**Migration Letters**

Volume: 21, No: S10 (2024), pp. 734-747

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

# Organized Crime And Cybercrime In Ecuador, A New Reality Of Complex Criminality

Jorge Edmundo Paspuel Hernández[1] , Christian Alexander Panchi Criollo[2] , Juan Sebastián Paredes Mera[3] , Marcos Willian Suquitana Segura[4]

## Abstract

*This article analyses the main problems that the computer revolution has brought with it in terms of a new form of committing crimes, in this case the creation of cybercrimes, crimes that have been perfected, allowing criminals to cross borders in a matt[1]er of seconds at a global level and forming part of organized crime. In conclusion, this criminal symbiosis has brought legal problems in terms of its application in criminal practice, especially in our Ecuadorian legislation, where prosecutors and judges are limited in their accusations and when judging organized crime offences related to cybercrime, as their modus operandi and organizational structure are complex. In that sense, this research is descriptive with a doctrinal and legal normative approach, hoping to answer the following research question: what is the scope of criminal liability in cybercrimes within organized crime in Ecuadorian legislation?*

***Keywords:*** *cybercrime, organized crime, legislation, crime, organized crime.*

## Introduction

Society is not static, it tends to modify itself with the passage of time, and with it the positive or negative characteristics that tend to transform at the same time as it advances; In this environment of coexistence, crimes are one of those negative characteristics that already existed a hundred years ago, some of which were repealed by different legislations, for example, it is impossible to think now of homosexuality as a crime, which less than fifty years ago was still typified in some Latin American countries as a crime (Simonetto, 2017), likewise, fifty years ago it was impossible to think that computer crimes would arise within organized crime and that it would bring serious problems in legal and social action, both in Ecuador and internationally.

On this fact, there have been several studies that aim to describe the problem of organized crime and cybercrimes, so it is important to carry out a historical-theoretical description that addresses the evolution of organized crime and its connection with cybercrimes, even more so than today and, above all, in Ecuador which, being in a globalized world, It is not exempt from organized crime in relation to cybercrimes, accepting that it is a problem not only in the country but also at a transnational level, which makes it a complex type of crime for the administration of justice, especially when there

[1]magíster Profesional En Derecho Con Mención En Estudios Judiciales Instituto De Altos Estudios Nacionales Quito Ecuador **Https://Orcid.Org/0009-0009-0095-8175**
[2]magister En Derecho Mención Estudios Judiciales, Especialista En Compras Publicas Instituto De Altos Estudios Nacionales Https://Orcid.Org/0009-0005-5593-3144
[3]magister En Derecho Con Mención En Estudios Judiciales Instituto De Altos Estudios Nacionales. Iaen Manta - Manabi - Ecuador. Https://Orcid.Org/0009-0002-4039-3139
[4]magister En Derecho Con Mención En Estudios Judiciales Instituto De Altos Estudios Nacionales. Iaen Esmeraldas - Ecuador. Https://Orcid.Org/0009-0001-1318-0798

are no specialized experts, nor is there an effective system that can obtain the necessary evidence to determine the crime.

This research is related to organized crime that emerged in the early 30's in the United States, so the first study carried out was by "John Landesco himself who published in 1929 a study called Organized Crime in Chicago", being the first formal study that deals with organized crime, but it has been a deep topic of study in recent decades. due to its spread and the need to understand what its characteristics are, and from a general perspective organized crime, according to the United Nations or the countries that make up the G8, use the expression to refer to a series of serious crimes that are especially difficult to control within a collective participation in production, the provision, financing of markets for illegal goods and services. As for the new technologies or information and communications technologies (ICT), their appearance and implementation in society began the emergence of cybercrimes, in the 70s computer crimes or cybercrimes such as computer espionage, software piracy, sabotage and computer extortion became visible. crimes mostly of an economic nature, which are gradually acquiring an evident notoriety in the world, and which have been modifying their actions until today, which causes many of the human activities to be in the sights of cybercrime, the patrimony, the sexual and reproductive integrity of minors in child pornography, black market for the illicit sale of goods and services, among others, but these cybercrimes have been organized at a transnational level, becoming organized crime structures. (Figueroa, 1999, p. 209) (Donzella, 2022)(Martínez, 2015)(Sain, Revista Pensamiento Penal, 2023)

The purpose of this article is to show a tour of the evolution of traditional organized crime that has had a development and development in its own modus operandi, updating its actions to the available services of technologies with reference to the Internet, which has facilitated the development of criminal actions by having access to more sophisticated equipment. or as cybercrime is known, and thus establish what have been the problems faced by the Ecuadorian justice system where it was tried to give a scope to the definition and typification by the legislature of organized crime, establishing it as a crime. This article is descriptive, so the methodology used includes a qualitative approach, a doctrinal and normative legal mode, normative documentary identification techniques, primary and secondary data collected from the doctrine of expert authors in the field.

