Phishing fra et strafferettslig perspektiv

En vurdering av nåværende lovgivnings vern mot phishing som fremgangsmåte

Kandidatnummer:17

Antall ord:14953

(PS! Bruk ordtellingsfunksjon. Fotnoter og sluttnoter skal medregnes i ordgrensen. Forord, forside, innholdsfortegnelse, registre, litteraturliste og vedlegg medregnes ikke.)

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.05.19

Innholdsfortegnelse

1 Innledning

1.1 Tema for oppgaven

Problemstillingen i oppgaven er hvordan phishing skal behandles etter norsk strafferett. Oppgaven deles inn i tre deler. Den første er en innledning, den andre er en analyse av phishing i forhold til gjeldende strafferett, herunder også en vurdering av forsøk, medvirkning og konkurrens. I den tredje delen vil jeg foreta en oppsummering av oppgaven. Jeg vil også komme med noen avsluttende bemerkninger om problemstillingen.

Sentrale problemstillinger er blant hvorvidt lovgivningen gir et tilstrekkelig vern mot phishing, og i forlengelsen av dette vil en sentral problemstilling være kriminaliseringen av forberedende handlinger.

1.2 Rettskildegrunnlag

Lovtekst er det naturlige utgangspunktet for oppgaven. Videre vil forarbeider være en sentral rettskilde.

Det finnes lite rettspraksis som tar for seg phishing i norsk rett. For øyeblikket er det kun publisert en lagmannsrettsdom[1] og en tingsrettsdom[2] på nett. I tillegg foreligger det en høyesterettsdom som tar for seg et tilfelle med visse likhetstrekk til phishing, dommen gir imidlertid intet i forhold til forståelsen av phishing.[3]Ettersom det kun kan vises til underrettspraksis oppstår spørsmålet om hvorvidt dette har rettskildemessig relevans og vekt. Utgangspunktet er at Høyesterett dømmer i siste instans, jf. Grl. §88[4]. Underrettspraksis er ikke en autoritativ rettskilde, og har i utgangspunktet ikke rettskildemessig relevans eller vekt. Skoghøy skriver at underettspraksis ikke kan få større vekt enn den argumentasjonsverdi som ligger til grunn for dommen.[5]

[1] LB-2013-56387
[2] TBERG2017-164611
[3] Rt. 2003 s. 825
[4] Lov 17.05.1814 Kongeriket Norges Grunnlov (Grunnloven eller Grl.)
[5] Skoghøy (2018) s. 227

Det meste av teori på området er fra utlandet, og tar i liten grad for seg phishing som fremgangsmåte.

Videre er temaet til en viss grad behandlet i utenlandsk rettspraksis. Særlig i England og USA har phishing hendelser regelmessig versert for domstolene. Ofte i form av store «mediedekkende» saker. Slik som «Operation Phish Phry»[6].

1.3 Kort om fremveksten av phishing, begrepsavklaring og dens praktiske betydning

Phishing er et begrep som er ukjent for mange, derfor vil oppgaven gi en kort innføring over hva det er, hvordan det fungerer og fremgangsmåtens aktualitet.

Phishing som strafferettslig fenomen vokste frem i begynnelsen av 2000-tallet med en rekke angrep mot kunder hos store etablerte foretak. Både Netflix og Nordea sitt navn ble på begynnelsen av 2000-tallet forsøkt benyttet i phishing[7].

Selve ordet phishing stammer fra det engelske ordet fishing, f-en er erstattet med «ph» som er vanlig hackersjargong.[8]

Phishing går kort fortalt ut på at man innhenter opplysninger fra en annen part ved å utgi seg for å være noen man ikke er. Som en hovedregel skjer dette ved at man oppretter falske e-post adresser eller nettsider(domener), i visse tilfeller SMS-kontoer. Både personer og foretak kan være subjekt for phishing.

I en e-post blir for mottakeren for eksempel bedt om å registrere ny brukerprofil eller fornye abonnementet til en tjeneste. E-posten er som regel innbydende og forsøker å få utfyllingen av informasjonen til å virke som en fordel for mottakeren. I skjemaet vil man bli bedt om personalia, kortopplysninger, kontoopplysninger og passord. Akkurat hvilke opplysninger som man blir bedt om vil variere. Som en hovedregel vil handlingen forsøke å fremstå så troverdig som mulig, og avsenderen ber derfor om de samme eller lignende opplysninger som

[6] Se https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709

[7] https://www.vg.no/forbruker/teknologi/i/wMma1/nordea-kunder-forsoekt-svindlet
[8] https://snl.no/phishing

det etablerte foretaket ber om i slike tilfeller. I de klassiske phishing tilfellene vil ofrene som regel bli bedt om å fylle inn passord til den tjenesten vedkommende pretenderer å være. Studier viser at mange bruker samme passord overalt[9], noe som gjør at man eksponerer seg selv for en større risiko

Konsekvensene av et phishing-tilfelle kan være store. Opplysningene vil kunne benyttes som ledd i en rekke straffbare handlinger, eksempelvis bedrageri, dokumentfalskneri og datainnbrudd.

Phishing som begrep er definert i LB-2013-56387 hvor det fremgår at:

«*«Phishing er en betegnelse på digital snoking eller fisking etter sensitiv informasjon som for eksempel brukernavn og passord. Fremgangsmåten er vanligvis at gjerningspersonen bruker falsk e-post for å få brukere til å oppgi slike data.»* [10]

I tillegg er begrepet definert av Inger Marie Sunde i «Datakriminalitet»

«En annen form er såkalt phishing, som er basert på opprettelsen av falske websider som er forvekselbare med nettsidene til etablerte foretak. Her oppfordrer lovbryteren godtroende kunder til «å oppdatere brukerprofilen» med brukernavn, passord, kredittkortopplysninger og fødselsnummer...» [11]

De to definisjonene tar for seg to ulike måter å begå phishing på. Som nevnt i LB-2013-56387 er e-post den mest normale formen.

Eksempelvis er det hvert år dokumentert flere bølger med phishing i forbindelse med skattemeldingen[12]. Gjerningspersonen sender ut en e-post til et stort antall mottakere hvor han utgir seg for å være skatteetaten, og ber mottakeren fylle inn informasjon i det vedlagte skjemaet eller i et eventuelt pop-up vindu. Når skjemaet er utfylt har gjerningspersonen tilstrekkelig med informasjon om mottakeren til å danne falske identifikasjons papirer, utføre internett bedrageri, eller eventuelt logge seg inn på datasystemer som tilhører mottakeren av e-posten.

For e-post tilfellene skilles det mellom tre former for phishing. Phishing(nettfiske) er tilfellene hvor man sender en e-post til en stor gruppe tilfeldige mottakere. Spearphishing er

[9] https://www.digi.no/artikler/bruker-samme-passord-overalt/201158
[10] LB-2013-56387
[11] Sunde (2018) s. 119
[12] https://www.hegnar.no/Nyheter/Naeringsliv/2019/03/Skatteetaten-advarer-Ikke-la-deg-lure

når man en målrettet e-post til en utvalgt gruppe mennesker eller bestemte personer. Whaling er når e-posten blir sendt til høyt profilerte mennesker, eksempelvis næringslivsledere eller politikere.[13]

Whaling og spearphishing er særlig relevant i forbindelse med foretak. Det har i norsk rettspraksis kun vært en sak hvor phishing mot et foretak har vært anført, i LB-2013-56387. Det fantes ikke noe bevis for at phishing var utført i saken.[14] I praksis ser man imidlertid at det verserer en del slike saker i mediene.[15] I de fleste saker blir den ansvarlige aldri oppdaget. Ifølge en rapport fra PWC av 2017 besvarte hele 74% av foretakene at de var blitt utsatt for phishing, og 61% besvarte at de fryktet cybertrusler mer nå enn for 6 måneder siden[16].

I dag er det relativt enkelt å opprette falske e-post kontoer og domener. I tillegg er det for e-post sin del kostnadsfritt. Muligheten for gevinst er stor. Mange foretak advarer derfor sine kunder mot phishing, spesielt phishing via e-post. Dette gjør at risikoen for at folk blir utsatt for phishing er høy.

Av Norsis sin rapport i forbindelse med sikkerhetsdagene i 2018 fremgikk det at særlig norske menn i 50-årene var utsatt for phishing. Ifølge rapporten rammes nordmenn i større grad av phishing enn dansker og svensker.[17]

I Norge er det særlig Nordea-saken fra 2015, hvor 2000 Nordea kunder ble svindlet, som har blitt viet mye oppmerksomhet.[18]

Mange foretak har nå gått til konkrete tiltak og begynte å advare sine kunder mot phishing-forsøk.

Senest den 31.03.19 publiserte Hegnar en artikkel hvor Skatteetaten advarer folk mot å la seg lure av falske e-poster eller tekstmeldinger i skatteetatens navn[19]. Dette er særlig viktig på denne tiden av året, ettersom skattemeldingen for 2019 blir klar for store deler av

[13] https://www.nsm.stat.no/globalassets/dokumenter/brosjyrer/phishing_nyn_web.pdf
[14] LB-2013-56387
[15] https://www.dagsavisen.no/rogalandsavis/stavanger-kommune-utbetalte-en-halv-million-til-svindlere-1.1149100

[16] https://www.pwc.no/no/publikasjoner/cybercrime-survey.html

[17] https://www.dinside.no/okonomi/menn-over-50-mest-lettlurte/61017861
[18] https://www.dinside.no/okonomi/menn-over-50-mest-lettlurte/61017861
[19] https://www.hegnar.no/Nyheter/Naeringsliv/2019/03/Skatteetaten-advarer-Ikke-la-deg-lure

befolkningen i begynnelsen av april. I 2018 ble det registrert hele 11 «bølger» med phishing, som foregikk gjennom e-poster og tekstmeldinger. Skatteetaten anmelder selv de groveste phishing forsøkene, men oppfordrer publikum til å være forsiktige[20].

I tillegg til de «sesongbaserte» phishing-forsøkene er det årlig en mengde phishing-forsøk som utgir seg for å være store foretak som Netflix eller Apple, og ber om fornying av abonnementer. Dette har gjentatte ganger vært omtalt i både norske og internasjonale medier[21].

[20] https://norsis.no/se-opp-for-skatterelatert-svindel/?fbclid=IwAR2UzjVYvGkFh_mJyo89_K5u1Al6lzhoGWp5R0Wu1_NMjND1v0d4D5y4LKg (lest 03.03.2019)
[21] https://www.smh.com.au/business/consumer-affairs/netflix-customers-urged-to-be-vigilant-as-high-quality-email-scam-circulates-20190129-p50udt.html

1.4 Avgrensning av oppgaven

I denne oppgaven har jeg hovedsakelig tatt utgangspunkt i phishing ovenfor private personer. Spearphishing og whaling er ikke begreper som benyttes i rettsvitenskapen, samt at disse begrepene sammenblandes med phishing i teorien. En vil imidlertid foreta en analyse av vernet mot phishing i straffeloven §208 som tar for rettstridig tilegnelse av forretningshemmeligheter.

Videre har jeg som følge av oppgavens ordgrense har jeg valgt å konsentrere meg om bestemmelsene som har en viss tilknytning til phishing sin natur. Det er klart at phishing vil kunne være en medvirkende faktor til en rekke lovbrudd. Bestemmelsene er straffeloven §201, §202,§ 204, §208, §321, §361,§370 og §371.

Det avgrenses mot tilfeller av keylogging eller tilfeller der phishing benyttes som middel til å oppnå keylogging. .

Keylogging vil si at man laster ned en programvare på noens datasystem, eller eventuelt villeder noen til å laste en programvare. Med denne programvaren kan man avlytte tastetrykk og informasjon som vedkommende benytter seg av på datamaskinen, i motsetning til et rootkit som gjør at man kan få fullstendig tilgang til en datamaskin. [22]

Jeg har videre valgt å avgrense oppgaven mot EU-EØS-rett, samt vurderinger av hvordan GDPR kan få innvirkning for fremgangsmåten phishing.

Videre avgrenses det i sin helhet mot straffeprosessuelle vurderinger. En ser at det kan være interessant å være ta en vurdering av straffenivået for phishing, men det er sparsommelig med praksis på område.

Avslutningsvis avgrenser en mot internasjonale konvensjoner og traktater som kan være av betydning for datakriminalitet.

[22] Se https://www.decamind.com/2018/07/06/malware-rootkits-keyloggers/

2 Betingelser for straff

2.1 Innledning

Ved innføring av den nye straffeloven[23] ble en rekke nye bestemmelser om datakriminalitet tatt inn i straffeloven. I tillegg til at bestemmelser som eksempelvis §201 og §202 fikk en annerledes utforming. Lovendringene var i stor grad et resultat av datakrimutvalgets utredning. Datakrimutvalget gir i sin utredning klart uttrykk for at straffeloven av 1902 var utilstrekkelig som vern mot datakriminalitet. [24]

2.2 Betingelser for straff

For å kunne idømmes straff etter norsk rett må en rekke vilkår være oppfylt.

Først og fremst er det et vilkår at vedkommende må ha utvist skyld, i norsk rett er skyldkravet forsett, jf. strl. §22. For visse bestemmelser som vil omtales i denne oppgaven er det i tillegg et krav om at man har videregående forsett. I tillegg er det en forutsetning for at man skal kunne domfelles, at det ikke foreligger straffrihetsgrunner.

I vurderingen av om en handling objektivt sett rammes av et straffebud fungerer legalitetsprinsippet som en skranke. Det innebærer at ingen kan dømmes uten etter lov eller straffes uten etter dom[25]. Begrunnelsen ligger i hensynet til rettssikkerhet og forutberegnelighet for borgerne. Et av de sentrale utgangspunktene for legalitetsprinsippet er at lovteksten må være tilstrekkelig tydelig og klar. Det stilles imidlertid ikke et krav om absolutt klarhet i straffebudet[26].

