Responsum vedr. intern viden, ekstern server & hacking

1. Baggrund

Topdanmark, har anmodet mig om at foretage en juridisk vurdering af den sag, der er omfattet af Finanstilsynets skrivelse af 13/10 2010, der er en partshøring over et udkast til politianmeldelse mod Topdanmark.

Til brug for udarbejdelsen har jeg fået forelagt skriftvekslingen mellem tilsynet og Topdanmark samt de bilag, der nævnes i skrivelserne. Jeg har således fået forelagt tilsynets ovennævnte skrivelse af 13/10 2010 med de deri nævnte bilag.

2. Sagens faktum

Sagen synes velbeskrevet i det fremlagte materiale og der synes ikke at være uenighed mellem parterne om det faktiske hændelsesforløb.

Meget kort gengivet flyttede en medarbejder i Topdanmark et eller flere filer fra deres placering i Topdanmarks interne server set-up, hvortil adgang udefra ikke er mulig, over til den eksterne server i forbindelse med forberedelsen af offentliggørelsen af Topdanmarks første kvartalsregnskab 2010 (Q1). Overførselen til den eksterne servers webroot muliggjorde ekstern adgang, men indebar **ikke** at oplysningerne lå frit tilgængelige som en hjemmeside, men alene, at udefrakommende ved såkaldt URL-hacking, kunne fremfinde scriptet og de informationer, der lå der. Overførselen fandt sted kl. 11:43. Kl. 11:44 tilgik en enkelt, ekstern PC de pågældende filer, og Kl. 11:52 kontaktede Reuters Topdanmark og meddelte, at de havde tal fra Q1, og at de ville offentliggøre disse tal straks på trods af Topdanmarks protester herover. Offentliggørelsen skete fra Reuters kl. 11:55-11:59, og kl. 12:01 foretog Topdanmark offentliggørelse i fuld overensstemmelse med reglerne herfor.

Jeg forstår Finanstilsynets skrivelser således, at tilsynet er enigt i dette hændelsesforløb, og at styrelsen accepterer, at man ikke foretog en "bevidst" eller "villet" offentliggørelse, men at der var tale om en af Topdanmark uønsket og utilsigtet situation. Spørgsmålet, som vil blive behandlet i det følgende, er herefter alene, hvilke retlige konsekvenser dette faktum kan have – herunder især om det kan indebære et strafferetligt ansvar for Topdanmark.

3. Retlig vurdering

3.1 Oplysningernes karakter

Der er ingen uenighed mellem parterne om, at Q 1 rummer oplysninger, der må karakteres som intern viden i værdipapirhandelslovens forstand. Dette lægges ubestridt til grund i det følgende, idet jeg er enig i vurderingen heraf.

3.2 Identifikation af den formodede strafbare adfærd.

Ved den retlige vurdering af det under punkt 2) beskrevne faktum, er det centralt at identificere hvor i forløbet, Finanstilsynet mener Topdanmarks medarbejder (og dermed Topdanmark) har handlet ansvarspådragende. Af Finanstilsynets skrivelse af 13/10 til SØK (i det følgende kaldet "notatet") fremgår, at det centrale tidspunkt for alle de bestemmelser, der, efter Finanstilsynets vurdering er overtrådt, er kl. 11:43, og at den strafbare adfærd for alle de nævnte bestemmelsers vedkommende derfor består i, at en medarbejder på dette tidspunkt overfører data fra den interne server til webroot 'en i den eksterne server.

Der nævnes således intet i vurderingen om Reuters efterfølgende URL-hacking, om Topdanmarks forsøg på at standse Reuters offentliggørelse af tallene eller om Reuters faktiske offentliggørelse heraf. Der nævnes heller intet om at Topdanmark mindre end 15 minutter efter de mulige lovovertrædelser faktisk foretager offentliggørelse på en måde, der mig bekendt lever op til alle regelsæt herom.

3.3 De enkelte forhold

3.3.1 forholdene overordnet herunder deres sammenhæng

Finanstilsynet henviser i sit notat til tre forskellige bestemmelser: VPL § 27a, stk. 1-3 om den korrekte offentliggørelsesmåde, VPL § 36 om videregivelse af intern viden og VPL § 37 om pligten til at udarbejde interne regler.

Det er ikke ganske klart om tilsynet er af den opfattelse, at alle tre regelsæt er overtrådt ved én og samme handling, eller om tilsynet er af den opfattelse, at nogle af regelsættene er gensidigt udelukkende.

