Universität Augsburg - Juristische Fakultät – LS Prof. Dr. Kaspar - 86135 Augsburg

Prof. Dr. Johannes Kaspar
Lehrstuhl für Strafrecht, Strafprozessrecht, Kriminologie und Sanktionenrecht

Juristische Fakultät
Universitätsstraße 24
86159 Augsburg
Zimmer 2030

Tel +49 (0) 821 598 - 4555
Tel +49 (0) 821 598 - 4556 (Sek.)
Fax +49 (0) 821 598 - 4557

johannes.kaspar@jura.uni-augsburg.de
www.jura.uni-augsburg.de/kaspar

Augsburg, den 23.06.2022

Questionnaire Project RAYUELA -
Empowering and educating young people for the Internet by playing

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

Yes, online grooming is a criminal offence according to § 176b section 1 StGB (German Penal Code).

Since a recent legal reform from 2021, the offence is now officially called „preparation of sexual abuse of children“ and is regulated in a separate provision. Before, online grooming had been regulated in § 176 section 4 no. 3 StGB as part of a more general provision concerning different types of sexual abuse and its preparation.

§ 176b StGB requires that the offender acts on a child (i.e. a person under 14 years of age) by making use of a content according to § 11 section 3 StGB in order to prepare a type of sexual abuse, either by making the child carry out a sexual act on or in front of the offender or a third person or to allow the offender or a third person to carry out a sexual act on the child. It is also punishable if the offender acts accordingly to produce or acquire child pornography in the sense of § 184b section 1 no. 3 or 184b section 3 StGB. If the content that is used by the offender when acting on the child is pornographic, the offender can be punished for „sexual abuse of children without physical contact with the child” (§ 176a section 1 no. 3 StGB), with a more severe threat of punishment from six months to ten years of imprisonment).

According to the legal definition in § 11 section 3 StGB, a „content“ is any content of documents, sound or picture carriers, data carriers (like e.g. USB-Sticks), pictures or other embodiments, independent of any storage via information or communication technology. That means that the offender is only punishable if he approaches the child by means of one of the before mentioned devices or ways of communication (including online communication as the most important example in practice), but not by talking to the child in person (with the intent of preparing a later act of sexual abuse). This unequal treatment of similar acts has been a point of criticism (cf. Fischer, StGB, § 176b mn. 3).

The sexual acts mentioned in § 176b section 1 StGB have not to be carried out in reality to constitute criminal liability - if they are, other offences with higher punishments like sexual abuse of children according to § 176 StGB will be applied primarily. For § 176b StGB, it suffices if the offender acts with the intent of influencing the child in that direction. Therefore, § 176b StGB is categorized (and sometimes criticized, cf. Fischer, StGB, § 176b mn. 6; Stoiber, Cybergrooming aus empirischer und kriminologischer Sicht, 2018, 214 et seq.) as a preparatory offence that is very remote from the actual harm inflicted upon the victim.

§ 176b section 3 StGB regulates that the attempt of online grooming is punishable in cases where the completion of the offence is not possible due to the fact that the offender only thinks that he is communicating with a child, but is in fact communicating with an adult (e.g. a police officer searching for potential offenders of online grooming and sexual abuse in the internet, making use of a false identity). This regulation was introduced in 2020 to facilitate police investigations and to close an alleged „gap of protection“ (see Bundesministerium des Inneren / Bundesministerium der Justiz, 3. Periodischer Sicherheitsbericht, 2021, S.120; objections against the reform are raised (e.g.) by Baumhöfener MMR 2021, 30 who denies an action worthy of punishment and holds that the ultima ratio principle is violated; see also van Endern, NJW 2020, 1033 who holds that punishing the mere attempt of a preparatory act would not be in line with general standards of the criminal law system).

The possible punishment for „preparation of sexual abuse of children“ ranges from three months of imprisonment to a maximum of five years of imprisonment. A fine (as an alternative to imprisonment) is not explicitly mentioned in the provision, but in less severe cases, a prison sentence of less that six months can be transformed into a fine (see § 47 section 2 StGB). As § 176b StGB does not constitute a felony („Verbrechen“), but a misdemeanor („Vergehen“), minor cases can also be dealt with by a termination of proceedings by the public attorneys office (instead of an indictment), either without any further consequences for the offender (§ 153 of the German Code of Criminal Procedure, StPO) or after the offender has fulfilled some obligation like compensating the victim or doing community work (§ 153a StPO). These regulations are an exception to the general obligation to prosecute and indict criminal behaviour (so-called principle of legality).

Furthermore, according to the general sentencing regulations, prison sentences of up to two years can be suspended on probation (see § 56 StGB). In the judicial practice, offenders of grooming are sentenced to prison sentences quite often (at least compared to other offences with a similar range of punishment, see Stoiber, Cyber-Grooming aus empirischer und strafrechtlicher Sicht, 2018). According to the Federal Criminal Justice Statistic of 2020 (more recent figures have not yet been published), 392 adult offenders were sentenced for sexual abuse of children without physical contact (§ 176 section 4

StGB) in that year, which inter alia contains cases of online grooming. 260 of them (66,3 %) received a prison sentence, 132 (33, 7 %) a fine.

In cross-border cases, German criminal law is generally applicable in different situations, e.g. if the victim and/or the offender are German nationals and if the act is a criminal offence at the place of its commission or if that place is not subject to any criminal law jurisdiction (§ 7 section 1 and § 7 section 2 no. 1 StGB, so-called active and passive personality principle). In cases of sexual offences, including § 176b StGB, German law is applicable if the offender is a German national, without regard to the legal situation in the place where the crime was committed (§ 5 no. 8 StGB) – with this regulation the legislator stresses that the German state has an urgent interest in law enforcement in these cases which per se constitutes a special „domestic connection".

According to the principle of territoriality, German criminal law is also applicable if the offence has been committed on German territory (§ 3 StGB). In cases of cross-border online grooming, it can be difficult to determine the actual place of the „commission" of the offence. If the offender acted on German territory when starting the online communication, German criminal law is applicable according to § 3 StGB. Problems arise, however, when the offender sent his message from abroad and only the victim was located in Germany when he or she received it. According to § 9 StGB, an offence is committed where the offender acted or where the „result" of the offence occurs. As § 176b StGB does not require a certain „result" (Taterfolg), but punishes a dangerous act as such, it is doubtful, if in the before mentioned example the offence was actually committed (also) on German territory.

