Notat

om

tilvalg af cybercrime-direktivet

1. Baggrund

I Stockholm-programmet, som medlemsstaterne vedtog i 2009, er det bl.a. anført, at internettet har skabt nye udfordringer i form af IT-kriminalitet, og at EU bør fremme politikker og lovgivning, som sikrer et meget højt beskyttelsesniveau. Kommissionen opfordres i den forbindelse til, hvor det er nødvendigt, at fremsætte forslag til præcisering af lovgivningen om IT-kriminalitet.

På denne baggrund fremsatte Kommissionen den 30. september 2010 et direktivforslag om angreb på informationssystemer. Formålet med forslaget var at sikre en yderligere tilnærmelse af medlemsstaternes lovgivning i forhold til den gældende rammeafgørelse om angreb på informationssystemer (2005/222/RIA).

Direktivet blev vedtaget af Europa-Parlamentet og Rådet den 12. august 2013 som direktiv 2013/40/EU om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (cybercrime-direktivet). Direktivet bygger på rammeafgørelse 2005/222/RIA og Europarådets konvention om IT-kriminalitet af 23. november 2001. Herudover er der i direktivet medtaget enkelte nye elementer.

Direktivet er vedtaget under henvisning til Traktatens artikel 83, stk. 1, og er dermed omfattet af Danmarks retsforbehold. Danmark deltog således ikke i vedtagelse af direktivet, ligesom direktivet ikke er bindende for eller finder anvendelse i Danmark.

Direktivet erstatter Rådets rammeafgørelse 2005/222/RIA i forhold til de medlemsstater, der er bundet af direktivet.

Rådets rammeafgørelse 2005/222/RIA (forslag til rammeafgørelse) og Europarådets konvention om IT-kriminalitet er gennemført i dansk ret ved lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.).

Direktivet indeholder ikke regler om gensidig anerkendelse. Danmark kan således allerede – uanset retsforbeholdet – ensidigt vælge at gennemføre regler svarende til direktivet.

2. Cybercrime-direktivet og dansk ret

2.1. Genstand

Artikel 1 angiver direktivets genstand. Det følger af bestemmelsen, at direktivet fastsætter minimumsregler vedrørende definitionen af strafbare handlinger og sanktioner i forbindelse med angreb på informationssystemer. Det følger endvidere af bestemmelsen, at direktivet sigter mod at lette forebyggelsen af sådanne strafbare handlinger og forbedre samarbejdet mellem retslige og andre kompetente myndigheder.

Der er således tale om et minimumsdirektiv, og medlemsstaterne kan derfor bl.a. vælge at kriminalisere i videre omfang, end direktivet kræver, eller at fastsætte højere strafferammer end de i direktivet angivne. Medlemsstaterne vil derfor f.eks. kunne opfylde direktivets krav om kriminalisering af bestemte handlinger ved en mere generel kriminalisering, som bl.a. omfatter de pågældende handlinger.

Bestemmelsen indeholder ikke i sig selv forpligtelser for medlemsstaterne og giver således ikke anledning til lovgivningsmæssige overvejelser.

2.2. Definitioner

Artikel 2 indeholder definitioner af begreberne ”informationssystem”, ”edb-data”, ”juridisk person” og ”uretmæssig”.

Ved ”informationssystem” forstås en enhed eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program, som automatisk behandler edb-data, som lagres, behandles, fremfindes eller overføres af denne enhed eller gruppe af enheder i forbindelse med dens eller deres drift, brug, beskyttelse og vedligeholdelse.

Ved "edb-data" forstås enhver form for gengivelse af fakta, informationer eller begreber i et format, der egner sig til behandling i et informationssystem, herunder et program, som kan anvendes til at få et informationssystem til at udføre en funktion.

Ved "juridisk person" forstås en enhed, der har status som juridisk person i henhold til den lovgivning, der finder anvendelse, med undtagelse af stater eller offentlige organer, der udøver deres statsmyndighed, eller offentlige internationale organisationer.

Ved "uretmæssig" forstås en adfærd som omhandlet i direktivet, herunder adgang, indgreb eller opfangning, som ejeren eller en anden rettighedshaver af systemet eller en del af det ikke har givet tilladelse til, eller som ikke er tilladt i henhold til national lovgivning.

Definitionerne svarer med visse mindre sproglige præciseringer til definitionerne i Rådets rammeafgørelse 2005/222/RIA om angreb på informationssystemer, der blev gennemført i dansk ret ved lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.). Man fandt i den forbindelse ikke anledning til at indføre egentlige definitionsbestemmelser i straffeloven.

2.3. Strafbare handlinger

2.3.1. Ulovlig adgang til informationssystemer

2.3.1.1. Artikel 3 forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at det er strafbart – i det mindste i grove tilfælde – forsætligt at skaffe sig uretmæssig adgang til et informationssystem eller en del heraf, når den strafbare handling er begået ved brud på en sikkerhedsforanstaltning.

Det bemærkes, at direktivets artikel 3 svarer til artikel 2 i rammeafgørelsen og artikel 2 i Europarådets konvention, idet det dog i direktivet præciseres, at den strafbare handling skal være begået ved brud på en sikkerhedsforanstaltning.

2.3.1.2. Efter straffelovens § 263, stk. 2, om krænkelse af datahemmeligheden (hacking) straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

Direktivets artikel 3 omfatter handlinger, der begås ved brud på sikkerhedsforanstaltninger. Det følger af straffelovens § 301 a, at det er strafbart uretmæssigt at skaffe eller videregive koder eller andre adgangsmidler til informationssystemer, hvortil adgangen er forbeholdt betalende brugere, og som er beskyttet med kode eller anden særlig adgangsbegrænsning. Bestemmelsen vedrører kommercielle informationssystemer, det vil sige systemer, hvor betaling er en forudsætning for brugen af systemet. Bestemmelsen fremrykker den strafferetlige beskyttelse, så det ikke kun er strafbart at skaffe sig adgang til et informationssystem ved at begå brud på en sikkerhedsforanstaltning men også at skaffe eller videregive adgangskoder, der kan anvendes til at skaffe den uretmæssige adgang. I forhold til ikke-kommercielle informationssystemer er det efter straffelovens § 263 a strafbart uretmæssigt erhvervsmæssigt at sælge eller i en videre kreds at udbrede, videregiver eller uretmæssigt skaffe koder eller andre adgangsmidler til et ikke offentligt tilgængeligt informationssystem, hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning.