I indledningen til notatet af 13/10 (den del, der bærer overskriften: "notat") anføres, at det er "Finanstilsynets vurdering, at Topdanmark har overtrådt" og derefter nævnes alle tre regelsæt uden angivelse af, om der er tale om en akkumulerende eller en alternativ opremsning. Sprogligt set forekommer opremsningen primært akkumulerende. Dette modsiges imidlertid længere omme i notatet i den del, der er udformet som en skrivelse til SØK. Det hedder således her s. 1, at Finanstilsynet anmoder om en politimæssig efterforskning af, om § 36 om videregivelse af intern viden er overtrådt. Derefter fortsættes: "Lægges det til grund, at der er sket offentliggørelse, gøres det gældende at…" Topdanmark har overtrådt § 27a ved at have offentliggjort på utilstrækkelig vis. Herefter skrives: "Lægges det til grund, at der hverken er sket videregivelse eller offentliggørelse" gør Finanstilsynet gældende, at der så er tale om en overtrædelse af VPL § 37 om manglende regelsæt til sikring af fortrolige oplysninger.

Tilsynet vender hverken før eller senere i den foreliggende brevveksling tilbage til disse spørgsmål om, hvorvidt anvendelse af den ene bestemmelse måtte udelukke anvendelse af den anden.

Jeg skal undlade på dette sted at forsøge at gisne om, hvorledes Finanstilsynet måtte opfatte det skrevne og reglernes anvendelse, men i stedet vurdere hver enkelt bestemmelse for sig, og derefter vende tilbage til spørgsmålet i den afrundende vurdering i afsnit 5.

3.3.2 VPL § 27a - offentliggørelsesmåden

VPL § 27 a, stk. 1 – 3 lyder således:

> »En udsteder af omsættelige værdipapirer omfattet af § 2, stk. 1, nr. 1, skal ved offentliggørelse af oplysninger i henhold til dette kapitel sikre, at offentliggørelsen sker på en sådan måde, at oplysningerne hurtigt bliver tilgængelige i hele Den Europæiske Union og lande, som Fællesskabet har indgået aftale med på det finansielle område.
> *Stk.2.* En udsteder som nævnt i stk. 1 skal samtidig med offentliggørelsen indsende oplysningerne til Finanstilsynet.
> *Stk.3.* En udsteder som nævnt i stk. 1 skal indsende oplysninger, der er offentliggjort i henhold til stk. 1, til Finanstilsynet, som opbevarer oplysningerne. Finanstilsynet kan udpege andre myndigheder eller juridiske personer i og uden for landet til at varetage opgaven.«

Bestemmelsen anviser, som det fremgår, en bestemt offentliggørelsesmåde. Anvendelsen af bestemmelsen forudsætter derfor, at Topdanmark har foretaget "offentliggørelse" af oplysninger.

Af VPL § 27 – som § 27a skal læses i sammenhæng med – fremgår (forenklet), at offentliggørelse af intern viden skal ske snarest muligt. Af VPL § 27, stk. 5, fremgår, at

> »En udsteder af værdipapirer som nævnt i stk. 1 skal uden ugrundet ophold og i et passende tidsrum efter, at offentliggørelse af intern viden er sket i henhold til stk. 1 eller 2, lade al sådan viden figurere på sin hjemmeside«

Man kan– forenklet – forstå reglerne således, at § 27 foreskriver offentliggørelse (af § 27, stk. 5, fremgår at "offentliggørelse" på hjemmesiden ikke betragtes som offentliggørelse i § 27's forstand), og at § 27a foreskriver, at offentliggørelse (i § 27's forstand) skal ske på en bestemt måde, samt at oplysningerne skal indsendes til Finanstilsynet.

For det tilfælde, at regelsæt kræver, at offentliggørelse kan ske via en hjemmeside, må man naturligvis stille visse krav til en sådan offentliggørelsesmåde, for at den kan antages at leve op til sit formål.

Et eksempel herpå kunne være CESR[1]'s guideline no. 5 til et af MIFID-direktiverne[2], hvor følgende angives:

> »GUIDELINE n°5:
> In respect of arrangements facilitating the consolidation of data as required in Article 32(b) of the Implementing Regulation, CESR considers information as being made public in accordance with that article, if it:
> i) is accessible by automated electronic means in a machine readable way;
> ii) utilizes technology that facilitates consolidation of the data and permits

[1] THE COMMITTEE OF EUROPEAN SECURITIES REGULATORS.
[2] Direktiv nr. 2004/39/EF

> commercially viable usage; and
> iii) is accompanied by instructions outlining how users can access the information.
> CESR considers that an arrangement fulfills the 'machine-readable' criteria where the data:
> i) is in a physical form that is designed to be read by a computer;
> ii) is in a location on a computer storage device where that location is known in advance by the party wishing to access the data; and
> iii) is in a format that is known in advance by the party wishing to access the data.
> CESR considers that publication on a non-machine readable website would not meet the MiFID requirements.«

Som det fremgår af ovenstående guideline, er det bl.a. en betingelse for, at offentliggørelse kan antages at have fundet sted, at brugere skal have oplysninger om, hvorledes de kan tilgå de relevante data, og for at der skal være tale om en maskinlæsbar offentliggørelse, skal såvel placering som format være kendt af den, der vil have tilgang til dataene. Ingen af delene er opfyldt i nærværende sag.

