QUESTIONNAIRE

RUSSIAN FEDERATION

Maria OSTASHENKO

ALRUD Law Firm

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.

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

Question 1: Is online grooming punishable by law in your country?

Answer:

Applicable rules

There are no direct rules that imply liability for online grooming in Russia. As a reference, in 2015, there had been an attempt to criminalize online grooming as the respective draft law was introduced. Nevertheless, it has not passed.

Nevertheless, there are several general criminal offences in Russian criminal law that may be applicable to actions undertaken in relation to minors in the course of online grooming as provided by the Criminal Code of the Russian Federation ("**Criminal Code**"):

i. Coercion to acts of a sexual nature in relation to minor (article 133 (2) of the Criminal Code)

Conditions for applicability: coercion is executed (i) by means of blackmail, threats of destruction, damage or seizure of property or (ii) by means of the use of the victim's material or other dependence.

Therefore, the application is quite limited. As the Supreme Court of the Russian Federation ("**Supreme Court**") stated, the actions of a person who obtains the consent of the victim to engage in sexual intercourse or to commit acts of a sexual nature by deception or breach of trust cannot be regarded as coercion to acts of a sexual nature or as other crimes against sexual inviolability and sexual freedom of the person[1]. It means that engagement of minor into sexual acts by means of emotional/romantic attachment is not punishable under the cited article.

Criminal sanctions: (i) compulsory labour for a term of up to 5 years with deprivation of the right to hold definite offices or to engage in definite activities for a term of up to 3 years or (ii) without such or by deprivation of liberty for a term of up to 5 years with deprivation of the right to hold definite offices or to engage in definite activities for a term of up to 3 years or without such.

Prescriptive period: 2 years.

ii. Depraved Actions (article 135 of the Criminal Code)

Conditions for applicability: committing any actions without violence were intended to satisfy the sexual desire of the perpetrator, or to arouse sexual arousal in the victim, or to arouse his interest in sexual relations.

The position of the Supreme Court is that actions with no direct physical contact with the victim may also be considered as **depraved actions**, including those committed using the Internet or other information and telecommunication networks[2]. We assume it is intended to include online grooming if it was committed without any non-physical violence (e.g. blackmail, threats etc., otherwise it is qualified as a coercion to acts of a sexual nature).

Article 135 of the Criminal Code is **only applicable to adults over 18 years old** as subjects of liability and to actions committed in relations to minors in the age from 12 to 16 years old (see para. iii below for sanctions in relation to actions committed against minors under 12 years old). Therefore, online grooming committed by other minors is not recognized as a described criminal offence.

---

[1] Resolution of the Plenum of the Supreme Court dated of 04.12.2014 N 16 on case law in relation to against sexual inviolability and sexual freedom of the person ("**Resolution N 16**"), para 15.

[2] Resolution N 16, para 17.

Criminal sanctions:

- In relation to minors under age 16: (i) compulsory labour for up to 440 hours, or (ii) restriction of liberty for up to 3 years, or (iii) compulsory labour for up to 5 years with or without disqualification to hold certain positions or engage in certain activities for up to 3 years, or (iv) imprisonment for up to 3 years with or without disqualification to hold certain positions or engage in certain activities for up to 10 years.
- In relation to minors in the age from 12 to 14 years old: imprisonment for 3 to 8 years with or without deprivation of the right to hold certain positions or engage in certain activities for up to 15 years and with or without restriction of liberty for up to 2 years.
- In relation to 2 or more minors: imprisonment for 5 to 12 years with or without deprivation of the right to hold certain positions or engage in certain activities for up to 20 years.
- In relation to minors committed by a group of persons by prior conspiracy or by an organised group: imprisonment for a term of 7 to 15 years with or without deprivation of the right to hold certain positions or engage in certain activities for up to 20 years and with or without restriction of liberty for up to 2 years.
- In relation to minors committed by a person who has already been convicted for depraved actions: (i) imprisonment for 10 to 15 years with disqualification from holding certain positions or (ii) engaging in certain activities for up to 20 years.

Prescriptive period: from 2 to 10 years (depending on the presence of aggravating circumstances).

iii. Violent actions of a sexual nature in relation to a minor (article 132 (4 (b)) of the Criminal Code)

Conditions for applicability: actions are committed (i) with violence or a threat of violence or (ii) by taking advantage of the victim's helpless state.

