QUESTIONNAIRE

UNITED KINGDOM

Michael MCGUIRE

Senior Lecturer in Criminology at the University of Surrey

1. Introduction

Please read carefully before answering the questionnaire

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

- ***Online grooming*** (further: OG) is the crime where the perpetrator (usually an adult) uses electronic communication services, including social media, to contact a minor and build rapport with the aim of eventually meeting in person for the purposes of sexual activity. The perpetrator may employ various strategies (deception, romantic/emotional attachment, promise of material or other benefits, blackmail, coercion, etc.) to lower a child's inhibitions, heighten their curiosity about sexual experiences, or otherwise convince them to meet up.
- ***Cyber bullying*** (further: CB) is a broad term that includes all types of bullying behaviour online. This includes cyber stalking and cyber harassment, and any other type of behaviour online aimed at hurting the victim. Cyber bullying may also have a sexual component.
- ***Misinformation and deception*** (further: MD) is a behaviour that may or may not be punishable by law depending on the context. It involves all kinds of information sharing that is fake, or deceptive. For a criminal qualification to apply, typically the behaviour will need to be intentional and there will need to be material consequences to this intention.
- ***Human trafficking with a cyber component*** (further: HT) is the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking.

The purpose of the game is to teach children how to remain safe online, while the obtained insights will be used to provide policy recommendations and educational tools.

The game does not focus solely on the threats of potentially falling victim to one of these four crimes. It also aims to raise awareness about the general threats of using IT, such as the Internet and connected devices, and minors' capacity to make responsible choices in this regard.

A particular point of interest is understanding whether minors are aware of when they, or someone else, is crossing the line in becoming offenders themselves, as this an important aspect of protecting children online. Due to the nature of online communication, inhibitions may be lowered, and certain actions may feel more innocent or less "real" than in real life. In addition, a perception may exist that what happens on the Internet has little or no impact beyond the digital world. This creates situations where minors engage in what they perceive to be relatively innocent behaviour ("everyone does this on the internet"), that may however have serious legal consequences.

One of the goals in RAYUELA is to ensure that minors realize when their behaviour may turn into actions that are punishable by law.

The present study and questionnaire are set up in the context of the RAYUELA project in order to provide an overview of the **legislative framework and relevant policies** in a number of countries, both in the EU and beyond, in relation to:

- How the main crimes of OG, CB, MD and HT are dealt with by the legal system i.e., which behaviours are punishable and under which conditions?
- How cybercrime and cyber-facilitated crime perpetrated by minors is dealt with in the legal system (both in general and specifically in relation to the crimes in focus)?
- What international instruments and cooperation mechanisms are available in dealing with cybercrime perpetrated by minors?

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

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

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

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

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

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

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

Answer:

In the UK, an act of sexual grooming is considered to take place whenever the trust of a child (defined as anyone under 16 in the UK) is sought for the purpose of sexual abuse or exploitation. Whilst grooming has traditionally occurred in immediate physical contexts it has now become a signal online offence and is punishable under the *Sexual Offences Act* (2003). Any online communication aimed at the sexual exploitation of minors is regarded as grooming under this statute, even where this is all that occurs and there is no additional offence.

Since no child under the age of 13 can ever consent to sexual activity under UK law, any act of grooming which leads to a sexual act takes place in that case is automatically classified as rape. Where guilt can be established, a maximum life sentence can be imposed

The Sexual Offences Act makes various specific provisions regarding grooming related offences.

Section 14 makes it an offence to *arrange* or *facilitate* a meeting with any child under the age of 16 where there is an intention by an individual to sexually abuse the child or there is an intention for another person to sexually abusing them.

Either of these offences can result in a term of up to six months' imprisonment and/or a fine in the magistrates' court. Where the case is heard before a judge, in the crown court, and a conviction obtained, a potential prison sentence of 4 years can be imposed.

Section 15 of the Sexual Offences Act makes it a criminal offence to *meet* a child under 16 (or if the offender does not reasonably believe that the victim is 16 or over). following the process of grooming.

This offence apples to individual persons over the age of 18 . They must have intentionally either met or communicated with the potential victim more than once. This applies even if they offender arranges to travel outside of the UK to meet the victim or travels with the intention of meeting them.

A sentence of six months in prison and/or a fine applies where found guilty in a magistrates' court. Where the offender is convicted in the crown court, there is a maximum prison sentence of 10 years.

Section 15 of the Sexual Offences Act 2003 has been subsequently amended by s67 of the Serious Crime Act (2015) in order to define *any* sexual communication with a child as a criminal offence. This provision, which came into force on 3 April 2017, means that any groomer who uses mobile phones, SMS texts, social media, emails or letters to communicate sexually with children or with the intention of eliciting a sexual response can be given a sentence of up to two years in prison.

An example of the crucial role of age in determining culpability here was seen in *Regina v Jenkins* 2019. Jenkins had begun communicating online with a young girl in April or May 2016 when the victim was then aged 15. She had entered a search term into Twitter with the letters DDLG, which stood for "Daddy Dom Little Girl" to which Jenkins responded by sending her a private message via Twitter, The victim made it clear to him that she was 15 and he told her he was in his forties (He was in fact 55), but he pursued an online relationship nonetheless. Jenkins groomed the girl until she began to engage in sexual activity, some of which was photographed and sent to him. Some of these activities were quite extreme, involving the administration of pain.

In September 2016, when the girl was five days short of her 16th birthday, Jenkins asked her to film herself masturbating. The images she sent of this formed the basis of the first of the offences - causing

or inciting a child to engage in sexual activity with penetration, contrary to section 10(1) of the Sexual Offences Act 2003

Jenkins second offence was causing or inciting a child to engage in sexual activity without penetration and this related to several other activities including photographs of the victim's breast with clothes pegs on and conversations about her touching herself.

The communications continued after 9 September 2016, however by this stage the victim had reached her 16th birthday and so the activities were no longer criminal.

In March Jenkins pleaded guilty to these offences and was sentenced to a term of four years' imprisonment for the first offence and two years concurrent for the second making a total sentence of four years' imprisonment. A Sexual Harm Prevention Order was made pursuant to section 103A of the Sexual Offences Act 2003.

Jenkins subsequently appealed on the basis that the way in which the communication between the parties started did not constitute clear evidence of grooming. The defendants lawyer argued for this to occur there must be a gaining of the trust of the victim so that what he or she previously considered unacceptable becomes acceptable. This, it was argued, did not occur given the circumstances of the communication between Jenkins and the victim.

However the appeal court did not agree. It ruled that by case law, grooming is simply a 'term of art' and so may cover a wide range of behaviour. The opinion of the original judge – that Jenkins drew the victim in using classic grooming techniques until she began to engage in sexual activity – was upheld and the appeal dismissed

Less ambiguous was the case of *Regina v Scarrott* which, because of the greater seriousness of the offending, resulting in a far more significant sentence. Scarrott had begun by contacting children over the internet and had built up a very significant following from a messages and other material he posted or uploaded. With an online profile which attracted over 70,000 followers Scarrott became regarded as a "social media influencer". He travelled significant distances from his home in Rochdale throughout England and Wales to meet children he had contacted. On one occasion he booked a hotel room in Cardiff in which to abuse a victim.

16 offences were committed over an eight-month period against six young females aged 14 or 15 years between 2018 and 2019. These included six offences of sexual activity with a child, contrary to section 9 of the Sexual Offences Act 2003; three offences of causing or inciting a child to engage in sexual activity, contrary to section 10 of the 2003 Act three offences of communicating with a child for the purposes of sexual gratification, contrary to section 15A of the 2003 Act; three offences of arranging or facilitating the commission of a child sex offence, contrary to section 14 of the 2003 Act (and one offence of meeting a child following sexual grooming contrary to section 15 of the 2003 Act (count 18).

The most serious offence on the indictment was count 16 (sexual activity with a child), which involved full vaginal sexual intercourse with a 15 year old girl, committed whilst on bail for the other offences. The applicant indicated a guilty plea to that offence only a week or so before trial, for which he was afforded appropriately limited credit of one-sixth. The sentence on that count was five years' imprisonment. Though Scarrott had no previous convictions, he was sentenced to a term of eight years and four months' imprisonment as result of sexual offences.

Both Scarrott and Jenkins, like anyone found guilty of the above offences, were also placed on the UK sex offenders' register. This requires an offender to notify the police of certain details, either for a specified amount of time or for life. A serious criminal offence occurs where the terms of the register is not adhered to with the risk of receiving a prison sentence.

New provisions for the investigation of child sexual exploitation offences were provided by the Anti-social Behaviour, Crime and Policing Act 2014 which allows the police to request the owner, operator or manager of premises they believe are being used for the purpose of child sexual exploitation. to provide information about their guests. This includes the name and address, and other relevant information, for example, age. Police can use this information to identify paedophile rings or other organised groups involved in child sexual exploitation. As a result these new provisions largely apply to offline abuse, though they can be tied into grooming investigations

The new Modern Slavery Act also has provisions covering the sexual exploitation of children, but this largely relates to trafficked children so will be discussed below.

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:

There is no legal definition of cyberbullying in U.K. law - which means that neither bullying nor cyberbullying are specifically criminal offences. However, there are criminal and civil laws that can be used to prosecute the perpetrators of cyberbullying. The key legal tools here include:

- The Public Order Act (1986)
- The Malicious Communications Act (1988)
- Protection from Harassment Act (1997)
- The Communications Act (2003)
- The Defamation Act (2013)

By contrast broader, more nuanced variants on bullying such as online harassment and cyberstalking *are* now both criminal offences under these legislations.

The oldest of these legal tools, the *Public Order Act* can be applied in cases of harassment, with Section 4 making it an offence to cause a person harassment, alarm or distress with intent by using: '... threatening, abusive or insulting words or behaviour, or disorderly behaviour, or displaying any writing, sign or other visible representation which is threatening, abusive or insulting. Offences under this act can be committed in both a private place and a public place and include written threats so could in theory be extended to online harassment, but in practice the Act has tended to be applied more in offline contexts – for example in the case of rioting or violent disorder.