Ser vi på gerningsindholdet I VPL § 27a, anviser dette en bestemt adfærd, når vi befinder os i en situation, der er beskrevet på følgende måde: "ved offentliggørelse af oplysninger i henhold til dette kapitel".

Den adfærd, der er foretaget fra Topdanmarks side, hvorefter data er blevet placeret i webroot 'en, men uden nogen form for linkadgang eller anden ydre angivelse på hjemmesiden af, hvorledes de pågældende data kunne fremfindes, vil helt oplagt **ikke** leve op til kravene om "offentliggørelse af oplysninger". Man kan således ikke tale om, at man foretager "offentliggørelse" ved at placere oplysningerne et andet sted, der er lige så skjult for omverdenen, som det hele tiden har været. Forestillede man sig, at en virksomhed blev bebrejdet, at den ikke havde offentliggjort de oplysninger, den skulle, og at den forsvarede sig med, at den havde lagt oplysningerne ind i sin webroot, uden at linke hertil – ville man med rette afvise et sådant forsvar: Når omverdenen ikke ved, at der ligger data det pågældende sted, og offentligheden ikke har mulighed for at finde frem til dataene på normal vis, må det være indlysende, at der ikke er sket "offentliggørelse". Det svarer til, at man ville påstå offentliggørelse, hvis man uset af andre flyttede sine oplysninger fra en låst skrivebordsskuffe (en server uden adgang udefra) til en ulåst skrivebordsskuffe (en server med adgang udefra).

Når Topdanmark hverken objektivt eller subjektivt har ønsket at offentliggøre Q1 kl. 11:43 overhovedet, er det meningsløst at bebrejde (og dermed ønske at straffe for) Topdanmark, at man ikke foretog offentliggørelse på den foreskrevne *måde*.

Forudsætningen for strafansvar for overtrædelse af § 27a stk. 1 vil således ud over det objektive krav, være det subjektive: at gerningsmanden indså eller burde have indset, at offentliggørelse fandt sted på en måde, der ikke efterkom kravene i § 27a. Da medarbejderen næppe havde forsæt til eller handlede uagtsomt i relation til, at dataene blev "offentliggjort" i og med overflytningen til den eksterne server og webroot 'en der, kan man selvsagt ikke bebrejde ham, at han ikke overvejede, om offentliggørelsesmåden nu levede op til kravene i § 27a – han tænkte ikke over dette, og han burde ikke have tænkt over dette.

Det må derfor konkluderes, at § 27a stk. 1-3 hverken objektivt eller subjektivt er overtrådt af Topdanmarks medarbejder, og at Topdanmark derfor heller ikke bærer noget strafansvar i den anledning. Straffelovens § 27,stk. 1, foreskriver således, at forudsætningen for selskabsansvar enten er, at der kan findes en medarbejder, der har handlet med den fornødne tilregnelse (hvilket, jf. ovenfor, ikke er opfyldt her), eller at man kan bebrejde Topdanmark "som sådan" den skete lovovertrædelse. Da der ikke objektivt er sket nogen lovovertrædelse, og da vi her ved, hvorledes "lækagen" er opstået, og hvilken medarbejder, der har været

involveret, og da der ikke i sagen er noget, der tyder på manglende instruktion eller lignende fra Topdanmarks side, er heller ikke de subjektive krav for selskabsansvar opfyldt.

3.3.3 VPL § 36 – videregivelse af intern information

Hvor den hævdede potentielle overtrædelse af VPL § 27a må forekomme noget malplaceret, når ingen offentliggørelse hverken var intenderet eller kunne siges at finde sted, er tanken om en uagtsom videregivelse af intern viden ved en "sjuskefejl", der ikke medfører "offentliggørelse" men nok at en anden person, der ikke har normal adgang til oplysningerne, kommer i besiddelse af dem, ikke udelukket på forhånd. Kan man med andre ord sidestille denne situation med en situation, hvor to medarbejdere i en virksomhed taler vel højlydt med hinanden om virksomhedens erhvervshemmeligheder, medens de sidder ved et bord i lufthavnen og venter på deres fly, og en storøret journalist ved nabobordet flittigt skriver på sin blok og dagen efter bringer erhvervshemmelighederne i avisen? I ingen af tilfældene var nogen form for videregivelse således intenderet, men den blev resultatet[3].

Omdrejningspunktet for den retlige vurdering er ordlyden af VPL § 36, der er ganske enkel:

> »Den, der er i besiddelse af intern viden, må ikke videregive denne viden til andre, medmindre videregivelsen er et normalt led i udøvelsen af vedkommendes beskæftigelse, erhverv eller funktion.«

Finanstilsynet behandler i sit notat spørgsmålet om, hvorvidt "videregivelsen" af oplysningerne kunne anses for berettiget, herunder hvorvidt videregivelsen var et "normalt led" i udøvelsen af vedkommendes beskæftigelse o.s.v.. Tilsynet synes imidlertid at forbigå det helt centrale spørgsmål: Var der overhovedet tale om "videregivelse", da dataene blev overført fra den interne til den eksterne server? Og det næste led – som heller ikke ofres megen opmærksomhed i notatet – er spørgsmålet om medarbejderens tilregnelse i den relation.