The structure of the article is divided into: a first part in which the origin and evolution of organized crime worldwide is analyzed. The second part discusses new technologies and the emergence of cybercrime. In the third part, a relationship that arises between organized crime and cybercrime is made. In the fourth part, results and a brief discussion are presented with ideas that address the previous bibliographic study, and at the end some conclusions are elaborated that answer the research question posed.

## Organized Crime

Dealing with organized crime is nothing new in the punitive sphere of crime, but the truth is that such criminal behavior has known how to take advantage of all the opportunities that modern society offers and use them to its advantage with the aim of obtaining benefits. This is how organized crime has been studied from different perspectives, thus occupying some definitions by different authors, but the particular one that maintains aspects such as the desire for profit as a determining central aspect of the activity, a structural organization and permanence over time. Organized crime has been a social phenomenon that is recurrent worldwide, but this criminality occurs under different manifestations, so we have that there are perspectives of organized crime in a violent way, to others that are more sophisticated, and that generates that the perspective of organized crime is looked at from a different perspective. (Zurita, 2017)(Rincón, 2018) (Sánchez, 2012)

According to Rivera (2011), Organized Crime is due to a series of factors, the first factor is due to the globalization of the economy, since technologies have facilitated the exchange of goods and services more quickly, but at the same time it can be used as a means of crime; the second factor is due to illegal immigration that in recent decades has increased drastically. what causes human trafficking; and the third factor refers to the technological advance that allows communication between different borders, being a means used by criminals to commit cybercrimes.

Today, criminal organizations have been characterized by competing among themselves, in addition to creating different collectives to be able to extend their power beyond their own borders, that is, if we start from the notion of organized crime, which always has as a means the generation of violence in different facets, with the aim of achieving economic gains, political and social (Cinosi, 2022). From another perspective, within organized crime, criminals associate with other criminals in order to achieve a certain power and spread to different parts of the world; In this sense, organized crime becomes transnational when, through more than one association of people who have and share a common interest in the same territory, they have decided to expand to other parts of the world, which leads to an operation on a global scale, and they do so through transnational connections.(Andrade, 2019)

The existence of organized crime and its transnationalization at a global level led to the signing of the Convention against Transnational Organized Crime in December 2000 in the city of Palermo, Italy. since crime was beginning to cross the different borders and, therefore, the same action should be implemented in the different legislations of the States parties. If the rule of law is undermined not only in one country, but in several countries of the world, it will not simply be possible to act in a limited way and only with the means and discretions of each country, so the Palermo Convention aimed to defend human rights and fight organized crime. corruption and trafficking in persons, of those enemies of progress and human rights who seek to benefit illicitly from the possibilities offered by globalization. (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2004)

Article 5 of the United Nations Convention against Transnational Organized Crime defines the criminalization of participation within an organized group, and mentions the following:

> One or both of the following conducts as offences other than those involving the attempted or consummation of the criminal activity: (i) Conspiracy with one or more persons to commit a serious offence for a purpose that is directly or indirectly related to obtaining an economic or other material benefit; where required by domestic law, involving an act perpetrated by one of the participants in carrying out such an agreement or involving the involvement of an organized criminal group; (ii) The conduct of any person who, knowing of the purpose and general criminal activity of an organized criminal group or its intention to commit the offences in question, actively participates in: Illegal activities of the organized criminal group; b. Other activities of the organized criminal group, knowing that their participation will contribute to the achievement of the criminal purpose described above. (b) Organizing, directing, aiding, abetting, facilitating or advising for the commission of a serious crime involving the participation of an organized criminal group (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2004, pág. 7)

In Ecuador, organized crime is defined in article 369 of the Organic Comprehensive Criminal Code, which states that:

> A person who, by agreement or concertation, forms a structured group of two or more persons who, permanently or repeatedly, finance, in any way, exercise command or direction or plan the activities of a criminal organization, with the purpose of committing one or more offences punishable by imprisonment for more than five years, whose ultimate objective is to obtain economic or other material benefits, shall be punished by imprisonment for a term of seven to ten years. The other collaborators will be punished with imprisonment of five to seven years (National Assembly of Ecuador, 2014, p. 144-145).

There is a difference between the regulations of the Organic Comprehensive Criminal Code (COIP) and what is established in the United Nations Convention against Transnational Organized Crime (UNTOC), since the UNTOC makes a distinction between what is understood as an organized group and when participation within an organized group should be penalized, which is how according to the UNTOC in its article 2 determines that an organized group must be made up of three or more On the other hand, article 5 determines the penalty for participation within an organized group, and this participation occurs with one or more persons with the intention of participating and not necessarily forming an organized group. which are different issues. (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2004)

From this differentiation, it is observed that the COIP does not first maintain the number as determined by the UNTOC, it does not make the distinction between participation and membership of an organized group, which could generate problems when determining criminal responsibility, since the organization is formed according to the UNTOC with three or more people.

