**QUESTIONNAIRE**

**BRAZIL**

Mattos Filho Advogados

## 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 behaviour 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*** (further: HT) is the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking.

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 is 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.

**Overview of Brazilian criminal legislation applicable to minors**

To provide a better understanding of the answers below, we have prepared this introduction to briefly explain the main points of Brazilian criminal law system related to children, adolescents, and youth.

The Child and Adolescent Statute (Federal Law No. 8,069 of 1990 or Estatuto da Criança e Adolescente - ECA) determines that **children** are individuals up to 12 years of age, while **adolescents** are individuals between 12 and 18 years old. In addition, the Youth Statute (Federal Law No. 12,852 of 2013 or Estatuto da Juventude – EJ) states that **youth** are individuals between 15 and 29 years old. This distinction is important for criminal law since the law will establish different legal frameworks depending on whether the offender/victim is a child, an adolescent, or a youth.

Under Brazilian law[1], minors under 18 years old are non-liable[2]. For that reason, minors do not commit crimes, but "acts of infraction". For acts of infraction committed by children, protective measures are applied, as provided in Article 101 of the ECA, while for acts of infraction committed by adolescents, social-educational measures are applied, as provided in Chapter IV of the ECA.

Protective measures and social-educational measures are diverse and will be applied according to the infraction committed by the child/adolescent taking into consideration their capacity to comply with the measure determined by the judge. The legislation aims to protect the minors' rights and guarantees since they are still in a development process. Therefore, the criminal repression applicable to crimes committed by adults is not applicable to minors.

Although young people are not fully protected by the ECA, the law provides special provisions for crimes committed by young people between the ages of 18 and 21, such as compulsory release in case of internment[3] and assistance from parents, guardians or curators as established by civil or procedural law.

To conclude, it is worth pointing out that the civil emancipation of minors under 18 does not interfere with their criminal capacity to answer for their actions. Although emancipated, minors under the age of 18 remain immune from criminal prosecution.

Regarding crimes committed against minors, the ordinary criminal law procedure applies. Individuals over the age of 18 already have the criminal capacity to answer for crimes, which is why, in case of a breach of the law, penalties will be applied. In these cases, the penalty is applied according to the type of crime committed, following a case-by-case analysis. However, if a crime is committed against a minor, the penalty may be subjected to aggravating circumstances, which consist of increasing the amount of the penalty.

---

[1] Please refer to Art. 228 of the Brazilian Federal Constitution, Art. 104 of the Child and Adolescent Statute and Art. 27 of the Criminal Code.

[2] Affirming that minors are "non-liable" for their crimes means that they do not have the criminal capacity to answer for their crimes. The Brazilian legislation establishes that protective or educational measures are more adequate since these individuals are still developing.

## 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 number 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:**

*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.** Under Brazilian law, grooming can be understood as the solicitation of minors, and it is foreseen in Article 241-D of ECA. The criminal conduct consists of alluring, harassing, instigating, or forcing, by any means of communication, a child to commit a libidinous act.

The penalty is confinement, from one to three years, and fine. The same penalties are incurred by those who: (i) facilitate or induce the access to the child to material containing explicit sex or pornographic scenes with the purpose of practicing libidinous acts; and (ii) practice the conduct with the purpose of inducing the child to exhibit itself in a pornographic or sexually explicit manner.

The Superior Court of Justice (Superior Tribunal de Justiça - "STJ") has analysed the judicial competence in the judgment of cybercrimes[4]. The discussion about competence occurs considering the difficulty in establishing the origin and destination of published information. In one of the cases, a user accused of sharing child pornography via internet sought a declaration of incompetence. However, STJ ruled to maintain the competence of the Brazilian Federal Courts to judge the case, as it understood that the files made available by the Internet user could be accessed from anywhere in the world.

**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:**

[4] The Superior Court of Justice published more details on the case at: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2016/2016-05-15_08-15_Decisoes-do-STJ-fortalecem-o-combate-a-violencia-sexual-contra-criancas.aspx

*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**. The Program to Combat Systematic Intimidation (Bullying) defines *bullying* as "any act of physical or psychological, intentional and repetitive violence that occurs without evident motivation, practiced by an individual or group, against one or more people, with the aim of intimidating or attacking them, causing pain and anguish to the victim, in a relationship of power imbalance between the parties involved".[5] In addition, it defines *cyberbullying* as "systematic intimidation on the world wide web, when using its own instruments to disparage, incite violence, adulterate photos and personal data in order to create means of psychosocial embarrassment.". Bullying, when in the form of a threat, constitutes a crime provided for in Article 147 of the Brazilian Criminal Code[6]. The threat consists of intimidating, announcing, or promising to cause unjust and serious harm to the victim, through word, writing, gesture, or other symbolic means. The evil promised must be unjust and serious. The threat is consummated the moment the content of the threat reaches the victim's knowledge.

The penalty for a threat is detention, from one to six months, or a fine. Anyone can be the perpetrator of the crime of threat.

In relation to the victim, this is configured as the individual who can understand the evil character of words, writings, gestures, or any other symbolic means. Thus, the mentally ill, young children, the complete drunk are excluded from the list of victims, that is, those who are unable to understand the seriousness of the conduct.

In addition, stalking is also a crime established in Article 147-A of the Criminal Code. It is the conduct of persecuting someone, repeatedly and by any means, threatening their physical or psychological integrity, restricting their ability to move around or, in any way, invading or disturbing their sphere of freedom or privacy. Such conduct may occur through cyberstalking. The consummation of such conduct occurs at the instant in which the active agent reiterates the pursuit.

The penalty for those who commit a stalking crime is imprisonment, from six months to two years, and a fine. It should be noted that the penalty is increased by half if the crime is committed against a child, adolescent, or elderly person; against women on grounds of female status; or by means of a contest of two or more people; or with the use of a weapon.