The increasing significance of online harassment is maybe indicated by the fact that convictions for section 4 offences of the Act declined from 9,500 offenders sentenced in 2006 to 6,500 offenders sentenced in 2016.

Under the more recent *Protection from Harassment Act* a criminal offence occurs where the perpetrator engages in repeated and unwarranted behaviour to the victim, causing them 'alarm or distress'. Section 1 of the Act specifically prohibits '... a course of conduct which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.' In the online context, typical behaviours here are defined to include:

- Repeated texts, voicemails, letters or emails
- Repeated comments or threats

For an offence to occur there must be contact on more than two occasions - though the law makes it clear that this does not have to involve the same kind of behaviour on both occasions. This would mean that if 100 people were each to send a single abusive tweet to one person, an offence would not have been committed under the 1997 Act.

The sanctions which can be imposed depend upon the level and severity of the harassment involved and a kind of 'sliding scale' in sentencing operates here with a maximum sentence for harassment of six months imprisonment. Where these offences are racially or religiously aggravated, the *Crime and Disorder Act* (1998) can also be invoked and there is a maximum sentence of two years imprisonment.

The severity of sanction increases further where the harassment or stalking puts the victim in fear of violence. Here the maximum sentence is 10 years custody or, where racially or religiously aggravated, 14 years custody.

The Public Order Act has certain advantages over the Protection from Harassment Act in that 'harassment', 'alarm' and 'distress' are considered to have different meanings: For example, it is clearly *possible* that one can be harassed, without also experiencing emotional disturbance or any upset. The court must therefore find that the words or behaviour were likely to cause some real, as opposed to trivial, harassment. Thus there is no need for alarm or distress to be present, which is required for a successful conviction under the Protection from Harassment Act
It is also the case that under the Public Order Act, harassment is not specifically defined - thus a specific variety conduct does not need to be present.

A criminal offence in relation to harassment or bullying may also occur under the *Malicious Communications Act* (1988) where a communication is sent with the intention of causing distress or anxiety. In turn Section 127 of the more recent *Communications Act* (2003) also prohibits the sending of any electronic message which is grossly offensive, indecent, obscene or has a menacing character. This includes messages sent across social media platforms like Facebook or Twitter and indeed practically any other communications medium. Anyone guilty of this offence can be imprisoned for a term not exceeding six months, a fine, or both

A case of this was seen in in 2013 when Caroline Criado-Perez, an active feminist campaigner publicly argued publicly that images of the author Jane Austen should be used on banknotes in England and Wales. As a result of campaign, she was subjected to horrific abuse on social media with comments posted ranging from the less 'shut up' to 'rape her nice ass.' One individual, Peter Nunn, was found to be instrumental in subjecting Ms Criado-Perez to this torrent of abuse. As the victim later reported, 'He dug up my work history. He dug up my relationship and family history. He dug up my family's work history - including publishing home addresses. He wrote reams of blogs about me and my every public move. He made numerous videos about me. He set up numerous [T]witter accounts all of which spoke almost exclusively about me. In these same [T]witter accounts he detailed the best way] to rape and drown a witch, alongside repeatedly naming me as the head of the "witches' coven". He also boasted on [T]witter in the same account about bought a gun, and wondered "how much death" this gun could buy him.'

However, despite Nunn's conduct appearing to constitute a clear case of harassment causing the victim distress he was not prosecuted under the Protection from Harassment Act but by way of the Communications Act 2003. Under this, he was found guilty of sending grossly offensive communications and received a six-week custodial sentence – far less than the six months sentence available under the 1998 Act. The case highlighted concerns in the UK that police were failing to adequately apply the Protection from Harassment Act in relation to social media offences.

An example of a successful prosecution under this act was the case of Chloe Cowan, who was sentenced to 3 years imprisonment in July 2016. This was for cyberstalking offences under the Protection from Harassment Act originating in a range of Twitter posts described as 'vile' by the presiding judge. Cowan had created a number of fake Twitter accounts aimed at stalking Denise Fergus, whose son James Bulger had been tragically murdered by two child offenders in 1993. The tweets mocked and taunted her about her son's death and were sent directly to Ms

Fergus' social media account. They resulted in considerable distress to the victim, leaving her fearing to leave her home.

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:

Disseminating misinformation remains a legally ambiguous act in the UK with a number of conditions needing to be in place before a conviction can be obtained. In particular it is **not** an offence under existing legislation to post disinformation, fake news or false stories, unless other conditions are met. For example, where the misinformation is considered to be defamatory to an individual. Defamation becomes libel where it involves a written record, so would include comments in emails or on websites. By contrast comments made in a chat room or on a bulletin board/forum are regarded as slanderous, since these resemble casual conversation. Defamation as a criminal offence in the UK was abolished under the Coroners and Justice Act 2009 and is now a civil action only. Conditions of proof extend beyond the statement merely being false or involving misinformation and can be difficult to establish. For libel, the claimant must be able to show that this was misinformation which caused 'serious harm' to them for example by exposing them to ridicule or hatred. Proving slander requires proving that the defamatory misinformation have had an adverse effect upon their reputation, very often in terms of financial damage or lost business.

Where a case is proven, damages determined by the court can be awarded and websites or other online sites be ordered to take down the misinformation and to stop any further distribution, sale or exhibition of this.

Posting misinformation over a public electronic communications network can also be an offence under the Communications Act 2003 if this is grossly offensive or of an indecent, obscene or menacing character. However if does not fit these categories then, again, it remains legal to post false information, such as 'fake news'.

By contrast, deception *can* be a criminal offence, though convictions have been most commonly associated with fraud i.e. "making a dishonest representation for your own advantage or to cause another a loss". Deceptions of this kind can involve perpetrators hiding their identities behind websites and email addresses, or making false claims or promises with the intention of for gaining illicit profit at the expense of a victim

Deceptions specifically associated with fraud and cyber-fraud are dealt with via *The Fraud Act* (2006). This requires there to also be an intention. Thus, the "act of setting up a false social networking accounts or aliases could amount to criminal offences under the Fraud Act 2006 if there was a financial gain,

The *Theft Acts* (1968 &1978), *Forgery and Counterfeiting Act* (1981), and *Proceeds of Crime Act* (2002) ('POCA') could be relevant here depending upon the nature of the offending

A recent review by the UK Law Commission has attempted to address some of the gaps in managing misinformation online. They found that existing provisions against misinformation or deception had failed to keep with developments in smartphone and social media usage and that key legislation such as the Malicious Communications Act 1988 and the Communications Act 2003 often under criminalise misleading or harmful communications. For example, whilst the Malicious Communications Act makes it illegal to post abusive or false messages in a public forum, no offence is committed if the message has no 'intended recipient'. The Commission also found that there can be a risk of overcriminalisation (criminalising innocent but silly behaviour, such as belligerent posts on satirical sites lije 'Finstagram' (aka fake Instagram, or 'Finsta')

As a result of the Law Commission's recommendations following the review, the new Online Safety Bill has been created. The Bill, which is still to be fully ratified, expands the legal powers against deception, by focusing more directly on situations where deception or providing false information results in harm, rather than financial loss alone. A new offence created in the Bill centres upon disinformation or false communications which are deliberately circulated to inflict harm - for example a hoax bomb threat.

However, it does *not* criminalise misinformation where people are unaware what they are sending is false or genuinely believe it to be true. For example, if an individual posted on social media encouraging people to inject antiseptic to cure themselves of coronavirus, a court would have to prove that the individual knew this was not true before posting it.

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:

Concepts of human trafficking under UK Law conform with The UN Protocol to Prevent, Suppress and Punish Trafficking in Persons ('Palermo Protocol') which provided (in Article 3) the first internationally recognised definition of human trafficking – specifically "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control of another person, for the purpose of exploitation".

The key UK legal tool for regulating trafficking is the *Modern Slavery Act* (2015) which consolidates existing offences of human trafficking and slavery and encompasses trafficking for all forms of exploitation including sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or removal of organs.". The Act applies only offences which have been committed after 31/07/2015. Offences under this act can carry a maximum sentence of life imprisonment, though punishment will more usually fall between a high level community order to 18 years custody

However, the Act does *not* specifically address trafficking facilitated by the internet or other digital networks, nor is there any specific offence in UK law of this kind. The most relevant aspect of the law to trafficking using online means is seen in Section 2 of the act which makes it an offence to arrange or facilitate the travel of another person with a view to 'exploitation'. Exploitation, defined in section 3 of the Act, is taken to mean "slavery, servitude and forced or compulsory labour" This is also defined to include sexual exploitation, so could in theory be extended to cases where grooming is used to entice a victim to travel for sexual purposes. In practice however, cases where both grooming and trafficking offences occur tend to result in two *distinct* sets of charges under the relevant legislation. Thus if, as with the 'lover boy' example, someone sets out to *arrange* or *facilitate* a meeting with any child under the age of 16 for the purpose of sexual abuse, they will have committed an offence (irrespective of the trafficking component) and be charged accordingly under the Sexual Offences Act. If trafficking then occurs as a result of this then they will be charged under the Modern Slavery Act. It is not common to find both offences combined.

An example of this was seen in the case of Mubarak Ali who was convicted, with his brother Adhel of trafficking offences in 2012. They groomed girls as young as 13 with offers of money, free car journeys and presents before taking them to a restaurant for sex. The girls were then trafficked to wider circle of up to 200 men around the UK. However, in addition to two offences of trafficking in the UK for the purpose of prostitution, involving two of the victims. Ali was not charged with the grooming related offences specified in section 14 of the sexual offences. Act. Rather he faced four charges of controlling

child prostitution and causing child prostitution (specified in Sections 47 – 50) and was sentenced to 22 years; 14 years immediate custody and eight years on licence for seven related offences.