Hvis den ulovlige adgang til et informationssystem har til formål at skaffe personen selv eller andre uberettiget vinding, og der ved adgangen til informationssystemer retsstridigt foretages ændringer, tilføjelser eller sletning af oplysninger eller programmer til elektronisk sagsbehandling, vil handlingen kunne straffes som databedrageri, jf. straffelovens § 279 a.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 3.

2.3.2. Ulovligt indgreb i informationssystemer

2.3.2.1. Artikel 4 forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at det er strafbart – i det mindste i grovere tilfælde – forsætligt og uretmæssigt at forårsage en alvorlig hindring eller afbrydelse af et informationssystems drift ved at indlæse edb-data, overføre, beskadige, slette, forvanske, ændre eller tilbageholde sådanne data eller gøre sådanne data utilgængelige.

Det bemærkes, at direktivets artikel 4 svarer til artikel 3 i rammeafgørelsen og indholdsmæssigt i det væsentlige svarer til artikel 5 i Europarådets konvention.

2.3.2.2. I dansk ret er rådighedshindring, driftsforstyrrelser og hærværk, herunder på data i et informationssystem, omfattet af straffelovens §§ 193, 291 og 293.

Det er således strafbart på retsstridig måde at fremkalde omfattende forstyrrelse i driften af bl.a. informationssystemer, jf. § 193.

Endvidere er det strafbart at ødelægge, beskadige eller bortskaffe f.eks. et informationssystem eller dele heraf, jf. § 291, stk. 1.

Endelig er det strafbart uberettiget at hindre en anden i helt eller delvist at råde over ting, herunder ved en elektronisk rådighedshindring, jf. § 293, stk. 2.

Dansk ret vurderes dermed at være i overensstemmelse med direktivets artikel 4.

2.3.3. Ulovligt indgreb i data

2.3.3.1. Artikel 5 forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at det er strafbart – i det mindste i grovere tilfælde – forsætligt og uretmæssigt at slette, beskadige, forvanske, ændre eller tilbageholde edb-data i et informationssystem eller at gøre sådanne data utilgængelige.

Det bemærkes, at direktivets artikel 5 svarer til artikel 4 i rammeafgørelsen og indholdsmæssigt i det væsentlige svarer til artikel 4 i Europarådets konvention.

2.3.3.2. Som anført ovenfor under pkt. 2.3.2.2 er det ifølge straffelovens § 291, stk. 1, strafbart at ødelægge, beskadige eller bortskaffe f.eks. data i et informationssystem. Endvidere er det ifølge straffelovens § 293, stk. 2, strafbart uberettiget at hindre en anden i helt eller delvist at råde over ting, herunder ved en elektronisk rådighedshindring af data i et informationssystem.

Dansk ret vurderes dermed at være i overensstemmelse med direktivets artikel 5.

2.3.4. Ulovlig opfangning

2.3.4.1. Artikel 6 forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at det er strafbart – i det mindste i grovere tilfælde – forsætligt og uretmæssigt ved hjælp af tekniske hjælpemidler at opfange ikke-offentlige overførsler af edb-data til, fra eller inden for et informationssystem, herunder elektromagnetisk udsending fra et informationssystem, der indeholder disse edb-data.

Det bemærkes, at der ikke findes en lignende bestemmelse i rammeafgørelsen eller i Europarådets konvention.

2.3.4.2. I dansk ret er det generelt strafbart uberettiget at skaffe sig adgang – herunder også ved hjælp af tekniske hjælpemidler – til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem, jf. straffelovens § 263, stk. 2.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 6.

2.4. Værktøjer

2.4.1. Artikel 7 vedrører værktøjer, der anvendes til at begå strafbare handlinger. Bestemmelsen forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at det er strafbart – i det mindste i grovere tilfælde – bevidst at fremstille, sælge, erhverve med henblik på brug, importere, distribuere eller på anden måde stille et af de omfattede værktøjer til rådighed uretmæssigt og med forsæt til, at det anvendes til at begå en af de strafbare handlinger, der er omfattet af direktivets artikel 3-6.

De værktøjer, der er omfattet af bestemmelsen, er edb-programmer, der hovedsageligt er beregnet eller tilpasset til at begå en af de strafbare handlinger, og edb-password, adgangskoder eller tilsvarende data, hvorved der kan opnås adgang til et helt informationssystem eller en del heraf.

Det bemærkes, at der ikke findes en lignende bestemmelse i rammeafgørelsen eller i Europarådets konvention.

2.4.2. I dansk ret er forsøg på og medvirken til at begå en strafbar handling omfattet af straffelovens §§ 21 og 23, jf. også nedenfor under pkt. 2.5.

Handlinger i artikel 7 foretages ifølge bestemmelsen med forsæt til, at værktøjet anvendes til at begå en af de strafbare handlinger, der er omfattet af direktivets artikel 3-6, jf. ovenfor under pkt. 2.4.1. Handlingerne må derfor i dansk ret antages være omfattet af bestemmelserne om forsøg og medvirken. Fremstilling af et edb-program omfattet af bestemmelsen med forsæt til selv at begå en strafbar handling efter artikel 3-6 vil således f.eks. kunne straffes som forsøg på at begå den pågældende strafbare handling, mens der vil kunne straffes for medvirken til lovovertrædelsen, hvis fremstillingen sker med forsæt til, at en anden skal begå den pågældende lovovertrædelse.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 7.

2.5. Medvirken og forsøg

2.5.1. Artikel 8 indeholder regler om forsøg og medvirken.

Ifølge *stk. 1* forpligtes medlemsstaterne til at sikre, at det er strafbart at anstifte eller medvirke og tilskynde til at begå en strafbar handling omfattet af direktivets artikel 3-7.

Efter *stk. 2* forpligtes medlemsstaterne til at sikre, at det er strafbart at forsøge at begå en handling omfattet af direktivets artikel 4 og 5.

Det bemærkes, at direktivets artikel 5 svarer til artikel 5 i rammeafgørelsen og i det væsentlige svarer til artikel 11 i Europarådets konvention.

2.5.2. Forsøg på og medvirken bl.a. til at begå lovovertrædelser, der er omfattet af direktivet, er strafbart i dansk ret.

Det fremgår således af straffelovens § 21, at handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse, når denne ikke fuldbyrdes, straffes som forsøg.

Efter straffelovens § 23 omfatter den for en lovovertrædelse givne straffebestemmelse alle, der ved tilskyndelse, råd eller dåd har medvirket til gerningen.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 8.

2.6. Sanktioner

2.6.1. Artikel 9, stk. 1, forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at de strafbare handlinger omfattet af direktivets artikel 3-8 kan straffes med strafferetlige sanktioner, der er effektive, står i et rimeligt forhold til den strafbare handlings grovhed og har afskrækkende virkning.

