QUESTIONNAIRE

THE NETHERLANDS

prof. Bert-Jaap KOOPS,

Tilburg University

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

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

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

Answer:

Yes, see art. 248e Dutch Criminal Code (Wetboek van Strafrecht) (hereafter: DCC).

Conditions for application: use of a computer or communication service; targeted at someone below 16 (or someone who pretends to be below 16, with or without the help of a virtual creation — e.g., an avatar or chatbot such as Terre des Hommes' creation Sweetie); proposing a meeting with the intention of committing a sexual offence with that person or creating sexual-abuse images of the person; and conducting an activity towards materialising the meeting (e.g., sending a map of the area of the meeting place, or booking a travel ticket). The latter is a necessary condition – only communicating about sex-related content is not punishable under art. 248e DCC.[1] To fulfil the requirement of a step towards materialising the meeting, it is sufficient if the perpetrator pressures the victim to meet soon and gives his phone number to her.[2]

Punishment: maximum two years' imprisonment or fine of the fourth category (i.e., maximum € 22,500). (The Netherlands does not have minimum sentences.)

Applicable policy: I am not aware of a specific policy in relation to grooming. Cybercrime in general has priority in criminal investigation, but that covers a wide range of offences. It will depend on the seriousness of the particular case, given all circumstances, whether it will get priority in prosecution. (E.g., if it will be difficult to trace a suspect, or if the suspect is likely abroad – particularly in a country with which mutual legal assistance is more complicated or non-existent –, the case will likely get low priority.)

Issues of application: Under previous law, in 2013, a man was acquitted of grooming because it turned out that the person he was grooming, whom he thought to be a minor, was in fact an adult policewoman.[3] Therefore he had not actually proposed a meeting to a minor. As a result, the law was changed to include 'someone who pretends to be below 16, with or without the help of a technical tool, including a virtual of someone below 16.'[4] The latter part – using a technical tool – was added because of the publicity given to Terre des Homme's campaign against webcam sexual abuse, using an avatar of a young Philippine girl called Sweetie. The law-maker considered it important that law-enforcement might also use such an avatar in grooming investigations. However, police use of avatars and/or chatbots on platforms known for grooming or webcam sexual abuse raises questions of entrapment. If law enforcement uses such tools – and also if they use actual police officers who pretend to be minors – they should make sure to comply with the so-called 'Tallon criterion' against entrapment: they should not induce someone to commit crimes that they otherwise would not have committed.

[1] Rb. [District Court] Oost-Brabant, 9 December 2014, ECLI:NL:RBOBR:2014:7494.
[2] HR [Dutch Supreme Court] 11 November 2014, ECLI:NL:HR:2014:3140.
[3] Hof [Court of Appeal] Den Haag, 25 June 2013, ECLI:NL:GHDHA:2013:2302.
[4] *Kamerstukken II* [Parliamentary Documents Second Chamber] 2016/17, 34 372, 15.

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 (or bullying in general) is not punishable as such. Depending on the concrete form it takes, cyberbullying behaviour might fall under one of the following offences:

- Stalking (which includes both physical and cyberstalking): art. 285b DCC: the systematic intentional infringement of someone's privacy, with the aim to force the person to do (or not do) or undergo something or to induce fear; punishable by at most three years' imprisonment or a fine of the fourth category. The offence can be prosecuted only upon complaint of the victim. The infringement of privacy does not have to be particularly serious; it suffices if there is an infringement.[5]
- Harassment: art. 284 DCC: without right forcing someone to do (or not do) or undergo something, using violence or some other factual circumstance, or the threat of violence or of another factual circumstance, against the victim or a third person, or by threatening with defamation; punishable by imprisonment of at most two years or a fine of the fourth category.
- Sexual harassment: art. 246 DCC: forcing someone to commit or to undergo lewd activities ('ontuchtige handelingen') by using violence or some other factual circumstance, or the threat of violence or of another factual circumstance; punishable with at most eight years' imprisonment or a fine of the fifth category (€ 90,000).
- Discrimination: art. 137c et seq. DCC: publicly offending a group (art. 137c) or making public a statement that offends a group (art. 137e) because of their race, religion, physical or mental impairment, or sexual orientation; punishable with imprisonment of at most one year (art. 137c) or six months (art. 137e) or a fine of the third category (€ 9000, art. 137c and 137e). This could apply to cyberbullying if the victim is verbally abused or harassed because of belonging to a certain minority in a non-closed group on social media.
- Doxing: proposed art. 285d DCC: doxing is not yet criminalized as such, but a Bill is being prepared to make doxing as a specific criminal offence. A draft published for consultation mid-2021 defined this offence as procuring, spreading, or making available personal data about someone with the aim of inducing fear in that person or seriously hindering him or her.[6]

Known issues of application:

- Stalking: the primary issue of application is when behaviour can be considered as 'systematic'. Case-law indicates that this depends on the nature, duration, frequency, and intensity of the contact.[7] For example, contacting someone three times and visiting her house three times, putting threatening messages in the mailbox, within the time-frame of one day was considered not sufficient evidence of 'systematic' infringement of someone's privacy.[8] In contrast, making several threatening phonecalls and various times having non-ordered goods delivered at someone's home, besides sending a not-ordered funeral car to the home, is clearly 'systematic'.[9] Another issue of application is when there is an infringement of privacy. This should be determined in an objectified way, implying that if someone has a nervous character and feels unreasonably quickly hampered in her

[5] HR 15 November 2005, ECLI:NL:HR:2005:AU3495.

[6] Wetsvoorstel strafbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden [Draft Bill on criminalising the use of personal data for intimidating purposes], 12 July 2021, available at https://www.internetconsultatie.nl/strafbaarstellinggebruikpersoonsgegevensvoorintimiderendedoeleinden.

[7] See, e.g., HR 11 March 2014, ECLI:NL:HR:2014:533.

[8] HR 11 March 2014, ECLI:NL:HR:2014:533

[9] HR 6 July 2021, ECLI:NL:HR:2021:1002.

privacy, where others in similar circumstances would not feel thus, this does not count as a relevant privacy infringement.[10]

- Harassment: the term 'violence' in art. 284 DCC is relatively clear; it includes causing someone to be unconscious or powerless.[11] Less clear is what the term 'factual circumstance' ('feitelijkheid') covers. Generally, these are all acts that are not violence; however, the act should be such as to create such a mental pressure on the victim that they cannot offer resistance.[12] A relevant example of threatening with a factual circumstance, which has been qualified as harassment, is threatening to publish the name and address of a victim on the internet with the statement that he is looking for homosexual contacts.[13]
- Sexual harassment: the threshold of what counts as sexual harassment ('ontuchtige handeling') seems to be relatively low. It includes, for instance, unexpectedly squeezing someone's buttocks in passing.[14] However, this may not be easy to prove: only a declaration by the victim is not sufficient in view of the minimum evidence requirements (unus testis nullus testis).[15] Covertly making visual recordings, e.g., in toilets or dressing rooms, does not qualify as sexual harassment because of the lack of interaction between perpetrator and victim.[16]
- Discrimination: one intrinsic issue of application is when the threshold of discrimination is reached, and when the public interest of free speech prevails; this depends very much on all the circumstances of the case.[17] One example where the artistic exception in free speech was not sufficient to warrant discriminatory statements was the publication of a rap video on YouTube which included texts such as "faggots I do not shake hands with" and "I hate them fucking Jews even more than the nazis" (my translation, BJK); the mere fact that the words rhymed was not sufficient to claim that the statements were necessary for artistic freedom of expression, and the statements also otherwise lacked of a functional relationship with the rest of the rap song. Hence, the perpetrator was convicted of discrimination (137c DCC).[18] Another issue of application is what counts as 'making public'. Making statements in closed groups on social media may not qualify as making public, but this will depend on the circumstances of the case, including not only the size of the group but also its character and the likelihood that a statement made in the closed group will subsequently be distributed more broadly.[19] If it is likely that the perpetrator only intended the statement to be read by a small number of like-minded persons, and could expect that it would remain within this group, this will not count as 'making public'.[20]

