FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

June 2023
– 20/2022

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

Investigations into online sexual crimes and cyber fraud conducted by the Danish police

1. Introduction and conclusion

1.1. Purpose and conclusion

1. This report concerns investigations of online sexual crime and cyber fraud by the Danish police.

As society becomes more and more digitised, information technology is becoming a factor in many criminal cases. When information technology is used to commit criminal offences, and the scenes of the crime are in a digital realm, the police is required to use other investigative skills and tools than they usually do. In particular economic fraud, which generally leaves a digital money trail, is increasingly committed using technology, but also the frequency of online sexual crime has increased in pace with the citizens' increasing interaction on social media and the access to share footage digitally.

According to the Danish Ministry of Justice, digital development is challenging the investigative resources of the police in several respects. The reason is that the scope of cybercrime and the speed at which this type of criminal activity spreads across police districts is unprecedented. It is, therefore, essential that the police collect digital evidence very quickly before it is lost. As part of their efforts against cybercrime, "Rigspolitiet" who leads the Danish national police force, have set up specialised units to conduct the preliminary investigation of it-related crime across the police districts. These units distribute the criminal cases to the relevant police district which then conducts a further investigation and potentially press charges and stop the criminal activity.

In 2014, Rigspolitiet set up the National Cyber Crime Center (the NC3) to enhance the professional and technological capabilities of police investigations into cybercrime. The NC3 conducts an initial inspection of the reported crimes and secure evidence of online sexual crime. The NC3 also provides technical assistance in other types of criminal cases involving information technology, for instance, by extracting data from telephones and computers. In November 2018, Rigspolitiet established another specialised unit, *Landsdækkende Center for It-relateret økonomisk kriminalitet* (the NCIK), which is a national center for IT-related cyber fraud, to strengthen the effort against cyber fraud. The purpose of a centralized referral of cases from the NCIK to the police district was, among other things, to create better terms for investigating cyber fraud.

Online sexual crime
Online sexual crime includes sharing footage without consent, sextortion (when a perpetrator threatens to expose sexually compromising pictures), grooming (when adults build trust and an emotional connection to children online with the intent to abuse them sexually).

Cyber fraud
Cyber fraud includes consumer to consumer transactions (for instance, fraud in connection with trade on a third-party selling platform), Ecommerce credit card fraud and abuse of access to streaming accounts. Contrary to the definition made by the Danish police, we do not include ransomware in the category of (economic) cyber fraud.

2. The purpose of the study is to assess whether the Ministry of Justice supported the investigation of online sexual crime and cyber fraud to a satisfactory degree in the years 2019 - 2022. The report answers the following questions:

- Have Rigspolitiet, through the NC3, adequately supported the police in their investigations of online sexual crime?
- Have Rigspolitiet, through the NCIK, adequately supported the police in their investigations of cyber fraud?

Rigsrevisionen initiated the study in May 2022.

Main conclusion

Rigsrevisionen assesses that the Ministry of Justice has not adequately supported the investigation of online sexual crime and cyber fraud in the years 2019 - 2022. Neither the NC3 nor the NCIK assisted the police districts with their initial investigations as intended, and too much time lapsed before cyber fraud cases were sent on to the police districts for further investigation. As a result, the police risk losing opportunities of investigation – particularly in cyber fraud cases.

Rigspolitiet have not, through the NC3, adequately supported the police in three out of four investigations into online sexual crime, but the case processing time has been considerably reduced in the study period

The number of cases where the NC3 conducts an initial investigation has dropped significantly for three out of four types of online sexual crime in the period. In 2019, almost all cases of *grooming* and *sextortion* were initially investigated by the NC3, before they were sent on to the police districts, whereas this was true of only 15% of these cases in 2022. Cases of *digital sex offences* are subject to the same trend. Throughout the study period, the NC3 has conducted initial investigations into almost all cases of *online sexual abuse of children,* i.e. the fourth type of online sexual crimes. The NC3 sends significantly more cases to the police districts without having conducted initial investigations, but, at the same time, the unit has reduced case processing considerably for all four types of online sexual crime. During the study period, case processing has been reduced from an average of 44.2 days in 2019 to an average of 2.7 days in 2022.

Rigspolitiet have not, through the NCIK, adequately supported the police in their investigations into cyber fraud

During the study period, the number of cyber fraud cases initially investigated by the NCIK has dropped. In 2019, approx. one-third of the cases that were sent on to the police districts had been investigated by the NCIK. In 2022, the NCIK investigated less than half of all cases. Although the NCIK conducts initial investigations into fewer cases, an average of 157.3 days elapsed in 2022 before the NCIK sent the cases on to the police districts. The case processing time and the drop in initial investigations into cases can affect the police districts' opportunities to press charges against crime suspects.

The number of cyber fraud cases finalised by the NCIK has increased every year. The NCIK definition of a finalised case is that it has either been shelved or sent on for investigation in a police district. Yet, by the end of 2022, the 25,181 cyber fraud cases had accumulated at the NCIK and were waiting to be sent on to a police district or shelved. By the end of 2022, the average age of the backlog cases was 604.3 days, which increases the risk that the statutory limitation period has passed before the cases are transferred for investigation in a police district.

Cases shelved
The Danish Administration of Justice Act, section 749, subsection 1 stipulates that the police can dismiss a report of a crime when no basis can be found for continuing an investigation. The police are only allowed to shelve cases when no charges have been pressed.

Accumulated cases
In this report, the term "accumulated cases" refers to pending reports that have not yet been finalised by the NCIK.