Bestemmelsen, hvor stk. 2-5 er nye i forhold til rammeafgørelsen og Europarådets konvention, fastsætter mindstekrav til de strafferammer, der skal gælde for overtrædelse af de af direktivet omfattede strafbare handlinger.

2.6.2. Artikel 9, stk. 2, forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at de strafbare handlinger omfattet af artikel 3-7 – i det mindste i grove tilfælde – kan straffes med fængsel med en maksimumstraf på mindst 2 år.

2.6.2.1. Ulovlig adgang til informationssystemer efter direktivets artikel 3 må som beskrevet ovenfor under pkt. 2.3.1 anses for omfattet af straffelovens § 263, stk. 2, om hacking, § 301 a om at skaffe eller videregive adgangsmidler til kommercielle informationssystemer, § 263 a om at skaffe eller videregive adgangsmidler til ikke-kommercielle informationssystemer og § 279 a om databedrageri.

Strafferammen for overtrædelse af § 263, stk. 2, er 1 år og 6 måneders fængsel. Begås handlingen med forsæt til at skaffe sig eller gøre sig bekendt med erhvervshemmeligheder eller under andre

særligt skærpende omstændigheder, eller når der er tale om overtrædelse af mere systematisk eller organiseret karakter, kan straffen stige til fængsel indtil 6 år.

Strafferammen for overtrædelse af § 301 a er 1 år og 6 måneders fængsel. Begås handlingen under særligt skærpende omstændigheder – navnlig hvor videregivelse mv. sker erhvervsmæssigt, i en videre kreds eller under omstændigheder, hvor der er særlig risiko for omfattende misbrug – er straffen fængsel indtil 6 år.

Strafferammen for overtrædelse § 263 a er 1 år og 6 måneders fængsel. Begås handlingen under særligt skærpende omstændigheder – navnlig hvor videregivelse mv. sker i særligt stort omfang eller indebærer særlig risiko for betydelig skade – er straffen fængsel indtil 6 år.

Overtrædelse af § 279 a kan medføre straf efter reglerne i §§ 285-286. Efter § 285 er strafferammen 1 år og 6 måneders fængsel. Er handlingen af særlig grov beskaffenhed, navnlig på grund af udførelsesmåden, eller fordi forbrydelsen er udført af flere i forening, eller som følge af omfanget af den opnåede eller tilsigtede vinding, eller når et større antal forbrydelser er begået kan straffen stige til fængsel indtil 8 år, jf. § 286.

2.6.2.2. Ulovligt indgreb i informationssystemer efter direktivets artikel 4 er som beskrevet ovenfor under pkt. 2.3.2 omfattet af straffelovens § 193 om driftsforstyrrelser, § 291 om hærværk og § 293 om rådighedshindringer.

Strafferammen for overtrædelse af § 193 er 6 års fængsel.

Strafferammen for overtrædelse af § 291 er 1 år og 6 måneders fængsel. Øves der hærværk af betydeligt omfang eller af mere systematisk eller organiseret karakter, eller er gerningsmanden tidligere fundet skyldig for overtrædelse af bl.a. den pågældende bestemmelse, kan straffen stige til fængsel i 6 år.

Strafferammen for overtrædelse af § 293, stk. 2, er 1 års fængsel. Straffen kan stige til fængsel i 2 år, hvis der er tale om en overtrædelse af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger særligt skærpende omstændigheder.

2.6.2.3. Ulovligt indgreb i data efter direktivets artikel 5 er som beskrevet ovenfor i pkt. 2.3.3 omfattet af straffelovens § 291, stk. 1, om hærværk, og § 293, stk. 2, om rådighedshindring. Der henvises for så vidt angår strafferammerne for overtrædelse af disse bestemmelser til pkt. 2.6.2.2 ovenfor.

2.6.2.4. Ulovlig opfangning efter direktivets artikel 6 er som beskrevet ovenfor i pkt. 2.3.4 omfattet af straffelovens § 263, stk. 2, om hacking. Der henvises for så vidt angår strafferammen for overtrædelse af denne bestemmelse til pkt. 2.6.2.1 ovenfor.

2.6.2.5. Fremstilling mv. af værktøjer efter direktivets artikel 7 med forsæt til at anvende disse til at begå strafbare handlinger omfattet af direktivet straffes efter straffelovens regler om forsøg og medvirken, jf. straffelovens §§ 21 og 23. Ved straf for forsøg på eller medvirken til at begå et strafbart forhold omfattet af direktivet, jf. artikel 7 og 8, anvendes strafferammerne i de konkrete straffebestemmelser.

2.6.2.6. Maksimumsstraffen på mindst 2 års fængsel i direktivets artikel 9, stk. 2, skal efter bestemmelsen som minimum være gældende ved grove overtrædelser af de strafbare bestemmelser. De omfattede bestemmelser i straffeloven indeholder som anført ovenfor alle strafferammer, hvor grove overtrædelser kan straffes med en maksimumsstraf på mindst 2 år.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 9, stk. 2.

2.6.3. Artikel 9, stk. 3, forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 4 og 5 kan straffes med fængsel med en maksimumstraf på mindst 3 år, når de begås forsætligt, og når et betydeligt antal informationssystemer er blevet berørt gennem anvendelsen af et af værktøjerne i direktivets artikel 7, der hovedsageligt er udarbejdet eller tilpasset til dette formål.

2.6.3.1. Som beskrevet under pkt. 2.3.2 er ulovligt indgreb i informationssystemer efter direktivets artikel 4 omfattet af straffelovens § 193 om driftsforstyrrelser, § 291 om hærværk og § 293 om rådighedshindringer. §§ 193 og 291 har begge en skærpet strafferamme på 6 års fængsel i grove

tilfælde, herunder når handlingen er mere systematisk eller har et betydeligt omfang. De skærpede strafferammer vil også kunne anvendes, når et betydeligt antal informationssystemer er blevet berørt, herunder gennem anvendelse af et redskab omfattet af direktivets artikel 7, hvis betingelserne i øvrigt er opfyldt. § 293, stk. 2, har en strafferamme på 2 års fængsel i grovere tilfælde.

2.6.3.2. Som beskrevet under pkt. 2.3.3 er ulovligt indgreb i data efter direktivets artikel 5 omfattet af straffelovens § 291, stk. 1, om hærværk, der har en strafferamme på 6 års fængsel i grove tilfælde. Den skærpede strafferammer vil også kunne anvendes, når der er anvendt et redskab omfattet af direktivets artikel 7, hvis betingelserne i øvrigt er opfyldt.