Another problem of the COIP is that it does not make a correct distinction between organized criminal group and structured group, which could have repercussions on judicial processes, the UNTOC defines the structured group as "a group not formed fortuitously for the immediate commission of a crime and in which its members have not necessarily been assigned formally defined functions nor is there continuity in the status of member or there is a developed structure", On the other hand, the COIP determines that the structured group must be permanent or repeated, since one of the current problems faced by the administration of justice is precisely the permanence that must be had to be considered part of the structured group when, according to the UNTOC, it is not necessary. (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2004, pág. 5)

## Cybercrime

The emergence of New Technologies and Communications (ICTs) has led to a new form and means of action for criminals, with a particularity that, being a new means of committing crimes, there is a lot of ignorance that becomes a characteristic of facilitating impunity, allowing technology to be a means of committing traditional crimes in a non-traditional way. From anywhere in the world and at any time, this is due to the entry of information and digital technology into all aspects of social, family and individual life, influencing new automatic, anonymous and decentralized personal and social risks that demanded the study of computer crimes, converted into a new paradigm of criminality. (Blano, 2023) (Fiscalía General del Estado, 2021)

Cybercrime comes from a totally Anglo-Saxon term that is Cybercrime, being a concept that has evolved along with the advance of new information and communication technologies, has influenced the modification of the way of thinking and human behavior of the new generations, and with it a new conception of crime. In this sense, the crime has not only changed from a tangible physical place to a cyberspace, but it has also generated a problem when it comes to punishing them with traditional methods, since, when they

enter the internet, it becomes a gray area that puts into debate the traditional principles of territoriality, legality and culpability. (Ochoa, 2021)

The term cybercrime is relatively new, as it appeared in the late 1990s, in the face of the spread of the Internet, specifically in France, where the "G8" was founded[2] The purpose of this study was to study the difficulties arising from criminality associated with the use of the Internet, and the definition of computer crime was initially used to describe crimes committed on the Internet or in telecommunications networks. (Zambrano, Dueñas, & Macías, 2016)

The first filter of difficulty is found in the conceptualization of cybercrime or computer crime, since it has not been easy to consider what should be understood by cybercrime, what are the behaviors that can be included, even the doctrine has different variations in the concept and there is no unitary concept, the discrepancies around it have even led some authors to admit the impossibility of giving a definition of cybercrime. But it will be a question of approximating a definition. (Hernández, 2009)

For Salom (2023), cybercrime can be understood as "a concept that we use socially to refer to a set of behaviors that violate the rights of third parties and occur in a technological scenario or medium, causing social rejection and on which criminal law mediates" (p.135).

For Corcoy (2007), computer crime, according to the sector of criminal doctrine, is "only a way of carrying out different types of crime. Consequently, the legal asset protected in computer crime will be the one protected in the crime that has allegedly been committed" (pp. 9-10), that is, it can be any protected legal asset such as patrimony, public administration, intimacy, privacy, sexual freedom, among others.

According to the United Nations Office on Drugs and Crime (2022), cybercrime is defined as:

> Cybercrime is a complex concept that encompasses a variety of illicit activities that target or use ICTs to commit crimes. Crimes considered cybercrimes are those facilitated by or based on cybernetics. Cyber-facilitated crimes are traditional crimes facilitated (in some way) by ICTs. In the case of cyber-facilitated crime, ICTs play a key role in the method of operation (the modus operandi) of the offender(s). By contrast, in cyber-based crimes, which include those that can only be committed using computers, computer networks or other forms of information communication technology, ICTs are targeted for such crimes. (p. 8)

Another approximation of definition is that cybercrime is the performance of a conduct, which meets certain characteristics that fit the concept of crime, and that is accompanied by the use of a computer element, either hardware or software, that is, only referring to the commission of crimes where a computer element intervenes and that can undoubtedly fit within the Criminal Law. And this means that even traditional crimes such as fraud can be committed by computer means. (Sain, Martínez, Temperini, & otros, 2018)

Some of the cybercrimes that the COIP has typified are: child pornography, punishable by imprisonment of 13 to 16 years; Violation of the right to privacy punishable by deprivation of liberty for a term of one to three years; Unlawful disclosure of database information punishable by imprisonment of one to three years; Interception of

[2] A group of eight countries (France, Canada, Germany, Italy, Japan, the United Kingdom, the United States and Russia, were the original members) that meet to discuss economic, political and global security issues, these meetings address a range of topics from international trade to climate change and international security cooperation (Bullard, 2007, p. 9).

communications punishable by imprisonment for a term of three to five years; Pharming and Phishing punishable by imprisonment of three to five years; Computer fraud punishable by imprisonment of three to five years; Attack on the integrity of computer systems punishable by imprisonment of three to five years; Offences against legally reserved public information punishable by imprisonment for a term of three to five years; and, non-consensual access to a computer, telematic or telecommunications system with a penalty of imprisonment of three to five years; but they are not exempt from the fact that other criminal offences can be applied through a computerised means such as human trafficking, organ trafficking, drug sales, extortion, money laundering, among other criminal offences (National Assembly of Ecuador, 2014).

