FINANSMINISTERIET

Folketingets Erhvervsudvalg
Christiansborg

29. oktober 2020

Svar på Erhvervsudvalgets spørgsmål nr. 561 (Alm. del) af 2. oktober 2020 stillet af Anni Matthiesen (formand) på udvalgets vegne

Spørgsmål
Med henvisning til samrådet den 30. september 2020 om ERU alm. del – samrådsspørgsmål Ø (Ecofin-rådsmødet den 6. oktober 2020) bedes ministeren oversende uddybende notater til udvalget vedr. følgende punkter:

a) Handlingsplanen for detailbetalinger, herunder hvordan denne spiller sammen med det nordiske samarbejde om at skabe fælles betalingsinfrastruktur.

b) Redegørelse for indholdet af og konsekvenser af forslaget om kryptoaktiver, herunder beskatningsmæssige aspekter, og hvilke konsekvenser forslaget vil få dels på EU-niveau, dels for Danmark.

c) Forslaget om digital operationel robusthed af den finansielle sektor (cyberrobusthed), herunder redegøre for, om Danmark i forhold til forslaget er forud vedrørende national robusthed, eller om der med forslaget vil ske en yderligere styrkelse af Danmarks cyberrobusthed – og i så fald på hvilke områder.

Svar
Kommissionen præsenterede 24. september 2020 sin pakke for digital finansiering bestående af:

1) Handlingsplan for digitalisering af finansielle tjenester
2) Handlingsplan for detailbetalinger
3) Forslag om regulering af kryptoaktiver
4) Forslag om digital operationel robusthed (cyberrobusthed)

Spørgsmålene a)-c) berører særligt punkterne 2)-4), der er nærmere redegjort for i det følgende.

Begge handlingsplaner er derudover beskrevet i grund- og nærhedsnotater oversendt til Folketinget. For de to forslag i Kommissionens pakke udarbejdes der aktuelt grund- og nærhedsnotater.

a) Handlingsplanen for detailbetalinger
Handlingsplanen skal medvirke til, at borgere og virksomheder i EU-landene kan opnå gavn af et bredt udvalg af digitale betalingsløsninger af høj kvalitet og til lave omkostninger. Handlingsplanen skal understøtte gode rammevilkår for innovation og konkurrence på betalingsområdet, hvilket Kommissionen anser som værende kritisk for europæisk økonomi. En bedre infrastruktur for betalinger kan ifølge Kommissionen også styrke EU-landenes uafhængighed ift. tredjelande (autonomi).

Kommissionen fokuserer særligt på at fremme såkaldte straksbetalinger ("instant payments") på tværs af EU, hvor betalinger kan gennemføres på alle tidspunkter og hurtigt er i hænde på modtageren, fx som det typisk kendes fra MobilePay i Danmark. Kommissionen lægger bl.a. op til, at der stilles krav til finansielle virksomheder om at sikre løsninger for straksbetalinger.

Derudover vil Kommissionen gennemgå reglerne for forbrugerbeskyttelse på området. Kommissionen vil bl.a. undersøge mulighederne for en EU-mærkningsordning for paneuropæiske betalingsløsninger og en EU-standard for kontaktløse betalinger (dvs. betalinger, fx med kort, som ikke kræver fysisk kontakt mellem forbruger og den fysiske betalingsmodtager, hvilket allerede er udbredt i Danmark).

Sammen med Den Europæiske Centralbank (ECB) vil Kommissionen derudover undersøge muligheden for at indføre en såkaldt "digital euro", også kaldet digital centralbanksvaluta ("Central Bank Digital Valuta" – CBCD). En digital euro er tænkt som et elektronisk alternativ til kontanter med det formål at give forbrugere mulighed for at foretage betalinger via centralbanker og uden involvering af almindelige banker. Formålet er at udbrede brugen af elektroniske betalinger, ligesom digitale euro vurderes at kunne styrke brugen af euroen som valuta internationalt.

Kommissionen vil også undersøge, om flere virksomheder skal omfattes af allerede eksisterende EU-regler på betalingsområdet, fx underleverandører. Kommissionens overvejelser vil skulle fremsættes i konkrete lovforslag.

Handlingsplanen bygger på allerede eksisterende EU-lovgivning, herunder EU's betalingstjenestedirektiv ("Payment Services Directive" – PSD2) og EU-forordningen om fælles euro-betalingsområde ("Single Euro Payments Area" – SEPA).

En række af de nordiske landes banker har allerede igangsat et samarbejde (kaldet P27), der skal sikre en nordisk betalingsinfrastruktur, som giver mulighed for pannordiske straksbetalinger. P27 har planlagt, at den første straksbetaling skal gennemføres via infrastrukturen i 2021. Deltagerne i samarbejdet har endvidere udgivet en hensigtserklæring om, at P27-infrastrukturen skal kunne fungere i sammenhæng med det nuværende fælles euro-betalingsområde (SEPA). Hvis P27-samarbejdet

forløber som planlagt, vil detailbetalinger mellem nordiske lande og internt i de nordiske lande i høj grad blive baseret på straksbetalinger som standard.