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 or fake news is not criminalised as such. If the misinformation serves to induce others to commit an offence, the perpetrator of the deception can be held responsible for the crime too as the intentional provocation (art. 47 DCC, the definition of the perpetrator of an offence). In special circumstances, depending on the content, it could be qualified under special criminal offences, such as

[10] HR 15 November 2005, ECLI:NL:HR:2005:AU3495.
[11] Van der Meij, *T&C Strafrecht* (Kluwer online, 2022), art. 284, comment 9b.
[12] Ibid., comment 9c.
[13] Rb. Alkmaar 30 July 2003, LJN AI0650.
[14] HR 6 November 2018, ECLI:NL:HR:2018:2061.
[15] HR 2 November 2021, ECLI:NL:HR:2021:1594.
[16] HR 14 February 2012, ECLI:NL:HR:2012:BU5254.
[17] See Ten Voorde, *T&C Strafrecht* (Kluwer online, 2022), art. 137c, comment 1 and 137e, comment 10b.
[18] HR 26 June 2018, ECLI:NL:HR:2018:1003.
[19] See generally HR 22 April 2014, ECLI:NL:HR:2014:952, on the factors that are relevant for considering a statement to be made 'in public'.
[20] Hof Den Haag 23 January 2008, ECLI:NL:GHSGR:2008:BC3441.

manipulating stock prices (art. 334 DCC: spreading a false message to influence the price of goods or stocks, punishable with up to two years' imprisonment or a fine of the fifth category). In theory, forgery (art. 225 DCC, punishable with up to six years' imprisonment or a fine of the fifth category) could apply, if the information has a purpose of proving a legally relevant fact; but this will not often be the case with deceptive information spread by minors.

If the deception includes the use of someone else's identity, the behaviour could fall under identity fraud (art. 231b DCC, punishable with at most five years' imprisonment or a fine of the fifth category). This is applicable if the abuse of someone else's identity is aimed at hiding one's own identity or to abuse the other's identity, and if such abuse causes any harm.

Case-law and known issues of application: since fake news is not criminalised as such, there are no relevant cases or issues of application. (A search in the main case-law database, on rechtspraak.nl, on 'fake news', 'misinformation', and 'fake information' only resulted in a few cases, where the term was used in the context of unreliable statements by witnesses in organised-crime cases, revolving around the question whether the statements could be used as evidence. No cases were found involving criminal liability for deceitful information.)

One potentially interesting element, however, is the term 'spreading a false message' to influence stock prices in art. 334 DCC. This has been interpreted as also covering falsely stating an expectation (so not only falsely stating facts), as well as providing facts that are in themselves true but at the same time holding back other facts that are essential for interpreting the facts.[21] Should the law-maker criminalise fake news in the future, then this interpretation is likely to play a role in the interpretation of 'fake news' as well. However, although the issue of criminalising fake news is being debated,[22] there are no pending proposals to do this. In the literature, it is noted that a criminalisation of fake news is complicated because it is such a broad term encompassing a wide variety of statements, and because a prohibition is very difficult to enforce.[23]

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

Answer:

The primary provision criminalising human trafficking ('mensenhandel') is art. 273f DCC, punishable with up to twelve years' imprisonment or a fine of the fifth category. This provision implements various international and supranational legal instruments, most importantly the UN Palermo Protocol (2001) and Directive 2011/36/EU.

