# NORGES HØYESTERETT

Den 20. desember 2012 avsa Høyesterett dom i

**HR-2012-02397-A, (sak nr. 2012/777), straffesak, anke over dom,**

Den offentlige påtalemyndighet (statsadvokat Carl Fredrik Fari)

mot

A (advokat Abdelilah Saeme – til prøve)

S T E M M E G I V N I N G :

(1) Dommer **Normann:** Saken gjelder straffutmåling for databedrageri ved inntrenging i nettbank og tapping av penger fra nettbankkonti.

(2) A ble 14. oktober 2011 satt under tiltale for forsøk på grovt databedrageri overfor Nordea Bank, Terragruppen og Sparebank 1(tiltalebeslutningen post I), grovt databedrageri overfor DnB NOR Bank (nå DNB Bank ASA) (post II) og datainnbrudd (post III). For Høyesterett er saken begrenset til å gjelde straffutmålingen for de forhold som er omfattet av tiltalebeslutningen post II og III.

(3) Tiltalen for overtredelsen av straffeloven § 270 første ledd nr. 2, jf. annet ledd, jf. § 271 (post II) bygger på følgende forhold eller medvirkning til dette:

> **"I tidsrommet februar – april 2011, via internett fra ukjent sted, modifiserte han, sammen med andre, trojaneren SpyEye som ved flere anledninger ble testet mot DnBNORs nettbankløsning i den hensikt å få tilgang via bankens nettbankkunder til kundenes bankkonti for deretter urettmessig å overføre penger til andre, for rettmessige kontoinnehaver ukjente personer. I perioden 2. april – 4. mai 2011 via internett, ved tilsammen 25 anledninger skaffet han seg uberettiget tilgang til 25 norske nettbankkunder sine bankkonti via kundens egen datamaskin. Han la inn overføringer/transaksjoner til utbetaling for tilsammen kr 809.883,- fra nettbankkundens konto til forhåndsprogrammerte bankkonti tilhørende andre kontoinnehavere. Handlingen medførte tape eller fare for tap for nettbankkunden eller DnBNOR."**

(4) Tiltalen for overtredelsen av straffeloven § 145 annet ledd, jf. første ledd og tredje ledd (post III) bygger på følgende forhold eller medvirkning til dette:

> **"Til tid og sted som nevnt i post II, forholdt han seg som der nærmere beskrevet."**

(5) Nedre Romerike tingrett avsa 21. november 2011 dom som hadde slik domsslutning:

> **"1. A, født 25.04.1985, frifinnes for post I i tiltalebeslutningen av 14. oktober 2011.**
>
> **2. A, født 25.04.1985, dømmes for overtredelse av straffeloven § 270 første ledd nr 2 jf annet ledd og § 271 og straffeloven § 145 annet ledd jf første ledd og tredje ledd til fengsel i 1 år og 8 måneder, jf. straffeloven § 62 første ledd. Varetekt kommer til fradrag med 203 dager beregnet t.o.m. 21. november 2011.**
>
> **3. A, født 25.04.1985, dømmes i medhold av strl § 35 til å tåle inndragning av 1 stk Acer Aspire 5739G bærbar pc.**
>
> **4. A, født 25.04.1985, dømmes til å betale kr 939.000 som erstatning til DNB Bank ASA. Oppfyllelsesfristen er 2 uker fra dommens forkynnelse.**
>
> **5. Saksomkostninger idømmes ikke."**

(6) Påtalemyndigheten anket til Eidsivating lagmannsrett over lovanvendelsen for frifinnelsen for tiltalens post I og straffutmålingen for de øvrige forhold. Anken over frifinnelsen førte delvis frem, idet frifinnelsen for forsøk på databedrageri overfor Nordea ble opphevet. For forholdene i tiltalens post II og III ble straffen redusert til fengsel i ett år. Lagmannsrettens dom har denne domsslutning:

> **"1. Tingrettens dom, domsslutningen pkt. 1, oppheves for så vidt gjelder frifinnelsen for medvirkning til forsøk på bedrageri mot Nordea. For øvrig forkastes anken over lovanvendelsen.**
>
> **2. I tingrettens dom, domsslutningen pkt. 2, gjøres den endring at straffen settes til fengsel i 1 – ett – år. Varetektsfradraget utgjør 317 – trehundreogsytten – dager."**

(7) Påtalemyndigheten har anket til Høyesterett over straffutmålingen og gjort gjeldende at den straff lagmannsretten har utmålt, er vesentlig for lav. Påtalemyndigheten har for Høyesterett nedlagt påstand om fengsel i to år og tre måneder. Domfelte har tatt til motmæle og har påstått straffen nedsatt.

(8) *Jeg er kommet til* at påtalemyndighetens anke over straffutmålingen må tas til følge, men at straffen må settes noe lavere enn det påtalemyndigheten har påstått.

(9) Domfelte er en 27 år gammel mann, estisk statsborger som har bodd og arbeidet i Norge i cirka fem år, stort sett som bygningsarbeider. Han er ikke tidligere straffet i Norge, men ifølge dokumentert informasjonen fra Europol er han bøtlagt i 2007 for forfalskning knyttet til kredittkort.

(10) For Høyesterett er saken begrenset til å gjelde straffutmålingen for medvirkning til databedrageri og datainnbrudd overfor DnB NOR Bank våren 2011. Domfellelsen gjelder følgende forhold:

(11) Den 3. desember 2010 opprettet domfelte en konto i DnB NOR med nettbankavtale. I julen 2010 overleverte han kodebrikke og passord for kontoen til personer i Estland. Disse tilpasset eller modifiserte dataprogrammet Spy Eye for å få tilgang til nettbankkonti i DnB NOR for å tappe disse for penger. Etter at banken hadde fått henvendelser fra kunder som ikke vedsto seg uttak på sine nettbankkonti, fikk DnB NOR etter nærmere undersøkelser mistanke om at A hadde drevet med nettbanktapping og anmeldte forholdet. Bankens detekteringssystem hadde funnet likheter mellom transaksjoner på As konti, og konti hvor kundene mente seg utsatt for tapping. Gjennom gransking av transaksjonslogger lyktes banken med å stoppe flere transaksjoner fra kunders konti som urettmessig var lagt klare for overføring til norske og utenlandske konti. Totalt var det foretatt 25 posteringer for overføring av et samlet beløp på 809 883 kroner. Fire overføringer var gjennomført. Av disse fire ble én tilbakeført, mens tre overføringer – for til sammen 125 661 kroner – ikke lot seg stoppe eller tilbakeføre.

(12) Det er to hovedformer for nettbanksvindel, "manuell" og "automatisk". I denne saken ble sistnevnte metode anvendt. I begge tilfeller må svindleren først skaffe seg tilgang til en bankkundes nettbankkonto. Denne kontoen blir benyttet som base for å trenge inn i andre kunders nettbankkonti. Den metoden som ble benyttet, er oppsummert slik av lagmannsretten:

> **"- Svindlerne må skaffe seg tilgang til et antall datamaskiner som blir brukt av kunder i den eller de nettbankene det er aktuelt å angripe.**
> **- Det må utvikles dataprogram ("angrepskoder") som passer til disse nettbankene.**
> **- Angrepskodene må installeres på de enkelte datamaskinene svindlerne har skaffet seg tilgang til, og disse kodene må videreutvikles og oppdateres, blant annet etter hvert som bankens sikkerhetssystem utvikler mottiltak.**
> **- Svindlerne må ha kontroll over et antall bankkonti dit overføringene kan styres. Dette er gjerne konti som tilhører helere ("muldyr") i utlandet. Muldyrenes oppgave er å sørge for at pengene til slutt havner hos svindlerne, men slik at overføringen dit ikke så lett lar seg etterspore."**

(13) For urettmessig å komme inn i nettbanken og videre inn på kunders nettbankkonti og foreta overføringer, benyttes særlige dataprogrammer med utgangspunkt i et verktøy som kalles Spy Eye, som igjen generer trojanere. Programvaren Spy Eye kan kjøpes på internett i forskjellige versjoner, kan tilpasses inntrengning på nettbankløsninger og kan infisere et større antall brukermaskiner. Infiseringen skjer for eksempel ved at en bruker er inne på en nettavis der trojaneren ligger skjult. Denne installeres dermed på datamaskinen.

