QUESTIONNAIRE

MEXICO

Dr. Cristos Velasco

Evidencia Digital.LAT, Protección Datos México (ProtDataMx)

1. Introduction

Please read carefully before answering the questionnaire

The RAYUELA project is aimed at protecting children in their online interactions. For this purpose, the project will develop a "game", which will present the children with realistic scenarios relating to the following cybercrimes/cyber-facilitated crimes:

- ***Online grooming*** (further: OG) is the crime where the perpetrator (usually an adult) uses electronic communication services, including social media, to contact a minor and build rapport with the aim of eventually meeting in person for the purposes of sexual activity. The perpetrator may employ various strategies (deception, romantic/emotional attachment, promise of material or other benefits, blackmail, coercion, etc.) to lower a child's inhibitions, heighten their curiosity about sexual experiences, or otherwise convince them to meet up.

- ***Cyber bullying*** (further: CB) is a broad term that includes all types of bullying behavior online. This includes cyber stalking and cyber harassment, and any other type of behaviour online aimed at hurting the victim. Cyber bullying may also have a sexual component.

- ***Misinformation and deception*** (further: MD) is a behaviour that may or may not be punishable by law depending on the context. It involves all kinds of information sharing that is fake, or deceptive. For a criminal qualification to apply, typically the behaviour will need to be intentional and there will need to be material consequences to this intention.

- ***Human trafficking with a cyber component*** i.e., the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking (further: HT).

The purpose of the game is to teach children how to remain safe online, while the obtained insights will be used to provide policy recommendations and educational tools.
The game does not focus solely on the threats of potentially falling victim to one of these four crimes. It also aims to raise awareness about the general threats of using IT, such as the Internet and connected devices, and minors' capacity to make responsible choices in this regard.
A particular point of interest is understanding whether minors are aware of when they, or someone else, is crossing the line in becoming offenders themselves, as this an important aspect of protecting children online. Due to the nature of online communication, inhibitions may be lowered, and certain actions may feel more innocent or less "real" than in real life. In addition, a perception may exist that what happens on the Internet has little or no impact beyond the digital world. This creates situations where minors engage in what they perceive to be relatively innocent behaviour ("everyone does this on the internet"), that may however have serious legal consequences.
One of the goals in RAYUELA is to ensure that minors realize when their behaviour may turn into actions that are punishable by law.
The present study and questionnaire are set up in the context of the RAYUELA project in order to provide an overview of the **legislative framework and relevant policies** in a number of countries, both in the EU and beyond, in relation to:

- How the main crimes of OG, CB, MD and HT are dealt with by the legal system i.e., which behaviours are punishable and under which conditions?

- How cybercrime and cyber-facilitated crime perpetrated by minors is dealt with in the legal system (both in general and specifically in relation to the crimes in focus)?
- What international instruments and cooperation mechanisms are available in dealing with cybercrime perpetrated by minors?

Importantly, we want to know both the legal rules and policies which are implemented in practice, and their effect on the **real enforcement situation**. If you have knowledge about the effects of current policies on crime rates by minors and on the crime rates for OG, CB, MD and HT, this would be of interest.

We are specifically interested in **case law** that illustrates the "why and how" of certain legal rules, principles and policies in practice. Case law will help us illustrate the similarities and differences between jurisdictions and is therefore *essential***.** Please ensure to have a good amount of case law processed in your answers.

In addition, we want input on **international legal instruments and international cooperation** relevant for cybercrime, and in particular for cybercrime perpetrated by minors. What happens when cybercrimes are perpetrated in a cross-border context? What are the legal rules in place for cooperation with authorities from other countries, and how does this work out in practice (issues, problems, etc.)?

Lastly, we are interested in some **statistical information on cybercrime** in your country and cybercrime by minors specifically.

The purpose of this questionnaire is to help you provide this information for your jurisdiction.

2. Questions relating to OG, CB, HT and MD with minors as victims

In this section, we will ask questions to understand how to main 4 crimes in focus in RAYUELA are regulated in your jurisdiction. In this section, the focus is on adult perpetrators with victims that are minors. We are interested in both the general rules, and whether the fact that the victim is a minor has an influence on the application of the law. We are also in particular interested in your thoughts on whether the scope of the law affects the amount of cases that are brought before the courts, in other words, are the current provisions sufficient to prosecute the diverse forms of crime present in reality? And are cases effectively prosecuted in practice or are there obstacles (e.g. lack of resources)?

Question 1: Is online grooming punishable by law in your country?
Answer:
Yes, Mexico reformed the Criminal Code in June 2018 in order to criminalize the conduct of 'online grooming'. Title Seventh Bis on Crimes against Indemnity of the Privacy of Sexual Information of the Criminal Code consisting of Art. 199 Septies currently provides:
Article 199 Septies.- An imprisonment from four to eight years and a fine from four hundred to one thousand days shall be levied upon to he who contacts a person under eighteen years of age, or someone who does not have the capacity to understand the meaning of the event or to a person who does not have the capacity to resist it and request him/her images, audio or video of explicit sexual activities, acts of sexual connotation, or requests for a sexual encounter through the use of broadcasting, telecommunications, computer or any other means of data transmission.