Art. 273f para. 1 has nine sub-paragraphs, describing different forms of human trafficking. The main form (sub 1°) is defined as forcing someone through coercion, force, or another factual circumstance (or threatening therewith), through extortion, deception, abuse of a vulnerable position, or by bribing someone who holds authority over the victim. If the victim is under 18, or otherwise in a vulnerable position, the act constitutes a qualified offence with a higher maximum sentence (up to fifteen years' imprisonment, art. 273f para. 3). It is relevant to note that coercion may also apply if the victim consented, since also in such cases there can be exploitation ('uitbuiting').[24]

[21] Van der Velden and De Jonge, *T&C Strafrecht* (Kluwer online, 2022), art. 334, comment 8a.
[22] See, e.g., https://www.ru.nl/rechten/alumni/@1356427/strafrecht-online-desinformatie-nepnieuws/ (accessed 29 June 2022).
[23] A.P. Engelfriet, 'Het fake news op de pijnbank van het Nederlands strafrecht', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2020 (2), p. 75-78.
[24] Van der Mey, *&C Strafrecht* (Kluwer online, 2022), art. 273f, comment 9c.

For the present study, possibly the fifth form is most relevant, since this could apply to the use of the internet to facilitate human trafficking by grooming or attracting potential victims. This act (art. 273f para. 1 sub 5) is defined as inducing someone under 18 to make themselves available for committing sexual acts with another person for payment. This element of the provision also applies to cases of 'lover boys', who sexually exploit women by pretending to act as their boy-friend.[25]

For human trafficking with a cyber-component, there is little case-law available. One important case is a case in which an underage perpetrator induced a 16-year-old girl to make pictures of herself in a bra and string underwear, which he subsequently published online as advertisements with the statement that she was available for sex. As a result, several men contacted the victim. The Dutch Supreme Court qualified this as human trafficking, noting that in the case of art. 273f para. 1 sub 5, there is no particular requirement of 'exploitation', given that it involves minors who deserve special protection. As a result, the fact that the victim in this case did not actually have sex with the men who contacted her, was not an obstacle to convicting the perpetrator for human trafficking, as he had induced the victim to make herself available for prostitution.[26]

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

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

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

Answer:

Minors below the age of 12 cannot be prosecuted for criminal offences. For those aged 12 and older, there is a special procedure in Dutch criminal procedure, laid down in Title VIII-A of the First Book of the Dutch Criminal Code (articles 77a through 77gg DCC). There rules not only for minors (under 18) but also for juveniles (under 23).

For minors between the age of 12 and 18, there are special rules and cases are dealt with before a juvenile court. Generally, the possible sanctions are much lighter than those for adult perpetrators. The highest criminal sanction is one year of youth detention (*jeugddetentie*) for minors between 12 and 16 and two years' youth detention for minors aged 16 or older (art. 77i DCC). The maximum fine is a fine of the second category (i.e., € 4500) (art. 77l DCC).

Instead of criminal prosecution, the police can opt for a different route, namely to send a minor to a special institution, Bureau HALT,[27] aimed at preventing and dealing with youth crime. This institution can give community service or other interventions. In these cases, the minor will not get a criminal record. Note that this is only possible for certain, generally less serious, offences. A HALT intervention is not possible for the four cybercrimes that this questionnaire focuses on.

[25] Hof Arnhem-Leeuwarden 26 February 2020, ECLI:NL:GHARL:2020:1656.
[26] HR 2 October 2018, ECLI:NL:HR:2018:1823.
[27] See https://www.halt.nl/ (accessed 6 July 2022).

In exceptional cases, minors aged 16 or 17 can be prosecuted under the adult criminal law (art. 77b DCC). This can only happen with very serious crimes, if the circumstances of the case warrant prosecution under adult criminal law, and if the minor's personality gives occasion for such prosecution. This happens rarely in practice.

