

GLOBAL FUND TO END MODERN SLAVERY

Legal and institutional responses to the online sexual exploitation of children

Norway country case study



Content notice

This report deals with the topic of online sexual exploitation of children (OSEC) and includes reference to abuses experienced by children in this context. The report does not recount the specific experiences involved in OSEC cases. However, it does describe types and patterns of behaviour associated with OSEC in general terms.

Authorship and acknowledgements

This report was funded by the Global Fund to End Modern Slavery (GFEMS). The opinions, findings, and conclusions stated herein are those of the author(s) and do not necessarily reflect the views of GFEMS.

This report was reviewed by lived experience experts, whose inputs and perspectives are integrated throughout the document. Special thanks to Ruby, Liberty, and Joy for their invaluable insights. Special thanks to Ruby, Liberty, and Joy for reviewing and advising on this report.

Rights Lab project team

Dr Ergul Celiksoy, Rights Lab Research Fellow in Modern Slavery and Criminal Justice, University of Nottingham (lead author)

Dr Katarina Schwarz, Rights Lab Associate Director (Law and Policy) and Associate Professor of Antislavery Law and Policy, School of Law, University of Nottingham.

Harriet Walker-Smith, Rights Lab Research Assistant

Agata Dudkiewicz, Rights Lab Research Assistant

Contents

| Content notice | 1 |
|--|---------|
| Authorship and acknowledgements | 1 |
| Figures | 2 |
| Tables Tables | 2 |
| Table of abbreviations | 3 |
| Background | 4 |
| 1. Overview of domestic legislation and policy | 5 |
| 2. Prosecuted OSEC cases in Norway | 8 |
| 2.1. Offender profile | 9 |
| 2.2. Victim profile | 9 |
| 2.3. Facilitator profile | 9 |
| 2.4. Payment for OSEC | 9 |
| 2.6. Streaming platform | 10 |
| 2.7. Investigation | 10 |
| 4. Investigation and prosecution of OSEC cases in Norway | 11 |
| 4.1. Investigation challenges | 12 |
| 5. Investigation of financial transactions in OSEC cases | 14 |
| 5.1. Payment methods | 15 |
| 5.2. Monitoring financial transactions | 16 |
| 5.3. Data sharing challenges due to privacy laws | 17 |
| Bibliography | 18 |
| Annex I: Summary of Prosecuted OSEC Cases in Norway | 19 |
| Figures | |
| Figure 1: Number of child sexual offences recorded in Norway, 2017 - 2021 | 11 |
| Figure 2: Number of CyberTiplines sent by NCMEC and number of reports which were further investigated by the Norwegian authorities between 2018 and 2021 | e 11 |
| Figure 3: Number of Suspicious Transaction Reports (STRs) related to OSEC | 14 |
| Tables Tables | |
| Table 1: Summary of Penal Code provisions relevant to OSEC crimes in Norway Table 2: Summary of OSEC cases prosecuted in Norway | 5 8 |
| Table 3: Number of reports sent by ESPs and percentages of reports investigated by police between 2018 and 2021 | 12 |
| Text boxes | |
| Text box 1: Human trafficking provisions in the Norwegian Penal Code | 7 |
| Text box 2. Example OSEC case Text box 3: Example offender profile | 8 9 |
| Text box 3: Example of OSEC payment | 9 |
| Text box 5: Example of streaming platform used for OSEC | 10 |
| Text box 6: Example of OSEC investigation | 10 |

Table of abbreviations

| BSI | Basic subscriber information |
|-----------|--|
| CSEM | Child sexual exploitation material |
| ESPs | Electronic Service Providers |
| FIU | Financial Intelligence Unit |
| ISPs | Internet Service Providers |
| KRIPOS | National Criminal Investigation Service |
| NCMEC | National Centre for Missing and Exploited Children |
| NOK | Norwegian Krone |
| OSEC | Online sexual exploitation of children |
| PPP | Public-Private Partnership |
| STRs | Suspicious Transactions Reports |
| VPN | Virtual Private Network |
| ØKOKRIM | Norwegian National Authority for Investigation and Prosecution of Economic |
| BKOKKIIVI | and Environmental Crime |

Background

Demand-side perpetration of the online sexual exploitation of children (OSEC) is a growing concern in Norway. The National Criminal Investigation Service (KRIPOS) in Norway reported an increase in online sexual exploitation of children (OSEC), recording around 2,000 attempts to access websites hosting child sexual abuse materials in December 2017 alone (ECPAT Norway, 2018, p. 13). Between February 2017 and February 2018, 15,000 unique Norwegian IP addresses were identified to be linked to sexual abuse materials (Politiet, Kripos - NCIS Norway, 2019, p. 17). Analysis of Norwegian case law indicates that different internet service providers (ISPs), including Skype, MSN, Nettby, Onlinebandit.no, Jippii and eMule, are used to access online child sexual abuse, webcam sexual exploitation, grooming, and human trafficking online (Politiet Kripos, 2015).

Norwegian law enforcement has investigated and prosecuted cases involving Norwegian citizens who ordered live streaming of sexual abuse from abroad (Politiet, Kripos - NCIS Norway, 2019, p. 30). Most reported cases were linked to the Philippines, where facilitators received payments from Norwegian perpetrators. Prosecuted cases show Norwegian perpetrators in contact with a number of adult facilitators through various online channels and engaging in live streaming for a long time (ibid).

In recent years, Norwegian courts have convicted offenders involved in live streaming of sexual abuse from the Philippines. Cases of live streaming were tried under the Penal Code (Straffeloven), invoking provisions on sexual offences and human trafficking. Norwegian courts held that Norwegian offenders should be treated as 'primary offenders' even though they did not physically abuse the child victims (ECPAT Norway, 2021, p. 39). This is because courts determined that both facilitators and children in the Philippines were dependent on the money from offenders. In a case involving a Norwegian man purchasing live streaming of sexual abuse from the Philippines, the court stated that the offender 'knew that the minor victims and their families were poor, meaning that they were dependent in the money he paid for the sexual acts', constituting a 'cynical exploitation of poor children dependent on the income provided by the abuse' (Bergen District Court's Judgment: TBERG-2016-61974).

Online sexual exploitation of children (OSEC) involves the use of technology and the internet to view and share child sexual exploitation material (CSEM), groom children online, or live stream sexual abuse of children. Abuse becomes exploitation where the offending involves an exchange of some kind of financial or other benefits. Generally, the offender pays through a money transfer agency to the trafficker who has access to exploited children to generate CSEM. This material is then transmitted from live streaming video communications platforms. These activities are classified as trafficking in persons according to the Palermo Protocol (IJM, 2020, p. 16)

This country report examines domestic legislation and policies relevant to OSEC in Norway, as well as exploring the investigation and prosecution of OSEC cases. Special attention is paid to financial flows involved in OSEC cases to analyse how payments made for OSEC are detected, reported, and investigated by Norwegian law enforcement agencies and other relevant domestic authorities.

1. Overview of domestic legislation and policy

Norwegian law is described as 'technology neutral', meaning that it does not make a distinction in terms of whether a sexual offence is committed online or offline (ECPAT Norway, 2021, p. 23). In other words, Norwegian law treats sexual acts committed physically or through online platforms in the same way. This indicates that sexual offences committed online are considered as serious as in-person sexual offences (ibid).

