Kryptovaluta og formuesforbrytelser

I hvilken grad beskytter straffeloven de økonomiske verdier som kryptovaluta representerer?

Kandidatnummer: 9

Antall ord:
14 945

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.05.2024

Innholdsfortegnelse

1 Introduksjon

1.1 Innledning

Gjennom strafferettens historie har den teknologiske utvikling utfordret den til enhver tid gjeldende strafferett, ved at nye forhold må vurderes opp mot eksisterende rettsregler. Denne samfunnsutviklingen har tvunget frem modernisering og oppdatering av lovverket for å gjøre det i stand til å omfatte nye klanderverdige og uønskede handlinger, sett fra samfunnets side. Internett er et eksempel på en slik samfunnsutvikling og handlinger gjort i den digitale sfære.

Selv om kjennetegnene ved de ulike forbrytelsene er de samme, uavhengig av den praktiske fremgangsmåten, har fremveksten av internettet slik vi kjenner det i dag, med stadig bedre prosessorkraft i alle datamaskiner, ført med seg flere nye metoder som muliggjør slike klanderverdige og uønskede handlinger. En kan gjøre seg skyldig i bedrageri ved å lyve til en annen ansikt-til-ansikt, men man kan også lyve via digital kommunikasjon. Hatefulle ytringer kan formidles via et fysisk brev, men formidles ofte gjennom sosiale medier[1]. Det er mulig å forfalske et dokument fysisk, men med litt digital kyndighet kan dokumenter også forfalskes ved hjelp av redigeringsprogrammer.

Det er liten tvil om at en viktig oppgave for Stortinget som formell lovgiver, er å følge samfunnsutviklingen, for på den måten å kunne reagere på nye uønskede handlemønstre. Ideelt sett burde lovgivningen hele tiden ligget i forkant av samfunnsutviklingen, men realiteten er ofte det motsatte. Dette fører til at de enkelte straffebud enten må tolkes dynamisk slik at de også omfatter handlemåter som ikke opprinnelig var en del av straffebudet, eller så må lovgiver vedta nye straffebud for å dekke de nye handlemåtene. En siste mulighet er å la nye uønskede handlemåtene, som passer dårlig inn i dagens lovverk, være straffefrie. Sistnevnte alternativ fremstår som en dårlig løsning. Om handlingen som er begått er av en tilstrekkelig klanderverdig karakter, er det av vesentlig betydning at handlingen omfattes eller blir omfattet av den til enhver tid gjeldende straffelov.

[1] https://www.ldo.no/globalassets/_ldo_2019/03_ombudet-og-samfunnet/rapporter/hatefulle-ytringer/ldo_hatefulle_ytringer_pa_nett.pdf

1.2 Problemstillingen for oppgaven

Kryptovaluta er et nytt fenomen som er muliggjort gjennom internett. Oppgavens problemstilling retter seg mot to aspekter ved strafferetten i forhold til kryptovaluta og den økonomiske verdien den representerer, nemlig 1) om de eksisterende bestemmelser i straffeloven dekker de ulike handlingsmåtene, der den økonomiske verdien kryptovaluta representerer er truet, og 2) dersom straffebudene dekker disse handlemåtene, gir straffebudene rom for å uttrykke den fulle klanderverdigheten som slike handlemåter 'fortjener'?

Disse spørsmålene retter seg mot graden av den beskyttelse straffeloven gir. En målestokk for klanderverdigheten en gitt handling fortjener, vil i denne oppgaven være de eksisterende straffebudene som verner om andres økonomiske verdier. Fremstillingen videre vil ta utgangspunkt i to ulike typetilfeller og for hvert av disse typetilfellene vil det være relevant å drøfte ulike straffebud. Med mindre annet fremgår uttrykkelig, vil alle bestemmelser som omtales eller refereres til i det videre knytte seg til straffeloven av 2005.

Straffebudene jeg ønsker å se nærmere på kan deles inn i to kategorier. Den første kategorien straffebud er de som retter seg mot datakriminalitet spesielt. Straffebudene i denne kategorien som jeg ønsker å vurdere nærmere, er §§ 201, 204, 351 annet ledd og 371 bokstav b). Dette er spesialstraffebud som retter seg mot data og er relevant å se nærmere på ettersom kryptovaluta kun eksisterer som data. Dette kommer jeg tilbake til under punkt 3.1. Den andre kategorien straffebud jeg vil se nærmere på er vinningsstraffebudene §§ 321, 343 og 345 i straffeloven kapittel 27. Disse har som formål å verne om andres økonomiske goder og hvordan disse disponeres, og er relevante å se på ettersom kryptovaluta representerer en økonomisk verdi. Det formuerettslige aspektet ved kryptovaluta forklares nærmere under punkt 3.2.

2 Problemstillingens relevans – Dagens rettstilstand

Økokrim har i de siste årene etterforsket flere tilfeller av «kryptotyverier». Senest i 2021 igangsatte Økokrim etterforskning på bakgrunn av et angrep mot spillet Axie Infinity. I denne saken ble det stjålet kryptovaluta til en verdi av omtrent 50 millioner kroner fra 750 norske brukere.[2] Etter e-post korrespondanse med Økokrim ble det gjort kjent for undertegnede at Økokrims syn er at «[d]et er ingen forskjell på bruken av straffebud enten det dreier seg om kryptovaluta eller "vanlige" penger. Stjeler man dem, kan det være tyveri.»[3] Økokrims forståelse av tyveribestemmelsen innebærer følgelig at det ikke er av betydning for bruk av straffebudene om det er kryptovaluta eller «vanlige» penger som er borttatt. Det kan likevel reises spørsmål ved om en slik forståelse av tyveribestemmelsen er rettslig holdbar.

I Ot.prp.nr.40 (2004-2005) s. 13-14 uttalte Økokrim i sin høringsuttalelse at «[s]traffeloven har relativt liten beskyttelse mot 'tyveri' av informasjon» og at «[s]traffeloven §§ 291 og 292 kan ramme endring eller sletting av data, men ikke det at informasjon/data kopieres eller tilegnes». Økokrim, sammen med Politidirektoratet og Datatilsynet, var av den oppfatning at «det strafferettslige vern om data [bør] i hvert fall være på linje med det man har for gjenstander».

I NOU 2007:2, punkt 9.6 ble det foreslått et straffebud som kriminaliserer datatyveri. Dette forslaget ble ikke fulgt opp av departementet i Ot.Prp.nr.22 (2008-2009). Det er uttalt på side 66 at «[d]epartementet ser ikke som utvalget grunn til å kriminalisere den uberettigete tilegnelsen i tillegg til den uberettigete tilgangen (forslaget § 204)». Begrunnelsen for dette var at «[e]n altfor omfattende kriminalisering av flere handlinger som overlapper hverandre, har lite for seg. Selv om de alminnelige bestemmelsene om utroskap, krenkelse av bedrifts- og forretningshemmelighet, brudd på taushetsplikt osv. (jf. ovenfor i punkt 2.16.1) ikke retter seg direkte mot vern av informasjon, nyter likevel informasjonen et indirekte vern ved disse

[2] https://e24.no/norsk-oekonomi/i/bGPxJ3/etterforsker-kryptotyveri-av-fem-milliarder-kroner

[3] Fra e-post korrespondanse med kommunikasjonsavdelingen i Økokrim, Katrine Hatlen Nylund, Seniorrådgiver. På spørsmål om hvordan Økokrim operer i saker angående kryptovaluta og formuesstraffebud, fikk til svar det siterte ovenfor, blant annet. Økokrim, 15.01.24. Det er gitt samtykke til at jeg bruker denne uttalelsen i min oppgave.

bestemmelsene». Departementets holdning var altså at det ikke er et behov for en spesialbestemmelse om datatyveri, ettersom vern av data allerede nyter beskyttelse etter de øvrige bestemmelsene i straffeloven kapittel 21. Uttalelsene tyder på at dagens tyveribestemmelse i § 321, ikke dekker 'tyveri' av data.

En mulig grunn til at Økokrim anser § 321 som dekkende ved 'tyveri' av kryptovaluta, kan være at det ikke finnes andre dekkende bestemmelser som i tilstrekkelig grad gir et vern mot «tyveri» av data. Dagens tyveribestemmelse i § 321 kan da være det nærmeste man kommer en bestemmelse som beskytter data som formuesgode. Ettersom dette spørsmålet aldri har blitt vurdert av Høyesterett, er det usikkert om en slik tolkning av § 321 er rettslig holdbar og i samsvar med legalitetsprinsippet. Det synes derfor å foreligge et sterkt behov for å avklare kryptovalutaens strafferettslige vern.

3 Om kryptovaluta

3.1 Hva er kryptovaluta?

På samme måte som «vanlige» valutaer, også kalt «fiat valutaer», som f.eks US dollar, euro og norske kroner, representerer også kryptovaluta en økonomisk verdi, selv om den ikke er utstedt av en sentralbank og eksisterer kun i digital form. Transaksjoner skjer mellom to parter uten en sentralisert tredjepart, som en nasjonal sentralbank. Per juni 2023 fantes det, ifølge CoinMarketCap[4], rundt 26.000 ulike varianter av krypto som kan kjøpes og selges i det åpne marked. Den første kryptovalutaen som slo igjennom var Bitcoin som ble lansert i 2009, og er, per 7. mai 2024, den største.[5]

Verdien av en gitt kryptovaluta kan sammenliknes med verdien av en råvare. Tilbud, etterspørsel, tilgjengelighet og konkurranse avgjør verdien.[6] Som de fleste råvarer, og andre fiat valutaer, er verdien av en kryptovaluta også gjenstand for svingninger. Per 7. mai 2024 er verdien på én Bitcoin rundt 698.000 kroner. Kryptovaluter kan kjøpes og selges på ulike plattformer, såkalte kryptobørser. En eier av et beløp kryptovaluta kan dermed realisere verdien av kryptovalutaen, til fiat valuta, eller omvendt, kjøpe kryptovaluta for fiat valuta. Det er også mulig å kjøpe varer og tjenester med krypto. Selskaper som for eksempel Microsoft, Tesla og Starbucks aksepterer enkelte kryptovaluter som betaling for sine varer og tjenester.[7]

Det er flere likheter mellom kryptovaluta og fiat valuta en bankkunde har på sin ordinære bankkonto. Så lenge begge typene valutaene er digitale, det vil si at de kun eksisterer som data, eksisterer de ikke andre steder enn i en database. Hovedforskjellen er, som nevnt, at kryptovaluten ikke er utstedt av en tredjepart, en sentralbank, og transaksjoner gjøres uavhengig av bankenes rutiner, kontroller og lovpålagte krav. Overføringen av krypto involverer kun to aktører, sender og mottaker, såkalt «peer-to-peer».

[4] https://www.forbes.com/advisor/au/investing/cryptocurrency/different-types-of-cryptocurrencies-explained/
[5] https://snl.no/kryptovaluta
[6] https://www.investopedia.com/tech/what-determines-value-1-bitcoin/
[7] https://milkroad.com/accept-crypto/

Konseptet kryptovaluta er i grunnen ganske enkelt, men teknologien bak er svært avansert og sofistikert. Selve navnet kryptovaluta, kommer av begrepet kryptering; alle transaksjoner er kryptert på det som kalles en blokkjede. Kort sagt er en blokkjede en lang digital kjede med blokker, en slags digital oppbevaringseske, som inneholder data og hele kjeden av blokker er lagret i et stort datanettverk. Hva slags data som er lagret i hver blokk avhenger av formålet bak bruken av blokkjeden. I BitCoin sin blokkjede er det blant annet lagret kryptert data som inneholder data om sender, mottaker og beløpet som er sendt. Dette gjør transaksjonene i praksis svært vanskelig, og tidvis umulig, å spore. I samme blokk er det også lagret en såkalt «hash». Dette kan sammenliknes med et digitalt «fingeravtrykk». Hver blokk har et unikt «fingeravtrykk» og dersom innholdet i blokken endres, endres også dette. «Fingeravtrykket» inneholder informasjon om selve blokken og innholdet lagret i den. I tillegg er «fingeravtrykket» til den forrige blokken i kjeden lagret i blokken. Slik er alle blokkene koblet sammen og verifisert av hverandre. Dersom en blokk endres, må alle blokkene etter denne også endres for at datanettverket skal godkjenne endringen. Når blokkjeden er svært lang (flere millioner blokker med kryptert data), krever dette enorm datakraft og er svært tidkrevende. Bitcoin sin blokkjede er konstruert slik at det i praksis er umulig å endre den.[8]

Blokkjeden fungerer da som en digital regnskapsbok: alle transaksjoner er registrert, verifisert og kan spores tilbake i tid på blokkjeden. Denne struktureringen av dataen er det som sikrer verdien av en gitt kryptovaluta. Selv om krypto i realiteten kun er data, er det ikke mulig å kopiere disse, noe som ville ha ført til at verdien kollapset. Teknologien muliggjør transaksjoner mellom individer, uten noen tredjepart som verifiserer transaksjonen.

Ved å bruke såkalte «kryptolommebøker» («crypto wallets»), kan kryptoen lagres på en fysisk enhet eller i et dataprogram. Enheten eller programmet inneholder en offentlig nøkkel («public key»), som fungerer som en adresse til lommeboken, og for å overføre kryptoen trenger man en privat nøkkel («private key») for å autorisere transaksjonen. Kryptoen er ikke lagret et spesifikt sted, men består av flere bits av data flere steder i en database. Lommeboken finner alle bitsene ved hjelp av den offentlige nøkkelen tilknyttet lommeboken, og dermed summerer opp beløpet på kontoen.[9] På plattformer som Coinbase.com kan man

[8] https://youtu.be/SSo_EIwHSd4?si=6K_-H80OKy7ieCyq
[9] https://www.investopedia.com/terms/b/bitcoin-wallet.asp

opprette kontoer for kjøp og salg av kryptovaluta, og slike kontoer sikres gjennom identifikasjon, altså et brukernavn og passord.