Utgangspunktet er videre at man ikke skal foreta analogiske eller utvidende fortolkninger av lovtekst på strafferettens område[27]. Unntak kan forekomme dersom det foreligger tungtveiende grunner.

[23] Lov av 20. mai 2005 nr. 28
[24] Nou 2007:2 s.9
[25] Lov av 17. mai 1814 nr. 1 § 96.
[26] Rt. 2001 s. 1303
[27] Rt. 1952 s. 989

2.3 Kriteriet "uberettiget"

For flere av bestemmelsene som behandles i denne oppgaven er det et krav om at handlingen må være «uberettiget». Dette gjelder for strl. §201 til strl. §206, i tillegg til at rettstridsvilkåret «uberettiget» omfattes av strl. §321 og strl. §371.

En naturlig språklig forståelse av begrepet tilsier at det er noe som ikke er tillatt, eller er gjort uten tillatelse, uten at det i seg selv kan omfavnes av definisjonen «ulovlig». Det vil normalt sett være et normativt skille mellom hva som er «ulovlig» og hva som er «uberettiget», grensen er imidlertid ikke alltid like klar.

Skillet mellom begrepene ulovlig og uberettiget er i forarbeidene uttrykt som at begrepet «Ulovlig» vanligvis viser til underliggende rettsforhold i henhold til lov eller forskrift. ««Uberettiget» viser for eksempel også til handlinger som er i strid med privatrettslig avtale eller instrukser eller som er i strid med akseptabel atferd på et bestemt livsområde.»[28]

For datakriminalitet var det foreslått av datakrimutvalget at begrepet skulle behandles motsatt. Slik at vilkåret «uberettiget» ville være det avgjørende straffbarhetsvilkåret i vurderingen av om en handling er ulovlig. [29] Departementet tok imidlertid avstand fra en slik forståelse av begrepet, «Uberettiget skal benyttes i de tilfellene hvor det er behov for en noe bredere enn henvisning enn det som naturligvis følger av ordet ulovlig.» [30]

Rettsstridsvilkåret «uberettiget» er normalt å regne som en snever sikkerhetsventil som avgjør hvorvidt en handling skal regnes som straffbar eller lovlig.

I sammenheng med kravet om videregående forsett får man en form for dobbel sikkerhetsventil som verner mot de antatt legitime eller uheldige formene for oppfyllelse av en gjerningsbeskrivelse.

[28] Ot,prp.nr.22 (2008-2009) s. 22
[29] Ot.prp. nr. 22 (2008-2009) s. 22
[30] Ot.prp. nr.22(2008-2009 s. 22 & Ot.prp nr. 8 (2007-2008)

3 Hvordan rammes phishing av straffeloven?

3.1 Straffeloven §201 – anskaffelse av tilgangsdata

Det fremgår av strl. §201 at:
«Med bot eller fengsel inntil 1 år straffes den som 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 samme måte straffes den som uten forsett om å begå en straffbar handling besitter et selvspredende dataprogram, og besittelsen skyldes uberettiget fremstilling eller anskaffelse av programmet.»*

Vilkårene for å oppfylle gjerningsbeskrivelsen er dermed at man «med forsett om å begå en straffbar handling» «uberettiget» «fremstiller, anskaffer bestiller, eller gjør tilgjengelig for en annen» objektene som er definert i bokstav a og b.

Bokstav a retter seg mot kunnskapsbasert tilgangsdata. Mens bokstav b retter seg i større grad mot verktøy eller innretninger som er særskilt egnet til å anvendes i hacking.

Bestemmelsen krever i tillegg til det alminnelige skyldkravet om forsett at man utfører gjerningsbeskrivelsen med forsett «om å begå en straffbar handling». En naturlig språklig forståelse tilsier at man avgrenser mot de rene legitime handlinger, eventuelt straffansvar fordrer i forhold til ordlyden at man har videregående forsett.

I tillegg til at handlingen må være begått forsettlig fastsetter §201 et krav om at befatningen med tilgangsdata må være «uberettiget».

Eksempelvis vil datasikkerhetseksperter ha tilgang til innretninger etter §201 bokstav b med hensikt til å bruke dem i forskning. De vil ha forsett om å begå handlinger som rammes av

diverse gjerningsbeskrivelser i straffeloven kapittel 21, men befatningen og bruken er ikke «uberettiget».

3.1.1 Strl. §201 bokstav a

§201 bokstav a kriminaliserer «befatning» som nevnt i §201 for «passord eller andre opplysninger» som kan gi tilgang til «datasystem eller databasert informasjon».

En naturlig språklig forståelse av passord tilsier at det er tale om en kode som åpner et «datasystem». Ordlyden «Andre opplysninger» omfatter alle opplysninger som kan gi tilgang. som kan gi tilgang.

3.1.2 Strl. §201 bokstav b

Bestemmelsen kriminaliserer befatning med «dataprogram» eller annet som er «særlig egnet» som middel til å begå straffbare handlinger som retter seg mot «datasystem eller databasert informasjon».

En naturlig språklig forståelse av begrepet dataprogram tilsier at det er et verktøy eller innretning som er på et datasystem. Et datasystem vil ikke kunne fungere uten et dataprogram.

Videre kriminaliserer bestemmelsen «annet som er» «særlig egnet» «som middel» til å begå straffbare handlinger. Nøyaktig hvilke straffbare handlinger som omfattes, er ikke spesifisert fordi lovgiver ønsket en fleksibel bestemmelse.[31]

Spørsmålet er hvorvidt «annet» som er «særlig egnet» omfatter falske e-post kontoer og domener. Videre er det et krav om at innretningen må benyttes «som middel» til å begå straffbare handlinger.

Vilkåret «særlig egnet» legger opp til en konkret helhetsvurdering. Av sentrale momenter er hvorvidt innretningen er utviklet eller ervervet med intensjon om å begå en straffbar handling.[32] Videre er det av betydning i hvilken grad dette er innretningens funksjon. Innretningen behøver ikke utelukkende å ha kriminelle bruksområder.

[31] Sunde, *Datakriminalitet*, s. 160
[32] Matningsdal (2019) note 1354

3.1.3 Bestemmelsens betydning for phishing tilfellene

Strl.§201 bokstav a

Spørsmålet er om phishing kan medføre at man «fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen, «passord eller andre opplysninger» som kan gi tilgang til «datasystem eller databasert informasjon».

Selve formålet med phishing er å få tak i sensitive opplysninger. Normalt sett vil det være tale om kredittkortopplysninger, personalia og passord. Opplysninger som i sin natur vil være egnet til å gi tilgang til «datasystem eller databasert informasjon.» .

Hvis en person eksempelvis oppretter et falsk domene, og en rekke godtroende kunder til et etablert foretak fyller inn skjemaet som kommer frem på skjermen, vil man da være i besittelse av en rekke opplysninger om vedkommende. I tillegg til at vedkommende vil kunne blitt bedt om å føre inn et passord. Dermed er handlingen innenfor gjerningsbeskrivelsen i henhold til at man da «uberettiget» har «anskaffet» og satt seg i «besittelse» av «passord eller andre opplysninger» som vil kunne gi tilgang.

For phishing vil det også kunne være aktuelt at man har anskaffet slik informasjon og videreformidlet det til en annen. Slik at man dermed rammes av handlingsalternativet «gjør tilgjengelig for en annen».

De samme vurderingene må gjelde for phishing via falsk e-post og SMS. I begge tilfeller utgir man seg for å være et etablert foretak og forsøker å få personer til å fylle ut et eller flere skjema.

Strl. §201 bokstav a er særlig egnet til å ramme phishing-tilfeller. I praksis vil det sjelden være problematisk med henblikk til videregående forsett i de rene phishing-tilfellene. Slik at den videre vurderingen kun beror på om den innhentede informasjonen er egnet til å gi tilgang til «datasystem eller databasert informasjon». Som en hovedregel vil informasjon som er innhentet via phishing være egnet til å oppnå tilgang til et datasystem, enten i form av at man innhenter passord eller benytter den sensitive informasjonen til å utlede passord eller sikkerhetsspørsmål. Slik at den alminnelige hovedregelen må være at strl. §201 bokstav a rammer phishing.

Strl. §201 bokstav b

Spørsmålet er hvorvidt falske e-post kontoer og falske nettsider kan være «særlig egnet» etter strl. §201 bokstav b. Det favner liten tvil om at kontoer og nettsider som er opprettet i et foretak eller en persons navn vil være straffbart, jf. §202. Spørsmålet er hvor grensen går for innretninger som er «egnet» og de innretninger som kan regnes som «særlig egnet».

«Særlig» legger opp til at den mest fremtredende funksjonen med innretningen er av kriminell karakter. Et eksempel på en innretning som har en særlig fremtredende kriminell funksjon er et root kit. Et root kit er et program som installeres hos brukeren uten at brukeren er klar over det. Vedkommende vil ha tilgang til hele datasystemet uten noen form for autorisasjon fra eieren.[33]

E-post kontoer og nettsider(domener) er som en hovedregel av legitim karakter. Dette stenger imidlertid nødvendigvis ikke for at innretningene kan benyttes til kriminell adferd.

En alminnelig forståelse av disse innretningene vil isolert sett ikke oppfylle lovens krav om at innretningen er «særlig» egnet. Ordlyden innebærer i seg selv at den ikke bare må være egnet, men at det er tale om kvalifisert egnethet.

Det må skilles mellom midler som er særlig egnet på egenhånd, midler som er særlig egnet i forbindelse med andre midler, og midler som kun vil være særlig egnet i konkrete kontekster.

Midler som er særlig egnet på egenhånd omfatter blant annet rootkit, som gir tilgang til et helt datasystem. Midler som er egnet i forbindelse med andre midler er for eksempel skimming-utstyr. Mens det for e-poster og nettsider fordres at de i visse kontekster vil være «særlig egnet».

Forutsetningen er at formuleringen av e-posten eller nettsiden er av en slik karakter at den åpenbart må betraktes å være iscenesatt til å mislede andre.

Det kan forekomme tvilstilfeller hvor innretningen ikke er «særlig egnet» men disse tilfellene vil fanges opp av den doble rettstridsreservasjonen.

[33] https://snl.no/root_kit

Kriteriet «som middel» skiller mellom først punktum og andre punktum i §201 bokstav b. Begrepet er å forstå slik at innretningen må benyttes som et verktøy i sammenheng med overtredelsen. Dette skillet er ment å skille fra kriminalisering av «selvspredende dataprogram» jf. strl. §201 bokstav b siste punktum.

Dersom e-post eller nettside er «særlig egnet» som innretning favner det liten tvil om at bruken vil være «som middel» til å begå en straffbar handling.

3.2 Strl. §202 identitetskrenkelse

Straffeloven §202 kriminaliserer identitetskrenkelser. Bestemmelsen lyder følgende:
«*Med bot eller fengsel inntil 2 år straffes den som uberettiget setter seg i besittelse av en annens identitetsbevis, eller opptrer med en annens identitet eller med en identitet som er lett å forveksle med en annens identitet, med forsett om å*

a) Oppnå en uberettiget vinning for seg eller en annen, eller

b) Påføre en annen tap eller ulempe»

Et identitetsbevis omfatter her pass, førerkort, bankkort som har bilde eller lignende. I tillegg omfattes elektronisk dokument. [34]

Datateknologien har gjort det lettere å opptre med andres eller forvekselbare identiteter. Strl. §202 ble utformet med vern mot identitetskrenkelser som formål. Bestemmelsen er i seg selv teknologinøytral, det vil si at alle alternativene i bestemmelsen kommer til anvendelse uavhengig av om handlingen er begått på internett eller fysisk. Vernet etter §202 gjelder både private personer og foretak, noe som er særlig sentralt i phishing lovbrudd, hvor det gjerne er tale om at både et foretak og en rekke private personer er utsatt for identitetskrenkelse.

Bestemmelsen suppleres i all hovedgrad av reglene om respekt et individs identitet som følger av grunnloven § 102 og EMK. Art 8.

I forarbeidene er det presisert at «identitetskrenkelse kan krenke menneskers integritet og sikkerhet uavhengig av om den rent faktisk fører til videre lovbrudd eller ikke»[35]. Dette er

[34] Ot. Prp. 22(2008-2009) s. 402
[35] Ot.prp. 22 (2008-2009) s. 44

særlig viktig i forhold til phishing lovbrudd. Ettersom det ikke nødvendigvis vil oppstå et videre lovbrudd i etterkant av at de sensitive opplysningene er mottatt.

Videre følger det av forarbeidene at «Det er enklere å bevise identitetskrenkelse enn (forsøk på) den fullbyrdete bedragerihandlingen.» [36]

Dette er relevant ved phishing. Det vil ofte være vanskelig å avdekke et forsøk på, eller bruk av de sensitive opplysningene i bedrageri, før bedrageriet har forekommet. Det vil være enklere å bevise at man har utsatt noen for phishing, enn at man har benyttet de samme opplysningene til å begå bedrageri.

Skyldformen ved identitetskrenkelser er forsett. I tillegg kreves det at forsettet må dekke vilkårene i den objektive gjerningsbeskrivelsen. Videre er det et krav om at vedkommende må ha forsett om å oppnå en uberettiget vinning for strl. §202 bokstav a eller påføre en annen tap eller ulempe etter strl. §202 bokstav b.

Som ved flere av de øvrige datakriminalitetsbestemmelsene er det rettstridsreservasjonen uberettiget som er avgjørende for hvorvidt handlingen kan anses straffbar eller ei. Politiet har for eksempel en rett til å sette seg i besittelse av andres identitetsbevis, jf. politiloven §8.