2.6.3.3. En gennemførelse af direktivets artikel 9, stk. 3, indebærer, at den skærpede strafferamme i straffelovens § 293, stk. 2, vil skulle hæves fra 2 års fængsel til 3 års fængsel. Den skærpede strafferamme finder ifølge § 293, stk. 2, anvendelse, hvor der er tale om overtrædelser af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger skærpende omstændigheder. Det bør i forbindelse med en forhøjelse af strafferammen nærmere overvejes, om det – med henblik på at sikre en fuld korrekt implementering af direktivet – i bestemmelsen udtrykkeligt bør angives, at den skærpede strafferamme finder anvendelse i tilfælde, hvor et betydeligt antal informationssystemer er blevet berørt gennem anvendelsen af et af værktøjerne i direktivets artikel 7, der hovedsageligt er udarbejdet eller tilpasset til dette formål.

Der henvises i øvrigt til pkt. 2.6.4 nedenfor, hvor der er redegjort nærmere for direktivets artikel 9, stk. 4, der stiller krav om en strafferamme på mindst 5 års fængsel for bl.a. overtrædelse af straffelovens § 293, stk. 2.

2.6.4. Artikel 9, stk. 4, forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 4 og 5 kan straffes med fængsel med en maksimumstraf på mindst 5 år i følgende tilfælde:

a) De er begået inden for rammerne af en kriminel organisation som defineret i rammeafgørelse 2008/841/RIA uanset den deri fastsatte straf.
b) De forvolder alvorlig skade.

c) De er begået mod et kritisk infrastruktur-informationssystem.

Ved et kritisk infrastruktur-informationssystem forstås ifølge præambelbetragtning nr. 4 et system, som er væsentligt for opretholdelsen af vitale samfundsmæssige funktioner, menneskers sundhed, sikkerhed, transportnetværk mv.

2.6.4.1. Strafferammerne for bestemmelserne i straffeloven, der omfatter direktivets artikel 4 og 5, er beskrevet ovenfor under pkt. 2.3.2 og pkt. 2.3.3.

Straffelovens § 193 om driftsforstyrrelser har en normalstrafferamme på 6 års fængsel. Tilfælde omfattet af direktivets artikel 9, stk. 4, vil derfor også være omfattet af denne strafferamme.

Straffelovens § 291 om hærværk har en strafferamme på 1 år og 6 måneders fængsel. Øves der hærværk af betydeligt omfang eller af mere systematisk eller organiseret karakter, eller er gerningsmanden tidligere fundet skyldig for overtrædelse af bl.a. den pågældende bestemmelse, kan straffen stige til fængsel i 6 år.

Ifølge bemærkningerne til straffelovens § 291, stk. 2, jf. lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.) skal bestemmelsen om, at hærværk af mere systematisk eller organiseret karakter henføres til den skærpede strafferamme ses i sammenhæng med rammeafgørelsen og EU's fælles aktion af 21. december 1998 om at gøre det strafbart at deltage i en kriminel organisation. Det må derfor antages, at handlinger begået inden for rammerne af en kriminel organisation som defineret i rammeafgørelsen, er omfattet af den skærpede strafferamme i straffelovens § 291, stk.2.

Hærværk begået mod et kritisk infrastruktur-informationssystem kan efter omstændighederne være omfattet af den skærpede strafferamme. Det bemærkes i den forbindelse, at det følger af Rigsadvokatens Meddelelse nr. 5/2005 om strafpåstande i sager om overtrædelse af straffeloven, at ved hærværk med en skadesstørrelse på mere end 15.000 kr., bør forholdet henføres under straffelovens § 291, stk. 2.

Ved et tilvalg af direktivet bør det dog overvejes nærmere, om hærværk begået mod et kritisk infrastruktur-informationssystem – med henblik på at sikre en fuld korrekt implementering af direktivet – udtrykkeligt skal omfattes af den skærpede strafferamme i straffelovens § 291, stk. 2.

Straffelovens § 293, stk. 2, har en skærpet strafferamme på fængsel i 2 år. En gennemførelse af direktivet nødvendiggør, at denne strafferamme hæves til 5 års fængsel i de i artikel 9, stk. 4 nævnte tilfælde. Det bemærkes, som anført under pkt. 2.6.3.3 ovenfor, at en gennemførelse af direktivet også indebærer, at den skærpede strafferamme i § 293, stk. 2, hæves til 3 års fængsel i de i artikel 9, stk. 3, nævnte tilfælde. Ved et tilvalg af direktivet vil det umiddelbart være nærliggende nærmere at overveje, om strafferammen bør hæves til 5 års fængsel i både de i artikel 9, stk. 3, og artikel 9, stk. 4, nævnte tilfælde.

2.6.5. Artikel 9, stk. 5, forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at når de strafbare handlinger i artikel 4 og 5 begås ved at misbruge en anden persons personoplysninger med det formål at vinde tredjemands tillid og derved skade den, som identiteten egentlig tilhører, kan det i overensstemmelse med national ret betragtes som skærpende omstændigheder, medmindre handlingen allerede er omfattet af en anden handling, der er strafbar i henhold til national ret.

Bestemmelsen omhandler således grove former for it-kriminalitet, som begås ved at misbruge en anden persons personoplysninger med det formål at vinde tredjemands tillid og derved skade den, som identiteten tilhører – såkaldt identitetstyveri.

Identitetstyveri som defineret i artikel 9, stk. 5, er ikke selvstændigt kriminaliseret i dansk ret.

Generelt begås identitetstyveri eller anden form for identitetsmisbrug som altovervejende hovedregel med henblik på at begå anden kriminalitet, herunder navnlig forskellige former for berigelseskriminalitet, hacking, databedrageri samt chikane og trusler. Identitetstyveri tjener således som middel til at begå andre former for kriminalitet.

Det bemærkes i den forbindelse, at det alene vil være rådighedshindringer, driftsforstyrrelser og hærværk efter direktivets artikel 4 og 5, som er omfattet af bestemmelsen i artikel 9, stk. 5, om, at

det er en skærpende omstændighed at misbruge en andens personoplysninger. Direktivet indeholder ikke i øvrigt bestemmelser vedrørende identitetstyveri.

Benytter nogen en anden persons navn og password til at logge på eksempelvis cpr-registeret, hvorefter den pågældende sletter informationer om alle, der hedder Jensen, vil handlingen være omfattet af direktivets artikel 9, stk. 5, jf. artikel 5. Forholdet vil efter dansk ret kunne straffes som hærværk, jf. straffelovens § 291.