Anonymiteten og muligheten for å overføre penger uten en tredjepart har gjort kryptomarkedet svært populært de siste årene, og interessen for å spekulere i krypto har dermed økt betraktelig. Da kryptomarkedet var på sitt høyeste, i april 2021, ble det handlet krypto for rundt 300 milliarder US dollar i løpet av ett døgn. Per 7. mai 2024 er tallet nærmere 90 milliarder US dollar.[10] Det er åpenbart at det er store verdier involvert i kryptomarkedet og det er en klar interesse at disse verdiene bør sikres gjennom lovgivning som beskytter disse mot uberettiget befatning[11]. Vanskene med å spore tilbake hvor kryptoen kommer fra og hva den har vært brukt til, har gjort myndighetene bekymret med tanke på hvitvasking, betaling for kriminelle handlinger og skattesvik.[12] Økokrim har slått fast at «[b]ruk av kryptovaluta er en svært attraktiv metode for å skjule utbytte fra kriminelle handlinger, hvitvaske penger samt finansiere ny kriminell aktivitet».[13] Bruken av disse midlene og hvem som eier dem, er derfor av stor interesse for myndighetene, som f.eks. Økokrim, som jobber med å forhindre og etterforske slike saker.

3.2 Kryptovaluta som formue

Dersom kryptovaluta er noe som i det hele tatt er vernet, eller bør vernes av straffeloven, må det være begrunnet i at det er et formuesgode på lik linje med for eksempel, fiat valuta, fast eiendom, løsøre og aksjer. Hva som skal regnes som et formuesgode, er ikke avklart i strafferetten, men av formueretten og sivilretten. Selve ordet «formue» sikter til at det gode det er snakk om har en økonomisk verdi. Statens innkrevingssentral forstår formuesgode slik: «[e]t formuesgode kan være fast eiendom (som for eksempel huset, hytte, tomt m.m.), bankkonti, verdipapir, bil, båt eller annet verdifullt løsøre som kan omgjøres til penger ved

[10] https://coinmarketcap.com/charts/
[11] Dette forutsetter at lovgiver ikke forbyr eierskap av eller handel med kryptovaluta. Å eie og handle med krypto er foreløpig lovlig.
[12] https://www.okokrim.no/bruk-av-kryptovaluta-i-kriminell-virksomhet.6343555-537788.html
[13] https://www.okokrim.no/getfile.php/4762586.2528.ntbmpquwkinkjm/Infoskriv+bruk+av+kryptovaluta+i+kriminell+virksomhet.pdf

utleie, salg m.m.»[14] I denne ikke-uttømmende listen er det flere fellestrekk ved de eksemplene som er gitt. Sentralt ved disse fellestrekkene er at godet kan omgjøres til penger. Selv om det ikke finnes en konkret definisjon på hva et formuesgode er, kan man si at et formuesgode «*typisk* har økonomisk verdi, at dei *typisk* kan gå over frå ein person til ei annan, og at vi *typisk* kan disponere over formuesgoda ved avtale»[15]. Kryptovaluta passer fint inn i denne forståelsen. Det har en økonomisk verdi, det kan selges og kjøpes, og man kan disponere over kryptovalutaen, enten selvstendig eller ved å opprette en konto hos tilbydere av slike tjenester.

I tillegg til at kryptovaluta kan regnes som et formuesgode, har staten gjort det klart at verdiene som kryptovaluta representerer, er skattbar formue. Dersom man har verdier i «virtuelle eiendeler», skal dette rapporteres i skattemeldingen. Kryptovaluta skal følge «de alminnelige skatteregler for formuesobjekter» og de ikke er «omfattet av unntak og spesielle skatteregler som gjelder for vanlig valuta (FIAT), aksjer, obligasjoner, finansielle instrumenter eller andre typer formuesobjekter med spesielle unntaksregler». [16] Ved salg av kryptovaluta mot oppgjør i en annen type kryptovaluta eller fiatvaluta, er dette å regne som en skattemessig realisasjon. Siden skatteretten fastslår at kryptovaluta skal følge de alminnelige skatteregler, kan det legges til grunn at kryptovaluta er å regne som et formuesgode og at det er mulig å ha en rett til dette formuesgode, ettersom det kan knyttes et eierskap til det gjennom skattemeldingen.

Den retten man kan ha til formuesgodet kryptovaluta, er da i realiteten en rett til å disponere et sett med data, ettersom kryptovaluta kun eksisterer digitalt. Ettersom denne dataen kan representere enorme verdier, er det av samfunnsmessig interesse at denne retten blir beskyttet mot uberettigete disposisjoner og befatning, på lik linje med andre formuesgoder, gjennom tilstrekkelig sanksjonering om noen krenker denne retten. Spørsmålet videre er om, og eventuelt i hvilken grad, straffeloven verner om denne retten.

[14] https://www.sismo.no/no/pub/ordforklaringer/formuesgode
[15] Lilleholt (2018) s. 20
[16] https://www.skatteetaten.no/person/skatt/hjelp-til-riktig-skatt/aksjer-og-verdipapirer/om/virtuell-valuta/skatteregler---virtuell-valuta/

4 De ulike typetilfellene

4.1 Formålet med å bruke ulike typetilfeller

Som nevnt i punkt 1.2 vil jeg ta utgangspunkt i to ulike typetilfeller der eiendomsretten til kryptovaluta som formuesgode er krenket eller truet. Jeg vil nedenfor i punkt 4.2 og punkt 4.3 redegjøre for typetilfellene. Typetilfellene har til felles at eiendomsretten til kryptovaluta tilhørende en person, blir utsatt for en krenkelse, men gjerningspersonens fremgangsmåte for å oppnå sitt formål, er ulik. Formålet med å bruke disse typetilfellene er for det første å oppstille realistiske senarioer der gjerningspersonen har til hensikt å uberettiget tilegne seg en annens kryptovaluta, og for det andre å bruke disse for å belyse de juridiske problemstillingene man kan støte på i slike senarioer. Jeg vil nedenfor i punktene 5, 6, 7, og 8 vurdere de enkelte typetilfellene opp mot de straffebudene jeg anser gjør seg mest aktuelle.

4.2 Typetilfelle 1

Person B har blitt gjort kjent med innloggingsinformasjonen til person A på en kryptobørs, ved å kikke over skulderen hans, idet person A tastet denne inn. Person B har på samme måte også blitt gjort kjent med den private nøkkelen som er nødvendig for å overføre kryptovaluta fra en kryptokonto til en annen. Det er på det rene at person A ikke har hatt noe ønske å dele denne informasjonen med person B, eller noen andre, ettersom det var lagret store verdier på denne kontoen, tilsvarende kr 1.000.000. Person B noterer ned innloggingsinformasjonen på et papir, og når person A har forlatt PC-en sin, logger person B seg inn på kontoen til person A og overfører all kryptovalutaen til sin egen kryptokonto.

4.3 Typetilfelle 2

Person A er eier av en harddisk der det er lagret kryptovaluta til en verdi tilsvarende kr. 1.000.000. Innholdet på harddisken er beskyttet med et passord og innholdet er kryptert, slik at det ikke er mulig å få tilgang til dataen uten at korrekt passord tastes inn når man kobler denne til en datamaskin. Person B stjeler denne harddisken, og han har blitt gjort kjent med

passordet tilhørende person A og kjenner til at det er lagret store verdier på den. Person B har et forsett om å ta harddisken med seg og tømme denne for verdier på et senere tidspunkt. Etter tømmingen av kryptovalutaen, har person B ikke lengre bruk for disken, og planlegger å legge harddisken tilbake stedet han stjal den fra, i håp om at person A ikke har oppdaget at den var borte. Før person B rekker å tømme harddisken for verdier, oppdager person A at harddisken er tatt av person B og varsler politiet. Person B får derfor aldri gjennomført hele planen sin.

5 Uberettiget befatning med tilgangsdata og datainnbrudd

5.1 Generelt om straffeloven kapittel 21 – Vern av informasjon og informasjonsutveksling

Som nevnt ovenfor ble det lagt til grunn av Justisdepartementet i Ot.prp.nr.22 at dagens bestemmelser om vern av informasjon, inntatt i straffeloven kapittel 21, gir et tilstrekkelig vern av data. Kapittelet ble tilføyd i 2009 som en konsekvens av fremveksten av datamaskiner slik vi kjenner dem i dag og hvordan disse, og derav informasjon på disse, kan være offer for uberettiget tilgang, innbrudd eller andre krenkelser. Kryptovaluta er en nyvinning som representerer en mulig utfordring når det kommer til straffelovens bestemmelser om vinningsforbrytelser og andre forbrytelser, der det er borttatt penger eller andre verdier.

Det fremstår rimelig klart at klanderverdige handlinger knyttet til kryptovaluta har en nær sammenheng med datakriminalitet. Dette fordi gjerningsobjektet i forbrytelsene av denne art er informasjon (data) lagret på et datasystem. Straffeloven kapittel 21, «[v]ern av informasjon og informasjonsutveksling», inneholder flere straffebud som sanksjonerer datakriminalitet. Kapitelets overskrift indikerer umiddelbart at formålet bak bestemmelsene er å verne om informasjon og data, og det er derfor relevant å se nærmere på i hvilken grad disse straffebudene verner om kryptovaluta som formuesgode i typetilfelle 1.

5.2 § 201. Uberettiget befatning med tilgangsdata, dataprogram mv.

5.2.1 Gjerningsbeskrivelsen.

§ 201 omfatter handlinger der en «med forsett om å begå en straffbar handling uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen a) passord eller andre opplysninger som kan gi tilgang til databasert informasjon eller datasystem» eller b) «dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som

retter seg mot databasert informasjon eller datasystem. På lik linje «straffes den som uten forsett om å begå en straffbar handling besitter et selvspredende dataprogram, og besittelsen skyldes uberettiget fremstilling eller anskaffelse av programmet». Strafferammen er bot eller fengsel inntil ett år. Bestemmelsen er et resultat av Norges ratifisering av Europarådets konvensjon om cyberkriminalitet artikkel 6.[17] Formålet bak bestemmelsen «er først og fremst at slike handlinger kan være – og ofte vil være – første skritt for å muliggjøre ulovlig inntrengning i datasystem eller for å foreta datamodifikasjon»[18]. I NOU'en uttales det videre at «[p]å denne måten vil befatning med tilgangskoder og skadelig programvare kunne sies å være innledende handlinger til andre straffbare handlinger».

Videre utales det i forarbeidene at «'[b]esitter' betyr at gjerningspersonen har tilgangsdataene på et sted han selv kontrollerer. Besittelsens karakter er uten betydning. Passordet kan for eksempel være skrevet ned for hånd, ligge lagret på et brukerområde på en lokal datamaskin eller på et nettsted på internett som vedkommende selv kontrollerer. Besittelsesalternativet vil også dekke tilfeller der besittelsen har oppstått uforsettlig, men hvor besitteren unnlater å slette tilgangskoden etter at han ble oppmerksom på besittelsen.»[19] Vilkåret vil altså være oppfylt der gjerningspersonen har kontroll over tilgangsdataene, og har disse lagret på et medium vedkommende kontrollerer. For typetilfelle 1, nevnt ovenfor i 4.2, er dette tilfellet. Ettersom person B har notert ned passordene, og har kontroll på dette notatet, er vedkommende i besittelse av disse passordene.

Gjerningspersonen må ha handlet med et videregående forsett om «å begå en straffbar handling». Ut ifra konteksten er det klart at det må det dreie seg om en annen straffbar handling, enn de som er angitt i § 201. Det er altså ikke tilstrekkelig at en kun er i besittelse av «passord», jf. bokstav a) eller et «dataprogram», jf. bokstav b). For typetilfelle 1 har person B forsett om å logge seg inn på person A sin kryptokonto. Person B har følgelig forsett om å begå datainnbrudd, jf. § 204.

[17] CETS 185 - Convention on Cybercrime, https://rm.coe.int/1680081561
[18] NOU 2007:2 s. 97
[19] Ot.prp.nr.22 (2008-2009) s. 400

§ 201, bokstav a) omfatter handlinger der noen uberettiget har fått tilgang til passord eller andre opplysninger som kan gi tilgang til informasjon eller et data system, med forsett om å begå en straffbar handling. Forarbeidene definerer «datasystem» som «enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer»[20] Med «passord eller andre opplysninger» menes «alle data som kan gi tilgang til fysiske eller logiske nivåer i et datasystem».[21] Bokstav b) omhandler «uberettiget» fremstillelse osv. av «dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem». Fremstilling, besittelse osv. av innretninger som datavirus og hackerverktøy som er innrettet mot data eller datasystemer, er straffbart. «[D]atabasert informasjon» forstås som «all informasjon uavhengig av om den er umiddelbart tilgjengelig (har et meningsinnhold) eller om den ikke er lesbar uten bruk av teknisk utstyr».[22]

5.2.2 Graden av vern § 201 gir

For typetilfelle 1 er person B i uberettiget besittelse av «passord […] som kan gi tilgang til databasert informasjon eller datasystem», ettersom passordet kan gi vedkommende tilgang til all informasjonen tilknyttet kontoen. Videre vil han bruke passordet for å komme seg inn i datasystemet der kryptovalutaen er lagret. Person B har da «forsett om å begå en straffbar handling», nemlig datainnbrudd, jf. § 204. I typetilfelle 1 har person B dermed gjort seg skyldig etter § 201. Det kan videre stilles spørsmål om i hvilken grad straffebudet verner om eiendomsretten til kryptovaluta.