Another recent example where the Modern Slavery Act was preferred over other legal tools was seen in the case of three individuals accused of operating as one of the UK's largest trafficking gangs. The three were charged with conspiracy to traffic an estimated 400 victims to the UK and coercing them to engage in compulsory labour. One of the gang, David Handy, was charged with the section 2 offence of conspiracy to facilitate transportation to the UK for exploitation was jailed for seven years. However, there was no specification of whether facilitation occurred by digital means or any charge of grooming. The other leading gang member, Mateusz Natkowski was found guilty of three charges, including conspiracy to require another to perform forced or compulsory labour and conspiracy to control another for the purposes of labour exploitation and was jailed for four years and six months. A third member, Lukasz Wywrinski had pleaded guilty to six offences at an earlier hearing and received a four-year and three month prison sentence.

Evidence for the extent of trafficking by electronic means in the UK is limited but some recent studies have suggested that the role of ICT is mainly in relation to recruiting victims, especially through online job advertisements. Such advertisements are not only published on classified job websites such as Backpage.com., but also posted and circulated on specialised job search ads across social media. Escort agency websites and ads provide other indicators.

It has been suggested that around half of trafficking in UK is related to sexual exploitation, with especially high numbers of victims from India and the Philippines. Digital tools, especially social media and online classified advertising websites appear to be important components of this trade, though proving this is difficult. However research has indicated that variables such as references to ethnicity or nationality' within advertisements can be used as a virtual sex trafficking indicators.

Indeed, prosecutions have often been related to websites or digital tools of this kind. For example in 2022 an organised crime group who were using an online escort site called the 'Golden Kiss' were charged under the Modern Slavery with offences relating to the trafficking of Polish women into UK brothels. Sebastian and Anna Zimoch, the husband and wife team who ran the ring were convicted of conspiracy to arrange or facilitate travel of another person with a view of exploitation and conspiracy to control prostitution for gain. Sebastian Zimoch was sentenced to 8 years imprisonment though his wife was given a two year suspended sentence, ordered to undertake 150 hours unpaid work and attend 30 days' rehabilitation requirement.

Another case of escort websites being used as a tool for trafficking was seen in 2021 with Cristian Simion and Mihaela Borcos. The couple recruited women from Romania who could not speak English and could not find any legal work in the UK and would upload their profiles onto adult websites and then move them around the country to carry out sex work. Simion Borcos was found guilty of one count of human trafficking and two counts of money laundering and was jailed for two years and five months. Mihaela Borcos was found guilty of one count of human trafficking and one count of money laundering, was jailed for two years and two months.

Questions regarding cybercrime or cyber-facilitated crime committed by minors

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:

In England and Wales the age of criminal responsibility is the age at which a child or young person can be charged and prosecuted for a criminal offence is 10 years. Children under 10 cannot be charged with committing a criminal offence. However, if necessary, they can be given:

Local Child Curfews The police can use this to ban children from being in a public place between 9pm and 6am, unless accompanied by an adult. The curfew can last for up to 90 days.

Child Safety Orders. Where a child breaks their curfew, they can be given a Child Safety Order which means they can be placed under the supervision of a youth offending team. These orders can last for between 3 - 12 months. Where a child doesn't conform with the rules of an order, a court can make a decision on whether the child should be taken into care.[1]

Between the age of 10 -18 minors *can* be arrested if they commit a crime by violating a law. As a result, they can then be taken to a court. However, they are treated differently from adult offenders in at least 3 ways:

- Their cases are dealt with by youth courts
- They are given different sentences
- Where convicted, they are not sent to adult prisons, but to special secure centres for young people

Young people between 18-25 **are** treated as adults in the eyes of the law, however there are still some differences in treatment from older offenders. For example, instead of being sent to prison, they are sent to a place that holds 18 to 25-year-olds, not a full adult prison'

Where anyone between 10-17 is arrested the custody officer is required (under the Police and Criminal Evidence Act 1984) to find out the identity of their parent, guardian, Local Authority carer or any other individual with responsibility for the juvenile's welfare and then inform them of the arrest.[2] Without an appropriate adult being present, the young person cannot be interviewed, sign a written statement under caution, or sign any record of an interview.

Following any interview, they can be issued with a reprimand or a final warning, but if formally charged a first appearance in the Youth Court is scheduled. Exceptions here include:

- Where the juvenile is jointly charged with an adult;
- Where the juvenile is charged with aiding and abetting an adult (or vice versa);
- Where the juvenile is charged with an offence arising from the same circumstances as those in which an adult is accused of committing an offence

The Youth Court is a type of magistrates' court specialised in offences by 10-17 years olds. Cases are handled by three magistrates or a single district judge. Offences that can be dealt with here include theft and burglary, anti-social behaviour and drugs offences. More serious offences are usually transferred to Crown Court but can be dealt with in Youth court"[3]

There are a number of key differences in the way proceedings are conducted in the youth court from the way that they are in an adult court. Most obviously the proceedings are less formal, with defendants addressed by their first name. The public cannot attend the court and if the victim wants to observe what takes place they have to specially request this with the court. If the accused are 16 or under, their parents, guardians or carers must attend court.

Where the case is more serious and comes to Crown Court, defendants can put more at ease by the prosecuting and defending counsel and the judge, removing their wigs and robes

[1] https://www.gov.uk/child-under-10-breaks-law
[2] https://en.wikipedia.org/wiki/Youth_justice_in_England_and_Wales
[3] https://www.cps.gov.uk/crime-info/youth-crime

There are a variety of sentences which UK Youth Courts can impose upon young offenders. These include:

Absolute discharge – the court decides not to impose a sanction because the experience of going to court has been punishment enough.

Discharge - These are the same as for adult offenders. They are given for the least serious offences and mean that the child or young person is released from court without any further action. They will, however, still get a criminal record.

Conditional discharge – if the child or young person commits another crime, they can be sentenced for the first offence as well as the new one

Fines - As with adults, the fine should reflect the offence committed and the child or young person's ability to pay. Where the child or young person is under 16 the parent/guardian is required to pay the fine and so it will be their ability to pay that is taken into account when setting the level of the fine

Referral orders- A referral order requires the child or young person to attend a youth offender panel (made up of two members of the local community and an advisor from a youth offending team) and agree a contract, containing commitments, which will last between three months and a year. The aim is for the child or young person to make up for the harm they have caused and do something about their offending behaviour. An order *must* be imposed for a first offence where the child or young person has pleaded guilty (unless the court decides that another sentence is justified) and may be imposed in other circumstances.

Youth Rehabilitation Order This is a community sentence which can include one or more requirements that the offender must comply with, and can last for up to three years. Some examples of the requirements that can be imposed are a curfew, supervision, unpaid work, electronic monitoring, drug treatment, mental health treatment and education requirements.

Custodial sentences -Children and young people *can* receive custodial sentences but they will be imposed only in the most serious cases. When they are given, they aim to provide training and education and rehabilitate the offender so they do not reoffend. Sentences can be spent in secure children's homes, secure training centres and young offender institutions. If a child or young person between 12 and 17 years old is sentenced in the youth court, they could be given a *Detention and Training Order*. This can last between four months and two years.

Detention and Training Orders These can also be given in the Crown Court. For more serious cases, **longer-term detention** can be imposed where the offence committed carries a maximum sentence of at least 14 years' imprisonment or is one of the offences

A sentence of **detention for life** or an **extended sentence of detention** may be imposed if a child or young person is convicted of a specified offence and the Crown Court considers that there is a significant risk of serious harm to members of the public from them committing further specified offences.

Detention during Her Majesty's Pleasure is a mandatory life sentence and will be imposed when a child or young person is convicted or pleads guilty to murder. Schedule 21 of the Sentencing Code states that the starting point for determining the minimum sentence where the offender is under 18 years of age is 12 years as opposed to 15 years for those over the age of 18.

Under 18 year olds can get a person under 15 with a detention and training order only if it is of the opinion he is a persistent offender.[38] In respect of other summary-only offences, the term of an order may be 4 or 6 months.[39] In respect of indictable offences, the term of such an order may be 4, 6, 8, 10,

12, 18 or 24 months.[40] In either case, the term must not exceed the maximum time that an adult could be imprisoned for the same offence

Young offenders institutions. A person aged 18–21 may be sentenced to detention in a young offender institution, for a term of between 21 days and the maximum prison term applicable to an adult convicted of the same offence.

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:

The UK has no special measures in place for cyber related offences beyond existing laws on the statute book and the standard judicial procedures for young offenders detailed above.

However, the UK National Crime Agency (NCA) has suggested that the average age of UK cybercrime suspects is now 17 and, as detailed below, young people are routinely charged with digital-based offences.

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:

Yes, minors can be prosecuted for activities which can be defined as grooming especially where there is subsequent sexual activity. Even if the alleged perpetrator is under ten, the starting principle of reporting to the police remains, though police will take a welfare, rather than a criminal justice, approach.

UK Sentencing guidelines currently allow for **six** sexual offences committed by offenders under the age of 18. These offences are:

- Sexual activity with a child, (Sexual Offences Act 2003: section 13)
- Causing or inciting a child to engage in sexual activity, (Sexual Offences Act 2003; section 13)
- Sexual activity with a child family member (Sexual Offences Act 2003 – section 2)
- Inciting a child family member to engage in sexual activity, (Sexual Offences Act 2003 section 26
- Engaging in sexual activity in the presence of a child, (Sexual Offences Act 2003 – section 13 (section 11 for adult offenders);
- Causing a child to watch a sexual act, (Sexual Offences Act 2003 – section 13 (section 12 for adult offenders).

All of these offences have a lower statutory maximum sentence of 5 years' imprisonment but, in all other respects, are equivalent to the adult offences discussed.

There is certainly evidence that young people in the UK, as elsewhere, use online resources like social media to engage in grooming and sexual exploitation of other young people. For example, a report by the UK Barnardo's Children's trust suggests that exploitation among peers now accounts for up to a quarter of their services. Elsewhere, reports by front line services and others involved in working with children have indicated this is more common than might be imagined. One study from 2014 (Hackett, 2014) suggested that between one-fifth and two-thirds of sexual abuse is now committed by other children.