One of the problems of application is the question what acting on a child („auf ein Kind einwirken") actually means (see Stoiber, Cyber-Grooming aus strafrechtlicher und kriminologischer Sicht, 2018, 157 et seq.).

In a case that was decided in 2015 by the German Federal High Court (BGH, Beschl. v. 22.01.2015, NStZ-RR 2015, 139), the offender sent a pornographic picture via WhatsApp to a girl that was 11 years old. On the same day, in other messages, he told her that he wanted to make her have an orgasm. The court stated that sending the picture alone did not fall under § 176 section 4 no. 3 or no. 4 StGB old version, because acting on the victim would require some kind of a deeper psychological influence on the victim; the mere display of pornography would not suffice for that. Sending the picture in combination with the following messages, however, was considered to be sufficient.

In 2016, the Higher Regional Court of Hamm had to decide on a case, where the offender was repeatedly chatting with a 9 year old girl via WhatsApp. He asked her several questions about her boyfriend, if she was happy with him, how she had spent the night with her boyfriend and if she could also find a girlfriend for himself. He suggested to „do something" together as two couples.
Later messages were not received by the victim anymore, but by her mother who had taken over the mobile phone of her daughter and who continued the conversation in her daughter´s name. In the following, the offender sent more explicit messages with sexual content. The court stated that the offender had sufficiently „acted" on the child according to § 176 section 4 no. 3 old version (OLG Hamm, Beschl. v. 14.1.2016, MMR 2016, 425). To act on the victim would include all forms of intellectual influence with a certain persistence, e.g. repeated urging, convincing, making promises, raising of curiosity, making use of authority, deception, intimidation or threatening. The court held that a relevant urging or convincing had not taken place here as the messages to the actual victim did not have a sufficient sexual content (and the later messages were not received by the victim). The early

messages, however, served the purpose of raising curiosity as the offender suggested a sexual experience the victim had not had before – this was sufficient for a relevant „acting“ on the victim. The court also stated that according to its wording, the offence was not excluded if offender and victim knew eachother, even though the legislator had the intention of sanctioning offences veiled by the anonymity of the internet.
The fact that the later messages were only received by the mother of the victim excluded criminal liability as at the time of the offence, § 176b section 3 StGB with its special regulation of a punishable attempt in cases where the offenders only thinks he is communicating with a child, did not exist.

If the communicative actions of the offender have to contain at least some sexual references to fulfill § 176b StGB is discussed controversially. The wording of the regulation does not mention such a prerequisite, which is why according to the leading opinion among scholars and practitioners, such a reference is not necessary. In practice, however, most cases of (potential) online grooming will probably only be prosecuted if at least some sexual element is recognizable (Baumhöfener MMR 2021, 30, 31).

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)?

There is no explicit offence of „cyberbullying“ or „bullying“ in German criminal law. However, bullying or harassing behaviour can fall under the scope of various criminal offences of the Penal Code.

First of all, the legislator introduced criminal liability for stalking (including online stalking) in 2007. § 238 StGB requires that the offender stalks another person in a manner which is suitable for seriously restricting that person’s lifestyle by repeatedly
1. seeking the other person’s physical proximity, or
2. trying to establish contact with the other person by means of telecommunications or other means of communication or through third parties, or
3. improperly using the other person’s personal data for the purpose of ordering goods or services for that person or inducing third parties to make contact with that person or
4. threatening the other person, one of his or her relatives, or someone close to him or her with causing injury to life or physical integrity, health or liberty, or
5. committing criminal acts according to §§ 202a, 202 b or § 202c (data espionage, data theft or preparatory acts) against the victim, one of his or her relatives or someone close to him or her, or
6. spreading or making accessible for the public a picture of the victim, of one of his or her relatives or someone close to him or her, or
7. spreading or making accessible for the public a content (§ 11 section 3 StGB) that is apt to degrade that person or to negatively affect public opinion about that person, pretending that the person is the author of this content, or
8. committing other comparable acts.

Even though there is no specific provision for „online stalking“, most of the before mentioned alternatives (except for the seeking of physical proximity as such) can be fulfilled by making use of means of online communication. In practice, these forms of stalking (e.g. by contacting or threatening the victim by E-Mail oder Messenger Services) play an important role. The fact that just recently, in October 2021, the legislator introduced new criminal actions in no. 5 through 7, which are all strongly related to the digital sphere, emphasizes the relevance of online stalking within § 238 StGB.

The punishment for stalking ranges from a fine to a maximum prison sentence of three years. In severe cases according to § 238 section 2 StGB the punishment is a prison sentence between three months and five years. For the purpose of this report, it is interesting that one of the reasons for assuming a „severe" case (which was also introduced in 2021) is the fact that the offender is older than 21 years and the victim younger than 16 years (§ 238 section 2 no. 7 StGB).
If the offender causes the death of the victim by his stalking activities at least negligently, the punishment ranges from one to ten years of imprisonment (§ 238 section 3 StGB).

A case of cyberstalking was decided upon by the Regional Court of Essen in 2014 (LG Essen, Urt. v. 20.3.2014, BeckRS 2014, 21640). The offender started stalking his former employer and landlord after the latter had terminated tenancy and the working contract. Inter alia, the offender regularly wrote degrading and threatening posts on a website. The court found the offender guilty of insult (§ 185 StGB), threat (§ 241StG) and stalking (§ 238 StGB) at the same time and imposed a prison sentence of 1 year and 6 months (which was not suspended on probation due to a negative prognosis of future crime).

Another offence that might become relevant is § 241 StGB: whoever threatens another person with the commission of a serious offence will be punished with a fine or imprisonment of up to two years (depending from the seriousness of the threatened offence). If the offence is committed publicly, in an assembly or by spreading a content (§ 11 section 3 StGB), punishment ranges from a fine to a maximum of three years of imprisonment; the latter will be relevant for threats that are made by means of online communication.