Under Russian criminal law, being in the age under 12 is considered as being in helpless state.

Therefore, this article in practice is applicable to online grooming, including via sending sexual messages only or by sending pornographic images, committed in relation to minors under 12 years old.

Criminal sanctions: imprisonment for 12 to 20 years with or without deprivation of the right to hold certain positions or engage in certain activities for up to 20 years and with restriction of liberty for up to 2 years.

Prescriptive period: 10 years.

Case law examples:

As we have already stated, different criminal offences are applicable to online grooming committed in relation to minors under 12 years old and in relation to minors over 12 years old but under 16 years old.

Example 1 (online grooming in relation to a minor under the age of 12 years old): between 15 and 16 December, 2012. a male individual over the age of 18, while at home, via VK social media, had started a communication with a female minor under the age of 12 years old, by repeatedly sending the victim test messages describing sexual relations in a crude and cynical manner, as well as files with photo images of genitals, relating to pornographic materials**.** The individual was convicted for committing other actions of sexual nature under article 132 (4 (b)) of the Criminal Code as well as for distribution of pornographic material to minors via Internet[3].

Example 2 (online grooming in relation to a minor over the age of 12 years old): between 28 February and 29 March, 2013, a male individual used VK social media to engage in sexual

3 Case No. 2-11/14 // Moscow City Court Archive.

correspondence with a minor who is over the age of 12 years old but under the age of 14. Further, the individual sent to the minor a file with a naturalistic image of the genitals relating to pornographic materials. In addition, during this period of time, by means of psychological pressure, the individual induced the minor to take intimate pictures of his/her own body and then send them to the perpetrator. The individual was convicted under article 135 of the Criminal Code.

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 is not defined and there are no specific rules that impose liability for such actions online. Therefore, cyberbullying is not directly punishable under Russian law.

Nevertheless, cyberbullying may result in committing certain criminal offences:

i. Inducement to suicide as a result of cyberbullying (article 110 of Criminal Code)

This article is of general application and does not include cyberbullying as a reason for other person's suicide. Nevertheless, we assume cyberbullying should regarded as a form of such inducement.

Conditions for applicability: (i) a victim committed a suicide or attempted to commit a suicide (ii) as a result of threats, ill-treatment or systematic humiliation of the victim's dignity by the other person.

Therefore, cyberbullying may qualify as a form of such ill-treatment and systematic humiliation of the victim's dignity as the Criminal Code does not specify the particular ways and methods of inducement.

Only individuals in the age over 16 years old may be subject to criminal liability under article 110 of the Criminal Code.

Criminal sanctions:

- General: (i) forced labour for up to 5 years with or without disqualification from holding certain positions or engaging in certain activities for up to 7 years, or (ii) imprisonment from 2 to 6 years with or without disqualification from holding certain positions or engaging in certain activities for up to 7 years.
- **In relation to minor** and/or **committed via Internet**: (i) imprisonment from 8 to 15 years with or without deprivation of the right to hold certain positions or (ii) engage in certain activities for up to 10 years and with or without restriction of liberty for up to 2 years.

Prescriptive period: 10 years in applicable period for inducement to suicide as a result of cyberbullying in relation to minors.

ii. Cyberbullying in the sexual context

We assume that cyberbullying in the sexual context (e.g. harassment, online stalking and etc.) may qualify as the following criminal offences under Russian law depending on the particular form and actions committed:

a) Violent actions of a sexual nature in relation to a minor (article 132 (4 (b)) of the Criminal Code)

As for online grooming, we believe that in relation to minors under the age of 12 cyberbullying which is expressed in some forms of sexual harassment online should be regarded as criminal offence article 132 (4 (b)) of the Criminal Code. We assume there is really a blurred line between online grooming and some forms of sexual cyberbullying. Nevertheless, some actions that are practically constitute sexual cyberbullying are not punishable under the Criminal Code. This does not cover "jokes" of a sexual nature, rating minor users on attractiveness/sexual activity, body shaming, 'outing' someone where their

individual's sexuality or gender identity, offensive or discriminatory sexual language and name calling online and other similar actions.