Concerning the legal qualification, this article may apply to adults, teenagers or children seeking to specifically groom minors (persons under 18 years old) for sexual related purposes through the use of online data transmissions, social media platforms, communication services or broadcasting platforms. This article does not provide any distinctions and aggravated penalties when the person that commits the conduct is an adult. This provision applies generally to any individual executing the conduct regardless of her/his age.
There are no special conditions for application. As long as the person provides sufficient and convincing evidence to the Ministerio Publico (Public Prosecutor) through data, screenshots that she/he is being contacted for sexual purposes, the Public Prosecutor should follow-up the investigation.

Rules on Prescription

Regarding the prescriptive period for this particular crime, Chapter VI consisting of articles 100 to 115 of the Criminal Code set forth specific rules for the prescription of the criminal conduct, the sanctions and fines. Articles 104, 105, 106 and 107 bis of the Criminal Code are of particular relevance.
Art. 104 provides that the penal action prescribes in one year if the crime only deserves a fine, and if the crime deserves imprisonment or an alternative sentence, then the rules for the statute of limitations will be followed in order to execute the imprisonment sentence.
Art. 105 provides that the criminal action shall prescribe within a period equal to the arithmetic average rule term for the imprisonment sentence established by the law concerning the crime in question, but it shall not be lower than three years.
Art. 106 provides that the criminal action will prescribe in two years, if the crime only merits dismissal, suspension, deprivation of right or disqualification, except as provided in other regulations.
Art. 107 Bis provides that the term of prescription for crimes under *Title Eight of the Second Book* of the Criminal Code concerning crimes such as corruption of minors, sexual exploitation and abuse of children, sexual tourism, lenocide (lenocidio) and human trafficking committed against minors will begin when the victim reaches the majority of age, which is 18 years old. For victims who do not have the capacity to understand the meaning of the act or who do not have the capacity to resist the crime, the term will start from the moment in which there is evidence of the commission of the crime file before the Ministerio Público (Public Prosecutor). In the case of crimes against freedom and the normal psychosexual development, as well as those provided for in the *Law to Prevent and Punish Trafficking of Human Beings*, committed against a person who is under eighteen years of age, the start of the term will begin from the day on which the victim reaches the age majority.

It is worth noting that the mentioned rules on prescriptive periods may be subject to the criteria of the Public Prosecutor that is in charge of the criminal investigation, there is no standard approach. Since online grooming falls under the scope of crimes of corruption of minors and sexual exploitation, the prescription rules and terms of Art. 107 Bis will be applicable.

The main problematic lies when the perpetrator of grooming is not specifically located within the jurisdiction or place where the victim resides. There is not sufficient evidence to confirm that the national investigative authorities, in particular the Ministerio Público conducts and follows-up investigations when the perpetrator is located in a foreign jurisdiction. Please note that Mexico has **not** yet signed and ratified the Council of Europe's Budapest Convention and the Lanzarote Convention, which are key instruments to facilitate international cooperation in cross-border investigations concerning cybercrime and the abuse and exploitation of children online (including online grooming), a situation that certainly limits national law enforcement authorities to cooperate with foreign authorities in cross-border cases concerning online grooming.

Concerning existing case law, please note that we could not have access to this information from the national investigative authorities. We know that there have been cases filed by victims at the national level, however the outcome of the investigations is largely unknown, and local NGO's who are supporting child and teenager victims have pointed out that the authorities are not sufficiently trained to follow-up of the criminal investigation.

Mexico has a legislation in place that protects the general rights of children and teenagers known as *General Law of the Rights of Children, Girls and Teenagers*. This legislation sets forth a national system for the protection of the rights of children, girls and teenagers. Art. 5 establishes that a minor is a person not older than 12 years old and a teenager a person between 12 years old and lower to 18 years old. For purposes of international treaties, a child may be considered a person younger than 18 years of age.
The purpose and scope of the law is very broad and is underlined in Art. 1.
Art. 2. establishes that the national authorities shall guarantee the protection of the rights of children and adolescents and shall conduct the following actions:
I. Guarantee a comprehensive, transversal approach with a human rights perspective in the design and implementation of government policies and programs;
II. Promote participation, taking into account the opinion and consider the cultural, ethical, affective, educational and health aspects of girls, boys and adolescents in relevant matters according to their age, evolution, cognitive development and maturity.
III. Establish transparent mechanisms for monitoring and evaluating the implementation of policies, government programs, legislation and commitments derived from international treaties.

This article specifically establishes that 'the best interest of the child' must be considered primarily in decision-making and debated issues involving children and adolescents. When different interpretations are presented, the provisions of the Constitution and the international treaties to which Mexico is a party shall apply and govern.

When a decision made affects girls, boys or adolescents, individually or collectively, the possible repercussions must be evaluated and weighed in order to safeguard their best interests and procedural guarantees.
The authorities of the Federation, of the federal entities, of the municipalities and of the territorial demarcations of Mexico City, within the scope of their competences are required to incorporate in their budget, the allocation of resources that allow compliance with the actions established by the law.

The Chamber of Deputies of the National Congress, the local Congresses and the Legislature of Mexico City are required to establish in their respective budgets, the resources that allow compliance with the actions established and mandated by the law.

Article 13 of the *General Law of the Rights of Children, Girls and Teenagers* enlists the rights of the children and teenagers. Of particular relevance are the following subsections:

[…]
VI. Right not to be discriminated;
VIII. Right to a life free of violence, and to a healthy development;
XIV. Right to freedom of expression and access to information;
XVII. Right to privacy; and
XX. Right of access to Information Communication Technologies.
The federal authorities, state and municipal entities and the territorial demarcations of Mexico City, within the scope of their respective competences shall adopt the necessary measures to guarantee the rights listed under Art. 13 to all girls, boys and adolescents without discrimination of any kind or condition.