Anyone can be an agent of stalking crime. In the same way, any person with the capacity to understand can be a victim of the crime of stalking.

Bullying can be understood as a crime of offense to honour, which is provided for in the Brazilian Criminal Code in the form of slander (Article 138), defamation (Article 139) and insult (Article 140). In crimes against honour, the rule is to pursue the penalty through private criminal action which is proposed by the victim or his/her legal representative. In these crimes, the legal interest protected is the victim's honour, that is, his/her reputation before third parties.

[5] Please refer to the following dispositions of the Program to Combat Systematic Intimidation (Federal Law No. 13,185, of November 6, 2015): Article 1(1); Article 2, sole paragraph.

Slander consists of imputing to someone, implicitly or explicitly, even if reflexively, a certain criminal fact, known to be false. For that, the agent can use words, gestures, or writings. The penalty for those who commit slander is imprisonment, from six months to two years, and a fine.

There will be slander when the alleged fact never occurred (falsehood that falls on the fact) or when the real event was not the person named as its author (falsehood that falls on the authorship of the fact).

The false imputation of a criminal misdemeanor does not characterize slander (inventive imputation of crime), but defamation (even rational for minors). A person who acts with the intention of playing *(animus jocandi*), advising (*animus consulendi*), narrating a fact, typical of the witness (*animus narrandi),* correcting (*animus corrigendi*) or defending the right (*animus defendand*) does not commit the crime described (given the absence of the subjective element).

As a rule, anyone can be an active subject of this crime, except for people who has imputability.

For most legal doctrines, the non-liable minor, practicing a fact defined as a crime (called an infraction), can be a victim of slander.

Slander against the dead is also punished[7], but since honor is an attribute of the living, their relatives will be passive agents, interested in preserving their memory (including for minors).

Defamation is the imputation of an offensive fact to someone's reputation, provided that such fact is not criminal. The means of execution is the same as for slander. The crime is consummated when third parties (even if only one) know of the dishonorable imputation. It is essential that the offense is reported to a third party. It is a formal crime, being consummated regardless of the damage to the reputation of the accused. The attempt is only possible in written form (defamatory letter intercepted by the defamed person). The penalty for those who practice defamation is imprisonment, from three months to one year, and a fine.

Article 139 of the Brazilian Criminal Code does not contain the provision of "propagating or disseminating" defamation. The omission, at first glance, can lead the careless person to think that the fact would be atypical. However, it is understood that anyone who spreads or divulges a dishonorable fact imputed to someone ends up defaming him/her, that is, practicing new defamation.

Anyone can be a victim of defamation, including minors and the dishonoured. The majority of the doctrine understands that legal entities can also be victims of this crime (but never of slander or insult). At the same time, any non-inviolable person can be an active agent of this crime.

Unlike slander, defamation against the dead is not punished.

To conclude, the insult consists in offending the dignity or decorum of someone. To insult is to emit a negative concept that affects the self-esteem of others. Honour comprises feelings related to moral attributes. If the offender attributes to the offended person the practice of vague facts, that is, without any precision, what could be slander or defamation will, in fact, become an insult.

The penalty for those who commit the crime of insult is imprisonment, from one to six months, or a fine. But if the injury consists of violence, the penalty is imprisonment, from three months to one year, and a fine, in addition to the penalty corresponding to the violence. If the insult consists of the use of elements referring to race, ethnicity, religion, origin, or the condition of an elderly or disabled person, the penalty is imprisonment from one to three years and a fine.

[7] Please refer to Article 138(2) of the Brazilian Criminal Code.

The Superior Court of Justice ("STJ") recognized that the educational establishment has a duty to guard and preserve the physical integrity of its students and must take preventive action to avoid damage or offenses to students, including cyberbullying[8].

**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 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.*

In relation to misinformation, there is no express provision for such conduct. However, those who spread false information may be liable for crimes against honour – please see question #2. Currently, the Chamber of Deputies is analysing Bill No. 2630/2020 that intends to fight the dissemination of false content on social networks and private messaging services.

Regarding online deception, the crimes of swindling, electronic fraud, fraud, and false identity - all provided for in the Criminal Code - applies. In the Criminal Misdemeanours Act (Federal Law No. 3,688, of October 3, 1941), the conduct of false alarm is also punishable.

Swindling, as provided for in Article 171 of the Criminal Code, consists of obtaining, for oneself or another, an illicit advantage, to the detriment of another, by inducing or maintaining someone in error, through artifice, trickery, or any other fraudulent means. The penalty for committing fraud is imprisonment for one to five years and a fine.

If the conduct uses information provided by the victim or a third party misled through social networks, telephone contacts or sending fraudulent electronic mail, or by any other similar fraudulent means, the penalty is imprisonment for four to eight years and a fine. Fraud, illicit advantage, and harm to others are required.

The penalty is increased by one-third (1/3) to two-thirds (2/3) if the conduct is committed using a server maintained outside Brazil. Furthermore, the penalty is increased by one-third (1/3) if the crime is committed to the detriment of a public-law entity or a popular economy institute, social assistance, or charity.

To conclude, the penalty is increased by one-third (1/3) to double if the crime is committed against an elderly or vulnerable person, considering the relevance of the onerous result.

In embezzlement, the legal asset protected is the patrimony of the deceived person. Anyone can be the active subject of this crime. Likewise, any person who suffers property damage or who was deceived by the fraudulent action undertaken by the agent can be a victim of embezzlement. The economic loss will not always fall on the person who suffered the bondage.

There is divergence in the legal literature regarding the nature of the advantage. Some legal writers claim that it can be any utility or benefit of a patrimonial nature that the agent may have to the detriment of the victim, without any legal justification. Other authors claim that it is enough for the advantage to be

[8] This was the Court's ruling on the judgment of "AREsp 1415362".

unfair. However, the advantage must necessarily be unlawful, because, if lawful, the crime will be the arbitrary exercise of one's own reasons.[9]

Even if the offended person allows himself to be deceived by the deception due to greed or for any other reason, the conduct of the embezzler is not excluded.