Verbal harassment can be a punishable insult according to § 185 StGB with a range of punishment from a fine up to a maximum prison sentence of one year. Like in § 241 StGB, the legislator recently introduced (as part of a general policy of tackling online hate crime) the possibility of a more severe punishment (up to two years of imprisonment) if the insult was committed publicly, in an assembly or by spreading a content (§ 11 section 3 StGB).

One of the most difficult problems in the application of § 185 StGB (insult) is the balancing of personal honour and personality rights on the one hand and freedom of speech on the other hand. A famous case in this regard was recently decided upon by the German constitutional court (BVerfG, Beschluss vom 19.12.2021, NJW 2022, 680). Someone wrote on an internetblog that politician Renate Künast from the Green Party had allegedly stated in the past that having sex with children was „ok", as long as no violence was involved (which was not true). This false statement was repeated on Facebook. Many users reacted to this post and made insulting comments, where Mrs. Künast was called insane and „pedophile dirt". The Regional Court of Berlin had denied criminal liability for insult (§ 185 StGB) with regard to freedom of speech, which was overruled by the Constitutional Court that stressed the importance of personality rights of the victim.

Sexual harrassment below the threshold of sexual abuse or rape (where violence or threats are used) has become a separate criminal offence in 2016 (see § 184i StGB). The provision, however, does not include cyber harassment, as one of its prerequisites is that the victim is touched physically in a sexually determined manner. Cyer harassment with sexual content can fall under the scope of the before mentioned provisions § 185 StGB (insult) and 238 StGB (stalking). It can also fulfill the prerequisites of § 176a StGB (sexual abuse of children without physical contact with the child), if the offender acts

upon a child by making use of a pornographic „content“ (§ 11 section 3 StGB), e.g. by sending pornographic pictures to a minor by e-mail or a messenger service.

In cross-boarder cases, German criminal law is applicable under the conditions already mentioned above. In cases of sexual abuse (§ 176a StGB), the active personality principle is modified with the result that German jurisdiction is given if the offender is a German national, even if the offence was not punishable under the law of the place of its commission (§ 5 no. 8 StGB).

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?

There is no specific criminal offence that relates to „fake news“, i.e. misinformation and deceipt, no matter if it happens online or offline. However, misinformation and deception can constitute a criminal offence, if certain special individual interests or legal goods (Rechtsgüter) are harmed.

First of all, the spreading of false facts that are apt to degrade that person or to negatively affect public opinion about that person can be a punishable „malicious gossip“ (§ 186 StGB) or – if the offender intently or knowingly spreads false facts – a defamation (§ 187 StGB). The range of punishment reaches from a fine to a prison sentence of up to one year (§ 186 StGB) or two years respectively (§ 187 StGB). Again, the maximum punishment is extended by one year if the offence is committed publicly, in an assembly or by spreading a content (§ 11 section 3 StGB).

Apart from that, (intentionally) deceiving another person and damaging his or her financial interests in order to gain monetary advantages for oneself or a third person can constitute the criminal offence of fraud (§ 263 StGB). The fact that the deception has been committed by making use of means of online communication has no legal relevance. In practice, online fraud has become increasingly relevant. One example is offenders ordering products online without being able nor willing to pay for these products. If the deceptive behaviour is not adressed at a human being, but is rather used in an interaction with a computer system, the offence of computer fraud (§ 263a StGB) becomes relevant.

German jurisdiction in cross-boarder cases follows the general rules described above.

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?

Human trafficking (Menschenhandel) is regulated in § 232 StGB. The complex regulation reads as follows: „Whoever recruits, transports, transfers, harbours or receives another person by taking advantage of that person’s personal or financial predicament or helplessness on account of being in a foreign country, or that person is under 21 years of age, incurs a penalty of imprisonment for a term of between six months and five years if

1. that person is to be exploited by way of

a) engaging in prostitution or performing sexual acts on or in the presence of the offender or a third person, or having sexual acts performed on them by the offender or a third person,

b) employment,

c) begging or

d) committing criminal offences,

2. that person is to be held in slavery, bonded labour, debt bondage or under corresponding or similar conditions or

3. an organ is to be illegally removed from that person.

Exploitation through employment within the meaning of sentence 1 no. 1 (b) occurs if the employment, in serving the ruthless pursuit of profit, takes place under working conditions which are strikingly different to those of others performing the same or a similar activity (exploitative employment).

(2) Whoever, with respect to another person who is to be exploited in the manner referred to in subsection (1) sentence 1 nos. 1 to 3,

1. recruits, transports, transfers, harbours or receives that person by force, by threat of serious harm or by deception or

2. abducts that person or gains physical control over him or her or encourages a third person to gain physical control over him or her

incurs a penalty of imprisonment for a term of between six months and 10 years.

(3) In the cases under subsection (1), the penalty is imprisonment for a term of between six months and 10 years if

1. the victim is under 18 years of age at the time of the commission of the offence,

2. the offender seriously physically ill-treats the victim or, by committing the offence or an act committed during the offence, at least recklessly places the victim in danger of death or at risk of serious damage to health or

3. the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences.

In the cases under subsection (2), the penalty is imprisonment for a term of between one year and 10 years if the offence was committed under one of the circumstances indicated in sentence 1 nos. 1 to 3“.

The regulation contains no specific provisions concerning the use of online communication. The criminal action of „recruiting“ victims is punished without regard to the way the recruitment has taken place. Online grooming activities before the actual human trafficking takes place do not constitute a separate criminal offence. However, trying to recruit victims (online or offline) can constitute a punishable attempt of human trafficking according to § 232 section 4 StGB.

In cases of human trafficking, where cross-boarder constellations are very common, German jurisdiction is independent from a domestic connection like the nationality of offender or victim or the place of commission: According to § 6 no. 4 StGB, German criminal law is always applicable, as the offence is considered to violate a universal, internationally protected legal interest. The importance of law enforcement in this area is emphasized by this regulation.

A case of human trafficking with an important role of cyber-communication was decided upon by the German High Court in 2018 (BGH, Urt. v. 12.4.2018, NStZ-RR 2018, 375). The offender contacted many women by internet and checked their willingness to work as a prostitute. He intensified his „relation" with some of them, urged them to work as prostitutes and made false promises with regard to a future together, thereby making the women pay considerable sums of money (which he used for himself). The Court confirmed criminal liability for human trafficking in a severe case according to § 232 section 1 s. 2 StGB, section 3 no.3 StGB.