Please see conditions for applicability, criminal sanctions and prescriptive period above in Q1 (1 (i)).

b) Depraved Actions (article 135 of the Criminal Code)

This may be applicable to some forms of cyberbullying in relation to minors over the age of 12 and under the age 16. For instance, it may include sending someone sexual content (images, emojis, messages), unwelcome sexual advances or requests for sexual favours and etc.

Please see conditions for applicability, criminal sanctions and prescriptive period above in Q1 (1 (ii)).

c) Violation of privacy (article 137 of the Criminal Code)

Cyberbullying in the form of "porn revenge" (sexual images/videos taken consensually but shared without consent) in practice usually qualified as a violation of privacy, however, a claim from a victim or its representative is required to initiate the criminal case. This legal rule is applicable not only to minors as victims, but to adult victims as well.

Conditions of applicability: collection or dissemination of private life information in any form. The important condition that such information should be subjectively attributed by an individual to anonymity, concerning an individual and his or her connections in society, previously not disclosed in public and of both a defamatory and non-defamatory nature.

Criminal sanction:

- General: (i) a fine of up to 200,000 RUB (approx. 3,273 EUR), or in the amount of the wages or other income of the convicted person for a period of up to 18 months, or (ii) by compulsory labour for up to 300,60 hours, or by corrective labour for up to 1 year, or (iii) by compulsory labour for up to 2 years with or without forfeiture of the right to hold certain positions or engage in certain activities for up to 3 years, or (iv) by arrest for up to 4 months, or by imprisonment for up to two years with forfeiture of the right to hold certain positions
- In relation **to minors** under the age of 16 or/and **via the Internet**: (i) a fine up to 300,000 RUB (4, 908 EUR) or in the amount of the wages or other income of the convicted person for a period of from 18 months to 3 years, or (ii) by deprivation of the right to hold certain positions or engage in certain activities for from 3 to 5 years, or (iii) by compulsory labour for up to 5 years with or without deprivation of the right to hold certain positions or engage in certain activities for up to 6 years, or (iv) by detention for up to 6 months, or by deprivation of liberty for a term up to 6 years.

Prescriptive period: 10 years for actions committed in relation to minors via Internet.

The issues of application of article 137 of the Criminal Code in relation to "revenge porn" is illustrated by one of the landmark decisions of the European Court of Human Rights ('**ECtHR**') *Volodina v. Russia*. An applicant tried to break off the relationship with her partner, who had previously beaten her repeatedly, abducted her and threatened to kill her. At the same time, an applicant's VK account was hacked in 2016 and fake pages later appeared. A former suitor listed her real details and posted intimate photos of an applicant for several years. In connection with this, a case for violation of privacy (Article 137 of the Criminal Code) was initiated in 2018, but two years later the police closed the case due to the end of the two-year limitation period.

ECtHR stated that Russian authorities have failed the obligation to conduct an effective investigation when an arguable claim of ill-treatment has been raised not only in relation to cyberbullying, but also to more serious physical harm.

Providing that the positions of ECtHR may be not applicable by Russian courts since Russia's membership was ceased from the Council of Europe in March, 2022, we may predict it will not influence the current enforcement practice. Nevertheless, Russian law enforcement authorities pay more careful attention to crimes committed in relation to minors, especially of sexual nature.

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:

Misinformation and deception online generally is deemed as a way to commit a crime (alongside with violence, threats and blackmail) but not as a criminal offence itself under Russian criminal law. For instance, an adult may incite minor to commit illegal actions by means of misinformation, deception, threats or in other ways and it will constitute a criminal offence under article 150 of the Criminal Code, but the fact of misinformation and deception separately.

However, in certain cases prescribed by the Criminal Code misinformation or deception can be directly qualified as a criminal offence:

i. Slander (article 128.1 of the Criminal Code)

Conditions for applications: dissemination of information which is (i) knowingly false and (ii) of defamatory nature.

Where the false information is not defamatory, liability for slander is excluded. Additionally, a convicted person must be aware that he or she is disseminating false information, i.e. information that does not correspond to reality.

Criminal sanctions:

- General: (i) a fine of up to 500,000 RUB (approx. 8,260 EUR) or in the amount of the wages or other income of the convicted person for a period of up to 6 months, or (ii) compulsory labour for a term of up to 160 hours.
- Publicly committed via the Internet: (i) a fine of up to 1,000,000 RUB (16,518 EUR), or the wages or other income of the convicted person for a period of up to 1 year, or (ii) compulsory labour for up to 240 hours, or compulsory labour for up to two years, or detention for up to two months, or imprisonment for up to two years.