Question 2: Is cyberbullying punishable by law in your country? Please take into account a broad understanding of cyberbullying (cyber/online stalking, harassment, sexual harassment)?

Answer:
Cyberbullying defined as the activity that a school peer uses to harass, insult or inflict damage to one other peer or classmate or colleague through social media or messenger communications platforms as such is not a conduct specifically regulated under Mexico's Federal Criminal Code. The traditional conducts of 'sexual harassment' and 'sexual abuse' are regulated under Arts. 259 Bis, 260, 261 of the Federal Criminal Code. These articles establish the following:

"Art. 259 Bis.- A person who repeatedly harasses another person of either sex with lewd purposes, by making use of his/her hierarchical position derived from work, teaching, domestic relations or any other that implies subordination shall be punished with a fine of up to eight hundred days. If the harasser is a public servant and uses the means or circumstances provided by the assignment, in addition to the penalties mentioned, he will be removed from office and may be disqualified from holding any other public position for up to one year.
Sexual harassment will only be punishable when it causes harm or damage.
Legal action against the harasser may only be conducted at the request of the offended party."

"Art. 260. The crime of sexual abuse is committed when someone who executes on a person, without her/his consent or forces her/him to execute for herself or on another person, sexual activities without the purpose of reaching intercourse.
A punishment from six to ten years imprisonment and up to two hundred days fine will be imposed to the person who commits this crime.
For the purposes of this article, sexual acts are obscene bodily touching or groping, or those that represent explicitly sexual acts or force the victim to execute them.
Sexual abuse is also considered as such when the victim is forced to observe a sexual act, or to expose her body without her consent.
If physical or psychological violence has been used, the penalty will be increased up to one half."

"Article 261. A person who commits the crime of sexual abuse against an individual under fifteen years of age or against a person who does not have the capacity to understand the meaning of the act, even with her/his consent, or that for any reason cannot resist it or force her/him to execute it to herself/himself or another person, a penalty from six to thirteen years imprisonment and up to five hundred days will be levied upon."

Concerning violence against women, and the regulation of distribution of non-consented sexual images, the Mexican government published in June 2021 a decree that reforms the *Federal Criminal Code* and the *General Law of Access for Women to a Life Free of Violence* in the Official Gazzete (Diario Oficial de la Federacion). These legal reforms arise as a result of a wide campaign of national activism from Olimpia Coral, whose former boyfriend shared and distributed sexual images and videos of her through social media when she was only 18 years old. This law is also known as the "Ley Olimpia" in honor and reference to said national female activist.

The decree introduced two relevant definitions to the *General Law of Access for Women to a Life Free of Violence*. One on 'Digital Violence' and another on 'Media Violence'. The definitions are the following:

"Art. 20 Quáter.- Digital violence is any fraudulent action carried out through the use of information and communication technologies, by which images, audio, or real or simulated videos of intimate sexual content of a person without his consent, without his approval or without his authorization are exposed, distributed, disseminated, exhibited, transmitted, commercialized and offered and that cause psychological, emotional damage, in the sphere of his private life or in his own image.
As well as those malicious acts that cause damage to the intimacy, privacy and/or dignity of women, which are committed through information and communication technologies."

"Art. 20 Quinquies.- Media violence is any act through any means of communication, which directly or indirectly promotes sexual stereotypes, makes reference to violence against women and girls, produces or allows the production and dissemination of hate speech, sexist hatred, gender discrimination or inequality between women and men, which causes psychological, sexual, physical, economic, patrimonial or femicide harm to women and girls.
Media violence is exercised by any natural or legal person who uses a communication medium to produce and disseminate content that threatens against the self-esteem, health, integrity, freedom and security of women and girls, that prevents their development and that threatens the equality."

The Decree published in June 2021 introduced a new chapter (Chapter II Breach of Sexual Intimacy) consisting of articles 199 Octies, 199 Nonies and 199 Decies of the Federal Criminal Code. These articles criminalize the conduct of sharing and distribution of sexual content without the consent of an individual and provide for specific punishments and aggravated circumstances. Said articles provide the following:

"Art. 199 Octies.- The person who discloses, shares, distributes or publishes images, videos or audio of intimate sexual content of a person who has the legal age without her/his consent, approval or authorization commits the crime of breach of sexual intimacy.
Likewise, whoever videorecords, audiorecords, photographs, prints or produces, images, audio or videos with intimate sexual content of a person without her/his consent, approval, or authorization.
Said conducts shall be punished with an imprisonment term from three to six years in prison and a fine of five hundred to one thousand Units of Measurement and Updating (Unidades de Medida y Actualizacion)."

"Art. 199 Nonies.- The same sanctions provided in the previous article will be imposed when the images, videos or audios with intimate sexual content that are disclosed, shared, distributed or published do not correspond to the person who is indicated or identified in them."

"Art. 199 Decies.- The minimum and maximum punishment will be increased up to one half:
I.- When the conduct is committed by the spouse, concubine, partner or by any person with whom the victim has or has had a sentimental, affective or trustworthiness relationship;
II.- When the conduct is committed by a public servant in the exercise of her/ his functions;
III.- When it is committed against a person who cannot understand the meaning of the act or does not have the ability to resist it;
IV.- When some kind of non-profit benefit has been obtained;
V.- When it is conducted for profit purposes, or
VI.- When, as a result of the effects or impacts of the crime, the victim attempts against her/his integrity or against her/his own life."