> Cybercrimes and cybercrimes in the broadest sense constitute a new and dangerous paradigm of criminality that we must combat with all the tools offered by the model of a social and democratic state based on the rule of law. A new criminality that has not only shown the existence of new social risks, but, in the legal field, has been transforming the theory of crime, professional practice, and invites us to rethink most of the fundamental structures of modern criminal investigation and procedure. It is clear that this type of crime cannot be accredited or demonstrated using ordinary investigative techniques in the obtaining, collection, packaging, etc. of the evidentiary material elements and relevant evidence that now, for the most part, is of a computer or digital nature. (Fiscalía General del Estado, 2021, págs. 31-32)

Certainly, cybercrimes or computer crimes have been extended to other types of criminal offences, in this sense, illicit behaviours linked to computer systems can be many and heterogeneous, since the possibilities opened up by cyberspace are infinite and offers users a multiplicity of options to commit crimes either individually or in groups. Cyberspace has transformed the commission of crime, allowing the improvement of new criminal behaviors and human behaviors that differ from the physical world, a reality that is palpable in the problems of Ecuadorian justice. (Hernández, 2009) (Ochoa, 2021)

**Organised crime and cybercrime**

With regard to Organized Crime, it is essential to conceive that some crimes, due to their complexity and their varied circumstances, cannot be committed by people acting alone, since the essence of the crime and the scenario requires collaboration, such collaboration can be counted on by associated individuals willing to do what is necessary to form a group that commits such a crime; In this sense, it can be argued that this group is a criminal structure, in which there will be a division of labor where the people who make up this structure have to perform different functions of collaboration with a view to the commission of the crime, also with a characteristic, that this structure remains over time and commits more crimes. This last circumstance is important if the network does not remain alive beyond a single or limited criminal opportunity, if its members do not organize themselves to continue committing crimes, if they do not consider themselves a criminal organization and if the network does not develop it, a permanence, a reputation, a continuity, it is not a genuine criminal organization. rather, it refers to a structured group that falls within the scope of article 5 of the UNTOC, in which case the act must also be punishable, if it is recognized in the domestic legislation of each country.(Rivera, 2011)

Within organized crime, a new modus operandi based on cybercrime has begun to develop, in which cybercrime is growing at a very accelerated rate, with new trends emerging continuously. Cybercriminals are becoming more agile, exploiting new technologies at breakneck speed, adapting their attacks using new methods, and cooperating with each other in ways never seen before. Criminal networks operate on a

planetary scale, coordinating complex attacks against their targets in a matter of minutes. (Donzella, 2022)

Information and communication technologies (ICTs) have certainly played an important role in the transformation of organized crime, as their influence is notable on the activities carried out by organized crime and the people who may be involved in it. The previous references demonstrate that transformation that includes changes within criminal organizations, being today a reference to the commission of crimes and the modes of operation that they have to use, in addition to the variety of people who can be participants in organized crime.

ICTs have transformed the way certain groups are structured and organized. They eliminate the need for face-to-face contact and make it possible for people who have never met to collaborate closely and coordinate their activities from anywhere in the world. Criminals who participate in these groups may collaborate in illicit activities and objectives using nicknames; Thus, the risk of revealing their identities and locations to other members of the group is relatively low, while at the same time causing a series of difficulties for the judicial and police authorities of the different countries, making it difficult to determine the perpetrator and the place where it is committed. (Oficina de las Naciones Unidas contra la Droga y el Delito, 2022)

It must be understood that organized cybercrime includes cyber-related crimes that are perpetrated by an organized criminal group or those who participate within such a group. According to the United Nations Office on Drugs and Crime (2022), organized cybercrime comprises the following:

> … organized cybercrime, an unlawful act must have a cyber dimension (it must be a cyber-facilitated crime or a cyber-based crime) and involve either the involvement of an organized criminal group (as defined in article 2 of the United Nations Convention against Transnational Organized Crime) or an offence established in accordance with article 5 of the Convention (i.e. conspiracy or criminal association) (p.3)

According to the UNODC, two types of crimes can be configured within organized cybercrime: organized crime based on cyber, where it is impossible to consummate this crime without ICTs, and in this type the confidentiality of users, the integrity of data, availability of computer systems and data is targeted; and, organized crime facilitated by cybernetics, in which are collected those crimes that are traditional, but that use ICTs to consummate crimes, among those are computer-related forgery, fraud and fraud, identity theft, extortion, crimes of sexual abuse and exploitation of children, trafficking in persons, smuggling of migrants and illicit goods, Money Laundering and Gambling. (Oficina de las Naciones Unidas contra la Droga y el Delito, 2022)