For juveniles between the age of 18 and 23, there is also the possibility of being prosecuted under youth criminal law rather than adult criminal law (art. 77c DCC). The court can decide to do so if the juvenile's personality or the circumstances of the case give rise to this. Prosecution under youth criminal law used to be possible for juveniles below 21, but the age limit was raised in 2013 to 23. Nevertheless, in practice this possibility is still used for juveniles aged 18 and 19 rather than older juveniles.

For the application of youth criminal law, there are policy guidelines to guide the police and Public Prosecutor.[28]

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: To my knowledge, there is no special policy for cybercrime committed by minors (or juveniles). The general rules of youth criminal law (see Question 5) will apply.

Minors are prosecuted for cybercrime in practice. A study from 2013 showed that 0.3% of all youth crimes registered by police involved cybercrime (hacking, spreading viruses, fraud, child pornography, forgery of bank cards, or online threats).[29] Although the report is nine years old and the incidence of cybercrime has risen, it is likely that cybercrime still constitutes a very small proportion of crimes for which minors are prosecuted. Some cases have been published of minors who have been prosecuted and convicted for hacking or spreading viruses.

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: Minors can be prosecuted for online grooming under the general rules of youth criminal law (see Question 5).

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: Obtaining sexually explicit material without consent of someone (e.g., by hidden cameras) is punishable under art. 139h para. 1 DCC (at most one year's imprisonment). Obtaining sexually explicit material of a minor (with or without consent) in principle constitutes acquiring or creating child pornography (art. 240b DCC). Obtaining sexually explicit material to force a victim to do something

[28] *Richtlijn en kader voor strafvordering jeugd en adolescenten, inclusief strafmaten Halt*, *Staatscourant* 2021, 2578.

[29] Sven Zebel et al., *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning*, The Hague: WODC 2013, p. 13.

constitutes harassment (art. 284 DCC). If these crimes are committed by minors, they can be prosecuted under the general rules of youth criminal law (see Question 5).

For sexual offences related to sexting, there are specific policy guidelines, which take into account, inter alia, the age difference between victim and perpetrator, intent, and whether violence or deception was involved.[30]

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: If cyberbullying takes the form of one of the crimes mentioned above (see Question 2), minors can be prosecuted for these under the general rules of youth criminal law (see Question 5).

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: If misinformation or deception takes the form of one of the crimes mentioned above (see Question 3), minors can be prosecuted for these under the general rules of youth criminal law (see Question 5).

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: If actions facilitating human trafficking take the form of one of the crimes mentioned above (see Question 4), minors can be prosecuted for these under the general rules of youth criminal law (see Question 5).

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: In theory, online piracy is a criminal offence (art. 31a Dutch Copyright Act (Auteurswet), punishable with up to one year's imprisonment or fine of the fifth category), but in practice, copyright violations are not combated through criminal law but only through private law.

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 is punishable under art. 138ab DCC (with at most two years' imprisonment or fine of the fourth category for 'simple' hacking, and at most four years' imprisonment or fine of the fourth category for aggravated hacking, which includes cases in which the hacker copies or intercepts data from the hacked computer). This also applies if IoT or connected devices are hacked, as long as these devices qualify as a 'computer' (*geautomatiseerd werk*), which likely is the case because of the broad definition of 'computer'. Minors can be prosecuted for hacking under the general rules of youth criminal law (see Question 5).

[30] *'Pubers in beeld'. Leidraad afdoening sextingzaken*, November 2017.

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: If Cybercrime as a Service is used for DDoS attacks, this constitutes the crime of blocking access to or hindering the use of a computer (art. 138b DCC). If the attack uses a botnet, the aggravated offence of art. 138b para. 2 DCC applies, punishable with at most three years' imprisonment or fine of the fourth category.

Depending on the specific activity, Cybercrime as a Service might also be punishable as computer sabotage (system interference) in art. 161sexies DCC (punishable with up to six years' imprisonment or fine of the fifth category if the behaviour results in danger to public goods or to delivery of services); or as system interference (art. 350c DCC, punishable with at most two years' imprisonment or fine of the fourth category).