Der er næppe nogen tvivl om, at "videregivelse" også kan ske ved passivitet eller ved en sløsethed, der fritlægger informationerne. *Vagn Greve* anfører[4] bl.a. at: "[e]n viderebringelse kan også ske gennem passivitet, f.eks. derved at fortrolige oplysninger ikke opbevares forsvarligt". *Greve & Langsted* anfører et andet sted[5] vedrørende selskabsledelsens tavshedspligt, at det "ikke kan udelukkes, at passivitet efter omstændighederne kan være tilstrækkeligt. Hvis direktøren undlader at rydde op på sit bord, skønt han/hun ved, at nogle journalister skal sidde der i en længere periode og vente på ham/hende senere på dagen, vil undladelsen kunne være en røbelse – i hvert fald af de oplysninger, som uden videre kan ses."

Fælles for de ovennævnte citater og eksempler er, at den person, der skal "passe på" hemmelighederne, blotlægger dem for en mindre eller større kreds ved sin uforsigtighed. Det afgørende i denne sag vil således være, om den uforsigtighed, der er udvist hos medarbejderen i Topdanmark er af en sådan karakter, at der er tale om uagtsomhed, dels om den opfylder gerningsindholdet i VPL § 36 om viderebringelse.

[33] Se for et tilsvarende eksempel *Vagn Greve* i FSRs årsskrift 1991, Skatteret/erhvervsret, s. 117 i artiklen "Erhvervsspionage – i strafferetlig belysning".
[4] A.st. s. 120
[5] I Hovedlinjer i Erhvervsstrafferetten, 6. udgave, s. 131.

Analysen heraf rummer to elementer: for det første om placeringen i webroot 'en kunne anses for en "prisgivelse" af oplysningerne, og for det andet hvilken betydning det har i den relation, hvorvidt andres adgang til informationen forudsatte strafbart forhold?

Som nævnt ovenfor i afsnit 3.3.1 er der ikke tale om, at medarbejderens adfærd har blotlagt oplysningerne på selve hjemmesiden, som det ellers ses i nogle tilfælde vedrørende følsomme oplysninger etc. Medarbejderen hos Topdanmark har overført dataene fra en "lukket" til en "åben" server, men har endnu ikke (kl. 11:43) lagt oplysninger eller links hertil ud på selve hjemmesiden. Det vil således ikke være muligt for en "tilfældig gæst ved nabobordet" at "lytte med". Herved adskiller nærværende sag sig fra de eksempler, der i øvrigt nævnes i litteraturen. Man kunne sige, at faktum i nærværende sag mere minder om en situation, hvor den, der er i besiddelse af oplysningerne, ikke taler med en kollega om dem i fuld offentlighed i lufthavnen (som i litteraturens eksempler), men derimod hjemme på kontoret, hvor en forbipasserende imidlertid stopper op uden for døren og lytter med. Tilsvarende afviger denne sag fra eksemplet med det rodede skrivebord, således at skrivebordet her faktisk er både rent og ryddeligt, og der ligger ingen dokumenter fremme, men da direktøren et øjeblik er ude, begynder gæsterne at rode rundt i lukkede skuffer og skabe på kontoret.

Det andet spørgsmål, der er relevant i denne sammenhæng er, om den person, der skal sætte sig i besiddelse af informationerne, vil begå noget strafbart ved at gøre det. For at kunne tale om en videregivelse skal der således være en afgiver og en modtager – og hvis modtageren ikke uden videre kan modtage informationen, men skal foretage sig en strafbar handling for at sætte sig i besiddelse af den, vil det naturligvis afsvække antagelsen af, at afgiveren har handlet strafbart.

Den anvendte metode til at sætte sig i besiddelse af de oplysninger, der var blevet overført fra den interne til den eksterne server var en såkaldt "URL-hacking". Den indebærer, at man i browserens adressefelt (URL'en) forsøger at skrive en række forskellige filadresser og filnavne for det tilfælde, at de skulle ramme en eksisterende fil/mappe. Der er således ikke tale om, at man "ved et uheld" kan komme til at ramme ned i data, der ligger på webroot 'en, men om at man skal søge målrettet efter de pågældende data for at finde dem. Det er ligeledes klart, at filer og data, der ikke ligger "oppe" i brugerinterfacet, men er "gemt" længere nede, ikke er filer og data, man umiddelbart ønsker at andre skal rode rundt i. Ønskede man nemlig det, ville man linke til dem eller lade dem optræde direkte på hjemmesiden.