I typetilfelle 1 er faktum det at en person har mistet verdier til kr. 1.000.000, og gjerningspersonen kan 'kun' straffes med bot eller fengsel inntil 1 år. Om handlingen var knyttet til en «gjenstand» av lik verdi, tilhørende en annen, slik straffeloven angir som tyveri, kan gjerningspersonen straffes med bot eller fengsel inntil 6 år, jf. §§ 322, jf. 321, forutsatt at øvrige vilkår er oppfylt. Fremgangsmåtene er ulike, men utfallet av begge handlingene er i realiteten det samme. Det økonomiske tapet som er påført virker ikke å være reflektert i

[20] Ot.prp.nr.22 (2008-2009) s. 400
[21] Schjølberg (2017) s. 69
[22] Ot. prp. nr. 22 (2008–2009) s. 400

straffenivået, grunnet den relativt lave strafferammen, jf. §201 første ledd. I tillegg får ikke § 201 markert den særlige klander ved krenkelse av en annens eiendomsrett for egen vinnings skyld. Straffebudet sanksjonerer uberettiget befatning med tilgangsdata, og gjerningsbeskrivelsen inneholder derfor ikke noe vilkår om vinningsforsett eller vilkår om tap eller fare for tap. Det fremstår derfor som at selvstendig bruk av § 201 ikke er egnet til å utvise den klander som ellers blir utvist der en krenker en annens eiendomsrett for å oppnå en økonomisk vinning. Både når det kommer til straffeutmåling og straffebudet gjerningsbeskrivelse, fremstår § 201 lite egnet til å verne om de verdier kryptovaluta representerer.

Jeg er av derfor av en annen oppfatning enn den Justisdepartementet synes å inneha. Som nevnt ovenfor er det anført i Ot.Prp.nr.22 (2008-2009) at informasjon «nyter […] et indirekte vern ved disse bestemmelsene». Dette stemmer til en viss grad, ettersom uberettiget befatning med tilgangsdata er kriminalisert. Likevel synes ikke bestemmelsen å i tilstrekkelig grad å reflektere vinningsforsettet til gjerningspersonen og tapet eieren av kryptovalutaen lider, både på grunn av den relativt lave strafferammen og hva straffebudet er ment å verne.

5.3 §204. Innbrudd i datasystem

5.3.1 Gjerningsbeskrivelsen

§ 204 fastsetter at «den som ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystem eller del av det» kan straffes med bøter eller fengsel. Mens § 201 verner mot uberettiget befatning med «passord», «dataprogram», osv., verner § 204 mot uberettiget tilgang til et datasystem. Likt som i § 201, skal «datasystem» tolkes vidt, og teknologivalg skal ikke være avgjørende om en innretning er å regne som et «datasystem».[23]

[23] Schjølberg (2017) s. 57

Bestemmelsen oppstiller to alternative måter å begå et datainnbrudd. Alternativet «å bryte en beskyttelse» forutsetter at den berettigede har opprettet sikkerhetsmekanismer, som for eksempel passord og brukernavn, som skal verne dataene mot andres tilgang. Alternativet «ved annen uberettiget fremgangsmåte» dekker handlemåter der det ikke har skjedd et beskyttelsesbrudd, men der uvedkommende på andre måter har tatt seg uberettiget inn i et datasystem.

Etter bestemmelsen er det den uberettigede tilgangen i seg selv som er straffbar. Det er ikke noe krav om at informasjon er lastet ned eller kopiert. Det er heller ikke av betydning om gjerningspersonen har gjort seg kjent med dataene. Bestemmelsen verner om selve tilgangen til datasystemet, men ikke nødvendigvis dataene som er lagret der. I lovens forarbeider uttaler Justisdepartementet at «bestemmelsen bare verner informasjon indirekte ved å hindre tilgang til informasjonen, mens det som direkte straffes er den uautoriserte inntrenging i systemet».[24]

For typetilfelle 1 har person B brutt en «beskyttelse», passordbeskyttelsen person A hadde opprettet, og skaffet seg tilgang til et «datasystem», programvaren hvor kryptovalutaen til person A er lagret. Person B har derfor gjort seg skyldig i datainnbrudd, jf. § 204.

5.3.2 Graden av vern § 204 gir

Etter bestemmelsen kan person B straffes med bot eller fengsel inntil to år. På samme måte som § 201, er § 204 i liten grad egnet til å markere den fulle klander en slik handling fortjener. Strafferammen er relativt lav, sett opp mot straffebud som verner andres formue, som for eksempel § 322. En slik lav strafferamme er i mindre grad egnet til å virke avskrekkende for potensielle gjerningspersoner fra å krenke andres formue av stor verdi. Videre vil den lave strafferammen heller ikke i tilstrekkelig grad signalisere den kritikk slike handlinger fortjener. Slik som i § 201, er gjerningsbeskrivelsen i § 204 heller ikke dekkende for det som faktisk er gjort. Det vinningsforsett som person B innehar og det tap som person A har lidt, kommer ikke til uttrykk i bestemmelsens ordlyd. Slik Justisdepartementet har uttalt i Ot.Prp.nr.22 (2008-2009), nyter informasjon «et indirekte vern» ved denne bestemmelsen, men, som ved § 201, gir § 204 en nokså dårlig grad av beskyttelse.

[24] Ot.prp.nr. 22 (2008-2009) s. 403

6 § 351 annet ledd. Dataskadeverk.

6.1 Bakgrunnen for bestemmelsen

Før jeg går nærmere inn på graden av vern skadeverkbestemmelsen gir kryptovaluta i typetilfelle 1, er det relevant å se litt nærmere på bakgrunnen for denne bestemmelsen.

§ 291 i straffeloven av 1902, som var det tidligere straffebudet om skadeverk, omfattet også skadeverk på data. Bakgrunnen for innføringen av en egen bestemmelse om dataskadeverk, var at Straffelovkommisjonen og Datakrimutvalget anså det som «mindre tilfredsstillende at man ved spørsmålet om straffbarheten av slike handlinger må basere seg på en tolking av den alminnelige skadeverksbestemmelsen som etter ordlyden slett ikke er åpenbar».[25] Departementet sa seg enig i dette i Ot.prp.nr. 22 (2008-2009) på side 62. Behovet for en egen bestemmelse kan også utledes av Rt. 2004 s. 1619, der det ble uttalt av en samlet Høyesterett at «det vil være hensiktsmessig med lovregler som er spesielt utformet med tanke på datarelaterte overtredelser».[26]

Overnevnte høyesterettsavgjørelse omhandlet uberettiget endring av lagrede data, og om dette kunne anses som skadeverk. Selv om det i 2004 ikke fantes en egen bestemmelse for dataskadeverk, uttaler førstvoterende at «[e]tter min vurdering kan ikke den omstendighet at det nå er foreslått en egen straffebestemmelse om skadeverk på elektronisk lagret informasjon, ses som uttrykk for at vi ikke allerede i dag har hjemmel til å straffe skadeverk på datamaskiner i visse høve»[27]. Denne bemerkning fra førstvoterende i Høyesterett, fremstår ikke som en åpenbar tolkning av straffebestemmelsen. At det var foreslått en egen straffebestemmelse om skadeverk på elektronisk informasjon, kunne også blitt tolket helt motsatt. Selv om det var blitt foreslått en endring, som nevnt i kjennelsen i avs. 29, valgte førstvoterende å tolke den eksisterende straffebestemmelsen som en hjemmel til å straffe skadeverk på datamaskiner. Videre la førstvoterende vekt på at forarbeidene i lang tid hadde hatt uttalelser om at bestemmelsen om skadeverk også gjelder for tilfeller av endring eller

[25] NOU 2002:4 Ny straffelov, s. 325
[26] Avs. 29 i kjennelsen.
[27] Rt. 2004 s. 1619 avs. 29

sletting av elektronisk lagret informasjon og at det allerede i Rt. 1930 s. 1005 «ble gitt uttrykk for et funksjonelt syn på skadeverksbestemmelsen». Førstvoterende i 2004 saken tar det standpund at selv om det ikke var snakk om skadeverk på en «gjenstand» i tradisjonell forstand, tilsa forarbeidene og et funksjonelt syn på skadeverkbestemmelsen at kravet til lovbestemt hjemmel, etter Grl. § 96 og EMK art. 7, var oppfylt. Løsningen en enstemmig Høyesterett kom frem til i saken fra 2004 var, som nevnt, ikke opplagt, og viser etter mitt syn at Høyesterett bevisst valgte en tolkning som var nødvendig for at handlingen, den uberettigede endringen av lagrede data, skulle kunne rammes av straffebudet.

Ordlyden i bestemmelsen, «gjenstand», ekskluderer data som gjenstand for skadeverk, noe førstvoterende uttrykkelig anerkjenner i avsnitt 27. Selv om lagringsmediet dataen er lagret på, som for eksempel en datamaskin, er å regne som en «gjenstand», var faktum i saken at gjerningspersonen kun hadde endret selve dataen, mens selve lagringsmediet forble uendret i fysisk forstand. En funksjonell forståelse av gjenstandsbegrepet kan tilsi at når data på en maskin endres, endres også maskinen ettersom den ikke lenger inneholder den samme informasjonen og heller ikke er ubrukeliggjort. Ingen fysisk endring har skjedd, men det kan likevel ha skjedd en så vesentlig endring av maskinens indre karakter, at maskinen som en gjenstand, i realiteten har blitt endret. Dette synes å være det avgjørende argumentet. Det var ikke skaden på dataene i seg selv som var sentral, men dataenes funksjon overfor datasystemet. Endring av dataene medførte en endring av gjenstanden, som igjen var å regne som et skadeverk.

For å klargjøre dette skillet mellom «gjenstand» og «data» i forhold til skadeverk, ble det i 2013 gjennom endringslov av 21. juni 2013 nr. 85[28], gitt en tilføyelse til § 351 for å avklare rettstilstanden. Bestemmelsen var også et resultat av Norges forpliktelse etter konvensjonen mot datakriminalitet (2001) til å kriminalisere uberettiget skade eller endring av data[29]. Når det kommer til skadeverk etter § 351, ble «data» og «gjenstand» likestilt.

[28] Lov om endringer i straffeloven 1902 og straffeloven 2005 mv. (forberedelse av terror m.m)
[29] Konvensjon om datakriminalitet – ETS nr. 185, art. 4

6.2 Gjerningsbeskrivelsen

§ 351 bokstav b) fastsetter at «[f]or skadeverk straffes også den som uberettiget endrer, gjør tilføyelser til, ødelegger, sletter eller skjuler andres data». Hva som menes med «data» er ikke definert hverken i loven eller i forarbeidene, ettersom det er «vanskelig å utforme presise og dekkende definisjoner som samtidig er føyelige nok».[30] Det er likevel naturlig å ta utgangspunkt i Datakrimutvalget og konvensjonen sine definisjoner.[31]

Konvensjonen om datakriminalitet definerer data som «enhver framstilling av fakta, informasjon eller begrep i en form som er egnet for behandling i et datasystem, herunder et program som kan få et datasystem til å utføre en funksjon».[32] Datakrimutvalgets definisjon av data lyder: «[e]nhver representasjon av informasjon som lagres eller behandles av et datasystem eller som overføres i elektronisk kommunikasjonsnett. I tillegg omfattes enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk utstyr»[33]. Kryptovalutaen representerer informasjon som behandles av et datasystem. Det fremstår etter dette som rimelig klart at kryptovaluta er å regne som «data».. Kryptovaluta er derfor etter mitt syn omfattet av § 351 annet ledd.

Bokstav b) oppstiller fem alternative måter å begå dataskadeverk på. Alle alternativene omfattes av alternativet «endrer», kanskje med unntak av alternativet «sletter».[34] De øvrige alternativene er tatt med «av informative grunner for å klargjøre hva bestemmelsen omfatter».[35] Det mest nærliggende alternativet å bruke for typetilfelle 1, er uansett alternativet «endrer». Ettersom person B har foretatt seg handlinger inne på person A sin konto, ved å overføre kryptovalutaen til sin egen, må han nødvendigvis ha, på en eller annen måte, endret den data som var tilknyttet person A sin konto. Dette er fordi en slik overføring ikke ville skjedd dersom person B ikke hadde foretatt seg noe inne på person A sin konto. I et slikt tilfelle er det nokså klart at person B har endret data.

[30] Jf. Ot.prp. nr.22 (2008-2009) s. 21.
[31] Jacobsen, Husabø, Gröning, Strandbakken (2020), s. 187.
[32] Jf. Konvensjonen om datakriminalitet (2001), art. 1 b
[33] Jf. NOU 2007: 2 s. 175.
[34] Sunde (2016)
[35] Jf. NOU 2007: 2, s. 81

Det må videre være snakk om «andres data». Det avgjørende for dette vilkåret er «at noen andre enn gjerningspersonen har rettighetene til dataene».[36] For det tilfellet der noen har opprettet en konto for å handle med og lagre kryptovaluta, er det rimelig å hevde at denne personen har rettighetene til all kryptovaluta, og samtidig dataen, som ligger lagret på kontoen. Selv om dataen kryptovalutaen representer kun eksisterer på blokkjeden, er blokkjeden konstruert slik at det knyttes et eierskap til disse dataene. Blokkjeden fører i realiteten kun oversikt over hvem kryptoen er overført til og fra. På denne måten kan det heves at blokkjede teknologien gir en rettighet til å disponere over dataene. I tillegg, som forklart under punkt 3.2, regnes kryptovaluta som skattbar formue. Kryptovaluta tilknyttet person A sin kryptokonto er derfor, fra person B sitt ståsted, å regne som «andres data».