(14) En trojaner er bærer av flere elementer (programmer), hvor et sentralt element er programvare som holder kontakt med servere svindlerne disponerer, som kan være plassert hvor som helst i verden. Trojaneren kan ved hjelp av slike program hente opp nye elementer og installere disse på den infiserte datamaskinen. Ved nettbanksvindel er det særlig aktuelt å hente opp nye angrepskoder etter hvert som disse blir utviklet. De nye angrepskodene kommer i tillegg til de angrepskoder trojaneren kan ha vært utstyrt med fra starten, og utvikles for å tilpasses de enkelte ulike nettbankløsningene banker benytter.

(15) Ved angrep mot en ny nettbank tar angriperne gjerne utgangspunkt i en allerede eksisterende angrepskode og utvikler denne slik at den passer til det nye angrepet. Utviklingsarbeidet forutsetter at svindlerne har adgang til den aktuelle nettbanken.

(16) Når angrepskoden er ferdig utviklet og tilpasset en bestemt nettbankløsning, legges den på en server som svindlerne disponerer. Derfra hentes koden automatisk av de brukermaskinene som allerede er infisert med en trojaner.

(17) Neste gang brukeren logger seg på, vil angrepskoden sørge for at det blir lagt inn en overføring som nettbankkunden ikke ser. Programmet sørger for at nettbanken får beskjed om å taste inn ny engangskode. Hvis det gjøres, bekrefter kunden uten å vite det overføringen som er lagt inn i programmet. Trojaneren er altså automatisk operativ uten at kunden merker dette.

(18) For Høyesterett er det fremlagt opplysninger fra Nasjonal Sikkerhetsmyndighet hvor det fremgår at det de siste årene er observert en kraftig økning i antall kompromitterende norske nettsider som sprer banktrojanere og annen skadevare. Dette koster samfunnet store summer å rydde opp i.

(19) Opplysningene bekreftes også av en omfangsvurdering av trusselbildet som er foretatt av Bankenes Standardiseringskontor på vegne av banknæringen. Det er opplyst at angrepene på Internett vokser kraftig i omfang og kompleksitet, at det de siste årene er blitt enklere for de kriminelle organisasjonene å utnytte sårbarheter i programvare, og at trusselbildet på internett er "høyst uforutsigbart". På grunn av angrepenes kompleksitet er det antatt at internasjonale organiserte kriminelle miljøer står bak. Norske banker samarbeider internasjonalt for å bekjempe kriminalitet mot nettbankene.

(20) I Norge har bankene foreløpig greid å iverksette effektive tiltak mot nettbanksvindel, slik at omfanget av gjennomførte bedragerier hittil har vært begrenset. Tapene var henholdsvis 490 000 kroner i 2011 og 1,3 millioner kroner i første halvår av 2012. Finansnæringen bruker imidlertid store ressurser på å bekjempe svindelen, og banknæringen har anslått at den i 2011 har avverget bedragerier på 55,5 millioner kroner. Tilsvarende tall for første halvår i 2012 er anslagsvis 151 millioner kroner.

(21) Det skal etter dette utmåles straff for 25 transaksjoner fra konti i DnB NOR. Tapsfaren for disse transaksjonene var samlet 809 883 kroner, og den fullbyrdete forbrytelse gjelder altså dette beløpet.

(22) Lagmannsretten har ved straffutmålingen tatt utgangspunkt i en beløpsbetraktning, men har gitt uttrykk for at det er vanskelig å finne et "normalt straffenivå" for bedrageri i størrelsesorden 800 000 kroner. Jeg enig i dette – noe som blant annet har sammenheng med at bedragerier dekker mange ulike forhold, og det er betydelige forskjeller i utmålingspraksis. Selv om det er vanskelig å operere med en alminnelig beløpsmessig norm, finner jeg likevel en viss veiledning i to saker som også gjaldt databedrageri.