Prescriptive period: 2 years.

ii. Dissemination of misinformation (so-called "fake news")

The Criminal Code additionally provide the following cases when dissemination of "fake news" shall qualify as a criminal offence directly:

- Public dissemination of information on circumstances posing a threat to the life and security of citizens and (or) the measures taken to ensure the safety of the population and territories, methods and means of protection against such circumstances e.g. epidemic, pandemic, natural disaster etc. (article 207.1 of the Criminal Code)
- Public dissemination of information that caused dire consequences (e.g. harm to health or death) (article 207.2 of the Criminal Code)
- Public dissemination of information on Russian military forces and public authorities acting in their powers outside the territory of Russia (article 207.3 of the Criminal Code)

Depending on the particular criminal offence, criminal sanctions may differ from criminal fines and compulsory labour to imprisonment up to 3-5 years. In exceptional cases under article 207.3 of the Criminal Code, the imprisonment term may exceed up to 15 years.

Prescriptive period: from 2 to 10 years (depending on a criminal offence and on the presence of aggravating circumstances).

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?

Article 127.1 of the Criminal Code implies a broad definition of **human trafficking** which includes the purchase or sale of human beings or other transactions involving human beings as an object, or the recruitment, transportation, transfer, harbouring or receipt of human beings for the purpose of their exploitation.

As the Supreme Court stated, recruitment as a part of human trafficking means selection and hiring of persons for the purpose of further exploitation of the person being recruited. For example, a promise of remuneration, blackmail, deception or breach of trust may be used to obtain the consent of the victim[4]. The law does not indicate particular means of recruitment which means it can be committed via online grooming.

Therefore, online grooming activities to find victims before the actual human trafficking is punishable as human trafficking itself (even if actual human trafficking does not take place afterwards).

Conditions for applicability: listed actions should be committed solely for the purpose of further exploitation of a human being.

Criminal sanctions:

- General: (i) compulsory labour for up to 5 years or (ii) imprisonment for to 6 years.
- *Inter alia*, in relation to **minors** and/or group of victims: (i) imprisonment for a term of 3 to 10 years with or without deprivation of the right to hold certain positions or (ii) engage in certain activities for up to 15 years and with restriction of liberty for up to 2 years or without such restriction.

Prescriptive period: 10 years for human trafficking committed in relation to minors.

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.

[4] Resolution of the Supreme Court dated of 24.12.2019 No. 58 on case law in relation to human abduction, illegal deprivation of liberty and human trafficking, para 13.

Answer:

As a general rule, minors may be subject to criminal liability only if they are 16 or older. In exceptional cases minors in the age from 14 to 16 may be criminally liable if they commit criminal offences particularly listed in article 20 of the Criminal Code (e.g. murder, rape, human trafficking, theft, robbery, act of terrorism etc.).

In Russia, there is no specific juvenile justice system.

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:

There are no specific rules in relation to crimes committed by minors in the cyber environment under Russian criminal law. General rules for criminal intent are applicable to investigate whether the crime was committed in cyberspace or not.

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:

As online grooming is not a separate criminal offence under Russian criminal law, we will focus on actions listed herein in Q1. Minors may only be prosecuted if (i) online grooming is committed in relation to minors under 12 years old and (ii) the convicted minor is over 14 years old.

Minors may be prosecuted in practice.

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 see Q7. The same is applicable.

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:

As cyberbullying is not a separate criminal offence under Russian criminal law, we will focus on actions listed herein in Q2. Minors may be liable if they commit violent actions of a sexual nature in relation to a minor which can be regarded as form of cyberbullying (some types of cyberharassment in particular).

Conditions for applicability are (i) violent cyberbullying is committed in relation to minors under 12 years old and (ii) the convicted minor is over 14 years old. Nevertheless, case-by-case assessment is required.

Minors may be prosecuted in practice.

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:

Minors may be subject to criminal liability for wilful misinformation or deception online only if (i) such actions qualify as on of the criminal offences listed herein in Q3 and (i) the convicted minor is over 16 years old.

Please note that some actions described by you (pretending to be someone else, pretending to be an expert, etc) may be a part of other criminal offence under Criminal Code and additional analysis is required on a case-by-case practice.