Videre må endringen være «uberettiget». Dette vilkåret gjøre det klart at dersom det foreligger et samtykke fra den berettigede, er det ikke snakk om et dataskadeverk. For typetilfelle 1 foreligger ikke et slikt samtykke fra person A. Ettersom «andres data» er uberettiget endret, kan det derfor konkluderes med at person B har gjort seg skyldig i dataskadeverk.

6.3 Grovt skadeverk

Ettersom person B har gjort seg skyldig i dataskadeverk, er det naturlig å drøfte om skadeverket er å anse som grovt, jf. § 352. Etter dette straffebudet skal det «ved avgjørelsen av om skadeverker er grovt» særlig legges vekt på «om skaden er av et stort omfang», jf. bokstav b). Ifølge forarbeidene sikter dette alternativet særlig til skadens økonomiske omfang.[37] Selv om alternativet ikke bruker utrykket «betydelig», sml. § 322 a), vil en skade som utgjør en «betydelig verdi», økonomisk sett, tale sterkt for at skadeverket er å regne som grovt. I HR-2021-2580-A ble det, i et spørsmål om det forelå «grovt bedrageri», jf. § 372, jf. § 371, fastsatt en grense på 1,5 G. Sett i lys av at § 351 har en lavere strafferamme enn § 371, er det nærliggende å legge til grunn at skadens omfang, økonomisk sett, i alle fall ikke bør settes høyere, men heller lavere, enn i forhold til grovt bedrageri. I typetilfelle 1 er skadeomfanget

[36] Jacobsen, Husabø, Gröning, Strandbakken (2020), s. 187.
[37] Ot.prp.nr. 22 (2008-2009), s. 458

på kr. 1.000.000. Dette er uansett langt over 1,5 G, som per april 2024 er kr. 118.620. Person B kan i dette tilfellet straffes for grovt dataskadeverk.

6.4 Graden av vern bestemmelsen gir

Når det kommer til strafferammen for grovt dataskadeverk, ligger denne på samme linje som andre grove formuesforbrytelser. Strafferammen for grovt dataskadeverk er «fengsel inntil 6 år», noe som for eksempel tilsvarer strafferammen for grovt tyveri, jf. § 322. Strafferammen i § 352, jf. § 351 annet ledd er derfor i større grad egnet til å utvise den skyld en slik krenkelse av en annens formue fortjener, enn §§ 201 og 204, når det kommer til straffereaksjonen.

I utgangspunktet kan det hevdes at § 352 b), jf. 351 annet ledd gir et godt vern for de økonomiske verdier kryptovaluta representerer. Selv om formålet med § 351 annet ledd var å klargjøre skillet mellom data og gjenstanden dataen er lagret på, kan det anføres at et resultat av dette skillet, ble at bestemmelsen direkte verner om «andres data». Slik som § 351, første ledd verner om andres formue, i form av «en gjenstand», kan det hevdes at annet ledd verner om andres formue i form av data. Det er likevel ikke et krav at gjenstanden etter bestemmelsens første ledd må ha økonomisk verdi. Det samme gjelder skadeverk av data etter § 351, andre ledd. I praksis vil de fleste gjenstander og data ha en større eller mindre økonomisk verdi, og det kan derfor hevdes at skadeverk etter bestemmelsens andre ledd, har som formål også å verne om andres formue. Selv om Sunde fremhever at formålet til bestemmelsen er «å styrke det generelle strafferettslige vernet for datasystemer og elektronisk kommunikasjon […]»[38], er jeg likevel av den oppfatning at bestemmelsens andre ledd gir et slags vern, ettersom den, i hvert fall indirekte eller som en konsekvens av ordlyden, verner andres data, som *kan* representere en økonomisk verdi.

På den andre siden treffer helheten av gjerningsbeskrivelsen dårlig i det tilfelle der en ønsker å tilegne seg de økonomiske verdier kryptovaluta representerer. Selv om det person B foretok seg kan anses som dataskadeverk i typetilfelle 1, hadde ikke person B som formål, i hvert fall

[38] Sunde (2016), s. 104.

ikke som hovedmotiv, å skade eller ødelegge dataen tilhørende person A. Han ønsket å tilegne seg dataen for å oppnå en økonomisk fordel for seg selv. Selv om det kan hevdes at gjerningsbeskrivelsen er egnet til å utvise den klander handlingen fortjener, ettersom data er endret, fremstår det for meg som at straffebudet i liten grad er egnet til å dekke hele den klanderverdige planen som ble gjennomført. Straffebudet tar hverken høyde for den vinning person B var ute etter eller det tap person A led. Gjerningsbeskrivelsen i § 351, annet ledd gir derfor et for lite rom til å utvise den fulle klander person A sin handling fortjener, sett i forhold til strafferammen i andre grove formuesstraffebud, og verner i liten grad kryptovaluta som formue.

7 § 371 bokstav b). Databedrageri

7.1 Generelt om bestemmelsen

Overskriften til § 371 – bedrageri - kan tyde på at en forutsetning for anvendelse av straffebudet, er at en person er bedratt eller lurt. Vanlig språklig forståelse av subjektet «bedrageri» er at det er en handling retten mot noen, altså det å bedra en (annen) person. For bokstav a) er dette tilfellet da det klart er presisert at den rettstridige handlingen er å forlede «noen». Bestemmelsens bokstav b) retter seg imidlertid mot en handling gjort overfor blant annet et «datasystem». Bokstav b) ble først tatt inn i straffeloven ved lovendring 12. juni 1987 nr. 54, med det formål å likestille de tilfeller der et datasystem blir manipulert, med tilfeller der en person blir manipulert. Bestemmelsen rammer handlinger som på ulike måter 'lurer' eller manipulerer et datasystem for egen vinning og som fører til tap eller fare for tap for «noen», det vil si en annen enn den som begår handlingen. Skillet mellom bokstav a og b er derfor om en person har blitt forledet eller lurt, ikke om handlingen involverer et datasystem.[39]

7.2 Gjerningsbeskrivelsen

7.2.1 Innledning

§ 371 bokstav b) fastsetter at «den som med forsett om å skaffe seg eller andre en uberettiget vinning b) […] endrer data eller datasystem […] eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen» kan straffes med bot eller fengsel inntil to år. Etter bokstav b) foreligger det to hovedvilkår som må oppfylles for å gjøre seg skyldig i et databedrageri. I tillegg til kravet om vinningsforsett, må gjerningspersonen uberettiget ha påvirket «resultatet av en automatisert databehandling». Det er listet opp flere eksempler på dette i lovteksten, og i praksis kan flere av disse passe på samme tilfelle[40]. Det andre hovedkravet er at handlingen må ha ført til «tap eller fare for tap for noen». Et databedrageri vil ofte medføre et tap eller fare for tap

[39] Sunde, (2016) s. 118.
[40] Jacobsen, Husabø, Gröning, Strandbakken, (2020), s. 230

umiddelbart etter at datasystemet- eller datamaskinen er 'lurt'.[41] Om det som er gjort i typetilfelle 1 kan regnes som et databedrageri, beror på en vurdering om en slik handling oppfyller de nevnte vilkår. Videre i 7.2.2 – 7.2.4 vil jeg vurdere om § 371 bokstav b) gjør seg gjeldende for typetilfelle 1.

7.2.2 «Uberettiget vinning» og vinningsforsett

Et sentralt gjerningselement i § 371, og andre formuesstraffebud, er vilkåret om at gjerningspersonen må ha forsett om å «skaffe seg eller andre en uberettiget vinning».[42] Selve begrepet «vinning» sikter til det å skaffe seg en økonomisk fordel. Det er klart at kryptovaluta representerer økonomiske verdier. Ettersom kryptovaluta er å regne som et formuesgode som man kan ha en eiendomsrett til, er det videre klart at det er mulig på en eller annen måte å krenke denne eiendomsretten. Vinningen må også være uberettiget. Dette betyr at gjerningspersonen ikke har noe rett på den økonomiske fordelen. For typetilfelle 1 er det klart at kryptovalutaen tilhørende person A er en økonomisk fordel som person B ikke hadde noen rett til.

Kravet om vinningsforsett dreier seg om at gjerningspersonen må ha til forsett å oppnå en økonomisk fordel for seg selv eller en annen. For typetilfelle 1 er det klart at vilkåret om vinningsforsett er oppfylt. Hensikten til person B var jo nettopp å skaffe seg en uberettiget vinning. Vinningen, den økonomiske verdien kryptoen representerer, er uberettiget fordi person A ikke hadde gitt samtykke til, eller inngått noen form for avtale om, at dette skulle overføres til person B, i typetilfelle 1.

[41] Ot.prp. 35 (1986-1987) s. 26.
[42] Jf. §§ 321, 327 og 371. § 324 om underslag bruker formuleringen «forsett om en uberettiget vinning for seg selv eller andre», men innholdet er det samme som i de øvrige straffebudene.

7.2.3 Tapsvilkåret

Kravet til årsakssammenheng er i utgangspunktet oppfylt dersom den krenkende handlingen har fått konsekvenser, et tap, som regnskapsmessig har påvirket fornærmedes samlede formue.[43] I den digitale verden oppstår det et tap eller fare for tap umiddelbart etter at data er påvirket. I Rt. 1994 s. 740 på side 741, viser Høyesterett til byrettens uttalelse om lovanvendelsen, hvor det siteres: «Etter rettens oppfatning var bedrageriet fullbyrdet allerede i det øyeblikk hun gikk inn i datasystemet og innmeldte kreditter og overtrekkslimiter. I det øyeblikk dette var gjort var adgangen åpen for å foreta belastninger på den ene eller annen måte, og banken var dermed påført fare for tap». Dette ble ansett av Høyesterett som riktig lovanvendelse. I typetilfelle 1, er det rimelig klart at person A har lidt et tap i det øyeklikk dataene ble endret slik at kryptovalutaen overføres fra den ene kontoen til den andre. Person A er ikke lengre i besittelse av kryptovalutaen og har derfor mistet tilgangen til den økonomiske verdien disse representerer. For typetilfelle 1 er tapsvilkåret oppfylt.

7.2.4 «på annen måte uberettiget påvirker resultatet av en automatisert databehandling»

Dette alternativet viser til at eksemplene som nevnes i bestemmelsen ikke er en uttømmende liste, ettersom det er gunstig med en teknologinøytral bestemmelse. Felles for alle alternativene er at data på en eller annen måte er «uberettiget» påvirket. Ordlyden i alternativet «endrer data» er nokså uproblematisk. En endring av data skjer der det er foretatt en manipulering av digitalt lagret informasjon, som ellers ikke ville forekommet dersom gjerningspersonen ikke hadde foretatt seg noe. Et eksempel på slik manipulasjon er beskrevet i Rt. 1991 s. 532. I denne saken hadde to ansatte i Bankenes Betalingssentral endret data knyttet til en pengeoverføring. De forsøkte å omdirigere et beløp til egne kontoer i utlandet. Andre eksempler kan være å hacke seg inn i nettbanken til en annen og overføre penger til seg selv. Endring av «datasystem» kan typisk være at programvare endres.

Om vi ser for oss typetilfelle 1: i det øyeblikk person B foretar seg handlinger inne på kontoen til person A og overfører verdiene til sin egen, er data manipulert. Dette eksempelet har mye

[43] Jacobsen, Husabø, Gröning, Strandbakken, (2020), s. 175

til felles med saken nevnt ovenfor i Rt. 1991 s. 532. Det er foretatt endringer av data slik at verdier ble uberettiget overført fra en konto til annen, og denne endringen ville ikke skjedd uten at person B foretok seg dette. Det tredje og siste vilkåret for at person B har gjort seg skyldig i et fullbyrdet databedrageri, er dermed oppfylt.

7.3 § 372. Grovt bedrageri

Som jeg konkluderte ovenfor, vil handlingen i typetilfelle 1 utgjøre et fullbyrdet databedrageri. § 372 fastsetter forhold som vil være av betydning for om bedrageriet skal anses som grovt. Lovens ordlyd gir klart uttrykk for at det «særlig [skal] legges vekt på» de forhold som er nevnt i bokstavene a) til g). Det første momentet fastsatt i bokstav a), er om «det har hatt til følge en betydelig økonomisk skade». Dette må ses i sammenheng med tapsvilkåret i § 371. Som nevnt under punkt 6.3 har Høyesterett fastsatt en grense for hva som skal regne som «betydelig økonomisk skade», på 1,5 G. For typetilfelle 1, der person A har lidt et tap på kr. 1.000.000, fremstår det klart at dette er å regne som en «betydelig økonomisk skade», og person B har gjort seg skyldig i et grovt databedrageri. Person B kan dermed straffes til fengsel inntil seks år.

7.4 Graden av vern bestemmelsen gir

I motsetning til de nevnte straffebud i straffeloven kapittel 21 og straffebudet om dataskadeverk, er gjerningsbeskrivelsen i straffebudet § 371 b) dekkende for person B sine handlinger som er klanderverdige, nemlig person B sitt vinningsforsett og det økonomiske tapet for person A. § 372 a) utrykker den klanderen handlingen fortjener, ettersom bestemmelsen åpner for ytterligere klander med tanke på tapets størrelse. For typetilfelle 1, der person B endret data med vinningsforsett og person A lider et større økonomisk tap som følge av dette, gir derfor § 372 a), jf. § 371 b) tilstrekkelig hjemmel for å dekke de klanderverdige elementer av person B sin handling. Strafferammen for grovt databedrageri er, som nevnt ovenfor, fengsel inntil seks år. Dette er på samme nivå som andre formuesforbrytelser der det dreier seg om større verdier. Straffebudet om databedrageri gir derfor et godt vern for de økonomiske interesser kryptovaluta representerer i typetilfelle 1.

