

[BOSCH]
MÉXICO

ALL

International Criminal Law

Transnational organized crime
and international crimes

Jesús Edmundo Coronado
Contreras
Editor

2021

BOSCH
MÉXICO

ALL

International Criminal Law

Transnational organized crime
and international crimes

2021

Collection
ALL

Jesús Edmundo Coronado Contreras
Editor

 Wolters Kluwer

© Authors, 2021
© Wolters Kluwer Legal & Regulatory Spain, S.A.

Wolters Kluwer Legal & Regulatory Spain, S.A.

C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@wolterskluwer.es
<http://www.wolterskluwer.es>

Edition: October 2021

Legal Deposit: M-26899-2021
ISBN print version: 978-84-9090-510-4
ISBN electronic version: 978-84-9090-511-1

Design, Prepress and Printing: Wolters Kluwer Legal & Regulatory Spain, S.A.
Printed in Spain

© **Wolters Kluwer Legal & Regulatory Spain, S.A.** All rights reserved. Under the terms of art. 32 of Royal Legislative Decree 1/1996 of 12 April 1996, approving the Law on Intellectual Property, Wolters Kluwer Legal & Regulatory Spain, S.A. expressly objects any use of the contents of this publication without prior express authorization from the publishers, which includes in particular any reproduction, modification, recording, copying, exploitation, distribution, communication, transmission, sending, reuse, publication, processing or any other total or partial use in any form or by any means or format of this publication.

Any form of reproduction, distribution, public communication or transformation of this work can only be carried out with the express authorization of its owners, except for the exceptions provided by the Law. Please contact to **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) if you need to photocopy or scan any part of this work.

The publisher and the authors accept no responsibility or liability whatsoever for any consequences to any natural or legal person who acts or fails to act as a result of any information contained in this publication.

WOLTERS KLUWER LEGAL & REGULATORY SPAIN shall not be liable for the opinions expressed by the authors of the contents, as well as in forums, chats, or any other participation tools. the authors of the contents, as well as in forums, chats, or any other participation tools. Likewise, WOLTERS KLUWER LEGAL & REGULATORY ESPAÑA shall not be held responsible for any possible infringement of intellectual property rights that may be attributable to these authors.

WOLTERS KLUWER LEGAL & REGULATORY SPAIN is exempt from any liability for damages of any kind that may be caused by such authors. damages of any nature that may be due to the lack of truthfulness, accuracy, completeness and/or timeliness of the contents transmitted, disseminated, disseminated and/or updated of the contents transmitted, disseminated, stored, made available or received, obtained or accessed through its PRODUCTS. nor for the Contents provided or offered by third parties or entities, persons or entities.

WOLTERS KLUWER LEGAL & REGULATORY SPAIN reserves the right to eliminate any content which is content which is untrue, inaccurate and contrary to the law, morality, public order and good customs.

Publisher's Note: The text of the judicial decisions contained in the publications and products of **Wolters Kluwer Legal & Regulatory Spain, S.A.** is supplied by the Judicial Documentation Center of the General Council of the Judiciary (Cendoj), except for those that have been provided to us from time to time by the communications offices of the collegiate judicial bodies. The Cendoj is the only body legally empowered to collect such decisions. The processing of the personal data contained in these resolutions is carried out directly by the aforementioned body, since July 2003, with its own criteria in compliance with the regulations in force on the matter, being therefore its sole responsibility for any error or incident in this matter.

3. CYBERCRIME

Once all this new theory has been described, then ubiquitous crimes and in particular cybercrimes, which can also be classified as a second glove of current crime, will be discussed in detail.

The victim can be a natural person or a company, neither of them is free to suffer from criminal actions. Given this, those that affect or have greater repercussions will be detailed.

4. IDENTITY

Within the first typology is identity; for this purpose, it would first be necessary to know what digital identity is. The identity, traditionally, is formed by the name and surname of the person, date of birth, address, sex, in some cases, the degree of studies or some specific capacity or function incorporated.

In cyberspace, these elements could well be taken up to form the digital identity, which could be even broader because it will depend a lot on the type of actions that are carried out in this meta-space.

It is frequent that e-commerce of any kind is made on portals or sites or that bank transfers are made through applications, obviously it implies a simplification in daily life, but also entails a significant challenge in terms of the security of the identity and privacy of the data that is handled.

Among the biggest problems is proving identity, since many times it is unknown who is the individual who performs a certain action in the digital environment.

In fact, trying to protect yourself from the Internet and depravity is considered by many as a lost cause, as the renowned actress Scarlett Johansson responded at the time in an interview for the Washington Post, where she recounted her attempts to stop pornographic deep fakes (the use of artificial intelligence to produce pornographic videos, especially celebrities are the ones who suffer this, but it can happen with any individual).