3.2.1 Kort om grensen mot fiktiv identitet

Det er innledningsvis foretatt en avgrensning mot tilfeller hvor det benyttes fiktiv identitet. Hvorvidt «fiktiv identitet» faller innenfor strl. §202 beror på en vurdering av ordlyden.

En fiktiv identitet må forstås som en konstruert identitet uten tilknytninger til virkeligheten. Spørsmålet er om ordlyden «lett kan forveksles med en annen identitet» omfatter de rent fiktive identiteter.

Matningsdal skriver at «Et typisk eksempel på dette kriteriet er bruk av fiktiv identitet».[37]

Det må imidlertid være av betydning i hvilken grad identiteten er «fiktiv». Hvor grensen mellom en «annens identitet» og noe som «lett kan forveksles» med en annens identitet skal gå.

[36] Ot. Prp. 22 (2008-2009 s. 44
[37] Straffeloven med kommentarer av Magnus Matningsdal (publisert på Rettsdata, revidert 01.01.19) note 1361

3.2.2 Konkret forhold til phishing

Utgangspunktet ved utarbeidelsen av loven var at phishing skulle rammes av bestemmelsen om identitetskrenkelser. [38] Spørsmålet om det faktisk rammes av bestemmelsen beror på om phishing oppfyller den objektive gjerningsbeskrivelsen i strl. §202.

Hvis man for eksempel oppretter en nettside som pretenderer å være et etablert foretak, og flere godtroende kunder skriver inn sine personlige opplysninger i skjemaet vil man som en hovedregel kunne motta for eksempel kredittkort opplysninger,som vil kunne benyttes til å tappe nettbanken eller annen kriminalitet. Koder til nettbank vil også falle innenfor et slikt identitetsbevis.

I det man mottar opplysninger som samsvarer med definisjonen av «identitetsbevis» vil man være i en slik straffbar besittelse som omfattes av strl. §202. I handlingsforløpet vil dette handlingsalternativet kunne være forberedende. Slik at man først kommer i besittelse av et eventuelt identitetsbevis, og deretter «opptrer» med denne identiteten ovenfor en tredje person. På dette tidspunktet er man innenfor strl. §371.

Forutsetningen for at uberettiget befatning med identitetsbevis skal rammes, er at man har forsett om å begå en slik handling som nevnt i §202 i tillegg til at man har forsett om at handlingen utføres for å oppnå en uberettiget vinning for seg eller annen, eller påføre en annen tap eller ulempe.

De mest vanlige phishing formene, som falsk domene, falsk e-post eller SMS vil være egnet til å medføre at vedkommende får besittelse av et identitetsbevis, og vil således kunne rammes av strl. §202, så fremt det foreligger et videregående forsett om at besittelsen skal medføre uberettiget vinning, påføre ulempe eller tap.

Dersom man uthenter en identitet via phishing og deretter benytter denne i transaksjoner ovenfor andre, vil man kunne domfelles for identitetskrenkelse ovenfor begge de berørte parter. Slik at bruk av kredittopplysninger ovenfor en bank, vil være straffbart som identitetskrenkelse både ovenfor den fornærmede som mistet identiteten og banken.

[38] Ot. Prp. 22 (2008-2009) s 46

3.3 Strl. §204 Datainnbrudd

Straffeloven §204 kriminaliserer datainnbrudd, det hitsettes i det følgende:

«Med bot eller fengsel inntil 2 år straffes den som ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystem eller del av det.»

Bestemmelsens ordlyd skiller mellom tilfellene hvor man «bryter» en beskyttelse, og andre «uberettigede» fremgangsmåter.

Skillet ligger primært i fremgangsmåten. En tolkning av ordlyden «bryte beskyttelse» taler for at formuleringen er tiltenkt «hacking», i de tilfellene hvor man bruker koding og andre virkemidler for å bryte ned sikkerhetsfunksjoner og brannmurer.

Hva som kan utgjøre en annen «uberettiget» fremgangsmåte må bero på kontekst. Det er imidlertid på det rene at anvendelsen av tilgangsdata som er ulovlig tilegnet etter §201 vil rammes av annen «uberettiget» fremgangsmåte.. Dette viser en god systematikk i lovgivningen.

Hvilke andre forhold som kan regnes som «uberettigede fremgangsmåter» må nok vurderes konkret og skjønnsmessig, ettersom det ikke foreligger nevneverdig praksis på området, er det vanskelige å sette grenser for hva bestemmelsens ordlyd vil ramme, selve ordlyden «andre uberettigede fremgangsmåter» sier lite om hva som rammes.

3.3.1 Forhold til phishing

Det første spørsmålet er om phishing er egnet til å «bryte» en beskyttelse. Selve ordlyden «bryte» tilsier at det er tale om en form for handling medfører at man kommer seg forbi en barriere eller en sikkerhetsanordning. Ordlyden er mer dekkende for hacking eller bruken av et rootkit.

Hvorvidt phishing direkte rammes av strl. §204 beror i det videre på om phishing kan regnes som en «uberettiget fremgangsmåte» som kan gi «tilgang til datasystem eller del av det.».

Det er på det rene at phishing ikke er en legitim fremgangsmåte, samt at man ved phishing vil kunne få tilgang til opplysninger som nevnt i redegjørelsen av strl. §201. Disse opplysningene er klart egnet til å gi «tilgang til datasystem eller del av det».

Dersom man har oppnådd slik uberettiget befatning med tilgangsdata som omfattes av strl. §201 via phishing, og anvender disse til bruk i datainnbrudd vil handlingen omfattes av strl. §204. Det eneste vilkåret er at innbruddet forekommer ved en «uberettiget» fremgangsmåte som kan gi «tilgang til datasystem eller del av det». Det avgrenses dermed fra tilfeller hvor man foretar datainnbrudd, men for eksempel har autorisasjon til å foreta slikt innbrudd fra den fornærmede.

Dersom vedkommende anskaffer tilgangsdata etter strl. §201, og deretter videreformidler disse til en annen person som benytter dette som ledd i straffbart datainnbrudd etter strl. §204, vil man kunne straffes for medvirkning til strl. §204 dersom man har forsett. Kravene til medvirkning vil i et slikt tilfelle være oppfylt, jf. strl. §15.

3.4 Strl. §208 – rettstridig tilegnelse av forretningshemmeligheter

Etter straffeloven §208 kan man straffes for rettstridig tilegnelse av forretningshemmeligheter.

Av bestemmelsen fremgår det at:

«Med bot eller fengsel inntil 1 år straffes den som rettstridig har oppnådd kunnskap om eller rådighet over en forretningshemmelighet eller tekniske tegninger, beskrivelser, oppskrifter, modeller eller lignende tekniske hjelpemidler.»

Vilkårene for at man skal kunne tiltales er altså at man «rettstridig» har «oppnådd kunnskap om» eller «rådighet over» en forretningshemmelighet eller et av de opplistede alternativene.

Spørsmålet er hvordan begrepet «rettstridig» skal forstås. En naturlig språklig forståelse av begrepet tilsier at det er tale om en handling som går utenfor det man har rett til å gjøre. Det er på det rene at en straffbar handling er rettstridig, dette betyr imidlertid ikke at rettstridige handlinger nødvendigvis er straffbare. [39]

Rettstridig som rettstridsreservasjon sier lite om hva som egentlig rammes av bestemmelsen. Når man derimot har valgt å benytte «rettstridig» istedenfor «uberettiget» i denne

[39] https://snl.no/rettsstridig

bestemmelsen tilsier dette at man har hatt et ønske om lavere terskel for domfellelse etter bestemmelsen. Spesielt sett i lys av at «uberettiget» som begrep er ansett å gå videre enn det som gjelder for «ulovlig».

Dersom man utgir seg for å være en ansatt i et foretak og via e-post forsøker å tilegne seg slik rådighet eller kunnskap som bestemmelsen omtaler, vil handlinger klart være rettstridig..

Det vil også være «rettstridig» dersom man går hen og henter et foretak sin post og åpner denne for å oppnå slik kunnskap eller rådighet som strl. §208 regulerer.

I Rt. 2003 s. 825 har man et tilfelle som reguleres av strl. §208 med nær tilknytning til phishing. I denne saken var imidlertid ikke intensjonen med å opprette et domene navn med likhet til et etablert foretak å utføre phishing, i dommen fremgår det at feilsendte e-poster i begynnelsen ble sendt tilbake. Dersom selskapet ikke hadde sendt e-postene tilbake ville det i realiteten vært tale om phishing.

3.4.1 Forhold til phishing

Phishing er et voksende problem for foretak. Dette viser PWCs cyberrapport[40].

Strl. §208 åpner for domfellelse av personer som «rettstridig» oppnår «kunnskap» eller «rådighet» over forretningshemmeligheter eller lignende. Bestemmelsen er særlig ment å verne mot de mer målrettede formene for phishing, spearphishing og whaling.

Dersom man ser for seg at noen sender en e-post til samtlige ansatte i et foretak, eller utpekte enkeltpersoner, hvor man utgir seg for å være en overordnet ansatt eller en avtalepart og ber om informasjon vedrørende en forestående avtale eller driftshemmeligheter vil man være innenfor bestemmelsens randsone. Slik sett er phishing en dekkende fremgangsmåte for den objektive gjerningsbeskrivelsen.

Det vil også i slike tilfeller være klart at handlingen er «rettstridig». At handlingen er vanskelig å avdekke, gjør den ikke mindre kriminell av den grunn.

Man vil gjennom å anskaffe tilgangsdata via phishing, og benytte dette i et datainnbrudd kunne få rådighet over forretningshemmeligheter, eller noen av de andre handlingsalternativene som er opplistet i strl. §208. I et slikt tilfelle vil selve phishing

[40] https://www.pwc.no/no/publikasjoner/cybercrime-survey.html

handlingen være en forberedende handling til bruddet på strl. §208. Hvis handlingsforløpet utføres av flere personer, vil den som utførte phishing kunne straffes for medvirkning til brudd på strl. §208, forutsatt at det foreligger forsett.

Problematikken med bestemmelsens anvendelsesområde er imidlertid at det ofte vil være vanskelig å bevise at forretningshemmelighetene er tilegnet rettstridig. Phishing er vanskelig å avdekke, og det fordres at den som begår handlingen vil utføre den så anonymt som overhodet mulig.

3.5 Strl. §371 – bedrageri

Reglene om bedrageri er regulert i straffeloven §371. Databedrageri reguleres i strl. §371 bokstav b. Bestemmelsen lyder som følger:

«Med bot eller fengsel inntil 2 år straffes den som med forsett om å skaffe seg eller andre en uberettiget vinning.

a) Fremkaller, styrker eller utnytter en villfarelse og derved rettstridig forleder noen til å gjøre noe eller unnlate noe som volder tap eller fare for tap for noen.

b) Bruker uriktig eller ufullstendig opplysning ,endrer data eller datasystem, disponerer over et kredittkort eller debetkort som tilhører en annen eller på annen måte uberettiget påvirker resultatet av en automatisert databehandling, og derved volder tap eller fare for tap for noen.

En naturlig språklig forståelse av ordlyden tilsier at man må ha et videregående forsett, jf. «Forsett om å skaffe seg eller andre en uberettiget vinning».

Videre er det etter strl. §371 bokstav a et krav om at man har «fremkalt, styrket eller utnyttet en villfarelse» og som følge av dette «forledet» noen til å «gjøre eller unnlate» noe som medfører tap eller fare for tap.

For at vilkårene i strl. §371 bokstav b skal være oppfylt, er det et krav om at man «uberettiget» har påvirket resultatet av en automatisert databehandling. Enten i form av de opplistede handlingsformene eller på «annen måte».

3.5.1 Forholdet mellom bedrageri og databedrageri

Det som skiller databedrageri fra alminnelig bedrageri er først og fremst «villfarelse med påfølgende forledelse»[41].

Brudd på bokstav a forutsetter at lovbryteren forleder en person ved å gi uriktig opplysninger, unnlate å gi eller korrigere opplysninger som vedkommende er klar over at vil være motiverende for den andre part. Mens det for databedrageri etter bokstav b er avgjørende hvorvidt påstått gjerningsperson foretar en handling ovenfor et automatisert datasystem.

Det avgjørende for valget mellom bestemmelsens bokstav a og bokstav b er dermed om personen blir forledet. Dette underbygges av at den alminnelige bedrageri bestemmelsen i bokstav a har forrang fremfor bokstav b. Dette betyr at bokstav a også skal benyttes der «forledelsen» skjer via datateknologi.[42]

I de tilfellene hvor det er tale om at lovbruddet innebærer et datasystem beror valget av bestemmelse på hvorvidt handlingen gjaldt en prosess som var «automatisert» eller om handling gikk ut på at en person ble «forledet». Skillet må vurderes ut i fra den underliggende konteksten.

Det foreligger fullbyrdet bedrageri der handlingen har «voldt tap» eller «fare for tap for noen». Ved alminnelig bedrageri vil tape være voldt av lovbryterens egen handling, ved «forledelsen» eller «villfarelsen». Mens det ved databedrageri vil foreligge tap ved den direkte handlingen som er begått av lovbryteren.

[41] Sunde (2018), s. 118
[42] Sunde (2018) s. 118

3.5.2 Phishing som virkemiddel i bedrageri

Spørsmålet er innledningsvis om phishing kan oppfylle gjerningsbeskrivelsen i strl. §371 bokstav a.

Phishing er en form for handling som er klart egnet til å medføre villfarelse ovenfor et annet individ. Spesielt dersom den falske nettsiden eller e-post adressen fremstår som legitim. Det er videre klart at man rettstridig «forleder» noen til å «gjøre» noe, ved å be dem fylle inn et skjema med personlig informasjon for å fornye for eksempel brukerprofilen hos det etablerte foretaket.

