growth of several crimes that further violate the security in our social environment. This problem is part of the present legal analysis, because it identifies the reasons that justify the excessive growth of cybercrimes and at the same time proposes a rethinking of the legal basis of cybercrimes according to the current reality, while making feasible the criminal transformation in Ecuadorian legislation with legal figures adopted, successfully in cybercrime Latin America.

In Ecuador we began to talk about computer crimes in 2009, and the legal system from that year until today in criminal matters has not advanced in the same proportion as cybercrimes. The current Ecuadorian regulations are insufficient; for this reason, a legal improvement is mandatory, so that there is a legal basis to punish the violation of human rights enshrined in the Ecuadorian supreme law.

This perspective includes the analysis and identifies constitutional principles that protect the right to property, honor and good name; reviewing the context of the crime of impersonation of tangible identity, currently typified and penalized in our country, to propose a design in homologation of the same legal criteria for the same crime, but in another scenario; geolocated, extensive and with greater social impact. Objectively, a legal change is proposed, which integrates the global vision of antijuridicity, typicity and criminality of the offenses committed in the virtual scenario, so that they are penalized according to the rules adopted in a legal framework as broad and diverse as the virtual scenario, In this effect, the legal regulations should be correlated with the legislation of Latin American countries, so that the criminal sanctions in Latin American cybercrime are unified as an example of a categorization of this crime in a certain territorial circumscription, despite the fact that we know the geolocation of this type of illicit conduct.

Materials and Methods

For the realization of this article we used academic inputs, information provided by scientific articles, which facilitated the identification of the crime and how constitutional rights are violated by the increasing use of technology and media.

The materials used provided a critical orientation, in the theory and practice of the inductive-deductive, analytical-synthetic, historical and documentary methods, in order to obtain the best result in the research carried out.

The inductive-deductive method was used in the investigated case, with the analysis of the same crime in virtual reality, with the identification of cybercrime through comparative law in Spanish-speaking legislation (Rojas Parra, 2016). The deductive method allowed us to start from the knowledge and structure of the typification of art. 212 of the Organic Integral Penal Code (COIP) to legally recognize the concept, characteristics and consequences of identity theft in real circumstances of time and place and thus conclude with the foundations to establish reforms in congruence to the international provisions of cybercrimes. It is important to point out that the new regulations on computer crimes must recognize the protection of legal assets that are violated, protection to the victims of cybercrime recidivism, and establish mechanisms to establish compensation for damages and losses in order to satisfy the demand for justice in cyberspace.

With the analytical-synthetic method, each of the components of the crime of identity theft was analyzed to achieve the typification and punishment in the COIP

Knowing the virtual problem allowed analyzing this crime as an independent variable, in order to determine its main causes and social and legal consequences and thus conclude with an accurate path to the legal informatics solution that regulates the general conditions of this crime in virtuality.

With the historical-logical method, the concrete trajectory of the theoretical framework on computer crimes, history and characteristics of the crime of identity theft by electronic means were analyzed. The violation of the effective protection and legal security of the rights of property, honor and good name, are part of the rights with greater vulnerability; so this method has allowed us to emphasize in this analysis the adherence to international cybercrime policies; as the safe way to social justice and penal reform in cyberspace.

With the application of the documentary method we processed documents in comparative law, archives, bibliographic material,

information on the evolution of cybercrimes derived from the crime of identity theft; which, being typified in other legislations, according to international treaties provides a sample for the realization of a final report of easy understanding and practical utility in criminal reforms to cybercrime.

Results

A legal specification in the Ecuadorian supplementary legislation.

From the criminal point of view, the typicity, antijuridicity and culpability of the crime of identity theft is regularized in a tangible reality described in the COIP; however, the lack of specification of these elements in the computer part, leads to the omission of such distinction of this crime in an exhaustive manner.