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.

In Germany, crime committed by juvenile offenders (youths between 14 and under 18 years) is dealt with within a separate juvenile justice system, with the JGG (Jugendgerichtsgesetz – Juvenile Court Act) being the central provision. The most important elements of the JGG are special rules for criminal responsibility (§ 3 JGG), criminal sanctions (§§ 4 – 30 JGG), juvenile courts (§§ 33-42) criminal proceedings (§§ 43 – 81 JGG) and the execution of sanctions against juvenile offenders (§§ 82 – 93a JGG). What doesn´t exist in the German system are special provisions for "youth offences" - all offences codified in the general Penal Code are also applicable regarding juvenile offenders without exceptions or modifications.
Children under the age of 14 are generally exempt from criminal liability (§§ 19 StGB, 1 Abs. 2 JGG).

Juvenile offenders between 14 and (under) 18 years are – as a rule – supposed to be criminally liable. However, in each individual case, the youth court must decide if at the time of the act, the offender showed a level of moral and intellectual maturity sufficient to enable him to understand the wrongfulness of the act and to conduct himself in accordance with such understanding (§ 3 JGG). In practice, however, this criterion is not checked very strictly – the exemption from criminal liability due to immaturity is a rare exception.

Young adults between 18 and (under) 21 years ("Heranwachsende") are a special group that falls under the scope of juvenile criminal law if the overall assessment of the offender´s personality, taking account of his living environment, demonstrates that at the time of the act he was still equivalent to a juvenile in terms of his moral and intellectual development, or if the type, circumstances and motives of the act indicate that it constituted youth misconduct ("Jugendverfehlung"), § 105 JGG.

The most striking feature of the German juvenile justice system and its most remarkable difference to general criminal law for adult offenders is a much broader, more flexible and – as a rule – less severe set of sanctions that can be imposed on the juvenile offender, with the principle of education ("Erziehungsgrundsatz") being the central objective of juvenile criminal law (see § 2 section 1 JGG).

There are three major categories of sanctions: 1. educational measures, e.g. the instruction to attend certain courses like a social skills training course or supervisory assistance (§§ 9-12 JGG); 2. disciplinary measures, e.g. the imposition of conditions or youth detention of up to 4 weeks (§§ 13-16a JGG) and, as a last resort, 3. youth penalty (§ 17 JGG). Only the latter sanction, which is executed in special youth prisons, is considered to be a real penalty in terms of criminal law.

An important part of this "special" character of the sanction system for juvenile offenders is the fact that there is no specific range of punishment for each offence. The judge can choose quite freely and individually from the set of sanctions described above, always with regard to an educative impact on the offender´s future life. There only exists a general provision limiting youth penalty to a duration of 6 months up to 5 years; in severe cases (like homicide or murder), the range is expanded to a maximum duration of 10 years (§ 18 JGG).

There is no explicit regulation listing certain mitigating / attenuating circumstances; the only sentencing rule concerning youth penalty is § 18 section 2 JGG, which states that youth penalty should be calculated in a way that promotes the intended educative effect. Nonetheless, following general sentencing rules and standards for adult offenders that also apply here, especially the principle of guilt ("Schuldprinzip") it is evident that circumstances like a confession or efforts towards victim-offender-mediation and other forms of Restorative Justice will lead to a more lenient sanction also for juvenile offenders.

The general rules for establishing German jurisdiction that were described above (especially §§ 3 and 7 StGB) are also applicable for juvenile offenders; there are no special provisions in this regard.

Generally, youth courts try to avoid youth penalty, especially when it comes to offenders with no (or no dramatic) criminal record. Many proceedings are terminated by the public attorney´s office according to § 45 JGG, e.g. if certain (non-punitive) educational measures have already been undertaken. This tendency of diversion is not only a way of dealing with a lot of cases in a fast and efficient manner but is also driven by the idea of avoiding harmful and counterproductive stigmatization of juvenile offenders. Studies show that this very lenient way of dealing with criminal offences without any formal sanction does not lead to higher recidivism rates compared with cases which lead to a formal sanction. In cases where such an early closing is not possible, youth courts will tend to impose non-custodial sanctions like the very popular instruction (§ 10 JGG) or condition (§ 15 JGG) to do community work. Youth penalty with its potentially stigmatizing and damaging consequences for the convict´s future life is restricted to cases of severe crimes and/or juvenile offenders with a considerable criminal record, where the court finds "harmful inclinations" (§ 17 section 2 JGG).

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?

As mentioned above, in principle there are no modifications concerning the scope of criminal offences regarding juvenile offenders. They are criminally liable in the same way as is the case for adult

offenders, which also relates to the question of criminal intent. It might be that police, public attorney and courts are a bit more "generous" in assessing the necessary intent/awareness of juvenile offenders. It might also be that in cases where the wrongfulness of the act is not evident for the juvenile offender, courts might tend acquit the offenders due to a mistake law ("Verbotsirrtum", § 17 StGB) that excludes guilt if the mistake was unavoidable (which is only very rarely assumed by courts). Both assumptions are, however, speculative as, to the best of my knowledge, neither empirical studies about the German situation nor an official and explicit policy of leniency for juvenile offenders regarding cybercrime do exist.

The age of the offender is only very rarely mentioned as a relevant factor within the wording of criminal offences, which also relates to cybercrime. One interesting exception has already been mentioned above: If the offender is under the age of 21 years, a severe case of stalking according to § 238 no. 7 StGB cannot be assumed, even if the victim is under the age of 16 years. Please note that the regulation merely excludes the assumption of aggravated stalking, but does not constitute a special mitigating factor for constellations where minor and offender are youths.