Please note a *Unidad de Medida y Actualizacion (UMA)* is the national reference measure used to calculate economic fines contained in the laws in Mexico. As of January 2022, an *UMA* is currently

worth MXN $96.22 daily (Approx. 4.70 Euros); MXN $2,925.09 monthly (Approx. 141 Euros); MXN $35,101.08 (Approx. 1696 Euros). INEGI updates the amounts from January each year.

Regarding the prescriptive period for this particular crime, Chapter VI consisting of articles 100 to 115 of the Federal Criminal Code set forth specific rules for the prescription of the criminal conduct, the sanctions and fines. Articles 104, 105, 106 and 107 bis of the Criminal Code are of particular relevance. See the answer on "Rules on Prescription' in question 1. Once again, the rules on prescriptive periods may be subject to the criteria of the Public Prosecutor that is in charge of the criminal investigation, there is no uniform or standard approach.

Even though Mexico has a modern legal framework on cyberviolence, there is no sufficient evidence on whether the national authorities are investigating the cases filed by the victims to the national investigative authorities.

Even though Mexico has legislation at the federal level, and in some States of the Mexican Republic, the local legislation punishes conducts of digital violence, media violence and the dissemination of intimate sexual content without consent, there remains many obstacles and challenges to the national criminal justice authorities to proceed with the investigations and for the judges to adjudicate these crimes and punish the perpetrators of these conducts. There are no official national statistics available on the crimes that are adjudicated by the local judges in Mexico.

In the area of prevention and awareness, the Federal Government of Mexico has created a specific website on 'Cyberbullying" with the aim to increase national awareness on this area and to help prevent this conduct among teenagers and children at the national level. https://www.gob.mx/ciberbullying

Regarding statistics on cyberbullying, the national authority for statistics, the National Institute for Statistics, Geography and Information (INEGI) publishes each year statistics concerning different forms of online harassment including cyberbullying in a report known as "Modulo Ciberacoso 2020 (MOCIBA 2020)" The MOCIBA 2020 reports presents results that show the prevalence of online harassment and cyberbullying during the 12 months prior to its happening and it includes numbers and the gender of the population that has experienced it through different situations. Among the major findings of the MOCIBA 2020 report are:
- 21% of the internet user population older than 12 years was a victim of cyberbullying between October 2019 and November 2020.
- The most frequent harassment situation experienced by women was sexual advances or proposals (35.9%), while for men it was contact through false identities (37.1%).
- The highest prevalence of cyberbullying was registered in the states of Colima, Tabasco and Tlaxcala.

Question 3: When would misinformation and deception online constitute a criminal offence in your country? In other words, what potential qualifications could apply to wilful misinformation and deception on the internet?
Answer:

Please note that misinformation, disinformation and deception on the Internet are not crimes specifically regulated under Mexico's Federal Criminal Code.

Art. 76 Bis section VII of the *Federal Law on Consumer Protection* establishes an obligation that supplier of good and services must abstain from using sales or advertising strategies that do not provide consumers with clear and sufficient information about the services offered, especially in the case of marketing practices on the Internet aimed at the vulnerable population, such as children, elderly and sick where providers should incorporate mechanisms warning said vulnerable groups when the information for them may not be suitable. Please note that this a consumer protection issue but not a concrete criminal issue.

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

Not applicable because the conducts of disinformation and deception on the Internet are not crimes specifically regulated under the Federal Criminal Code.

Question 4: What constitutes human trafficking and how is human trafficking facilitated by electronic means punished in your country? Are online grooming activities to find victims (e.g. lover boys) before the actual human trafficking punishable in itself? In addition, are these activities punishable as a separate crime if human trafficking does take place afterward?
Answer:

Mexico has a *General Law to Prevent, Punish and to Eradicate Crimes of Human Trafficking and the Protection and Support for Victims of said Crimes*. This law generally regulates the competencies and the coordination between the federal, state and municipal entities responsible for the prevention, investigation, enforcement and prosecution of crimes of human trafficking.

As stated in Art 2., the main purpose of this law is:
"I. to establish powers and forms of coordination for the prevention, investigation, prosecution and punishment of crimes related to trafficking in persons between the Federal Government, State and municipal entities;
II. Establish the criminal conduct concerning the trafficking of human beings and penalties and sanctions;
III. Set forth the criminal procedures applicable to these types of crimes;
IV. Establish the distribution of powers and forms of coordination in matters of protection and assistance to the victims of these crimes;
V. Establish effective mechanisms for the protection of life, dignity, freedom, integrity and security of people, as well as the free development of children and adolescents, when they are threatened or injured by the commission of the crimes contained in this law;
VI. Repair the damage made to victims of human trafficking in a comprehensive, adequate and effective way, proportional to the seriousness of the damage caused and the damage suffered."

Art. 3 of this law sets forth in eleven subsections, the principles that the national authorities must observe in the interpretation, application and the definition of the actions for the enforcement of the law, in the design and implementation of activities on prevention, investigation, enforcement and prosecution of crimes of human trafficking, as well as for the protection and assistance to the victims, offended parties and witnesses.