Det nævnes til tider[6], at URL-hacking ikke skulle være strafbar. Dette er imidlertid højest usikkert. Straffelovens § 263, stk. 2 og 3, der omfatter hacking, strafbelægger således den, der »uberettiget skaffer sig adgang til en andens oplysninger eller programmer«. Det afgørende er, om hackeren handler "uberettiget" ved at skaffe sig adgang til oplysningerne, ikke som udgangspunkt hvorledes oplysningerne har været opbevaret, herunder om hackeren i forvejen måtte have adgang til systemet (men ikke til oplysningerne). Af Straffelovrådet anførtes i betænkningen om datakriminalitet[7], at man kunne forestille sig områder, hvor "den ansatte vel må siges at være gået udenfor sine arbejdsopgaver, men dog ikke på en sådan måde, at han bør straffes".

[6] Ikke i den juridiske litteratur, hvor spørgsmålet i den danske litteratur i hvert fald er uomtalt, men på nogle websider, hvor spørgsmålet diskuteres.
[7] Bet. 1032/1985, s. 26.

Mads Bryde Andersen anfører[8], at der i retsanvendelsen "… nødvendigvis [må] foretages en udskillelse af de mindre alvorlige former for uautoriseret adgang (jf. forbeholdet: "den, der uberettiget skaffer sig …"). Dette retsstridighedskrav vil typisk være opfyldt, når tilgangen til de pågældende data eller programmer er muliggjort gennem anvendelse af passwords eller kalderutiner, som almindeligvis holdes konfidentielle, eller som i øvrigt ikke er almindeligt tilgængelige … "

Der er for mig ingen berettiget tvivl om, at det forhold, at data ligger på en server, hvortil der er offentlig adgang, ikke i sig selv fratager dataene/programmerne beskyttelsen efter § 263. Heller ikke selv om det er muligt at "komme til" de pågældende data via dataejerens egen hjemmeside. Faktisk vil mange former for hacking foregå via offerets hjemmeside og om "bag" denne[9]. Det er ganske det samme, der er sket i denne sag. Som det oplyses i notatet, vil tilgang til oplysningerne kunne ske ved, at hackeren "gætter sig" til stier enten »manuelt eller maskinelt«. Denne proces er ganske den samme, som når hackere forsøger at "gætte sig" til passwords. Forskellen ligger således ikke i den teknik, hackeren skal bruge, men alene i, at oplysninger, der er "gemt" bag et password, synligt for alle er uvedkommende for andre, medens andre oplysninger ikke så tydeligt er det. Da det imidlertid, jf. ovenfor er klart i teorien, at man også kan krænke § 263 ved at søge efter oplysninger, selvom man er legalt i besiddelse af det password, der normalt beskytter disse oplysninger mod uvedkommende, kan man ikke opstille som et krav, at man kun er beskyttet mod hacking, hvis man "gemmer" oplysninger bag et password.

Som det er fremgået, er det usikkert – og der findes mig bekendt ingen retspraksis om det – hvorvidt URL-hacking er strafbar som en overtrædelse af straffelovens § 263. Spørgsmålet vil næppe kunne besvares generelt, men må afhænge af en konkret vurdering. At oplysningerne konkret ikke har været beskyttet af et password eller lignende taler imod, mens oplysningernes karakter og det forhold, at de ikke var "lagt frem" på hjemmesiden endnu (det var øjensynligt hackeren bekendt, at oplysningerne snart ville blive offentliggjort), men skulle offentliggøres umiddelbart efter på en bestemt måde, taler klart for at anse anskaffelsen af oplysningerne som uberettiget og dermed som en sandsynlig overtrædelse af straffelovens § 263, stk. 3 – og måske endda stk. 4.

Sammenfattende er det ikke min vurdering, at medarbejderen ved Topdanmark kan siges at have »videregivet« oplysningerne ved at lægge dem fra den ene server til den anden, som beskrevet. Uanset om det er strafbart for hackeren eller ikke, er der utvivlsomt tale om oplysninger, som ikke er beregnet for andre, og som derfor hverken er offentliggjort eller videregivet. Det ville de først blive på det tidspunkt, de bliver "synlige" på hjemmesiden.

Der er således ikke tale om en overtrædelse af VPL § 36, ligesom medarbejderen ikke har handlet uagtsomt i relation til VPL § 36. Hvad angår medarbejderens erkendte "fejl", henvises til afsnit 3.3.4 umiddelbart nedenfor.

[8] IT-retten, 1. udgave, s. 682. Tilsvarende *Tranberg & Langsted*, "Internet-kriminalitet" i bogen Internetretten (2008), s. 525 ff.

[9] Se f.eks. også BRÅ-rapport 2000:3 »IT-relateret Brottslighet«, hvor det s. 16 nævnes, at en anden form for dataindtrængning er den, der består i at man ændrer en andens hjemmeside, f.eks. ved at ændre links, så de viser hen til f.eks. utugtige billeder etc. Ved en sådan hacking, der utvivlsomt er omfattet af § 263, omgås således intet password eller anden angivelse af sikkerhed – man ændrer ganske enkelt i kodningen af siden, således at linket ændres. Denne adfærd er åbent for enhver »uberettiget« for gerningsmanden og »uønsket« af offeret. Ganske som URL-hackingen i nærværende sag.