7.5 Forsøk på databedrageri

I tillegg til det vern som § 371 b) gir kryptovaluta i typetilfelle 1, vil jeg se nærmere på om forsøksbestemmelsen i § 16 kan anvendes for typetilfelle 2. I dette tilfellet vil ikke bedrageribestemmelsen gjøre seg gjeldende ettersom data, et datasystem eller «en automatisert databehandling», ikke er uberettiget endret på dette stadiet i hendelsesforløpet. Det er kun stjålet en harddisk med det forsett å ta den med seg og tømme denne for verdi på et senere tidspunkt. Ettersom det ikke foreligger et fullbyrdet databedrageri, vil spørsmålet være om vilkårene for forsøk i § 16 kan anses oppfylt i typetilfelle 2.

§ 16 fastsetter at «[d]en som har forsett om å fullbyrde et lovbrudd som kan medføre fengsel i 1 år eller mer, og som foretar noe som leder direkte mot utføringen, straffes for forsøk, når ikke annet er bestemt». Forsøksbestemmelsen er derfor relevant å vurdere nærmere i forhold til typetilfelle 2. Forsøksbestemmelsen er kun relevant når et lovbrudd ikke er fullbyrdet. Forsøksbestemmelsen oppstiller to inngangsvilkår. Før det første må det aktuelle lovbruddet kunne medføre fengsel i 1 år eller mer, «når ikke annet er bestemt». Unntaket gir uttrykk for at utgangspunktet kan fravikes, jf. også bestemmelsen i § 1. For det andre må den aktuelle bestemmelsen ikke gi et unntak for forsøksansvar. Begge disse vilkårene er oppfylt i forhold til bedrageribestemmelsen. I tillegg til disse vilkårene, er det i hovedsak to vilkår som må oppfylles for å kunne bli straffet for forsøk på et lovbrudd. Det første er at gjerningspersonen må ha hatt «forsett om å fullbyrde et lovbrudd». Dette kan beskrives som at gjerningspersonen ville noe mer enn det som allerede var gjort. Dette forsettet må dekke alle elementene som er del av straffebudet. I typetilfelle 2, er det klart at person B har et forsett om «å skaffe seg […] en uberettiget vinning». Videre er det klart at vedkommende hadde forsett om å «endre data», ettersom overføring av den lagrede kryptovalutaen fra harddisken til sin egen maskin, rent faktisk endrer den dataen som er på disken. Om endringen hadde blitt gjennomført, er det videre klart at dette hadde voldt et tap for eieren av kryptovalutaen, jf. § 371 b).

Det andre vilkåret som må være oppfylt er at gjerningspersonen må ha foretatt seg «noe som leder direkte mot utføringen». I dette ligger det at gjerningspersonen må ha gjort noe mer enn

å ønske å utføre forbrytelsen. Det er ikke nok at gjerningspersonen har besluttet å fullbyrde et straffebud, men denne viljen må omgjøres til handling. I typetilfelle 2 har person B borttatt harddisken og tatt den med seg for å tømme den. Likevel har han ikke rukket å endre dataen. Ettersom det ikke er noe vilkår for databedrageri å ha borttatt en datalagringsenhet, kan det stilles spørsmål ved om gjerningspersonen i dette tilfellet i det hele tatt har påbegynt et eventuelt databedrageri.

Dommen i Rt. 1991 s. 532, også nevnt i 7.2.4 ovenfor, omhandler forsøk på databedrageri i henhold til den tidligere straffelov av 1902, § 270, første ledd, nr. 2 (som var den tidligere bestemmelse om databedrageri). Her hadde to ansatte i Bankenes Betalingssentral instruert oppgjørssystemet til å overføre flere beløp til sine egne konti i utlandet. Grunnet tilfeldigheter, blant annet ved ett av beløpenes størrelse, ble det iverksatt nærmere undersøkelser noe som førte til at manipulasjonen av dataene ble avdekket og transaksjonene stanset før gjennomføring. Høyesterett uttalte at de to gjerningspersonene ikke kunne dømmes for fullbyrdet databedrageri, kun for forsøk, fordi manipulasjonen, den uriktige dataen som var matet inn i oppgjørssystemet, ikke var å anse som et fullbyrdet databedrageri etter § 270 nr. 2. For typetilfelle 2, er situasjonen derimot en annen enn den i overnevnte dom. På det tidspunkt person B ble avslørt, hadde han kun harddisken i sin besittelse og forsett om å «endre data» på denne. Det kan derfor stilles spørsmål ved om dette er nok til å ha passert den nedre grensen for forsøk og dermed kan komme i ansvar. Spørsmålet blir da om man kan gjøre seg skyldig i forsøk på databedrageri selv om dataen ikke er endret. Dette spørsmål knytter seg til hvor den nedre grensen for forsøk går.

7.5.1 Den nedre grensen for forsøk

Hvor den nedre grensen for forsøk går der gjerningspersonen har gjenstående ting å utføre ut ifra planen sin og ikke har begynt å oppfylle deler av gjerningsbeskrivelsen, er vanskelig å si noe konkret om. Ordlyden «foretar noe som leder direkte mot», er i utgangspunktet lite veiledende for hvor mye som skal til av en forberedende handling for å oppfylle dette vilkåret. Av rettspraksis følger det at vurderingen beror på en helhetsvurdering hvor både subjektive og objektive forhold kan vektlegges. I Rt. 2008 s. 867, i avsnitt 20, ble det listet opp en rekke momenter som inngår i denne vurderingen: «Ved denne vurderingen må det blant annet legges

vekt på den tidsmessige nærhet mellom det som er gjort, og det som gjenstår, handlingenes karakter og den psykologiske forskjell mellom dem».

For typetilfelle 2 kan det legges til grunn at person B sin plan var å ta harddisken med hjem, og dagen etter borttakelsen skulle han koble denne til sin egen datamaskin for å tømme den for verdier, altså «endre data». Den «psykologiske forskjell» mellom borttakelsen og tilkoblingen av harddisken synes å være nokså liten. Dette kan beskrives som en slags psykologisk terskel som vil måtte passere for å gå videre fra de handlinger som er gjort, til å fullbyrde forbrytelsen.[44] Harddisken er allerede fratatt person A og den gjenværende handlingen, for person B, som vil fullbyrde forbrytelsen, er å koble denne til en datamaskin og overføre verdiene. Læren om den psykologisk forskjell har imidlertid blitt kritisert ettersom den forutsetter at man kan sette seg inn i rollen som gjerningsperson.[45] Selv om man skulle legge avgjørende vekt på den psykologiske forskjellen mellom det som er gjort og det som gjenstår, er det i typetilfelle 2, en nokså liten barriere som må passeres.

Tiden som gjenstår til fullbyrdelse av databedrageriet i typetilfelle 2, er én dag. Det er ikke noe klart svar på hvor kort tid som må gå mellom det som er utført og det som gjenstår, for å utløse straffeansvar. Noen former for bedrageri krever betydelig planlegging og forberedelser, mens i andre tilfeller oppstår fullbyrdelsesforsettet spontant og kan gjennomføres på svært kort tid. Tidsaspektet kan derfor ikke alene gi svar på om straffeansvar har inntrådt. I typetilfelle 2, oppstod fullbyrdelsesforsettet dagen før, og den første innledende handlingen til å gjennomføre bedrageriet er gjennomført, nemlig å bortta harddisken. Tidsskillet mellom den fullførte forberedelsen og fullbyrdelsen er da så liten at det etter min vurdering kan anføres at person B har passert den nedre grense for straffbart forsøk. På den andre siden oppstod person B sin plan nokså spontant. Han så en mulighet til å relativt enkelt og på kort tid å tilegne seg de verdier som var lagret på harddisken. Planen hans krevde få forberedelser og kunne derfor gjennomføres raskt. For andre forbrytelser som krever langsiktig planlegging og forberedelser, som for eksempel spionasje, kan man pådra seg straffeansvar under forberedelsesstadiet, ettersom fullbyrdelse ofte krever et lengre tidsperspektiv. I Rt. 1991 s. 95 hadde den tiltalte gjort betydelige forberedelser, men det gjenstod likevel noen dager før

[44] NOU 1992: 23, s. 82
[45] Gröning, Husabø, Jacobsen, (2023), s. 376, fotnote 1726

bedrageriet kunne gjennomføres. Tiltalte ble likevel dømt for forsøk på bedrageri. Generelt kan man si at der det er gjort omfattende forberedelser, men det gjenstår en del tid før forbrytelsen kan gjennomføres, vil man kunne dømmes for straffbart forsøk. Jeg er av den oppfatning at selv om person B sin handlingsplan oppstod spontant og krevde få forberedelser, taler den korte tiden mellom borttakelsen og muligheten for endringen av dataen for at det foreligger et straffbart forsøk.

For typetilfelle 2 er det lite som gjenstår for å oppfylle gjerningsbeskrivelsen. Det eneste som gjenstår for person B er å koble til disken og «endre dataen». I Rt. 1996 s. 766 ble to personer dømt for forsøk på ran. I denne saken hadde gjerningspersonene gjort omfattende forberedelser i form av å stjele en bil, tatt med tåregass og et uladd våpen. Det siste som gjenstod, var at ransofferet skulle dukke opp. Her var nærheten av alt som var gjort, til det som gjenstod, så liten at de tiltalte ble funnet skyldig. I deres plan var det meste av det som måtte gjøres, allerede gjennomført. I tilfellet der en borttar en harddisk for «endre data» på den den, kan det stilles spørsmål ved hvor mange «ledd» et slikt databedrageri inneholder. Dette er vanskelig å si noe generelt om ettersom det finnes flere fremgangsmåter for å begå disse. Det kan likevel argumenteres for at det kun gjenstår få vesentlig skritt for å fullbyrde lovbruddet. Etter at person B har tatt med seg harddisken hjem til seg, gjenstår det få enkle skritt i vedkommendes plan, nemlig å koble denne til sin datamaskin, taste inn passord og overføre verdiene.

Handlingens karakter er i teorien omtalt som en sammenheng mellom det som er gjort og det som gjenstår. Om en gjerningsperson allerede har oppfylt ett eller flere gjerningselementer, eller foretatt ulovlige handlinger som en del av forberedelsen, kan være et karaktertrekk på at forsøksgrensen er passert.[46] I typetilfelle 2 har ikke gjerningspersonen enda begynt på handlinger som oppfyller gjerningsbeskrivelsen, ettersom data ikke er endret. Det kan her trekkes en parallell til tyveribestemmelsen, og hvor lite flytting av gjenstanden som skal til før et tyveri kan regnes som fullbyrdet.

[46] Ibid, s. 376

I eldre rettspraksis ble det oppstilt en nokså lav terskel for når et tyveri kan regnes som fullbyrdet. I Rt. 1894 s. 484 kom Høyesterett frem til at var det tilstrekkelig at et kjøttlår var flyttet ut av en tønne og lagt på en annen. Denne linjen ble videreført i straffeloven av 1902 og lagt til grunn i flere avgjørelser avsagt i Høyesterett mange tiår etter. I Rt. 1965 s. 223 hadde to personer tatt seg inn i et havnelager og flyttet noen kartonger med vin bort til en dør, med den hensikt å ta dem med seg. Også i Rt. 1971 s. 667 var det tilstrekkelig for fullbyrdet tyveri at gjerningspersonen hadde samlet en del varer i en haug på butikkgulvet. Den sentrale tanken synes å være at gjerningspersonen har større kontroll på gjenstanden enn eierens rådighet. For databedrageri er det ikke et krav om besittelseskrenkelse av en gjenstand, men det er likevel relevant at det for tyveribestemmelsen skal svært lite til før tyveriet er fullbyrdet. I typetilfelle 2 har person B en større rådighet over harddisken enn person A, og denne rådighetsoverføringen var helt nødvendig for person B sin videre plan.

Selv om data ikke er endret, har person B lagt alt til rette for å fullbyrde forbrytelsen. Vedkommende har allerede gjort seg skyldig besittelseskrenkelse[47], og fratatt eieren tilgang til verdiene sine. Det kan likevel stilles spørsmål ved om dette setter grensen for databedrageri for lavt. Før det første, i motsetning til overnevnte dom, Rt. 1991 s. 532, er data ennå ikke endret. Person B har ikke engang begynt å fullbyrde forbrytelsen. På den andre siden har Høyesterett i Rt. 2010 s. 1011 slått fast at den nedre grensen for forsøk kan være passert selv om det gjenstod flere viktige skritt. Saken omhandlet tilvirkning av narkotika, og var av et så stort omfang og profesjonell karakter at tiltale ble dømt for forsøk. Selv typetilfelle 2 ikke er av en slik karakter som i overnevnte dom, er det relativt lite som gjenstår for person B i typetilfelle 2, før databedrageriet er fullbyrdet. Selv om det ikke er mange fysiske handlinger som gjenstår, er det i grunnen få, relativt enkle handlinger som gjør at forbrytelsen blir fullbyrdet, som kan gjøres raskt uten andre forberedelser. Når dette er gjort vil, data være endret, vinningen oppnådd og tap påført person A.

Slik jeg ser det er det mye som tilsier at person B har gjort seg skyldig i forsøk på databedrageri. Det sentrale for dette standpunktet er at person B allerede har gjort seg skyldig i besittelseskrenkelse og det er svært lite i planen til vedkommende som gjenstår for å

[47] Dette kommer jeg nærmere inn på under punkt 8.2.2

fullbyrde databedrageriet. Jeg mener derfor at borttakelsen av harddisken med forsett om å gjennomføre et databedrageri, er å regne som et forsøk på databedrageri.