In this sense, the crime of false identity consists of attributing a third false identity to obtain an advantage, for one's own benefit or for someone else's benefit, or to cause harm to others[10]. Attributing comprises a commissive crime (committed by action), not occurring if the agent is silent about the mistaken identity attributed to him. For scholars, "identity" should be interpreted broadly, involving name, age, marital status, affiliation, sex, among others. It is essential that the agent practices the action aiming to obtain an advantage (of any nature), for his own benefit or that of others, or to cause harm to others. the consummation occurs when the agent attributes a false identity to himself or to someone else. It is not necessary for the agent to achieve the intended advantage or cause effective harm.

The penalty is detention, from three months to one year, or a fine, if the fact does not constitute an element of a more serious crime.

In the crime of false identity, the legal interest protected is the public faith. Anyone can be an active agent of the crime, including minors. The passive agent is the State and, secondarily, any injured person by the criminal action.

In addition, there is the false alarm, which consists of causing alarm, announcing disaster or non-existent danger, or performing any act capable of producing panic or turmoil.[11] Conduct can be practiced by various means such as written, telephone, orally. In addition, the subject who activates the public or private authority reporting a disaster or other form of danger not classified as a crime.

The penalty is simple imprisonment, from fifteen days to six months, or a fine.

Anyone can be an active subject of the false alarm. For the characterization of the misdemeanor, it is necessary for the agent to be aware that the information he is spreading is not true. In this way, the agent acts with the purpose of taking away public peace.

The protected legal interest is public order aimed at protecting the community, which is the "victim" of the conduct.

It is worth mention that Article 45 of the Criminal Misdemeanor Act punishes those who pretend to be a public servant, with the intention of obtaining an advantage due to the pretending of the position. The penalty for this conduct is simple imprisonment, from one to three months, or a fine.

Moreover, Article 47 of the Criminal Misdemeanor Act prohibits the conduct of publicly wearing a uniform or badge of a public function that he does not exercise; use, improperly, of a sign, badge, or denomination whose use is regulated by law. In practice, this can happen, for example, when a person pretends to be a police officer or delegate or other type of authority to gain an advantage. The respective penalty is a fine, if the fact does not constitute a more serious criminal offence.

**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.**

[9] See Article 345 of the Brazilian Criminal Code.
[10] Please refer to Article 307 of the Brazilian Criminal Code.
[11] The false alarm crime is provided for in Article 41 of the Criminal Misdemeanor Act.

**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:**

*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.*

*Human trafficking* is the conduct of "agency, enticement, recruiting, transporting, transferring, purchasing, housing, or receiving a person, through serious threat, violence, coercion, fraud or abuse, with the purpose of (i) remove organs, tissues or body parts; (ii) subjecting her to work in conditions similar to slavery; (iii) subject it to any type of servitude; (iv) illegal adoption; or (v) sexual exploitation.[12] These actions include:

- Removing organs: The removal of organs, tissues or body parts is governed by Federal Law No. 9,434/97. Post-mortem removal of tissues, organs or parts of the human body intended for transplantation or treatment is permitted, if brain death is diagnosed by two physicians who are not part of the transplant team (Article 3). The Law also allows the legally capable person to freely dispose of tissues, organs, and parts of the living body, for therapeutic purposes or for transplants in a spouse, blood relatives up to the fourth degree, even if he preferably authorizes in writing and in front of witnesses, specifically the tissue, organ or part of the body being removed.
- Submitting to work in conditions analogous to slavery: This purpose refers directly to the crime of Article 149 of the Criminal Code, which punishes the conduct of reducing someone to a condition analogous to that of a slave.
- Subjecting to any type of servitude: The purpose of committing human trafficking to subject the individual to any type of servitude does not find a specific corresponding autonomously typified in criminal legislation. It is understood, based on other international regulations, that the conduct of this wording may be included in the conduct characterized in the previous item.
- Illegal adoption: The criminal type is not restricted to human trafficking for the purpose of the illegal adoption of minors through human trafficking. Due to the complex process of adoption of children and adolescents, permeated by rules that aim to protect the adoptee, rules that are not repeated in the adoption of adults, except regarding guidelines such as the minimum age difference between adopters and adopted and the prohibition of adoption of descendants by ascendants and between siblings.
- Sexual exploitation: As per relevant studies on the field, sexual exploitation can be defined as a domination and abuse of the body of children, adolescents, and adults (offer), by sexual exploiters (merchants), organized, often in a network of local and global commercialization (market), or by parents or guardians, and by consumers of paid sexual services (demand), admitting four modalities:
- Prostitution: activity in which sexual acts are negotiated in exchange for payment, not just monetary;
- Sex tourism: is the sex trade, well-articulated, in tourist cities, involving national and foreign tourists and mainly young women;

[12] Please refer to Article 149-A of the Brazilian Criminal Code.

- Pornography: production, exhibition, distribution, sale, purchase, possession and use of pornographic material, also present in literature, cinema, advertising, etc.; and
- Trafficking for sexual purposes: clandestine and illicit movement of people across national borders, with the objective of forcing adults, adolescents, and children, mainly women, to enter sexually oppressive and exploitative situations, for the profit of enticers, traffickers.

The crime is consummated with the performance of the actions provided for in the criminal type, regardless of the effective exercise of the purpose that moves the agent. In the subject, induce, attract, and facilitate modalities, the crime is consummated at the moment the victim begins to dedicate itself to prostitution, constantly placing itself at the disposal of clients, even if he/her has not attended any. In the modality of preventing or hindering the abandonment of prostitution, the crime is consummated when the victim decides to leave the activity and the agent prevents this attempt, delaying the consummation during the entire period of embarrassment (as a permanent crime). The attempt is possible in all modalities (the agent performs the acts able to complete the conduct and does not achieve his purpose due to circumstances beyond his control).