In Norway, there is no specific legislation defining and specifying online sexual exploitation of children (OSEC). Rather, different provisions of the Penal Code are applicable to sexual offences committed against children online. Table 1 provides a summary of Penal Code provisions relevant to OSEC crimes in Norway.

Table 1: Summary of Penal Code provisions relevant to OSEC crimes in Norway

| Penal Provision | Penalty |
|--|--------------------------------------|
| § 258 - Human trafficking | Imprisonment up to 6 years |
| § 259 - Aggravated human trafficking | Imprisonment up to 10 years |
| § 299 - Sexual assault on a child under 14 years of age | Imprisonment up to 10 years |
| § 300 - Sexual assault involving intercourse on a child under 14 years of age | Imprisonment from 3 to 15 years |
| § 301 - Aggravated sexual assault on a child under 14 years of age | Imprisonment up to 21 years |
| § 302 - Sexual activity with a child between 14 and 16 years of age | Imprisonment up to 6 years |
| § 303 - Aggravated sexual activity, etc. with a child between 14 and 16 years of age | Imprisonment up to 15 years |
| § 304 - Sexual act with a child under 16 years of age | Imprisonment up to 3 years |
| § 305 - Sexually offensive conduct, etc. directed at a child under 16 years of age | Imprisonment up to 1 year |
| § 306 - Arranging a meeting to commit sexual abuse | Imprisonment up to 1 year |
| § 309 - Purchase of sexual services from minors | A fine or imprisonment up to 2 years |
| § 310 - Showing of sexual abuse of a child or shows which sexualise children | A fine or imprisonment up to 3 years |
| § 311 - Depiction of sexual abuse of children or depiction which sexualises children | A fine or imprisonment up to 3 years |

As noted above, Norwegian law is 'technology neutral'. In a landmark decision, the Supreme Court of Norway dealt with whether an offender can be convicted of rape even when the abusive acts take place online (Supreme Court of Norway's Judgment: HR-2017-1282-A). The Supreme Court stated that sexual abuse over the Internet should not generally be punished more leniently than other forms of abuse. In this case, the offender contacted children over the Internet and made them perform sexual intercourse with themselves and each other, filming sexual abuse and sending to the offender. No physical contact was made between the offender and victim children. Nevertheless, the Supreme Court convicted the offender of rape under the Penal Code because the court stated that:

"[the court does] not see it as doubtful that abuse over the internet can be experienced as very serious and have serious damaging effects. There is reason to emphasize that even if the perpetrator is not physically in the same place, he or she can have a strongly controlling and invasive role towards the victim. Many people today, not least young people, use the internet, including social media, to a very large extent, and this forms an important and necessary part of their everyday life. This means that a perpetrator almost at all times, regardless of where the victim is, will easily be able to come into contact with the victim and be responsible for a sustained exercise of threats and pressure."

This judgment of the Supreme Court is significant because the court explicitly held that the law on sexual offences should be applied and implemented in the same way to the cases of both offline and online sexual abuse and exploitation against children.

Although no distinction is made between online and offline offending, Sections 310 and 311 of the Penal Code define OSEC-related offences. Section 310 punishes the acts of 'showing of sexual abuse of a child or shows which sexualise children' with a fine or a prison sentence not exceeding three years. Section 311 punishes offenders who produce, publish, offer, sell, supply, make available or otherwise seek to disseminate, acquire, import, or possess a depiction of sexual abuse of children or a depiction which sexualises children. The punishment is a fine or a prison sentence not exceeding three years.

Several Norwegian offenders have been convicted under the Penal Code for buying live streamed sexual abuse from the Philippines. In one case, an offender from Norway contacted facilitators in Romania, the Philippines, Madagascar and elsewhere via the Internet to sexually abuse and exploit children under 14 years old (Bergen District Court's Judgment - TBERG-2019-31526-2). The offender was a 56-year-old man. From 2012 to 2017, he paid a total of NOK 95,250 (equivalent to \$9,100 USD) via various payment services such as Western Union, World Remit, Pay Pal, and various camera sites. Chat logs showed that the offender negotiated with the facilitator regarding the amount of payment per session. Chat logs also demonstrated that the offender instructed the sexual abuse to be inflicted on children while he was watching the abuse from his home. The offender was convicted under Sections 301, 303, 311, and 312 of the Penal Code and sentenced to 16 years imprisonment.

In this case, the prosecution also argued that the offender should be convicted under the human trafficking provisions of the Penal Code (Sections 257 and 258). The court stated that an offender buying live streaming of sexual abuse may be convicted of human trafficking 'if the defendant has helped to establish a position where children are sexually exploited via the Internet'. What this means is that the prosecutor should prove that victim children are put in sexually abusive position because of the defendant's action. After assessing the facts of the case, the court concluded that:

"There is such doubt about the fact that the court cannot assume that the defendant has contributed to the children being in a position where they are exposed to abuse. There is much evidence that the children were already in a position where they were exposed to abuse. The court considers it so that it falls outside the provision [Sections 257 and 258] that the defendant contributes to them remaining in a situation of abuse."

Text box 1: Human trafficking provisions in the Norwegian Penal Code

Section 257: Human Trafficking

Any person who by violence, threats, taking advantage of a vulnerable situation or other improper conduct forces, exploits or deceives another person into/for

- a. prostitution or other sexual services,
- b. labour or services, including begging,
- c. active military service in a foreign country, or
- d. consenting to the removal of one of the person's internal organs,

shall be punished for human trafficking with imprisonment for a term not exceeding six years.

The same penalty shall be applied to any person who

- a. facilitates such force, exploitation or deception as specified in the first paragraph by procuring, transporting or receiving the person,
- b. otherwise contributes to the force, exploitation or deception, or
- c. provides payment or any other advantage to obtain consent for such a course of action from a person who has authority over the aggrieved person, or who receives such payment or advantage.

Any person who commits an act as specified in the first or second paragraph against a person who is under 18 years of age shall be subject to punishment regardless of whether the act involved violence, threats, taking advantage of a vulnerable situation or other improper conduct. Any person who was ignorant of the fact that the aggrieved person was under 18 years of age shall be subject to a penalty if he/she may be held to blame in any way for such ignorance.

Section 258: Aggravated Human Trafficking

Aggravated human trafficking is punishable by imprisonment for a term not exceeding 10 years. In determining whether the violation is aggravated, particular weight shall be given to whether the person subjected to the act was under 18 years of age, whether severe violence or force was used and whether the act generated significant proceeds. Any person who was ignorant of the fact that the aggrieved person was under 18 years of age shall be punished if he/she may be held to blame in any way for such ignorance.

In 2016, an offender was convicted of aggravated human trafficking and sentenced to eight years imprisonment because of his involvement in live streaming of sexual abuse from the Philippines (Bergen District Court's Judgment: TBERG-2016-61974). In this case, the offender contacted the facilitator over the Internet and ordered sexual abuse of children to be streamed to the offender. The prosecutor argued that by taking advantage of the victim's position of vulnerability or through other improper conduct, the offender was an accomplice to human trafficking because he purchased the service and also occasioned the sexual exploitation of the children (Council of Europe, 2018, p. 71). The importance of this case was underlined by the National Authority for Prosecution of Organised and Other Serious Crime, who stated that 'We have not seen corresponding indictments in Norwegian case law, [...] where the person who places orders sexual exploitation of children is indicted for being accomplice to human trafficking' (ibid, p. 72).