3.3.4 VPL § 37 – interne regler

De relevante bestemmelser, som påberåbes af Finanstilsynet er VPL § 37, stk. 2, jf. stk.3, nr. 1. der er sålydende:

> »Stk.2. En udsteder af værdipapirer som nævnt i § 34, stk. 1, nr. 1, skal udarbejde interne regler med det formål at hindre, at intern viden er tilgængelig for andre end dem, der har behov herfor. Tilsvarende regler skal udarbejdes af offentlige myndigheder og virksomheder, herunder værdipapirhandlere, advokater og revisorer, som i kraft af deres virksomhedsudøvelse regelmæssigt kommer i besiddelse af intern viden.
> Stk.3. Interne regler udarbejdet af en udsteder i henhold til stk. 2, 1. pkt., skal som et minimum indeholde bestemmelser, hvorigennem det effektivt sikres, at
> 1) andre personer end de, der skal have adgang dertil som led i udøvelsen af deres funktioner hos udstederen, ikke får adgang til intern viden«

Det er ubestridt af Finanstilsynet, at Topdanmark havde udarbejdet regler, der teoretisk sikrede, at intern viden ikke kom i forkerte hænder, jf. notatet s. 14. Samme sted anføres imidlertid, at dette »ikke er tilstrækkeligt«, idet det ud fra en »formålsfortolkning af § 37« og en »direktivkonform« fortolkning må være således, at reglerne også faktisk forhindrer videregivelse til andre end de, der har brug for at have kendskab til oplysningerne.

Ser man på ordlyden af bestemmelsen, kræver den, at der af en udsteder skal udarbejdes interne regler. Dette er ubestridt sket. Det, der antageligt volder vanskeligheder, er den vending, at det gennem regelsættet »effektivt [skal] sikres«, at oplysningerne ikke kommer videre. Rationalet bag Finanstilsynets fortolkning af bestemmelsen må være, at såfremt der rent faktisk opstår en lækage af en eller anden art, så demonstrerer det, at regelsættet ikke har virket, idet det jo i den konkrete situation netop ikke har »sikret effektivt« mod videregivelse.

Bestemmelsens formål er at være præventiv[10]. Man skal således kunne slå ned på udstedere m.v., såfremt de undlader at lave interne retningslinjer eller laver disse, således at de forekommer utilstrækkelige. Hvorvidt der faktisk måtte forekomme videregivelse eller ikke videregivelse er underordnet for reglens anvendelse og formål. Såfremt det havde betydning for anvendelsen af bestemmelsen (og sanktioneringen heraf), om der havde fundet uberettiget videregivelse sted eller ej, måtte man for det første acceptere, at virksomheden ”pr. automatik” ville få en bøde, hver gang der slap intern viden ud til uvedkommende, helt uanset hvordan videregivelsen havde fundet sted – det ville så at sige være en ”automatreaktion”. For det andet måtte man vel så også acceptere, at virksomhedernes regelsæt var lovmedholdelige, såfremt der aldrig havde fundet uberettiget videregivelse af intern viden sted. Begge dele er dog lige uantagelige.

Anvendt på denne måde ville reglen nemlig ikke have nogen selvstændig funktion, og det er derfor ikke rigtigt, at en »*formålsfortolkning*« vil føre frem til den forståelse, Finanstilsynet anlægger, tværtimod. Det forekommer også vanskeligt at forstå, hvorved en anvendelse som foreslået af Finanstilsynet skulle være »direktivkonform«. At en fortolkning er »*direktivkonform*« betyder blot, at reglen skal fortolkes således, at den forstås i overensstemmelse med det direktiv, hvoraf den har sit udspring.

VPL § 37, stk. 3, nr. 1 udspringer af DIREKTIV 2003/124/EF, art. 3, stk. 2, hvor det bl.a. hedder:

[10] Jf. også *Paul Krüger Andersen & Nis Jul Clausen*, Børsretten II, 3. udgave, s. 370.

»2. Ved anvendelsen af artikel 6, stk. 2, i direktiv 2003/6/EF kræver medlemsstaterne, at en udsteder, for at sikre, at den interne viden behandles fortroligt, kontrollerer adgangen til en sådan viden, og især:

a) at udstederen har indført effektive foranstaltninger for at forhindre andre personer i at få adgang til denne viden end de personer, der skal have adgang dertil som led i udøvelsen af deres funktioner hos udstederen«

I direktiv 2003/6/EF, artikel 6, stk. 2 hedder det:

»En udsteder kan på eget ansvar udsætte offentliggørelsen af intern viden, jf. stk. 1, for ikke at skade sine berettigede interesser, forudsat at dette ikke vil kunne vildlede offentligheden, og at udstederen kan sikre, at denne viden behandles fortroligt. Medlemsstaterne kan kræve, at en udsteder øjeblikkelig skal underrette den kompetente myndighed om sin beslutning om at udsætte offentliggørelsen af intern viden.«

I ingen af de nævnte direktiver findes i artiklerne, i præambelen, i definitionerne eller i gennemførelsesbestemmelserne nogen antydning af, at man må kræve en sanktion af udstederen, såfremt der de facto slipper intern viden ud på markedet. Formålet med direktiverne er i overensstemmelse hermed bl.a. angivet som sikkerheden på markedet, vigtigheden af at handel sker på lige vilkår, og at intern viden derfor skal beskyttes »effektivt«.