If the behaviour is 'somewhat innocent', i.e., if there is no criminal intent, the act might be punishable under one of the negligence offences: art. 161septies DCC (the negligent causing of computer sabotage, involving a computer used for the common good or delivery of services; punishable with at most six months' imprisonment or fine of the fourth category) or art. 350b DCC (negligent data interference, punishable with at most one month's imprisonment or fine of the second category). For criminal negligence to apply, the non-intentional behaviour must be reproachable, against the yardstick of what can be normally expected in human interactions.

Minors can be prosecuted for these offences under the general rules of youth criminal law (see Question 5).

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: Jurisdiction is established for offences on Dutch territory (art. 2 DCC), for particular crimes committed abroad (art. 4 DCC; the only cybercrime for which this applies is forgery), for serious crimes committed abroad against persons with Dutch nationality or permanent residence (art. 5 DCC), for crimes committed by Dutch persons abroad if they also constitute an offence in the country where they were committed (art. 7 para. 1 DCC), and for particular crimes committed by Dutch persons abroad, also in the absence of double criminality (art. 7 para. 2 DCC; the only cybercrime for which this applies is child pornography).

The Netherlands generally deals with jurisdiction issues and extra-territorial effect under the rules of international law.

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: The main supranational legal instruments that apply in the Netherlands in this context are the Budapest Convention and EU Directives (in particular Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2013/40/EU on attacks against information systems). As far as the provisions of these instruments were not already in place in

Dutch law, they have been implemented in the Dutch Criminal Code and the Dutch Code of Criminal Procedure. The answers above reflect the provisions as they have been, where necessary, adapted to these supranational instruments, so Dutch law should be read and interpreted in accordance with the provisions of these instruments.

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: The Netherlands is actively involved in international cooperation in cybercrime cases, primarily in the networks of Europol and the Octopus community of the Budapest Convention. EU law applies to cross-border cooperation among EU member states. The European Convention on Mutual Assistance in Criminal Matters (ETS 30) applies to cooperation among member states of the Council of Europe. Under the Budapest Convention, all the mutual legal assistance provisions apply for countries that have ratified this Convention.

Mutual legal assistance is also available for countries with which the Netherlands has a bilateral treaty: Argentina, Australia, Bahamas, Canada, India, Japan (*), Kenya, Liberia, Malawi, Morocco (*), Mexico, Monaco, New Zealand, Pakistan, San Marino, Suriname, Tanzania, Uganda, and United States.[31]

(*) designates countries with which the bilateral treaty only involves legal aid; the other countries cover both extradition and legal aid.

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: I am not aware of any particular effect or impact on minors in relation to jurisdiction or mutual legal assistance.

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: Statistics Netherlands (CBS) publishes two-yearly reports on crime incidence, based on victim surveys. These statistics include

A graphic from 2020 shows that cybercrime incidence has risen somewhat in recent years (see Figure 1).[32]

[31] https://www.internationalerechtshulp.nl/wat-is-rechtshulp/juridische-basis-voor-rechtshulp (accessed 6 July 2022).

[32] CBS, 'Minder traditionele criminaliteit, meer cybercrime', October 2020, https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime (accessed 6 July 2022).