Another example (outside the scope of cybercrime) is sexual abuse of children (§ 176 StGB): Even though the offender has performed a sexual act on a victim of less than 14 years of age (or has had the victim perform a sexual act on himself), the court can refrain from any punishment if the sexual act was based on a mutual agreement and the difference between offender and victim both concerning age and maturity is only a slight one (as long as the offender does not take advantage of the victim´s missing ability to exercise sexual self-determination), § 176 section 3 StGB. An example would be a 14 year old boy petting or even just intensely kissing his 13year old girlfriend. This regulation was just recently introduced in 2021. In these cases, the legislator acknowledges the problem of constellations with young offenders and victims at the same time that might not be as worthy of punishment as constellations with adults on the one side and young victims on the other. In this context, he explicitly relates to the German constitution which forbids a disproportionate punishment. However, there is no comparable differentiating regulation regarding the other before mentioned offences where similar problems exist, especially with regard to online grooming (§ 176b StGB). A possible reason for this unequal treatment is that contrary to § 176b StGB, § 176 StGB in its new form (since 2021) has become a felony (Verbrechen, § 12 I StGB) that is always punished with at least one year of prison – which automatically excludes the possibility of closing the proceedings in less severe cases according to §§ 153 et seq. StPO or § 45 JGG.

As will be shown in more detail later (see question 19), minors are in fact prosecuted for cybercrime (at least in a broad sense), but it strongly depends on the offence in question. The share of youth offenders is comparably high regarding spreading child pornography via the internet, whereas there are only few cases of online grooming or stalking and almost no cases at all of human trafficking committed by minor offenders. For cybercrime in a narrow sense (i.e. offences aiming directly at the internet and systems of online communication), minor offenders are only rarely prosecuted and punished.

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?

Yes, minors can be punished for online grooming under German law. As mentioned above, there is no explicit legal restriction of the scope of criminal liability for this offence when the offender is a juvenile between 14 and (under) 18 years. A legal possibility to deny criminal liability at least in theory would be to declare the sexual act intended by the offender as not being "grave" ("erheblich") enough (e.g. if the offender is 14 years old and approaches the victim which is 13 years old with the intention of preparing a future sexual act that is supposed to be mutually agreed upon). In this case, the act might not fall under the scope of criminal law (see the legal definition § 184h no 1 StGB). There is no published case law, however, so it is not clear if courts actually choose this way in practice.

An explicit possibility to refrain from punishment in cases where there is no big difference in age and maturity between victim and offender performing a sexual act (see § 176 section 3 StGB) does not exist regarding online grooming (§ 176b StGB). At least at first sight this is a strange and inconsistent result (see e.g. Lederer StV 2021, 322, 326; see also https://netzpolitik.org/2022/strafrecht-die-meisten-tatverdaechtigen-bei-kinderpornografie-sind-minderjaehrig/): The mere preparation of a sexual act by online grooming would be punishable even if in the concrete case the act itself might not be considered worthy of punishment. Therefore, the possibility of refraining from punishment should be applied to cases of online grooming as well by means of analogy, even though there does not seem to be published case law in this regard. As mentioned above, a possible reason for the unequal shape of the two provisions is that § 176b StGB allows for a solution via diversion: many of these constellations are obviously dealt with by generously making use of the possibility of terminating the procedure (§ 45 JGG) or a lenient way of sanctioning according to juvenile criminal law (see supra).

One possibility in this regard (that would be applicable for other juvenile offences as well) is the instruction (§ 10 JGG) of not using a smartphone or the internet in general for a certain period of time which is proposed by some scholars and courts for adult offenders (see e.g. Nicolai NStZ 2021, 136 et seq.; OLG Hamm NJW 2016, 582). However, there is no sufficient data available concerning the different ways these cases are dealt with.

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?

Again, there are no special regulations for juvenile offenders, so minors can be held criminally liable for such a behaviour just like adults (bearing in mind that on the sanction side, as mentioned above, there will be huge differences between both groups). Even purely online behaviour with a sexual intent can fall under one of the following provisions, if the offender is at least 14 years old:

- § 176a section 1 no. 3 StGB: sexual abuse of children without physical contact as described above (e.g. if the offender acts upon a minor victim by making use of pornographic content).

- § 176b StGB: online grooming as described above (e.g. if the offender acts upon the minor victim by using (any) content with a sexual intention (including the intention of committing an offence of child pornography).

- § 177 section 2 StGB: Sexual coercion (e.g. if the offender threatens to make explicit pictures of the victim public in order to force the victim to perform sexual acts – even the latter does not happen, the mere (online) threat would constitute a punishable attempt of sexual coercion, § 177 section 3 StGB).

- § 184 StGB: Spreading of pornographic material (e.g. if the offender sends pornographic material to a victim under 18 years).

- § 184b StGB: Child pornography (e.g. if the offender distributes nude pictures of a person under 14 years).

- § 184c StGB: youth pornography (e.g. if the offender distributes nude pictures of a person between 14 and 18 years – this might even be the case if a 17 year old sends pornographic material showing exclusively himself to other persons).

In a case decided by the German High Court in 2019, a juvenile offender had secretly produced self-deleting Snapchat-Videos and had recorded videocalls of his juvenile communication partner performing sexual acts without the victim´s consent. The Court found the offender guilty of producing youth pornography according to § 184c section 1 no. 3 StGB (BGH, Beschluss vom 5. September 2019 – 4 StR 377/19). The privilege in section 4 (where criminal liability is excluded when youth pornography is produced for own use with the victim´s consent) was not applicable as the victim did not know about the recording.

- § 201a section 2 StGB: violation of personality rights by taking photos or other images (e.g. if the offender gains possession of pictures showing nudity of a person under 18 years and sells it to a third party).

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?

Yes, the before mentioned criminal offences covering different forms of cyberbullying (§§ 176a, 185, 238, 241 StGB) are fully applicable regarding juvenile offenders. There are no restrictions of the scope of criminal liability (whereas on the sanction side, of course, the special system of juvenile criminal law sanctions is applicable).

This shows in a case decided by the District Court of Munich in 2014: The juvenile offender had insulted and threatened his (minor) victims via Facebook and Whatsapp and had even urged one of them to produce a video while masturbating which he posted on Facebook afterwards (AG München, Urteil vom 24.03.2014 – Az. 1013 LS). The court made use of the full spectrum of juvenile criminal law sanctions. It not only imposed a youth prison sentence of two years (which was suspended on probation), but also a youth detention of 4 weeks and the obligation to start a sexual therapy, to pay a compensation for pain and suffering of 1500 Euro to two of his victims and – especially interesting –

to delete his accounts on Facebook, WhatsApp and Instagram and to refrain from using these services for six months.