In the UK this problem is often referred to as 'peer on peer abuse' - a term which not only includes peer-on-peer grooming, but other categories which are covered in answers to the questions below. For example, coercion and exploitation, the distribution of sexualised content, sexting and harassment.

Detailed evidence for this remains limited but have been certain recurring patterns. One example where young girls act as 'groomers' by drawing other vulnerable minors into potentially abusive situations. Another is where young people recruit others into gang related activity by promises of money, drugs or other 'gifts' Other cases can involve minors who are influenced by adults to engage in grooming related offences.

For example, in 2014 a 16 year old boy was arrested in a child sex grooming investigation relating to two girls, aged 13 and 15 in Oldham and Rochdale along with six men. The boy was charged with conspiracy to engage in sexual activity whilst the adults were charge variously with child abduction, arranging or facilitating commission of a child sex offence. sexual activity with a girl aged 13 to 15 and sexual activity with a girl aged 13 to 15. The men had befriended the boy in Rochdale town centre and he then introduced them to the girls who were given alcohol and drugs over a period of nearly a month. One man was sentenced to seven years in prison and made subject to a Sexual Offences Prevention Order. Another who helped facilitate the child sex offence sentenced to two years in prison. The boy (who could not be named) was not sentenced because of undue influence from the adults.

However, peer on peer grooming is not always about exclusively about sex. Young people can be groomed to engaged in criminal activities such as transporting drugs or acting as a money mule. Very often, though gifts are promised at first, blackmail or violence can be usde to ensure they do what the perpetrator(s) want. Sometimes it can be purely about gaining or maintaining status.

A particularly tragic example of peer to peer grooming where status, as well as sex was a factor was the case of teenager Lewis Daynes who, in 2014 befriended 14 year Breck Bednar in an internet gaming group called TeamSpeak where Daynes was a prominent figure. Daynes played games like Call of Duty and Battlefield and Daynes gradually gained a hold over Bednar by claiming that he worked for the US government. He enticed Bednar into visiting his home by offering him a job in his fictional computer business where he could make 'a lot of money'. Daynes sexually assaulted the victim before murdering him and was sentenced to a minimum of 25 years. Daynes denied four other charges of rape, attempted rape and two of engaging a person in sexual activity without consent of another victim who was aged 15 at the time of the incidents between April and July 2011 when Daynes was under 18. These charges were dropped in the face of the murder charges though it was not clear why and parents made subsequent complaints against the police.

Where a case of possible peer to peer grooming has occurred, responses will depend upon the context. If, as is often the case, it occurs insider] a school, the school will normally implement standard school procedures (which can vary across institutions) and work with parents. If a report is made to the police, this will generally be made in conjunction with a referral to social services. Where a report of rape, assault by penetration or sexual assault is made, the starting point will be always be contact with the police. Even where the perpetrator is below the age of criminal responsibility at ten, the principle of reporting to the police remains, though they will take a welfare, rather than a criminal justice, approach.

The UK Sentencing Council has defined 3 categories of harm in this context:

Category 1	Penetration of vagina or anus (using body or object) Penile penetration of mouth. In either case by, or of, the victim
Category 2	Masturbation by, or of, the victim
Category 3	Other sexual activity

In turn, and with special reference to grooming type behaviours, the level of culpability of the minor (and hence their sentence) is determined by whether "activity is exploitative, coercive or bullying and whether peer pressure has been used to gain acquiescence to the sexual activity."

Culpability A: this higher level of culpability on the part of the minor is considered to apply where there are factors indicating that the minor has manipulated or coerced their victim in some way. These factors involve:

CULPABILITY A
Use of gifts/bribes to coerce the victim
Use of threat (including blackmail)
Use of alcohol/drugs on victim to facilitate the offence
Abuse of position of trust
Vulnerable child targeted
Offence racially or religiously aggravated
Offence motivated by hostility towards the victim's presumed or actual sexual orientation
Offence motivated by hostility towards the victim's presumed or actual disabilities

Culpabilty B does not have any such additional factors since merely exposing a child to sexual imagery/activity is considered to be inherently corrupting or abusive on its own.

Sentencing will result in custodial or non custodial outcomes, depending upon the level of culpability exhibited. These are as follows:[4]

	Culpability A	Culpability B
Category 1	Starting point: 8 months' detention and training order	Starting point 4 months' detention and training order
	Category range Youth rehabilitation order: 12 months' detention and training order	Category range Youth rehabilitation order: 12 months' detention and training order
Category 2	Starting point Youth rehabilitation order	Starting point Youth rehabilitation order
	Category range Youth rehabilitation order – 4 months' detention and training order	Category range Youth rehabilitation order
Category 3	Starting point Youth rehabilitation order	Starting point Youth rehabilitation order
	Category range Youth rehabilitation order	Category range Youth rehabilitation order

[4] https://consult.justice.gov.uk/sentencing-council/child-sex-offences-young-offenders/supporting_documents/sexual%20offences%20consultation_Offences%20committed%20by%20offenders%20under%20the%20age%20of%2018.pdf

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:

There are certainly situations under UK Law where minors can be punished for online behaviour with sexual intent. Perhaps the most familiar and common set of circumstances here revolve around where a minor obtains sexual images or other materials from a victims and uses these in ways for which permission has not been granted or which involve some degree of coercion

For example - section 33 of the *Criminal Justice and Courts Act* now makes it a specific criminal offence:

> '... for a person to disclose a private sexual photograph or film if the disclosure is made without the consent of an individual who appears in the photograph or film; with the intention of causing that individual distress'

However, images which have been altered in some way are not usually counted:

> 'The photograph or film is not private and sexual if ... it is only by virtue of the alteration or combination mentioned in subsection (4) that the person mentioned in section 33(1)(a) and (b) is shown as part of or with, whatever makes the photograph or film private and sexual

Where minors are involved in this kind of an offence, there has been an increasing reluctance to prosecute. As a result of this more considered approach UK police can now record a so-called "Outcome 21" against a reported crime, meaning it is not in the public interest to pursue a charge. The majority of youth involved sexual imagery (such as sexting) would fall into this category. Police action leading to a criminal charge does however remain valid where there is any evidence of coercion, exploitation, further harm or aggravated behaviours.

The situation is evolving, but at present, the Interim Code of Practice on Online CSEA is as follows

- children may produce images that do not meet the definition of an 'indecent image' so are not illegal but could be harmful to the child because of the risk of wider circulation or the image being picked up by an offender. When requested by the child in the image, steps should be taken to remove and prevent future circulation of these images
- where material is not illegal, reporting to authorities is not required but associated illegal CSEA activity should be reported.
- Where information is available that might differentiate between consensual self-produced indecent imagery and grooming, this should be included in any report to assist law enforcement.
- However, because children are often unsure about the boundaries of the law here, various child-centred initiatives have been created to ensure that they are properly protect and nor criminalised unnecessarily. A typical example of this is the "Report Remove" portsl developed by the IWF, in partnership with the NSPCC's Childline. This permits children to "anonymously report sexual imagery of themselves which they are concerned may be subject to wider distribution to

the IWF. Imagery assessed as illegal is hashed and shared with tech companies, while the NSPCC via Childline supports the child.".[5]

One extreme case of this occurred in May 2020 when a 17-year-old boy pleaded guilty to six counts of taking indecent photographs of a child, three counts of making indecent photographs of children and one count of possession of prohibited images of children, which related to a number of indecent images found on his electronic devices. However these offences involving sexual images were aggravated by more serious crimes against the two minors (a female child under the age of two and an 11-year-old girl) with the defendant also pleading guilty to three counts of sexually assaulting a child under 13, one count of raping a child under 13, one count of assaulting a child under 13 by penetration. The youth was sentenced to eight years and five months and was directed to commence his sentence in a Young Offenders' Institution before being moved to a prison to serve the remainder, after he turns 18.

Question 9: Can minors be punished for cyberbullying behaviour, without there being a physical component to the crime? This includes behaviours such as cyberstalking and cyberharassment. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

As noted above, bullying is not a criminal offence in the UK and most bullying incidents are not treated as crimes. For minors, as with adults, a threshold is crossed where bullying involves violence or assault; theft; harassment and intimidation over a period of time including calling someone names or threatening them, making abusive phone calls, and sending abusive emails or text messages (one incident is not normally enough to get a conviction); and anything involving hate crimes. Only at this point – and still relatively rarely, the behaviour could be reported to the police

As above, the key legal tools here include the Malicious Communications Act 1988 and the Protection from Harassment Act 1997. Whilst prosecution remains rare in the UK, there have been a few instances where cases have bee directed to the courts

In addition, for minors The Education and Inspections Act (2006) is also relevant. This act provides for staff and teachers to confiscate items from pupils who may be involved in bullying, such as mobile phones. Under this legislation "All UK schools are now required to have an anti-bullying policy either under the School Standards and Framework Act 1998 or the Education (Independent Schools Standards) Regulations 2003."

Though prosecutions of minors for these offences are rare, they have occurred. The first UK case of a minor being given a custodial sentence came in 2009, when a teenage girl was jailed for cyberbullying. The girl was 18 when sentenced but had conducted a campaign of abuse against her victim for nearly four years, one which culminated in her posting a series of death threats on Facebook. As a result she was sentenced under the *Protection From Harassment Act* to 3 months in a young offenders institution. This unprecedented sentence was a direct result of previous convictions against the perpetrator, one for assault when the victim was walking home, another for criminal damage when she kicked the victim's front door.

The difficulties and ambiguities in securing cyberbullying related convictions for minor was seen in another case where a 16 year girl was arrested at school, in the middle of a lesson. Police also raided her home and confiscated her laptop and tablet. She had been accused by another girl who said she was targeting her online, making threats to 'get her' and hacking into her family's webcam. These allegations

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944034/1704__HO__INTERIM_CODE_OF_PRACTICE_CSEA_v.2.1_14-12-2020.pdf

turned out to be untrue and police were forced to issue an apology for their heavy0handed (and mistaken) attempt to enforce harassment laws.