Benytter en person derimod en anden persons navn og cpr-nummer til at købe mobiltelefoner over internettet, hvorefter den "misbrugte" person får tilsendt en række regninger for telefoner, som den pågældende aldrig har bestilt, vil forholdet falde uden for direktivets anvendelsesområde. Forholdet vil i dansk ret være strafbart som bedrageri over for sælgeren af telefonerne, jf. straffelovens § 279.

Ved straffens fastsættelse finder de almindelig principper i straffelovens kapitel 10 (§§ 80-89 a) anvendelse. Det fremgår af straffelovens § 80, stk. 1 og 2, at der ved straffens fastsættelse bl.a. skal lægges vægt på lovovertrædelsens grovhed, herunder den med lovovertrædelsen forbundne skade, fare og krænkelse. Straffelovens § 81 indeholder herudover en ikke-udtømmende opregning af forhold, der i almindelighed ved straffens fastsættelse skal indgå som skærpende omstændigheder. Her nævnes bl.a., at gerningen er udført af flere i forening eller er særligt planlagt eller led i omfattende kriminalitet, jf. nr. 2 og 3.

De gældende regler for strafudmåling giver således allerede mulighed for ved strafudmålingen at tage højde for de relevante konkrete omstændigheder i forbindelse med eksempelvis hærværk, der begås ved misbrug af en anden persons identitet.

Direktivets artikel 9, stk. 5, fastsætter ikke en egentlig pligt for medlemsstaterne til at kriminalisere identitetstyveri. Bestemmelsen fastslår således alene, at i det omfang identitetstyveri ikke er selvstændigt kriminaliseret i national ret, skal det kunne anses som en skærpende omstændighed, hvis en strafbar handling er begået ved misbrug af en anden persons personoplysninger med det formål at vinde en tredjemands tillid og derved skade den, som identiteten egentlig tilhører.

Som nævnt ovenfor indeholder straffeloven ikke en selvstændig bestemmelse, som kriminaliserer identitetstyveri som defineret i artikel 9, stk. 5. Straffeloven indeholder endvidere ikke en bestemmelse, der specifikt foreskriver, at misbrug af en andens identitet i forbindelse med en strafbar handling kan betragtes som en skærpende omstændighed i forbindelse med straffens fastsættelse. Da straffelovens § 81 ikke er udtømmende, har domstolene dog allerede i dag mulighed for at tillægge det betydning som en skærpende omstændighed, at en strafbar handling er begået ved hjælp af misbrug af en anden persons identitet.

Med henblik på at sikre en fuld korrekt implementering af direktivet i dansk ret vil der dog ved et tilvalg af direktivet være behov for at lovfæste artikel 9, stk. 5. Dette vil kunne ske ved at udvide straffelovens § 81, så misbrug af en andens personoplysninger i tilfælde omfattet af direktivet i almindelighed skal betragtes som en skærpende omstændighed ved straffens udmåling. Det kan alternativt overvejes nærmere at indføre en selvstændig bestemmelse om et sådan misbrug.

2.7. Juridiske personer

2.7.1. Artikel 10 vedrører juridiske personers ansvar. Bestemmelsen forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at juridiske personer kan drages til ansvar for de i artikel 3-8 omhandlede strafbare handlinger, som er begået for at skaffe dem vinding af en person, der handler enten individuelt eller som medlem af et organ under den juridiske person, og som har en ledende stilling inden for den juridiske person, idet den pågældende har beføjelse til at repræsentere den juridiske person, bemyndigelse til at træffe beslutninger på den juridiske persons vegne eller bemyndigelse til at udøve intern kontrol inden for den juridiske person.

Medlemsstaterne skal endvidere sikre, at den juridiske person kan drages til ansvar, hvis manglende tilsyn eller kontrol fra en af de i stk. 1 omhandlede personers side har gjort det muligt for en person, der er underlagt den juridiske persons myndighed, at begå en strafbar handling omfattet af artikel 3-8 med henblik på at skaffe den juridiske person vinding, jf. bestemmelsens *stk. 2*.

Bestemmelsens *stk. 3*, angiver, at en juridisk persons ansvar i henhold til bestemmelsens stk. 1 og 2 ikke udelukker strafferetlig retsforfølgning af fysiske personer, der begår eller anstifter eller medvirker til nogen af de i artikel 3-8 omhandlede strafbare handlinger.

Det bemærkes, at direktivets artikel 10 svarer til artikel 8 i rammeafgørelsen og indholdsmæssigt i det væsentlige svarer til artikel 12 i Europarådets konvention.

2.7.2. I dansk ret kan der pålægges juridiske personer (selskaber mv.) strafansvar efter reglerne i straffelovens kapitel 5 for overtrædelser af straffeloven, jf. straffelovens § 306.

Strafansvar for en juridisk person er efter straffelovens § 27 undergivet nogle almindelige betingelser, der gælder for denne ansvarsform. Strafansvar for en juridisk person forudsætter således, at der inden for dens virksomhed er begået en overtrædelse, der kan tilregnes en eller flere personer, der er knyttet til den juridiske person, eller den juridiske person som sådan. Bestemmelsen omfatter alle ansatte mv. i den juridiske person, og den er således ikke begrænset til overtrædelser, der kan tilregnes ledelsen.

Adgangen til at pålægge juridiske personer strafansvar indebærer ikke en begrænsning i mulighederne for at pålægge enkeltpersoner strafansvar i anledning af de samme overtrædelser. Dette spørgsmål afgøres i overensstemmelse med de almindelige principper for ansvarsplacering.

I Rigsadvokatens meddelelse nr. 5 af 6. oktober 1999 er der fastsat nærmere retningslinjer for anklagemyndighedens valg af ansvarssubjekt i tilfælde, hvor anklagemyndigheden finder at kunne gennemføre en straffesag mod en juridisk person og en eller flere enkeltpersoner i anledning af samme strafbare handling. Det følger af meddelelsen, at der som udgangspunkt rejses tiltalte mod den juridiske person som sådan. Har ledelsen eller en overordnet ansat, herunder en direktør, handlet forsætligt eller udvist grov uagtsomhed, rejses der også tiltale mod den eller de personligt ansvarlige. Der rejses i almindelighed ikke tiltale mod underordnede ansatte, medmindre der foreligger særlige omstændigheder. Dette kan f.eks. være tilfældet, hvis der er tale om en grov overtrædelse, som den underordnede ansatte har begået forsætligt og eventuelt også på eget initiativ. Der rejses i disse tilfælde tiltale mod både den juridiske person og den underordnede ansatte.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 10.