The penalty is imprisonment from four to eight years and a fine. The penalty is increased from one-third to one-half if (i) the crime is committed by a public official in the exercise of his functions or on the pretext of exercising them; (ii) the crime is committed against a child, adolescent or elderly person or person with a disability; (iii) the agent takes advantage of kinship, domestic, cohabitation, hospitality, economic dependence, authority or hierarchical superiority inherent to the exercise of employment, position or function; or (iv) the victim of trafficking in persons is removed from the national territory.

It is important to note that with the enactment of Federal Law No. 13,344/16, the Brazilian legislator migrated the use of violence or fraud of increase to the alternative execution of the crime of trafficking in persons. Therefore, without violence, coercion, fraud or abuse, there would be no crime. Faced with this new scenario, the valid consent of the person excludes typicality, following, in this regard, the Additional Protocol to the United Nations Convention against Transnational Organized Crime on the Prevention, Suppression and Punishment of Trafficking in Persons, which in Article 3 (a) and (b), alert:

1. The recruitment, transport, transfer, housing, or reception of persons, using the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of authority or a situation of vulnerability or the giving or acceptance of payments or benefits to obtain the consent of a person having authority over another for the purposes of exploitation
2. The consent given by the victim of trafficking in persons with a view to any type of exploitation described in subparagraph a) of this Article shall be considered irrelevant if any of the means referred to in subparagraph a) have been used."

The judge, therefore, will assess the validity of the offended party's consent based on the circumstances of the specific case, presuming dissent:

1. If consent is obtained through threat or use of force or other forms of coercion, kidnapping - kidnapping or false imprisonment, fraud, deception;
2. Whether the agent abused authority to gain the victim's consent;
3. If the offended who approved your trade is vulnerable;
4. If the injured party acquiesced in exchange for the delivery or acceptance of payments or benefits.

The penalty is reduced from one to two thirds if the agent is a primary and does not belong to a criminal organization.

Any person can be an active subject of human trafficking, either acting as an "entrepreneur or employee of the human trafficking" or as a consumer of the trafficked "product". Likewise, anyone can be a victim.

The peculiarity of this crime is that, as sexual exploitation is part of the conduct, some scholars believe that if the crime is committed against a child or adolescent, Article 11(V) of the Criminal Code applies, which provides that the statute of limitations will run from the date on which the person turns 18 years old.

The possibility of the minor's participation as a participant or in a contest of people is not excluded, as provided for in Article 29 of the Criminal Code.

It should also be noted that Article 218-B of the Criminal Code, which provides for the promotion of prostitution or any other form of sexual exploitation of children or adolescents, or vulnerable persons. Such a crime consists of submitting, inducing, or attracting to prostitution or any other form of sexual exploitation someone under 18 years old or who, due to mental illness or disability, does not have the necessary discernment to perform the act, facilitates, impedes, or hinders that abandon him/her.

The penalty is imprisonment from four to ten years. If the crime is committed with the aim of obtaining economic advantage, a fine is also applied.

The same penalties apply: (i) whoever practices sexual intercourse or other lewd acts with someone under 18 and over 14 years old in the situation described in Article 218; (ii) the owner, manager, or person in charge of the place where the practices referred to in the caput of this article take place.

In this crime, the legal interest protected is the sexual dignity of the vulnerable who is subjected, induced, or attracted to prostitution.

Anyone can be an active agent of this crime. In relation to the taxable person, only persons under 18 years old or who, due to illness or mental disability, do not have the necessary discernment to practice the act, whether male or female, can be victims.

Finally, in relation to online grooming, the same provisions as in the answer to question 1 apply.

## 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.**

**Answer:**

*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.*

As mentioned above in "Overview of Brazilian criminal legislation applicable to minors", under Brazilian law, minors under 18 years old lack criminal capacity and therefore do not commit crimes, but "acts of infraction". For acts of infraction committed by children, protective measures are applied, as provided in Article 101 of the ECA, while for acts of infraction committed by adolescents, social-educational measures are applied, as provided in Chapter IV of the ECA.

Protective measures and social-educational measures are diverse and will be applied according to the infraction committed by the child/adolescent taking into consideration their capacity to comply with the measure determined by the judge.

According to Article 112 of the ECA, the following socio-educational measures are applicable to adolescents who commit infractions: (i) warning; (ii) obligation to repair the damage; (iii) provision of services to the community; (iv) assisted liberty; (v) insertion in a semi-liberty regime; (vi) admission to an educational establishment; (vii) forwarding to parents or guardians, by means of a disclaimer; (viii) temporary guidance, support and follow-up; (ix) mandatory enrolment and attendance at an official elementary school; (x) inclusion in official or community services and programs for the protection, support and promotion of families, children and adolescents; (xi) request for medical, psychological or psychiatric treatment, in a hospital or outpatient basis; (xii) inclusion in an official or community program of assistance, guidance and treatment for alcoholics and drug addicts; (xiii) institutional reception; (xiv) inclusion in a foster family program; and (xv) placement in a surrogate family.

ECA also establishes that the measure applied to the adolescent will consider his ability to comply with it, the circumstances, and the seriousness of the infraction. In addition, under no circumstances and under any pretext shall the provision of forced labour be permitted. Furthermore, adolescents with mental illness or disability will receive individual and specialized treatment, in a place appropriate to their conditions.

**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.*

There are no specific rules for minors in this regard. Minors who commit a crime are subject to socio-educational measures.

**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.*

There are no specific rules for minors in this regard. The same logic applies to other crimes: minors who commit a crime are subject to socio-educational measures, because of the infraction described as a crime or criminal misdemeanour.

**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.*

There are no specific rules for minors in this regard. The same logic applies to other crimes: minors who commit a crime are subject to socio-educational measures, because of the infraction described as a crime or criminal misdemeanour.