Within this type of crimes, problems arise, the first is due to the fact that they are committed in cyberspace, in which they are easily committed, they can be committed in a jurisdiction of a country without being physically present in the territory subject to it, in addition to the fact that they can benefit from the punishability that may exist for being in a territory different from the consummation.(Pons, 2017)

According to the Attorney General's Office (2021) in Ecuador, cybercrimes within organized crime maintain some problems, one of the problems is the time that it can last in the preliminary investigation stage within the criminal process, its duration can extend up to two years in said phase, in which the Prosecutor's Office, being the owner of the criminal action, is in charge of directing the pre-procedural and criminal procedural investigation, having as an auxiliary body the Judicial Investigative Police and with the possibility of having specialized professionals (civil investigators), who will act as experts within the investigation, but despite having such collaboration, there are not enough experts specialized in the area of cybercrimes within organized crime.

The second problem faced by Ecuador is the implementation of the special techniques of vital importance for the investigation of organized crime, provided for in the United Nations Convention against Transnational Crime of Palermo of 2000, the development of which in our domestic law was urgent because Ecuador is the only country in Latin America where they do not exist. and these special investigative techniques for this type of crime are as follows:

> Covert operations.- These consist of trained agents getting involved or entering criminal organizations while concealing their official identity, with the aim of identifying the participants, gathering information and collecting the necessary elements of conviction that effectively contribute to the investigation (Attorney General's Office, 2012, p. 5).
>
> Controlled delivery.- It consists in authorizing and permitting illicit or suspicious shipments or remittances of instruments that have served or could be used for the commission of crimes; the effects and proceeds of illicit activities and controlled substances; or instruments, objects, species or substances by which they have been totally or partially replaced, moved, stored, intercepted or circulated within the national territory, exit, transit or enter it, under the supervision or control of the competent authority, for the purpose of identifying and identifying the persons participating in the execution of such acts, to know their plans, to avoid the illicit use of the species referred to or to prevent and prove crimes (Attorney General's Office, 2012, p. 5).
>
> The informant, the effective cooperator. - Provision is made for the formation of joint investigation teams between one or more countries, subject to international criminal assistance standards, as well as the Mutual Legal Assistance System (Attorney General's Office, 2012, p. 5).

The third problem faced by Ecuador with regard to cybercrimes within organized crime is the lack of distinction maintained by the COIP in its article 369 between an Organized Criminal Group and a Structured Group, in addition to the determination that in order for criminal conduct to fit as organized crime, it must meet one of the two requirements. This is that this organization is permanent over time and the other that the purpose of committing crimes is carried out repeatedly.

Both the Organized Criminal Group and the Structured Group have as a common denominator the union or grouping of people and with the objective of committing crimes, but there is the differentiation that the Organized Criminal Group requires stability or constitution for an indefinite time, in addition to a distribution of defined tasks or functions and permanence as a member. On the contrary, the Structured Group lacks temporality, lack of designation of functions of the members, i.e. lack of structure, lack of permanence as a member, and this distinction is important to respond to the analogous phenomena that can spread in society but that do not meet all the structural requirements properly understood by the Palermo Convention. For them, the Structured Group as a form of criminal concentration that does not fit into the archetype of the aforementioned organizations, but they do provide a plus of criminal dangerousness to the actions of their components. In this way, it can be understood that "the classification of the criminal group arises because they can commit serious or violent crimes and to this must be added the actions of their components that constitute the extra dangerousness, although they do not have a structural and organized character". (Zurita, 2017, pág. 161)

From this perspective, a problem can be observed in terms of the classification of Organized Crime established in Article 369 of the COIP, since the criminal classification does not make a distinction between Organized Crime Group and Structured Group, and the requirements for Organized Crime to be proven are first the constitution of the group

of at least two people, that this group has stability, maintains a structure in which there is a distribution of functions or tasks, in addition that it maintains permanence, that is, that it has a temporality of formation of the group and another requirement is that the action with the purpose of committing crimes is repeated, although the same article is also contradicted since it then mentions that the group must have the purpose of committing one or more crimes, In other words, there is no clear delimitation.

With these considerations that the legislator has contemplated within the criminal category of Organized Crime, those Structured Groups would be excluded, since they can be sporadic since they cannot have stability or temporality, lack of specific distribution of tasks or pre-established structure of division of functions, there is no permanence as a member, nor does it maintain a reiteration for the commission of crimes, which would cause problems when trying to establish criminal responsibility of the participants, let's take the following example: Juan, Pedro and José form a group, the purpose is to be able to sell child pornography, it is the first time they form the group and they want to commit such a crime, it does not have a clearly established division of labor.