2. Prosecuted OSEC cases in Norway

In this country-case study report, we have collected and analysed prosecuted OSEC cases in Norway. OSEC cases prosecuted in Norway were collected through the search of known legal databases (i.e., LovData), official websites of domestic courts and law enforcement agencies, internet searches, and news media reporting. Searches were conducted in both English and Norwegian to capture the available case reports in both languages. For all cases, we sought to cross-check multiple sources to ensure the accuracy of information presented in each case, and to gain a full understanding of the case and offence.

We reviewed 110 cases on child sexual abuse and exploitation where a Norwegian offender was involved. Of these cases, only seven included Norwegian offenders committing OSEC-related offences against children in the Philippines. The relatively low number of identified OSEC cases in Norway resulted from the challenges in accessing complete case reports. Legal databases and court websites do not generally include the full text of cases. Online searches did not produce many OSEC-related cases prosecuted in Norway. Therefore, we have collated and analysed only seven cases where Norwegian offenders were found to have purchased OSEC from the Philippines and elsewhere such as Madagascar and Romania.

Table 2: Summary of OSEC cases prosecuted in Norway¹

| # | Offender gender | Offender age | Date of offending | Date of sentencing | Payment method | Communication platform | Sentence: imprisonment |
|---|--------------------|-----------------|-------------------|--------------------|---|--|------------------------|
| 1 | Male | 61 | 2010-2017 | 2020 | Unknown | Skype | 16 years |
| 2 | Male | 51 | 2016 | 2017 | Unknown | Unknown | 12 years |
| 3 | Male | 73 | 2014 | 2016 | Unknown | Skype | 8 years |
| 4 | Male | 48 | 2015 | 2019 | Western Union, WorldRemit, PayPal, SegPay, adult sex chat websites (Bongacam) | Skype, Yahoo Messenger, Bongacam | 16 years |
| 5 | Male | 56 | 2015 | 2019 | Western Union, WorldRemit, PayPal, adult sex chat websites | Skype, Yahoo Messenger | 16 years |
| 6 | Male | 61 | 2011-2016 | 2020 | Unknown | Unknown | 21 years |
| 7 | Male | Unknown | 2021 | Unknown | Unknown | WhatsApp | Unknown |

Text box 2: Example OSEC case

The offender contacted women and men, residing in Romania, the Philippines, Madagascar and elsewhere via the Internet. He conveyed in sexualised chats instructions to the facilitators about the conduct of sexual abuse against children for 18 years and transferred money as remuneration for the abuses. Both the facilitators and children were in a vulnerable situation because they lived under very difficult economic and social conditions.

(Norway - Case No. 1; Supreme Court of Norway - Judgment 20-064622STR-HRET)

¹ Details of OSEC cases prosecuted in Norway are further summarised in Annex I.

2.1. Offender profile

All seven cases concerned Norwegian offenders prosecuted for purchasing OSEC crimes in the Philippines between 2016 and 2020, with some offences being committed as early as 2010. All offenders were located in Norway. Of the seven cases, all offenders were male. The age of two was unknown, but the five others were aged between 48-73, with an average age of 58.

Text box 3: Example offender profile

A 48-year-old man was sentenced to prison for 16 years for complicity in a number of sexual assaults against children under 14 and under 16. A number of the victims were under the age of 10. The conviction also concerned a large number of attempts. The number of victims was around 190.

(Norway - Case No. 4; Bergen District Court – Judgment TBERG-2018-51923)

2.2. Victim profile

Of seven cases, five involved children located in the Philippines. For the remaining two cases, victims were located in the Philippines, Madagascar, and Romania. Victims were aged in the range of 10 months to 16 years old. They were both girls and boys. In the majority of cases—six out of seven—the offenders committed OSEC crimes on more than one child victim. One of the offenders was found to have committed OSEC on a total of 190 children.

2.3. Facilitator profile

Of seven cases reviewed in this research, four did not include any information with respect to the facilitators of OSEC. In the remaining three cases, facilitators were found to be the mother, both parents, and the carer of the child victims respectively. They were all located in the Philippines.

2.4. Payment for OSEC

In five out of seven cases, the payment for OSEC was not identified. In the remaining two cases, offenders were found to have used different payment platforms including Western Union, WorldRemit, PayPal, and SegPay. Further, one case reported that the offender was also using Tokens on Bongacams, an adult sex chat website, to pay for OSEC.

Text box 4: Example of OSEC payment

The defendant has mainly used global payment services from Western Union, WorldRemit, PayPal and others such as SegPay. The defendant was eventually banned from payment services. He was already banned from Western Union in 2012. He used WorldRemit to some extent in 2013 and 2014 but was banned from this service in 2014. The latter justified this with 'unusual activity'. The police were later informed that there were indications of fraud or small amounts sent for 'Adult Services' where there was reason to believe that the payer had not had contact outside of the Internet, while the recipients also received similar payments from others in the world. From 2014 to 2016, the defendant often used PayPal. He also used SegPay a good deal in 2016.

(Norway - Case No. 4; Bergen District Court – Judgment TBERG-2018-51923)

2.6. Streaming platform

Of seven cases, three did not include any information with respect to streaming platforms used to facilitate OSEC. The remaining four cases showed that offenders and facilitators used different communication platforms including Skype, Yahoo Messenger, and Bongacam.

Text box 5: Example of streaming platform used for OSEC

In the period from spring 2011 to October 2016, the offender from Norway had contacted with women, men, and minor children in the Philippines over the Internet. The offender used Skype, Yahoo Messenger, or Bongacams to convey sexualised dialogues and instructions to the facilitators, engaging in sexual abuses of at least 16 children under the age of 14. These sexual abuses were filmed and transmitted live via the facilitators to the offender. Before, during or after the instructions, the offender transferred money as consideration for the child sexual abuse or promised such payment.

(Norway - Case No. 4; Bergen District Court - Judgment TBERG-2018-51923)

2.7. Investigation

The prosecuted OSEC cases reviewed in this research showed that the OSEC investigations were mainly undertaken by the Norwegian police, KRIPOS. The Norwegian law enforcement agencies collaborated with foreign law enforcement authorities. For example, in one case, the National Criminal Investigation Service in Norway worked closely with the National Bureau of Investigation in the Philippines. In this case, the Nordic Liaison officer in Manila facilitated investigation of OSEC crimes for both law enforcement agencies (Norway - Case No. 7).

In investigating OSEC cases, the police used different investigation techniques including using Open-Source Intelligence to identify the offenders, facilitators, and child victims involved in the case. Further, the police also relied on chat logs and financial transactions to evidence that child sexual abuse was carried out.