Hence, according to the sample taken from statistics on active users of social networks, in the year 2022 plus the estimated increase of 3% per calendar year, total 4760 million users in the most used social networks in the world (Fernandez, 2022); according to the study conducted by (Hall, 2022), which cites the following pages most frequently in contact with the user: Facebook, Youtube, WhatsApp, Instagram, WeChat, Tik Tok, Messenger, Telegram, Snapchat, Douyin, kuaishou, Sina Weibo and Pinterest. From this information, it is concluded that the utility objectives of these platforms are: entertainment, communication and economic transactions (latam.kaspersky.com, 2023).

On the other hand, the information on the geographical volume of cyber attacks in Latin America (Figure 1) in the same year shows that Ecuador is one of the countries with the highest incidence of cyber attacks. Of the 100% of the graph, Ecuador registers 53%, of cyber attacks; which demonstrates the lack of legal security in our territory, the vulnerability to individual and collective property rights of people in social networks; and essentially the lack of a policy of prevention and increase of this criminal reality (Bestuzhev, 2017).

The crime of cyber impersonation leads to the commission of other crimes such as those affecting the right to property, such as cloning of debit and credit cards, forgery and alteration of documents, fraud and swindles; and, in the part of the affectation of personal rights and against humanity, it facilitates the commission of crimes such as: human trafficking, child pornography, trafficking of undocumented

persons, trafficking of minors, usurpation of functions, terrorism and evasion of justice, among the most relevant crimes.

It is important to point out that justice intends to homologate the sanctions foreseen for the same crimes in a tangible reality, to the virtual reality; without taking into consideration that these crimes are committed in a different scenario and that; without the legal protection, the administration of justice so demanded in our country will not prosper; as well as there is not the same affectation to the legal goods protected in the informatics scenario.

In order for a legal reform to be feasible, it is necessary not only to make known the statistics on the reality of the crime, but also to describe the importance of criteria such as:

20

1.- Ownership over data and right over data, which circulate through social networks, and the context that these data acquire according to the time of validity and the concept of privacy. The personal management of the digital identity and its socio-economic value.

3.- The balance between fundamental rights (Constitution) and public order (criminal law).

4.- Analysis of cybercrimes in Latin American comparative law.

Criterion 1.- Ownership of data and data law

Property, legally defined as the right of every person to use, enjoy, enjoy and dispose of their property according to the law. This right will be protected by the Ecuadorian constitution, so that no one may be deprived or disturbed in the enjoyment of their property but by virtue of a trial that complies with the essential formalities of civil procedure. The conception of the word “right” is wide and varied, however, within the subjective meaning it is conceptualized as the power to do or demand what the law or the authority establishes in our favor, or what is allowed by the owner of a good or service. Natural consequences derived from the status of a person, or relations with other legal subjects, according to the legal dictionary of Cabanellas de Torres (2006).

From the above definitions, we focus attention on the fact of identifying that our personal data belong to a digital identity that becomes important according to time, use and the purpose for which it is delivered; thus we have data, which ordered in frequency from highest

to lowest, are those contained in the digital identification of the pages of social networks (Figure 2). Name, photos, nationality, friends, home address, activities (hobbies, sports, places visited), likes and dislikes, cell phone number, work history, websites visited, passport number, financial information (salaries, bank details, credits), medical information (medical records, health information), correspond to the information shared as part of each user's profile.

Even from the information shared, the question arises: Is this accumulation of data essential and necessary in a particular management? No; was the answer, in relation to the users' experience, according to the survey conducted in 2011 by the European Union (De Miguel, 2024).

21

The excessive load of information is worrying, since it circulates in an open way; without legal restrictions that are subject to a legal regulation homologated to international jurisdiction, where computer crimes are sanctioned, knowing that virtual reality is the place where computer crimes are committed without being able to specifically identify the cyber offender and/or sanction computer crimes and infractions. This includes the crime of identity theft, since that computer space has extended borders without limits and without international regulations to protect the human rights that are actively violated.