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?

Yes, also juvenile offenders can be punished for wilful misinformation or deception in the before mentioned cases of violating a person´s reputation (insult, malicious gossip or defamation, §§ 185 – 187 StGB) or financial interests (fraud, § 263 StGB). There are no restrictions in the scope of these offences for juvenile offenders.

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?

Yes, juvenile offenders can be punished for human trafficking according to § 232 StGB (including the attempt to recruit persons online); again, there are no restrictions for these offenders concerning the scope of § 232 StGB. In practice, human trafficking committed by juvenile offenders is a very rare exception (see infra).

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?

The illegal use and distribution of content protected by intellectual property rights is regulated not within the German Penal Code (StGB), but in a special intellectual property rights act (Urhebergesetz, UrhG) that contains regulations of certain criminal offences (§§ 106 et seq. UrhG). According to the central regulation in § 106 UrhG, a person will be punished with a fine or a prison sentence of up to 3 years if he or she duplicates, distributes or publicly displays a protected work without the consent of the owner of the affected intellectual property right. Again, this offence is fully applicable to juvenile offenders of at least 14 years. In the past, law enforcement in this regard against juvenile offenders became very relevant regarding illegal filesharing (music, videos…) on platforms like napster. The offences can only be prosecuted if the victim files a request (“Strafantrag”), unless the public attorney confirms a public interest in law enforcement (§ 109 UrhG). A problem of application is the scope of § 53 UrhG which allows duplicating protected content for “private use” (which is not applicable if the content is shared at the same time like it was the case with the before mentioned filesharing platforms). Some youths were probably surprised that this constituted criminal liability, but as mentioned before, a mistake of law is handled very strictly under German law and only excludes liability in exceptional cases (§ 17 StGB).

Universität Augsburg University

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?

Minors can be punished for "hacking" especially in cases, where they obtain access to data, which were not intended for them and were specially protected against unauthorised access by circumventing the access protection (§ 202a StGB, data espionage). "Data" in this sense are those which are stored or transmitted electronically, magnetically or otherwise in a manner which is not immediately perceptible (§ 202a section 2 StGB). This can also apply to exploiting vulnerabilities in IoT and connected devices, as long as there was some kind of relevant access protection the offender circumvented.

For adult offenders, the range of punishment is a fine or up to three years of prison. Juvenile offenders can be punished with the full range of special sanctions mentioned above; in practice, courts will impose a non-custodial sanction in almost all cases due to the less severe character of the offence.

Another relevant provision is § 202b StGB (phishing); offenders are criminally liable if they intercept data which are not intended for them, either for themselves or another party, by technical means from non-public data transmission or from an electromagnetic broadcast from a data processing facility. The offence is punished with a fine or prison of up to two years (for adult offenders), unless the offence is subject to a more severe penalty under other provision. Juvenile offenders will be sanctioned according to juvenile criminal law.

In addition to these two provisions, also preparatory acts to data espionage or phishing can be punished according to § 202c StGB, e.g. the producing, acquiring, selling, supplying to another, disseminating or making available in another way of passwords or other security codes which provide access to data or computer programs for the purpose of a commission of the before mentioned offences. Adult offenders can be punished with a fine or prison up to two years. Juvenile offenders are sanctioned according to juvenile criminal law.

In addition to that, since 2015, (adult) offenders are punished with a fine or prison of up to two years if they procure, for themselves or another person, supply to another person, disseminate or otherwise provide access to data which are not generally accessible and which another person has obtained by an unlawful act for the purpose of personal enrichment or the enrichment of a third party or to harm another person (§ 202d StGB, handling of stolen data). The legislator introduced this provision as the classical handling of stolen goods (Hehlerei, § 259 StGB) was only applicable to tangible objects, but not to data.

If the (adult) "hacker" unlawfully deletes, suppresses, renders unusable or alters data, he can be punished with a fine or a prison sentence of up to two years (§ 303a StGB, data manipulation).

Another possibly relevant criminal offence is computer sabotage according to § 303b StGB. If the (adult) offender interferes with data processing operations which are of substantial importance to another by committing an offence under § 303a section 1, by entering or transmitting data with the intention of adversely affecting another or by destroying, damaging, rendering unusable, removing or

altering a data processing system or a data carrier will be punished with a fine or with a prison sentence up to three years.

Criminal liability for all of these data offences mentioned before requires intentional behaviour; mere neglicence is not sufficient. And again, all of these offences are applicable for juvenile offenders in the same way as for adult offenders; the only difference is that sanctions of juvenile criminal law are imposed.

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?

Like adults, minors can be punished for acts of using Cybercrime as a service. There are various possible scenarios with different relevant criminal offences.

An important example has been mentioned above: If the offender (e.g.) buys certain passwords or security codes on a darknet platform in order to commit data espionage (§ 202a StGB) or phishing (§ 202b StGB), this preparatory act itself is punishable according to § 202c StGB.

If the offender "orders" the commission of a certain cybercrime (like e.g. data espionage or phishing) by other persons online, criminal liability depends on the question if this crime is actually committed. If this is the case, the offender would be liable for this offence in terms of incitement (§ 26 StGB), with the same range of punishment a perpetrator would have to face. If the cybercrime is not committed for whatever reason, the offender is only criminally liable for attempted incitement to this offence if the latter is a felony (Verbrechen) according to § 12 StGB, i.e. a severe crime like robbery or homicide with a minimum statutory punishment of at least one year of prison. Neither of the before mentioned cybercrime offences is a felony, however, so the attempt of incitement would not be punished in these cases.

A somewhat "innocent" intent would – as a rule – not exclude criminal liability, as long as the offender still acted with sufficient intent (Vorsatz) concerning the objective elements of the offence in question, i.e. willingly and knowingly fulfilled these elements. If the "innocent" intent leads to a mistake of law (Verbotsirrtum), where the offender lacks the awareness of acting unlawfully, punishment is legally excluded if this mistake was unavoidable (which is, however, only rarely assumed by the courts).

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?

