tidligere end den nuværende kriminalisering, som først indtræder ved forsøg på at *anvende* sådanne adgangsmidler.

Den i lovforslaget foreslåede bestemmelse i straffelovens § 263 a svarer til den af Brydensholt-udvalget foreslåede bestemmelse med enkelte mindre ændringer.

Justitsministeriet er enig i, at den fremrykkede strafferetlige beskyttelse på dette område som udgangspunkt bør omfatte erhvervsmæssigt salg og udbredelse i en videre kreds af koder eller andre adgangsmidler til ikke offentligt tilgængelige informationssystemer, hvortil adgangen er beskyttet med kode eller anden særlig adgangsbegrænsning, samt videregivelse af et større antal koder mv. til sådanne informationssystemer.

Med hensyn til visse ikke-kommercielle informationssystemer, der må anses for særligt beskyttelsesværdige, kan Justitsministeriet endvidere tiltræde Brydensholt-udvalgets forslag om, at den strafferetlige beskyttelse af disse systemer bør svare til den, der gælder for kommercielle informationssystemer, jf. ovenfor.

Efter den foreslåede bestemmelse i straffelovens § 263 a, stk. 3, straffes den, der uretmæssigt skaffer sig eller videregiver en kode eller andet adgangsmiddel som nævnt i stk. 1 til et samfundsvigtigt informationssystem, jf. straffelovens § 193, eller et informationssystem, der behandler følsomme oplysninger, som er omfattet af § 7, stk. 1, eller § 8, stk. 1, i lov om behandling af personoplysninger, om flere personers personlige forhold.

Bestemmelsen vil efter Justitsministeriets opfattelse eksempelvis være anvendelig ved uberettiget rekvirering og efterfølgende misbrug af certifikater, eksempelvis det nyligt lancerede borgercertifikat (OCES-certifikatet). Ved uberettiget rekvirering og misbrug heraf skaffes der adgang til oplysninger om den borger, certifikatet angiver at vedrøre, hvilket er omfattet af den foreslåede § 263 a, stk. 3, uanset at misbruget ikke sker med henblik på økonomisk vinding.

Efter straffelovens § 264 c finder de i straffelovens §§ 263-264 a indeholdte straffebestemmelser tilsvarende anvendelse på den, der uden at have medvirket til gerningen skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet ved overtrædelsen. Bestemmelsen omfatter visse former for efterfølgende medvirken. Det forudsættes således, at oplysningerne er fremkommet ved bl.a. hacking eller husfredskrænkelse.

Forslaget om at indsætte en ny § 263 a i straffeloven tilsigter i overensstemmelse med Brydensholt-udvalgets forslag ikke at udvide anvendelsesområdet for straffelovens § 264 c. Der henvises til bemærkningerne til lovforslagets § 1, nr. 11.

Betingelsen om, at forholdet skal være uretmæssigt, indebærer, at adgangsmidler til ikke-kommercielle informationssystemer, der videregives til lovlige formål, f.eks. som led i en systemadministrators arbejde, ikke er omfattet af bestemmelsen.

Bestemmelsens normalstrafferamme foreslås fastsat til bøde eller fængsel indtil 1 år og 6 måneder. Om baggrunden for denne afvigelse i forhold til udvalgets forslag henvises til pkt. 2.3.1.1.

Justitsministeriet kan ligeledes tiltræde Brydensholt-udvalgets forslag om en skærpet sidestrafferamme i kvalificerede videregivelsestilfælde. I lighed med det anførte under pkt. 2.3.1.1. vedrørende adgangsmidler til kommercielle informationssystemer finder Justitsministeriet dog, at den skærpede sidestrafferamme bør være anvendelig i forhold til alle handlinger, der er kriminaliseret i § 263 a og ikke kun i videregivelsestilfælde.

Justitsministeriet finder endvidere, at strafmaksimum i sidestrafferammen bør fastsættes til 6 års fængsel, jf. ovenfor under pkt. 2.3.1.1, og at den skærpede strafferamme ikke bør begrænses til særligt grove overtrædelser af § 263 a, stk. 1 og 2, men tillige bør omhandle særligt grove overtrædelser af § 263 a, stk. 3. Justitsministeriet har herved lagt vægt på, at § 263 a, stk. 3, tilsigter at give visse særlige informationssystemer en strafferetlig beskyttelse svarende til den, der foreslås for kommercielle informationssystemer i § 301 a. Efter den foreslåede § 301 a, stk. 2, straffes videregivelse mv. af adgangsmidler til kommercielle informationssystemer under særligt skærpende omstændigheder med fængsel indtil 6 år. Henset hertil bør videregivelse mv. af adgangskoder til et af de i § 263 a, stk. 3, nævnte informationssystemer tilsvarende være omfattet af den skærpede strafferamme i § 263 a, stk. 4.

Om den nærmere affattelse af den skærpede sidestrafferamme, hvorefter denne finder anvendelse under »særligt skærpende omstændigheder«, henvises til Justitsministeriets overvejelser gengivet under pkt. 2.3.1.1.

Justitsministeriet finder endelig, at den skærpede strafferamme efter en konkret vurdering i det enkelte tilfælde af samtlige sagens omstændigheder bør kunne anvendes også i andre tilfælde end de, der er opregnet i udvalgets betænkning.

Særligt skærpende omstændigheder vil efter Justitsministeriets opfattelse navnlig foreligge i tilfælde, hvor videregivelsen mv. af koder eller andre adgangs-