At the same time, it is identified that the data belonging to the user in social networks are not susceptible to personal use and enjoyment of the same user; as it was in the beginning, it now belongs to a variety of companies that commercialize data for the benefit of advertising and marketing in order to manage such information for multiple commercial purposes, different from the personal ones. This is because, in the information uploaded by each user, the right of use and enjoyment of this information is also obtained by the social network to which the information was transferred, so to speak. Thus, there is a legal separation, because the domain over the data uploaded by each person is not absolute and even less a global privacy policy has been generated in the use of personal identity for social networks.

Hence the importance of prevention of actions carried out with our personal information, responsibility on self-education in the management of the Internet, knowledge of privacy policies, training on the proper use of technologies that allow setting early warnings in case of risk situations and joining efforts against the impunity of cybercrime.

It is true that as users we are so far from knowing that the information entered to the networks is not deleted in case of disuse, nor is it of our interest to know if this information was at some point stolen, lost or altered and even less we have noticed to check if any emergency notice was made on the above mentioned fact and at this point the social networks are not consistent with the realization of alarms to these negligent and / or illicit facts presented in social networks.

Giving up information in the face of the good service requested should not be the objective of the use of social networks, nor should giving up privacy in exchange for connectivity. Users should analyze the wisdom of filling out unnecessary information fields. The degree of tolerance at the moment of giving up information will establish the difference between the cause and effect of legal problems in the virtual space.

22

Criterion 2- Personal management of digital identity and its socio-economic value Managing digital identity in social networks is a task that involves several conceptualizations such as: knowing that our interactivity with social networks generates a trace, computer footprints that represent a marketable product that is acquired by companies for advertising purposes. By commercializing this information, a breach is created that allows the installation of the famous computer intrusions, thus compromising the security of the data exposed by customers.

We can cite cases such as the intrusion of Epsilon, Sony, City, Expedia and RSA in which the damage is not only economic but also commercial as the credibility of the brand in the world market is damaged, and in relation to the exposed data of customers of business services; for this reason in some social networks privacy policies have been established to provide security to sensitive data in the execution of computer crimes, according to the recommendations of the United Nations, in the magazine Fundación Telefónica (2013).

From this privacy policy it is clear that the user's consent is necessary and important in the management of digital identity, paying special attention to the new criterion of preserving the essential information to work actively within the virtual context. The user must recognize that, in the virtual context, the same protocols used for sensitive information that are commonly used in the tangible social context must be applied.

In conclusion, the value of privacy is in competition with the potential for IT and commercial benefits in the global digital scheme of things, and is removed from real-world social considerations.

Criterion 3- The balance between fundamental rights (Constitution) and public order (Criminal Law), citing additionally legal norms in support of the judicial controversy that sanctions the violation of the right to personal information.

In this criterion, the capacity, responsibility and identity according to the current Constitution, related to the Law of Civil Registry, Identification and Identification, Criminal Code and Criminal Procedure Code are analyzed as the first point.

- Capacity, Responsibility and Identity under the Constitution
All persons of legal age are legally capable, according to the constitution; this capacity entails the responsibility for the actions performed in the human, social, personal sphere; and it is this responsibility; the action that will regulate human relations and in such reason will set parameters of behaviors that allow objectives such as justice, equity, respect, democracy, among others, to be possible for each society.

Hence, identifying the actors of rights and obligations, classifying each individual in society and establishing their characteristics, legally conceptualizes that personality includes specifications such as: name, capacity, domicile, nationality, affiliation, citizenship and marital status, among the most relevant information.

This right is enshrined in the Constitution not only of Ecuador but also worldwide, and is even protected by International Organizations and Treaties (Osorio, 2008), hence, the concept of personal identity is established as “set of elements and circumstances that allow affirming that a person is the one who claims to be or the one who is sought, either by circumstances of civil or criminal order”. It is not simply the set of elements by which a person differs from others, but his experiences, his character and mainly his past are part of the concept of identity.