Videre kan det stilles spørsmål ved om et slikt forsøk er å regne som et forsøk på grovt databedrageri, jf. § 372 a). Ordlyden av bokstav a), «det har hatt til følge en betydelig økonomisk skade», kan isolert sett tilsi at en skade faktisk må ha oppstått. En slik tolkning er det likevel ikke støtte for i rettskildene. I Rt. 1991 s. 532 ble de to tiltale dømt for forsøk på grovt bedrageri, selv om det ikke forelå noe økonomisk skade. I tillegg fastsetter bestemmelsens første ledd at det kun skal «særlig legges vekt på» de følgende alternativer. At en skade faktisk har oppstått, er derfor ikke et vilkår for å gjøre seg skyldig i forsøk på databedrageri. Som nevnt ovenfor i punkt 7.3, har Høyesterett fastsatt en grense på 1,5 G, og verdiene det er snakk om i typetilfelle 2 er kr. 1.000.000. Dersom person B sine handlinger er å regne som et straffbart forsøk, vil det i så fall være et forsøk på grovt databedrageri.

7.5.2 Graden av vern bedrageri- og forsøksbestemmelsen gir

Selv i det tilfellet hvor overføringen av kryptovalutaen ennå ikke har skjedd, kan forsøksbestemmelsen gi verdien av kryptovaluta et vern på lik linje med de tilfeller der disse faktisk er overført. Om hendelsesforløpet i typetilfelle 2 kan regnes som et straffbart forsøk på grovt databedrageri, er de økonomiske verdiene som ligger i kryptovaluta godt vernet ettersom gjerningsbeskrivelsen i §§ 372, jf. 371 og forsøksbestemmelsen dekker person B sine handlinger.

Når det kommer til straffeutmålingen gir § 16 ingen ramme for straffenivået for forsøkshandlinger, men § 80 første ledd bokstav b) fastsetter at straffen kan settes under minstestraffen. Bestemmelsen gir kun en mulighet for dette, og det er derfor ikke et krav om at straffen settes under minstestraffen. Om person B kan straffes med bot eller fengsel inntil 6 år, jf. § 371, er vanskelig å si noe konkret om. I Rt. 2011 s. 1013 ble det uttalt at det ikke kan oppstilles «faste normer for kva ein slik reduksjon skal vere. Til det vil omstenda, ikkje minst ved forsøkshandlinga, kunne variere for mykje»[48]. Matningsdal uttaler i forbindelse med

[48] Avs. 19

dommen at «[d]et overordnede synspunktet i denne dommen er at man ved utmålingen av straff for forsøk må ta utgangspunkt i hvor stor andel av de momentene som begrunner straffenivået ved fullbyrdet overtredelse av straffebudet allerede er realisert».[49]

Begrunnelsen for strafferammen ved grovt databedrageri er den økonomiske konsekvens slike handlinger kan ha. En krenkelse av person A sin formue har allerede matrealisert seg, ved at person B tok fra ham harddisken. Det tas med i vurderingen om straffeutmåling at forsøket var kommet nokså langt: harddisken var ute av person A sin kontroll, og det gjenstod kun å endre dataen på harddisken for person B. Videre må det legges vekt på at skadevirkningen forsøket hadde, var betydelig. Person A ble fratatt tilgangen til et formuesgode av stor verdi. Dette tilsier at straffen ikke bør settes under minstestraffen. På den andre siden, rakk aldri person B å overføre verdien til seg selv, og ettersom harddisken med alle verdiene ble levert tilbake til person A, ble formuen tilbake ført i sin helhet. Dataen som var lagret på harddisken ble heller aldri endret, og derfor kan det anføres at det § 371 b) er ment å verne, nemlig data, aldri ble utsatt for en krenkelse.

Ettersom et forsøk alltid skal betraktes som en formildende omstendighet, jf. § 78 a), mener jeg at straffen for person B bør ligge på linje med straffen satt i rettsavgjørelser som omhandlet forsøk på grovt databedrageri, justert etter beløpet det gjaldt. I Rt. 1991 s. 532 ble straffen satt til fengsel i to år samt en bot. En slik strafferamme gir et godt vern for de den økonomiske verdier kryptovaluta representerer.

[49] Matningsdal, Juridika, kommentar til § 78 a, note 2.2.1

8 Tyveri og tilgrensende vinningsstraffebud

8.1 § 321. Tyveri

8.1.1 Gjerningsbeskrivelsen

§ 321 fastsetter at «den som tar en gjenstand som tilhører en annen, med forsett om å skaffe seg eller andre en uberettiget vinning ved å selge, forbruke eller på annen måte tilegne seg den» kan straffes for tyveri med bot eller fengsel inntil to år. Straffebudet verner om eiendomsretten til sine egne ting. Bestemmelsen oppstiller et dobbelt videregående forsett som innebærer at gjerningspersonen må 1) ha forsett om å tilegne seg tingen og 2) forsett om deretter å oppnå en uberettiget vinning. Av § 22 følger det at gjerningspersonens forsett må dekke alle elementene i straffebudet. Dette innebærer at gjerningspersonen må ha forsett om å tilegne seg tingen, at tingen var i en annens eie og besittelse og at den ble tatt fra en annens besittelse. Ettersom det som er gjort av person B i typetilfelle 2 innebærer borttakelse av en gjenstand, anser jeg det som relevant å se nærmere på om tyveribestemmelsen gjør seg gjeldende, og eventuelt i hvilken grad den beskytter den formue kryptovaluta representerer.

8.1.2 «Gjenstand»

Før jeg drøfter vilkårene om tilegnelse- og vinningsforsett er det relevant å vurdere hva som er gjerningsobjektet i tyveribestemmelsen.

Det fremgår av ordlyden at straffebudet verner om eiendomsretten til en «gjenstand». Straffeloven inneholder ingen legaldefinisjon av gjenstandsbegrepet, men det har likevel en alminnelig språklig betydning: det omfatter i utgangspunktet alle ting, både fast eiendom og løsøre. Ettersom det ikke er praktisk mulig å bortta en fast eiendom, må «gjenstand» i § 321 forstås som løsøregjenstand. Dette omfatter alle fysiske rørlige ting. Forarbeidene til bestemmelsen uttaler at «gjenstand» ikke omfatter alle formuesgoder. «Penger er eksempelvis

en gjenstand, mens immaterielle rettigheter ikke er det»[50]. Ut ifra sammenhengen må «penger» her forstås som kontanter, sedler og mynter. Immaterielle rettigheter, som opphavsrett til åndsverk, er av en ikke-materiell karakter. Slike rettigheter knytter seg til intellektuell eiendomsrett, og kan derfor ikke regnes som en «gjenstand», nettopp fordi eiendomsretten ikke er knyttet til en fysisk ting. Selv om en skulle stjele dokumentet der en slik rett var nedfelt, vil en ikke krenke opphavsretten i seg selv.

I typetilfelle 2, der en harddisk som inneholder kryptovaluta blir borttatt, er det ingen tvil om at selve harddisken er å regne som en «gjenstand». Etter straffebudet er i alle fall harddisken i fokus for selve tyveriet, men dataen som forsvinner ut av eierens besittelse, skjer naturligvis samtidig og som en følge av dette. Det kan stilles spørsmål ved om dataen lagret på harddisken også er å regne som en «gjenstand» på lik linje med fysiske ting. Her er det ulike syn i rettskildene.

I NOU 1985:31 drøftes det om data kan anses som en gjenstand i bestemmelsen om skadeverk. Det er uttalt at «[e]tter alminnelig språkbruk må en gjenstand være av fysisk beskaffenhet, slik at immaterielle objekter faller utenfor begrepet. Rent fysisk er lagrede data bare magnetiske impulser, og den informasjon dataene representerer, er selvsagt av utpreget immateriell karakter».[51] Det uttales likevel at det ikke er grunnlag for å anse skadeverk mot «manuelle registre» som annerledes enn skadeverk mot «EDB-teknikk» (elektronisk databehandling). Straffelovrådet anså det likevel som utelukket at data skulle anses som «gjenstand». Dette synet på data i forhold til gjenstandsbegrepet ble lagt til grunn som korrekt i Ot.prp.nr.35 (1986-1987) på side 8, under punkt 3.2.

Uttalelsene fra overnevnte utredning ble anvendt i Rt. 2004 s. 1619, omtalt i punkt 6.1. I kjennelsen kom Høyesterett til at skadeverk på dataene tilknyttet en datamaskin, fører til at selve datamaskinen også endres, og på den måten er det begått skadeverk på en «gjenstand». Høyesterett sin tolking av gjenstandsbegrepet var i tråd med synet som ble lagt frem i NOU 1985:31 og det funksjonelle gjenstandsbegrepet i henhold til «damluke-dommen» i Rt. 1930

[50] Ot.prp.nr.22 (2008-2009) s. 280
[51] NOU 1985:31 s. 9

s. 1005. Selv om dataen i kjennelsen fra 2004 var det som ble skadet, ble dette likevel regnet som skadeverk på lagringsmediet, ettersom dataen var en så sentral del av lagringsmediet.

I juridisk teori er det funksjonelle gjenstandsbegrepet Høyesterett brukte, kritisert. Inger Marie Sunde (2006) påpeker flere svakheter ved dette synet. Det er uttalt at en slik tilnærming er dårlig i «samsvar med datasikkerhetskrav som gjelder data og datatjenester» og «når det ikke egentlig er det fysiske utstyret som er objektet, leder det funksjonelle gjenstandsbegrepet til en begrunnelse for straff som treffer på siden av krenkelsen.» [52]. Det er også påpekt at det å hevde at lagringsmediet er skadet når det er dataene som har vært uberettiget påvirket, er en søkt slutning. Problemstillingen Høyesterett stod ovenfor i Rt. 2004 s. 1619, «gjaldt først og fremst hvorvidt skadevilkåret var oppfylt når endringene ikke hadde rammet den vanlige brukerfunksjonaliteten i de angrepne anleggene.»[53] Høyesterett trengte derfor ikke å ta stilling til om data kunne regnes som «gjenstand», og Sunde legger til grunn at dette spørsmålet forble åpent i forhold til skadeverkbestemmelsen. Dette er jeg enig i. Dommen rettet seg mot spørsmålet om skadeverk av en «gjenstand», ikke nødvendigvis mot straffbarheten av skade på data. At data ble skadet eller slettet, var kun en måte å begå skadeverk av en gjenstand på.

Gitt det manglende svar på spørsmålet om den strafferettslige betydningen av gjenstandsbegrepet i forhold til data i kjennelsen fra 2004, antar Sunde at rettstilstanden er slik at data er omfattet av gjenstandsbegrepet. Selv om NOU 1985:31 taler direkte mot dette, trekker Sunde frem flere vesentlige mangler i utredningen. For det første ble det ikke tatt hensyn til de nye problemstillingene som følge av den teknologiske utviklingen. Utviklingen hadde skapt et behov for å anse data som gjenstand. For det andre ble det ikke gitt en tilstrekkelig karakteristikk av hva data er. Det ble kun definert som «magnetiske impulser». For det tredje var konklusjonen som ble trukket i utredningen, i stor grad basert på analogi forankret i svært gamle rettsoppfatninger. Høyesteretts kjennelse av 29. september 1928 står sentralt i drøftelsen i utredningen. Kjennelsen omhandler en uberettiget overføring av en fordring tilhørende en herredskasserer. I saken kom Høyesterett frem til at begrepet gjenstand kun omfattet fysiske ting. Straffelovrådet trakk da en analogi mellom fordring og data, og konkluderte derfor med at data ikke er å regne som gjenstand. Denne analogien var sentral for

[52] Sunde, Lov og rett i cyberspace, 2006, s. 101-102
[53] Ibid, s. 104

konklusjonen, og Sunde påpeker at avgjørelsen fra 1928 har vært trukket lenger, enn det har vært grunnlag for.

I hennes doktoravhandling argumenterer Sunde videre for at data er å regne som «gjenstand».[54] Hun anfører at det ut ifra lovgiverviljen er naturlig å anse data som gjenstand, ettersom begrepet brukes i bestemmelser som verner om en eiendomsrett og det vil stride mot loven formål om noe som etter sin art kan eies, faller utenfor begrepet.[55] Dette synspunktet er jeg kun delvis enig i. Ettersom det er mulig å ha eiendomsrett til data, kan det være naturlig å anse data som «gjenstand». Jeg er likevel noe kritisk til påstanden om at dette følger av lovgivers vilje. For det første har hverken forarbeidene eller rettspraksis konkludert med at data er å regne som gjenstand, og for det andre har lovgiver aldri uttalt at data faller inn under det strafferettslige gjenstandsbegrepet. Videre anføres det at det ikke er noe språklig problem å «henføre data under «gjenstand»», fordi «man med «data» mener elektroniske signaler, og at det er elektroniske signaler som kan identifiseres og som man har under kontroll, for eksempel en konkret fil i filsystemet under «mine dokumenter», med en bestemt plass rent fysisk på serveren, med et filnavn, og med en størrelse (bytes)».[56] Jeg er av en annen oppfatning. Selv om data kan identifiseres, kontrolleres og har en størrelse på samme måte som fysiske gjenstander, har begrepet «gjenstand» en allmennspråklig betydning. Det brukes i dagligtalen om fysisk rørlige ting. Dersom data er å regne som «gjenstand», oppstår det, slik jeg ser det, et nytt problem. Begrepet «gjenstand» må forstås som «løsøregjenstand», og etter min oppfatning er data enda lengre unna dette begrepet. En slik tolkning av disse begrepene er så utvidende at det samsvarer dårlig med legalitetsprinsippet i strafferetten. Det kan i tillegg trekkes en parallell til § 12, som inkluderer «elektrisk energi eller annen energi» som «gjenstand». Bestemmelsen er tilsvarende i innhold som straffeloven 1902, § 6, og ble tatt inn i loven for å understreke at rettstridig tilegnelse av elektrisitet også rammes av straffelovens formuesstraffebud.[57] Dette kan tilsi at lovgiver anså det som nødvendig å definere strøm som en gjenstand, ettersom det ikke er naturlig å betrakte strøm som en gjenstand etter ordlyden. Jeg mener det samme gjelder for data. Slik som strøm, anser jeg det som unaturlig å anse data som «gjenstand».