2.7.3. Artikel 11 vedrører sanktioner over for juridiske personer. Bestemmelsen forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at juridiske personer, der drages til ansvar efter artikel 10, stk. 1, kan straffes med sanktioner, der er effektive, står i et rimeligt forhold til handlingens grovhed og har afskrækkende virkning, som omfatter strafferetlige og andre bøder, og som kan omfatte udelukkelse fra offentlige ydelser eller tilskud, midlertidigt eller varigt forbud mod at udøve erhvervsvirksomhed, anbringelse under retsligt tilsyn, tvangsopløsning efter retskendelse eller midlertidig eller permanent lukning af forretningssteder, der er blevet brugt til at begå den strafbare handling.

I s*tk. 2*, forpligtes medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at juridiske personer, der kendes ansvarlig efter artikel 10, stk. 2, kan straffes med sanktioner eller andre foranstaltninger, der er effektive, står i et rimeligt forhold til handlingens grovhed og har afskrækkende virkning.

Det bemærkes, at direktivets artikel 5 svarer til artikel 9 i rammeafgørelsen og indholdsmæssigt i det væsentlige svarer til artikel 13 i Europarådets konvention.

2.7.4. I dansk ret kan en juridisk person straffes med bøde, når det er bestemt ved eller i medfør af lov, jf. straffelovens § 25. Herudover vil f.eks. rettighedsfrakendelse efter straffelovens § 79 kunne anvendes i forhold til juridiske personer.

Dansk ret vurderes på den baggrund at være i overensstemmelse med direktivets artikel 11. Det bemærkes, at bestemmelsen alene forpligter medlemsstaterne til at sikre, at juridiske personer kan pålægges bøder, mens der er valgfrihed med hensyn til andre sanktioner.

2.8. Straffemyndighed

2.8.1. Artikel 12 indeholder bestemmelser om straffemyndighed (jurisdiktion).

Ifølge *stk. 1* fastlægger hver medlemsstat sin strafmyndighed med hensyn til de i artikel 3-8 omhandlede strafbare handlinger, a) når en handling er begået helt eller delvist på medlemsstatens

område eller b) af en af medlemsstatens statsborgere, i det mindste i de tilfælde, hvor handlingen er en strafbar handling dér, hvor den blev begået.

Stk. 2 angiver, at når en medlemsstat fastlægger sin straffemyndighed i overensstemmelse med bestemmelsens stk. 1, litra a), er medlemsstaten forpligtet til at sikre, at straffemyndigheden omfatter tilfælde, hvor gerningsmanden begår den strafbare handling, mens vedkommende fysisk befinder sig på dens område, uanset om den strafbare handling er rettet mod et informationssystem på dens område, eller hvor den strafbare handling begås mod et informationssystem på dens område, uanset om gerningsmanden på gerningstidspunktet fysisk befinder sig på dens område.

Ifølge *stk. 3* skal en medlemsstat underrette Kommissionen, hvis den beslutter at fastlægge straffemyndighed med hensyn til en af de i artikel 3-8 omhandlede strafbare handlinger, som er begået uden for dens område, herunder når gerningsmanden har sit sædvanlige opholdssted på dens område, eller den strafbare handling er begået til fordel for en juridisk person, som har sit hjemsted på dens område.

Det bemærkes, at direktivets artikel 5 svarer til artikel 10 i rammeafgørelsen.

2.8.2. Efter dansk ret kan der foretages retsforfølgning i Danmark af strafbare forhold, som er undergivet dansk straffemyndighed efter straffelovens §§ 6-12.

Efter straffelovens § 6 omfatter dansk straffemyndighed handlinger begået i den danske stat og – i visse nærmere angivne tilfælde – handlinger foretaget på et dansk fartøj (territorialprincippet). Det bemærkes, at når en del af en lovovertrædelse er begået i den danske stat, anses lovovertrædelsen i sin helhed for at være begået her i landet, jf. straffelovens § 9, stk. 4. Forsøgs- og medvirkenshandlinger anses for foretaget i den danske stat, hvis gerningsmanden befandt sig her i landet ved handlingens foretagelse, uanset om lovovertrædelsen fuldbyrdes eller tilsigtes fuldbyrdet uden for den danske stat, jf. straffelovens § 9, stk. 3.

Har den strafbare handling ingen tilknytning til Danmark, kan der i stedet være dansk straffemyndighed efter straffelovens § 7. Ifølge straffelovens § 7 er det en betingelse for dansk straffemyndighed i forhold til udlandshandlinger, at gerningsmanden er dansk statsborger, har

bopæl eller har lignende fast ophold i Danmark. Det vil endvidere i de fleste situationer være en betingelse, at handlingen også er strafbar efter lovgivningen på gerningsstedet (dobbelt strafbarhed). Handlinger foretaget uden for et myndighedsområde af en person, der på tidspunktet for sigtelsen har den anførte tilknytning til Danmark, er undergivet dansk straffemyndighed, hvis handlinger af den pågældende art kan medføre højere straf end fængsel i 4 måneder, jf. straffelovens § 7, stk. 2. Ifølge straffelovens § 7, stk. 3, finder bestemmelserne i stk. 1 og 2 tilsvarende anvendelse på udlandshandlinger begået af en person, der har indfødsret eller bopæl i de andre nordiske lande, og som opholder sig i Danmark.

Ifølge straffelovens § 9, stk. 1, anses handlinger for foretaget, der hvor gerningsmanden befandt sig ved handlingens foretagelse. For så vidt angår juridiske personer, anses handlinger for foretaget, hvor den eller de handlinger, som medfører ansvar for den juridiske person, er foretaget. Hvis en handlings strafbarhed afhænger af eller påvirkes af en indtrådt eller tilsigtet følge, anses handlingen tillige for foretaget, hvor virkningen er indtrådt, eller hvor gerningsmanden har forsæt til, at virkningen skulle indtræde, jf. straffelovens § 9, stk. 2. Hvis lovovertrædelsen vedrører tekst-, lyd- eller billedmateriale mv., som ved en handling i udlandet er gjort alment tilgængeligt her i landet gennem internettet eller et lignende system til spredning af information, anses lovovertrædelsen for begået i Danmark, hvis materialet har særlig relation her til landet, jf. straffelovens § 9 a.

Danmark har på denne baggrund efter gældende ret straffemyndighed, i det omfang artikel 10 kræver det.