Please note that the *General Law to Prevent, Punish and to Eradicate Crimes of Human Trafficking and the Protection and Support for Victims of said Crimes* does neither provide nor does it make any reference to the facilitation of human trafficking crimes through electronic means.

The *General Law to Prevent, Punish and to Eradicate Crimes of Human Trafficking and the Protection and Support for Victims of said Crimes* contains a specific chapter (consisting of Arts. 10 to 38 that enlist a broad catalogue of crimes on human trafficking.

Art. 10 of said law defines the conduct of human trafficking as *"Any malicious action or omission of one or several persons to capture, engage, transport, transfer, retain, deliver, receive or accommodate one or more persons for the purpose of exploitation"*. The conduct of human trafficking is punished with 5 to 15 years imprisonment and from one thousand to twenty thousand days of fine, without

prejudice to the sanctions that correspond to each of the crimes committed, foreseen and sanctioned in this law and in the respective Penal Codes of other States.

The second paragraph of Art. 10 defines *'Exploitation of a Person'* as follows:
I. Slavery, in accordance with article 11 of this law;
II. The condition of serf, in accordance with article 12 of this law;
III. The prostitution of others or other forms of sexual exploitation, in accordance with Arts 13 to 20 of this law;
IV. Labor exploitation, in accordance with Art. 21 of this law;
V. Forced labor or services, in accordance with Art. 22 of this law;
VI. Forced begging, in accordance with Art. 24 of this law;
VII. The use of persons under the age of eighteen years for criminal activities, in accordance with Art. 25 of this law;
VIII. Illegal adoption of a person under eighteen years of age, in accordance with Arts. 26 and 27 of this law;
IX. Forced or servile marriage, in accordance with Art. 28 of this law, as well as the hypothesis provided for in Art. 29;
X. Trafficking of organs, tissues and cells of living human beings, in accordance with Art. 30 of this Law; and
XI. Illicit biomedical experimentation on human beings, in accordance with Art. 31 of this law.

Concerning the question on whether online grooming activities to find victims (e.g. lover boys) before the actual human trafficking occurs. The answer is NO. The *General Law to Prevent, Punish and to Eradicate Crimes of Human Trafficking and the Protection and Support for Victims of said Crimes* nor the Criminal Code provide for that specific hypothesis or conduct.

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

Regarding the prescriptive period for crimes of human trafficking, Chapter VI consisting of articles 100 to 115 of the Criminal set forth specific rules for the prescription of the criminal conduct, the sanctions and fines. Articles 104, 105, 106 and 107 bis of the Criminal Code are of particular relevance. See the answer on "Rules on Prescription' contained in Question 1. Once again, the rules on prescriptive periods may be subject to the criteria of the Public Prosecutor that is in charge of the criminal investigation, there is no uniform or standard approach.

One specific challenge identified is when the perpetrator of human trafficking related activities is not specifically located within the jurisdiction or place where the victim resides. There is not sufficient evidence to confirm that the national investigative authorities, in particular the Ministerio Público conducts and follows-up investigations when the perpetrator of human trafficking activities is located in a foreign jurisdiction. Please note that Mexico has not yet signed and ratified the *Council of Europe Convention on Action against Trafficking in Human Beings*, which is another relevant instrument that facilitates and enables international cooperation in cross-border investigations concerning human trafficking activities, a situation that certainly limits national law enforcement authorities to cooperate with foreign authorities in cross-border cases concerning human trafficking activities.

Regarding existing case law, please note that we could not have access to this information from the national investigative authorities. We know that there have been cases filed by victims at the national level, however the outcome of the investigations is largely unknown, and local NGO's who are

supporting victims of human trafficking have pointed out that the authorities are not sufficiently well trained to follow-up with the criminal investigation filed by the victims.

3. Questions regarding cybercrime or cyber-facilitated crime committed by minors

This section is aimed at understanding how cybercrime or cyber-facilitated crime committed by minors is dealt with in your jurisdiction. In particular we are trying to assess to what extent the rules and policies in place create leeway for minors who may not always be aware of when their behaviour is crossing a line. We are also interested to know the real enforcement situation. In addition to the general rules on the juvenile justice system and the punishment of minors, the 4 crimes of focus of RAYUELA are addressed, as well as two particularly relevant crimes committed by minors online: online piracy and hacking.

Question 5: How is crime committed by minors dealt with in your country, in general? Is there a specific juvenile justice system? If yes, please explain in detail how this works.

Please explain the applicable rules, the conditions for application (general age limit, limits for certain crimes), the range and types of punishment that may be imposed on minors, rules about mitigating/attenuating circumstances, and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

Answer:
Crimes committed by minors (persons between 12 and 18 years old) is punished under a special law known as *National Law of the Comprehensive Criminal Justice System for Adolescents.* This law is of public order and general observance throughout the Mexican Republic. It is applicable to minors between twelve years of age and less than eighteen years of age who are attributed the performance of a conduct typified as a crime by criminal law and, and who are under the jurisdiction of the Federation or the States, within the framework of the principles and rights enshrined in the Political Constitution of the United Mexican States and in the international treaties to which Mexico is a party to.

Yes, the juvenile justice system in Mexico is governed specifically by said law. The law contains an article on the general principles applicable to the procedure. Art 22. establishes that the system shall be based on an accusatory and oral process in which the principles of publicity, contradiction, concentration, continuity and immediacy will be observed with the adaptations and exceptions of the specialized system.