**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.*

**Yes**. As mentioned in Question 2, according to Brazilian Law, bullying is "any act of physical or *psychological*, intentional and repetitive violence that occurs without evident motivation, practiced by an individual or group, against one or more people, with the aim of intimidating or attacking them, causing pain and anguish to the victim, in a relationship of power imbalance between the parties involved." In addition, cyberbullying is "systematic intimidation on the world wide web, when using its

own instruments to disparage, incite violence, adulterate photos and personal data in order to create means of psychosocial embarrassment." Therefore, minors who commit a crime are subject to socio-educational measures.

**Question 10: Can minors be punished for wilful 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.*

**Yes.** As in Question 3, the crimes of Slander (Article 138, Criminal Code), Defamation (Article 139, Criminal Code), Swindling (Article 171, Criminal Code), False Identity (Article 307, Criminal Code), False Alarm (Article 41, Law of Misdemeanours), Pretending to be a Public Official (Article 45, Law of Misdemeanours), and Illegal Exercise of a Profession (Article 47, Criminal Misdemeanours Act) applies to this conduct, whenever the minor uses the cyberspace in a way that the crimes can be verified.

All the crimes described above can be committed by minors because they are "common" crimes, which means they can be committed by any individual, not requiring specific characteristics or age. Therefore, if a minor commits the typical conduct, as described in question #3, he/she can be prosecuted and penalized for an infraction corresponding to the criminalized conduct.

In addition, there is a feasible possibility that electoral crimes that punish the individual who creates or disseminates false information can be applied to minors:

- Slander (Electoral): The act of slandering someone in electoral propaganda, or for propaganda purposes, falsely imputing to them a fact defined as a crime is punishable[13]. The same penalty is incurred by the person who spreads or disseminates the information, knowing it to be false. It can be spread by any means that divulges the false imputation.

  The crime is configured even when the accusation is of non-electoral crimes, involving practices carried out before the election. However, the false criminal accusation must occur during the campaign period. If it was made previously, this is not an electoral crime, but a common criminal law offense.

  Slander is the imputation of a crime to another that is known not to exist, not corresponding to the truth. Therefore, the person who creates the false accusation and the one who spreads it are punished in the same way.

  The active agent, although in most cases candidates or members of political parties, can be any voter while the passive subject can be any citizen, even those who are not directly involved in the electoral process.

[13] Please refer to the following dispositions of the Brazilian Electoral Code: Article 324; Article 324(1)(2).

Proof of truth consists in verifying that the imputation made is true. About the above-mentioned persons, this exception is not permitted due to the principle of presumption of innocence, the magnitude of the position held, and the security of judicial decisions.

Proof of the truth of the alleged fact excludes the crime, but is not admitted in the following cases: a) if, since the alleged fact constitutes a private action crime, the victim has not been convicted by unappealable decision; b) if the fact is alleged against the President of the Republic or the head of a foreign government; c) if the victim of the alleged crime, although a public action crime, has been acquitted by unappealable decision.

- **Defamation (Electoral):** This crime aims to prevent the defamation of someone in electoral propaganda, or for propaganda purposes, by imputing to him a fact that is offensive to his reputation (Article 325 of the Electoral Code). Defamation is the targeting of an offensive fact to the honour of a citizen, narrating the circumstances of this fact. It can be implemented by any means that discloses the imputed facts.

  Its active agent can be any citizen, whether a candidate or a common citizen. Classifying it as a formal crime, it does not depend on the demonstration of damage.

  The crime is also configured when the accusation is of non-electoral crimes, involving practices performed before the election, but it is necessary that the false criminal accusation occurs during the campaign period. If it was made beforehand, this electoral crime is not committed, but remains in the sphere of common criminal law. It is enough that the defamatory conduct be practiced in the typical scope of electoral propaganda for the crime to occur.

  Since the fact affects people's honour, the exception of the truth is only admissible if the offended person is a public official and the offense is related to the exercise of their functions, because the protection of public res obliges them to blameless conduct (Article 325, sole paragraph, of the Electoral Code).

In theory, both crimes can be committed by minors. According to jurisprudence, minors can commit electoral crimes. According to jurisprudence, the competence to judge an infraction that is equivalent to an electoral crime lies with the Juvenile Court. Therefore, the conduct of a minor, if it fits the penal type, can be subject to prosecution. However, no jurisprudence was found that constitutes a precedent for the criminal types described, having a minor as the agent.

**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.*

**Yes.** The crimes of Human Trafficking and Promoting Prostitution specifically for minors[14] are also applicable when the perpetrator is a minor – please see question #4. Since these are common crimes, minors can also commit them as an infraction equivalent to the crime in question. However, minors are subject to the special regime provided for in the ECA.

In addition, nothing prevents the minor from also committing the crime of promoting prostitution in relation to adult individuals. Therefore, Article 228 of the Criminal Code (Promoting Prostitution) is also applicable, which consists of inducing or attracting someone to prostitution or another form of sexual exploitation, facilitating it, or preventing or hindering someone from leaving it.

The crime is outlined in the Brazilian Criminal Code, and it aims to protect the sexual dignity of the victim and can be committed by anyone (common crime). Any person can also be a victim, and no special quality is required of the passive subject.

The agent's conduct consists of performing any one of the five typical nuclear actions: induce (inspire, instigate), attract (entice), someone to prostitution or another form of sexual exploitation, facilitate it (provide someone with means, remove difficulties), impede (oppose) or make it difficult (create obstacles) for someone to abandon it.

The promotion may occur through action or omission, the latter in the hypothesis that the agent, who is under a legal duty to prevent the victim from entering prostitution, does nothing, subjectively adhering to the conduct.

Only the agent who acts maliciously, aware that they are inducing or attracting someone to prostitution or another form of sexual exploitation, facilitating it or preventing someone from abandoning it, commits the crime.