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:

As indicated above, under UK Law there are no specific offences related to deception, circulating misinformation or false news online, unless it is attached to other offences like defamation or fraud. Minors cannot therefore be prosecuted for spreading fake news, pretending to be someone else and so on without this other conditions being in place.

The most common offence of this kind for which minors have been prosecuted is deception when attached to the pursuit of financial gain, which falls under the Fraud Act (2006).

For example a schoolboy from Lincolnshire was recently convicted for creating a fake website , but was prosecuted for false representation under the Fraud Act, along with money laundering charges because the sites were to harvest personal details of dozens of victims. The site, created in the boy's bedroom was almost indistinguishable from the official Love2Shop site, an online business which sells gift vouchers. He had managed collect over 12,000 credit card numbers which were stored on his computer and he had opened 197 PayPal accounts. His scam was enhanced by paying for Google advertising which meant his fake site was actually listed above the genuine site when individual conducted web searched for the Love2Shop. By using the data he had gathered he managed to convert £6,500 worth of vouchers to his own Love2Shop account. This resulted over £323,000 that was received through his PayPal accounts. This sum was then transferred into cryptocurrency, helping him to amass a fortune of over £2 million. The boy was still only 17 when convicted and so was given a 12-month youth rehabilitation order to include a supervision requirement and 150 hours of unpaid work. The judge also ruled that £2m should be confiscated from his assets. She commented that if he had been an adult then he would have been ordered to serve a 'substantial' prison sentence.

Similarly, in late 2020 a 17 year old from South London was arrested as a result of creating fake websites. He was charged under the Fraud Act with fraud by false representation because the sites were claiming to offer tax refunds, but were in fact aimed at gathering users bank details. The case is awaiting trial in the Youth Court

The age of the defendant can make a significant difference in subsequent prosecutions for deceptions involving fraud. For example, a 16 year old schoolboy in Wolverhampton was found to have used false advertising to fool victims into paying for car insurance policies which didn't exist, making over £4,000 from the scam. Because the case wasn't brought before the court until he was 19 he could be named as Azeem Mahmood Hussain, 19, and he was finally sentenced to 12 months youth custody for four frauds. However, the verdict was challenged at the Court of Appeal and the three senior judges who presiding said that his young age at the time was not taken into account. They also judged that Hussain had since obtained qualifications and a job and wanted to go on to higher education. As a result, his sentence was cut to eight months

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:

Minors can be punished for actions which facilitate online trafficking, with the usual qualifications in term of the criminal justice process for under 18s which have been noted above.

In practice however this is very rare and there few examples which have come before the Youth Courts. One example is the case of Eva Dambrauskaite who became affiliated with a gang which recruited trained and transported teenage girls around the UK in order to engage in refund frauds in High Street stores. The gang placed fake barcodes on items to pay a much cheaper price, before later asking for refunds using fake receipts at the full price. In 2022 Dambrauskaite was charged under the Modern Slavery Act with the trafficking offence "conspiracy to arrange or facilitate travel or another person with a view to exploitation" committed in 2018 (when she was below the age of 18). She was also charged with 2 counts of conspiracy to commit fraud by false representation and possession of articles for use in frauds on and transferring criminal property. She is currently awaiting sentencing

Question 12: Can minors be punished for acts of online piracy in your jurisdiction, i.e. the illegal use and/or distribution of content protected by intellectual property rights? Please focus on the elements of criminal nature. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Online piracy such as the illegal use ad distribution of copyrighted content is covered under UK law by the *Copyright, Designs and Patents Act - CDPA* (1988).

Most young people follow the example of adults by conducting this via peer-to-peer sharing or torrenting – which usually means streaming movies online. This involves downloading and uploading a file via the BitTorrent network. Generally, using torrenting technology isn't illegal in the UK. However if the file is copyrighted, UK law makes it illegal to upload or download this without permission from the person who owns the rights. Thus, file sharing services can, in theory, be used legally, but, in practice, nearly all the content on them is illegal. The only safe way to use them legally is to be sure that shared materials are not protected by someone else's copyright, although most material is copyrighted.

Where there is an infringement, this is usually treated as civil offence though it can, in certain circumstances, also be deemed a criminal offence, with damages awarded by a court. Depending on the severity of the infringement, the result can be a fine or even imprisonment.

If the re-use results in financial loss for the content creator – such as lost income from licensing the work – an offender may also face claims for compensation. However, a compromise can be reached before any action reaches the courts. For example, the offender can pay an author retrospective fee for the use of their work and give them credit on the work.

However, the regulation of digital piracy in the UK has been very uneven and it is extremely unusual for minors to be prosecuted for offences here. Government ministers have made it clear that they "do not want to see teenagers prosecuted for file sharing in their bedrooms" and even cases against adults have been relatively limited.

An example of the inconsistencies in approach here can be seen in the case of the Bit Torrent tracking site OiNK's Pink Palace. In 2010, Alan Ellis, the founder of the site became the first person in the UK to be prosecuted for illegal file sharing. Ellis was in his early 20s when he started the site so was not technically a minor. However, the case is worth noting because he was found not guilty – partly as a result of the prosecution's decision to pursue him for fraud rather than copyright infringement, partly because he was able to claim that OiNK was only a 'search engine, and so did not physically host illegal material, rather it merely connected existing users' shared files.

The music industry's determination to pursue charges against users of the site, irrespective of their age was seen in the case of 17 year old Matthew Wyatt who shared files on OiNK. In 2007 Wyatt's home was raided by police, Trading Standards officers, members of the International Federation of the Phonographic Industry (IFPI) and the British Phonographic Industry (BPI) and he was charged with illegal downloading. In fact the youth had only shared three albums and one single. Wyatts solicitor argued that he was a "victim of a cynical attempt by the record industry to legitimise its heavy-handed tactics and dubious methods by using police resources and the public purse" and prosecutors eventually dropped the case against Wyatt, saying that it wasn't in the public interest to pursue the case.

However in 2011 the BPI were successful in pursuing a case against a young adult called Kane Robinson who was arrested for running the download site Dancing Jesus. Robinson was a minor when he had originally begun to engage in file sharing but was 22 when arrested. When the case eventually came to court in 2015, he was given a prison sentence of over two years - the longest ever sentence for music piracy in the UK.

The legal frameworks around digital piracy were tightened up in 2017 with Digital Economy Act which imposed obligations on Internet Service Providers(ISPs) to take measures against subscribers with excessive copyright infringement reports made against them. These measures include slowing down their internet connection speed or suspending their service altogether. The Act also set out an amendment to the CDPA permitting harsher sentences against downloaders. There is now in possibility of a fine up to £50,000 and a jail term of up to six months. Where the case reaches a Crown Court, fines can be unlimited and the maximum sentence up to ten years' imprisonment.

This enhanced legislation has created new uncertainties. Whilst prosecution of minors remains minimal, it has permitted the emergence of 'copyright trolls' – companies which observe file-sharing networks in order to gather the IP addresses of individuals who (they claim) are sharing content like movies. They then compel ISPs to hand over the identities of those related to the IP addresses and begin to send letters threatening civil action unless a financial settlement is made. In 2022 Virgin Media customers began to receive letters from one such company, Voltage Holdings who were threatening action against those who had downloaded the film 'Ava'. The letter threatens the holder of the ISP account, which is in effect a household and so could implicate minors responsible for the download. However, no data is yet available on who was involved in this action and it remains extremely unlikely that police will intervene to take criminal action.

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:

Minors in the UK can be and routinely are charged with hacking offences. A significant number have also been prosecuted and convicted. The prevailing attitude in the UK, as elsewhere is that minors have a disproportionate role in hacking and therefore need to be tackled with the full force of the law. For example, the National Crime Agency have suggested that 61% of computer hackers identified in UK begin their activity before the age of 16**.**

The main legal tool used against hackers (whether above or below the age of 18) is the *Computer Misuse Act* (1990) which contains three key sections defining computer related offences

Section 1 effectively criminalises hacking by making it offence to obtain 'unauthorised access to computer material'. There is a maximum penalty of two years imprisonment available to the courts for such actions

Section 2 extends the remit against hacking by making it an offence to obtain unauthorised access (to a computer/digital network) with intent to commit or facilitate commission of further offences. For example, access obtained in order to transfer funds from one account to another It is not necessary to prove that any intended further offence has actually been committed. The maximum penalty for this is five years imprisonment

Section 3 contains the most stringent provisions and is directed at ways in which hackers can disrupt or damage computer functionality. This makes it an offence to commit unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computer. This covers acts such as inserting malware or spyware, modifying or deleting data and suspending operations via a DDos attack. Where found guilty, a more substantial sentence of 10 years imprisonment can be imposed.

Any charge under section 2 or 3 automatically also includes a charge under section 1.

Alternative legal tools here include the *Fraud Act* (2006) which can be used against those involved in pharming (cloning false websites for fraud) or the installation of trojan malware, again for the purpose of fraud. The *Investigatory Powers Act* (2016) can also be directed against hackers who have been involved in unauthorised interception of a public or private telecommunication systems.

There have been a number of examples of cases brought against minors under the CMA legislation. For example in 2016, Kane Gamble - a 16 year old boy associated with the 'Crackas with Attitude' hacking gang - was arrested for hacking into the email account of John Brennan, the Director of the CIA. Gamble was able to release over 40 sensitive documents into the public domain as well as resetting the Directors AOL email account. He was given a two year prison sentence of which he spent 8 months in the high security Belmarsh prison with a one year probation with no internet access.

A lesser sentence under the Computer Misuse Act was imposed upon Jack Chappell who was 16 when he engaged in a series of DDos attacks on leading multinational corporations like Netflix, Amazon, BBC, Vodafone, Nat West and even the UK National Crime Agency. Chappell, who worked in conjunction with a digital crime group called VDos was responsible for launching over 2,000 attacks. Though he was 19 when the case came to court, the sentencing judge decided that Chappell has had been taken advantage of by the gang and that imposing a custodial sentence would be make him extremely vulnerable. As a result he was sentenced only to 16 months in a young offenders institution, suspended for two years.