Det bemærkes, at hvis direktivets krav til dansk straffemyndighed ikke allerede var opfyldt, ville en dansk tiltrædelse af direktivet indebære, at Danmark fik straffemyndighed, i det omfang direktivet kræver det. Det følger således af straffelovens § 8, nr. 5, at handlinger, som foretages uden for den danske stat, hører under dansk straffemyndighed, uden hensyn til hvor gerningsmanden hører hjemme, når handlingen er omfattet af en mellemfolkelig overenskomst, ifølge hvilken Danmark er forpligtet til at foretage retsforfølgning. Bestemmelsen omfatter bl.a. EU-retlige forpligtelser.

Det bemærkes i øvrigt, at Danmark ved en tiltrædelse af direktivet vil skulle underrette Kommissionen om reglerne om dansk straffemyndighed over handlinger, som foretages på dansk fartøj efter straffelovens § 6, stk. 1, nr. 2 og 3, som foretages af en person, der er bosat i den danske

stat eller har lignende fast ophold her i landet efter straffelovens § 7, stk. 1 og 2, og af en person, der har indfødsret i eller er bosat i Finland, Island, Norge eller Sverige, og som opholder sig her i landet, jf. § 7, stk. 3. Danmark bør også underrette Kommissionen om, at reglerne om straffemyndighed over handlinger foretaget af danske statsborgere også finder anvendelse på handlinger foretaget af danske juridiske personer.

2.9. Udveksling af oplysninger

2.9.1. Artikel 13 vedrører udveksling af oplysninger. Bestemmelsen angiver, at medlemsstaterne med henblik på udveksling af oplysninger om de i artikel 3-8 omhandlede strafbare handlinger skal sikre, at de har et funktionsdygtigt nationalt kontaktpunkt, og at de gør brug af det bestående netværk af kontaktpunkter, der står til disposition døgnet rundt på alle ugens dage. Medlemsstaterne skal endvidere sikre, at der findes procedurer, så den kompetente myndighed i forbindelse med hasteanmodninger om hjælp inden for 8 timer fra modtagelsen kan angive som minimum, om anmodningen vil blive imødekommet, samt på hvilken måde og på hvilket tidspunkt dette forventes at ske.

Stk. 2 angiver, at medlemsstaterne skal underrette Kommissionen om dens udpegede kontaktpunkt efter stk. 1. Kommissionen videresender oplysningerne til de øvrige medlemsstater og kompetente specialiserede EU-agenturer og -organer.

Stk. 3 forpligter medlemsstaterne til at træffe de nødvendige foranstaltninger til at sikre, at der stilles passende anmeldelseskanaler til rådighed med henblik på at lette anmeldelse uden unødig forsinkelse til de kompetente nationale myndigheder om de i artikel 3-6 omhandlede strafbare handlinger.

Ifølge præambelbetragtning nr. 22 har bestemmelsen til formål at øge vigtigheden af bestående netværk, såsom G8 eller Europarådets netværk af kontaktpunkter, der står til disposition døgnet rundt på alle ugens dage. Disse netværk bør kunne yde effektiv bistand og derved f.eks. lette udvekslingen af tilgængelige relevante oplysninger og adgangen til teknisk rådgivning mv. For at sikre netværkets funktionsdygtighed bør hvert kontaktpunkt have kapacitet til hurtigt at kommunikere med andre kontaktpunkter.

I forhold til de forpligtelser, som de eksisterende netværk af kontaktpunkter allerede er undergivet, indføres som noget nyt en forpligtelse til i forbindelse med hasteanmodninger om hjælp inden 8 timer fra modtagelsen som minimum at kunne angive, om anmodningen vil blive imødekommet, samt på hvilken måde og på hvilket tidspunkt dette forventes at ske. Ifølge præambelbetragtning nr. 22 er den nye forpligtelse begrundet i den hastighed, hvormed der kan foretages omfattende it-angreb.

2.9.2. Artikel 13, der vedrører udveksling af oplysninger inden for de eksisterende netværk af kontaktpunkter, herunder i regi af Europarådet, giver ikke anledning til lovgivningsmæssige overvejelser.

Danmark har afgivet en erklæring i henhold til Europarådets konvention om IT-kriminalitet om, at Rigspolitiet er udpeget som Danmarks kontaktpunkt.

Rigspolitiet har oplyst, at direktivet på dette punkt er gennemført forskelligartet i de enkelte medlemsstater. Generelt anvender medlemsstaterne som udgangspunkt deres i forvejen udpegede generelle nationale kontaktpunkter (i Danmark Rigspolitiets Kommunikationscenter), der herefter varetager kommunikationen til de enheder i de øvrige medlemsstaters retshåndhævende myndigheder, der varetager efterforskning af IT-kriminalitet (i Danmark Nationalt Cyber Crime Center (NC3)). En del af udvekslingen af oplysninger (særligt inden for almindelig kontortid) foregår dog i praksis også direkte mellem de enheder i medlemsstaternes retshåndhævende myndigheder, der varetager efterforskning af IT-kriminalitet.

Danmark tager, som det kræves efter direktivet, allerede del i hastende udveksling af oplysninger om IT-kriminalitet enten via Rigspolitiets Kommunikationscenter eller direkte via NC3 med bl.a. de øvrige EU-medlemsstater, idet lignende bestemmelser om hastesikring af data fremgår af Europarådets konvention. Dette samarbejde fungerer smidigt og effektivt. Der er dog på årsbasis kun brug for hastesikring af data i et meget begrænset omfang.

2.10. Overvågning og statistik

2.10.1. Artikel 14, stk. 1, vedrører overvågning og statistik. Bestemmelsen angiver, at medlemsstaterne skal sikre, at der findes et system til registrering, fremstilling og fremlæggelse af statistiske oplysninger om de i artikel 3-7 omhandlede strafbare handlinger.

Stk. 2 angiver, at de statistiske oplysninger efter stk. 1 mindst skal omfatte de eksisterende oplysninger om det antal strafbare handlinger, der henvises til i artikel 3-7, som er registreret i medlemsstaterne, og det antal personer, der er blevet retsforfulgt og dømt for de strafbare handlinger.

Medlemsstaterne skal ifølge *stk. 3* fremsende de indsamlede oplysninger til Kommissionen, der sikrer, at der offentliggøres en konsolideret oversigt over de statistiske rapporter, og at denne fremsendes til de kompetente specialiserede EU-agenturer og -organer.

Bestemmelsen, der er af rent administrativ karakter, giver ikke anledning til lovgivningsmæssige overvejelser.

Det bemærkes, at de oplysninger, som skal sendes til Kommissionen, formentlig allerede registreres i politiet og anklagemyndighedens sagsbehandlingssystemer.

