den enkelte sag. Ved vurderingen af, om risikoen for skade er væsentligt større end den, der altid ligger i en videregivelse af adgangsmidler, kan ifølge udvalget bl.a. indgå, til hvem adgangsmidler videregives (f.eks. til en organiseret hackergruppe), og hvad der videregives. Efter udvalgets opfattelse må en målrettet videregivelse af adgangsmidler til samfundsvigtige informationssystemer normalt forventes at være omfattet af den foreslåede bestemmelse i § 263 a, stk. 4.

Herudover fremgår det af betænkningen, at hvis betingelserne for at straffe for forsøg i relation til anden kriminalitet, f.eks. hacking (§ 263, stk. 2) eller databedrageri (§ 279 a), er opfyldt, vil der – uanset den foreslåede nye bestemmelse i straffelovens § 263 a – fortsat kunne dømmes for forsøg.

Selv om udbredelse via Internettet af et password til en anden persons bankkonto isoleret set indebærer en overtrædelse af den af udvalget foreslåede nye bestemmelse i straffelovens § 263 a, stk. 1, vil der således kunne straffes for forsøg på medvirken til f.eks. databedrageri efter straffelovens § 279 a, jf. § 21.

På samme måde vil der som hidtil kunne straffes for forsøg på hacking efter straffelovens § 263, stk. 2, jf. § 21, hvis en person skaffer sig f.eks. et password til en virksomheds interne informationssystem med forsæt til uberettiget at trænge ind i systemet. Dette gælder uanset, at dette forhold måtte falde uden for anvendelsesområdet for den foreslåede bestemmelse i straffelovens § 263 a, hvorefter tilegnelse alene er strafbar, hvis der er tale om adgangsmidler til et samfundsvigtigt informationssystem eller et informationssystem, der indeholder særlig personfølsomme oplysninger, jf. § 263 a, stk. 3.

2.2.1.4. Udvalget har overvejet, om strafferammen i § 263, stk. 2 (hacking), på 6 måneders fængsel er tilstrækkelig i de situationer, der ikke omfattes af stk. 3. Efter Brydensholt-udvalgets opfattelse er der behov for en forhøjelse af strafmaksimum i § 263, stk. 2, for bedre at afspejle forbrydelsens alvor i strafferammen. Udviklingen på dette område siden bestemmelsens indsættelse i 1985 gør, at der i dag er behov for en forhøjelse af strafmaksimum. Udvalget har herved bl.a. lagt vægt på, at det IT-baserede samfund er meget sårbart, og at selv et forsøg på hacking er meget føleligt for offeret, der i praksis ofte er nødt til at gennemgå hele systemet for at være sikker på, om der er sket skader. På den baggrund foreslår udvalget, at strafferammen i § 263, stk. 2, hæves til bøde eller fængsel indtil 1 år og 6 måneder.

2.2.2. Industrispionage

2.2.2.1. Brydensholt-udvalget har i betænkning nr. 1417/2002 om IT-kriminalitet overvejet, om der tillige bør være en strafferetlig regulering af tilfælde, hvor en virksomhedsgæst udnytter besøget til utilbørligt at skaffe sig information, eller hvor den besøgende ubeføjet videregiver eller benytter erhvervshemmeligheder, som den pågældende tilfældigt eller uagtsomt er kommet i besiddelse af under besøget, uden at man er kommet i besiddelse af oplysningerne som led i den almindelige fremvisning.

I betænkningen er som eksempler nævnt tilfælde, hvor en virksomhedsgæst under besøget skaffer sig information fra lokaliteter, der ikke er omfattet af rundvisningen, eller hvor den pågældende fotograferer eller medtager prøver trods forbud herom. Endvidere anføres tilfælde, hvor en besøgende ubeføjet videregiver eller benytter erhvervshemmeligheder, som den pågældende tilfældigt eller uagtsomt er kommet i besiddelse af under besøget, uden at dette er sket som led i den almindelige fremvisning. Af betænkningen fremgår det, at begrundelsen for disse situationers straffrihed hidtil er blevet søgt i, at virksomheden selv er herre over, hvem den vil lukke ind i virksomheden.

Af betænkningen fremgår det, at det i erhvervslivet som regel er acceptabelt, at virksomheder søger at skaffe sig kendskab til konkurrenternes produktionsformer, markedsføringsplaner, kundekredse mv. Det strafværdige er således ikke, at man søger sådant kundskab, men derimod måden hvorpå det eventuelt sker. Udvalget finder, at udnyttelse af muligheder, der er skabt ved, at man befinder sig i den pågældende virksomhed, f.eks. som gæst, bør være omfattet af den strafferetlige regulering i markedsføringsloven, jf. betænkningen side 71-72 og 146.

På den anførte baggrund foreslår udvalget, at der indsættes en ny bestemmelse i markedsføringslovens § 10, stk. 3, hvorefter reglerne i § 10, stk. 1 og 2, finder tilsvarende anvendelse på andre personer, der har lovlig adgang til virksomheden.

2.2.2.2. Efter udvalgets opfattelse bør der desuden være en mere ensartet strafferetlig regulering, således at strafmaksimum for ansattes industrispionage mv. ikke afhænger af, om der sker en overtrædelse af straffelovens § 263, stk. 3, der har en strafferamme på fængsel indtil 4 år, eller markedsføringslovens § 10, jf. § 22, stk. 4, der har en strafferammen på fængsel indtil 2 år. I betænkningen foreslås det på den baggrund, at der indsættes en overbygningsbestemmelse om grove overtrædelser af markedsføringslovens § 10 i en ny § 299 a i straffeloven. Der henvises til betænkningen side 72-73 og 146-147.