The general rules for assuming German jurisdiction have already been explained above. It mostly depends on the question if the victim and / or the offender are German nationals or if the crime has been committed on German territory. In exceptional cases (like it is the case with human trafficking or the spreading of child pornography) where important "universal" legal interests are violated, German criminal law is also applicable if none of the before mentioned "domestic connections" are given. Specific regulations concerning minor offenders do not exist.

Universität Augsburg University

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)?

The Budapest Convention on Cybercrime of 2001, the only treaty under international law concerning the fight against cybercrime was signed and ratified by Germany in 2009. The treaty is supported by the EU as the most important global instrument in the fight against cybercrime. In Germany it has led to a number of legal and institutional reforms, inter alia an extension of the scope of cybercrime offences and more international cooperation in the fight against cybercrime. In November 2021, the second additional protocol of the convention has been decided. It is supposed to further enhance international cooperation and to facilitate the disclosure of electronic evidence. This might be the first step towards a harmonization of electronic evidence law throughout Europe (not only within the EU). As this is a new development and the protocol has not been ratified yet by Germany, one will have to wait for the consequences regarding law enforcement.

Especially the fight against sexual abuse of children and child pornography has been influenced by several legal acts of the European Union, e.g. the framework decision of the European council to fight sexual exploitation and child pornography which was implemented into German law in 2008 (BGBl. I S. 2149). Another relevant act was the guideline 2011/93/EU of the European council and the European Parliament that was also implemented into German law (BGBl. I S. 10).

The Lanzarote Convention of the Council of Europe is another relevant point of reference. It contains best-practice-standards to strengthen the legal position of minors and to protect them against sexual violence, including the obligation to introduce certain criminal offences; apart from that, preventive and educative measures are recommended. All 46 member states have ratified the convention in the meantime, Germany did so in November 2015.

Influenced by these supranational acts, Germany has seen several reform bills concerning sexual crime and child pornography in recent years which were all strongly focused on increasing the scope of criminal liability and making punishment more severe. In the last reform step in 2021, all types of child pornography (including the possession of such material) became a felony with a punishment of at least one year of prison with no possibility of assuming a less severe case or to close the proceedings according to §§ 153 et seq. StPO or (regarding juvenile offenders) § 45 section 1 JGG. Some critics say that this is a form of over-criminalization that would in some cases lead to disproportionate punishment at least for adults (where there is less flexibility compared to juvenile criminal law).

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.)?

According to the Federal Report on Cybercrime (Bundeslagebild Cybercrime, 2021) the Federal Criminal Police Office (Bundeskriminalamt) is connected with all relevant cybercrime units worldwide 24/7 and is engaged in many joint operations against offenders of cybercrime. This cooperation is supported and intensified by a mutual exchange of embedded agents. On the European level there is a close and institutionalized cooperation with Europol, on the international level with Interpol. Apart

from these measures, there is a steady bilateral exchange with various countries regarding the threat of cybercrime and best practices in fighting it.

Within the EU, general tools like the principle of mutual recognition and the European Arrest Warrant are applicable to facilitate law enforcement in cross-boarder cases. For cybercrime in general, but also human trafficking and child pornography, it is no prerequisite for the Arrest Warrant that criminal liability exists in both countries involved.

There are two institutions on the European level that also have to be mentioned in this context. The European Cybercrime Center is an EU organization which is located at the European Police Agency Europol. It was founded in 2013, but actually began its work in 2015. Its objective is to coordinate cross-boarder law enforcement of cybercrime within the EU. Its work mostly aims at cybercrime in a narrow sense, darknet marketplaces and illegal trade, therefore at economic cybercrime.

The European Network and Information Security Agency (ENISA) was founded in 2004 on the legal basis of Regulation 2019/881 of the European Parliament. It connects different EU institutions, national agencies and private companies to facilitate the exchange on established procedures and best-practice standards. Furthermore, it publishes scientific reports and reports regarding the status quo of the fight against cybercrime within the EU.

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?

To the best of my knowledge, there is no specific impact on cybercrime committed by minors by the before mentioned rules and policies.

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.

According to the German Federal Police Cybercrime Statistic (Bundeslagebild Cybercrime, see https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html), 143.363 cases of cybercrime were registered in 2021, which is an increase of 12 % compared to 2020, continuing an ongoing trend over the past years. This statistic only refers to cybercrime in a narrow sense, i.e. crime directed against the internet or systems of information technology (like hacking, phishing, DDoS-attacks etc.). Offences that were just committed by making use of the internet (like cyber-fraud or online grooming) are not included. The rate of cybercrime cases that were “solved” (in the sense that at least a suspect could be identified) was comparably low (29,3 %), as investigation in this area is difficult due to the (somewhat) anonymous character of the internet. The “solving rate” (Aufklärungsquote) has dropped over the years, possibly due to a more professional modus operandi of offenders. The Federal Police also stresses that the “dark area” of undetected (or at least unregistered) cybercrime was comparably big. Unfortunately, this report

contains no information concerning the age of offenders of cybercrime in the before mentioned narrow sense.
According to the general Federal Police Crime Statistic (Polizeiliche Kriminalstatistik, PKS), 383.469 offences that were committed by using the internet were counted in 2021, which is an increase of 19 % compared to 2020. 44.226 of these offences (11 %) were directed against sexual self-determination. Unfortunately, the statistic contains no information on the age of offenders of this whole group of delinquency. Taking a look only at §§ 202a-d StGB (being cybercrime in narrow sense) one can see that offenders under 18 years are prosecuted not very often: the PKS 2021 showed that only 8,8 % of all 2.711 suspects in this area were under 18 years; for data manipulation and data sabotage (§§ 303a, 303b StGB), the share of persons under 18 years was 13,3 % out of 959 suspects. If we take a look at the persons actually convicted for these crimes, the numbers are even smaller: in 2020, only 48 persons were convicted for a crime according to §§ 202a-d StGB, with only one person being under the age of 18 years (2 %). For data espionage or computer sabotage (§§ 303a and b StGB), 89 persons were convicted in 2020, with a share of 15 % of persons under the age of 18 years.