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:

Yes, minors may be punished for online actions facilitating human trafficking if they are over 14 years old.

Minors may be prosecuted in practice.

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:

Online piracy may be qualified as infringement of copyright or related rights as a criminal offence under article 146 of the Criminal Code. Only minors over the age 16 years old may be subject to criminal liability.

Conditions of applicability: actions are committed on the large scale or on the especially large scale i.e. the value of the copies of the works or phonograms or the value of the rights to use the copyright and related rights objects exceeds 100,000 RUB (approx. 1,652 EUR), and on an especially large scale, 1,000,000 RUB (approx. 16,521 EUR).

Minors may be potentially prosecuted, nevertheless, the cited article is rarely applicable to online privacy as the content subject to piracy usually does not meet the applicability conditions laid down therein. Acts of online piracy for personal use (e.g. downloading content illegally etc.) do not constitute a criminal offence under the Criminal Code.

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:

Hacking usually qualifies as unauthorized access to a computer information under article 272 of the Criminal Code. Minors may subject to criminal liability only if they are in the age over 16 years old.

We believe that cited article will also apply to various scenarios exploiting vulnerabilities in IoT and connected devices if it results in obtaining authorized access to information which is protected by law, including confidential information, personal data, state, banking or tax secrecy etc. Please note that IoT may be regarded as a crucial information infrastructure object in certain cases. If so, individuals who accessed computer information without auhorization are subject to criminal liability under article 274.1 (2) of the Criminal Code which provides higher criminal sanctions.

Criminal sanctions:

- As a general rule, (i) a fine of up to 200,00 RUB (approx. 3,345 EUR), or in the amount of the wages or other income of the convicted person for a period of up to 18 months, or (ii) corrective labour for a term of up to 1 year, or (iii) restriction of liberty for a term of up to 2 years, or (iv) compulsory labour for a term of up to two years, or (v) imprisonment for the same term.
- Criminal sanctions may be higher depending on the particular aggravating circumstances (e.g. major damage, abuse of power etc.).

Prescriptive period: from 2 to 10 years (depending on the presence of aggravating circumstances).

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:

Using Cybercrime as a Service should be qualified as a **complicity** in crimes described in Q13 above. Complicity is regarded as equal to committing a criminal offence under Russian criminal law and is punishable. The general rule that only minors **in the age over 16 years old** may be subject to criminal liability is also applicable herein.

Minors may be prosecuted in practice.

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:

Criminal Code may have extra-territorial scope of application and Russian courts obtain jurisdiction to adjudicate in criminal proceedings in the following cases:

i. **Due to nationality principle:** Russian nationals or stateless individual who are permanently resident in the Russian Federation commit a crime on the territory of the other state if such crime is covered by Criminal Code unless there is already a corresponding court decision of a foreign court.

ii. **Due to principle of mission:** Russian members of the armed forces commit a crime on the territory of the other state unless otherwise is provided by an international treaty.
iii. **Protection of interest principle:** foreign nationals or stateless individual who are not permanently resident in the Russian Federation commit a crime on the territory of the other state if such crime (i) is directed against the interests of the Russian Federation, a Russian national or a stateless person who is permanently resident in the Russian Federation or (ii) in cases provided by international treaties.

Therefore, Russian courts may have jurisdiction in relation to cross-border cybercrimes over Russian nationals in any case, if they have not been prosecuted in a foreign state, and over foreign nationals if they meet criteria laid down above e.g., when committing a cybercrime in relation to a Russian national online. Please note that we are not aware of any international treaties that establish specific jurisdiction of Russian courts in relation to foreign nationals, including the field of cybercrime.

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: .

- **Budapest Convention on Cybercrime**

We draw your attention that Russian Federation is not a member state the Budapest Convention on Cybercrime, the first international framework treaty on cybercrime and electronic evidence developed by the Council of Europe. Due to previous critics of this international document by Russian authorities, current geopolitical situation, and cessation of the Russian Federation's membership in the Council of Europe, we cannot foresee Russia's further signing and ratification of the Budapest Convention on Cybercrime in the upcoming few years.