Text box 6: Example of OSEC investigation

The investigation revealed large amounts of chat logs which showed that the defendant had extensive contact with Filipino users. In particular, the defendant used the global services from Skype and Yahoo, but also a service called Bongacams. Facebook and other services have also been used. The defendant had several accounts, including on Yahoo. Analysis carried out by the police showed that, for example, he has sent/received around 125,000 individual messages on his Yahoo accounts in the period covered by the indictment. A few thousand have been found on the Bongacams service, exclusively in 2016. On Skype's service, over 60,000 individual messages have been registered in the period from November 2012 until the arrest. Here he was registered with a total of 503 individual contacts.

(Norway - Case No. 4; Bergen District Court - Judgment TBERG-2018-51923)

4. Investigation and prosecution of OSEC cases in Norway

In Norway, the recording of child sexual offences is not distinguished according to whether they take place 'online' or 'offline'. Rather, the cases investigated by the police are recoded as child sexual offences under the Penal Code. Therefore, there is no disaggregated data on OSEC crimes in Norway. Nevertheless, Figure 1 below shows trends in the number of child sexual offences recoded by the police in Norway between 2017 and 2021, including both online and offline child sexual offences.

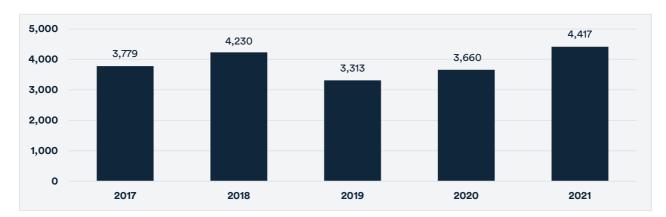


Figure 1: Number of child sexual offences recorded in Norway, 2017 - 20212

Although the exact numbers of OSEC cases investigated by the police is unknown, the number of CyberTiplines by the National Centre for Missing and Exploited Children (NCMEC) indicates the scale of the problem. Figure 2 below shows the number of CyberTiplines received by the Norwegian authorities between 2018 and 2021.

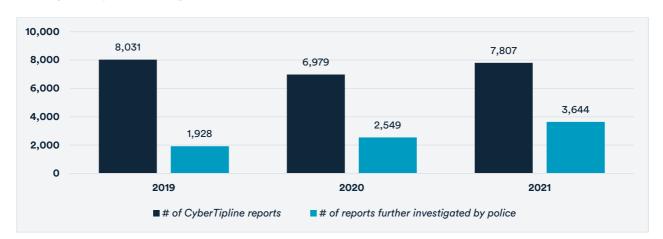


Figure 2: Number of CyberTiplines sent by NCMEC and number of reports which were further investigated by the Norwegian authorities between 2018 and 2021³

CyberTipline reports concerning Norwegian citizens and IP addresses are sent by the NCMEC to the KRIPOS, which then distributes the reported cases to regional police districts (Dorotic & Johnsen, 2023, p. 15). Upon receiving CyberTipline reports, the Norwegian police make an assessment as to whether these reports should be further analysed and investigated. As shown in Figure 2 above, the Norwegian police did not investigate all CyberTipline reports sent by NCMEC. 28% of all CyberTipline reports were investigated in 2019. This rose to 36% in 2020 and 46% in 2021.

² (Dorotic & Johnsen, 2023).

³ (NCMEC, 2021); (NCMEC, 2020); (NCMEC, 2019). The data concerning CyberTiplines which were further investigated by the Norwegian police were taken from Dorotic & Johnson (2023).

Law enforcement officers in Norway stated that cooperation with Electronic Service Providers (ESPs), both nationally and internationally, was the main source of information for the investigation of OSEC crimes (Dorotic & Johnsen, 2023, p. 46). Table 2 below shows the number of reports received by Norwegian law enforcement from various ESPs, as well as the percentages of these reports that were further investigated by the police.

Table 3: Number of reports sent by ESPs and percentages of reports investigated by police between 2018 and 2021⁴

| | 2018 | | 2019 | | 2020 | | 2021 | |
|-----------|----------------|------------------------|----------------|------------------------|----------------|------------------------|-------------|------------------------------|
| ESPs | ESP reports | Cases investigated (%) | ESP reports | Cases investigated (%) | ESP reports | Cases investigated (%) | ESP reports | Cases investigated (%) |
| Discord | 0 | 0 | 247 | 91.9% | 65 | 90.8% | 122 | 81.1% |
| Dropbox | 7 | 100.0% | 13 | 100.0% | 36 | 88.9% | 139 | 73.4% |
| Facebook | 7,982 | 6.6% | 4,341 | 11.1% | 3,819 | 20.2% | 2013 | 14.0% |
| Google | 197 | 70.6% | 220 | 77.3% | 312 | 71.5% | 427 | 80.1% |
| Instagram | 263 | 13.3% | 535 | 21.3% | 793 | 22.7% | 341 | 19.1% |
| KIK | 0 | 0 | 0 | 0 | 62 | 98.4% | 114 | 86.8% |
| Microsoft | 175 | 86.9% | 78 | 89.7% | 154 | 81.2% | 207 | 76.8% |
| Omegle | 23 | 47.8% | 17 | 35.3% | 170 | 28.8% | 405 | 10.1% |
| Reddit | 436 | 84.9% | 669 | 79.5% | 1,082 | 67.0% | 3,105 | 64.3% |
| Snapchat | 436 | 84.9% | 669 | 79.5% | 1,082 | 67.0% | 3,105 | 64.3% |
| TikTok | 0 | 0 | 3 | 100.0% | 64 | 82.8% | 327 | 53.8% |
| Øvrige | 1,376 | 16.2% | 744 | 41.7% | 474 | 56.8% | 571 | 42.6% |
| Total | 10,463 | | 6,868 | | 7,039 | | 7,850 | |

As seen in Table 2, the proportion of reports that were further investigated by law enforcement in Norway varies depending on the source of reports. Although some ESPs reported a significant number of reports, only a small proportion of these reports were further investigated by police (Dorotic & Johnsen, 2023, p. 48). On the other hand, while some ESPs reported a lower number of cases, the police took the initiative to investigate a higher proportion. This is explained by the quality of information sent alongside these reports. When reports are sent with sufficient information, police are able to initiate further investigation (ibid). For example, although Facebook sent more than 75% of all reports, the police investigated only between 10% to 20% of these reports. By contrast, reports sent by KIK, Microsoft, or Dropbox were investigated at a rate between 75% and 100% because sufficient information and evidence was contained in these reports (ibid).

4.1. Investigation challenges

The Norwegian police, KRIPOS, published a report identifying the investigation and prosecution challenges for OSEC crimes. KRIPOS stated that identification of perpetrators and victims is hampered by the lack of regulation requiring storage of IP address subscriber information (Politiet, Kripos - NCIS Norway, 2019, p. 72). It was noted that ISPs are not obliged to store information about subscribers and IP addresses. The lack of this information means that the police struggle to identify offenders and victims (ibid). Another challenge for law enforcement authorities was the requirement for ISPs to delete data about subscribers and IP addresses, if stored, within 21 days (ibid). Although there is no obligation to store data about subscribers and IP addresses, ISPs would still gather and store such data.

⁴ Data in Table 2 is reproduced from Dorotic & Johnsen (2023, p. 47).