[54] Sunde, Automatisert inndragning, doktorgradsavhandling (PhD) nr. 37 ved det juridiske fakultet, Universitetet i Osl0. Utgitt i Copmlex 3/11, Senter for rettsinformatikk, s. 178.
[55] Ibid, s. 177.
[56] Ibid.
[57] Indst. O. I. (1901/1902) s. 29

Spørsmålet om data er omfattet av gjenstandsbegrepet er, slik jeg ser det, et ubesvart spørsmål. På den ene siden er NOU 1985:31 og Ot.prp.nr.35 (1986-1987) klar på at data ikke er å regne som gjenstand. Kjennelsen fra 2004 gjentar dette og bygger i stor grad på argumentasjonen i utredningen. I tillegg ble forslaget som kriminaliserer datatyveri ikke fulgt opp, med den begrunnelse at data nyter et indirekte vern gjennom andre bestemmelser. Dette taler for at data ikke er å regne som gjenstand. På den andre siden er det påpekt av Sunde at det rådende synet på data som gjenstand, som kom frem i utredningen av 1985, er utdatert, lider av en manglende forståelse av hva data er i dag, og bygger på svært gamle rettsoppfatninger og analogier det ikke var grunnlag for. Selv om Sunde er kritisk til den gjeldende rettsoppfatningen om hvordan data er definert, kan dette etter mitt syn ikke veie opp for det faktum at lovgiver ikke eksplisitt har slått fast at data er å regne som en gjenstand. Det kan også stilles spørsmål om hvorfor Sunde, i hennes kritikk, ikke nevner proposisjonen fra 1986-1987. Denne har større rettskildemessig vekt enn utredningen, og ettersom proposisjonen gjentar standpunktet til Straffelovrådet, er jeg noe kritisk til hennes utsagn om at «den eneste rettskilden som med styrke taler imot et slikt resultat [, (at data er omfattet av det strafferettslige gjenstandsbegrepet),] er den nevnte utredningen […]».

Selv om det finnes gode argumenter for å kritisere utredelsen fra 1985 og Høyesteretts bruk av denne samt lovgivers passivitet de senere år rundt data og gjenstand, må dette likevel vurderes opp mot det faktum at lovgiver ikke har konkludert entydig med at data er å regne som gjenstand. Jeg mener man skal utvise tilbakeholdenhet med å foreta denne type utvidende tolkning av straffebudet, og gjenstandsbegrepet for øvrig. Frem til lovgiveren – Stortinget- tar stilling til dette spesifikke spørsmålet, bør data, etter mitt syn, ikke anses å være omfattet av det strafferettslige gjenstandsbegrepet.[58]

Dersom vi legger til grunn data ikke kan regnes som en «gjenstand», vil det, i typetilfelle 2, kun være harddisken som er omfattet av begrepet «gjenstand» tyveribestemmelsen, jf. § 321. Dataen følger kun med som en konsekvens av borttagelsen. Om det er hensiktsmessig å skille mellom dataen og innholdet på denne måten, er ikke opplagt. Jeg mener likevel at for og

[58] Andre teoretikere er av samme oppfatning, at data ikke er omfattet av gjenstandsbegrepet, se Jacobsen, Husabø, Gröning, Strandbakken (2020), s. 168

typetilfelle 2 er det nødvendig å skille dem, ettersom tyveribestemmelsen retter seg mot gjenstander, som en harddisk er, og ikke hva som er lagret på den. Dersom det som er lagret på den, ikke er å regne som en gjenstand, faller borttagelsen av dataen utenfor straffebudet i § 321.

Realiteten er likevel at selv om dataen i seg selv ikke kan være en «gjenstand» for et tyveri, er det likevel klart at det var dataen gjerningspersonen var ute etter, ikke harddisken i seg selv. Det kan dermed stilles spørsmål om hvordan en slik situasjon knytter seg opp mot vilkåret om tilegnelsesforsett og vinningsforsett.

8.1.3 Tilegnelsesforsett og vinningsforsett

Som nevnt ovenfor under punkt 7.2.1, vil en gjerningsperson som har forsett om å berike seg selv ved å få tak i andres kryptovaluta uten samtykke, ha oppfylt kravet om vinningsforsett. Selv om ikke person B hadde tenkt til å beholde disken etter borttakelsen, er dette ikke relevant for om det foreligger vinningsforsett eller ikke. I Rt. 2012 s. 1669, som gjaldt datainnbrudd, uttalte førstvoterende i avsnitt 35 at «[d]et er generelt lagt til grunn at når en person uberettiget skaffer seg goder med økonomisk verdi til eget bruk, har han vinnings hensikt uavhengig av hva slags personlig motiv han eller hun har». I det tilfellet der en borttar en harddisk med det forsett om å tilegne seg de økonomiske verdiene lagret på den, er det klart at gjerningspersonen har til forsett å «skaffe seg en uberettiget vinning». For tyveribestemmelsen må likevel dette vilkåret ses i sammenheng med tilegnelsesforsettet.

Det som skiller tyveribestemmelsen fra andre vinningsstraffebud, som for eksempel ulovlig bruk av løsøre, er vilkåret om tilegnelsesforsett. Vilkåret springer ut av ordlyden «tilegne». Dette kan beskrives som å definitivt unytte tinge som sin egen.[59] Til forskjell fra bestemmelsen om underslag, er det tilstrekkelig for tyveri at gjerningspersonen har forsett om tilegnelse. Dersom en tar en ting for å selge eller forbruke den på et senere tidspunkt, er vilkåret oppfylt. Lovteksten gir to eksempler på dette. Det første er «å selge». Ved å selge en ting er det klart at man definitivt unytter tingen som sin egen. Det andre eksemplet er «å

[59] Jacobsen, Husabø, Gröning, Strandbakken (2020), s. 202

forbruke». Mat som spises opp eller penger som er brukt for å kjøpe noe, er da forbrukt. For andre objekter er de forbrukt «når de brukes på en måte som gjør at gjenstanden ikke lenger eksisterer slik som før.»[60]. Juridisk teori gir noen eksempler på dette som å spise opp andres mat, å smøre inn en annens krem på seg selv eller å svelge noen andres tabletter. Eksemplene gitt her tilsier at gjenstanden, eller deler av den, må være irreversibelt brukt opp eller konsumert for at det skal kunne regnes som et forbruk.

I typetilfelle 2 har gjerningspersonen tatt en gjenstand, harddisken, med det forsett om å bruke den for å hente ut verdiene som ligger lagret på den, for deretter å levere den tilbake på et senere tidspunkt. Spørsmålet blir om et slikt forsett kan regnes som et tilegnelsesforsett.

Om man hevder at en harddisk kun er definert av dens rørlige egenskaper, vil det vanskelig kunne hevdes at en harddisk kan forbrukes. Både før og etter eventuelle endringer som gjøres inne i selve disken, vil dens fysiske egenskaper være lik. Den kan fremdeles lagre informasjon slik den var ment for og har ikke endret form eller nytteevne. Om man på den andre siden har som utgangspunkt at egenskapene ved en harddisk, eller andre lagringsmedier, er definert av innholdet, så vil alle endringer som foretas inne på disken kunne regnes som et forbruk. Harddisken har ikke lengre de samme egenskapene ettersom det lagrede innholdet ikke eksistere slik som før, eller er helt borte. Dette kan på et vis sammenliknes med et konsum av fysiske gjenstander, som for eksempel matvarer. På den andre siden vil det ikke være naturlig å hevde at en matboks en har stjålet er forbrukt, dersom hensikten var å spise maten som er i matboksen og senere levere den tilbake. (i dette tilfellet vil jo likevel maten kunne regnes som en «gjenstand», og slik ville det ikke vært noe spørsmål om en gjenstand er forbrukt). Slik jeg ser det oppfyller ikke slik bruk av en harddisk alternativet om forbruk. Selv om innholdet på harddisken ikke vil være helt lik etter tømmingen av kryptovalutaen, er ikke harddisken brukt opp eller konsumert. På samme måte som i eksempelet om matboksen, er harddisken like hel etter tømmingen av innholdet.

De to eksemplene på tilegnelse, salg og forbruk, utgjør ikke en uttømmende liste over alle mulige måter å tilegne seg noe, jf. «på annen måte». I straffeloven av 1902 § 255 var også

[60] Jacobsen, Husabø, Gröning, Strandbakken (2020) s. 206

pantsettelse nevnt som eksempel på tilegnelse, og det er presisert i forarbeidene til straffeloven av 2005 at dette fremdeles skal gjelde.[61] Å innløse et pant på et senere tidspunkt og deretter levere tingen tilbake, regnes også som tilegnelse.[62] Et annet eksempel er å beholde en ting som er levert til deg, men skulle vært levert til/mottatt av en annen. Dersom du nekter for at du er i besittelse av tingen, kan dette utgjøre en disposisjon i retning av å beholde den. Eksemplene nevnt her likner ikke på det person B hadde forsett om å gjøre med harddisken. Harddisken skulle kun brukes midlertidig, for så å leveres tilbake. Forsettet om vinningen springer ut av den midlertidige bruken, ikke det å eventuelt beholde den. I Rt. 1967 s. 365 kom Høyesterett til at herredsretten ikke i tilstrekkelig grad hadde avgjort om det forelå et tyveri eller kun et brukstyveri av en sykkel. Dommer Heiberg uttaler på side 366-367 at «[d]et fremgår etter min mening ikke tilstrekkelig klart av dette hvorvidt retten har funnet det bevist at A hadde til hensikt å skaffe seg en uberettiget vinning «ved tilegnelsen» av sykkelen – med andre ord å utnytte den som sin egen – eller om han bare har hatt til hensikt å bruke den ulovlig. I siste tilfelle kan han ikke straffes for tyveri, jfr. Andenæs: Formuesforbrytelser 14-15». Magnus Matningsdal henviser til dommen og uttaler at det ikke «foreligger […] tilegnelsesforsett dersom gjerningspersonen ikke har som forsett å beholde gjenstanden etter bruken».[63]

I det tilfellet der en borttar en harddisk med det forsett om å bruke den midlertidig for å hente ut verdiene på den for så å levere den tilbake, mangler altså gjerningspersonen tilegnelsesforsett og kan ikke straffes for tyveri. Det er også utelukket å tale om forsøksansvar i denne forbindelse. § 16 fastsetter at gjerningspersonen må ha hatt «forsett om å fullbyrde et lovbrudd», og ettersom gjerningspersonen mangler tilegnelsesforsett, jf. § 321, kan ikke gjerningspersonen straffes for forsøk på tyveri. Tyveribestemmelsen verner altså ikke de verdier kryptovaluta representerer i typetilfelle 2, forutsatt at data faller utenfor gjenstandsbegrepet.

[61] Ot.prp. nr. 22 (2008-2009) s. 452
[62] Rt. 1964 s. 1076
[63] Matningsdal, Juridika, kommentar til § 321, punkt 7.2

8.2 Besittelseskrenkelse og ulovlig bruk av løsøre

8.2.1 § 345. Besittelseskrenkelse

§ 345 fastsetter at «[d]en som urettmessig setter seg eller andre i besittelse av en løsøregjenstand, straffes med bot». I likhet med tyveribestemmelsen er det et vilkår at den rettmessige eier fratas besittelsen. For tyveribestemmelsen er det tilstrekkelig at gjerningspersonen oppnår en kortvarig rådighet over gjenstanden. Etter § 345 kreves det en mer langvarig rådighet, jf. «setter seg […] i besittelse».[64] Om vi ser for oss at person B var i besittelse av harddisken et par dager, er det nokså klart at han har skaffet seg en mer varlig og selvstendig rådighet over disken, som truer eierens posisjon som eier.

8.2.2 Graden av vern bestemmelsen gir

Strafferammen for brudd på § 345 er bot. Slik jeg ser det gir en slik sanksjon et dårlig vern for de verdier som kryptovaluta lagret på en harddisk kan representere. I typetilfelle 2 var en verdi på kr 1.000.000 borttatt. Ileggelse av en bot som eneste straffereaksjon fremstår ikke tilstrekkelig for, for det første, å utvise tilstrekkelig klander (individualpreventivt), og for det andre å være tilstrekkelig avskrekkende for eventuelle gjerningspersoner (allmennpreventivt). Gjerningsbeskrivelsen er også dårlig egnet til å utvise den skyld en slik handling fortjener. Selv om gjerningsbeskrivelsen omhandler urettmessig besittelse av en løsøregjenstand, noe som er en del av person B sin handling i typetilfelle 2, er den i liten grad dekkende for å fange opp de momenter som gjør person B sitt forbryterske forsett klanderverdig.

Slik jeg ser det verner § 345 de økonomiske verdiene som kryptovaluta representerer i typetilfelle 2, i en meget begrenset grad. Selvstendig bruk av straffebudet gir derfor ikke en tilstrekkelig grad av vern.

8.2.3 § 343. Ulovlig bruk

[64] Jacobsen, Husabø, Gröning, Strandbakken (2020), s. 190

§ 343 fastsetter at «den som ulovlig bruker eller forføyer over en løsøregjenstand som tilhører en annen, slik at den berettigede påføres tap eller ulempe» kan straffes med bot. I typetilfelle 2 er det klart at harddisken «tilhører en annen» og at den er en «løsøregjenstand». Det sentrale i bestemmelsen for dette typetilfellet er om harddisken er ulovlig brukt eller forføyd over og at dette har ført til «tap eller ulempe» for person A.