Identity is a constitutional right recognized in its peculiar reality. People differentiate ourselves according to our attributes, qualities, characters, actions that distinguish us from any other individual, so that the field of law, the concept of identity is broad, because it goes beyond knowing their genetic origin, includes his individual personality, in the social and psychological sense, including refers to the cultural modes of each individual. The right to identity is a personality right because it is a quality, the way each person represents himself/herself to others, in relation to the society in which he/she develops; as such it is a

fundamental right, in essence very personal and in transcendence conceived for life.

At the same time, it is important to mention that the unification of the concept of human person and identity complement each other, so that all the characteristics derive from the genetic material from the zygote, subsists evolving in a natural way as it acquires the forms of embryo, fetus, child, adolescent and adult. In this way, it is stated that the right to personal identity is specific, because it allows to establish the origin of the children with respect to the parents, it is a right that emanates from a natural and undeniable fact that no one can ignore and constitutes the most important relationship of life, its incidence is manifested not only in the family but in the social conglomerate, which allows the configuration of the identity of a person.

24

From the personal identity established as a right, legal responsibility is born as part of the obligation of this person with the society in which he/she develops.

“The elements of the right of identity are: paternity, maternity, physical and moral characters, profession, residence”. This is a right that not only protects children, but also protects the human person from conception to adolescence, adulthood, and in my opinion until senescence and ends with death, hence in all stages of a person's life there will be and will remain the legal protection of his personal actions with society.

Additionally, it is worth mentioning that the Constitution of the Ecuadorian State, art. 66, numeral 19, establishes as a citizen right “the protection of personal data, which includes the access and decision on the information and data of this nature, as well as its corresponding protection. The collection, filing, processing, distribution or dissemination of such data or information shall require the authorization of the owner or the mandate of the law”. This right must also be prosecuted in case of non-compliance in the virtuality.

According to the Law of Civil Registry, Identification and Identification, the right to identity is a legal and obligatory civil act of all persons in order to acquire our own identity. In the Third Title “of the Identification”, Chapter One “of the Personal Identity”, Article 97, textually states: “document that accredits the personal identity. - The personal identity of the inhabitants of the Republic shall be accredited by means of the identity card and citizenship, which shall be issued by the Head Offices of the Civil Registry, Identification and Cedulation

based on the filiation data contained in the records of the Civil Registry...”. In the third chapter of the same legal body, regarding the Identity and Citizenship Card, Article 106, states: “Objective. - The purpose of the identity or citizenship card is to identify Ecuadorians in enjoyment of political rights. This card will also be the appropriate document to exercise the right of suffrage”.

It is important to mention that not only the right to vote but also the other rights that are established in the Ecuadorian constitution, international organizations and human rights. As we can see there are several entities that protect the human identity, for being a fundamental part of human rights and the natural person for being the main axis of a State.

25

The Organic Integral Penal Code in its Book II, Title III, Chapter II, refers to the crimes of: “Usurpation of Functions, Titles and Names”, with respect to this chapter, in each article we find, the criminal types and penalties for those who impersonate the identity of a public official. In the same body of law, Article 239, it states: “False identification. - Whoever publicly takes a name that does not belong to him shall be punished with imprisonment of eight days to three months and a fine of eight to sixteen United States dollars, or with one of these penalties only”.

The protection of personal identity, in our country is also mentioned in the Penal Code, there is an entire chapter dedicated to penalize the usurpation of functions, titles and names, in a tangible reality, but it does not specify anything regarding the impersonation of persons, in the virtual reality.

The Code of Criminal Procedure, regarding the identity of the defendant, according to the regulations applied in the tangibility of the fact, according to art. 168 determines the competence, form and content of the decision, pointing out that the preventive detention can only be dictated by the competent Judge or Judge of Criminal Guarantees, at the request of the Prosecutor or the Prosecutor and must contain:

1. The personal data of the defendant or, if unknown, those that serve to identify him/her;
2. A succinct enunciation of the fact or facts with which he/she is charged and their criminal qualification;

3. The clear and precise substantiation of each one of the premises provided for in the preceding article; and

4. The citation of the applicable legal provisions.

This legal provision must be complied with by the Prosecutor, who requests the Judge to order the arrest of the persons suspected of a crime, however, by not establishing the full name and surname of the alleged offender, the rights of other persons who are arbitrarily detained or deprived of their freedom would be violated, This leads to being immersed in a case of homonyms, harming people's right to identity, causing them great economic expenses and moral damage, which are not compensated by the Prosecutor who requested the order, nor by the Judge, nor the State. Therefore, it is also necessary a legal reform that covers all the regulations regarding the crime of identity theft in the computer media so that the dissipations of the current code of criminal procedure are not distorted in a legal controversy.