Art 23. establishes that all the authorities of the system must be trained, qualified and specialized in matters of justice for adolescents within the scope of their attributions.
The law establishes the following:

A chapter on the rights and duties of teenagers (Chapter II);
A full section on the rights of teenagers subject to the system (Arts. 35 to 45);
A section on the rights of teenagers in preventive prison or internment (Arts. 46 to 58);
A full chapter on the rights of the victims (Arts. 59 to 60);
Rules to establish the jurisdiction and competence of federal and state entities (Arts. 61-62);
A Public Prosecutor specialized in Justice for Adolescents with specific rules and mandates for crimes committed by teenagers and juveniles (Art. 66);
A full chapter on Judges and magistrates specialized in Justice for Adolescents with specific rules and mandates for crimes committed by teenagers and juveniles (Art. 70)
A full chapter on the execution of measures by administrative authorities and areas of expertise (Arts. 71 to 72)

A full chapter on national information statistics for the criminal justice system for teenagers and juveniles (Arts. 78 to 81)
An entire section on alternative dispute resolution systems and forms of anticipated termination (Arts. 82 to 105); among others.

The range and types of punishment imposed to minors vary and are subject to the criteria of the judges and magistrates specialized in Justice for Adolescents and juveniles on a case-by-case basis.

The *National Law of the Comprehensive Criminal Justice System for Adolescents* does not specifically provide rules on jurisdictional aspects in cross-border cases.

Question 6: Are there specific rules or is there a specific policy that deals with cybercrime by minors as a special topic, acknowledging the special characteristics of crime by minors in the cyber environment, and the fact that minors may not knowingly or intentionally break rules (issues with criminal intent)? Even absent a written policy, are minors prosecuted for cybercrime in practice?
Answer:
Please explain the applicable rules or policies, if any, and their impact in practice.
Please provide details on known issues of application.

No, there are no specific rules or policies dealing with cybercrime by minors in Mexico.
Further, there is no sufficient evidence to affirm whether minors are being prosecuted for cybercrime related activities by the respective national authorities of the criminal justice system for adolescents. It is not a priority of the national authorities to investigate, prosecute and adjudicate cybercrime committed by minors.

Question 7: Can minors be punished for online grooming in your country? I.e. the situation of a minor capable of providing sexual consent (e.g. 17 year-old) grooming a minor who has not reached the age of sexual consent (e.g. 13 years old) to meet up with the intent to perform sexual activities? Please focus not only on the specific crime of online grooming (which, if present as a separate crime in your jurisdiction, often requires an adult perpetrator), but also on other crimes that would punish the activities that constitute online grooming (i.e. the use of different strategies to force a meeting with the minor victim with the intent to perform sexual activities). If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

Yes, minors committing online grooming activities may be punished under the Criminal Code. As previously mentioned in the answer to question 1, online grooming is criminalized in Art. *199 septies* of the Criminal Code. Concerning the legal qualification, this article may apply to adults, teenagers or children seeking to specifically groom minors (persons under 18 years old) for sexual related purposes through the use of online data transmissions, social media platforms, communication services or broadcasting platforms. This article does not provide any distinctions and aggravated penalties when the person that commits the conduct is an adult. This provision applies generally to any individual executing the conduct regardless of her/his age. There are no special conditions for application. As long as the person provides sufficient and convincing evidence to the Ministerio Publico (Public Prosecutor) through data, screenshots that she/he is being contacted for sexual purposes, the Public Prosecutor should follow-up the investigation.

However, in practice we could not find sufficient evidence to confirm that minors targeting other minors through online grooming activities are being prosecuted by the national authorities of the criminal justice system in Mexico.

Question 8: Can minors be punished for purely online behaviour with a sexual intent when other minors are the victim? E.g. the situation where a minor perpetrator obtains sexually explicit material from the minor victim in order to sell this or to force the victim to do something. If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

NO, minors cannot be punished for purely online behavior with a sexual intent when the victim is a minor. Once again, in practice, there is no sufficient evidence to confirm that a minor could be prosecuted by the national authorities of the criminal justice system when he/she forces the victim to do or perform a sexual explicit activity.

Question 9: Can minors be punished for cyberbullying behaviour, without there being a physical component to the crime? This includes behaviours such as cyberstalking and cyberharassment. If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

As previously mentioned in the answer to question number 2, cyberbullying is not a conduct specifically criminalized in the Federal Criminal Code. However, the traditional conducts of 'sexual harassment' and 'sexual abuse' are regulated under Arts. 259 Bis, 260 and 261 of the Federal Criminal Code. Under said articles minors can be punished. Once again, in practice, there is no sufficient evidence to confirm that a minor could be prosecuted by the national authorities of the criminal justice system when committing cyberstalking and cyberharrasment.

Regarding the prescriptive periods for said particular crimes, Chapter VI consisting of articles 100 to 115 of the Federal Criminal Code set forth specific rules for the prescription of the criminal conduct, the sanctions and fines. Articles 104, 105, 106 and 107 bis of the Federal Criminal Code are of particular relevance. See the answer on "Rules on Prescription' in question 1. Once again, the rules on prescriptive periods may be subject to the criteria of the Public Prosecutor that is in charge of the criminal investigation, there is no uniform or standard approach.