Den fremsatte handlingsplan er derudover beskrevet i grund- og nærhedsnotat oversendt til Folketinget, herunder høring af handlingsplanen blandt danske interesseorganisationer og andre høringsparter.

b) Forslaget om regulering af kryptoaktiver
Forslaget består af en forordning, som har til formål at regulere og fremme kontrolleret brug af kryptoaktiver under hensyn til finansiel stabilitet og forbrugerbeskyttelse. Forslaget skal vedtages af både Rådet og Europa-Parlamentet. Et eksempel på kryptoaktiver er virtuelle valutaer, bl.a. Facebooks Libra. De bliver med forslaget omfattet af EU-lovgivning.

Kryptoaktiver er særligt kendetegnet ved deres decentralisering, fx ved at de handles uden om eksisterende finansielle aktører, fx banker og traditionelle børser. Decentraliseringen udfordrer investorbeskyttelsen og den nuværende finansielle EU-regulering, der ikke er indrettet til at håndtere kryptoaktiver. Kommissionen vurderer, at kryptoaktiver og deres underliggende teknologier indebærer betydelige muligheder for at udvikle finansielle produkter og tjenester til gavn for borgere og virksomheder i EU-landene, men at kryptoaktiver også er forbundet med betydelige risici, hvis området forbliver ureguleret.

Kommissionens forslag indebærer, at udbydere af kryptoaktiver skal have fysisk tilstedeværelse og have tilladelse af en national tilsynsmyndighed i et EU-land, hvorefter en udbyder vil kunne udbyde et kryptoaktiv i alle EU-lande uden yderligere tilladelse ("EU passport"). Udbydere vil skulle efterleve kapitalkrav, standarder om organisering ("governance"), og de vil skulle adskille egne midler fra deres kunders midler samt efterleve krav til deres IT-systemer for at undgå cybertyveri og -angreb. Hvis der er tale om et signifikant kryptoaktiv vil tilsynet skulle føres af den europæiske banktilsynsmyndighed, EBA. Kriterierne for hvornår et kryptoaktiv er signifikant fastsættes senere af Kommissionen ved gennemførelsesretsakter, hvori en række minimumskriterier vil blive specificeret.

Forslaget sigter også på at undgå markedsmisbrug med kryptoaktiver, herunder insiderhandel (hvor en person med ikke-offentliggjort viden relevant for værdien af et aktiv opnår personlig vinding heraf). Kommissionen foreslår et øvelsesregime, et såkaldt pilotregime, hvor udbydere af kryptoaktiver i en periode kan teste deres produkter under særlige lovgivningsmæssige rammer.

Forslaget vurderes i øjeblikket nærmere i forbindelse med udarbejdelse af grund- og nærhedsnotat, herunder mhp. at afklare konsekvenser for dansk lovgivning, samt statsfinansielle, erhvervsøkonomiske og samfundsøkonomiske konsekvenser af forslaget.

c) Forslaget om digital operationel robusthed (cyberrobusthed)
Forslaget har til formål at styrke EU-landenes finansielle sektorers digitale operationelle modstandsdygtighed (cyberrobusthed) og specificerer krav til tilsyn og overvågning af bl.a. udbydere af it-drift mv.

Forslaget består af en forordning, der indeholder de materielle regler om operationel modstandsdygtighed og et direktiv, der indeholder ændringer af de forskellige retsakter, som gælder for de enkelte virksomhedstyper.

Den foreslåede forordning omfatter næsten hele den finansielle sektor, dels ud fra et ønske om at skabe et ensartet tilsyn med sektorens cyberrisici. Derudover er de cyberkriminelle og andre fjendtlige cyberaktører ofte gode til metodisk at lokalisere de svage led i processer, der gør det muligt at angribe it-infrastrukturer (fx for at opnå adgang til databaser eller at sætte et it-system ud af drift).

Lovgivningsmæssigt er området allerede berørt af EU's net- og informationsdirektiv, der har til formål at styrke cybersikkerheden bredt i EU-landene. Til sammenligning har forslaget om digital operationel robusthed til formål at adressere de mere specifikke hensyn til den nationale sikkerhed, som cyberrisici i den finansielle sektor særligt kan påvirke.

Forslaget indeholder detaljerede regler om styring, herunder it-risikostyring, sikkerhedstest, hændelsesrapportering, beredskaber, leverandørstyring og et fællestilsyn med kritiske tredjepartsleverandører vedr. it-drift.