Where this was the case, the Norwegian Data Protection Authority required ISPs delete the data after 21 days. This presented a challenge for the law enforcement because 21 days provided little time to investigate criminal acts, resulting in the failure to identify persons suspected of having exploited children sexually online (ibid). In practice, around 30% of the cases of child sexual abuse were classified 'unresolved', mostly due to the lack of information and data concerning subscribers and IP addresses (Dorotic & Johnsen, 2023, p. 42). In 2021, Norway introduced a new regulation extending the timeframe for ISPs to delete data from 21 days to 12 months, allowing ISPs to keep data for 12 months.

The importance of the availability of data about subscribers and IP addresses is underlined by an officer working in Norway's national crime unit:

"The challenge is that electronic service providers operate in such a way that they delete or block an offending account on the grounds that it breaks their service terms or community standards. When the profile is deleted, all incriminating evidence is gone. Police can only penalize offenses for which there is evidence, and for that to happen they need to ask for information, but they cannot do so if the information has been deleted or is not available." - (Dorotic & Johnsen, 2023, p. 42).

The police are also challenged by the fact that the providers of Virtual Private Network (VPN) services are not regulated in Norway. When investigating an OSEC case involving the use of VPN, the police have to rely on user information logged by service providers (Politiet, Kripos - NCIS Norway, 2019, p. 73). However, VPN service providers and sub-providers are not obliged to log such information. When requested, VPN service providers claim that they do not log user information or activity, and state that they do not have any information or data to hand over the law enforcement authorities (ibid).

Norwegian law enforcement struggles to gather data from ISPs based overseas. The procedure to request such data is highly complicated and time consuming as highlighted by a criminal investigator in Norway:

"Most of the service providers have headquarters abroad, mostly in the USA. The police can ask for basic subscriber information (BSI) out of the information given by people when they establish an online profile. The police can obtain this information without a warrant. However, the situation becomes much more difficult when the police try to obtain information on the content connected to a certain profile. Then, the police must obtain a warrant from a regional public prosecutor's office, which is then sent to the Director of Public Prosecutions, which then goes to the Ministry of Justice, then to the Ministry of Foreign Affairs, which sends the case to the US Ministry of Foreign affairs, from where it is transmitted to state authority entities, then to local authority bodies, which then apply US regulations compliance checks (in California, for example). In Norway, we may have different regulatory frameworks than in the US, but the case must be punishable in both countries to be eligible. In line with US laws, the Norwegian police must document that the content connected to those profiles is related to the criminal offense. It is not their problem [California's regulators'] if the Norwegian police cannot document the relationship between the case and the profile because they cannot access the content associated with that profile. The Norwegian police are fully dependent on cooperation with service providers and their rapid response." - (Dorotic & Johnsen, 2023, p. 41)

Issues and uncertainties are also found at the national level. For example, law enforcement officers stated that they were unable to follow child sexual abuse trends over time because the Penal Code does not distinguish online crimes from offline crimes (ibid, p. 41). This means that police did not follow a uniform and consistent recording procedure to label offences, 'which leads to subjectivity in coding' (ibid). It was further underlined that the law enforcement failed to ensure sufficient sharing of investigative methods across regions in Norway. This is coupled with high turnovers of expert officers working on OSEC cases, which consequently contributes to knowledge gaps (ibid).

The Norwegian police highlighted that foreign children who are sexually abused by Norwegian offenders are not given victim status in Norwegian criminal cases (ibid, p. 74). This has significant consequences for victim children because no Norwegian counsel is appointed to safeguard their interests. This means that significant victim rights in criminal cases are not usually enforced in cases involving foreign children, because they do not have counsel appointed to safeguard their rights and interests, including seeking compensation and the opportunity to appeal (ibid, p. 74). KRIPOS noted that there were no cases where foreign child victims were awarded compensation even though this is common practice for victims in Norway.

5. Investigation of financial transactions in OSEC cases

Norwegian law enforcement authorities state that there is a flow of money transfers from Norwegian nationals to known facilitators of live streaming of child sexual abuse (Politiet, Kripos - NCIS Norway, 2019, p. 30). The majority of money transfers made for OSEC remain undetected although the Financial Intelligence Unit (FIU) at the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM) receives an increasing number of suspicious transactions reports (STRs) linked to live-streamed sexual abuse of children abroad (ibid).

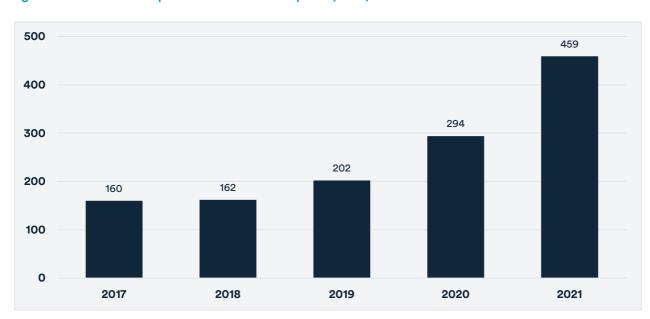


Figure 3: Number of Suspicious Transaction Reports (STRs) related to OSEC⁵

Figure 3 shows the number of STRs related to OSEC in Norway. Between 2017 and 2021, the FIU in Norway filed a total of 1,277 STRs related to OSEC (Dorotic & Johnsen, 2023, p. 49). The number of STRs related to OSEC increased from 160 reports in 2017 to 459 reports in 2021. This increase is attributed to the growing awareness of financial transactions involved in OSEC cases, as well as development of indicators and building experience and expertise by the FIU working on these crimes (ibid). Cooperation and collaboration between the FIU in Norway and other national FIUs are considered another important factor in terms of intelligence sharing, contributing to the detection of a higher number of STRs related to OSEC (ibid).

In Norway, the Financial Intelligence Unit (FIU) is the primary law enforcement agency investigating OSEC transactions. Terje Nordtveit and Kirsti Solberg Løtveit, Police Superintendents at the FIU stated that FIU Norway is receiving an increasing number of STRs, including information related to OSEC-crimes. There might be a potential of having more resources for the analysis and evaluation of all kinds of AML-reports, especially reports related to OSEC (Interview #14).

⁵ This data is reproduced from Dorotic & Johnsen (2023, p. 49).

The FIU in Norway investigates and analyses the sender, receiver, and modus operandi of transactions (ibid). The FIU also examines other related cases to identify any potential connections or similarities. Based on their findings, the FIU prepares information for the police, which may be included in an Intelligence Report indicating suspicions without sufficient grounds for a criminal report. If the FIU has substantial suspicion, they can file a report to prompt an investigation by the law enforcement (ibid).

5.1. Payment methods

Prosecuted OSEC cases in Norway indicate that offenders use global payment platforms such as Western Union, WorldRemit, PayPal, and Segpay to pay for live streamed sexual abuse of children (ECPAT Norway, 2021, p. 39). Offenders sometimes create payment accounts with different payment platforms or move to another payment platform if their account is blocked due to 'unusual activity' (ibid).

For example, an offender made a total amount of NOK 149,454 to facilitators abroad between 2011 and 2016 (Bergen District Court's Judgment: TBERG-2018-51923). The offender was investigated by the police in an operation named 'Dark Room'. It was discovered by the police that the offender had used various payment services including Western Union, WorldRemit, PayPal, Segpay, and some other payment methods. The defendant was initially using Western Union until his account was suspended from payment services. When he was banned by Western Union in 2012, he started using WorldRemit in 2013 and 2014 until he was also banned from this service due to his unusual activity in 2014. Between 2014 and 2016, the offender used PayPal to transfer money overseas for OSEC. He also used SegPay in 2016 (ibid).