Concerning existing case law, please note that we could not have access to this information from the national investigative authorities. We know that there have been cases filed by victims at the national level, however the outcome of the investigations is largely unknown, and local NGO's who are supporting child and teenager victims of these type of crimes have pointed out that the authorities are not sufficiently trained to adjudicate and follow-up the criminal investigation.

Question 10: Can minors be punished for willful misinformation or deception online (sharing false news, false information, pretending to be someone else, pretending to be an expert, etc.)? Which crimes/qualifications could possibly apply? If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

NO, minors cannot be punished for willful misinformation or deception online because these conducts are not specifically criminalized in the Federal Criminal Code or other state laws in Mexico.

Question 11: Can minors be punished for online actions facilitating human trafficking? Typically, this includes the selection and grooming of victims (e.g. lover boy phenomenon). If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases).
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

The answer is NO. Neither, the *General Law to Prevent, Punish and to Eradicate Crimes of Human Trafficking and the Protection and Support for Victims of said Crimes* nor the *Federal Criminal Code* criminalize online actions facilitating human trafficking, therefore minors cannot be punished for the selection and grooming of victims.

Question 12: Can minors be punished for acts of online piracy in your jurisdiction, i.e. the illegal use and/or distribution of content protected by intellectual property rights? Please focus on the elements of criminal nature. If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

The answer is YES. Title Twenty-Six of the *Federal Criminal Code* contains the legal hypothesis and punishes crimes in the area of copyright. The crimes contained in such title are prosecuted as a result of an individual petition of the victim to the federal authorities (*querella de parte ofendida*) except for section I of Article 424 – with regards to the speculation of the publication of free textbooks distributed by the Mexican government – which is prosecuted by the authorities without the need for an individual petition (de oficio).

Art. 424 section III provides imprisonment from six months to six years and a penalty from 300 to 3,000 days to the individual who illegally uses works protected under the *Federal Law on Authors Rights (FLAR)* with the intention to profit and without the corresponding authorization.

Art. 424bis provides imprisonment terms from three to ten years and fines from 2,000 to 20,000 salary days of sanctions to:

(i) the individual who produces, reproduces, introduces into the country, stocks, transports, sells or leases copies of works, phonograms, videos or books protected under FLAR in an illegal form, with commercial purposes and without the corresponding authorization of the party entitled to the rights of the author or related rights pursuant to said law;
(ii) those who knowingly, provide prime sources and materials destined to the production or reproduction of works, phonograms, video programmes or books referred in the aforementioned paragraph; and
(iii) to the individual who manufactures a device or system with the intention to profit, the purpose of which is to deactivate electronic protection devices of computing programms.

Art. 424ter provides imprisonment from six months to six years and a penalty from 5,000 to 30,000 days of salary to the individual who sells copies of works, phonograms, videos or books to a final consumer in public spaces, illegally and with commercial speculation purposes.

Article 425 stipulates imprisonment from six months to two years or a fine from 300 to 300,000 days of salary to the individual who knowingly and without any right exploits an interpretation or execution with commercial speculation purposes.

Art. 426 stipulates imprisonment from six months to four years and a fine from 300 to 3,000 days of salary when the following hypothesis occur:

(i) Anyone who manufactures, modifies, imports, distributes, sells or leases a device or system to decipher an encrypted satellite signal, carrier of programs, without authorization from the legitimate distributor of said signal;

(ii) Anyone who conducts any act for profit with the purpose of deciphering an encrypted satellite signal, carrier of programs, without authorization from the legitimate distributor of said signal;

(iii) Whoever manufactures or distributes equipment for the reception of an encrypted cable signal carrying programs, without authorization from the legitimate distributor of said signal, or

(iv) Whoever receives or assists another to receive an encrypted cable signal carrying programs without the authorization of the legitimate distributor of said signal.

Art. 427 Ter. provides imprisonment from six months to six years and a fine from five hundred to one thousand days to anyone with the intention to profit, manufactures, imports, distributes, leases or in any way commercializes devices, products or components intended to circumvent an effective technological protection measure used by producers of phonograms, artists or performers, as well as authors of any work protected by copyright or related rights.

Article 428 provides that the monetary penalties provided in this title shall be applied regardless of the redress damage, amount of which may not be lower than 40% of the final sale price to the public for each product or as a result of the rendering of services involving a breach of one or some of the rights provided under the FLAR.

It is worth pointing out that in practice, there is no sufficient evidence to conclude that minors that commit these types of conducts are being prosecuted by the national law enforcement authorities.

Concerning existing case law, please note that we could not have access to this information from the national investigative authorities.

Question 13: Can minors be punished for acts of hacking (i.e. unauthorized access to a computer system)? In particular, would this also apply to various scenarios exploiting vulnerabilities in IoT and connected devices? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:
Please explain the applicable rules (all applicable legal qualifications/articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

The answer is YES, the *Federal Criminal Code* contains a full chapter prohibiting and sanctioning illegal access to computer equipment and information technology systems. Crimes pertaining to unauthorized access to computer systems are prosecuted as the result of an individual petition by the victim to the federal authorities (querella de parte ofendida). Title Nine, Chapter II of the FCC titled *Illegal Access to Systems and Informatics Equipment* consists of seven articles Articles 211*bis* 1–211*bis* 7 that are generally used to criminalize and investigate illegal access to computer systems pertaining to the State, including information systems of the national financial and banking entities.

Regarding existing case law, please note that we could not have access to this information from the national investigative authorities.