I de danske forarbejder[11] til den nuværende bestemmelse i VPL § 37, siges:

»Den foreslåede bestemmelse i stk. 3 gennemfører dele af artikel 3, stk. 2, i Kommissionens første direktiv om intern viden og kursmanipulation og fastsætter nærmere krav til indholdet af de interne regler, som udstedere af værdipapirer er forpligtede til at udarbejde i henhold til den foreslåede § 37, stk. 2, 1. pkt.

Af den foreslåede bestemmelse følger et overordnet krav om, at de interne regler er effektive, jf. formuleringen "bestemmelser, hvorigennem det effektivt sikres". Reglerne må udformes på en måde, så det sikres, at de relevante personer i udsteders virksomhed har kendskab til rækkevidden af lovens forbud mod videregivelse af intern viden herunder om forståelsen af begrebet intern viden. Udsteder skal endvidere sikre, at ledelsen og andre relevante personer til enhver tid er bekendt med indholdet af de interne regler.

Med det i bestemmelsens stk. 3, nr. 1 , foreslåede krav fastsættes, at udsteder ved formulering af de interne regler skal sikre, at intern viden alene er tilgængelig for de personer hos udsteder, der har brug herfor som led i deres funktioner. De interne regler skal således ikke alene sikre, at intern viden ikke kommer til en udenforstående tredjemands kendskab men også, at intern viden kun tilgår de personer internt i udsteders virksomhed, der har brug herfor, som led i deres funktioner«

Hverken her eller andre steder i lovforslaget nævnes, at reglen skulle fortolkes således, at en videregivelse af intern viden til en uvedkommende pr. automatik også ville konstituere en overtrædelse af § 37, stk. 2 og 3.

Skulle reglen forstås, som anført af Finanstilsynet, ville det indebære et objektivt ansvar for udstederen, idet det så ikke ville være nødvendigt at kunne bebrejde udstederen det skete som forudsætning for straf, men alene konstatere, at en læk havde fundet sted. At reglen ville indebære et objektivt strafansvar med denne forståelse fremgår tydeligt af, at Finanstilsynet vurderer, at Topdanmarks interne regelsæt »teoretisk« er effektivt. At ikende straf på objektivt grundlag må, jf. straffelovens § 1, kræve helt sikker hjemmel,

[11] Bemærkningerne til lovforslag nr. 13 af 6/10 2004 om ændring af lov om værdipapirhandel m.v. og lov om finansiel virksomhed (Gennemførelse af markedsmisbrugs- og prospektdirektivet).

idet et sådant objektivt ansvar er en fravigelse fra straffelovens § 19, hvorefter der kræves enten forsæt eller uagtsomhed som forudsætning for straf.

Sådan sikker hjemmel findes ikke her, og allerede af den grund må Finanstilsynets forståelse af bestemmelsens krav afvises.

4. Supplerende overvejelser

Inden den endelige konklusion i afsnit 5, er det nødvendigt at supplere de retlige overvejelser vedrørende de enkelte forhold i afsnit 3 med en helhedsbetragtning over sagens karakter. Det er således værd at overveje, om den overvejende bærer præg af ansvarspådragende adfærd fra Topdanmarks side eller den tværtimod er kendetegnet ved, at Topdanmark har været "offer" for en muligt ansvarspådragende adfærd.

Som gengivet i afsnit 2 er faktum ganske enkelt og peger éntydigt på, at Topdanmark har været udsat for et uretmæssigt "angreb" mod deres interne oplysninger. Topdanmark har således været udsat for en (må det antages med en høj grad af sikkerhed) målrettet ekstern søgen efter intern viden på Topdanmarks servere. Da det lykkes den eksterne indtrænger at finde de interne informationer (som indtrængeren ved, skal holdes "dybt" fortrolige), kontakter indtrængeren eller den, som af indtrængeren har modtaget oplysningerne, (Reuters) Topdanmark og meddeler, at man straks vil offentliggøre disse interne oplysninger. Uagtet Topdanmark protesterer, foretages offentliggørelsen af Reuters, og Topdanmark reagerer herefter korrekt ved umiddelbart efter selv at foranledige offentliggørelse. Hele dette forløb er således præget af, at Topdanmark har været udsat for et "ondsindet" angreb.

Heroverfor står Topdanmarks mulige "brøde", der skulle bestå i, at en medarbejder for tidligt lægger nogle oplysninger over på den eksterne server. Vel at mærke oplysninger, der alligevel skulle være offentliggjort i umiddelbar forlængelse heraf.