Also in 2016, Conor Allsop - who was 17 at the time - admitted to involvement in a DDos based cyber-attack on the TalkTalk website and the leaking of customer details. TalkTalk lost over £70 million and had a £400,000 fine imposed as a result of the huge data breach. Though Allsop was one of 10 individuals believed to have been involved in the attack and it was accepted that he did not expose the vulnerability which led to the attack he was sentence to 8 months imprisonment under the CMA as he was over 18 when the case was eventually heard.[6]

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:

[6] https://www.ispreview.co.uk/index.php/2016/11/talktalk-hack-boy-admits-7-charges-computer-misuse-act.html

Making, adapting, supplying or offering to supply any article which can be used to commit a cyberdependent related offence is an offence under Section 3a of the Computer Misuse Act (1990). The maximum sentence for this is 2 years imprisonment.

This clause in the CMA specifically targets the market in 'hacker tools'; commonly used for breaking into, or compromising, computer systems. It thus covers many activities related o the use of CaaS such as using it to acquire malware, hiring botnets, adapting ransomware or similar

Providing software or devices which permits the exploitation of IoT or other connected devices for the purpose of fraud can also be an offence under the Fraud Act and can carry a sentence of up to 10 years Prosecution generally follows intention or demonstrable harm so where the minor is purely involves as a joke, it is unlikely that there would be consequences. Using the Fraud Act to secure a conviction in this context involve conditions for this are especially rigorous. The individual must be proved to have knowledge that the CaaS object can be used for fraud has been adapted it to that end or has explicit intentions to use it for that purpose.

Mere possession of these tools can also be grounds for prosecution – though again with the above conditions attached.

In general, prosecutions tend to occur more for using the tool than for merely obtaining it, though UK case law is still being established here. For example, in 2005 a minor was charged with obtaining a CaaS mail-bomber tool called Avalanche. He used this to overwhelm the mail server of the D&G insurance company with over 5 million e-mails called Domestic and General from which he had been fired. Hs defence was a technical one. It suggested that since every e-mail that is sent to an e-mail server is in fact "authorised" to modify it (otherwise e-mail wouldn't work) there is no specific point at which a large quantity of such e-mails suddenly become "unauthorised". The Court rejected this argument but felt that the Computer Misuse Act remained sufficiently ambiguous at that point for the prosecutions case not to be proved. They argued it was not up to them but to Parliament to properly extend this law.

By 2015, interpretation of the Computer Misuse Law ha=d tightened. Six teenagers, aged between 15 to 18 were arrested for accessing and using the CaaS tool called Lizard Stresser. They used this to attack a number of gaming sites such as Microsoft's Xbox Live and Sony's Playstation network. The youths were bailed and because of their age were not ultimately given a custodial sentence, but clear precedents had been set about the consequences of using CaaS tool, irrespective of age.

Minors who *create* or distribute tools used for CaaS are also routinely prosecuted. Adam Mudd, who created and sold the Titanium Stresser CaaS tool when he was 15 was charged with two offences under the Computer Misuse Act following his arrest in 2016. The tool was used in over 1.7m cyberattacks and Mudd was estimated to have made around £370,000 from its distribution. Though he was 20 when the case eventually came to court he was treated as a youth offender and sentenced to two years imprisonment in a youth offenders institution.

An interesting adjunct to these examples is where minors operate a cybercrime market themselves. In 2011 three UK teenagers who created Ghostmarket, one of the largest online crime forums and markets were arrested but were not charged under the Computer Misuse Act, even though the site provided hacking 'tools' in the form of tutorials and tips. Because Ghostmarket also sold details of credit card numbers resulting in estimated losses of over £16 million they were charged with offences under the Fraud Act. Two of the youths, Nicholas Webber and Ryan Thomas were under 18 when the site was first created, but were handed substantial custodial sentences – Webber received 5 years and Thomas 4 years

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:

The problem of policing and responding to cybercrimes committed in other jurisdictions is as challenging for the UK as it is for other countries. In the absence of a comprehensive, internationally binding jurisdictional framework for dealing with cybercrime, the UK, as elsewhere needs to look carefully at the circumstances around the offence. Where jurisdiction is ambiguous or is challenged, the key determinant for the courts is to look at where an offence is committed, where an site is hosted, its intended audience, what, if any material posted, the nationality of the webmaster and where the information was created and downloaded. The 'substantial measure' principle set out in *R v Smith (Wallace Duncan) (no.4)* (2004) 2 Cr App R 17, is then applied. This states:

"The English Courts ... seek ... to apply the English criminal law where a substantial measure of the activities constituting the crime take place in England and restricts its application in such circumstances solely to cases where it can be seriously be argued on a reasonable view that these activities should on the basis of international comity not be dealt with by another country."

One of the key legislative tools where jurisdictions can apply beyond the UK is the *Computer Misuse Act* (1990). Under this act the UK follows the principle of territoriality, but should an offence occur the United Kingdom, its courts may still have jurisdiction to try someone who has offended against this act. Under Section 4 and 5 it stipulates that if the offence is 'significantly linked' to the UK it does not matter whether it is committed outside of the territory of United Kingdom. This can include a foreign national committing an offence in the UK a target computer which is located in the UK, or a UK national committing an offence whilst outside the UK.

A second tool of this kind is the *Data Protection Act* (2018). This can apply to the processing of personal data which is in the UK by anyone such as processor or a controller who is outside of the UK, but which provides goods and services or monitors preferences or behaviours of someone in the UK. An offence will also occur if an individual in the UK illicitly processes that data of someone outside of the UK.

A third tool is the *Regulation of Investigatory Powers Act – RIPA* (2000), which permits the police and other relevant agencies to obtain communications data for the purpose of detecting crime. One rationale for RIPA was to give United Kingdom authorities a legal basis for requesting communications data from communications providers (CSP's) based overseas where they operate a service in the United Kingdom. However, it is the case that CSPs often refuse to acknowledge that RIPA has an extra-territorial application or will refuse to respond to RIPA requests. At other times CSPs may comply but emphasise that they are doing so on a voluntary basis. At that stage the only way in which United Kingdom law enforcement authorities can access the data is through the arrangements for an international MLA (mutual legal assistance) – see below. This may permit the judicial authorities in one state to request assistance from another stage to help in crime prevention, detection or prosecution.

Where a UK based data processor outsources data processing to a provider located outside the UK that processor will themselves be liable if they offer goods or services (even free of charge) to data subjects in the EU/UK or monitors their behaviour with the EU/UK. However the offshore processor is likely to become subject to the GDPR *indirectly* via contract as the data controller will need to impose certain contractual obligations on the data processor under Article 28 GDPR. In 2003, a new extradition treaty between the United Kingdom and Northern Ireland and the United States of America was signed. This

states that *any* crime that is punishable by a maximum sentence of or more in both the requesting and the requested state is subject to extradition.

A key example of some of these conditions was seen in *R v Sheppard and Whittle* (2010) EWCA Crim 65. Sheppard had posted racially hateful content on a website that was registered in his name and operated by him, but which was based in California. However once the material was loaded onto the server in California, it was posted online and so became available to anyone in the jurisdiction of England and Wales who visited the site, including people. The defendants received convictions for possessing, publishing and distributing racially inflammatory material contrary to the Public Order Act 1986. They appealed but the court ruled that jurisdiction was governed by the substantial measure principle enunciated by the court in *R v Smith*.

Extra national jurisdiction is also seen in cases relating to sexual offending. For example, Gary Shin who groomed two children in the UAE, both online and offline by offering gifts and holidays. Shin then sexually assaulted the children (aged 8 and 9) on several occasions and took indecent photographs of them. Upon his return to the UK he was charged with six counts of child sexual abuse under section 72 of the Sexual Offences Act, which allows British nationals to be prosecuted in the UK for abuse committed overseas and was sentenced to 10 years in prison, two years on licence and was made subject of a Sexual Harm Prevention Order.

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 UK has a a number of international agreements which may have relevance to the UK response to cross border cybercrime. These are summarised below, with additional reflections on any adjustments post Brexit.

A first and crucial requirement where jurisdictionality has been established, is to be able to extradite a cybercriminal. The UK follows the **1957 Convention on Extradition** on this and key requirements in this are implemented in the **2003 Extradition Act** , with different processes in relation to *Category 1* territories (comprising most EU nations, along with other nations like Sweden) and *Category 2* nations (comprising most other nations).

For extradition of a cybercriminal **from** the UK to Category 1 countries, the usual arrangements have been for a warrant to be submitted by the requesting state (usually electronically, via Interpol) and certificate can then be issued by the relevant UK authority (after a proportionality test is applied). This is followed by arrest, an initial hearing and then an extradition hearing The National Crime Agency (NCA) holds authority over category 1 cases, but must ensure that the requirements of section 2 of the 2003 Act are met (such as a proportionality test) before it can issue a certificate. Once this has been issued the cybercriminal who has been requested for extradition can be arrested and brought before a district judge at the magistrates' court. Provided the documentation is valid the identification of the suspect confirmed then a date for the extradition hearing can be set, should the suspect not agree to the extradition. This date must be within 21 days.

At this hearing, the judge whether the offending behaviour set out in the warrant constitutes an extradition offence - which will usually mean that it also amounts to a criminal offence in the UK. They will also decide whether any of the statutory bars to extradition apply. For example, whether the prosecution case against the accused is sufficiently advanced, how much time has elapsed since the request or whether it would be more appropriate for the requested person to be prosecuted in the UK instead. Age forms an important bar here, A minor will not generally be eligible for extradition, nor would any individual who, because of their age, could not be guilty of the offence

If none of these bars hold, the judge must then make a decision on whether extradition might infringe the requested person's human rights. If not, extradition must be ordered. An appeal against the decision if made within 7 days -first to the High Court with a right to a final appeal to the Supreme Court, though this usually only involves a point of law of general public importance. Extradition usually follows within 10 days of the final court order.