The consummation of the crime varies according to the modality described in the type:

> a) Inducing, attracting, or facilitating: the offense is consummated at the moment in which the victim begins to engage in prostitution or another form of sexual exploitation, placing themselves, in a constant manner, at the disposal of clients, even if they have not served any.
>
> b) Impeding or hindering the abandonment of sexual exploitation is consummated at the moment in which the victim decides to leave the activity and is hindered (permanent crime).

The criminal action is public and unconditional, which means the crime can be prosecuted even if the victim does not press charges.

We have not found instances where minors were effectively convicted of these charges, however, it could possibly be due to the fact these processes usually occur in secrecy to protect the minor (agent) and the victim, which could also be a minor.

**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:**

[14] Please refer to the following dispositions of the Brazilian Criminal Code: Article 149-A; and Article 218-B.

*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.** According to the Criminal Code, it is a criminal conduct to violate the copyright of another individual.[15]The Brazilian Criminal Code aims to guarantee to the author the right of paternity of the work and to enable him to derive pecuniary benefits from its reproduction, representation, performance, recitation, adaptation, transposition, arrangements, dramatization, translation, and radio broadcasting.

Any person can commit the crime and, therefore, nothing prevents a minor from committing an infraction equivalent to this conduct (common crime).

The victim will be, in principle, the author of the work, unless it has been transmitted to the heirs or to a legal entity (of public or private law), hypothesis in which they will figure in the passive pole.

The conduct typified in the caput foresees only one nucleus: to violate, which means to transgress, disrespect, offend the author's right by publishing, reproducing, or modifying, by default, his work. It is a blank criminal rule, whose content (copyright) must be complemented by Federal Law No. 9,610/1998.

For the crime to be established, it is necessary the wilful intent to violate the author's rights, that is, the conscious will to violate the copyright of another person. The consummation moment will depend on the type of violation. Finally, the attempt may be admitted in those modalities in which the fractioning of the execution is possible.

A portion of the doctrine understands that the provision of Article 29, IX, of Law No. 9,610/98, which determines that storage in a computer is a form of violation, makes the conduct of downloading a copyrighted work typical according to Article 184 of the Criminal Code.

For this reason, it is perfectly possible for minors to be prosecuted for this crime. However, there is a trend, identified in the jurisprudence, that the crime has been attributed only to agents who use the violation for profit, although this element is not required for its configuration.

We have not found instances where minors were effectively convicted of these charges, however, it could possibly be due to the fact these processes usually occur in secrecy to protect the minor (agent) and the victim, which could also be a minor.

**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.*

[15] See Article 184 of the Brazilian Criminal Code.

**Yes.** According to Criminal Code, the action of accessing or invading another individual's computing device (including smartphones, tablets, or others), without due authorization constitutes a crime.[16]

The typification of this crime aims to protect the inviolability of secrets, whose protection is focused on intimacy, private life, honor, inviolability of communication and correspondence, in short, the free manifestation of thought, without any interference from third parties. The typical incriminating figure seeks to punish those who violate not only the telematic communication, but also the computer devices, which keep relevant data of its owner.

Any person, including minors, can be victim or agent of this crime. As for the active agent, no special quality is required, which is why it doesn't matter whether he/she is a computer technician or an adventurer in the area. As far as the subject of the crime is concerned, it is pointed out that the computer device belongs to another person in any capacity (ownership or possession).

The crime is committed by anyone who breaks into (violates, transgresses, enters by force somewhere) a computer device. The agent's conduct is not simply to enter another's computing device but to occupy an unpermitted space.[17] Such a computing device needs to be alien (belonging to a third person). Express mention is made to the state of the device regarding the computer network, including, of course, the Internet, as it doesn't matter if there is a connection or not.

Finally, the other conduct, of an alternative character, is to install (prepare something to work) vulnerability (mechanisms capable of generating openings or flanks in any system). The purpose of the agent is to obtain any illicit advantage by making the computing device accessible for violation. It is important to point out that performing the invasion or the installation constitutes an alternative mixed type, that is, committing one or both conducts imply a single crime. Note that the mere installation of vulnerability (e.g., malicious software that allows access to the content of the computer device as soon as it is connected to the network) does not cause the violation but its preparation. In case the agent installs it, but another person invades, each one commits a different crime, both typified in Article 154-A. If two people, working together, divide tasks (one installs; the other invades), it is a single crime, with multiple agents (Article 29 of the Criminal Code).

For the crime to be configured, it is also necessary that the invasion of a computer device be done with the purpose of obtaining, altering, or destroying data or information, with conscious will. The focus is on the obtaining (having access to something), alteration (modification of the original state) or destruction (total or partial elimination) of data (elements appropriate for the use of something) or information (knowledge of something in relation to a person, thing, or situation). As for the installation of vulnerability, it must have the purpose of obtaining an illicit advantage (any profit or gain contrary to the legal system). It can even be the obtaining of the invasion of the computer device at a later time to obtain data and information.

The crime is consummated the moment the agent invades the victim's computer device, by means of undue violation of security mechanisms, or installs vulnerabilities in it, regardless of the production of the result sought by the invader (tampering with or destruction of the victim's data or information or obtaining illicit advantage).

In the crimes defined in Article 154-A, the accusation can only be made through a complaint from the victim (press charges), except when the crime is committed against the direct or indirect public

[16] Please refer to Article 154-A of the Brazilian Criminal Code.

[17] The legal doctrine understands as computer devices any desktop computers, notebooks, tablets, laptops, as well as smartphones, which today constitute true "mini-computers", among others to emerge with the same purpose.

administration of any of the powers of the Union, the States, the Federal District or Municipalities, or against public service concessionaires.

There are reports[18] of minors being apprehended by authorities for acts of hacking or correlated actions, however, we have not found case law to prove that minors are being convicted of such crimes.