The actress who plays as "black widow" is one of the main victims of the illegal use of images in pornographic, erotic, or similar products, as there are many robots with her face on the most popular portals or platforms of that turn.

Deep fakes have spawned an entire video counterfeiting industry that surpasses public figures, since they have also been used to destroy people's reputations or as revenge.

The actress concluded that nothing may stop someone from using her image or someone else's on another body and making it look realistic and she legally considers her struggle useless because the Internet is a huge wormhole of darkness that devours itself and that this does not affect her because people assume that it is not really her in the pornographic film.

That is why many people consider that these type of situations as a losing battle. However, its complexity must be combated because deep fakes help the commission of crimes against identity, defamation, and fraud, since within the victims of this alte-

ration not only the image of people is taken for videos, but it is also possible to use audio to modify what is said. An instrument that becomes a very dangerous weapon and can expose any partner or legal representative of a company, alluding to the fact that it carried out acts or operations or made certain comments.

In this regard, it is vital to highlight that there is also *phishing*, which for computer experts consists of taking a person's data and using it for different purposes; This term refers to fishing, which would be to "fish" in this case the data or information of a victim through deception or other machinations.

This conduct is one of the most frequent threats today, affecting companies and individuals because if data is illegally stolen, severe consequences can occur.

From an eminently legal point of view, it cannot be argued that phishing is a crime, but we must refer to three different behaviors that they are often misused as synonyms. For this reason, it is essential to describe in detail what theft, impersonation and usurpation consist of and how they affect identity. In the first place, these are three different events and could be precisely three different cybercrimes.

Strictly, the theft would be the starting point because with it the other two acts can be carried out, both impersonation and usurpation, both imply the theft of information and data from an individual. It would then be the first criminal act. This is because there may be the theft of information or data without necessarily using them to impersonate or usurp a person, since it may be that whoever committed that act sells or uses them to extort money (*ransomware*, for computer scientists) by affected people.

Impersonation consists in replacing an individual through the misuse of identity, posing as her/him particularly. And usurpation implies holding the position or functions of the affected person, in other words, it not only entails replacing an individual, but also exercising or executing the powers that he/she has by virtue of a particular commission.

From the above, it can be argued that these are three different circumstances. Although they can be concatenated, they cannot necessarily be consummated by the same agent.

Therefore, in practice it has been difficult to regulate these criminal acts because many legislators (not only in Mexico) have tried to encompass these three acts in a single criminal type, because they handle theft, impersonation, and usurpation as equivalent, although there are substantial differences between the concepts.

Particularly in the case of Mexico, part of the complications presented begins because the identity theft is considered a "tax crime", as it is provided in section VI of article 110 of the Federal Tax Code. A sanction will be imposed from three months to three years in prison to whom, through any physical, documentary, electronic, optical, magnetic means or any other kind of technology, impersonates the identity, representation or personality of a taxpayer, which can be very ambiguous because they mix concepts like personality and identity.

Such concepts are not synonymous because identity is the set of characteristics of an individual that characterizes him from others and therefore distinguishes him (name,

surname, place of birth, etc.). The proof of identity is called identification; therefore, it is the demonstration and materialization of all the characteristics of identity.

The State is interested in individualizing the subject to attribute rights and obligations, that is, granting him legal personality. Consequently, personality is the ability to be subject to rights and obligations recognized by law. Thus, when "impersonating" is used, it is to refer to the use of a person's characteristic data as one's own or to falsify an identification; but when it comes to impersonating the personality, it is to use false identifications to achieve some legal effect. In no provision of a similar nature is it stated what is understood as identity theft and what difference it would have with that of impersonating personality. At the local level, some federative entities in Mexico have tried to regulate identity theft or usurpation, such is the case of Mexico City (art. 211 Bis), Jalisco (art. 143-Quáter), Nuevo León (art. 444), Oaxaca (art. 232 Bis), Quintana Roo (art. 195 Sexties), Sonora (arts. 241 Bis and 241 Bis 1), Tlaxcala (art. 282) and Zacatecas (art. 227 Bis), to name a few. However, each one has done it, in a particular way and they do not stand out for doing it correctly; for example, in Quintana Roo impersonation and usurpation are used interchangeably, and in Sonora a similar situation with identity and personality is done.

These inconsistencies mean that, in practice, it is materially impossible to punish and prevent certain illegal acts from being carried out. Therefore, the importance of properly distinguishing each of the behaviors that are intended to be punished.