Spørsmålet er imidlertid om man på et så tidlig stadium i et eventuell bedrageri forløp som ved phishingen kan si at vedkommende har et videregående forsett med henhold til at man skal skaffe «seg eller andre en uberettiget vinning» ved å utføre den nevnte handlingen. Dette beror konkret på en vurdering av kontekst.

Phishing er egnet til å oppfylle store deler av gjerningsbeskrivelsen i strl. §371 bokstav a Man er derimot ikke på stadiet for «villfarelse» eller «forledelse» ved utføringen av phishing, det er klart at phishing er egnet til å skape «villfarelse» eller «forledelse» men det er ikke slike tilfeller strl. §371 er myntet på å verne mot.

Inger Marie Sunde skriver at phishing «*...Neppe er å regne som bedrageriforsøk, man er fremdeles på forberedelsesstadiet hvor man «høster» eller «fisker» opplysninger som kan brukes i etterfølgende bedragerier.»*[43]

Det er først når opplysningene fra phishing benyttes til å skape villfarelse eller forlede noen at man er innenfor rammen av strl. §371 bokstav a. Eksempelvis dersom opplysningene benyttes til å opprette falske id-papirer som benyttes til kjøp i butikk. Slik at phishing rent objektivt sett ikke vil kunne oppfylle gjerningsbeskrivelsen i strl. §371 bokstav a. Hva gjelder straffeloven §371 bokstav b, er det som nevnt lagt til grunn at bokstav a har forrang, og i tillegg faller ikke phishing inn under noen av handlingsalternativene i bestemmelsens bokstav b.

At phishing vil være et potensielt virkemiddel til bedrageri er på det rene. Innhentingen av sensitive opplysninger vil kunne benyttes både til villfarelse og forledelse av personer eller

[43] Sunde(2018) s.119

foretak som regulert i §371a. Samtidig vil de samme opplysningene kunne benyttes til å foreta automatiserte handlinger etter §371b.

I tilfeller hvor man anvender opplysninger som er innhentet ved phishing av en annen person, til å begå et bedrageri kan man kan stille seg spørsmålet om hvorvidt phishing-handlingen skal anses som medvirkning til bedrageri etter §371. [44]

3.6 Strl. §361 Dokumentfalsk

Etter strl. §361 vil man kunne straffes for dokumentfalsk dersom nærmere vilkår er oppfylt. Bestemmelsen lyder som følgende:

> «Med bot eller fengsel inntil 2 år straffes den som
> a) ettergjør eller forfalsker et dokument, eller anskaffer et ettergjort eller forfalsket dokument med forsett[2] om bruke det eller la det fremstå som ekte eller uforfalsket,
> b) rettsstridig bruker et dokument som nevnt i bokstav a og lar det fremstå som ekte eller uforfalsket, eller
> c) utsteder et dokument og uriktig tillegger seg en stilling som er av vesentlig betydning for dokumentets bevisverdi, og lar dokumentet fremstå som riktig.
>
> Med dokument menes i dette kapittel en informasjonsbærer[3] som gjelder et rettsforhold eller ellers egner seg som bevis for et rettsforhold.»

Etter bestemmelsens bokstav a vil den som «ettergjør eller forfalsker» et dokument eller anskaffer et «ettergjort eller forfalsket dokument» med forsett om å bruke det eller la det fremstå som «ekte eller forfalsket».

Etter bokstav b er det å «rettstridig» bruke et dokument som nevnt i bokstav a og la det «fremstå som ekte eller uforfalsket.» forbundet med straff.

Bestemmelsens bokstav c tar for seg utstedelse av et dokument som «uriktig tillegger seg en stilling» som er av «vesentlig betydning» for «dokumentets bevisverdi» og lar «dokumentet fremstå som riktig».

Med dokument menes i dette kapittelet en informasjonsbærer som gjelder et rettsforhold eller egner seg som bevis for et rettsforhold.[45] Ordlyden i strl. §76 uttrykker at definisjonen av

[44] Se oppgavens pkt. 4 og 5
[45] Straffeloven §76

informasjonsbærer gjelder i «denne bestemmelse». En naturlig forståelse av dette synes å være at det kan foreligge andre definisjoner av begrepet informasjonsbærer som ikke er i tråd med hva som gjelder i strl. §76.

Informasjonsbærer skal ifølge bestemmelsen forstås som «trykt skrift» eller «annet som formidler» en «skriftlig, visuell, auditiv eller elektronisk lagret informasjon».

Etter bestemmelsens ordlyd vil informasjon som overføres via datasystem rammes av bestemmelsen, jf. «elektronisk lagret informasjon». Dette vil i realiteten omfatte enhver informasjon lagret på et datasystem, således også sensitive opplysninger som er lagret på egen datamaskin, eller sensitive opplysninger som lagres via et falsk domene.

For at bestemmelsen skal få anvendelse er det et krav at man har «forsett om å bruke det eller la det fremstå som ekte eller uforfalsket.».

Kravet til videregående forsett betyr at vedkommende må ha en intensjon om å faktisk begå dokumentfalsk, det at man danner eller ettergjør et dokument er ikke i seg selv tilstrekkelig til at man har begått dokumentfalsk, man må i tillegg ha til intensjon å bruke det eller ikke endre det tilbake til sin originale forstand.

3.6.1 Forhold til phishing

For dokumentfalsk vil phishing som en hovedregel være en forberedende handling. Man nettfisker etter sensitive opplysninger, og anvender deretter disse til å opprette falske dokumenter, id-papirer med videre som man kan benytte til kjøp via nett eller fysisk i butikker.

Moderniseringen av §361 med begrepet «informasjonsbærer» innebærer at bestemmelsen er særlig egnet til å ta for seg datakriminalitetstilfellene.

Phishing vil imidlertid i utgangspunktet være mest relevant som medvirkende faktor til dokumentfalsk.[46]

I slike tilfeller vil §201 imidlertid være anvendbar ovenfor phishing-tilfellet, gjerne også §204 i tilfeller der informasjonen fra phishing-svindelen har medført at man får tilgang til et

[46] Se pkt. 5

datasystem, og fra dette utleder dokumenter som man forfalsker. Sånn sett har loven en god systematikk hva gjelder rammen rundt datakriminelle handlinger.

3.7 Forberedelse til dokumentfalsk

Straffeloven §370 tar for seg forberedelse til dokumentfalsk. Bestemmelsens ordlyd er som følger:

«*Den, som til forberedelse av dokumentfalsk tilvirker, erverver, innfører, utfører, overdrar, besitter eller oppbevarer falsk segl, stempel eller merke eller andre gjenstander, som tilkjennegir seg som bestemte til å benyttes til ettergjørelse eller forfalskning, eller i slik hensikt tilvender seg et ekte segl, stempel eller merke, straffes med bot eller med fengsel inntil 3 år.»*

Selve bestemmelsens utforming er til en viss grad lik slik den var i strl. §186 (strl.1902). Det var imidlertid ikke intensjonen å videreføre strl. §186[47]. §370 var ikke med da man innførte ny straffelov av 2005. Bestemmelsen ble ført innført ved straffelovens ikraftsettingslov av 19.juni.2015.

Det uttaltes i den anledning «Departementet vurderer det på det nåværende tidspunkt slik at det heller ikke er uheldig om bestemmelsen omfatter straffansvar som tidligere ikke var tilsiktet videreført.» [48]

Grunnlaget for at bestemmelsen ble bestemt videreført var at man i rettspraksis benyttet strl. 186(1902) på tilfeller av befatning med skimmingutstyr ut i fra ordlyden «andre gjenstander» som «tilkjennegir seg som bestemte til å benytte seg til ettergjørelse eller forfalskning.». Dersom bestemmelsen ble avskaffet ville man ha et juridisk tomrom for befatning med skimming utstyr, noe som ville være uheldig.

I Rt. 2010 s.1217 kom man til at daværende strl. §186 ikke kunne ramme besittelse av skimming utstyr som var anskaffet i utlandet. På grunn av dommen ble handlealternativene «Innfører, utfører, overdrar, besitter eller oppbevarer» tilføyd.

I praksis er det kun ordlyden «andre gjenstander» som «tilkjennegir seg som bestemte..» som anvendes. Formuleringen «falsk segl, stempel eller merke» er i alle tilfeller utdatert.

[47] Prop. 64L (2014-2015) s. 43
[48] Prop. 64 L (2014-2015 s. 43-44)

Det mest interessante for phishing er hvorvidt «andre gjenstander, som tilkjennegir seg som bestemte til å benyttes til ettergjørelse eller forfalskning,» omfatter falske e-post kontoer, domener og SMS-kontoer. Det er i praksis kun denne delen av bestemmelsen som i dag er anvendbar.

Av bestemmelsen fremgår det et krav om at handlemåten er gjort til «forberedelse av dokumentfalsk». «Dette må tolkes som et hensiktskrav». [49]

Vurderingen beror først og fremst på om e-post kontoer, domener og SMS- kontoer kan regnes som «gjenstand». Etter gjeldende rett er det ingen definisjon av begrepet gjenstand. En naturlig forståelse av begrepet taler for at det er snakk om ting. I strl.§12 er det lagt til grunn at gjenstand omfatter «elektrisk energi eller annen energi». Begrepet gjenstand omfatter i følge forarbeidene hverken opplysninger i en datamaskin eller fra en datamaskin. [50]Slik at bestemmelsen rent objektivt sett ikke rammer phishing. Det vil imidlertid kunne være spørsmål om phishing som medvirkende faktor til brudd på strl. §370.

3.8 Strl. §321 – Tyveri

Det fremgår av strl. §321 at:

«For tyveri straffes 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. Straffen for tyveri er bot eller fengsel inntil 2 år»

Etter bestemmelsen kreves det at man tar en «gjenstand». Begrepet gjenstand er som nevnt ikke definert i hverken lovgivning eller forarbeider. Begrepet er i alminnelig tale synonymt med ting, en gjenstand kan ikke være opplysninger i en datamaskin eller fra en datamaskin. Gjenstanden man tar må «tilhøre en annen», man kan ikke stjele fra seg selv.

Videre er det et krav om at man har videregående forsett, jf. «forsett» om å skaffe «seg eller andre» en «uberettiget vinning». Forsettet må i tillegg omfatte at tyveriet skjer «ved å selge, forbruke eller på annen måte tilegne seg det.»

[49] Husabø (1999) s. 336
[50] NOU 1985:31kap. 4.3.3 s.9 og Ot.prp nr. 90 (2003-2004) kap. 12.2.4 s.165

Phishing vil normalt sett ikke kunne karakteriseres som tyveri. Det er intet som er til hinder for at man har vinnings forsett med henhold til bestemmelsen dersom man utfører phishing. Det som imidlertid stenger bestemmelsen fra å kunne anvendes på phishing tilfellene er begrepet «gjenstand».

Ettersom informasjon fra en datamaskin eller i en datamaskin ikke regnes som gjenstand er det klart at phishing ikke kan omfattes av strl. §321. Selv som forutgående handling til tyveri er det vanskelig å se phishing som en effektiv fremgangsmåte.

.

4 Forsøk

4.1 Generelt om forsøk

Reglene om forsøk er regulert i straffeloven §16. Bestemmelsen lyder som følgende:

«Den 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.

Den som frivillig avstår fra å fullbyrde lovbruddet eller avverger at det blir fullbyrdet, straffes likevel ikke for forsøk».

Vilkårene for å kunne dømmes for forsøk er at man må ha forsett om å fullbyrde en objektiv gjerningsbeskrivelse i et straffebud som vil kunne medføre fengsel i 1 år eller mer. Etter gjeldende rett henviser «forsett om å fullbyrde et lovbrudd» til en vurdering av hvorvidt tiltalte på forsøkstidspunktet hadde fullbyrdelsesforsett for forbrytelsen. I henhold til forarbeidene følger det at alle former for forsett er aktuelle, samt at dekningsprinsippet legger til grunn at vedkommende må ha et forsett som dekker hele gjerningsbeskrivelsen.

Videre er det et krav om at man må foreta noe som «leder direkte mot utføringen.»

Etter gjeldende rett henviser vilkåret til at den nedre grense for straffbar forberedelse må være brutt. Ut i fra rettspraksis beror dette på en helhetlig vurdering hvor hva som er gjort og hva som gjenstår er sentralt. Momenter som er av betydning er «Nærhet i tid, nærhet i omgang og handlingens karakter». I tillegg er den «psykologiske forskjellen» mellom det som er gjort og det som gjenstår av betydning[51].

Man skal ved vurderingen av den «psykologiske forskjellen» legge til grunn den alminnelige oppfatningen og ikke gjerningsmannens subjektive vurdering[52].

Man straffes imidlertid ikke for forsøk dersom man har «frivillig» avstått fra å fullbyrde lovbruddet eller avverger lovbruddet.

[51] Rt. 2008 s. 867 og Rt. 2011 s. 1455
[52] Husabø (1999) s. 292

Grensen for straffbart forsøk er vanskelig å trekke. Spesielt når forsøkshandlingen er av en medvirkende karakter, og det ikke foreligger hverken «nærhet i tid» eller «nærhet i omgang»[53].

4.2 Grensen mellom straffri forberedelse og forsøk

Grensen mellom straffri forberedelse og forsøk ligger først og fremst i ordlyden til straffeloven §16. Etter ordlyden må man ha foretatt noe som er «men å lede direkte til utføringen.». I henhold til forarbeidene formuleres dette som at «Det lovbryteren har foretatt må stå i en tilstrekkelig nær sammenheng med utføringen av lovbruddet, jf. §16 første ledd.»