In this case, the police also discovered large amounts of chat logs showing the conversations between the offender and different facilitators in the Philippines. The defendant used different digital platforms such as Bongacams, Facebook, Skype, and Yahoo. It was found that the defendant sent and received around 125,000 messages on his Yahoo accounts, 60,000 messages on his Skype account and several thousand messages on the Bongacams service. The court in this case used the evidence of money transfers alongside chat logs when analysing whether or not children were sexually abused.

It is interesting to note that the defendant also used Tokens on Bongacams, an adult sex chat website. The evidence showed that the defendant was introduced children by facilitators who were also the users of Bongacams. He was asked to pay Tokens for the abuse of children. The offender instructed what abuse should be carried out on children, and he paid facilitators as Tokens (Bergen District Court's Judgment: TBERG-2018-51923).

In another case, the prosecution uncovered that the offender paid a total of NOK 95,250 between 2012 and 2017 via Western Union, WorldRemit, PayPal, and various camera sites (Bergen District Court's Judgment: TBERG-2019-31526-2). Money transfers were made to facilitators in Romania, Madagascar, and the Philippines. For example, the offender transferred PHP 1,000 on five occasions to a facilitator in the Philippines via WorldRemit. In addition to the payments through Western Union, WorldRemit, and PayPal, the offender also made payments to facilitators as Tokens on Cam4, an adult sex chat website. It was discovered that the offender and facilitators communicated on Cam4, negotiating the nature of abuse, duration, and payment. Once the offender made the payment as Tokens on Cam4, they used Skype for live streamed sexual abuse of children. The offender made a number of Token payments on different dates. The court determined that the amount of Token payments was higher when a child was involved. It was found that the offender was paying more than 100 Tokens for sexual abuse of children.

The prosecution uncovered that there were at least 10 transactions with more than 100 Tokens paid in each. The transaction evidence showed that the offender also used other similar adult sex chat website, such as Cumcams, to communicate with facilitators and make payments (Bergen District Court's Judgment: TBERG-2019-31526-2).

Participants in this study indicated that offenders look for the availability of payment methods to send and receive money. For example, Terje Nordtveit and Kirsti Solberg Løtveit, Police Superintendents at Financial Intelligence Unit (FIU) in Norway, stated that:

"We think it's a possibility, it's depending on the possibility of payment methods in Norway and of course in the receiving country. So, if the facilitators in the Philippines are saying to the Norwegian guy that you have to pay me in the Western Union or you have to pay me within crypto, OK, then you have to do that. But it should be a possibility to do it from his home, you know. And that is why we are saying that it's developing all the time. It's increasing the amount of payment methods. So if we see that today it's Western Union, or remotely, or PayPal, tomorrow it will be something else" - (Interview #14).

Terje Nordtveit and Kirsti Solberg Løtveit stated that most of the transactions made for OSEC in Norway have been made via money transfer services such as Western Union and PayPal (Interview #14). Terje Nordtveit and Kirsti Solberg Løtveit underlined that they have not found cryptocurrency or mobile banking payments made for OSEC from Norway (ibid). However, they also emphasised that this does not mean that cryptocurrency or mobile banking payments are not used, but they are not reported to FIU in Norway.

To improve the investigation of financial transactions made for OSEC, the FIU in Norway works to develop 'typologies' or 'indicators' to flag suspicious payments (ibid). The biggest challenge for the FIU working on OSEC-related transactions is to identify the purpose of the payment because both the senders and receivers are generally unknown to law enforcement (ibid). In addition to developing 'indicators' for OSEC-related transactions, the FIU also work to identify if any money transfers have been made to known facilitators in the Philippines (ibid).

5.2. Monitoring financial transactions

In Norway, the financial sector monitors their systems and services to flag suspicious transactions associated with predicate offences under the Anti-Money Laundering Law. However, a Representative of a Financial Institution in Norway stated that the financial sector is not well-informed by the government of what to look at when monitoring OSEC-related transactions (Interview #9). They highlighted that OSEC is not 'clearly' included in the Anti-Money Laundering Law as a predicate offence. By emphasising the importance of monitoring OSEC-related transactions, they said that 'it has to be clear part of the legislation' (ibid).

Although OSEC is not specifically included in the Anti-Money Laundering Law, the FIU states that they are dealing with OSEC transactions under this legislation. Further, the FIU provides the financial sector with a general list of indicators based on reports and various sources (Interview #14). These indicators are aimed to help financial institutions to monitor their systems and services for OSEC-related transactions. Terje Nordtveit and Kirsti Solberg Løtveit stated that:

"...the procedure under the Anti-Money Laundering Law is a way of handling this until we have a kind of legislation. Because we cannot just close our eyes that this is not happening. We know that this is happening. We know that a lot of suspects are transferring money. The suspects are completely unknown for the police, and this is the way we and the police can identify them, by money transactions." - (Interview #14).

The financial sector can play 'a major role' in identifying and investigating OSEC-related transactions. A Representative of a Financial Institution in Norway stated that:

"If it weren't for us, no one would be able to do anything either with money laundering or fraud, and the police can't do anything. They don't have the data. If they have it, it's static data, [and] that's old. They need us. And they don't have the capacity either. We spend billions compared to what the police spend on this sort of stuff. So, if we had to work more on this topic as well, then it would be better. And so yeah, I think we could do a lot, if we were told to clearly." - (Interview #9).

The Anti-Money Laundering Law requires the financial sector submit STRs to the FIU. These reports are sent through a national system specifically designed for this purpose. However, this system serves as a one-way channel for sharing information and does not involve the exchange of sensitive data between the financial sector and law enforcement authorities (Interview #9). Although there is a public-private partnership (PPP) between financial institutions and the police, this collaboration focuses more on high-level discussions regarding market trends and general types of crime rather than exchange of data and information (ibid).

Given the lack of exchange of knowledge and data, the financial sector seems to struggle to improve their efforts in identifying and reporting OSEC-related transactions. The Norwegian law lacks the necessary strength and clarity to mandate the financial sector's actions effectively in dealing with OSEC transactions in their systems and services (Interview #9). A representative of a Financial Institution in Norway stated that the challenges of cooperative work with law enforcement persist despite the financial institutions' willingness and interest in collaboration (ibid). Stringent privacy laws and restrictions on information exchange hinder the financial sector's ability to share case-specific information that could be beneficial to both parties (ibid).

5.3. Data sharing challenges due to privacy laws

Experts working in the financial sector indicated that legal obligations to secure privacy and confidentiality hamper the development of effective measures and initiatives to flag suspicious payments that may have been made for OSEC (Dorotic & Johnsen, 2023, p. 50). The procedure for intelligence sharing is rather complicated, and the police's communication and feedback in terms of improving the sector's efforts in detection remain 'minimal' (ibid). The police appear to refrain from sharing intelligence about financial transactions with the financial sector due to sensitive information and privacy concerns. An expert from the financial sector explained that:

"I have to say that I have been given free reins by firms and resources to set up a system for the detection of CSA, but I met quite some resistance, specifically from certain police authorities. What happens is that they say it is not possible to share any information with us. However, it is important to have examples of cases, profiles and patterns that they could share with us, so that we can create systems; however, no one dares to share the information, and I have spoken to all of them. They do not come back to us with concrete information or examples that could help set up flags in the system, probably because of these rules about sharing sensitive information about people and protecting the privacy of the people under investigation." - (Dorotic & Johnsen, 2023, p. 50).