**Question 14: Can minors be punished for acts of using Cybercrime as a Service? If yes, under what qualification? In particular, how would this apply to using such services for exploiting vulnerabilities in IoT and connected devices e.g., the device of a friend or acquaintance? Does it matter if the intent is somewhat innocent (i.e., the minor thinks it's a joke or a prank)? 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.*

In Brazil, there is no rule that specifically penalizes the act of using cybercrime as a service. However, due to the existence of elements of a crime for cybercrimes (see Article 154-A of the Criminal Code), if a person contracts the performance of a cybercrime, it is possible that he/she will be punished under the dictates of the Brazilian legislation in the condition of concerted action.

Article 29 of the Criminal Code defines concerted action as the crimes in which more than one person contributes to the criminal result, so that each one will answer in the measure of their guilty. For the existence of concerted action, it is necessary plurality of agents and conducts, besides causation between those conducts, and the awareness, on the part of the agents, that they are cooperating for a criminal purpose.

Therefore, considering the engagement of a cybercrime, the one that performs the typical act, would be the author, while the person who pays for it would be an accessory, because, although it contributes directly to the performance of the criminal type, it is not the one who performs the criminal practice, reason why it cannot be deemed as the author of the crime. Therefore, each one answers according to the contribution to the criminal practice

Although there is no criminal typification for the engagement of cybercrimes, the law provides aggravating factors for criminal penalties in cases where criminal actions are committed by means of violence. Article 62 (IV) of the Criminal Code provides that the penalty will be aggravated in relation to the agent who executes the crime or participates in it by means of payment or promise of reward.

Therefore, if a person breaks into an electronic device (criminal action, according to article 154-A of the Criminal Code) in exchange for a reward, in addition to suffering the sanction present in the legal provision, **the agent will have an aggravated punishment since the crime was carried out by contracting a third party.**

[18] "Hacker child apprehended in Baixada Fluminense created a program to swindle when he was 13". Accessed in: Jun 14, 2022. Link

Since we are specifically considering the engagement of a cybercrime, a hypothesis in which the agent pays for the accomplishment of the criminal practice, the Brazilian criminal law does not admit guilt in this case, so that if the minor participates in the crime, even if thinking it is a "joke", it will have no relevance in the contract case.

Note that if this crime is committed by a minor, the typification of the crime, i.e., its description under Brazilian criminal law remains the same, so that what changes is only the type of sanction applied, as explained in the brief introduction present in this questionnaire.

We have not found instances where minors were effectively convicted of these charges. However, it could possibly be due to the fact these processes usually occur under judicial secrecy to protect the minor (agent) and the victim.

## 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.*

The way Brazilian law deals with cross-border cybercrimes are the same for all cases. In fact, it is the same for crimes committed on the internet or not. Therefore, it is necessary to evaluate all the legal mechanisms present in the Brazilian legal system to deal with cross-border crimes.

The application of Brazilian jurisdiction in case of crimes is regulated by two laws.

The first is the Law of Introduction to the Rules of Brazilian Law (Federal Law No. 4,567/1942 or LINDB). Article 12 determines that the Brazilian judicial authority is competent to judge in cases where the defendant is domiciled in Brazil. Article 15 provides that a judgment declared abroad may be enforced in Brazil if (i) it was declared by a competent judge; (ii) the parties have been served with process of summons or there is a legal default; (iii) it has been adjudicated and is vested with the formalities necessary for enforcement where it was declared; (iv) it has been translated by an authorized interpreter; and (iv) it has been homologated by the Federal Supreme Court (this legal obligation is also provided for in Article 105 (I)(i) of the Federal Constitution). The presence of all these elements is necessary for a judgment declared abroad to be enforced in Brazilian territory.

Although Brazilian law adopts a jurisdiction friendly to other legislations, Article 17 is clear in establishing that laws, acts and sentences from other countries, as well as any declarations of will, will not be effective in Brazil when they offend national sovereignty, public order, and good customs.

The second law that regulates Brazilian jurisdiction in criminal cases is the Brazilian Criminal Code. Article 5 determines that Brazilian law is applied in cases where crimes are committed within the national territory, without prejudice to the application of conventions, treaties, and rules of international law.

In this sense, for criminal purposes, paragraph 1 considers the extension of the national territory to include Brazilian ships and aircraft, of a public nature or at the service of the Brazilian government wherever they may be, as well as Brazilian merchant or privately owned ships and aircraft that are, respectively, in the corresponding airspace or on the high seas. Paragraph 2 has the same concept, determining that Brazilian law is also applicable to crimes committed on board foreign aircraft or ships of private property, when the former is landing in the national territory or flying in the corresponding airspace, and the latter in port or territorial sea of Brazil.

Article 7(I) of this Law deals with the cases of extraterritoriality of the Brazilian criminal law (cases of application of the Brazilian criminal law for crimes committed beyond the national territory). Therefore, crimes committed against the life or liberty of the President of the Republic; against the assets or the public faith of the Union, the Federal District, the State, the Territory, the Municipality, a public company, a mixed-economy society, an autarchy or foundation established by the Public Power; against the public administration, by those in its service; and genocide, when the agent is Brazilian or domiciled in Brazil, are punished according to Brazilian law regardless of whether the agent has been acquitted or convicted abroad.

Article 7(II) determines the application of Brazilian criminal legislation for crimes that, by treaty or convention, Brazil is obliged to repress; committed by Brazilians and committed on Brazilian aircraft or vessels, merchant or privately owned, present in foreign territory, and are not judged there. However, paragraph 2 determines that the provisions of Article 7 (II), will only apply if the following requirements are cumulatively present: (i) the agent enters national territory; (ii) the fact is also punishable in the country where it was committed; (iii) Brazilian law allows extradition for the crime committed; (iv) the agent has not been acquitted abroad or has not served a sentence; and (v) the agent has not been pardoned abroad or his guilty has not been extinguished.

To conclude, Article 9 regulates the effectiveness of the foreign judgment, determining that if it produces the same effects as would occur in Brazil, it may be enforced in cases of compensation for damages, restitution, and other civil effects and security measures.