In cyberspace it could be the case that an individual can "impersonate" the identity of a company and pretend to provide a service and obtain a profit, although this conduct may be fraud, it is also an identity theft in a strict sense, because there would be two victims, on one hand, who suffers the impersonation and on the other, who sees the loss of their assets due to "cyber fraud".

5. PRIVACY, INTIMACY, INFORMATION, AND OTHER PERSONAL DATA

Another of the assets that is constantly in question in cyberspace is privacy. Many persons maintain that it no longer exists in the digital age because by accepting the famous "terms and conditions" you are yielding or allowing our information to be used by third parties.

Digital information is precious at an unmatched level and has radically changed the rules of the market. In Mexico, there are specific laws on the matter, one is the Federal Law for the Protection of Personal Data Held by Private Parties (acronyms in Spanish, LFPDPPP) and the other is the General Law for the Protection of Personal Data Held by Obligated Subjects (acronyms in Spanish, LGPDPPSO). In addition, we have the existence of the National Institute for Transparency and Access to Information (acronyms in Spanish, INAI).

Private companies and other organizations have had to change the way in which they collect the personal data of their clients, partners, and employees, to avoid millionaire fines that can be imposed if the provisions of the LFPDPPP are not complied with.

However, by handling and processing of personal data, companies and individuals are exposed to cybercrimes against privacy and information protection, we can find that

there are documents that due to their special nature should not be available to third parties, but they are stolen, because they were saved in the famous "cloud", which is a typical computer theft risk.

In this sense, article 67 of the LFPDPPP indicates that three months to three years in prison will be imposed on those whom, being authorized to process personal data for profit, cause a security breach of the databases in their custody.

A similar situation is held with the types of fraud in the processing of personal data, where article 68 of the LFPDPPP specifies that a prison sentence of six months to five years will be sanctioned to whom, to achieve an undue profit, treat personal data through deception, taking advantage of the error in which the owner or the person authorized to transmit them is found. It has even been detailed that companies have the right to privacy, as has been upheld by the Supreme Court of Justice of the Nation of Mexico through the jurisprudence of the heading: **LEGAL PERSONS. THEY HAVE THE RIGHT TO THE PROTECTION OF THE DATA THAT MAY BE EQUIPPED TO PERSONS, EVEN WHEN SUCH INFORMATION HAS BEEN DELIVERED TO AN AUTHORITY**, visible in the Gazette of the Federal Judicial Weekly, Tenth Era, Registry: 2005522, Jurisprudence: P. II / 2014 (10th), February 2014.

The illegal recording of conversations could also be considered as an affectation of privacy, both of those who make up the legal entity and itself.

Traditionally, the characteristic of "privacy" is that it can be defined as that sphere within the scope of the life of any individual that takes place in a reserved space, and which must be kept confidential.

Thus, it can be argued that everyone has the right to protect from any interference within the said sphere because they belong to a zone that is psychologically and spiritually considered intimate and reserved either for themselves or exclusively from a group to which they belong, as can be, for example, his family.

Under the vision that companies handle a lot of information that can be considered as sensitive or personal of their clients, in recent years, Mexico has joined the international trend in consumer protection through provisions such as the LFPFPPP and obliges public officials to follow the same type of guidelines under the LGPDPPSO. You cannot lose sight of the privacy of the companies themselves when they not only have to look after their customers.

Thus, the responsibility of companies must be effectively defined when they are intermediaries and must follow confidentiality schemes and, furthermore, when they in turn provide information that can be "a weapon" for their competitors.

Every day more and more companies and corporations use different social networks to get closer to their audience. The *Cambridge-Analytica* scandal revealed the amount of information that transnational companies like *Facebook* can have not only from individuals but also from legal entities. In Mexico, about a million people were affected by this incident.

ALL International Criminal Law

The world is constantly changing. Advances in science and technology have generated a globalized society, which faces many challenges, one of them is the criminal phenomenon.

Crime evolved to levels never imagined, growing exponentially across borders and affecting a greater number of people. The impact of certain criminal acts has consequences not only at the local level, but also reaches the international level.

In this context, International Criminal Law acquires greater relevance, being that subject that studies and analyzes the greatest crimes, which by their particular nature affect all the world.

The commission of crimes against humanity, war crimes, and genocide has marked the history of humanity and demanded the presence of international tribunals. However, the growth of transnational organized crime activities has also severely affected the world, both physical and digital.

This book focuses on some essential aspects of the development of this novel legal matter, which details its importance from different perspectives, combining the theoretical and practical experience of its authors, all recognized specialists in the field of International Criminal Law.

BOSCH
MÉXICO

ISBN: 978-84-9090-508-1



9

788490

905081



3652K29141



EN-0280/2005

GA-2005/0100