I forhold til straffbarhetsgrad ligger den straffrie forberedelse forut for forberedelse og forsøk. Straffri forberedelse må vurderes konkret opp mot gjerningsbeskrivelsen til den enkelte bestemmelsen, og vurderes med henhold til hvorvidt forberedelse i det hele tatt er straffbart etter bestemmelsen.
I forhold til bestemmelsene som kriminaliserer forberedelse vil selve problemstillingen bli vanskeligere jf. Pkt. 4.2.

[53] Se pkt. 5.2

4.3 Nærmere om phishing som forsøkshandling i forhold til konkrete straffebud

Spørsmålet er i hvilke tilfeller phishing vil kunne betegnes som en forsøkshandling til følgende straffebud.

4.3.1 Strl. §201

Utgangspunktet er at straffeloven §201 rammer phishing. Tilfellene hvor man ikke fullbyrder handlingen vil som en hovedregel kunne karakteriseres som forsøk, jf. §16.

Hvis en person for eksempel oppretter et falsk domene, eller en falsk e-post adresse, men de «falske» mediene ikke fremstår som troverdige nok til at noen rammes av handlingen, vil det være tale om forsøk, da man ikke har lykkes med å få tak i tilgangsdata. I de aller fleste tilfeller hvor phishing-forsøket ikke slår til, vil vedkommende kunne tiltales for forsøk på brudd på §201.

Spørsmålet om hvorvidt man faktisk kan dømmes for forsøk beror på hvorvidt man kan sies å ha foretatt noe som «leder direkte mot utføringen».

Skillet her går mellom de rent forberedende handlinger og handlinger som har en nærhet i tid, omfang og handlingens karakter.

Et spørsmål er hva som må fremgå av en slik nettside eller e-post for at handlingen skal kunne sies å lede «direkte mot utføringen». Kravene til utformingen av nettsiden eller e-posten må bero på en sammenligning med det etablerte foretak sin nettside eller utsendte e-poster. Det er likhetstrekkene med det originale som bør fastsette hvor langt man har kommet i forhold til utføringen av handlingen.

4.3.2 Strl. §202

For å kunne dømmes for forsøk på identitetskrenkelse må man ha foretatt noe som «leder direkte mot utføringen». For identitetskrenkelsene vil man ha foretatt en slik handling når man oppretter et domene eller en e-post som er «lett å forveksle» med slik domene eller e-post er utformet hos det etablerte foretaket.
Ordlyden «lett å forveksle» setter ikke store krav til hvor nært utformingen av nettside eller e-

post skal være til det etablerte foretaket. Avhengig av kontekst vil det gjerne kunne være tilstrekkelig at det etablerte foretakets logo er på nettsiden, og at den resterende utformingen har trekk av likhet. Det kan neppe forventes at den alminnelige person tar en «skikkelig» sjekk av legitimiteten til en eventuell nettside eller e-post. Dette fordrer at vedkommende allerede er klar over problemstillingene rundt phishing, samt at vedkommende oppfatter nettopp denne e-posten eller nettsiden som et «fare» moment. I slike tilfeller vil man nok gjerne kunne si at e-post eller domene ikke er «lett å forveksle» med den originale.

Tidspunktet for når man trer over fra forberedelse til forsøk er imidlertid vanskelig å avgrense for phishing. Særlig med tanke på at de rene phishing tilfellene forutsetter at man har en falsk e-post konto eller et falsk domene.

Det beror også på hvordan man definerer grensen for identitetskrenkelse etter §202. I Det skal ikke mye til for at et tilfelle subsumeres som identitetskrenkelse etter §202, vilkårene er i praksis ikke særlig strenge. Dette bør også ha betydning for forsøkstilfellene[54]

4.3.3 Strl. §204

Forsøk på datainnbrudd etter §204 fordrer at man har forsett om å «bryte» seg inn eller benytte en annen «uberettiget fremgangsmåte» for å skaffe seg tilgang til «datasystem eller del av det».

Det er «uberettiget fremgangsmåte» som er vurderingstema for phishing. Selve phishing handlingen vil i et slikt tilfelle normalt sett være en forutgående handling for et eventuelt datainnbrudd. Dersom man bruker phishing for å anskaffe tilgangskoder, og deretter anvender disse for å «bryte» seg inn i et datasystem, vil man kunne domfelles for både strl. §201 og §204.

Det konkrete spørsmålet for phishing tilfellene er hvorvidt en phishing handling leder «direkte mot utføringen» av et brudd på straffeloven §204.

Hvis man først utfører phishing for å innhente informasjon, og denne informasjonen deretter forsøkes benyttet i datainnbrudd. Fordres det at phishingen vil være i en slik nærhet i tid, omfang og karakter tid at handlingen skal subsumeres som forsøk. Særlig hvis både phishing

og datainnbrudd begås av samme person, vil det være nærliggende å si at den psykologiske forskjellen mellom det som er gjort og det som gjenstår er liten, ettersom man allerede besitter det man antar vil gi adgang til datasystemet.

I de tilfeller hvor phishing utføres og en annen person benytter informasjonen til å begå datainnbrudd vil det være spørsmål om phishingen kan bedømmes som medvirkning, eller forsøk på medvirkning dersom hovedgjerningsmannen ikke fullfører handlingen. Det vil her være vanskeligere å stadfeste at det foreligger en handling som leder «direkte mot utføringen». Dette avhenger først og fremst av hvor nært handlingene er i tid og omfang.

4.3.4 Strl. §208

Straffeloven §208 ivaretar et vern mot cyberkriminalitet for foretak. I lys av PWCs rapport er dette et voksende problem[55].

Vilkåret er at man «rettstridig» har «oppnådd kunnskap om» eller «rådighet over» en forretningshemmelighet eller et av de andre virkemidlene som listet i bestemmelsen.

For at et phishing tilfelle skal kunne rammes av §208, jf. §16, kreves det først og fremst at vedkommende har foretatt en aktiv handling i relasjon til å utføre den objektive gjerningsbeskrivelsen i §208.

Formålet med phishing ovenfor foretak er i utgangspunktet å oppnå kunnskap eller rådighet over de handlingsalternativene strl. §208 tar for seg.

For at man skal bedømme en phishing handling som forsøk etter §208 er første forutsetning at man har fullbyrdelsesforsett, deretter er spørsmålet hvorvidt handlingen leder «direkte mot utføringen.».

En e-post til foretakets ansatte eller overordnede som ledd i å få kunnskap eller rådighet over forretningshemmeligheter vil normalt være forberedende. Dette fordi man på dette tidspunktet ikke besitter de nødvendige opplysningene til å faktisk få tilgang til slik informasjon, dette fordrer at man har passord eller andre opplysninger som gjør at man får tilgang til «datasystem eller del av det», jf. §204.

[55] https://www.pwc.no/no/publikasjoner/cybercrime-survey.html

Dersom man for eksempel sender en e-post til foretakets ansatte og utgir seg for å ha rettmessig adgang til en forretningshemmelighet, og ber om å få tilsendt informasjon i forhold til denne vil dette være å regne som et forsøk på brudd på strl. §208. Da man klart har foretatt noe som leder «direkte mot utføringen». Det eneste som mangler for at man skal ha fullbyrdet handlingen i et slikt tilfelle, er at man har «oppnådd kunnskap» eller «rådighet» over en forretningshemmelighet.

4.3.5 Strl. §371

Spørsmålet er om phishing vil kunne straffes som forsøk på bedrageri etter strl. §371.

Phishing vil som nevnt være en forutgående handling til eventuelt bedrageri. Denne rekkefølgen i hendelsesforløpet er også den mest normale. I de aller fleste tilfeller utføres phishing som ledd i bedrageri virksomhet. Man benytter den sensitive informasjonen til å begå internettkjøp, opprette falske identifikasjonspapirer eller tappe nettbanken for penger.

Ved phishing vil man «fremkalle» en villfarelse som er egnet til å forlede noen til å unnlate eller gjøre noe som vil kunne volde tap eller fare for tap. Det er klart at tap av sensitive opplysninger vil kunne medføre fare for tap.

Phishing vil klart være en handling som «leder direkte mot utføringen» av hovedgjerningen.

Eksempelvis hvis noen utfører phishing, og opplysningene som er innhentet via phishing benyttes til å opprette nettkontoer til internettkjøp. Da vil man først ved opprettelsen av nettkontoene kunne tale om en fullbyrdelse av den objektive gjerningsbeskrivelsen. Det er imidlertid klart at phishing «leder direkte mot utføringen» av handlingen i et slikt tilfelle.

4.3.6 Strl. §361

Bestemmelsen om dokumentfalsk forutsetter at man «ettergjør» eller «forfalsker» et dokument. Utgangspunktet er at phishing vil være en forberedende handling til dokumentfalsk, da man for å kunne «forfalske» eller «ettergjøre» trenger opplysninger eller et dokument, noe som phishing kan benyttes til å innhente.

Hvis en person eksempelvis benytter phishing som fremgangsmåte for å innhente informasjon som skal anvendes til å utforme et falskt dokument, vil det være spørsmål om hvorvidt phishing handlingen kan bedømmes som forsøk på brudd på strl. §361. Dette avhenger først og fremst av hvorvidt phishing handlingen kan sies å lede «direkte mot utføringen» av dokumentfalsk.

Av særlig betydning er her nærheten i tid og omfang, samt den psykologiske forskjellen mellom det som er utført og det som gjenstår.

Forutsetningen for dokumentfalsk er altså at man har informasjon som kan benyttes eller er i besittelse av, et dokument som skal endres. Når phishing benyttes til å innhente slik informasjon er det klart at handlingen har en nærhet i tid, omfang og karakter til dokumentfalskneriet.

Hvorvidt phishing kan bedømmes som forsøk på dokumentfalsk avhenger dermed av den kontekst som handlingen er utført i. Er phishing utført som ledd i å innhente et dokument som skal ettergjøres eller forfalskes, foreligger det en slik nærhet i handlingens karakter, at den bør bedømmes som forsøk på brudd på strl. §361.

Dersom phishing imidlertid ikke er en nødvendig faktor for at dokumentfalsk skal forekomme, altså at phishingen for eksempel er utført for å dobbeltsjekke troverdigheten av opplysninger man allerede innehar, vil det måtte foretas en konkret vurdering med henhold til momentene som inngår i at handlingen skal lede «direkte mot utføringen».

Phishing som virkemiddel i dokumentfalsk er sånn sett mer relevant som en forutgående handling, i form av forberedelse. I tillegg kan phishing være interessant i forhold til dokumentfalsk som del av organisert kriminalitet.

4.3.7 Strl.§ 370

Phishing kan ikke oppfylle den objektive gjerningsbeskrivelsen i strl. §370. Derfor kan heller ikke på brudd bli en realitet.

I alle tilfeller må det spørres om det i det hele tatt er mulig å oppstille et forsøksansvar for en forberedende handling, selv når denne forberedende handlingen er straffbart etter et eget straffebud. Dette vil kunne være av betydning for fremtidig kriminalisering av forberedende handlinger.

Forholdet mellom forsøk og forberedelse er glidende. Grensen mellom straffbar forberedelse og forsøk er ikke alltid like klar. Grensen mot den straffri forberedelse er også uklar.

Utgangspunktet må være at når lovgiver har tatt et prinsipielt standpunkt om at forberedelse skal straffes, så må også forsøk på forberedelse straffes med mindre annet fremgår av lov. En kan ikke se at forarbeidene tar for seg denne vurderingen.

Det vil være en glidende overgang mellom forsøk og forberedelse med henblikk til strl. §370. De tilfellene hvor det er straffri forberedelse vil således være tilfellene der man ikke er på stadiet for forsøk på forberedelse, altså noe man gjerne kan benevne som «forberedelse» til den straffbare forberedelsen som nevnes i §370. For eksempel vil et kjøp av en datamaskin eller lamineringsmaskin være en form for forberedelse som er straffri. Mens det vil gå over til straffbar forberedelse i det tidspunkt man med sikkerhet kan legge til grunn at lamineringsmaskinen skal benyttes til dokumentfalsk.[56]

Hvis forsøk på forberedelse i det hele tatt skal vurderes som straffbart, forutsetter dette at man vurderer hvorvidt forsøk på forsøk er straffbart. Det har i juridisk teori vært alminnelig konsensus om at forsøk på forsøk ikke er straffbart. Dette ble også slått fast i forarbeidene til strl. 2005[57]

I juridisk teori har blant annet Ståle Eskeland gitt uttrykk for at forsøk på forsøk burde være straffbart[58].

Det er intet i rettspraksis som utelukker at man kan ramme et forsøk på overtredelse av et forsøksdelikt. Selve vurderingen beror i og seg selv på en ordlydsvurdering av straffeloven. Forarbeidene til straffeloven av 2005 har imidlertid utelukket forsøk på forsøk som en ansvarsform. Uten at det gis en generell forklaring på hvorfor.

Det er imidlertid klart at hjemmelskravet i legalitetsprinsippet i grl. §96 og EMK art.6 setter grenser for hvor presis, klar og tilgjengelig lovgivningen skal være. Forsøk er i seg selv et vagt uttrykk, og i den anledning man åpner for forsøk på forsøk vil dette skape åpenbare presisjonsproblemer, og være skadende muligheten til å forutberegne sin egen rettsstilling.

[56] Rt. 2010 s. 1217
[57] Ot. prp. Nr. 90 (2003-2004) s. 417-418
[58] Eskeland (2017) s. 219-220

Ettersom supplering av forsøksreguleringen av strl.§16 med forsøksdelikter er utelukket, må det samme gjelde for eventuell vurdering av forsøk på forberedelse. Da forsøk på forberedelse vil skape de samme presisjonsproblemer som man får ved forsøk på forsøk. Forberedelse er forut for forsøk i handlingsforløpet. Hensynet til borgernes forutberegnelighet vil tale mot en slik ansvarsform[59].