Once again, it is worth pointing out that in practice, there is no sufficient evidence to conclude that minors that commit these types of conducts are being prosecuted by the national law enforcement authorities.

Question 14: Can minors be punished for acts of using any instance of Cybercrime as a Service? If yes, under what qualification? If criminal sanctions could apply, are minors prosecuted in practice?
Answer:
Please explain the applicable rules (all applicable legal qualifications/articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.
Please provide case law to illustrate the application of the rules in practice.
Please provide details on known issues of application.

The answer is NO. Neither the *Federal Criminal Code* nor the *National Law of the Comprehensive Criminal Justice System for Adolescents* criminalize acts using any instance of cybercrime as a service (CasS) by minors.

4. General questions regarding cross border cybercrime, international legal instruments applicable to fighting cybercrime and regarding international cooperation

Question 15: How does your country deal with the cross-border nature of many cybercrimes? When is jurisdiction established? Can judgements have extra-territorial effect?
Answer:
Please explain the applicable rules or policies, if any, and their impact in practice.
If there is a specific impact on cybercrime committed by minors, please explain this as well.
Please provide details on known issues of application.

Unfortunately, Mexico is not yet a party to the *Council of Europe Convention on Cybercrime* (Budapest Convention) or the *Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention) which are two of the main relevant international instruments used to deal with cross-border related cybercrime investigations. Mexico is only part of the *UN Convention on Transnational Organized Crime* (Palermo Convention), however, there is not much evidence that this instrument is currently being used for cross-border investigations related to cybercrime.

For aspects concerning cybercrime jurisdiction and international cooperation in Mexico, see the monograph *Cyber Law in Mexico*, Fourth Edition, Wolters Kluwer, 2019. See Part IX Computer and Internet related Crime, paragraphs 756-760 and paragraphs 762-765, available upon request to Jos Dumortier or for purchase at:
https://law-store.wolterskluwer.com/s/product/cyber-law-in-mexico-4e/01t0f00000NY5cA

Question 16: What international legal instruments (bi-lateral, multi-lateral) apply in your country to the fight against (cross-border) cybercrime and how have they been implemented in national law (if implementation is necessary)?
Answer:
Please explain the applicable legal instruments (Budapest Convention, bilateral treaties), if any, their implementation in national law (if necessary) and their impact in practice.
If there is a specific impact on cybercrime committed by minors, please explain this as well.
Please provide details on known issues of application.

See the answers to Question 15.

Question 17: What forms of international cooperation exist in your country to the fight against cross-border cybercrime? Please describe different routes/options/procedures and the measures that can be requested (e.g. asking for investigative actions, exchange of information/evidence, etc.)?
Answer:
Please explain the applicable rules or policies, if any, and their impact in practice. E.g. Mutual Legal Assistance (based on a specific bi-lateral treaty, or on the Budapest Convention and national law or purely on the basis of national law), EU instruments, participation in INTERPOL Cybercrime Information Sharing, etc.
If there is a specific impact on cybercrime committed by minors, please explain this as well.
Please provide details on known issues of application.

The national law enforcement authorities in Mexico rely mostly in the provisions on mutual legal assistance contained in the *UN Palermo Convention* and the provisions on international cooperation of the *National Criminal Procedural Code*, as well as the current bilateral agreements that Mexico has entered with other countries to request the exchange of information and the preservation of electronic evidence concerning investigation of cross-border cybercrime.

Question 18: Do the rules (national, international) and policies mentioned in your answers in this section have any particular effect or impact on cybercrime committed by minors?
Answer:
Please indicate relevant rules or policies, if any, and their impact on cybercrime committed by minors in practice.
Please provide details on known issues of application.

The answer is NO, the international instruments and national laws mentioned in the previous question are used irrespective of cybercrime conducts committed by minors or persons under 18 years of age. Said rules and national laws do not specifically provide a distinction or special treatment to minors.

5. Other

Question 19: Do you have any information on the rates/statistics of cybercrime in your country and their recent evolution? Of particular interest would be statistics related specifically to the crimes covered in this questionnaire and statistics on cybercrime by minors (ideally also specifically for the crimes covered above)? If there were any (relatively) recent legislative or policy changes, please try to find statistical information on how this has impacted the incidence of cybercrime in practice, and in particular cybercrime by minors.

Answer:
Please provide us with any information from official sources you may have and, if possible, of the impact of any changes in legislation or policy.

The answer is NO, the Mexican government does not have official statistics on the national evolution of general cybercrimes and cybercrime activities conducted or committed by minors.

Further, there is no current legislative or policy changes in this field. Although there have been some law initiatives on cybercrime and cybersecurity, however, none of said law initiatives have been agreed among the Chamber of Deputies (Camara de Diputados) and the Senators Chamber (Camara de Senadores) of the National Congress.

Question 20: Do you have any other comments to make that may be relevant to your jurisdiction?
Answer:
Please provide us with any other comments you think are relevant for us to understand the legal and policy situation in your country.

For additional information on computer and internet related crime in Mexico, see the monograph *Cyber Law in Mexico*, Part IX Computer and Internet related Crime, pp. 387-431, Fourth Edition, Wolters Kluwer, 2019, available upon request to Jos Dumortier or for purchase at:
https://law-store.wolterskluwer.com/s/product/cyber-law-in-mexico-4e/01t0f00000NY5cA