Following Brexit, the UK is no longer part of the European Arrest Warrant (EAW) framework,. However, a new agreement between the UK and the European Union (EU) came into effect on 1 January 2021 which allows for streamlined extradition warrant-based arrangements (similar to the EU's surrender agreement with Norway and Iceland).

Part 1 of the Extradition Act 2003 (the '2003 Act'), and the 2003 Act as amended by the Future Relationship Act, implements the EAW and the arrangements under Title VII (Surrender) of the UK-EU Trade and Co-operation Agreement

Extradition requests from Category 2 countries also require a decision by the Secretary of State. Only if they decide to grant the request can the case proceed to the courts. As before, a preliminary hearing is followed by a extradition hearing on the basis of which the Secretary of State decides whether to order extradition

Where the extradition judge has decided to send a case to the Secretary of State, this can be appealed within 14 days. However, the High Court will not hear the appeal unless and until the Secretary of State actually orders the requested person's extradition, The Secretary of State is legally obliged to order extradition unless this is barred by certain provisions in the 2003 Act. These include the requirement that the person will not face the death penalty.

Unless there is an appeal, a requested person must be extradited within 28 days of the Secretary of State's decision to order extradition. Where the UK has no extradition arrangement or treaty with a particular territory, that territory can make an exceptional extradition request to the UK. The Secretary of State then decides whether to enter into 'special extradition arrangements'.

Effective control of cybercrime may also necessitate the extradition of criminals from other countries to the UK. For EU states, where an extradition warrants has been issued under the mechanisms outlined within the EU-UK Trade and Cooperation Agreement then it is processed.

Extradition requests made to territories not covered by the 2003 Act can be made under the Royal Prerogative and the UK Home Office will forward and extradition requests prepared by the prosecuting authorities in England and Wales and Northern Ireland (e.g. CPS, Serious Fraud Office or Public Prosecution Service Northern Ireland) to the requested state through te diplomatic routes.

As a matter of policy, the UK seeks to extradite its own nationals, providing there are no bars to this which apply. Some countries are not permitted to extradite their own nationals, but usually have provisions in place that mean that although they will not extradite their own nationals, they may be prepared to prosecute them.

Other transnational treaties tools which can assist in fighting cybercrime include:

1959 **Convention on Mutual Assistance in Criminal Matters** (including the 1978 & 2001 additional) In line with UN requirements, such requests can extend to many crucial aspects of cybercrime investigation such as Executing searches and seizures, and freezing of asets, Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records; Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes (see below)

1990 **Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime**

2001 **Convention on Cybercrime ("the Budapest Convention")**

Following the UKs withdrawal from the European it does remain "a signatory to the Budapest Convention on Cyber crime, though it is no longer be a formal participant in the transnational cooperation mechanisms it recommends. Under Article 22 of section 3 in the Cybercrime Convention there are rules for the contracting parties to the treaty are obliged to establish jurisdiction over the criminal offense. Paragraph (a) is a restatement of the principle of territoriality which is a basic characteristic of criminal law. It states that the contracting parties shall adopt legislations necessary to punish the commission of crimes defined in the treaty that are committed within its territory.

Paragraph (b) and (c) are also based on the principle of territoriality. When the crime is committed on board a ship or an aircraft registered under the laws of the United Kingdom while passing through the territory of United States, is the United Kingdom deprived of its jurisdiction to prosecute the offense? Following paragraph (b) and (c) the treaty requires that contracting parties to establish jurisdiction over criminal offense committed inside its ship or aircraft registered under its name. As a matter of legal principle the crimes committed inside the ship or aircrafts of a particular nation even when they are outside its territory are still considered committed within its territory since they are considered as extensions of the territory of the state. Paragraph (d) on the other hand is a restatement of the principle of nationality as basis for conferring jurisdiction upon a state. It states that the nationals of a particular state are not immune from criminal liability of their own state even if they are outside its territory. They are still obliged to comply with their domestic law even when they are beyond the territory of their own state. For instance, a British man who goes to a country which does not have a law against hacking and while within the territory of the country uses a computer to hack through a computer of a person in the United Kingdom is still within the jurisdiction of his own state.

A seminal case indicating some of the challenges associated with extraditing cybercrime suspects was seen with Gary MacKinnon who hacked into 97 United States military and NASA computers from his home computer in 2001 & 2002. Investigation by the UK National Hi-Tech Crime Unit identified McKinnon as the culprit he was arrested under Computer Misuse Act. Though no charges were brought by UK against him. the United States requested his extradition under the new UK/US extradition treaty. McKinnon's legal team challenged this extradition on the ground that the location of the criminal act, the facilities and the computers were all in the United Kingdom. Their tactic was to highlight the UK's jurisdiction over the case – larhely because of its greater leniency towards those guilty of computer crime If McKinnon had been extradicted he could have faced many years in prison and in May 2006, the judge at Bow Street Magistrates' Court ruled that this should occur. This decision was backed by the Home Secretary who signed an order allowing McKinnon's extradition to the United States. The UK CPS found that there is insufficient evidence to prosecute McKinnon under Section 3 of the Computer Misuse Act since it was not established whether there was malicious intent on the part of McKinnon. In 2012, following a long campaign Theresa May, the then Home Secretary finally reversed the extradition decision on the grounds of Mackinnons diagnosis of Aspergers syndrome and the likelihood that such a decision would infringe his human rights

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 UK is party to a wide range of co-operations with international partners, both formal and informal which facilitate more effective responses to cybercrime. Amongst these can be included;

MLA: Mutual Legal Assistance - This is a method of cooperation between states for obtaining assistance in the investigation or prosecution of criminal offences. MLA is generally used for obtaining material that cannot be obtained on a police cooperation basis, particularly enquiries that require coercive means. Requests are made by a formal international Letter of Request (LOR), usually on the basis of a bilateral treaty or multilateral convention. In cases where the requirement of information may be for only traffic or communications data (rather than content), then an LOR is unlikely to be required; some information could be sought directly from the CSP.

JIT - Joint Investigation Teams: Complex cybercrime investigations often span several jurisdictions. Investigators and prosecutors need to be able to co-ordinate their approach and respond quickly to developments and opportunities to disrupt or prevent illegal activity, obtain evidence and make arrests. Consideration should be given as to whether a Joint Investigation Team ('JIT') is appropriate. A JIT is a team set up between two or more countries, under judicial supervision, for the purpose of investigating specific serious cross-border crime and with a limited duration. The legal basis of a JIT is under Article 13 of the EU Convention on Mutual Legal Assistance in Criminal Matters 2000, Article 20 of the Second Additional Protocol to Council of Europe Convention on Mutual Assistance in Criminal Matters 1959, the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988, UN Convention against Transnational Organised Crime 2000, or the UN Convention against Corruption 2003.

There are a number of advantages in considering a JIT for a complex case. For example, it allows JIT members to:

- share information directly / request investigative measures without the need for MLA;

    - be present at house searches, interviews, etc;
    - co-ordinate efforts on the spot;
    - informally exchange specialised knowledge;
    - build mutual trust between practitioners from different jurisdictions working together and deciding on investigative and prosecution strategies;
    - enable Eurojust and Europol to be involved with direct support and assistance.

Eurojust can assist when considering the creation of a JIT, or when dealing with jurisdictional and logistical issues where offending occurs in more than one country. It provides a neutral venue for meetings where prosecutors and investigators from two or more Member States can review such cases and agree future actions. Early consultation with the UK desk at Eurojust when dealing with transnational crime is recommended, particularly if the offending occurs in three or more EU Member States.

The aim of a JIT is to encourage and modernise co-operation between judicial and law enforcement agencies in EU Member States.

GPEN - The Global Prosecutors E-Crime Network. This was launched in 2008 with the aim of assisting countries to establish a safe and secure online environment, by ensuring prosecutors have the tools to deal effectively with cybercrime. Under the umbrella of the International Association of Prosecutors ('IAP') each organisational member nominates at least one prosecutor to be registered as the GPEN national contact point. The GPEN network provides a:

- database of nominated e-crime prosecutors from around the world;
- forum for the exchange of expertise, queries and advice;

- collection of e-crime prosecution resource material, for example; national legislation and legal guidance;
- virtual Global E-Crime Prosecutors' College, a database of e-crime training courses and presentations; and
- global community of e-crime prosecutors sharing expertise and experience.

GPEN was the initiative of the CPS and since its inception the CPS has promoted GPEN both nationally and internationally, has contributed training material to the GPEN library and has assisted in capacity building in a number of countries.

However the UK's changing relationship with Europe has inevitably impacted on wider forms of cybersecurity co-operation with Europe and its role in fighting cybercrime.

Part three of the Trade and Cooperation Agreement (TCA) now forms the basis of cooperation between the UK and the EU on law enforcement and judicial cooperation in criminal matters. This was agreed in December 2020 and was applied provisionally from 1 January 2021 but formally entered into force on 1 May 2021. The operation of the TCA is overseen by the Partnership Council and a number of specialised committees, including the Specialised Committee on Law Enforcement and Judicial Cooperation, which addresses matters covered by part three. Article 776 of the TCA itself provides for a joint review of the implementation of the agreement every five years. Article 691 allows for part three to be "jointly reviewed in accordance with article 776 or at the request of either party where jointly agreed". Under article 692, "each party may at any moment terminate this part by written notification through diplomatic channels". Should that happen part three would "cease to be in force on the first day of the ninth month following the date of notification".

A key issue to address is the loss of easy access to key EU policing and security databases, which is likely to pose new challenges in the fight against cybercrime. New challenges are also posd by the UK's withdrawal from the European Arrest Warrant noted above. Though this has replaced under the TCA by extradition arrangements "akin to the EU's Surrender Agreement with Norway and Iceland" the loss of the EAW poses some obvious challenges in cross border co-oeparation in fighting cybercrime. Part three of the TCA does allows the UK to maintain different levels of access to certain EU databases, for example DNA and fingerprint data can continue to be exchanged through the Prüm system subject to certain restrictions and preconditions. However, the UK has lost access to the Schengen Information System (SIS II) and no longer has a position in the EU Agency for Cyber security (ENISA). It has also lost its seat on the management board for Europol and with that the capacity to lead Europol cyber crime operations which it once had. The TCA does however enable UK liaison officers to be present in Europol's headquarters to facilitate cross-border cooperation. This also gives them access to EUROPOL's secure messaging system, the ability to attend and organise operational and other meetings at EUROPOL, the ability to contribute to EUROPOL analysis projects in order to benefit from the agency's coordination and analytical functions, and the fast and effective exchange of data.