A Representative of a Financial Institution in Norway also highlighted the challenges due to privacy laws:

"The privacy laws do not let us cooperate especially with the police, and they are not able to share information with us either. They can give us some lists of indicators, but they're useless, basically. It's the privacy laws ... [However] we have to remember that our privacy is an illusion anyway. That's what I think, as a citizen, not representing the bank. It is an illusion. Whatever you do online is collected by someone and someone is looking at it. Both your own government and other governments, whatever. In Norway most, or all of the transactions, if it's done outland, in a foreign country I mean, they are sent automatically to the government. So, someone's looking at it, but they're not looking for this purpose." - (Interview #9).

Bibliography

- Council of Europe. (2018, October 16). Report submitted by the Norwegian authorities on measures taken to comply with Committee of the Parties Recommendation CP(2017)30 on the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings. Retrieved April 2023, from https://rm.coe.int/cp-2018-22-rr2-nor-en/16808ef28e
- Dorotic, M., & Johnsen, J. W. (2023). Child Sexual Abuse on the Internet: Report on the analysis of technological factors that affect the creation and sharing of child sexual abuse material on the Internet. Retrieved April 2023, from https://biopen.bi.no/bi-xmlui/bitstream/handle/11250/3055430/SOBIrapport_finalversion_BIOpen.pdf?sequence=1&isAllowed=y
- ECPAT Norway. (2018). Global Study on Sexual Exploitation of Children on Travel and Tourism: Country-Specific Report - Norway. Retrieved April 2023, from https://ecpat.org/wpcontent/uploads/2021/08/COUNTRY-NORWAY.pdf
- ECPAT Norway. (2021, March). Online Child Sexual Exploitation and Abuse: A Review of Norwegian Case
 Law. Retrieved April 2023, from
 https://static1.squarespace.com/static/55e5a4aae4b0a8e8abf5dcac/t/6062d3248f03b063e7d4b7
 2a/1617089319499/ECPAT+Norway+Report+Online+and+media+facilitated+child+sexual+abuse+1
 9+March+2021.pdf
- IJM. (2020). Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society. Retrieved June 2023, from https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020_2021-02-05-055439.pdf
- NCMEC. (2019). 2019 CyberTipline Reports by Country. Retrieved April 2023, from https://www.missingkids.org/content/dam/missingkids/pdfs/2019-cybertipline-reports-by-country.pdf
- NCMEC. (2020). 2020 CyberTipline Reports by Country. Retrieved April 2023, from https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-country.pdf
- NCMEC. (2021). 2021 CyberTipline Reports by Country. Retrieved April 2023, from https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf
- Politiet Kripos. (2015). Trendrapport 2016: Organisert Og Annen Alvorlig Kriminalitet I Norge. Retrieved April 2023, from https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/kriminalitetsutvikling/trendrapport-2016.pdf
- Politiet, Kripos NCIS Norway. (2019, March). Online Sexual Exploitation of Children and Young People.

 Retrieved April 2023, from https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/seksuelle-overgrep-mot-barn/online-sexual-exploitation-of-children-and-young-people.pdf

Annex I: Summary of Prosecuted OSEC Cases in Norway

| Annex I: Summary of Prosecuted OSEC Cases in Norway | | | | | |
|---|-----------------------------|--|--|--|--|
| Norway Case #1 | Summary | The offender was found to have paid for the live streaming of child sexual abuse in the Philippines, Romania, Madagascar and other countries. The offender was found to have been making payments for OSEC from 2010-2017. Victims were aged from two to 13 years. The investigation found that the offender had been making contact with a number of facilitators over the internet. The evidence of chat logs showed that the offender instructed the abuse that he would like to see. The offender was also found to be possessing images and videos of child sexual abuse. | | | |
| | Offender Characteristics | Male, 61 | | | |
| | Year of Offence | 2010-2017 | | | |
| | Year of Sentencing | 2020 | | | |
| | Payment (Method/Total) | Unknown | | | |
| | Communication Platform | Skype | | | |
| | Court | Supreme Court of Norway | | | |
| | Laws | Criminal Code (1902) §195 b, §301; | | | |
| | | Criminal Code (1902) §196 a b, §224a; | | | |
| | 01 | Criminal Code (2005) §258, §303 | | | |
| | Charges/Convictions | Guilty of 4 offences: Complicity in sexual intercourse with children under 14 Attempted complicity in sexual intercourse with children under 14 Complicity in sexual relations with children under the age of 16 | | | |
| | Sentencing | 16 years in prison | | | |
| | Source | Supreme Court of Norway - Judgment HR-2020-2137-A: | | | |
| | | https://lovdata.no/dokument/HRSTR/avgjorelse/hr-2020-2137-a?q=HR-2020-2137-A | | | |
| Norway Case #2 | Summary | The offender was found to have paid for the live streaming of child sexual abuse in the Philippines. The offender was found to have paid for the assault including rape, and sexual intercourse with animals. The investigation also found that the offender was involved in the production and sharing of child sexual abuse material. The offences were described as cynical, targeted and grossly offensive abuse of underage girls. | | | |
| | Offender Characteristics | Male, 51 | | | |
| | Year of Offence | 2016 | | | |
| | Year of Sentencing | 2017 | | | |
| | Payment (Method/Total) | Unknown | | | |
| | Communication Platform | Unknown | | | |
| | Court | Supreme Court of Norway | | | |
| | Laws | Criminal Code (2005) §263, §291, §299, §300, §302, §305, §311; Animal Welfare Act, §37 | | | |
| | Charges/Convictions | Guilty of 6 offences: Rape by causing a child under the age of 14 to perform actions that correspond to sexual intercourse Rape by threatening D and C to carry out actions that correspond to sexual intercourse, with themselves and to have sexual intercourse with each other Sexual acts with children under the age of 16 Sexually offensive behaviour Dealing with sexual representations of abuse of children or depictions that sexualise children Sexual intercourse with animals | | | |
| | Sentencing | 12 years in prison | | | |
| | Source | Supreme Court of Norway – Judgment HR-2017-1282-A: https://www.domstol.no/globalassets/upload/hret/avgjorelser/2017/avgjorelser-juni-2017/sak-2017-391-anonymisert.pdf | | | |