Det stiller seg imidlertid annerledes i vårt tilfelle. Da det er tale om forsøk på straffbar forberedelse, altså et tilfelle hvor selve forberedelsen er gjort straffbar. Forutberegnelighetshensynet vil i all realitet være ivaretatt ved at det foreligger en lovtekst som straffer en forberedende handling. Da må det kunne tenkes at forsøk på den forberedende handlingen er straffbart. Spørsmålet er imidlertid hvor man skal sette den nedre grensen for forsøk i et slikt tilfelle. En kan ikke se at denne konkrete vurderingen er omtalt, og en legger dermed til grunn at vi er i en juridisk gråsone.

Hovedregelen i norsk rett er at forberedende handlinger ikke er straffbare. Selv om man ser et økt fokus og ønske om kriminalisering av forberedende handlinger, blant annet ved innføringen av strl. 201 og videreføringen av strl. §370 er det i utgangspunktet forsøk som er den nedre grensen for straffansvar.

I et tilfelle hvor man har å gjøre med forsøk på forberedelse, vil det være vanskelig å definere hvor grensen for et eventuelt forsøk går, og vurderingene av forsøk og forberedelse vil fort gli inn i en annen.

4.3.8 Strl. §321

Som en følge av at phishing ikke kan oppfylle den objektive gjerningsbeskrivelsen i strl. §321 vil forsøk på brudd på strl. §321 også være uaktuelt.

Hvis phishing skal være straffbart som ledd i tyveri må det være i form av medvirkning, jf. strl. §15.

[59] Frøberg (2012) s. 70

4.4 Tilbaketreden fra forsøk jf. Straffeloven §16 annet ledd

Et spørsmål som reiser seg i forhold til phishing er hvorvidt man kan tre tilbake fra forsøk. For eksempel ved å formidle en beskjed til de personene man har forsøkt å sende ut e-poster eller falske domener til, eventuelt slette det falske domenet før noen har registrert opplysninger. Da vil man i realiteten ha tilbake trådt fra forsøk, forut for at handlingen har blitt fullbyrdet.

En forutsetning for en fullbyrdet phishing handling er nemlig at man har fått rådighet over sensitive opplysninger som følge av handlemåten.

Det kan også være interessant med tilbaketreden fra forsøk i de tilfeller hvor man har utført selve phishing handlingen, men på stadiet hvor man skal utføre internettkjøp med falsk identitet, eller benytte identiteten fysisk i en butikk ombestemmer man seg. Man er da åpenbart innenfor gjerningsbeskrivelsen i §201 og 202, men vil ikke kunne dømmes for forsøk på §371 såfremt man foretar en aktiv tilbaketredelse fra forsøket.

5 Medvirkning

5.1 Generelt om medvirkning

Medvirkning til overtredelsen er av et straffebud er regulert av strl. §15, av bestemmelsen fremgår det at «Et straffebud rammer også den som medvirker til overtredelsen, når ikke annet er bestemt.»

Bestemmelsens ordlyd taler i retning av at medvirkningansvar forutsetter at hovedmannen fullfører sin gjerning, jf. «medvirker» til «Overtredelsen». Det er imidlertid sikker rett at medvirkning er et selvstendig straffansvar[60]. I de tilfeller hvor hovedgjerningsmannen ikke har fullbyrdet sin handling vil imidlertid medvirkeren kun kunne straffes for forsøk på medvirkning. Denne løsningen har konsekvent blitt lagt til grunn i teori, og er ikke endret med ny straffelov av 2005[61].

Ordlyden «medvirker til overtredelsen» innebærer at det må foreligge årsakssammenheng mellom medvirker og overtredelsen av straffebudet.

I tillegg er det på det rene at medvirkeren vil kunne straffes til tross for at hovedmannen er utilregnelig, død, ikke har utvist forsett eller ikke kan straffes fordi handlingen ikke er rettsstridig.

Det skilles mellom medvirkning og samvirke. Samvirke er hvor handlingen er utført av 2 personer sammen, som for eksempel i ran. Det er videre et krav om medvirkeren sin handling må ligge nært opp mot hovedgjerningsmannen handling, formulert av Husabø som følger:

«Utan at medverkaren si handling i tid og karakter ligg nær til ei fullending av sjølve hjelpe, kan det ikkje ein gong bli tale om forsøk på medvirkning»[62].

Det skilles mellom fysisk og psykisk medvirkning. Fysisk medvirkning er tilfellene hvor man fysisk foretar en handling i anledning overtredelsen, gjerne i form av å være sjåfør i et ran eller at man gir et balltre til en person som er i en slåsskamp.

[60] Innst. O nr. 72 (2004-2005) s. 18
[61] Husabø, *Strafferettens Periferi,* s. 200
[62] Husabø, *Strafferettens periferi*, s. 44-45

Den rene psykiske medvirkningen er som regel oppfordring til straffbare handlinger, gjennom ord, handling eller passivitet. Psykisk medvirkning forutsetter positiv tilskyndelse, altså at man «aktivt» har oppfordret vedkommende til å foreta en handling. For psykisk medvirkning gjelder videre et krav om at den som medvirker har styrket gjerningsmannens forsett[63].

Både fysisk og psykisk medvirkning kan være relevant ved datakriminalitet, men den rene fysiske medvirkningen vil være mer normalt.

Det avgrenses mot etterfølgende bistand, avtaler om etterfølgende bistand som er gjort forut for lovbruddet regnes som psykisk medvirkning og vil være straffbart.

[63] Grøning, Husabø, Jacobsen (2016) s.343

5.2 Phishing som medvirkende årsaksfaktor

5.2.1 Strl. §201

Spørsmålet er hvorvidt phishing kan være en handling som medvirker til overtredelse av strl. §201.

Et tilfelle som kan være relevant er hvor en person utfører phishing og kommer i besittelse av opplysninger. Hvilke opplysninger han er i besittelse av er han imidlertid ikke klar over. Disse opplysningene videreformidles til en tredjemann som benytter dette til å anskaffe tilgangskoder. I et slikt tilfelle vil man ha medvirket til gjerningsmannens overtredelse. Etter strl.§201 vil handlingen imidlertid måtte regnes som et fullbyrdet brudd på straffebudet, med bakgrunn i bestemmelsens formulering: «gjør tilgjengelig for en annen». Dermed vil man ikke kunne tale om medvirkning, dersom handlingen benevnes som å «gjøre tilgjengelig for en annen», og som en hovedregel vil de opplysninger som innhentes via phishing være egnet til å dekkes av strl. §201 bokstav a.

Som et utgangspunkt er altså phishing som handling rammet av strl. §201, dette medfører at eventuelt medvirkningansvar for brudd på strl. §201 ikke er særlig praktisk, da man i utgangspunktet vil ha fullbyrdet straffebudet på egenhånd, eller i samvirke.

5.2.2 Strl. §202

Straffeloven §202 er en praktisk bestemmelse ovenfor salg av opplysninger, samt i forhold til bistand ved opprettelse av nettsider, e-poster eller SMS-kontoer.

Et problem med phishing er muligheten for videresalg av opplysninger.[64] Enten det er identitetsinformasjon eller passord til sosiale medier.

Det er ubestridt at den som begår phishing-handlingen vil kunne straffeforfølges for identitetskrenkelse, spørsmålet er om man i tillegg vil kunne straffes for handlingen som er utført av den man har solgt opplysningene til. Det mest naturlige er å besvare et slikt spørsmål bekreftende. Man har klart medvirket til overtredelsen, og spørsmålet om dette skal tillegges

[64] https://www.dinside.no/okonomi/sa-mye-er-opplysninger-om-deg-verd-for-kriminelle/69969257

straffansvar beror på om medvirkning har en slik nærhet i tid og karakter til fullbyrdelsen av forbrytelsen at det vil være naturlig å forbinde den med straffansvar.

Bistand til opprettelse av nettside, e-post konto eller SMS-konto vil også være relevant. Dersom en IT-kyndig person hjelper et annet individ å opprette slike kontoer, i den intensjon at disse skal benyttes til phishing vil det kunne stilles spørsmål til om vedkommende kan dømmes for medvirkning til brudd på strl. §202. En slik domfellelse fordrer først og fremst at vedkommende er klar over hva den innretningen han oppretter skal benyttes til. I tillegg til at det må foreligge en nærhet i tid og karakter som gir grunnlag for å si at man har medvirket til brudd på strl. §202. Det foreligger ikke en identitetskrenkelse før noen har plottet inn informasjonen sin i skjemaet og sendt det inn, iallefall ikke ovenfor de fornærmede, ovenfor foretaket vil det foreligge en identitetskrenkelse på tidspunktet man oppretter slike kontoer, og da synes det klart at det foreligger medvirkning.

5.2.3 Strl. §204

For at man skal kunne domfelles etter §204 er det som nevnt et vilkår at man har «brutt» seg inn på datasystem eller fått tilgang ved annen «uberettiget fremgangsmåte».

For phishing sin del er det vurderingen av om det foreligger en «uberettiget fremgangsmåte» som er relevant.

Innbrudd i et datasystem forutsetter ikke nødvendigvis at man «bryter» seg inn. Man kan få tilgang blant annet gjennom å få tak i passord, tilgangskoder eller andre former for godkjennelsesbevis som datasystemet vil godta.

Hvis man med forsett begår phishing for å tilegne seg passord til et datasystem som skal benyttes til datainnbrudd av en annen person, favner det liten tvil om at man «medvirker til overtredelsen». Medvirkeren sin handling i et slikt tilfelle en forutsetning for at hovedgjerningsmannen skal kunne begå sitt lovbrudd.

En phishing handling vil både kunne betegnes som psykisk og fysisk medvirkning. Fysisk medvirkning i form av at man overleverer passord, psykisk medvirkning i form av at man ved å overlevere passord oppfordrer hovedgjerningsmannen til å begå lovbruddet.

Dersom tilgangskoder eller passord overleveres en annen uten at er klar over at det har skjedd, vil det kunne betegnes som passiv medvirkning dersom man oppdager overleveringen forut

for fullbyrdelsen av lovbruddet. Forutsetningen er at man har et handlingsalternativ, altså at man kan foreta en aktiv handling for å forhindre lovbruddet. I dette ligger det videre et spørsmål om hvorvidt man har tid og mulighet til å gjennomføre en handling, samt om det er rimelig å forvente av vedkommende sett i lys av situasjonen.

Dersom man vil utsette seg selv for særlig fare ved å foreta en slik aktiv handling vil det normalt sett ikke være forbundet med straffansvar. Høyesterett har imidlertid i visse tilfeller forbundet straffansvar med passiv medvirkning til tross for at det har vært fare for medvirkeren[65].

5.2.4 Strl. §208

Straffeloven §208 verner om forretningshemmeligheter og andre driftshemmeligheter.

For at et phishing tilfelle skal kunne subsumeres som medvirkning til brudd på §208 er utgangspunktet at man må ha gitt noen informasjon som kan gi tilgang til «kunnskap» om forretningshemmeligheter eller «rådighet over» slike hemmeligheter.

Hvis man eksempelvis bistår noen med å opprette en e-post konto som fremstår som en ansatt i et foretak, og denne benyttes til å oppnå kunnskap om eller rådighet over forretningshemmeligheter er man klart innenfor medvirkningsansvaret etter §15.

Phishing som medvirkning til strl. §208 forutsetter i realiteten at man foretar noe fysisk. Det er lite som tilsier at man gjennom phishing passivt kan medvirke til brudd på strl. §208. Med henhold til årsakskravet som oppstilles mellom den medvirkende handling og overtredelsen synes dette å være korrekt.

Forsøk på medvirkning vil kunne forekomme både i form av oppfordring og fysisk handling.

5.2.5 Strl. §371

Som en hovedregel vil phishing alltid være en forberedende handling til bedrageri.

Som en forberedende handling til bedrageri bør det kunne forutsettes at handlingen har en slik medvirkende karakter at den styrker gjerningsmannens forsett, samt at det er

[65] Rt. 1995 s. 355

årsakssammenheng mellom medvirkerens handling og hovedgjerningsmannens overtredelse av straffebudet.

Det er klart at phishing vil kunne være medvirkende til både å villede personer eller foretak etter strl. §371 bokstav a og vil kunne være en medvirkende faktor til brudd på strl. §371 bokstav b. I form av at man kan få tak i passord eller andre former for opplysninger som gjør at man endre på en automatisert databehandling.

Selve bedrageriet kan forekomme på en rekke forskjellige måter. Enten i form av internettkjøp, bankuttak eller andre økonomiske disposisjoner.

En kan vanskelig se for seg et tilfelle hvor phishing er benyttet som ledd i bedrageri, og dette ikke rammes av medvirkningsbestemmelsen i strl. §15. Da informasjonen enten den blir brukt eller ei vil ha hatt betydning for gjerningsmannens forsett, enten i form av fysisk eller psykisk påvirkning.

5.2.6 Strl. §361

Medvirkning til brudd på strl. §360 om dokumentfalsk vil være praktisk mulig ved phishing. Særlig ettersom man for å kunne begå dokumentfalsk trenger informasjon eller dokumentasjon som er egnet til å være troverdig ovenfor den alminnelige person.

For dokumentfalsk, vil phishing som medvirkende årsaksfaktor ligge i kort tid forut for hovedgjerningen, og vil som et utgangspunkt være det som starter dokumentfalskneriet. Det fordres at ethvert phishing tilfelle som er ledd i dokumentfalskneri vil kunne bedømmes som medvirkning til dokumentfalsk, i det tilfellet at hovedgjerningsmannen ikke utfører sin handling vil man være innenfor grensene for forsøk på medvirkning.