**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.*

The Budapest Convention, also known as the Convention on Cybercrime, is the only international legal instrument applicable in Brazil to fight cross-border cybercrimes. In general, the Convention aims to establish a common criminal policy among the signatory states to ensure a safe cyber environment for society.

As it is a multilateral treaty, which creates a legal bond between the signatory state and the international treaty, the signatory States have the obligation to observe all the obligations and values therein, under penalty of having a reaction from the other signatory states of the treaty. However, it is important to

note that the Budapest Convention does not create the types of criminal offences contained therein, since only the National Congress has the competence to determine what is and what is not a crime in Brazil.

The Budapest Convention establishes the crimes for which States must adopt legislation and other measures to combat, such as: illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights, and attempt and aiding. In addition, it also sets out guidelines for the realization of procedural laws related to cybercrime and for international cooperation.

The Convention was recently acceded by the Brazilian State (the Federal Senate ratified the Convention on December 15th, 2021), thereby there are still few implementation mechanisms. Among them, the realization of workshops and webinars by the Federal Public Ministry ("Ministério Público Federal - MPF") to explain the application of the Convention in the Brazilian legal system for members and servants of the MPF, state public prosecution offices and judges.

**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.*

Brazilian legislation establishes several forms of international legal cooperation in legal and procedural terms – please see question #15. However, in addition to these implements, Brazil also contributes through international conventions, treaties, and projects with the specific purpose of fighting cybercrime.

The main forms of international legal cooperation to fight cybercrime are those provided in Chapter III of the Budapest Convention. It provides for the following forms of cooperation: extradition, mutual assistance as established by the Convention, spontaneous offering of information, confidentiality, preservation of stored computer data, cross-border access to stored computer data, and contact network available 24 hours a day, 7 days a week. As the country has recently joined the Convention, there is still not enough data to determine the impacts of these measures in the fight against cybercrime in Brazil, especially regarding crimes committed by minors.

Another form of international cooperation of which Brazil is a part is INTERPOL. In addition to its usual function of helping the country to protect itself from global crimes, there is a specific project to fight cybercrime, the Cybercrime Capacity Building Project in Americas which aims to increase the capacity of Latin American police to investigate and fight cybercrime.

Furthermore, Brazil is also a member of the United Nations ("UN") commission that fights drugs and crime, following the guidelines established by the UN. One of the formal measures taken by Brazil is the provision of legal assistance to other States if reciprocity is guaranteed.

**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.*

**No.** The mentioned rules and policies do not have a specific impact for cybercrimes committed by minors. Moreover, as Brazil's adhesion to the Cybercrime Convention is quite recent, there are still not enough elements to assess its impact on the Brazilian society, especially in the field of crimes committed by 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.*

In relation to cybercrimes in general, a survey done by the German consulting company Roland Berger revealed that, in relation to virtual crimes, Brazil is the fifth largest target in the world. The Roland Berger survey indicates that Brazil has already surpassed last year's volume of attacks only in the first half of 2021, with a total of 9.1 million cases, taking into account only the crimes of digital kidnapping (ransomware).[19]

Furthermore, Brazil currently has 24.3 million children and adolescents who use the Internet. This number is equivalent to 86% of people between 9 and 17 years old.[20]

Reports of exposure of children and adolescents on the Internet are among the five types of violations most reported to Dial 100. The survey on this type of violence, considering the place where it occurs, includes cases of pedophilia, cyberbullying and child pornography. Data from Safer Net Brazil show that in 2018, Brazil recorded a total of 133,732 complaints of virtual offenses, 110% more compared to the previous year. The main crime reported was child pornography.

---

[19] It is possible to find more details at: https://canaltech.com.br/seguranca/brasil-e-o-5o-maior-alvo-de-crimes-digitais-no-mundo-em-2021-195628/

[20] Survey on Internet Use by Children in Brazil. ICT KIDS ONLINE BRAZIL. 2020. https://cetic.br/media/docs/publicacoes/2/20211125083634/tic_kids_online_2020_livro_eletronico.pdf

According to the organization, in the last 14 years, more than 4.1 million anonymous complaints were counted against 790,000 electronic addresses for disseminating inappropriate content on the Internet. Also in 2019, according to Tic Kids, 18% of boys, between 9 and 17 years old, have seen an image or video of sexual content on the internet; 20% of them have received messages of sexual content; and 13% of girls, between 9 and 17 years old, have been asked to send intimate photos or videos.[21]

Finally, we are not aware of any specific statistical survey on cybercrimes committed by minors in Brazil.

**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.*

We do not have any further comments. To understand the legal and policy situation in Brazil, please refer to the "Overview of Brazilian criminal legislation applicable to minors". In addition, please find below a summary with main definitions and helpful resources regarding the legislation mentioned in this questionnaire.

| **Main definitions** | |
|---|---|
| "ECA" | The Child and Adolescent Statute/Estatuto da Criança e Adolescente (PT)<br>Federal Law No. 8,069 of 1990 |
| "EJ" | Youth Statute/Estatuto da Juventude (PT)<br>Federal Law No. 12,852 of 2013 |
| "STF" | Brazilian Supreme Court |
| "STJ" | Superior Court of Justice/Superior Tribunal de Justiça (PT) |
| "MPF" | Federal Public Ministry/Ministério Público Federal (PT) |
| "UN" | United Nations/Organização das Nações Unidas (PT) |
| **Legislation** | |
| Brazilian Criminal Code | |
| ECA / EJ | |
| Brazilian Electoral Code | |
| Criminal Misdemeanours Act | |
| LINDB | |
| Legislative Decree No. 37 of 2021 – The Budapest Convention | |
| Program to Combat Systematic Intimidation (Bullying) | |

***

[21] Information extracted from a publication on the website of the Ministry of Women, Family and Human Rights of Brazil available at https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet-ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100

*Written by Mattos Filho Advogados in June 2022 as part of the Rayuela Project.*