A new Security of Information Agreement(SOIA) has also been formulated between the UK and Europe which will enable a continuing exchange of classified information vital for staying one step of cybercriminal actions. This permits certain forms of operational cooperation to persist, in particular re-engagement with ENISA, EU-CERT (EU Computer Emergency Response Team) and the NIS Cooperation Group. However, this will be on a mutually consensual basis and the UK will be a 'third country' under these arrangements and excluded from most, if not all, of the EU's strategic cybersecurity decision-making.[7]

Other recent EU cybersecurity regulations will continue to have force within the UK's statute books. A important example here is the EU Security of Networks and Information Systems (NIS) Directive. This

[7] https://www.kcl.ac.uk/cyber-security-brexit-and-beyond

imposes control and regulations on how well prepared those who own or operate the UK critical national infrastructure against cybersecurity threats and was ratified into British law in May 2018

Secondly, the EU General Data Protection Regulation (GDPR), continues its function in protecting citizen and consumer data and in raising awareness of the issues here.

Elsewhere the UL maintains co-operation with other strategic partnerships, like the Anglophone intelligence alliance, the Five Eyes (FVEY). The overlap between cybersecurity and signals intelligence (SIGINT) is substantial and FVEY SIGINT agencies, like UK'S GCHQ, are key conduits for the exchange of cyber threat intelligence (CTI) essential to UK national cybersecurity. For example, the UK's National Cyber Security Centre (NCSC) is part of GCHQ, where much of Britain's cybersecurity experience and sovereign capabilities reside. CTI will also flow between FVEY and European partners like France and the Netherlands through the 'Nine Eyes' arrangement and with the wider SIGINT Seniors Europe (SSEUR) group. Similarly, most EU states are also members of NATO, which has its own cybersecurity agenda and responsibilities.

Though the changes have been significant, there are signs that co-operation can continue to be effective. For example, during the last nine months, the continued working relationship between the UK NCA and EU partners via Europol has resulted in:

- The takedown of both the Emotet malware and the DoubleVPN cybercrime service;
- The arrest of a man wanted by Belgium authorities in connection with the smuggling of 39 migrants found dead in a lorry in Essex in October 2019;
- The capture of six fugitives wanted in Romania, Hungary and Lithuania for offences linked to modern slavery, human trafficking and people smuggling.
- Attended or initiated more than 150 operational meetings between Jan and May 2021

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:

None of special note beyond the provisions detailed above,

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:

Hacking & Computer Misuse based Offences 2021

- In 2021, an estimated **1 in 20** UK youths were involved in hacking related offences – a 21% increase over the previous year
  - 5.6% of male teenagers admitting to hacking, compared to only 3.9% of girls;
  - 1.5% of boys sent Internet viruses/malware, compared to only 0.3% of girls.

- On the basis of these figure, hacking and represent a higher rate of offending for young people than shoplifting (3.6%), vandalism (3.6%), smoking (2.7%), joining a gang (2.2%) stealing from other persons (1.3%), or assaulting another person with a weapon (1.1%)

- "The UK's National Crime Agency (NCA) said that data from its National Cyber Crime Unit (NCCU) showed a 107% increase in police reports from 2019 to 2020 of students deploying DDoS attacks.
- The median age for referrals to the NCCU's "Prevent" team is reportedly 15, and a recent NCA report revealed that children as young as nine have been caught launching DDoS attacks.

Online grooming

- There were 5,441 Sexual Communication with a Child offences recorded between April 2020 and March 2021, an increase of around 70% from recorded crimes in 2017/18
- Nearly a third of UK children accepted a friend request from someone they did not know
- An estimated 1 in 50 children (2%) said that they spoke to or messaged someone online in the previous 12 months who they thought was their age but later found out were much older.
- An estimated 5% of children aged 10 to 15 years met up in person with someone they had only spoken to online (equivalent to 212,000 children) in the previous 12 months.
- Around 1 in 10 children (11%) aged 13 to 15 years reported receiving a sexual message, while 1 in 100 reported sending a sexual message, in the previous 12 months.
- Girls aged 13 to 15 years were significantly more likely to report receiving sexual messages than boys (16% compared with 6%) in the previous 12 months."
- There were some clear patterns in this across different forms of social media
- The NSPCC found that sex offenders groomed children on Instagram more frequently than on any other online platform (32% of the 1,317 cases where a method was recorded), closely followed by Facebook (23%) and Snapchat (14%).
- The NSPCC also estimated that an average of one online abuse offence against a child was recorded every 16 minutes in England and Wales in just over nine months (based on police data from April to June 2019)."

Online Bullying & Harassment

- Around one in five children aged 10 to 15 years in England and Wales (19%) experienced at least one type of online bullying behaviour in the year ending March 2020, equivalent to 764,000 children"[8]
- Between 2015 and 2016, BBC data suggests there had been an increase of 36,462 police reports involving malicious communication
- Following the 2017 UK General Election, Amnesty International conducted research directly examining the scale of abuse during the election campaign.132 They found that between 1 January 2017 and 8 June 2017, 900,223 tweets were sent to 177 female MPs, of this 25,688 were deemed abusive.
- In 2016 Ditch the Labels annual bullying survey found that 65% of participants had experienced some form of cyberbullying, an increase of 3% on the previous year.136 By 2018 66% of participants had been subjected to cyberbullying, an increase of 1% since 2016.137
- Each year the UK CPS conducts a report examining violence against women and girls in England and Wales. The 2017 report exposed that the number of prosecutions brought under the Protection from

8

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/onlinebullyinginenglandandwales/yearendingmarch2020

Harassment Act relating to stalking and harassment had decreased by 8.4% compared to the previous year.

- A BBC Freedom of Information request found an 85% rise in reports made to the police concerning online harassment and trolling. 155 It can be suggested that despite the increase in reports made to the police relating to cyberstalking and cyber harassment, fewer prosecutions are being pursued in the criminal justice system.

Peer to Peer sexual abuse

- In autumn last year, the NSPCC announced a 29% increase in children seeking help from Childline due to peer-on-peer sexual abuse.
- Research suggests that peer-on-peer abuse is one of the most common forms of abuse affecting children in the UK.
- For example, more than four in ten teenage schoolgirls aged between 13 and 17 in England have experienced sexual coercion.
- Two thirds of contact sexual abuse experienced by children aged 17 or under was committed by someone who was also aged 17 or under

Trafficking

- In 2021 in UK 8,730 modern slavery offences recorded by the police, a 5% increase from 8,354 in the year to March 2020 in England and Wales.[9]
- In terms of prosecutions, there has been a 20% increase in referrals to the Crown Prosecution Service (CPS) in England and Wales, which have resulted in charge, (from 427 to 476 pre-charge decisions).
- an increase of 27% (to 3,239) in the number of modern slavery offences involving a child victim recorded by the police in England and Wales in the year ending March 2021 compared with the previous year[10]
- 16,830 episodes of need for child sexual exploitation and 2,710 for trafficking identified by the Department for Education's children in need census in the year ending March 2021, both representing a 10% decrease from the previous year; likely the result of a fall in referrals from schools during the pandemic
- In 2021 there was a increase of 9% in the number of potential child victims referred to the national referral mechanism compared with the previous year (from 5,028 to 5,468)

Illegal Downloading & Piracy

- In 2021 the overall level of infringement for all content categories (excluding digital visual images) was 25%, which is 2% higher than the previous year but the same as in four of the previous five years
- Some categories have higher levels of infringement than the average – e.g. live sports – (29% infringement), digital magazines – 27%
- Other categories were around, or just below, average infringement levels: audiobooks – 24% software – 23% film - 20%
- Others were notably lower than average infringement levels: music -15% TV – 14% e-books - 14% video games - 11%

---

[9] https://www.gov.uk/government/publications/2021-uk-annual-report-on-modern-slavery/2021-uk-annual-report-on-modern-slavery-accessible-version

[10] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/childvictimsofmodernslaveryintheuk/march2022

- According to the Ministry of Justice, 180 people were found guilty of offences under the Trade Marks Act (TMA) and one under the Copyright Designs and Patents Act 1988 (CDPA) during 2020, compared with 401 and 23 in the previous year.

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

Answer:

Whilst there are many aspects of the UK CJS response to transnational cybercrime which are in a state of flux following the Brexit transition, overall policy towards digital offending remains fairly constant

Perhaps most notable feature is the very mixed stance towards many forms of cybercrime. On the one hand there is a tendency to 'talk tough' and to hand out substantial (but often symbolic) sentences in some cases. On the other, the Police and Courts often take a more liberal position. Financial crime such as online fraud tend to be pursued quite rigorously, but prosecution and sentencing of computer misuse offences like hacking remains surprisingly mild. Though minors tend to prosecuted for hacking related offences more than other categories of cybercrime, figures from HM Courts and Tribunals Service revealed there were a total of just 422 prosecutions brought under the Computer Misuse Act 1990 (CMA) over the decade 2009-2019, with the figure rising to 441 including the year 2007.

Criminals convicted of CMA offences are often likely to avoid prison, with (for example) just nine (including young offenders sent to youth prisons) receiving custodial sentences out of 45 convictions in 2018. Between 2008 and 2018, 79 people – 24 per cent of the total prosecuted in that period – were found not guilty at court or otherwise had their cases halted. Of the guilty, 16 per cent were given immediate custodial sentences. That number rises to 45 per cent where suspended sentences are included.

The most common range of fines fell between £300 and £500, with one criminal having been fined more than £10,000 last year – the only one to be so punished since 2012. In general, around five fines were issued per year over this period.