Based on the example established, if the prosecution wishes to charge for the criminal type of Organized Crime as determined by Article 369 of the COIP, it would not meet the objective elements of the criminal type, because first: although there is a formation of a group with the objective of committing a crime, that group is sporadic, There is no repetition in committing crimes, there is no permanence as members of the group because it is new, there has been no permanence in the formation of the group over time, and therefore they could not be accused or tried.

In addition to this problem that Ecuador faces with organized cybercrime, there are other problems that aggravate the situation, since there is not enough specialized contingent for the investigation of crimes, there are not enough specialized experts and the due protocols mentioned above, since in addition to this it must be faced that in such organized cybercrime the people who participate in this organized structure are in different In parts of the country as well as the world, the problem of territoriality is another factor influencing the problem that further deepens the administration of justice.

## Methodology

The methodology to develop this research work maintains a qualitative approach, with a descriptive scope that will design the study using the bibliographic technique from the doctrine with tools such as academic articles, legal reports, legal regulations, books, manuals, among other documentary instruments that are fundamental for the understanding and answer of the research question posed.

## Results

The results presented in this research are based on the bibliographic review based throughout the academic study presented in the previous section, hence the following results are shown:

1. That cybercrime is an international crime partially defined by its different and partially unknown modalities of commission, which makes cybercrime a recent phenomenon, very little explored and especially in cases where criminal individuals associate to form organized crime groups to consummate the varied crimes that may exist in cyberspace.
2. That there are criminological investigative techniques that can be studied in depth in order to gather a much more complete knowledge about the modality of cybercrime in organized crime operations. Although this is relatively new, it is possible to start with the bibliographic research that has been gathered by experts in countries where the legislation that punishes cybercrimes covers the different variations of crime in a slightly more complete way.

3. Criminal responsibility in crimes that originate from cybercrime in which organized crime groups operate is a source of uncertainty because the terms that are based on organized crime are not structured as demanded at the international level, differentiating between groups, associations and other concepts. Another situation is one in which the criminal type of computer crime depends on the criminal type already determined, which means that cybercrime does not exist as such in the criminal regulations, even more so that it is not configured with organized crime crimes, so within an investigation it is not possible to determine the criminal responsibility of one of these groups with a computer crime.

## Discussion

In this section, notions will be discussed that are based on the results presented that arise from the bibliographic study carried out in this research, for this, in addition to providing critical and personal ideas about the research, it is necessary to contrast it and set up an argumentative and academic debate with the opinion of different authors from the positions of each idea developed. In this sense, the following premises are presented:

### The Contemporary Phenomenon of Cybercrime

Based on the bibliographic study, it is evident that cybercrime has become a relatively new phenomenon. Appearing with the birth of the internet, it is known that the first cybercrime occurred between 1988 and 1991 when Kevin Pulsen consummated the crime of falsifying documents such as birth certificates, citizenship IDs, then it is known about the famous Trojan virus in 1989, a virus that posed as a benign computer program that in the end ended up destroying the entire database of an operating system (OGDI, 2024).

It is important to place this context, because from here a succession of different events have developed within cyberspace where different types of crimes are consummated, starting from forgery to the alteration of computer systems or even generating videos where crimes are committed that threaten people's lives.

Authors such as Wall (2007) argue that cybercrime is a complex global phenomenon that challenges national and traditional boundaries, argues that the rapid evolution of technology has outstripped the ability of legal and law enforcement systems to keep pace and in new places, resulting in a significant gap between online crime and regulatory responses.

This generates a discussion about the changing nature of cybercrime, Broadhurst and Grabosky (2014) have discussed this issue and its impact on the way criminal organizations operate, they argue that digital technologies have allowed the creation of global criminal networks, which take advantage of the speed, reach and anonymity of the internet to commit financial crimes, identity and other issues.

Which is pretty spot on in terms of adjusting to reality. The documentary study presented understands that cybercrimes need to be addressed from a multidisciplinary approach, that the total understanding of this phenomenon requires collaboration between law, criminology, computer science and other disciplines such as sociology, the development of these perspectives is essential to increase effective prevention and law enforcement strategies.

The challenges that arise and are associated with cybercrime include jurisdiction, extraterritoriality and privacy in a very general way, Brenner (2010) analyzes that these are the legal challenges that must be taken into account for the prevention and enforcement of regulations, Kerr (2012) agrees with Brenner understanding that the cross-border nature of

cybercrime poses these challenges that are significant for the law to be applied in the different contexts and Countries.

**Criminological Techniques for Investigating Cybercrime in Organized Crime Groups**

Criminologists and researchers can collect and analyze digital data to identify patterns of illicit activities and dismantle online criminal networks, Brenner (2010) provides an overview of techniques that are applied to cybercriminals, and that can even be used to dismantle networks of organized criminal groups, this author calls them online scams because, The criminal investigation technique addresses more the knowledge of how to understand the form of digital scams, a topic that is quite well known today.