Skadevirkningen af, at Topdanmarks medarbejder lagde dataene over på en ekstern server, indtræder imidlertid først, da en indtrængende tredjepart "griber" oplysningerne og løber med dem. Den indtrængende tredjemand gør sig muligvis skyldig i en strafbar overtrædelse af straffelovens regel om hacking og derefter sandsynligvis skyldig i videregivelse af intern viden, jf. VPL § 36.

Det er således intet i helhedsbilledet, der giver grund til at antage, at Topdanmark har handlet ansvarspådragende, og det forekommer vanskeligt at forstå, at en tilsynsmyndighed så ensidigt finder, at der bør pålægges et strafansvar, når en almindelig proportionalitetsafvejning taler for, at den dadelværdige adfærd i den langt altovervejende grad ikke ligger hos Topdanmark men hos den indtrængende.

5. Konklusion

Som det er fremgået ovenfor i afsnittene 3 og 4, er det min klare opfattelse, at Topdanmark ikke kan drages til ansvar for overtrædelse af nogen bestemmelser i VPL i anledning af denne sag.

I forhold til **VPL § 27a** er gerningsindholdet, hvorefter der kræves "offentliggørelse", således ikke opfyldt. Det at overføre data fra en intern til en ekstern server kan således ikke opfattes som en "offentliggørelse" hverken ved sædvanlig eller udvidende fortolkning. Det savner herefter mening at bebrejde Topdanmark, at man ikke har "offentliggjort" på en bestemt måde, idet man hverken har foretaget eller tilsigtet en offentliggørelse overhovedet.

Da gerningsindholdet ikke er opfyldt, savner det mening at søge at vurdere, hvorvidt medarbejderen hos Topdanmark kan siges at have handlet uagtsomt eller ej, idet konstateringen af en given uagtsomhed forudsætter identifikation af et bestemt gerningsindhold, så man kan spørge, om den pågældende har handlet uagtsomt i relation til netop dette.

I forhold til **VPL § 36** er gerningsindholdet heller ikke her opfyldt. Det er således ikke muligt at forstå ordet »videregive« som omfattende en for omverdenen skjult overførsel af data fra en intern til en ekstern server. Begge steder var dataene skjult for omverdenen og befandt sig på et område, som udelukkende var Topdanmarks. Forskellen var blot, at det ene sted var det fysisk udelukket for indtrængende at bemægtige sig dataene, det andet sted var det fysisk muligt – men fortsat klart for enhver: uønsket. Ovenfor i afsnit 3.3.3 nævnes som eksempel på videregivelse af oplysninger ved uagtsomhed den situation, at nogle personer, for hvem det er tilladt at diskutere virksomhedens erhvervshemmeligheder, gør dette i fuld offentlighed, så alle kan høre det. Skal man parallelisere nærværende situation til den fysiske verden, ville det svare til, at to medarbejdere i en virksomhed for lukkede døre på den enes kontor diskuterede nogle af virksomhedens fortrolige oplysninger. Samtidig stod en tilfældig gæst i virksomheden udenfor og lyttede ved døren, hvorefter han straks offentliggør hemmelighederne, da han kommer hjem. Man kunne måske diskutere, om der var tale om videregivelse af oplysninger, men det ville være indiskutabelt, at de to medarbejdere i hvert fald ikke har handlet uagtsomt. Det gør ingen forskel heri, om der ved, at de to medarbejdere diskuterede sagen, samtidig forelå en mindre overtrædelse af nogle interne regler om, hvem der måtte få hvad at vide hvornår.

Det kan i øvrigt bemærkes, at anvendelsen af § 27 og anvendelsen af § 36 må være gensidigt udelukkende, når talen er om den samme handling. Den samme handling kan således ikke på én gang både udgøre en uberettiget videregivelse og en fuldt legal offentliggørelse, der blot foregår på en forkert måde. Den samme handling kan imidlertid udmærket – som her – hverken være en overtrædelse af § 27 eller af § 36.

Hvad endelig angår kritikpunktet vedrørende **VPL § 37** må også dette afvises. Topdanmark havde således efterlevet bestemmelsen ved at have effektive interne regler. Bestemmelsen kræver hverken efter sin ordlyd eller efter sit formål, at reglerne i praksis altid og ubetinget skal sikre, at intern viden ikke kommer i de forkerte hænder – endsige pålægger sanktion herfor. Som nævnt ville en sådan anvendelse af bestemmelsen indebære et objektivt ansvar for udsteder, og et sådant ansvar savner ganske hjemmel i VPL.

Der er således efter min bedste opfattelse intet grundlag for at indgive politianmeldelse mod Topdanmark i nærværende sag, og der er heller ikke i Finanstilsynets notat af 13/10 d.å. nogen retlig argumentation for, at man trods de af mig her fremhævede omstændigheder skulle kunne gøre et strafferetligt ansvar gældende mod Topdanmark.

Århus d. 25. oktober 2010

Lars Bo Langsted