Other regulations protecting the right to personal information, right to confidentiality

Art. 6 of the Organic Law of the National System of Public Data Registry declares confidential personal data, such as ideology, political or union affiliation, ethnicity, health status And other data related to personal privacy (...). Access to this data will only be possible with the express authorization of the owner of the information, by mandate of the law or by court order

Article 21 of the Statistics Law provides that “individual data obtained for statistical and census purposes are of a reserved nature (...) individual information of any kind may not be disclosed, nor may it be used for other purposes...”.

Organic Code of the Social Economy of Knowledge, Creativity and Innovation. General Provisions of Title IV, paragraph number twenty-seven. The processing of personal data that includes actions such as the collection, systematization and storage of personal data, shall require the prior and informed authorization of the holder. The authorization of the holder shall not be required when the processing is carried out by a public institution and has a statistical or scientific purpose; for the protection of health or safety; or is carried out as part of a policy to guarantee constitutionally recognized rights (...).

Conclusions

As a consequence of the above, it is important and necessary to reform the criminal law on impersonation in digital media, a legal solution that establishes special dedication to the procedural path with the aim of making the complaints, procedure and consistent demonstration of the evidence correctly viable in order to conclude with an effective sanction to those responsible.

The reform proposed to the crime of impersonation in the cyberspace of social networks should protect essential rights such as security and privacy, taking into consideration that personal information, once it has been massified, becomes a commercial value for large advertising companies, where consumer loyalty is the strategy and our information is just another number.

The security and privacy of personal information are elements of dignity, a legal asset to be constitutionally protected, they share an intrinsic value with the protection of tangible assets, they are susceptible to a non-economic valuation, for this reason it is important for the legal regulations to specify that these fundamental rights of the human being, also participate in the virtual judgment. Example: patents, copyrights, trademarks, business knowledge and trade secrets, are identified as elements of the right to privacy, they entail the protection of dignity and good name; consequently, the protection must frame the protected legal property and not only judicialize the transgressed elements

It is important to validate and delimit the information generated by each user in social networks in order to establish means and ways to prevent computer attacks, considering that current technology also creates more and more limits to this type of actions.

References

- Osorio, Manuel. Diccionario de Ciencias Jurídicas, Políticas y Sociales
https://drive.google.com/file/d/1T_GGBiLa3lUpj9W3M6UwovUKEmwt6tAE/view?pli=1
- Código Orgánico Integral Penal COIP 2014 recuperado
<http://www.asambleanacional.gob.ec/es/noticia/este-10-de-agosto-entra-en-vigencia-ensu-totalidad-el-codigo>

- De Miguel, J. (mayo,2024). Redes Sociales mas usadas y 41 estadísticas <https://www.doofinder.com/es/blog/estadisticas-redes-sociales>
- De Miguel, J. (enero 2023). Redes Sociales más usadas y 41 Estadísticas Actualización 2023
- Fernández, A. (26 de octubre, 2022). Las redes sociales mas utilizadas: cifras y estadísticas. <https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales>
- Fundación Telefónica. (2013). Identidad Digital. El nuevo Usuario en el mundo digital https://www.ufasta.edu.ar/biblioteca/files/2017/02/identidad_digital.pdf
- Hall, S. (enero 2022) Digital Report. El informe sobre las tendencias digitales, redes sociales y mobile
- Rojas Parra, J. H. (2016). Análisis de la penalización del cibercrimen en países de habla hispana. *Revista Logos, Ciencia & Tecnología*, 8(1), 220-231.