To understand criminological research techniques, it is necessary to understand the behavior of the criminal, which is why Jaishankar (2011) had already been investigating it, from an exhaustive analysis of behavior on social networks to the mining of digital data, understanding that on many occasions internal criminal groups are generated that incur in illegal activities

Holt and Bossler (2013) examine in detail the forensic investigation techniques used to track and attribute cybercrime to organized crime groups. Holt and Bossler discuss the specific challenges investigators face in collecting and preserving digital evidence, as well as strategies to overcome these barriers in the law enforcement process. These techniques include digital forensics, which refers to the examination of electronic devices and networks; social network analysis; cyber intelligence, which includes monitoring underground forums, dark web sites, and encrypted communication channels that are often used by organized crime groups.

**Criminal Liability of Organized Crime Groups Operating in Cyberspace in Ecuadorian Law**

In a legal context, the legal and legal challenges in the criminal liability of organized crime groups operating in cyberspace have been discussed in Ecuadorian law and it is argued that current laws may not be sufficiently updated or specifically designed to address the complexities of cybercrimes committed by criminal organizations (López, 2022).

The criminological approach analyzes the criminal responsibility of organized crime groups in cyberspace in Ecuador, explores how power dynamics, organizational structure and economic incentives influence online criminal activities and how these can be addressed from a criminological perspective in the legal field, however, it is argued that criminal responsibility maintains an insufficient scope in this area because very little is known.

Making a brief international comparison, where notable differences are found between jurisdictions. For example, the United States has a wide range of federal and state laws that address cybercrime, including the Computer Fraud and Abuse Act and the Espionage Act. The main difference with Ecuador could lie in the availability of resources and technical capacities to investigate and prosecute these crimes, as well as in the more robust international cooperation in the fight against cybercrime (Montenegro and Recalde, 2018).

The Netherlands is known for having a strong legal and technical infrastructure to combat cybercrime. They have established specialized law enforcement teams and prosecutors dedicated to investigating cybercrimes, which could contrast with the situation in Ecuador, where resources and training may be more limited (Pérez, 2021).

The main difference between Ecuador and these countries probably lies in the resource capacity, legal infrastructure, and international cooperation in the fight against

cybercrime. While some countries may have more advanced systems and more robust resources, Ecuador could face challenges in terms of updating legislation, availability of technical and financial resources, and international collaboration in prosecuting cybercrimes perpetrated by organized crime groups.

From a personal perspective, it is evident that Ecuadorian law faces significant challenges in the criminal accountability of organized crime groups operating in cyberspace. While there has been progress in enacting laws related to cybercrime, there is still a gap in terms of adapting to the rapid evolution of online criminal technologies and tactics.

A key criticism is the need for greater clarity and specificity in laws related to cybercrime, including the precise definition of the roles and responsibilities of organized crime groups in cyberspace. In addition, greater collaboration between legal authorities, law enforcement agencies, and other relevant actors is required to effectively address these challenges.

It is critical that Ecuador continues to review and update its legal framework to keep up with new online threats and ensure that organized crime groups operating in cyberspace are held accountable for their actions under the law. This will require a comprehensive approach combining legal, technological and international cooperation measures.

## Conclusions

There is no doubt that information and communication technologies (ICTs) have had a great impact on modern society, becoming indispensable in all areas of social life, but at the same time this resource has brought with it a means for the commission of crimes that has developed to the point of being implemented by organized crime worldwide. Therefore, justice and legislation must adapt to this new modus operandi to avoid impunity, i.e. justice must be updated and legislation must adapt to the social changes that occur.

It is evident that the commission of crimes has been transformed, the physical presence of the offender is not necessary for him to consummate the crime, since it now has cyberspace, a place where new crimes have been created and the modus operandi of traditional crimes has been changed, using the network as a means of perpetration. Therefore, it is essential to have people specialized in the field as experts who help against the fight against this type of crime and find the whereabouts of the perpetrators.

Organized cybercrime at the global level presents problems, such as the territoriality of the consummation of crimes, since criminals can cross borders in a matter of minutes without being detected, making specialized international cooperation between the member countries of the United Nations indispensable.

In Ecuador, the poor classification of organized crime and the lack of personnel causes impunity in criminal groups, article 369 of the COIP must be reformed in accordance with the parameters established according to the Palermo Convention of 2000, the types of organized crime are not defined, so an adequate classification of organized cybercrime by the legislative power is urgent.