| Norway Case #3 | Summary | The offender was found to be making payments to facilitators in the Philippines for the live streaming of child sexual abuse. |
|-------------------|-----------------------------|--|
| Case #3 | Offender Characteristics | Male, 73 |
| | Year of Offence | 2014 |
| | Year of Sentencing | 2016 |
| | Payment (Method/Total) | Unknown |
| | Communication Platform | Skype |
| | Court | Bergen District Court |
| | Laws | Criminal Code (1902) §62, §64, §195, §200, §201 c, §204 a, §224 |
| | Charges/Convictions | Guilty of 5 offences: Contributing to sexual relation with children under the age of 14 Leading a child under the age of 16 to exhibit sexually offensive or other indecent behaviour as mentioned in section 201 Having contributed to the exploitation of persons under the age of 16 for sexual purposes and human trafficking Having produced, been in possession of or handed over to another, representation of child sexual abuse or representation that sexualises children Having exhibited sexually offensive or other indecent behaviour towards children under the age of 16 in word or in deed |
| | Sentencing | 8 years in prison |
| | Source | Bergen District Court – Judgment TBERG-2016-61974: https://lovdata.no/dokument/TRSTR/avgjorelse/tberg-2016-61974?q=TBERG-2016-61974 |
| Norway Case #4 | Summary | The offender was found to have paid for the live streaming of child sexual abuse in the Philippines. The offender paid for the abuse of around 190 victims, with a number of victims under the age of 10 years. The investigation found that the offender contacted facilitators over the internet, and chat logs evidenced conversations in which payment was promised for specific sexual acts, and found sexualised chat with children. The offender was also found to posses indecent images and video recordings of children. |
| | Offender Characteristics | Male, 48 |
| | Year of Offence | 2015 |
| | Year of Sentencing | 2019 |
| | Payment (Method/Total) | Western Union, WorldRemit, PayPal, SegPay, adult sex chat websites (Bongacam) |
| | Communication Platform | Skype, Yahoo Messenger, Bongacam |
| | Court | Bergen District Court |
| | Laws | Criminal Code (1902) §49, §195 b c, § 195a b c, §196, §200, §201 c, §204 a, §224, §299 a, §301, b, §305 b; Criminal Code (2005) § 304; Criminal Code (2005) §305 a, §311, §312; Criminal Law (2005) §258 |
| | Charges/Convictions | Guilty of 14 offences: Contributing to someone having sexual intercourse with a child under the age of 14 Attempting to assist sexual intercourse with children under the age of 14 Contributing to someone having sexual intercourse with children under the age of 16 Leading children under the age of 16 to commit sexually offensive or other indecent behaviour Contributing to someone having sexual intercourse with a relative in the descending line Exhibiting, in word or in deed, sexually offensive or other indecent behaviour towards children under the age of 16 |

| | | Producing, introducing, or being in possession of or handing over to another, or for consideration to have become familiar with the preparation of sexual assaults against children or representations that sexualise children |
|-------------------|-----------------------------|---|
| | Sentencing | 16 years in prison |
| | Source | Bergen District Court - Judgment TBERG-2018-51923: |
| | | https://lovdata.no/dokument/TRSTR/avgjorelse/tberg-2018-51923?q=TBERG-2018-51923 |
| Norway Case #5 | Summary | The offender was found to have paid for the live streaming of sexual abuse in the Philippines, Romania and Madagascar. The investigation found evidence of chat logs in which the offender instructed the abuse he wanted to see. |
| | Offender Characteristics | Male, 56 |
| | Year of Offence | 2015 |
| | Year of Sentencing | 2019 |
| | Payment (Method/Total) | Western Union, WorldRemit, PayPal, adult sex chat websites |
| | Communication Platform | Skype, Yahoo Messenger |
| | Court | Bergen District Court |
| | Laws | Criminal Code (1902) §195 b, §196 b; §197, §204 b, §224 |
| | Charges/Convictions | Criminal Code (2005) §15, §258, §301, §311, §312, §315 Guilty of 8 offences: |
| | | Contributing to someone having sexual relations with children under the age of 14 Contributing to someone having sexual intercourse with a child under the age of 14, that a child under the age of 14 has performed actions that correspond to sexual intercourse with himself or has performed qualified sexual acts with children under the age of 14 Attempting to contribute to someone having sexual relations with children under 14 years of age Contributing to someone having sexual intercourse with children under the age of 16 Contributing to someone having sexual relations with children between 14 and 16 years of age Contributing to someone having sexual intercourse with a relative in the descending line Contributing to someone having sexual intercourse with a relative in the descending line or causing the person concerned to carry out actions that |
| | | amounted to sexual intercourse with themselves |
| | Sentencing | 16 years in prison |
| | Source | Bergen District Court – Judgment TBERG-2019-31526-2: https://lovdata.no/dokument/TRSTR/avgjorelse/tberg-2019-31526-22 2?q=TBERG-2019-31526-2 |
| Norway Case #6 | Summary | The offender was found to have paid for the live streaming of sexual abuse of a large number of children in the Philippines. The offender paid carers to abuse their children whilst he watched on the internet. |
| | Offender Characteristics | Male, 61 |
| | Year of Offence | 2011-2016 |
| | Year of Sentencing | 2020 |
| | Payment (Method/Total) | Unknown |
| | Communication Platform | Unknown |
| | Court | Supreme Court of Norway |
| | Laws | Criminal Code (1902) §201 c, §224; Criminal Code (1902) §200, §204; |
| | | Criminal Code (2005) §305 a b; |

| | | Criminal Code (1902) §201 c; |
|-------------------|-----------------------------|--|
| | | Criminal Code (1902) §257. |
| | Charges/Convictions | Guilty of 4 offences: Sexually offensive behaviour towards children under 16 Being involved in depictions of child abuse and depictions that sexualise children Complicity in leading children under the age of 16 to engage in sexually offensive behaviour Complicity in serious human trafficking, Criminal Code (1902) § 224 and Criminal Code (2005) § 257 |
| | Sentencing | 21 years in prison (deducted by 1835 days) |
| | Source | Supreme Court of Norway – Judgment HR-2020-2136-A: https://www.domstol.no/globalassets/upload/hret/avgjorelser/2020/november-2020/hr-2020-2136-a.pdf https://www.domstol.no/globalassets/upload/hret/avgjorelser/2020/november-2020/hr-2020-2136-a.pdf |
| Norway Case #7 | Summary | The offender was found to have paid for child sexual abuse in the Philippines. The investigation found the offender made payments to a female facilitator in return for indecent images and video of children. The investigation also found chat logs on WhatsApp in which the financial transactions were discussed. The victim of the sexual abuse was 4 years old at the time of the offences. |
| | Offender Characteristics | Male |
| | Year of Offence | 2021 |
| | Year of Sentencing | Unknown |
| | Payment (Method/Total) | Unknown |
| | Communication Platform | WhatsApp |
| | Court | Unknown |
| | Laws | Unknown |
| | Charges/Convictions | Unknown |
| | Sentencing | Unknown |
| | Source | Manila Bulletin: https://mb.com.ph/2022/12/05/nbi-nabs-woman-from-cebu-city-arrested-for-sexual-exploitation-of-daughter-4-online/ Rappler: https://www.rappler.com/nation/visayas/nbi-rescues-child-from-suspected-cybersex-trafficking-cebu/ |







GLOBAL FUND TO END MODERN SLAVERY

Discover more about our world-class research



nottingham.ac.uk/rights-lab



rightslab@nottingham.ac.uk



@rightsbeacon

Published in September 2023. The University of Nottingham has made every effort to ensure that the information in this report was accurate when published. Please note, however, that the nature of this content means that it is subject to change, therefore consider it to be guiding rather than definitive. © The University of Nottingham 2023. All rights reserved.