Praktisk sett er det den rent fysiske medvirkningen som vil være relevant. Fordi man ved phishing er ute etter fysisk informasjon som kan benyttes til å skape troverdighet over det dokument man har dannet. Enten dette er et elektronisk eller fysisk dokument jf. strl. §76.

5.2.7 Strl. §370

Spørsmålet er i hvilken grad phishing som handling kan være medvirkende til forberedelse til dokumentfalsk etter strl. §370.

Phishing kan som et utgangspunkt være en medvirkende handling til forberedelse til dokumentfalsk, da handlingen ikke oppfyller den objektive gjerningsbeskrivelsen.

Hvis man utfører phishing og opplysningene brukes til å danne falske identifikasjonspapirer, vil man kunne straffes for medvirkning til forberedelse til dokumentfalsk.[66]

Bistand til opprettelse av falske kontoer som skal benyttes til å innhente informasjon til bruk i dokumentfalsk vil også kunne rammes som en medvirkende handling til strl. §370.

Det største skillet er at man ved phishing som medvirkende handling til strl. §370 vil kunne dømmes selv om hovedgjerningsmannen ikke utføres dokumentfalsk, ettersom selve forberedelsen er straffbar.

5.2.8 Strl. §321

Phishing vil som nevnt ikke kunne fullbyrde et brudd på strl. §321 på grunn av ordlyden "gjenstand".

Spørsmålet er om phishing kan være medvirkende til et brudd på strl. §321.

Dersom man eksempelvis utgir seg for å være et forsikringsselskap og ber kunder om å fylle inn en oversikt over eiendeler og verdi, vil man være i besittelse av informasjon kan skape store gevinster ved tyveri. Dersom opplysningene benyttes av en annen til å begå tyveri, vil den som har utført kunne straffes for medvirkning til overtredelsen.

Det fordres at man også vil kunne straffes for bistand til opprettelsen av e-post eller nettside som utgir seg for å være forsikringsselskapet.

Dersom gjerningsmannen avstår fra å fullbyrde sin handling vil personen som utførte phishing kunne domfelles for forsøk på medvirkning.

[66] LB-2016-50124

5.3 Særlig om forsøk på medvirkning

Etter straffeloven §15 kan man straffes for medvirkning dersom man «medvirker til overtredelsen».

Hovedregelen er at medvirkning et selvstendig ansvar. Fra straffebudets ordlyd kan det trekkes ut at man må «medvirke» til en «overtredelse.» En forutsetningen for at man skal kunne medvirke er dermed at hovedmannen faktisk fullfører den straffbare handlingen. En slik tolkning av loven er i tråd med den juridiske teori og rettspraksis[67].

I tilfellene hvor hovedmannen ikke fullfører sin handling er det lagt til grunn at man kan straffe den som «medvirket» for forsøk på medvirkning. Man vil for eksempel ha et tilfelle av forsøk på medvirkning dersom en person fisker etter opplysninger og overgir disse til en annen person, men opplysningene viser seg å være feilaktige. Dette vil kunne medføre straffansvar for den som utfører phishingen, for forsøk på medvirkning.

Et krav for at man kan straffes for forsøk på medvirkning er imidlertid som for annen medvirkning at medvirkeren sin handling har en nær relasjon til hovedmannens gjerning.

Best formulert av Husabø ved følgende sitat:

«Utan at medverkaren si handling i tid og karakter ligg nær til ei fullending av sjølve hjelpe, kan det ikkje ein gong bli tale om forsøk på medvirkning»[68].

For phishing sitt vedkommende er dette av betydning. Hvis en person fisker etter sensitive opplysninger, og deretter legger disse til sides, uten intensjon om at de skal benyttes av noen. En del år senere videreformidles opplysningene til en annen. Spørsmål om handlingen har den tilstrekkelige nærheten i tid og omfang som gjør at den medvirker til hovedmannens gjerning vil da oppstå. I det konkrete eksempelet er imidlertid opplysningene av en så essensiell verdi for hovedmannens gjerning at vedkommende bør dømmes for medvirkning. En motsatt løsning ville hverken vært i tråd med den allmenne rettstanken eller de rådende hensyn på strafferettens område.

[67] Husabø (1999) s. 200
[68] Husabø (1999) s. 44-45

6 Konkurrens

6.1 Generelt om konkurrens

Konkurrens er spørsmålet om ulike bestemmelser som rammer en og samme handling kan anvendes om hverandre, og i tillegg hvorvidt like straffbare handlinger skal bedømmes som ett fortsatt forhold, samlet forhold eller som flere enkeltstående forhold. Det skilles mellom idealkonkurrens og realkonkurrens.

Flere av bestemmelsene som tar for seg datakriminalitet ble først inntatt ved straffeloven av 2005, det er således sparsommelig med praksis hva gjelder konkurrens på området. En vil således i stor grad måtte se til forarbeidenes vurdering av konkurrens.

Reglene om konkurrens fremgår først og fremst av ulovfestet rett[69].

Strl. §79 som tar for seg forhøyelse av straff er av betydning. Etter bestemmelsen kan man dersom det foreligger et av tilfellene som er definert i bestemmelsens bokstav a til c foreta en forhøyelse av straffen opptil det dobbelte. Det er bestemmelsens bokstav a som er av betydning for konkurrens tilfellene. Av denne fremgår det at man kan forhøye straffen inntil det dobbelte når:

«En lovbryter ved en eller flere handlinger har begått flere lovbrudd og det skal idømmes en felles straff.»

I tillegg er strl. §29 annet ledd av betydning for konkurrens da den stiller et krav om en proporsjonalitetsvurdering. Enhver reaksjon må stå i et proporsjonalt forhold til lovbrudd(ene) som er begått.

Bestemmelsene sett i sammenheng gir et utgangspunkt for konkurrens vurderinger, særlig proporsjonalitetsvurderingen etter §29. Selve reglene om konkurrens følger imidlertid av ulovfestet rett.

[69] Rt. 2003 s. 1376

I denne oppgaven anser man ulikeartet idealkonkurrens for å være det mest interessante. Altså spørsmålet om hvorvidt man kan anvende flere straffebud ovenfor en og samme handling.

Vurderingen må foretas etter ulovfestet rett, momentene er utpenslet i rettspraksis. Den ulovfestede læren om konkurrens er formulert på følgende måte:

«Konkurrenslæren innebærer at når en straffbar handling omfattes av flere straffebud, anvendes bare ett straffebud dersom det fullt ut dekker samtlige sider av det straffbare forholdet. Flere straffebud anvendes når dette er nødvendig for å markere momenter ved den straffbare handling som ikke blir markert om man bare anvender et straffebud. Når retten er avskåret fra å anvende et straffebud på grunn av konkurrensreglene, følger av rettskraftreglene at det ikke kan reises ny tiltale etter dette straffebudet når det er avsagt dom i saken.» [70]

Vilkårene for at man skal kunne anvende flere straffebud er altså at man ved å anvende flere straffebud favner over noe mer ved handlingen. I denne vurderingen spiller hvilke formål og hensyn som ligger bak straffebudet sentral betydning. I tillegg er det vært å bemerke seg at man ikke kan anvende gradsbestemmelser i konkurrens. I utgangspunktet vil derfor strl. §361 og strl. §370 ikke kunne anvendes i konkurrens ovenfor samme tilfellet. Altså man kan ikke tiltale noen både for forberedelse til dokumentfalsk og dokumentfalsk. Strl. §370 tar for seg en mer forebyggende effekt enn det som er ment ved strl. §361, hensynsforskjellen har imidlertid ikke betydning, da man ikke markerer en større del av den straffbare handlingen ved å anvende begge. Forarbeidene uttrykker at dataspesifikke lovbrudd skal kunne anvendes i konkurrens med andre straffebud.[71]

6.2 Konkret om konkurrens

Systematikken i lovgivningen legger opp til at det for et tilfelle av datakriminalitet vil kunne straffeforfølges etter flere bestemmelser. Som nevnt vil for eksempel informasjon som uthentes ved phishing være straffbart etter §201, bruken av denne til å oppnå tilgang til datasystem er straffbart etter §204, og begge handlinger vil være å regne som en identitetskrenkelse ovenfor den fornærmede, enten dette er en enkeltperson eller et foretak.

[70] Se Rt. 2003 s. 1376.
[71] NOU 2007:2 s. 43: «*Dataspesifikke lovbrudd forutsettes overtrådt ved dataspesifikke fremgangsmåter og følgelig skal kunne anvendes i konkurrens med andre straffebud, der det er naturlig.»*

De enkelte bestemmelsene i straffelovens kapittel 21 har sine egne formål og favner om ulike hensyn.

Eksempelvis er Strl. §202 ment til å forebygge og forhindre krenkelse av personers identitet, det rådende hensynet er vernet av enkeltindividers identitet. Sammenlignet med strl. §208 er denne ment til å vernet foretak mot cyberkriminalitet som ledd i oppnå forretningshemmeligheter. Det er således klart at disse to bestemmelsene vil kunne anvendes i konkurrens.

Som et utgangspunkt gjelder dette også de øvrige bestemmelsene i straffelovens kapittel 21, foruten særbestemmelser og gradsbestemmelser.

Man vil ved å tiltale både etter §201 og §202 ikke bare verne over flere hensyn, men også ramme en større del av den handlingen som er forekommet, og dette er en av nøklene ved forståelsen av konkurrens.

Også innad i strl. §201 vil man kunne anvende strl. §201a i konkurrens med strl. §201b. Dette skyldes at de tar for seg forskjellige hensyn. Punkt a er ment til å forebygge passordinnbrudd, mens bokstav b tar for seg forbud mot hacker-verktøy som i realiteten skal hindre at man blir utsatt for forsøk på innbrudd mot et datasystem, jf. §204. Slik sett er §204 og §201b nært tilknyttet. Men også disse bestemmelsene bør som en hovedregel kunne anvendes i konkurrens, ettersom de tar for seg forskjellige deler av handlingsforløpet.

I henhold til den konkrete anvendelsen av §201 i forhold til de øvrige bestemmelsene i kapittel 21, og tilhørende bestemmelser som er nevnt i denne oppgaven fordres det at § 201 kan anvendes i konkurrens med §§204, 205(b), 206, 351, 361 og 371.

Den kanskje mest interessante konkurrens vurderingen med henhold til strl. §201 er hvorvidt bestemmelsen kan anvendes i konkurrens med strl. §370. Særlig også sett i lys av at man vurderte å plassere strl. §370 som et eget ledd i strl. §201[72].

Strl. §201 og Strl.§370 vil kunne dekke deler av samme handlingsforløp. Særlig ettersom Strl. §201 er ment til å dekke også deler av forberedende handlinger. Dette følger blant annet av at Norge tidligere hadde reservert seg mot art. 6 i datakrimkonvensjonen, som kriminaliserer dataverktøy som er tilpasset eller utviklet med hensikt om å begå straffbare handlinger, jf.

[72] NOU 2007:2

Art. 6 nr.3. Ved innføringen av strl. §201 trakk man reservasjonen ovenfor art. 6. Forarbeidene til bestemmelsen legger opp til at det ved særskilt behov vil kunne straffe forberedende handlinger, men forholder seg i tråd med at forsøk fortsatt er å anse som den nedre grensen for straffbarhet i norsk rett.

Dette skaper en nærhet i hva bestemmelsen skal dekke av handlingsforløp, og man vil få en viss overlapping. Denne overlappingen vil imidlertid ikke dekke samme sider av handlingen, ettersom en forberedelse til dokumentfalsk, og innhentelse av tilgangsdata i realiteten vil være forskjellige hendelser. Begge deler kan i realiteten skje før den andre, avhengig av hva man er ute etter. Under visse omstendigheter kan disse anvendes i konkurrens.

Visse spesialbestemmelser vil imidlertid stenge for at man anvender andre bestemmelser såfremt man er innenfor spesialbestemmelsen sitt område. Dette gjelder blant annet for strl. §203 som tar for uberettiget tilgang til fjernsynssignaler.

Innenfor område for spesialbestemmelser vil man altså ikke kunne anvende i konkurrens såfremt handlingen dekkes av denne bestemmelsen. De deler av handlingsforløpet som faller utenfor spesialbestemmelsens regulering vil imidlertid kunne rammes av generelle lovbestemmelser. Ved en konkurrens vurdering vil man derfor måtte se fra det generelle til det spesielle, altså foreta en konkret vurdering av om handlingen rammes av en særbestemmelse.

7 Konklusjon

7.1 Hvordan rammes phishing av nåværende lovgivning?

Oppgavens overordnede problemstilling er hvordan phishing rammes etter nåværende lovgivning. Et videre spørsmål er hvorvidt lovgivningen anses tilstrekkelig til å verne mot tilfeller av phishing.

Som redegjort for vil phishing kunne rammes av flere av bestemmelsene i straffeloven. For visse bestemmelser er det klart at phishing må betraktes som en forberedende handling til hovedgjerningen, slik at det eventuelt må bli tale om medvirkningansvar.

Selv om phishing er en forberedende handling, vil forsøk på phishing kunne rammes av strl. §201 og strl. §202. Forsøk på phishing ovenfor foretak vil også kunne rammes av strl. §208 hvis man er ute etter forretningshemmeligheter eller lignende.

Bruken av opplysningene man uthenter vil kunne rammes av strl. §204 dersom de benyttes til datainnbrudd. Dersom opplysningene benyttes til straffbare handlingen vil den som utførte phishingen kunne straffes for medvirkning til overtredelsen.

Phishing vil kunne være en forberedende handling til dokumentfalsk, men handlingen vil ikke kunne oppfylle vilkårene i strl. §361. Phishing som medvirkende faktor til brudd på strl. §361 er derimot praktisk. Opplysningene som innhentes via phishing vil kunne benyttes til å danne falske dokumenter.