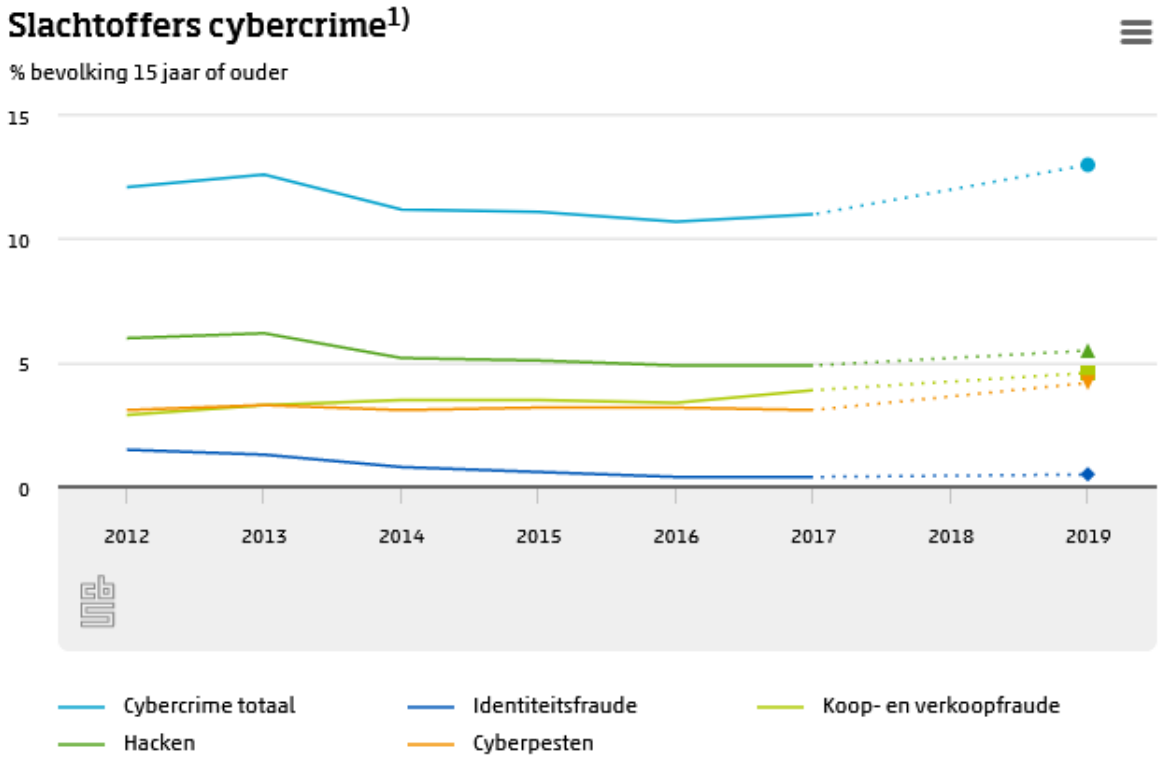

*Figure 1. Victims of cybercrime in the Netherlands, as **percentage of Dutch population aged 15 or older.** (Cyberpesten = cyberbullying; Koop- en verkoopfraude = buying or sales fraud.) Source: CBS, 'Minder traditionele criminaliteit, meer cybercrime', October 2020.*

The most recent report shows that the trend of an ongoing rise continues (Figure 2).[33] As the report states:

> 'In total, the victimization rate of online crime has increased by 22 percent since 2012 (index 2021 = 122). especially in recent years we see an increasing trend. The largest increase since 2012 has been the victimization of purchase fraud (index 2021 = 219), followed by sales fraud (index 2021 = 165) and online bullying (index 2021 = 126). The percentage of victims of hacking is quite stable over time. Fewer people come into contact with identity fraud, although there has been a slightly increasing trend in recent years.'[34]

[33] CBS, *Veiligheidsmonitor 2021*, 1 March 2022, available at https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021 (accessed 6 July 2022).
[34] Ibid., Ch. 5, available online at https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021/5-online-criminaliteit (accessed 6 July 2022) (my translation, BJK).