(23) Rt. 1990 side 955 gjaldt databedrageri på i overkant av 1,2 millioner kroner, som tilsvarer rundt 2 millioner kroner i dagens pengeverdi. Straffen ble satt til fengsel i 1 år og 6 måneder. Domfelte hadde bokført fiktive fakturaer i virksomheten hvor han var ansatt, og fått beløpene overført til sin konto. Beløpet er høyere enn i vår sak, og tillitsmomentet

som ble vektlagt der, er ikke like fremtredende i vår sak. Sakene har likevel det til felles at begge handler om å utnytte et system.

(24) Dommen i Rt. 1994 side 740 gjaldt en bankansatt som opprettet fiktive konti med den følge at hun selv fikk urettmessig utbetalt 361 768 kroner, tilsvarende cirka 600 000 kroner i dagens pengeverdi. Straffen ble fengsel i 10 måneder, hvorav 45 dager ubetinget. Forholdet var imidlertid der fem år gammelt da saken kom til pådømmelse.

(25) Det foreligger imidlertid forhold som tilsier at straffen her må bli betydelig strengere. En rekke av de hensyn som er tillagt vekt ved fastsettelsen av det alminnelige straffenivået for organisert kredittkortkriminalitet, gjør seg gjeldende i vår sak, jf. Rt. 2009 side 397.

(26) På samme måte som ved organisert kredittkortkriminalitet krever også nettbankkriminalitet planlegging og organisering over tid, og potensialet for økonomisk gevinst er betydelig ved begge former for kriminalitet.

(27) Jeg viser videre til avsnitt 20 i den nevnte dommen, der det er uttalt:

> **"Det er karakteristisk at virksomheten ikke bare rammer det enkelte kortselskap og den enkelte korteier. Den undergraver også tilliten til de elektroniske betalingssystemer som i dag er dominerende, og står slik sett ikke nevneverdig tilbake for pengefalsk hva straffverdighet angår. Denne forbindelsen er også påpekt i Rt. 2004 side 1701 i avsnitt 17. I dommen fremheves også at misbruk av giro- og kortbaserte betalingsordninger lett kan få større økonomisk omfang enn pengefalsktilfellene. Jeg nevner Internett-baserte bank- og betalingsløsninger som andre eksempler på eksponerte transaksjonsformer. Utmålingspraksis i tilknytning til pengefalsk kan naturligvis ikke overføres direkte, blant annet ettersom straffeloven § 174 har en minstestraff på tre års fengsel. Men slektskapet tilsier at man trekker veksler på pengefalsk, både med hensyn til nivået og for vekten av ulike straffutmålingsmomenter (uthevet her)."**

(28) I avsnitt 21 er førstvoterendes konklusjon at "[d]et ligger i det jeg nå har sagt … at det bør gjelde et strengt alminnelig straffenivå i saker som dette, jf. uttalelsene blant annet i Rt. 1995 side 475 og Rt. 1995 side 1314, som gjaldt pengefalsk".

(29) Jeg er enig i at det også ved nettbanksvindel bør gjelde et strengt alminnelig straffenivå.

(30) Forsvareren har vist til at tapene i norske banker – til tross for massive trojanerangrep – hittil har vært små, og at tapene knyttet til nettbanksvindel har vært langt mindre enn ved kortsvindel, for eksempel som følge av at passord og engangskoder er blitt stjålet. Jeg tillegger ikke denne innvendingen særlig vekt. Internettkriminalitet er et økende samfunnsproblem som ikke bare berører bank- og finansnæringen nasjonalt og globalt, men som også er en alvorlig vinningsforbrytelse som truer tilliten til en betalingsform som dagens betalingsformidling er basert på. Det er opplyst for Høyesterett at i 2011 ble 66 % av alle regninger betalt over nettbank, totalt 379 millioner transaksjoner. Jeg tillegger det også vekt at bankene benytter betydelige ressurser på å avverge og oppdage denne type svindel. Allmennpreventive hensyn tilsier en streng reaksjon.