39.171 cases of spreading, acquiring, possessing or producing child pornography (§ 184b StGB) and 5.105 such cases regarding youth pornography (§ 184c StGB) were registered in the PKS 2021. Compared to 2020, both figures have risen dramatically by 108 % (§ 184b StGB) and 63, 3 % (§ 184c StGB). One of the reasons for this development is the increase of internet investigations by the police, together with a growing social and political awareness for this type of delinquency which has led to several legal reforms expanding the scope of criminal liability and punishment at the same time. Another plausible explanation is an increasing tendency of children and youth to share and spread illegal pornography in group chats (WhatsAp, Instagram, Snapchat, Facecbook…) without sufficient awareness of the illegal (criminal) background (Deutsches Jugendinstitut, Zahlen – Daten – Fakten, Jugenddelinquenz im Kontext von Digitalisierung 2022, S. 18, see https://www.dji.de/veroeffentlichungen/aktuelles/news/article/aktuelle-zahlen-zur-cyberkriminalitaet-von-jugendlichen.html). This is supported by the fact that regarding this crime, the percentage of suspects under 18 years registered by the police is 41,4 % (18.069 out of a total number of 43.677 suspects, see PKS 2021, S. 13). If one looks only at child pornography offences that have been committed via the internet (31.383, 80 % of all cases), the number of registered cases has increased since 2020 by 150 %. In this important subgroup of child pornography offences, the share of minor offenders under 18 years is 54 % (15.536 out of 28.661 suspects, see https://www.polizei-beratung.de/startseite-und-aktionen/aktuelles/detailansicht/polizeiliche-kriminalstatistik-2021/). The share of minor offenders between 14 and 18 years is much smaller when we take a look at the persons actually convicted of an offence of child pornography (§ 184b StGB): in 2020, 2602 persons were convicted, with only 12 % of them being minor offenders. This indicates that many of these cases with minor offenders have been dealt with informally via diversion by the public attorney´s office (which is much more difficult from now on due to the legal reform mentioned above).

In 2021, cases of insult committed by making use of the internet had a share of 7,6 % of all cases of insult. The number of internet insults in 2021 was 17.980, which is an increase of about 24 % compared to 2020 (PKS 2021, S. 20). 9 % of all suspects of insult offences were under the age of 18 years. It is plausible that the increase of offences is due to new legislation in the area of hate crime which comes

along with more social and political awareness for this phenomenon and (possibly) increased investigative work by the police.

20.464 cases of stalking (§ 238 StGB) were registered in 2021, of which 2.829 (14 %) were cyberstalking cases which had been committed via the internet. Only 2 % of suspects registered in the police statistics were under the age of 18 years. It is possible that due to the new legislation (which now includes more and different types of cyberstalking), the share of cases committed via the internet will increase in the future. In 2020, 407 persons were convicted for a stalking offence; only 2 of these persons (0,5 %) were between 14 and 18 years old.

In the same year, 4.464 potential[1] cases of grooming (§§ 176 section 4 no. 3 and 4 StGB old version) were registered, which is an increase of 16,3 % compared to 3.839 registered cases in 2020. This increase is in line with a long-term trend in recent years with a steadily rising number of reported online grooming cases. In 2021, 3.539 cases (79%) had been committed via the internet – compared to 2020, the number of this offences has increased by 34 %. 44 % of all suspects regarding § 176 section 4 no. 3 and no. 4 StGB were under the age of 18 years. Now that there exists a special regulation for online grooming alone in § 176b StGB, it will be interesting to see how figures of reported cases will develop in the next years. The number of convicts is much smaller: in 2020 (the last available data), 537 persons were convicted for any offence according to § 176 section 4 StGB (which, as mentioned before, also includes other sexual offences apart from online grooming). 91 of these persons (16,9 %) were between 14 and 18 years.

Human trafficking (§ 232 StGB) was only registered 160 times in 2021; none of these cases was committed by using the internet and none of it had a suspect under 18 years. In 2020, 23 offenders were convicted for human trafficking, of which 2 (8,7 %) were minor offenders under 18 years.

Of course, regarding all this figures, one must consider that the official statistics only contain cases that were detected and registered by the police. Offences that remained in what is called the “dark area” (Dunkelfeld) are not listed here, so it is hard to determine if a statistical increase of a certain offence is due to an actual increase or rather due to the fact that more of these offences came to the attention of police authorities (e.g. because more cases were reported to the police and/or the police increased their investigative efforts). It is estimated that more than 90 % of cybercrime remains within the dark area (BKA, Bundeslagebild Cybercrime 2021, S. 4).

There are some attempts to shed some light on the amount of this unregistered crime by conducting research, mostly by questionnaires (self-reported delinquency and / or victimization surveys).

In a recent victimization survey in Germany, 30 % of all interviewed persons reported that they had become victim of cybercrime (in the before mentioned narrow sense) at least once in their lifetime; 14 % reported a victimization over the past 12 months. The respective figures for cybercrime in a broad sense were 37 % and 24 %. 6 % reported that they had been threatened via the internet over the past 12

[1] The problem is that in the former version of the Criminal Code, grooming was not registered separately; all cases of §§ 176 section 3 no. 3 and 4 were registered together, which also included acting on a child by using explicit pornographic material, without disguising the sexual background of the communication at all.

months, 7 % had been approached via the internet with a sexual motivation against their will, 8 % had been sent explicit photos or videos without their consent (Deutsches Jugendinstitut 2022, S. 14 et seq).

In another survey conducted by the German Youth Institute, 7.375 children not more than 14 years old were asked about their experiences with mobbing. 19 % reported that they had experienced mobbing, 4 % even daily or several times per week. 15 % admitted to have been "offenders" of mobbing at least once. Cyber-Mobbing (in the sense of being humiliated of insulted online) was reported by 11 % (Deutsches Jugendinstitut 2022, S. 19).

Concerning the phenomenon of cyber-grooming, a survey published by the State Media Agency (Landesmedienanstalt) of North Rhine-Westphalia (see https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Medienorientierung/Cybergrooming/211216_Cybergrooming-Zahlen_Praesentation_LFMNRW.pdf) showed that of all of the 2.163 interviewed persons between 8 and 18 years, 14 % had been asked to send photos with sexual content by online communication (within the group of 16-18 years, the share was 20 %). 15 % had received pictures with nudity via online communication (16-18 years: 27 %); 10 % were threatened via internet (16-18 years: 12 %).

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

There is nothing else I would like to comment.