2.11. Afsluttende bestemmelser

Direktivet indeholder i *artikel 15-19* afsluttende bestemmelser.

Det fremgår heraf bl.a., at direktivet erstatter rammeafgørelse 2005/222/RIA i forhold til de medlemsstater, der er bundet af direktivet.

Endvidere indeholder de afsluttende artikler bestemmelser om direktivets ikrafttræden, gennemførelse og Kommissionens evaluering heraf.

Bestemmelserne giver ikke anledning til lovgivningsmæssige overvejelser.

3. Konsekvenser

Direktivet har overordnet til formål at sikre et højt beskyttelsesniveau på området, idet det er af afgørende betydning for borgere og virksomheder, at de kan have tillid til informationssystemers funktionsdygtighed og sikkerhed.

Et tilvalg af direktivet vil forpligte Danmark til at have samme minimumsregler som resten af EU med hensyn til afgrænsningen af strafbare handlinger i forbindelse med angreb på informationssystemer og strafferetlige sanktioner herfor. Danmark vil efter et tilvalg af direktivet således ikke kunne ændre den eksisterende lovgivning vedrørende disse spørgsmål på en måde, der fraviger direktivets minimumskrav.

Direktivet svarer i vidt omfang til Europarådets konvention om IT-kriminalitet fra 2001 samt Rådets rammeafgørelse 2005/222/RIA, som er gennemført i dansk ret ved lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.).

Dansk ret vurderes i vidt omfang allerede at være i overensstemmelse med direktivet. Et tilvalg af direktivet forventes dog at nødvendiggøre visse lovændringer. Der vil – ud over at en strafferamme skal hæves – navnlig være tale om ændringer af mere teknisk karakter.

Det vurderes således som anført i pkt. 2.6.3.3 og pkt. 2.6.4.1 ovenfor, at en gennemførelse af direktivets strafferammekrav nødvendiggør, at strafferammen i straffelovens § 293, stk. 2, hæves til henholdsvis 3 og 5 års fængsel i nærmere angivne tilfælde. Dette vil dog ikke nødvendigvis have betydning for den konkrete strafudmåling.

Som anført under pkt. 2.6.3.3 ovenfor bør det endvidere overvejes nærmere om det – med henblik på at sikre en fuld korrekt implementering af direktivet – udtrykkeligt bør anføres i § 293, stk. 2, at den skærpede strafferamme finder anvendelse i tilfælde, hvor et betydeligt antal informationssystemer er blevet berørt gennem anvendelsen af et af værktøjerne i direktivets artikel 7, der hovedsageligt er udarbejdet eller tilpasset til dette formål.

Det bør som anført under pkt. 2.6.4.1 ovenfor også overvejes nærmere, om hærværk begået mod et kritisk infrastruktur-informationssystem – med henblik på at sikre en fuld korrekt implementering af direktivet – udtrykkeligt skal omfattes af den skærpede strafferamme i straffelovens § 291, stk. 2.

Desuden vil det som anført under pkt. 2.6.5 være nødvendigt – med henblik på at sikre en fuld korrekt implementering af direktivet – at lovfæste direktivets artikel 9, stk. 5 om misbrug af en anden persons personoplysninger inden for direktivets anvendelsesområde. Dette vil kunne ske ved at udvide straffelovens § 81, så misbrug af en andens personoplysninger i tilfælde omfattet af direktivet i almindelighed skal betragtes som en skærpende omstændighed ved straffens udmåling. Det kan alternativt overvejes nærmere at indføre en selvstændig bestemmelse om et sådan misbrug.

Herudover bør som anført under pkt. 2.2.2 ovenfor overvejes nærmere, om der – med henblik på at sikre en fuldstændig korrekt implementering af direktivet – skal gennemføres en lovændring af mere teknisk karakter, således at visse af direktivets definitioner indarbejdes i de relevante bestemmelser i straffeloven eller eventuelt i bemærkningerne hertil.

Med hensyn til direktivets bestemmelse om udveksling af oplysninger, bemærkes, at dette skal ske inden for rammerne af eksisterende netværk af kontaktpunkter, herunder navnlig i regi af Europarådet, som Rigspolitiet allerede deltager i. Efter direktivet skal hasteanmodning i de eksisterende netværk af kontaktpunkter håndteres inden for 8 timer. Rigspolitiet tager imidlertid allerede i dag del i hastende udveksling af oplysninger, idet lignende bestemmelser om hastesikring af data følger af Europarådets konvention.

Til illustration af direktivets praktiske anvendelse kan anføres følgende eksempler:

En person, der hindrer adgangen til et betydeligt antal informationssystemer (e-boks, netbank mv.), vil efter direktivet skulle straffes med indtil mindst 3 års fængsel. Dette vil allerede kunne straffes efter dansk ret, idet det bemærkes, at strafferammen er 2 års fængsel.

En person hindrer adgangen til oplysninger om enkeltpersoners aktuelle og historiske behandlinger i sundhedsvæsenet, der er lagret i et informationssystem. Et informationssystem til lagring af sådanne behandlingsoplysninger vil som udgangspunkt være væsentligt til opretholdelse af menneskers

sundhed, og hindring af adgangen til oplysningerne vil kunne påvirke enkeltpersoners behandling. Efter direktivet vil et sådant hærværk skulle straffes med indtil mindst 5 års fængsel. Dette vil allerede være strafbart efter dansk ret, idet det bemærkes, at strafferammen for en sådan rådighedshindring er 2 års fængsel, hvis der er tale om en overtrædelse af mere systematisk eller organiseret karakter, eller der i øvrigt foreligger særligt skærpende omstændigheder.

Som det fremgår af de anførte eksempler forventes direktivet at medføre visse ændringer i form af en skærpelse af en enkelt strafferamme. Det bemærkes dog, at dette ikke nødvendigvis vil få betydning for den konkrete strafudmåling.

Et tilvalg af direktivet vurderes således isoleret set ikke at medføre væsentlige ændringer for borgerne, virksomheder og myndigheder.

4. Økonomiske og administrative konsekvenser

Et tilvalg af direktivet vil kunne have økonomiske konsekvenser for det offentlige, idet direktivets bestemmelser om indsamling af statistiske oplysninger om it-forbrydelser kan medføre, at der skal foretages systemtilpasninger hos Rigspolitiet. Omkostningerne til tilpasning af de nuværende systemer vurderes umiddelbart at kunne udgøre i størrelsesordenen 3-5 mio. kr. Skønnet er behæftet med en betydelig usikkerhed.