- **Agreement on cooperation of member state of the Commonwealth of Independent States in combating crimes in the sphere of computer information of 2001**

Russian Federation is a member state of a regional treaty of the Commonwealth of Independent States aimed to combating crimes in the sphere of computer information. It is referred as Agreement on cooperation of member state of the Commonwealth of Independent States in combating crimes in the sphere of computer information of 2001.

It covers the following computer crimes:

i. implementation of illegal access to the computer information protected by the law if this act entailed destruction, blocking, modification or copying of information, violation of operation of the computer, the computer system or their network

ii. creation, use or distribution of malicious applications

iii. abuse of regulations of operation of the computer, the computer system or their network by person having access to the computer, the computer system or their network, the entailed destruction, blocking or modification of information of the computer protected by the law if this act did essential harm or heavy effects

iv. illegal use of the computer programs and databases which are copyright objects, and is equal authorship assignment if this act caused essential damage

Nevertheless, it does not concern such crimes like dissemination of child pornography,

- **Bilateral agreements on combating cybercrime**

Furthermore, there are no specific bilateral treaties that are focused on cybercrime. Nevertheless, general bilateral treaties of the Russian Federation on mutual legal assistance in criminal proceedings are applicable to investigation and prosecution of cybercrimes.

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:

- **Interpol's information systems**

Russian law enforcement authorities may interact with Interpol's crime databases via its network when investigating cybercrimes, especially in cases of international search for persons to combat crime.

Russian law enforcement authorities interact with Interpol via Interpol National Central Bureau of the Ministry of Internal Affairs of the Russian Federation.

- **Forms of cooperation under Agreement on cooperation of member state of the Commonwealth of Independent States in combating crimes in the sphere of computer information of 2001**

In relation to computer crimes covered (please see above), it contains several articles on international cooperation (articles 5-7), which list the forms of cooperation covered by the agreement (namely: exchange of information; provision of legal assistance under international instruments; prevention, detection, suppression and investigation of computer-related crime, etc.), as well as the ways in which Member States may request assistance and guidance to Member States on the execution of requests.

Article 8 of the Agreement sets out the circumstances in which a request for assistance may be refused (namely, where the execution of the request is contrary to the national law of the requested State) and the requirement for a State refusing to execute the request to notify the requesting State in writing of the refusal, indicating the reasons for the refusal.

- **Forms of cooperation provided by bilateral international treaties on mutual legal assistance in criminal proceedings**

In relation to cybercrimes not covered by the Agreement on cooperation of member state of the Commonwealth of Independent States in combating crimes in the sphere of computer information of 2001, different forms of cooperation may be provided by general bilateral international treaties on mutual legal assistance in criminal proceedings concluded with the Russian Federation. They usually include legal assistance in information exchange, gathering evidence, obtaining materials and documents (e.g. from private organizations), enforcing so-called external (foreign) confiscation orders and restricting transactions in property that may be subject to "external" confiscation orders and etc. At the same time, such bilateral treaties can include cases when foreign authorities are not obliged to provide any legal assistance (usually when it is in contrary with domestic law).

Such bilateral treaties are of general application but can be enforced in the course of investigation of cross-border cybercrimes by Russian law enforcement authorities.

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:

There is no specific effect or impact on cybercrime 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:

According to the recent official crime statistics for January-October 2021 provided by the Ministry of Internal Affairs of the Russian Federation[5], almost one in four crimes is committed through the use of IT technology. At the same time, the growth rate of their number has slowed down. While the number of cybercrimes increased by 20.3% in the first half of 2021, in the first ten months of this year it has risen by 8.1%.

The growth rate of recorded crimes committed through the use of information and telecommunication technologies (e.g. via the Internet) has slowed down. In the first 12 months of 2021, their number increased insignificantly by 1.4%.

Report states positive results have been achieved grace to the activity of specialised units for detecting and investigating high-tech crime. They have been set up in the operational and investigative services of the Ministry of Internal Affairs and its territorial bodies, their staff receive special training and the necessary equipment, which makes it possible to step up efforts in the fight against IT crime.

However, the recent report does not specifically include any data on online grooming, cyberbullying, misinformation and deception human trafficking.

As for crimes committed by minors or with the complicity of minors, a study of socio-criminological data shows a 15.6 per cent drop in the overall number.

Question 20: Do you have any other comments to make that may be relevant to your jurisdiction?

Answer:

N/A.

[5] Available in full in Russian only here.