Med «tap» menes økonomisk tap.[65] Ved borttakelsen av harddisken, er kryptovalutaen fremdeles lagret på den. Selv om verdiene fremdeles er lagret på disken og kan hentes ut dersom eieren får disken tilbake, har eieren ved borttakelsen mistet tilgangen til dem. I juridisk teori er det uttalt at «det foreligger et økonomiske tap dersom handlingen har fått konsekvenser som regnskapsmessig påvirker offerets samlede formue» og «[h]vorvidt det økonomiske tapet er endelig for offeret, eller om vedkommende på en aller annen måte kan få tapet kompensert, kan ikke være avgjørende.»[66] Det faktum at den rettmessige eier i typetilfelle 2, har mistet tilgangen til verdien lagret på disken, som igjen påvirker hans tilgjengelige formue, tilsier at det er påført et «tap».

Selv om det foreligger et tap, er det et alternativt vilkår at gjenstanden er brukt. For bruk er det ikke tilstrekkelig å ha skaffet seg tilgang til gjenstanden. Den må i noen grad utnyttes til noe den er ment for.[67] Å kun ha tilgang til harddisken er da ikke tilstrekkelig for vilkåret.[68] Ettersom poenget med en harddisk, og dermed også det den er egnet til, er å lagre, lese og bruke data, vil det først være snakk om bruk når i det minste harddisken kobles til en datamaskin. Dette er ikke tilfellet i foreliggende typetilfelle. Person B har kun borttatt den, men har ennå ikke koblet den til sin datamaskin. Det er derfor ikke snakk om bruk i dette tilfellet. Det andre alternativet rammer den som «forføyer» over andres gjenstand. Dette rammer andre disposisjoner som er forbeholdt eieren, som å gi den bort eller pantsette den. I lys av § 345 kan det ikke være tilstrekkelig å kun ha tingen i besittelse. I scenariet der person B har borttatt en harddisk, men kun har den i sin besittelse, vil det heller ikke være snakk om

[65] Jacobsen, Husabø, Gröning, Strandbakken (2020) s. 192
[66] Ibid, s. 175-176
[67] Ibid s. 191
[68] Jf. bla. Rt. 1958 s. 1147, s. 1148

forføyning, da dette forutsetter mer enn bare en borttakelse fra person A. Person B har ikke gjort seg skyldig i ulovlig bruk, jf. § 343.

8.2.4 Forsøk på grov ulovlig bruk

Selv om person B ikke har gjort seg skyldig i ulovlig bruk av løsøre, er det likevel relevant å se til forsøksbestemmelsen ettersom person B hadde som mål å bruke harddisken, men kom ikke så langt. Ettersom strafferammen i § 343 kun er bot, kommer ikke forsøksbestemmelsen til anvendelse, jf. § 16, første ledd. Det må derfor vurderes om § 344 kan gjøres gjeldene, og om forsøksbestemmelsen gir et vern for de verdier kryptovaluta representerer.

For at det i det hele tatt kan være snakk om forsøk på grov ulovlig bruk av løsøre, må det være snakk om en «betydelig vinning» eller et «betydelig tap». For andre formuesstraffebud er det satt en veiledende verdigrense på 1,5 G. Forarbeidene uttaler imidlertid at for overtredelse av § 344, ligger grensen vesentlig lavere.[69] For typetilfelle 2 er det snakk om en potensiell vinning/tap på kr. 1.000.000, noe som klart er å regne som en «betydelig vinning» for person B og «betydelig tap» for person A, dersom person B hadde gjennomført hele sin plan. Det må videre være en sammenheng mellom bruken og vinningen/tapet, jf. «og ved det skaffer seg». I det tilfellet der person B hadde koblet harddisken til sin maskin og overført dataen, er det nokså klart at dette kvalifiserer til bruk, og at denne bruken ville ført til en betydelig vinning. Det er da en direkte sammenheng mellom bruken og vinningen/tapet. § 344 omfatter etter mitt syn typetilfelle 2.

I tillegg til vilkåret om strafferamme, oppstiller § 16 to vilkår for at en gjerningsperson kan straffes for forsøk. I typetilfelle 2 kan det kort slås fast at person B hadde «forsett om å fullbyrde et lovbrudd», jf. § 16 første ledd, ettersom planen hans var å nettopp koble harddisken til sin datamaskin, noe som er å regne som bruk, jf. 344. Det sentrale spørsmålet blir derfor om person B har «foretatt noe som leder direkte mot utføringen». Som nevnt under punkt 7.5.1, er det vanskelig å si noe generelt om hvor mye som skal til før man har passert

[69] Ot.prp.nr.35 (1986-1987) s. 24

den nedre grense for forsøk. Den tidsmessige nærhet, handlingens karakter og omfang er momenter i en konkret vurdering. For typetilfelle 2 gjenstod det kort tid, kun en dag. Det var lite som gjenstod for person B for å oppfylle gjerningsbeskrivelsen, kun å koble harddisken til maskinen sin. I tillegg har person B allerede gjort seg skyldig i besittelseskrenkelse, jf. § 345. At det er begått andre ulovlige handlinger trekker i retning av at den nedre grensen er passert.[70] Disse momentene ved person B sin handling, tilsier, etter min vurdering, at den nedre grensen for forsøk er passert. Person B kan dermed straffes for forsøk på grov ulovlig bruk av løsøre.

8.2.5 Graden av vern bestemmelsen gir

Graden av vern § 16, jf. § 344 gir, er i noe større grad egnet til å vern om person A sine økonomiske interesser enn § 345. For det første er strafferammen høyere, noe som i større grad reflekterer alvorligheten av person B sin gjerning. Likevel kan det hevdes at en straff med bot og inntil 2 år i fengsel, ikke er tilstrekkelig der verdier for kr 1.000.000 er truet. For andre formuesforbrytelser, som §§ 322 og 372, er strafferammen vesentlig høyere. I tillegg skal et forsøk alltid betraktes som en formildende omstendighet, jf. § 78 a), og straffen vil da trolig settes under lengstestraffen.

For det andre er gjerningsbeskrivelsen § 344 i noe bedre grad egnet til å utvise tilstrekkelig skyld, ettersom person B sin plan ikke bare var å være i besittelse av harddisken, men bruke den, og dermed oppnå en uberettiget vinning. Selv om det var verdien av kryptovalutaen person B var ute etter, var bruk harddisken en nødvendig betingelse for å tilegne seg denne. Gjerningsbeskrivelsen er da mer treffende.

[70] Jf. Rt. 1991 s. 95 og Rt. 2011 s. 1011

9 Konklusjon på oppgavens problemstilling

Problemstillingen for oppgaven var å undersøke hvilket vern straffeloven gir de økonomiske verdier som kryptovaluta representerer. Selv om enkelte straffebud kommer til kort, enten det dreier seg om straffebudets ordlyd, som ikke er egnet for å dekke hele den klanderverdige handlingen, eller at den øvre strafferammen er for lav, sett opp mot andre formuesstraffebud, fremstår det for meg som at straffeloven som helhet gir et godt vern av kryptovaluta som formue. Her er det særlig § 371 bokstav b), om databedrageri, som gir det beste vernet. Straffebudet gir, etter min vurdering, en tilstrekkelig hjemmel for å utvise den klander der noen har oppnådd en uberettiget vinning ved å krenke en annens eiendomsrett til kryptovaluta. Selv om § 371 bokstav b) gir et godt vern for kryptovaluta, mener jeg det likevel er en nødvendig fremtidig oppgave for lovgiver å avklare det strafferettslige gjenstandsbegrepet i forhold til data.

Litteraturliste

Lover:

LOV-2005-05-20-28, Lov om straff (straffeloven), 2005.

LOV-1902-05-22-10, Almindelig borgerlig Straffelov (Straffeloven), 1902.

LOV-2013-06-21-85, Lov om endringer i straffeloven 1902 og straffeloven 2005 mv. (forberedelse av terror m.m).

Forarbeider:

Indst. O. I. (1901/1902) Indstilling fra justiskomiteen angaaende den kongelige proposition til en almindelig borgerlig straffelov, en lov om den almindelige borgerlige straffelovs ikrafttræden samt en lov, indeholdende forandringer i lov om rettergangsmaaden i straffesager af 1ste juli 1887.

NOU 1985: 31 Datakriminalitet.

Ot.prp. nr. 35 (1986-1987) Om endringer i straffeloven (datakriminalitet).

NOU 1992: 23 Ny straffelov – alminnelige bestemmelser Straffelovkommisjonens delutredning V.

NOU 2002: 4 Ny straffelov.

Ot.prp. nr. 40 (2004-2005) Om lov om endringer i straffeloven og straffeprosessloven mm.

Ot.prp. nr. 22 (2008–2009) Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon – sluttføring av spesiell del og tilpasning av annen lovgivning).

Prop.131 L (2012–2013) Endringer i straffeloven 1902 og straffeloven 2005 mv. (forberedelse av terror m.m.).

Rettsavgjørelser:

Rt. 1894 s. 484

Rt. 1958 s. 1147

Rt. 1964 s. 1076

Rt. 1965 s. 223

Rt. 1967 s. 365

Rt. 1971 s. 667

Rt. 1991 s. 95

Rt. 1991 s. 532

Rt. 1994 s. 740

Rt. 1994. s 1002

Rt. 2004 s. 1619

Rt. 2008 s. 867

Rt. 2011 s. 1011

Rt. 2011 s. 1013

HR-2021-2580-A

Faglitteratur:

Jacobsen, Husabø, Gröning, Strandbakken, «*Forbrytelser i utvalg*», 1. utgave, Fagbokforlaget, 2020.

Juridika, lovkommentar av Magnus Matningsdal, https://juridika.no/no/lov/2005-05-20-28/%C2%A7321/kommentar, hentet 22.04.23.

Gröning, Husabø, Jacobsen, «*Frihet, forbrytelse og straff*», 3. utgave, Fagbokforlaget, 2023.

Lilleholt, Kåre, «*Allmenn formuerett*», 2.utgave, Universitetsforlaget, 2018.

Schjølberg, Stein, «*Cyberkriminalitet*», Universitetsforlaget, 2017.

Sunde, Inger Marie, «*Lov og rett i cyberspace*», Fagbokforlaget, 2006.

Sunde, Inger Marie, «*Datakriminalitet*», Fagbokforlaget, 2016.

Sunde, Inger Marie, «*Automatisert inndragning*», doktorgradsavhandling (PhD) nr. 37 ved Det juridiske fakultet, 2011, Universitetet i Oslo. Utgitt i Copmlex 3/11, Senter for rettsinformatikk.

Internasjonale konvensjoner:

Convention on Cybercrime, Budapest, 23. November 2001. (ikrafttredelsesdato i Norge: 1. oktober 2006) (Konvensjon om datakriminalitet).

Nettsider:

CoinMarkedCap, «Global Live Cryptocurrency Charts & Market Data» https://coinmarketcap.com/charts/ (hentet 31.01.24).

Cointelegraph, «How to start mining cryptocurrency: A beginner's guide» https://cointelegraph.com/learn/how-to-start-mining-cryptocurrency (hentet 08.02.24).

E24, «Etterforsker kryptotyveri av fem milliarder kroner» https://e24.no/norsk-oekonomi/i/bGPxJ3/etterforsker-kryptotyveri-av-fem-milliarder-kroner (hentet 28.02.24).

Forbes, «Different Types Of Cryptocurrencies Explained» https://www.forbes.com/advisor/au/investing/cryptocurrency/different-types-of-cryptocurrencies-explained/ (hentet 31.01.24).

Investopedia, «What Determines Bitcion´s Price» https://www.investopedia.com/tech/what-determines-value-1-bitcoin/ (hentet 30.01.24).

Investopedia, «Cryptocurrency Wallet: What It Is, How It Works, Types, Security» https://www.investopedia.com/terms/b/bitcoin-wallet.asp (hentet 31.01.24).

Likestillings- og diskrimineringsombudet, «Hatefulle ytringer på nett», 2021, https://www.ldo.no/globalassets/_ldo_2019/03_ombudet-og-samfunnet/rapporter/hatefulle-ytringer/ldo_hatefulle_ytringer_pa_nett.pdf» (hentet 29.01.24).

Milkroad, «Major Companies That Accept Crypto Payments» https://milkroad.com/accept-crypto/ (hentet 31.01.24).

Skatteetaten, «Skatteregler - Virtuelle eiendeler» https://www.skatteetaten.no/person/skatt/hjelp-til-riktig-skatt/aksjer-og-verdipapirer/om/virtuell-valuta/skatteregler---virtuell-valuta/ (hentet 29.02.24).

Store norske leksikon, «Kryptovaluta» https://snl.no/kryptovaluta (hentet 30.01.24).

Store norsk leksikon, «Blokkjede», https://snl.no/blokkjede, (hentet 31.01.24).

Youtube, «How does a blockchain work - Simply Explained» https://youtu.be/SSo_EIwHSd4?si=6K_-H80OKy7ieCyq (hentet 28.02.24).

Økokrim, «Bruk av kryptovaluta i kriminell virksomhet» https://www.okokrim.no/bruk-av-kryptovaluta-i-kriminell-virksomhet.6343555-537788.html (hentet 01.02.24).

Økokrim, «Infoskriv bruk av kryptovaluta i kriminell virksomhet» https://www.okokrim.no/getfile.php/4762586.2528.ntbmpquwkinkjm/Infoskriv+bruk+av+kryptovaluta+i+kriminell+virksomhet.pdf (hentet 01.02.24).

Personlig meddelelse:

Økokrim, e-post, 19.01.2024 fra Katrine Halten Nylund.