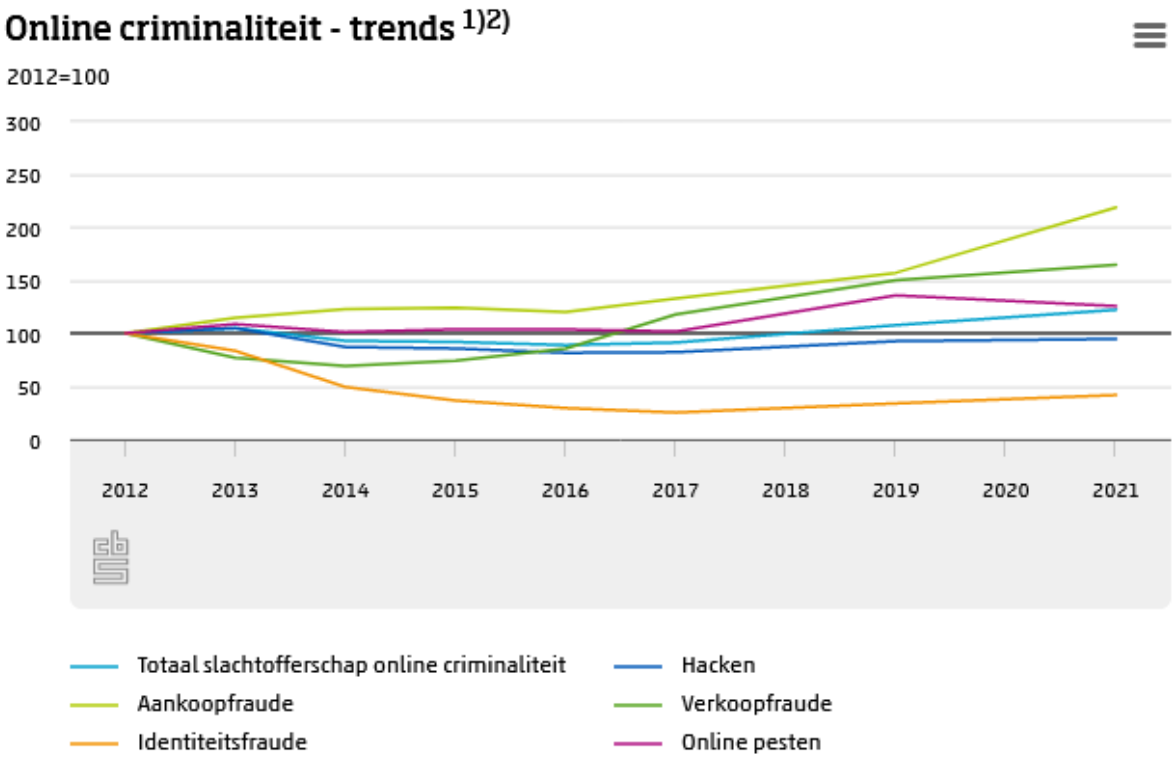

Figure 2. Trends in online crime in the Netherlands, based on a victim survey of Dutch population aged 15 or older. (Totaal slachtofferschap = Total victimisation; Aankoopfraude = purchase fraud; Verkoopfraude = sales fraud; Online pesten = cyberbullying.) Source: CBS, Veiligheidsmonitor 2021.

In total, in 2021, 17% of the Dutch population suffered one or more cybercrimes. It should be noted that this includes a wide variety of behaviour, broadly defined, including online threats and cyberbullying.

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

Answer: Dutch criminal procedure applies the **opportunity principle**, i.e., it is up to the Public Prosecutor to decide whether or not to prosecute a case, in contrast to the legality principle applied in some other countries where in principle each case should be prosecuted. This not only impacts the application of criminal law, of course, but also affects the content of the criminal law itself: the definition of offences is sometimes rather broad, covering also relatively trivial forms of behaviour that do not cause much harm, which is considered defensible because the Public Prosecutor will not prosecute such cases in practice. Particularly where it concerns relatively light instances of cybercrimes committed by minors, it is not likely that these minors will be prosecuted. If the crime has serious consequences, however, e.g., causing substantial damage or societal uproar, it will be more likely that the minor is prosecuted, also for the general prevention purpose of showing other minors that such behaviour is illegal.