In other words, the scope of criminal responsibility for cybercrimes perpetrated by organized crime groups is a complex and insufficient area in several respects. Because, in this context, it is influenced by a number of factors, including the ability of existing laws to address cybercrime, the effectiveness of law enforcement agencies in investigating and prosecuting these crimes, and international cooperation in the fight against cybercrime. In

this sense, it could be argued that the scope of criminal liability in cybercrimes within organized crime in Ecuadorian law is not sufficient to fully address the problem.

## References

Andrade, X. (2019). General Guide on Corruption and Organized Crime. Madrid: El Pacto.

National Assembly of Ecuador. (2014). Organic Comprehensive Penal Code. Official Gazette Supplement No. 180 of February 10, 2014, latest reform of the Official Gazette Second Supplement No. 496, of February 9, 2024.

Blano, J. (2023-05-03). Organized crime and new technologies. Retrieved from El Fisco: http://elfisco.com/articulos/revista-no-151-el-crimen-organizado-y-las-nuevas-tecnologias

Brenner, Susan W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.

Broadhurst, Roderic, & Grabosky, Peter. (2014). Cybercrime: The Transformation of Crime in the Information Age. Routledge.

Bullard, N. (2007). G8 Club Governance. Power and Politics in a Global World. Critical currents no. 1. https://www.researchgate.net/publication/282440703_G8_Club_Governance_-_power_and_politics_in_a_global_world

Corcoy, M. (2007). Problems of the criminal prosecution of so-called computer crimes: particular reference to criminal participation and the spatio-temporal scope of the commission of the acts. Barcelona: Eguzkilore.

Donzella, B. (2022). Organized crime in the digital world. Valencia: Universidad Europea de Valencia.

Figueroa, R. (1999). Money laundering in Mexican criminal law. Mexico: UNAM.

Attorney General's Office, F. (2021). Cybercrimes. Quito: Scientific Journal of Legal Sciences, Criminology and Security.

Grabosky, Peter, & Smith, RG. (1998). Crime in the Digital Age: Controlling telecommunications and cyberspace illegalities. Transaction Publishers.

Hernandez, L. (2009). Computer crime. San Sebastián: Eguzkilore.

Holt, Thomas J., & Bossler, Adam M. (2013). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. Routledge.

Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.

Kerr, Orin S. (2012). Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes. University of Chicago Law Review, 79(2), 591-646.

Lopez, J. (2022). On the scope of the purposes of punishment in the criminal phenomenon of cybercrime. Chilean Journal of Law and Technology 11(1), pp. 121-146. DOI: http://dx.doi.org/10.5354/0719-2584.2022.60913

Martinez, J. (2015). Multidisciplinary security strategies to prevent organized crime. Barcelona: Universitat Autònoma de Barcelona. .

Montenegro, B., & Recalde, G. (2018). Computer crime in America. Revista digital de Ciencias Jurídicas UNIANDES 1(1), pp. 3-14.

Ochoa, A. (2021). Global Challenges of Cybercrime. Quito: Universidad Andina Simón Bolívar.

United Nations Office on Drugs and Crime, O. (2004). United Nations Convention against Transnational Organized Crime and its Protocols. New York: United Nations.

United Nations Office on Drugs and Crime, U. (2022). Compendium of Organized Cybercrime. Vienna: United Nations.

Perez, J. (2021). Cybercrime: towards the new -virtual- reality of criminal law. International Journal of Doctrine and Jurisprudence, pp. 175-193.

Pons, V. (2017). The Internet, the new era of crime: cybercrime, cyberterrorism, legislation and cybersecurity. Quito : Revista Latinoamericana de Estudio de Seguridad - FLACSO.

Rincón, D. (2018). Corruption and State Capture: Criminal Liability of Public Servants Who Take Part in Organized Crime. Bogotá: Revista Prolegómenos - Derechos y Valores.

Rivera, J. (2011). Organized crime. Guatemala: Institute for Security Studies.

Sain, G. (2023-05-05). Revista Pensamiento Penal. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf

Sain, G., Martinez, M., Temperini, M., & others. (2018). New criminal offences in the internet age. Buenos Aires: Erreius.

Salom, J. (2023-05-01). Cyberspace and Organized Crime. Retrieved from Dialnet: Dialnet-TheCyberspaceAND OrganizedCrime-3837304%20(1).pdf

Sanchez, C. (2012). On the concept of organized crime. Significance of its content in Salvadoran penal legislation. El Salvador: Police and Public Security Magazine.
Simonetto, P. (2017). Homosexual liberation movements in Latin America. Historiographical contributions from a comparative perspective between Argentina, Brazil, Chile, Colombia and Mexico (1967-1982). Revista Iberoamericana XVII, 65, pp. 157-177.
Wall, David S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
Zambrano, J., Dueñas, K., & Macías, L. (2016). Computer crime. Criminal Procedure in Ecuador. Chone: Universidad Laica Eloy Alfaro.
Zurita, A. (2017). The crime of criminal organization: grounds of responsibility and legal sanctions. Seville: University of Seville.