En væsentlig ny kategori af tredjepartsudbydere af it-drift er cloud-udbydere, som leverer it-platforme, databaser, software og lign. gennem internettet (fx til håndtering af kundedata). Cloud-udbydere i den finansielle sektor er bl.a. virksomhederne Microsoft, Amazon og IBM, der alle har meget store markedsandele i EU. Cloud-udbydernes fremkomst i den europæiske finansielle sektor har været en væsentlig motivation for at regulere vigtige (kritiske) tredjepartsudbydere. Regelsættet ventes også at omfatte cloud-udbydere såsom Google, Oracle og Salesforce samt de kinesiske udbydere Alibaba og Huawei, i det omfang disse vil blive anset for at være kritiske leverandører på europæisk niveau.

En udfordring er aktuelt, at markedet for cloud-løsninger er koncentreret på få udbydere med store markedsandele, hvilket betyder, at cyberangreb på cloud-platforme kan få en systemisk betydning for den finansielle sektor. Samtidig er de markedsledende cloud-udbydere alle hjemmehørende uden for EU, hvilket er en yderligere tilsynsmæssig udfordring, fordi det kræver samarbejde med tilsynsmyndighederne i cloud-udbyderens hjemland. Cloud-udbyderne er hver især ofte så store, at det selv for de største europæiske banker kan være vanskeligt at opnå en tilstrækkelig grad af kontrol med leverandørens it-risici. Dette har betydet, at fordelen ved direkte tilsyn med leverandører også er blevet tydelig på europæisk niveau.

Danmark har i mange år haft en national ordning for direkte tilsyn med kritiske it-leverandører i den finansielle sektor. Det direkte tilsyn med de største it-leverandører indebærer en væsentlig administrativ lettelse både for de små og mellemstore danske finansielle virksomheder og for Finanstilsynet, idet ordningen sparer begge parter for et betydeligt ressourceforbrug, der ellers er forbundet med et detaljeret tilsyn med de mindre finansielle virksomheders styring af deres større leverandører.

Kommissionens forslag indebærer en ordning, hvor der sikres et direkte tilsyn med store tredjepartsudbydere på europæisk niveau, dvs. en af de tre eksisterende EU-tilsyn, ESA'erne. Ordningen med direkte tilsyn af tredjepartsudbyderen er derfor sammenlignelig med tilgangen i det danske tilsyn. Et fælleseuropæisk tilsyn med kritiske tredjepartsudbydere vil kunne styrke og forenkle tilsynet med de finansielle virksomheder, der benytter store cloud-udbydere (Microsoft, Amazon, IBM, mv.), og forslaget kan derved lette væsentlige administrative byrder for både den finansielle sektor samt de nationale tilsynsmyndigheder (herunder Finanstilsynet). Forslaget indebærer dog ikke en ændring af tilsynet med de danske fælles datacentraler, der ikke anses for at være kritiske leverandører på EU niveau. Det fremgår af forslaget, at tilsyn med nationalt kritiske leverandører fastsættes af medlemsstaterne selv, og den danske tilsynsordning på dette område vil derfor fortsætte som hidtil.

I Danmark er der tillige tilsyn med den fælles betalingsinfrastruktur, som svarer til it-tilsynet med de fælles datacentraler. Den fælles betalingsinfrastruktur har en meget væsentlig, central og systemisk betydning for den finansielle sektor og for hele samfundet, hvilket især er tydeligt i lande som Danmark, hvor almindelige betalinger mellem borgere og virksomheder i vid udstrækning er elektroniske. Et alvorligt nedbrud i betalingsinfrastrukturen vil i yderste konsekvens betyde, at de fleste betalinger ikke kan finde sted. Tilsyn med betalingsinfrastrukturer er imidlertid ikke medtaget i det nuværende forslag til forordningen, men ventes at være et tema i de kommende forhandlinger, bl.a. fordi det forventes at betalingsinfrastrukturen i flere lande (inkl. Danmark) i fremtiden kan komme i udenlandsk ejerskab.

Samlet set vurderes Kommissionens forslag at styrke cyberrobustheden i Danmark, hvilket særligt skyldes det foreslåede fællestilsyn af store tredjepartsudbydere. Fællestilsynet ventes at bidrage til et mere effektivt tilsyn, og det ventes bedre at kunne modvirke at tredjepartsudbyderne kan omgå tilsyn ved at placere sig i lande med mindre restriktive tilgange. Derudover vurderes det, at oprettelsen af et fællestilsyn med cloud-udbydere vil kunne frigøre ressourcer hos den finansielle sektor samt de nationale tilsynsmyndigheder.

Forslaget vurderes i øjeblikket nærmere i forbindelse med udarbejdelse af grund- og nærhedsnotat, herunder mhp. at afklare konsekvenser for dansk lovgivning, statsfinanser, erhvervsøkonomi samt samfundsøkonomi.

Med venlig hilsen

Nicolai Wammen
Finansminister