Et videre spørsmål er hvorvidt phishing rammes av strl. §370 om forberedelse til dokument falsk. Bestemmelsen er ikke anvendt på lignende tilfeller tidligere. Men forarbeidene har som vist åpnet for at bestemmelsen kan ramme videre enn det strl. §186(1902) gjorde. Ordlyden «gjenstand» stenger for at bestemmelsen kan anvendes på phishing.

Phishing rammes av flere av bestemmelsene i straffeloven. Lovgivningen anses å gi et tilstrekkelig vern mot phishing som fremgangsmåte, også i form av forsøk eller medvirkning. Det kan imidlertid vurderes om det ville vært hensiktsmessig å gjøre befatning med innretninger som er egnet til phishing straffbart, slik som man har for skimming-tilfellene.

Slik sett vil man kunne domfelle for datakriminelle handlinger på et tidligere stadium i hendelsesforløpet. Problematikken med datakriminalitet er at man ofte sliter med å avdekke hvem som er gjerningsmannen, dersom man åpner for å straffe befatning med innretninger som er egnet til datakriminalitet vil man i større grad kunne strafferettslige verne mot datakriminelle handlinger.

Eksempelvis vil en kriminalisering av befatning med falske e-post adresser eller nettsider kunne medføre at flere tilfeller blir oppdaget tidligere. Det fordres at innretningene som benyttes til phishing vil fremstå som troverdige, slik at dersom man oppdager at noen er i besittelse av slike innretninger vil det være uproblematisk å legge til grunn at disse er tiltenkt benyttet i phishing eller annen lignende datakriminalitet.

Reguleringen av forberedende handlinger vil kunne være hensiktsmessig for å få et mer effektivt vern mot datakriminelle handlinger.

7.2 Lovvurdering

Et interessant spørsmål er hvorvidt ytterliggere lovgivning, eller endring av nåværende lovgivning vil gi en mer tilfredsstillende strafferettslig regulering av phishing-tilfellene.

I forarbeidene til straffelovens ikraftsettingslov av 19.juni 2015 var det et spørsmål om hvorvidt man skulle innføre strl. §186 som egen bestemmelse eller legge til et nytt ledd i strl. §201. Dette resulterte i at man utarbeidet strl. §370. Bestemmelsen er i liten grad prøvd i rettslig sammenheng, og man har således ikke fått en «pekepinn» på hvor langt bestemmelsen rekker. Selve formuleringen har imidlertid medført at informasjon fra og i data faller utenfor bestemmelsen.

I forarbeidene ble det vurdert hvorvidt man ønsket å i større grad ramme forberedende handlinger. [73] En har i forarbeidene lagt til grunn at strl. §370 var et bedre valg enn et nytt ledd i strl. §201 blant annet fordi den ville kunne «fange opp nye metoder som ikke rammes av forslaget til strl. §201 annet ledd.»

Det ble gjort et poeng ut av at innføringen av strl. §370 ville kunne blitt gjort som et ledd i å i større grad kriminalisere forberedende handlinger. [74] Høringsinstansen har uttrykt dette som at

[73] Prop. 64l (2014-2015) s. 43
[74] Prop. 64l (2014-2015) s. 43

«Det er ikke helt upraktisk at man kommer over bedrageri forsøk knyttet til dokumenter hvor det kunne ha vært ønskelig å ha mulighet til å straffe også forberedende handlinger.»

For visse handlingsformer vil det kunne være ønskelig å ramme på et forberedende stadium. Spesielt for de typene handlinger som er særlig alvorlige eller vanskelige å avdekke hvem som har utført. Kan avstraffelse på et tidligere stadium være forebyggende. Phishing er en type fremgangsmåte som normalt sett utføres av datakyndige personer som ikke har et ønske om å bli oppdaget, via internett kan man skjule både identitet og lokasjon, slik sett er det forståelig at få tilfeller av phishing domfelles.

Det var ønskelig at bestemmelsen skulle ramme videre enn tidligere, samt at man gav uttrykk for et ønske om å i større grad straffe forberedende handlinger. Når man da valgte å videreføre strl. §370 med formuleringen «gjenstand» stengte man for at bestemmelsen kunne anvendes på datakriminelle innretninger. I tillegg er det merkverdig at man videreførte formuleringen «falsk segl, stempel eller merke» når de tilfellene som har forekommet i praksis har falt under samle betegnelsen «andre gjenstander».

Hvis bestemmelsen hadde vært innført som et nytt ledd i straffeloven §201 hadde dette neppe gått utover reguleringen av skimming-tilfellene. Det er vanskeligere å oppdage at noen utfører phishing enn det er å ta fra dem utstyret som de kan benytte til å begå phishing.

I alle tilfeller synes det klart at strl. §370 tar for seg de samme tilfellene som var under §186. I praksis har man iallefall ikke sett noen nye metoder som rammes etter bestemmelsen.

Sannsynligvis vil datakriminalitet som forberedende handling til andre straffebud rammes av medvirkningsansvaret. Men spørsmålet er om dette vil være tilstrekkelig. I visse tilfeller er phishing begått såpass langt forut i tid til hovedgjerningen at man ikke kan tale om et medvirkningansvar. I slike tilfeller vil det være hensiktsmessig å kunne straffe på forberedelsesstadiet.

I tillegg fordres det at en av grunnene til at man ikke avdekker gjerningspersonene bak phishing er at phishing som en hovedregel vil være forberedende. At personen som utfører phishing ikke vil være den samme som utfører bedrageriet, og at den som utførte phishingen forholder seg anonym.

Spørsmålet er om en strafferettslig kriminalisering av forberedende handlinger vil kunne forebygge mot phishing i en større grad.

Dersom den som «tilvirker, erverver, innfører, utfører, overdrar, besitter eller oppbevarer» falske e-poster, domener eller SMS-kontoer som pretenderer å være andre kunne domfelles etter strl.§370 ville man klart kunne straffe phishing forut for at det handlingen skjer. En slik forståelse vil også innebære at man vil kunne tiltales for hver part som er krenket som følge av de falske fremgangsmåtene. Grensen mellom handlinger som faller utenfor og innenfor bestemmelsen må i så tilfelle bero på troverdigheten av det falske middelet.

En slik bestemmelse vil også være uproblematisk med henhold til konkurrens. Strl. §201 og §202 vil som en hovedregel ramme phishing. Strl. §370 verner om allmennhetens sikkerhet på internett. I tillegg til at den tar for seg noe mer med handlingen en hva som dekkes gjennom de to ovennevnte bestemmelsene , selve bruken av en falsk innretning. I tillegg er det intet som tilsier at man ikke er i besittelse av flere falske innretninger.

Dersom man endret strl. §370 til å ta for seg «innretning» istedenfor «gjenstand» ville man ha løst problemet. Eller som nevnt innført et nytt ledd i strl. §201.

7.2.1 "Masseutsendelse av elektroniske meldinger"

I datakrimutvalgets utredning ble en rekke nye forslag til bestemmelser fremmet. Ikke alle bestemmelsene ble tatt inn. I utkast §14 var en bestemmelse som ville kunne ramme phishing på et tidligere stadium enn det man oppnår med nåværende lovgivning.

Utkastet lyder:

«For ulovlig masseutsendelse straffes den som sender elektroniske meldinger som ledd i masseutsendelse til mottakere som ikke har samtykket. Denne bestemmelsen gjelder ikke utsendelse av meldinger i eksisterende kundeforhold, til medlemmer eller lignende med mindre mottakeren har reservert seg mot slike meldinger.»[75]

En naturlig språklig forståelse av ordlyden tilsier at bestemmelsen kriminaliserer såkalt «spam» post. I følge en rapport fra Datasikkerhetsselskapet Kaspersky er 54% av all e-post som mottas spam post, en rekke av disse spam e-postene er phishing-tilfeller.[76]

Phishing vil være egnet til å dekke den objektive gjerningsbeskrivelsen i bestemmelsen.

[75] NOU 2007:2 kap. 9.14 s. 166
[76] https://www.duocircle.com/phishing-protection/top-phishing-email-attacks-worldwide-in-2018

Det at man hadde et ønske om å straffe allerede på stadiet for «masseutsendelse» viser at bestemmelsen var ment å ha et forebyggende element ovenfor slike former for svindel som phishing. Bestemmelsen ville sannsynligvis ha virket avskrekkende på datakriminelle. I tillegg vil bestemmelsen verne mot invasjonen av søppel post i personers private innbokser, noe som gjerne ikke er straffbart per dags dato, men fortsatt kan oppfattes som krenkende.

Dersom lovgiver ikke har som intensjon at phishing skal rammes av strl. §370 vil en slik bestemmelse om spam post være svært effektiv i reguleringen av phishing.

8 Avsluttende bemerkninger

Avgjørende for straffbarheten av phishing er altså en forståelse av hva phishing utgjør i hendelsesforløpet, dette er sentralt for hvorvidt et phishing tilfelle kan bedømmes som fullbyrdet brudd på et straffebud, forsøk eller medvirkning. I tillegg kan phishing medføre vanskelige vurderinger mht. skille mellom straffbar forberedelse og forsøk.

I praksis ser man at domfellelses av personer for datakriminalitet ikke nødvendigvis stopper at handlingene forekommer, ofte vil det i realiteten føre til at noen andre «overtar» prosessen. I tillegg er det i mange tilfeller tale om gjengangsforbrytelser, hvor det er en stor mengde fornærmede, dette er av betydning for straffutmålingen.

Norge fikk i Januar 2019 en egen digitaliseringsminister. Dette vil bidra til at man får flere rettspolitiske vurderinger og debatter rundt hvordan lovgivningen rundt datakriminalitet bør utformes. Storbritannia fikk digitaliseringsminister i 2016 og har etter det bestemt seg for å danne en egen spesialdomstol som tar for seg datakriminalitet. En kan sånn sett forvente at det blir et økt fokus på datakriminalitet i Norsk rett fremover, og at man derfor vil få flere bestemmelser som tar for seg datakriminalitet.

9 Litteratur

a. Litteraturliste

- Husabø (1999), Erling Johannes Husabø – Strafferettens periferi – Medvirkning, forsøk, førebuing, Universitetsforlaget 1999.

- Matningsdal(2016), Magnus Matningsdal, Norsk Spesiell strafferett, Fagbokforlaget 2016.

- Grøning, Husabø, Jacobsen(2016), Linda Grøning, Erling Johannes Husabø og Jørn Jacobsen, Frihet, forbrytelse og straff – En systematisk fremstilling av norsk strafferett. – Fagbokforlaget 2016.

- Matningsdal(2017, revidert 01.01.19), Magnus Matningsdal – Straffeloven med kommentarer – universitetsforlaget 2017 (publisert på rettsdata).

- Eskeland (2017), Ståle Eskeland – Strafferett 5. utgave – Cappelen Damm Akademisk 2017

- Sunde (2018), Inger Marie Sunde, Datakriminalitet – En fremstilling av strafferettslige regler om datakriminalitet, 2. opplag, fagbokforlaget 2016.
-

- Skoghøy (2018), Jens Edvin A. Skoghøy, Rett og rettsanvendelse, Universitetsforlaget 2018.

b. Tidsskrifter eller publikasjoner

- Thomas Frøberg «Forsøkansvarets yttergrenser: Forsøk på forsøk og uaktsomt forsøk(2012), tidsskrift for rettsvitenskap 2012 s.49-90(TFR-2012-49), Universitetsforlaget
-

c. Lovgivning

- Kongeriket Norges Grunnlov, gitt i riksforsamling på Eidsvoll 17.mai 1814.
- Lov om straff (straffeloven), LOV-2005-05-20-28
- Lov om menneskerett (menneskerettsloven) , LOV-1999-05-21-30.

d. Forarbeider

- Ot. Prp. Nr. 22 (2008-2009) om lov om endringer i straffeloven 20.mai 2005 nr. 28
- NOU:2007:2 Datakriminalitetsutvalget. Lovtiltak mot datakriminalitet
- Prop. 64L (2014-2015) om Straffelovens ikraftsettingslov av 19.06.15
- NOU 1985:31 om Datakriminalitet
- Ot.prp nr. 90 (2003-2004) om lov om straff av 2005.

e. Domsregister

- Rt..1952 s.989
- Rt. 1982 s. 1315
- Rt. 1984 s. 1320
- Rt. 2003 s.1276
- Rt. 2003 s.825
- Rt. 2008 s. 867
- Rt. 2010 s. 1217
- Rt. 2011 s. 1455
- Rt. 2011 s. 1232
- LB-2013-56387
- TBERG2017-164611
- TOSLO-2010-1173
- TFOLL-2008-99861-2

f. Artikler

- https://www.datatilsynet.no/personvern-pa-ulike-omrader/politi-justis/terrorbekjempelse-og-regelverksutvikling/om-datalagringsdirektivet/
- https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709
- https://snl.no/root_kit
- https://no.wikipedia.org/wiki/Phishing
- https://www.dinside.no/okonomi/menn-over-50-mest-lettlurte/61017861
- https://www.pwc.no/no/publikasjoner/cybercrime-survey.html
- https://www.digi.no/artikler/bruker-samme-passord-overalt/201158
- https://www.hegnar.no/Nyheter/Naeringsliv/2019/03/Skatteetaten-advarer-Ikke-la-deg-lure
- https://www.smh.com.au/business/consumer-affairs/netflix-customers-urged-to-be-vigilant-as-high-quality-email-scam-circulates-20190129-p50udt.html
- https://snl.no/phishing
- https://www.dinside.no/okonomi/sa-mye-er-opplysninger-om-deg-verd-for-kriminelle/69969257
- https://www.duocircle.com/phishing-protection/top-phishing-email-attacks-worldwide-in-2018
- https://snl.no/rettsstridig
-