(31) Nettbanksvindel dreier seg dessuten ofte om grenseoverskridende virksomhet slik som i saken her. Serveren som styrer utviklingen av trojanerne på de infiserte datamaskinene, kan plasseres hvor som helst i verden, og pengene som tappes fra nettbanken kan også overføres til konti i utlandet. På samme måte som ved grenseoverskridende mobil vinningskriminalitet, er det små muligheter til å få tilbake de verdiene gjerningsmannen

har tilegnet seg ved den straffbare handlingen og som er tatt ut av landet. Også dette tilsier en streng reaksjon.

(32) Aktor har sammenlignet datainnbruddene med innbrudd i private hjem. Denne sammenligning finner jeg ikke treffende. Datainnbruddene rettet seg utelukkende mot nettbanken. Selv om inntrengning i nettbanken forutsetter infisering av kundens datamaskin, gjør invaderingen i den private sfære seg gjeldende på en helt annen og mindre alvorlig måte ved nettbanksvindel enn ved innbrudd i private hjem.

(33) As medvirkning besto i at han opprettet konti i DnB NOR og deretter overlot kode og kodebrikke til andre involverte. Etter dette holdt han dessuten jevnlig kontakt via chattelogger med andre involverte i Estland.

(34) Lagmannsretten har tillagt det vekt i formildende retning at A langt fra var noen hovedmann, at hans konkrete bidrag var relativt beskjedent, og at han befant seg i en utsatt posisjon når det gjaldt oppdagelsesrisiko. Det er riktig at A eksponerte seg for oppdagelsesrisiko, men for øvrig er denne beskrivelsen ikke treffende. At A opprettet konti i DnB NOR og deretter overlot kode og kodebrikke til andre involverte, var en helt nødvendig forutsetning for at de kriminelle kunne skaffe seg tilgang til de ulike konti i nettbanken. A holdt dessuten etter dette jevnlig kontakt via nettet med andre involverte i Estland. Han utgjorde et viktig og nødvendig ledd i gjennomføringen av databedrageriet.

(35) Det betydelige vinningspotensialet ved nettbanksvindelen tilsier at det heller ikke kan tillegges særlig vekt at utbytte for de involverte i denne saken var beskjedent, cirka 125 000 kroner, jf. Rt. 2009 side 397 avsnitt 23. Grunnen til at det ikke ble høyere, var utelukkende at banken greide å stoppe de fleste overføringene før de ble gjennomført.

(36) A er også domfelt for datainnbrudd. Selv om dette isolert sett innebærer et invaderende element på bankkundens datamaskin og i hans nettbank, innebærer innbruddet i vår sak ingen "snoking" i den privat sfære. Forholdene ligger således helt annerledes an enn i Høyesteretts dom fra 31. oktober i år (HR-2012-02056-A), hvor domfelte blant annet hadde kopiert informasjon om e-postadresser og personlige bilder. Innbruddet i nettbanken er dessuten en forutsetning for databedrageriet, og datainnbruddet kan derfor ikke bidra vesentlig ved straffutmålingen.

(37) Etter en samlet vurdering er jeg kommet til at straffen passende kan settes til fengsel i ett år og ti måneder.

(38) Jeg stemmer for denne

D O M :

I lagmannsrettens dom, domsslutningen punkt 2, gjøres den endring at straffen settes til fengsel i 1 – ett – år og 10 – ti – måneder.

(39) Dommer **Bårdsen:** Jeg er i det vesentlige og i resultatet enig med førstvoterende.

(40) Dommer **Skoghøy:** Likeså.

(41) Dommer **Indreberg:** Likeså.

(42) Justitiarius **Schei:** Likeså.

(43) Etter stemmegivningen avsa Høyesterett denne

D O M :

I lagmannsrettens dom, domsslutningen punkt 2, gjøres den endring at straffen settes til fengsel i 1 – ett – år og 10 – ti – måneder.

Riktig utskrift bekreftes: