Bättre skydd för tekniska företagshemligheter

Ds 2020:26

Regeringskansliet
Justitiedepartementet

Bättre skydd för tekniska företagshemligheter

Ds 2020:26

Regeringskansliet
Justitiedepartementet

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Omslag: Regeringskansliets standard
Tryck: Elanders Sverige AB, Stockholm 2020

ISBN 978-91-38-25119-5
ISSN 0284-6012

Innehåll

Sammanfattning

I denna promemoria föreslås ett utvidgat straffansvar för vissa angrepp på företagshemligheter. Detta föreslås ske genom att det införs två nya straffbestämmelser – en om olovligt utnyttjande av företagshemlighet och en om olovligt röjande av företagshemlighet. Utvidgningen omfattar endast företagshemligheter av teknisk natur. Förslaget innebär att den krets av personer som omfattas av ansvar enligt lagen utvidgas något och att även exempelvis bemanningsanställda kommer att omfattas av ansvaret.

Den föreslagna kriminaliseringen syftar till att skydda företag och forskningsinstitutioner från angrepp av personer med lovlig tillgång till företagshemligheter. Ett förstärkt straffrättsligt skydd för företagshemligheter av teknisk natur ska bidra till bättre förutsättningar för företagande och teknisk utveckling, men även till att möta det hot som industrispionage utgör mot svensk industri och det svenska samhället.

Straffskalan, som är densamma för båda bestämmelserna, ska vara böter eller fängelse i högst två år. Om brottet är grovt, är straffet fängelse i lägst sex månader och högst sex år.

Enligt förslaget ska gärningarna i ringa fall inte vara straffbara. Som huvudregel ska angrepp som äger rum efter att deltagandet i den angripna verksamheten har upphört inte heller vara straffbara.

Den föreslagna utvidgningen av straffansvaret för angrepp på företagshemligheter föreslås följas av att skadeståndsansvaret utökas i viss mån.

Det föreslås även att brottstypen olovlig befattning med företagshemlighet utvidgas med anledning av att röjande av företagshemlighet kriminaliseras.

I promemorian föreslås även att möjligheten till användning av hemliga tvångsmedel utökas på så sätt att den föreslagna brottstypen olovligt röjande av företagshemlighet ska kunna föranleda

användning av hemliga tvångsmedel under samma omständigheter som företagsspioneri. Det innebär att det under förundersökning ska finnas möjlighet till användning av hemliga tvångsmedel vid misstanke om olovligt röjande av företagshemlighet, om det finns anledning att anta att den brottsliga verksamheten utövats på uppdrag av eller understötts av främmande makt eller av någon som agerat för främmande makts räkning. Det ska även under vissa omständigheter finnas möjlighet till hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning. Det ska vidare finnas möjlighet att vidta åtgärder enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott samt inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet i fråga om brottstypen olovligt röjande av företagshemlighet, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understöds av främmande makt eller av någon som agerar för främmande makts räkning.

Lagändringarna föreslås träda i kraft den 1 juli 2022.

1 Promemorians lagförslag

1.1 Förslag till lag om ändring i lagen (2018:558) om företagshemligheter

Härigenom föreskrivs i fråga om lagen (2018:558) om företagshemligheter

dels att 5, 22, 26 och 27 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 26 a, 26 b och 27 a §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 §	
Den som gör sig skyldig till brott enligt 26 eller 27 § ska ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten utnyttjas eller röjs.	Den som gör sig skyldig till brott enligt 26, *26 a* eller 27 § ska ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten *annars* utnyttjas eller röjs.
22 §	
En talan enligt 12–15, 17 och 18 §§ förs av innehavaren av företagshemligheten.	
En talan enligt 12–15, 17 och 18 §§ får föras även i samband med åtal för brott som avses i 26 och 27 §§.	En talan enligt 12–15, 17 och 18 §§ får föras även i samband med åtal för brott som avses i 26, *26 a* och 27 §§.

26 §

Den som uppsåtligen och olovligen bereder sig tillgång till en företagshemlighet ska dömas för *företagsspionerи* till böter eller fängelse i högst två år, *eller, om brottet är grovt, till fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.*	Den som uppsåtligen och olovligen bereder sig tillgång till en företagshemlighet ska dömas för *företagsspionerи* till böter eller fängelse i högst två år. *Om brottet är grovt döms till fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.*
För försök eller förberedelse till företagsspionerи ska det dömas till ansvar enligt 23 kap. brottsbalken. *Det ska inte dömas till ansvar enligt denna paragraf om gärningen är belagd med strängare straff i brottsbalken.*	
	26 a § *Den som uppsåtligen och olovligen utnyttjar en företagshemlighet av teknisk natur som han eller hon har fått del av i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution, eller genom att delta i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund, ska dömas för olovligt utnyttjande av företagshemlighet till böter eller fängelse i högst två år.* *Den som uppsåtligen och olovligen röjer en företagshemlighet av*

	teknisk natur som han eller hon har fått del av på ett sätt som anges i första stycket ska dömas för olovligt röjande av företagshemlighet till böter eller fängelse i högst två år.
	Om ett brott enligt första eller andra stycket är grovt döms till fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.
	I ringa fall ska det inte dömas till ansvar enligt denna paragraf. Det ska inte heller dömas till ansvar om gärningen begås efter att deltagandet i rörelsen eller verksamheten har upphört och det inte finns synnerliga skäl för ansvar.
	26 b §
	För försök eller förberedelse till företagsspionerі, olovligt utnyttjande av företagshemlighet eller olovligt röjande av företagshemlighet ska det dömas till ansvar enligt 23 kap. brottsbalken.
	27 §
Den som uppsåtligen anskaffar en företagshemlighet med vetskap om att den som tillhandahåller hemligheten eller någon före honom eller henne i sin tur har berett sig tillgång till denna genom en gärning som avses i 26 §, ska dömas för *olovlig befatt-*	Den som uppsåtligen anskaffar en företagshemlighet med vetskap om att den som tillhandahåller hemligheten eller någon före honom eller henne i sin tur har berett sig tillgång till denna genom en gärning som avses i 26 §, ska dömas för *olovlig befatt-*

ning med företagshemlighet till böter eller fängelse i högst två år eller, om brottet är grovt, till fängelse i högst fyra år.	*ning med företagshemlighet* till böter eller fängelse i högst två år eller, om brottet är grovt, till fängelse i högst fyra år. *Detsamma gäller den som uppsåtligen anskaffar en företagshemlighet av teknisk natur med vetskap om att hemligheten tillhandahålls, eller tidigare har tillhandahållits, genom ett sådant röjande som avses i 26 a § andra stycket, och röjandet inte är fritt från ansvar enligt fjärde stycket i samma paragraf.*
Det ska inte dömas till ansvar enligt denna paragraf om gärningen är belagd med strängare straff i brottsbalken.	*27 a §* *Det ska inte dömas till ansvar enligt 26, 26 a, 26 b eller 27 § om gärningen är belagd med strängare straff i brottsbalken.*

Denna lag träder i kraft den 1 juli 2022.

1.2 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 27 kap. 2, 20 d och 33 §§ rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
27 kap.	
2 §[1]	
En skriftlig handling får inte tas i beslag om	
1. den kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § inte får höras som vittne om, och	
2. handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för.	
Ett skriftligt meddelande mellan den misstänkte och en närstående som avses i 36 kap. 3 §, eller mellan sådana närstående inbördes, får tas i beslag hos den misstänkte eller en närstående endast vid en förundersökning om	
1. ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,	
2. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,	
3. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,	
4. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,	
5. högförräderi, krigsanstiftan, spionering, grovt spionering, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 7, 8, 10, 10 a eller 10 b § brottsbalken,	
6. företagsspionering enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har	6. företagsspionering *eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om före-

[1] Senaste lydelse 2018:559.

begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,	tagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,

7. terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, brott enligt 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

8. försök, förberedelse eller stämpling till brott som avses i 2–7, om en sådan gärning är belagd med straff.

Ett beslut enligt andra stycket 2–8 får meddelas endast av rätten eller åklagaren.

Om åklagaren har beslutat om beslag enligt tredje stycket, ska han eller hon utan dröjsmål anmäla åtgärden hos rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

20 d §[2]

Med hemlig rumsavlyssning avses avlyssning eller upptagning som

1. görs i hemlighet och med ett tekniskt hjälpmedel som är avsett att återge ljud, och

2. avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Hemlig rumsavlyssning får användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år,

2. spioneri enligt 19 kap. 5 § brottsbalken,

3. brott som avses i 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på	3. *företagsspioneri eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företags-

[2] Senaste lydelse 2020:174.

uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning och det kan antas att brottet inte leder till endast böter,	hemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning och det kan antas att brottet inte leder till endast böter,

4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i fyra år och det är fråga om

a) människohandel enligt 4 kap. 1 a § brottsbalken,

b) grov människoexploatering enligt 4 kap. 1 b § tredje stycket brottsbalken,

c) våldtäkt enligt 6 kap. 1 § första stycket brottsbalken,

d) grovt sexuellt övergrepp enligt 6 kap. 2 § andra stycket brottsbalken,

e) våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken,

f) grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken,

g) grovt utnyttjande av barn för sexuell posering enligt 6 kap. 8 § tredje stycket brottsbalken,

h) grovt koppleri enligt 6 kap. 12 § tredje stycket brottsbalken,

i) grov utpressning enligt 9 kap. 4 § andra stycket brottsbalken,

j) grovt barnpornografibrott enligt 16 kap. 10 a § sjätte stycket brottsbalken,

k) grovt övergrepp i rättssak enligt 17 kap. 10 § tredje stycket brottsbalken,

l) grovt narkotikabrott enligt 3 § narkotikastrafflagen (1968:64), eller

m) grov narkotikasmuggling enligt 6 § tredje stycket lagen (2000:1225) om straff för smuggling,

5. försök, förberedelse eller stämpling till brott som avses i 1–3, om en sådan gärning är belagd med straff,

6. försök, förberedelse eller stämpling till brott som avses i 4, om en sådan gärning är belagd med straff och det med hänsyn till omständigheterna kan antas att gärningens straffvärde överstiger fängelse i fyra år.

33 §[3]

Om det gäller sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) för uppgifter som avses i 32 §, ska en underrättelse enligt 31 § skjutas upp till dess att sekretess inte längre gäller.

Om det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades, behöver underrättelsen inte lämnas.

En underrättelse enligt 31 § ska inte lämnas, om förundersökningen angår

1. brott som avses i 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,

2. brott som avses i 13 kap. 4 eller 5 § brottsbalken,

3. brott som avses i 18 kap. 1, 3, 5 eller 6 § eller 19 kap. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 10 a, 10 b, 12 eller 13 § brottsbalken,

4. brott som avses i 3 eller 4 kap. brottsbalken, om brottet är av det slag som anges i 18 kap. 2 § eller 19 kap. 11 § samma balk,

5. brott som avses i 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,	5. brott som avses i 26 § *eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,

6. brott som avses i 2 § lagen (2003:148) om straff för terroristbrott, 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

7. försök, förberedelse eller stämpling till brott som anges i 1–6 eller underlåtenhet att avslöja sådant brott, om gärningen är belagd med straff.

Denna lag träder i kraft den 1 juli 2022.

[3] Senaste lydelse 2018:559.

1.3 Förslag till lag om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott

Härigenom föreskrivs att 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
Tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första och andra styckena rättegångsbalken eller hemlig kameraövervakning enligt 27 kap. 20 a § första stycket rättegångsbalken får meddelas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar	
1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,	
2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,	
3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,	
4. högförräderi, krigsanstiftan, spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6 eller 8 § eller 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,	
5. företagsspionerі enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten kommer att utövas på uppdrag av eller understödjas av en främmande makt	5. företagsspionerі *eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten kommer att

[1] Senaste lydelse 2018:560.

eller av någon som kommer att agera för en främmande makts räkning,	utövas på uppdrag av eller understödjas av en främmande makt eller av någon som kommer att agera för en främmande makts räkning,

6. terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

7. mord, dråp, grov misshandel, synnerligen grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1, 2 eller 6 § eller 4 kap. 1 § eller 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Tillstånd enligt första stycket får också meddelas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet som avses i första stycket och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Denna lag träder i kraft den 1 juli 2022.

1.4 Förslag till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs att 2 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §[1]	
Uppgifter får hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar	
1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,	
2. sabotage enligt 13 kap. 4 § brottsbalken,	
3. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,	
4. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,	
5. spioneri, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,	
6. företagsspioneri enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understöds av en främmande makt eller av någon som agerar för en främmande makts räkning,	6. företagsspioneri *eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understöds av en främmande makt eller av

[1] Senaste lydelse 2019:499.

någon som agerar för en främmande makts räkning,

7. grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet,

8. grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Uppgifter får bara hämtas in om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Denna lag träder i kraft den 1 juli 2022.

2 Inledning

2.1 Skyddet av företagshemligheter är ett samhällsintresse

Immateriella tillgångar får allt större betydelse

Sverige är en innovativ och kreativ kunskapsnation med tekniska produkter, tjänster och lösningar i världsklass. Enligt FN-organisationen World Intellectual Property Organization finns det bara en nation som är mer innovativ i världen (Global Innovation Index 2020). Hela 55 procent av företagen i Sverige bedriver innovationsverksamhet. Särskilt innovativa är informationstjänsteföretagen, där 85 procent bedriver innovationsverksamhet. Andra exempel på särskilt innovativa branscher är industri för datorer, elektronikvaror och optik samt forsknings- och utvecklingsinstitutioner (Statistiska centralbyråns undersökning om innovationsverksamhet i svenska företag med 10 eller fler anställda under åren 2016–2018).

För svenska företag är ett fungerande skydd för företagshemligheter och andra immateriella tillgångar en förutsättning för att de ska ha möjlighet att få täckning för sina investeringar och kunna skapa nya verk, uppfinningar, produkter och tjänster. Det är också av stor betydelse för innovationskraften i svenska forskningsmiljöer, på t.ex. universitet. Ett fungerande skydd krävs också för att företag ska kunna fortsätta att bidra till vår samhällsekonomi och välfärd. Exempelvis genererar de immaterialrättsintensiva företagen mer än vart tredje arbetstillfälle i Sverige och mer än 40 procent av vår bruttonationalprodukt (European Union Intellectual Property Office, IPR-intensive industries and economic performance in the European Union, 2019).

För att Sverige även i fortsättningen ska vara en kunskapsekonomi i framkant är det av största betydelse att företagens konkurrenskraft säkerställs och att förutsättningarna för innovation

och kunskapsöverföring är goda. Innovationer, produkter och lösningar måste tillvaratas och skyddas effektivt för att arbetstillfällen ska skapas även i fortsättningen, trots att Sverige möter nya och mer komplexa utmaningar och hot såsom bl.a. digitala strukturella sårbarheter, som rör hur den digitala teknikutvecklingen organiseras, och industrispionage.

Regeringen har vidtagit ett flertal åtgärder i syfte att trygga Sveriges ställning som innovationsland. Ett exempel är att straffskalorna för de allvarligaste fallen av immaterialrättsrättsintrång och varumärkesintrång skärpts genom att särskilda straffskalor för uppsåtliga grova brott införts i samtliga immaterialrättsliga lagar (prop. 2019/20:149). Ändringarna trädde i kraft den 1 september 2020. För att skydda Sveriges säkerhet vid överlåtelser av säkerhetskänslig verksamhet föreslås även nya krav för den som planerar att överlåta hela eller någon del av en säkerhetskänslig verksamhet och viss egendom. Verksamhetsutövaren ska bl.a. vara skyldig att inför överlåtelsen samråda med en samrådsmyndighet, som ytterst kan besluta att en överlåtelse inte får genomföras (se prop. 2020/21:13). Lagändringen föreslås träda i kraft den 1 januari 2021. Ett annat exempel är den nya lagen om tystnadsplikt för privata tjänsteleverantörer som innebär att uppgifter från en myndighet som hanteras av en tjänsteleverantör ska få ett sekretesskydd som är likvärdigt med det som gäller när en annan myndighet tillhandahåller en motsvarande tjänst. Lagen föreslås träda i kraft den 1 januari 2021.

Under åren 2016–2019 har PRV och Vinnova haft i uppdrag att bl.a. höja kunskapen om immateriella tillgångar och dess värde både hos företag, allmänhet och akademi, för att skapa ännu bättre förutsättningar för svenska företag och svensk ekonomi. PRV ska nu ta det kunskapshöjande arbetet vidare inom ramen för sin ordinarie verksamhet (vilket förtydligats i myndighetens instruktion och regleringsbrev). Regeringen har vidare fortsatt arbetet i Nationella innovationsrådet, som har en rådgivande funktion och tillför nya perspektiv på frågor av betydelse för innovationspolitikens hela område, både på kort och på lång sikt. Dessutom har Sverige en framträdande roll i genomförandet av ett enhetligt patentsystem i EU. Regeringen har även tillsatt utredningar för att möta kommande behov, t.ex. ska en kommitté utveckla en

samordnad och accelererad policyutveckling kopplad till den fjärde industriella revolutionens teknologier (dir. 2018:85).

Förslagen i denna promemoria är ytterligare en del i arbetet för att stärka Sverige som innovationsland.

Sverige har under lång tid skyddat företagshemligheter

En hörnsten i skyddet för företags immateriella tillgångar, och i förlängningen företagens konkurrenskraft, är ett starkt skydd för företagshemligheter. Företagen är beroende inte bara av ensamrätter till produkter och produktionsmetoder utan också av skydd mot att det samlade kunnandet inom företaget om bl.a. produktionen, branschförhållanden, affärsförbindelser och marknadsföring utnyttjas av andra på ett otillbörligt sätt. Den immaterialrättsliga lagstiftningen skyddar i allmänhet inte detta kunnande. Från företagens synpunkt framstår ett skydd för företagshemligheter ofta som minst lika angeläget som skyddet för materiella tillgångar och immateriella rättigheter. Det är därför naturligt att det enskilda företaget betraktar sitt unika och strategiska kunnande som en värdefull tillgång som det gäller att slå vakt om (prop. 2017/18:200 s. 19). Skyddet för företagshemligheter fungerar vidare inte bara som ett komplement till de immaterialrättsliga skydden, utan kan också i enskilda företag vara ett alternativ till sådant skydd. Företaget söker då inte någon ensamrätt för t.ex. en uppfinning utan förlitar sig helt på skyddet för företagshemligheter.

Sverige har under lång tid sökt skydda företagens konkurrensförmåga genom lagstiftning till skydd för företagshemligheter. Redan 1919 infördes bestämmelser som syftade till att motverka illojal konkurrens och skydda yrkeshemligheter. Regelverket överfördes sedan till lagen (1931:152) med vissa bestämmelser mot illojal konkurrens. En första lag om skydd för företagshemligheter ersatte i början av 1990-talet den tidigare lagstiftningen. Lagen (1990:409) om skydd för företagshemligheter utgjorde ett nära nog unikt helhetsgrepp i ett europeiskt perspektiv. Den lagen innehöll regler om straff, skadestånd, vitesförbud och andra skyddsåtgärder till motverkande av angrepp på företagshemligheter.

2.2 Det straffrättsliga skyddet för företagshemligheter ska ses över

Skyddet för företagshemligheter stärktes i den nya lagen om företagshemligheter…

Lagen (2018:558) om företagshemligheter ersatte den 1 juli 2018 den äldre lagen om skydd för företagshemligheter. Den nya lagen kom till som ett led i genomförandet av ett direktiv med EU-gemensamma regler om skydd för företagshemligheter (Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation [företagshemligheter] olagligen anskaffas, utnyttjas och röjs). Direktivet är ett s.k. minimidirektiv. Medlemsstaterna får alltså föreskriva ett mer långtgående skydd mot att företagshemligheter olagligen anskaffas, utnyttjas eller röjs än vad som gäller enligt direktivet, dock under uppfyllande av de unionsrättsliga bestämmelserna i EUF-fördraget och artikel 1.1 i direktivet.

I flera avseenden ger den nya lagen ett bättre skydd för företagshemligheter än den äldre lagen. Bland annat omfattar den nya lagen fler former av olovligt anskaffande av företagshemligheter. Den nya lagen ger även större utrymme att ingripa med civilrättsliga åtgärder, som förbud och andra skyddsåtgärder, mot den som angriper en företagshemlighet. Lagen medför sammantaget att utökade möjligheter står till buds för den innehavare som vill skydda sina företagshemligheter mot angrepp.

… men frågan om ett bättre straffrättsligt skydd återstår att behandla

Under en längre tid har det ifrågasatts om det straffrättsliga skyddet för företagshemligheter är tillräckligt starkt (se nedan avsnitt 4).

I det betänkande som låg till grund för den nya lagen om företagshemligheter lämnades ett förslag på ett nytt straffansvar för bl.a. anställda som missbrukar företagshemligheter.

Regeringen uttalade i propositionen till den nya lagen att möjligheterna till straffrättsliga ingripanden mot angrepp på företagshemligheter av personer inom företagets egen verksamhet är otillräckliga. Samtidigt betonades vikten av att en utvidgad kriminalisering på området sker återhållsamt. Slutsatsen var att straffansvaret

bör omfatta endast mer kvalificerade fall av utnyttjande och röjande. Något underlag för en sådan mer begränsad utvidgning av straffansvaret fanns inte. Regeringen förklarade därför att den hade för avsikt att efter sedvanlig beredning återkomma till riksdagen i frågan om hur ett straffansvar för mer kvalificerade fall kan utformas (prop. 2017/18:200 s. 122 f.).

I denna promemoria behandlas förutsättningarna för att införa ett förstärkt straffrättsligt skydd för företagshemligheter mot angrepp från personer inom ett företags rörelse eller en forskningsinstitutions verksamhet.

Det har även tidigare gjorts försök att införa ett utvidgat straffansvar för personer som får del av företagshemligheter genom att delta i en näringsidkares verksamhet. Frågan har sedan 2007 utretts två gånger och en lagrådsremiss med förslag på en ny straffbestämmelse beslutades 2013.

De förslag som har lämnats har mött invändningar av olika slag (se närmare avsnitt 4). En kritik som har återkommit är att de lämnade förslagen har varit för långtgående. Flera remissinstanser har kritiserat förslagen på den grunden att de har föreskrivit ett straffansvar för handlingar som enligt remissinstansernas mening inte kan anses straffvärda. Samtidigt har det riktats invändningar mot hur begränsningar i de föreslagna straffbestämmelsernas räckvidd har utformats.

En central fråga i promemorian är därför – utöver om det finns tillräckliga skäl för att införa ett straffansvar – hur ett straffansvar bör avgränsas så att det endast träffar sådana kvalificerade fall som bedöms vara straffvärda.

3 Skyddet för företagshemligheter i dag

3.1 Lagen om företagshemligheter balanserar flera viktiga intressen

Lagen om företagshemligheter slår vakt om flera viktiga samhällsintressen. Lagen skyddar företagens rättigheter och möjligheter till utveckling. Den skyddar också samhällsekonomin genom att skapa goda förutsättningar för företagen att skapa arbetstillfällen och bidra med skatteintäkter till staten. Mot dessa skyddsintressen vägs arbetstagarnas rättigheter och möjligheter till visselblåsning, liksom det fria informationsutbytet och yttrandefriheten. Lagens tillämpning aktualiserar bl.a. frågor om vissa grundläggande fri- och rättigheter enligt regeringsformen samt frågor kring tryckfrihetsförordningen, yttrandefrihetsgrundlagen, de arbetsrättsliga lagarna och de immaterialrättsliga lagarna.

Lagen om företagshemligheter ligger alltså i skärningspunkten mellan flera viktiga samhällsintressen och ger uttryck för en noggrant avvägd balans mellan dessa olika intressen.

3.2 Innehållet i lagen om företagshemligheter

Lagen om företagshemligheter innehåller regler om skadestånd, vitesförbud, straff och andra åtgärder vid obehöriga angrepp mot företagshemligheter.

Ett uttryck för den intresseavvägning som har gjorts finns i själva definitionen av vad som utgör en företagshemlighet (2 §).

Företagshemligheter definieras som information om affärs- eller driftförhållanden i en näringsidkares rörelse eller i en forskningsinstitutions verksamhet, som varken som helhet eller i den form dess

beståndsdelar ordnats och satts samman är allmänt känd hos eller lättillgänglig för den som normalt har tillgång till information av det aktuella slaget. För att informationen ska omfattas av lagens skydd krävs att innehavaren, dvs. den som lagligen kontrollerar företagshemligheten, oftast ett företag, har vidtagit rimliga åtgärder för att hemlighålla informationen. Därutöver förutsätts att ett röjande av informationen är ägnat att medföra skada i konkurrenshänseende för innehavaren. Erfarenheter och färdigheter som en arbetstagare har fått vid normal yrkesutövning är inte en företagshemlighet. Inte heller är information om något som utgör ett brott eller ett annat allvarligt missförhållande en företagshemlighet (2 §).

Med angrepp på en företagshemlighet avses att någon utan innehavarens samtycke bereder sig tillgång till, tillägnar sig eller på något annat sätt anskaffar företagshemligheten eller utnyttjar eller röjer företagshemligheten (3 §).

Lagen gäller endast obehöriga angrepp på företagshemligheter (4 §). I kravet på obehörighet ligger att skyddet för företagshemligheter ska vägas mot andra intressen (prop. 2017/18:200 s. 146). I lagen anges att ett angrepp på en företagshemlighet aldrig är obehörigt då det sker för att offentliggöra eller inför en myndighet eller ett annat behörigt organ avslöja något som skäligen kan misstänkas utgöra brott med fängelse i straffskalan, eller kan anses utgöra något annat missförhållande och offentliggörandet eller avslöjandet sker till skydd för allmänintresset. Det har även kommit att utvecklas en princip med innebörd att en arbetstagares utnyttjande eller röjande av en tidigare arbetsgivares företagshemligheter inte anses som ett obehörigt angrepp så länge det inte finns synnerliga skäl (jfr 7 § andra stycket samt prop. 2017/18:200 s. 62 f. och 147).

Lagen innehåller ett flertal bestämmelser om skadestånd.

Den som gör sig skyldig till brott enligt lagen ska ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten utnyttjas eller röjs (5 §). Detta innebär att gärningsmannens skadeståndsansvar för utnyttjande och röjande av företagshemligheten inte bara avser hans eller hennes eget brottsliga handlande, utan bl.a. även ett utnyttjande eller röjande av den angripna företagshemligheten som utförs av någon annan.

Den som uppsåtligen eller av oaktsamhet angriper en företagshemlighet hos en näringsidkare eller en forskningsinstitution som

han eller hon i förtroende har fått del av i samband med en affärsförbindelse med näringsidkaren eller forskningsinstitutionen, ska ersätta den skada som uppkommer genom förfarandet (6 §).

Vidare ska en arbetstagare som uppsåtligen eller av oaktsamhet angriper en företagshemlighet hos arbetsgivaren, som han eller hon fått del av i sin anställning under sådana förhållanden att han eller hon insåg eller borde ha insett att den inte fick avslöjas, ersätta den skada som uppkommer genom förfarandet. Om ett utnyttjande eller röjande har ägt rum sedan anställningen upphört gäller ansvaret endast om det finns synnerliga skäl (7 §).

Det finns även ett skadeståndsansvar för parter, partsrepresentanter och andra som under vissa omständigheter får del av företagshemligheter i samband med en rättegång (8 §).

Också den som uppsåtligen eller av oaktsamhet angriper en företagshemlighet som, enligt vad han eller hon inser eller bör inse, i ett tidigare led har angripits av någon annan, ska ersätta den skada som uppkommer genom förfarandet (9 §).

Därutöver föreskrivs ett skadeståndsansvar för den som uppsåtligen eller av oaktsamhet annars anskaffar en företagshemlighet. Han eller hon ska ersätta den skada som uppkommer genom förfarandet eller genom att han eller hon därefter uppsåtligen eller av oaktsamhet utnyttjar eller röjer företagshemligheten. Från detta skadeståndsansvar undantas dock vissa kategorier av uppdragstagare (10 §).

Vid sidan om skadeståndsansvaret finns bestämmelser om vitesförbud och andra åtgärder till skydd för företagshemligheter.

Vitesförbud får beslutas vid angrepp eller nära förestående angrepp på företagshemligheter (12–15 §§). Rätten får vid vite förbjuda den som har angripit en företagshemlighet att fortsätta med angreppet på företagshemligheten. Rätten får också, vid vite, förbjuda den som har angripit en företagshemlighet och därigenom orsakat att informationen inte längre är företagshemlig att för viss tid utnyttja informationen. Vitesförbud får även beslutas interimistiskt. En talan om förbud förs av innehavaren av företagshemligheten och får även föras i samband med åtal för brott enligt lagen (22 §).

På ansökan av en innehavare av en företagshemlighet kan en domstol besluta om ett antal olika skyddsåtgärder (17 och18 §§).

Om någon har angripit en företagshemlighet, eller har handlat på ett sätt som medför att ett angrepp är nära förestående, får rätten

efter vad som är skäligt besluta att en handling eller ett föremål som den som har utfört angreppet har i sin besittning och som innefattar hemligheten, ska överlämnas till innehavaren av företagshemligheten. Rätten får besluta att överlämnandet ska ske mot lösen, om det finns skäl för det. Om handlingen eller föremålet inte kan överlämnas utan olägenhet, får rätten efter vad som är skäligt besluta att handlingen eller föremålet ska återkallas från marknaden, förstöras, ändras eller utsättas för någon annan åtgärd som är ägnad att förebygga missbruk. Ett sådant beslut får fattas även om handlingen eller föremålet inte finns i angriparens besittning. Ett beslut ska inte meddelas om ett förverkande eller någon annan åtgärd som är ägnad att förebygga missbruk ska beslutas enligt 36 kap. brottsbalken (20 §).

Lagen ger utrymme för rätten att i vissa fall besluta att en angripare av en företagshemlighet mot skälig ersättning till innehavaren ska få fortsätta att utnyttja företagshemligheten (21 §).

På yrkande av en innehavare av en företagshemlighet får rätten under vissa omständigheter besluta att den som har angripit företagshemligheten ska bekosta lämpliga åtgärder för att sprida information om domen i målet (25 §). Ett sådant beslut kan även avse den som vidtagit åtgärder som innebär att ett angrepp på en företagshemlighet är nära förestående.

Vid sidan av dessa bestämmelser finns det i lagen ett straffansvar vid vissa former av angrepp på företagshemligheter (26 och 27 §§). Dessa bestämmelser redovisas mer ingående i nästa avsnitt.

Det kan tilläggas att det vid lagens tillämpning finns bakomliggande principer att beakta. En sådan är att lagen inte ska tillämpas för det fall den kommer i konflikt med grundläggande rättigheter och friheter enligt grundlagarna.

3.3 Det straffrättsliga skyddet för företagshemligheter

För att straffansvar ska aktualiseras krävs till en början att det är fråga om en företagshemlighet (2 §) som utsätts för ett angrepp (3 §) som är obehörigt (4 §).

Straffansvar för företagsspionerі kan komma i fråga när någon olovligen bereder sig tillgång till en företagshemlighet (26 §).

Gärningsmannen kan bereda sig tillgång till företagshemligheten på olika sätt. I uttrycket ligger att gärningsmannen utövar en aktivitet. Det förutsätts att det är fråga om information som gärningsmannen inte redan har tillgång till. Den som har lovlig tillgång till den företagshemliga informationen kan inte anses göra sig skyldig till företagsspionerі genom att kopiera informationen. Den som av en slump kommer över en företagshemlighet har inte heller berett sig tillgång till den (prop. 2017/18:200 s. 120 med hänvisningar).

I fråga om anställda är det straffbart när en anställd olovligen bereder sig tillgång till information som ligger klart utanför ramen för hans eller hennes arbetsuppgifter. Däremot omfattas inte fall där en anställd får del av överskottsinformation som finns tillgänglig på den del av arbetsplatsen där han eller hon normalt har rätt att uppehålla sig eller som finns i material som han eller hon använder i tjänsten (prop. 2017/18:200 s. 120).

Straffet för företagsspionerі är böter eller fängelse i högst två år. För de allvarligaste fallen av företagsspionerі föreskrivs ansvar för grovt brott med en straffskala om fängelse i lägst sex månader och högst sex år. Även försök och förberedelse till företagsspionerі är straffbart.

Straffansvaret för olovlig befattning med företagshemlighet omfattar den som anskaffar en hemlighet med vetskap om att den som tillhandahåller hemligheten, eller någon före honom eller henne, i sin tur har berett sig tillgång till den genom en gärning som avses i bestämmelsen om företagsspionerі (27 §). Liksom när det gäller företagsspionerі är det själva anskaffandet som är straffbart. Med anskaffande avses varje slags förvärv av uppgiften, men i överensstämmelse med vad som gäller beträffande företagsspionerі kan den som av en tillfällighet eller utan att själv ha bett om det får reda på den hemliga informationen inte straffas (prop. 1987/88:155 s. 40). Från det straffbara området utesluts de fall då gärningsmannen anskaffar en företagshemlighet genom att tillägna sig den. I dessa fall kan gärningsmannen nämligen vid anskaffandet inte sägas ha tillhandahållits företagshemligheten på ett sådant sätt som krävs för straffansvar (prop. 2017/18:200 s. 178).

En förutsättning för straffansvar för företagsspionerі eller olovlig befattning med företagshemlighet är att angreppet inte omfattas av regleringen i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Om anskaffandet av en företagshemlighet sker i syfte att

offentliggöra den i ett grundlagsskyddat medium gäller grundlagsskyddet och angreppet kan inte bestraffas enligt lagen om företagshemligheter (jfr prop. 2017/18:200 s. 177 f. med hänvisningar).

4 Tidigare överväganden om straffansvar vid angrepp på företagshemligheter

4.1 1990 års lag innebar en avkriminalisering av vissa handlingar

Skyddet för företagshemligheter har förändrats i takt med att samhällsekonomin och synen på företag har förändrats. Den första regleringen av något som liknar företagshemligheter infördes i lagen den 19 juni 1919 (nr 442) med vissa bestämmelser mot illojal konkurrens m.m. I och med lagen infördes bl.a. straff för obehörigt användande eller yppande av yrkeshemligheter. Yrkeshemlighet definierades inte i lagen, men innefattade information om bl.a. fabrikationssätt, anordning och affärsförhållande. Yrkeshemligheter kunde materialiseras i tekniska förebilder, t.ex. ritningar.

Regleringen överfördes till lagen (1931:152) med vissa bestämmelser mot illojal konkurrens (nedan 1931 års lag). I lagen föreskrevs såväl straffansvar som skadeståndsansvar för anställda som under vissa omständigheter bl.a. obehörigen använde sig av eller yppade arbetsgivarens yrkeshemlighet. Anställdas straff- och skadeståndsansvar för olovlig hantering av yrkeshemligheter upphörde i och med anställningens avslutande. Lagen innehöll inte någon straffregel motsvarande företagsspionerі.

Lagen (1990:409) om skydd för företagshemligheter medförde ett ändrat fokus i fråga om kriminalisering av missbruk av företagshemligheter. Kriminaliseringen kom då att inriktas mot att någon olovligen bereder sig tillgång till en företagshemlighet. Det straffansvar som funnits i 1931 års lag för arbetstagares missbruk av sådana företagshemligheter som de fått del av inom ramen för anställningen avskaffades. I stället kom kriminaliseringen att avse

endast företagsspionerі och olovlig befattning med en företagshemlighet.

Som skäl för avkriminaliseringen av arbetstagares angrepp på företagshemligheter anfördes att straffansvar för brott mot avtalsförpliktelser enligt lång tradition i svensk rätt bör undvikas när det finns andra effektiva sanktioner för att upprätthålla respekten för ingångna avtal. Skadestånd ensamt eller i kombination med andra arbetsrättsliga reaktioner bedömdes normalt vara tillräckliga sanktioner. För arbetstagare som t.ex. röjde företagshemligheter som de lovligen fått del av under sin anställning kunde därför inte ansvar för brott komma i fråga, men väl ett skadeståndsansvar (jfr prop. 1987/88:155 s. 17 f.).

4.2 Ett utsträckt straffansvar föreslogs av 2007 års utredning om skyddet för företagshemligheter

Det s.k. Ericsson-målet (Svea hovrätts dom den 20 oktober 2003 i mål nr B 5221-03) gav upphov till en diskussion om huruvida lagen om skydd för företagshemligheter verkligen ger ett tillräckligt skydd mot att en arbetstagare olovligen utnyttjar eller röjer en företagshemlighet som han eller hon tagit del av inom ramen för anställningen.

I målet var det bl.a. fråga om en anställd vid telekomföretaget Ericsson som hade lämnat ut företagshemliga och säkerhetsklassade dokument till en utomstående person. Den person som dokumenten lämnades ut till, och som i sin tur vidarebefordrade dem till en utländsk underrättelseofficer, dömdes för grovt spionerі till åtta års fängelse. Åtalet mot den anställde ogillades däremot. Eftersom de dokument som han lämnat ut var arbetsmaterial som han hade lovlig tillgång till hade han inte olovligen berett sig tillgång till informationen. Han dömdes därför inte för företagsspionerі.

Med anledning av framför allt domen i Ericsson-målet uttalade riksdagen under våren 2005 att regeringen borde ta initiativ till en översyn av lagen (bet. 2004/05:LU12 och rskr. 2004/05:179).

Den dåvarande regeringen tillsatte en utredning, som hade i uppdrag att överväga om lagens straffstadganden hade getts en ändamålsenlig utformning (dir. 2007:54).

Utredningen bedömde att det fanns ett behov av att utvidga straffansvaret till att även omfatta olovligt röjande och olovligt utnyttjande av företagshemlighet. Utredningens lagförslag avgränsades till personer som fått del av en företagshemlighet med anledning av att de deltagit i näringsidkarens verksamhet som anställda. Avsikten var att även andra med lovlig tillgång till företagshemligheter, såsom anställda i bemannings- och konsultföretag, s.k. ensamkonsulter, styrelseledamöter och revisorer skulle omfattas. Om företagshemligheten hade utnyttjats eller röjts efter att deltagandet i verksamheten upphört, skulle ansvar enligt förslaget dömas ut endast om gärningsmannen agerat särskilt illojalt eller om gärningen var att bedöma som grovt brott. Det skulle inte heller dömas till ansvar om gärningen begåtts senare än två år efter det att deltagandet i näringsidkarens rörelse upphörde eller om gärningen var ringa (SOU 2008:63 s. 175 f.).

4.3 Ett förslag om utsträckt straffansvar i 2013 års lagrådsremiss

Ett förslag som utgick från 2007 års betänkande

I december 2013 beslutade den dåvarande regeringen lagrådsremissen Ett bättre skydd för företagshemligheter. I remissen fanns förslag på ett förstärkt straffrättsligt skydd för företagshemligheter som i mycket utgick från 2007 års betänkande.

Enligt förslaget i lagrådsremissen skulle en ny brottstyp införas som avsåg olovligt utnyttjande eller röjande av företagshemlighet för den som haft lovlig tillgång till hemligheten genom sitt deltagande i näringsidkarens rörelse till följd av anställning eller uppdrag eller på annan liknande grund. I ringa fall skulle det inte dömas till ansvar enligt förslaget, vilket innebar en begränsning av det straffbara området. Det skulle heller inte dömas till ansvar om gärningen hade begåtts senare än två år efter det att deltagandet i näringsidkarens rörelse upphörde.

Det utvidgade straffansvaret skulle enligt den dåvarande regeringen i första hand träffa näringsidkarens egna anställda men även andra som har en motsvarande eller nästintill motsvarande

insyn i företaget, t.ex. vissa uppdragstagare eller personer som genom uthyrning eller utlåning från bemanningsföretag utför arbete åt näringsidkaren. Till kretsen kunde också höra personer som medverkar i arbetsmarknadspolitiska program och studerande som genomför en längre praktikperiod eller utbildning förlagd till en arbetsplats. Däremot omfattades inte personer som utför tjänster av skilda slag och som hade en lös koppling till den näringsidkare som anlitat dem. Det förutsattes enligt förslaget att personen deltog i näringsidkarens verksamhet under omständigheter som liknar dem som förekommer i ett anställningsförhållande.

Den dåvarande regeringen uttalade att en arbetstagare i princip kan sägas ha handlat lika klandervärt om han eller hon utnyttjar eller röjer en företagshemlighet direkt efter det att anställningsförhållandet upphört som om det skett något tidigare. Det bedömdes därför inte finnas skäl att begränsa straffansvaret till endast vissa särskilt illojala förfaranden i dessa fall, såsom utredningen hade föreslagit.

Gärningen kunde enligt förslaget vara att anse som ringa, och därmed straffri, om den framstod som ursäktlig eller försvarlig, eller annars inte var straffvärd. Även den uppkomna skadan eller risken för skada borde vara en viktig faktor vid bedömningen. Som exempel på fall som i allmänhet kunde vara att anse som ringa angavs då en anställd berättar om sitt arbete för en nära anhörig och samtidigt i allmänna ordalag lämnar ut hemlig information, eller då en företagshemlighet avslöjas i samband med ett allmänt informationsutbyte mellan branschkollegor vid en konferens.

Som en följd av den förslagna kriminaliseringen av olovligt röjande av företagshemlighet föreslogs ett breddat straffansvar för olovlig befattning med företagshemlighet. Även den som anskaffade en företagshemlighet med vetskap om att någon olovligt röjt den föreslogs således kunna dömas till ansvar.

Det föreslogs även en skärpning i straffskalan för företagsspioneri.

Lagrådets kritik mot förslaget

Enligt Lagrådet (protokoll vid sammanträde den 8 januari 2014) framstod det som rimligt att utvidga det kriminaliserade området till

sådana fall som Ericsson-målet rörde. Den föreslagna straffbestämmelsen bedömdes dock enligt Lagrådet komma att omfatta även situationer där ett straffansvar ter sig diskutabelt. Som exempel angavs att en anställd berättar för en konsument att beskrivningen i marknadsföringen av en tjänst som företaget tillhandahåller är vilseledande på någon viktig punkt, så att undantaget för ringa fall inte blir tillämpligt.

Lagrådet angav vidare att lagen om skydd för företagshemligheter visserligen endast gäller för obehöriga angrepp och att uppgiftslämnande av det angivna slaget många gånger kommer att hamna utanför det straffbara området. Det stod dock enligt Lagrådet klart att bedömningen av vad som är obehörigt kan bli avgörande för avgränsningen och att svåra gränsdragningsproblem kan uppkomma i tillämpningen.

Till detta kom att något behov av att inrymma även mindre allvarliga fall, som inte kunde bedömas som ringa, inte hade redovisats i remissen. Inte heller hade det enligt Lagrådet redovisats någon avvägning av hur nykriminaliseringen i sådana fall förhöll sig till intresset av yttrandefrihet för anställda. Det kunde enligt Lagrådets mening ifrågasättas om remissen innefattade tillräckliga skäl för en så pass omfattande nykriminalisering som förslaget innebar. Regeringen borde enligt Lagrådet överväga om ytterligare någon begränsning av det straffbara området borde ske.

Den dåvarande regeringen lämnade inte något förslag till riksdagen om ett förstärkt straffrättsligt skydd för företagshemligheter.

4.4 Ännu ett förslag om utvidgat straffansvar lämnades 2017

Förslag från 2016 års utredning till utvidgat straffansvar

År 2016 gavs en ny utredning i uppdrag att se över frågor om företagshemligheter (dir. 2016:38). Huvudsakligen skulle utredningen överväga hur det då nyligen beslutade EU-direktivet om skydd för företagshemligheter skulle genomföras i svensk rätt. I uppdraget ingick dock även att överväga hur ett straffansvar som utvidgas till att omfatta också den som obehörigen utnyttjar eller

röjer en företagshemlighet som han eller hon har fått tillgång till inom ramen för sina arbetsuppgifter borde utformas, för att lagen ska uppfylla de krav som Lagrådet ställt med anledning av en sådan utvidgning. Utredningen lämnade sitt betänkande i maj 2017 (SOU 2017:45).

Utredningen föreslog att det skulle införas bestämmelser om straff för olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet, för den som haft lovlig tillgång till den angripna företagshemligheten genom deltagande i en näringsidkares rörelse till följd av anställning eller uppdrag eller på liknande grund. Utredningen lutade sig i flera avseenden mot förslaget i den tidigare lagrådsremissen.

Från straffansvaret undantogs enligt förslaget dels personer som utför tjänster av skilda slag med lös anknytning till näringsidkaren, dels styrelseledamöter och revisorer. När det gäller styrelseledamöter och revisorer uttalade utredningen att dessa personer inte kan sägas utföra arbete under omständigheter som liknar dem som utförs i ett anställningsförhållande (SOU 2017:45 s. 353).

Utredningen bedömde att det saknades behov av att bestraffa mindre allvarliga gärningar. Det föreslogs därför undantag för ”mindre allvarliga” respektive ”försvarliga” gärningar.

Huruvida en gärning är att anse som mindre allvarlig ska enligt förslaget avgöras efter en samlad bedömning av omständigheterna i det enskilda fallet. Vid bedömningen bör det få betydelse hur omfattande näringsidkarens skada är i konkurrenshänseende till följd av det olovliga angreppet, och även beaktansvärd risk för slutlig förlust borde jämställas med skada.

I fråga om vilka angrepp som kan anses försvarliga anförde utredningen att ett angrepp på en företagshemlighet visserligen kan orsaka så pass stor skada att gärningen knappast kan anses som mindre allvarlig men att gärningen ändå, med hänsyn till syftet, kunde anses som försvarlig. Generellt borde det enligt utredningen vara försvarligt att röja information som är företagshemlig, om informationen avslöjar att ett företags marknadsföring är otillbörlig enligt marknadsföringslagen. Som ytterligare exempel på försvarliga angrepp angavs då ett företag marknadsför ett tvättmedel som särskilt effektivt och en anställd avslöjar att tvättmedlet har samma sammansättning som ett i handeln betydligt billigare tvättmedel. Agerandet är enligt förslaget att anse som försvarligt eftersom

konsumenter har ett berättigat intresse av att inte utsättas för en missvisande marknadsföring. Samtidigt uttalades att förfarandet – beroende på omständigheterna – skulle kunna vara skadeståndsgrundande. Ett annat exempel på ett försvarligt röjande var då ett företag, för att få en bättre förhandlingsposition i förhandling med ett annat bolag, ljuger om resultatet av en marknadsundersökning och en anställd i företaget avslöjar det riktiga resultatet av undersökningen för det andra bolaget (SOU 2017:45 s. 356 f).

Utredningen föreslog att samma förutsättningar för straffansvar borde gälla oavsett om gärningen begås under eller efter anställningen och att straffansvaret inte borde omfatta olovligt utnyttjande eller röjande av företagshemlighet som sker senare än två år efter att deltagandet i näringsidkarens rörelse upphört.

Straffet för de nya brotten föreslogs vara böter eller fängelse i högst två år eller, i grova fall, fängelse i lägst sex månader och högst sex år.

I likhet med förslaget i 2013 års lagrådsremiss föreslogs att den som anskaffar en företagshemlighet från den som gör sig skyldig till olovligt röjande eller utnyttjande av företagshemlighet skulle kunna dömas för olovlig befattning med företagshemlighet.

Remissbehandlingen av förslaget om utvidgat straffansvar

Remissutfallet för den föreslagna utvidgningen av straffansvaret var blandat. Många remissinstanser som bl.a. Säkerhetspolisen (Säpo), Företagarna, Svenskt Näringsliv och IT&Telekomföretagen tillstyrkte förslaget om utökad kriminalisering eller hade ingen invändning mot det.

Några av de remissinstanser som ansåg att det var bra att straffansvaret utvidgades i den omfattning som föreslogs hade synpunkter på bestämmelsernas utformning.

Många remissinstanser var kritiska eller mycket kritiska till förslaget. Svea hovrätt avstyrkte förslaget och anförde att det nya straffansvaret brast i förutsebarhet och inte tillgodosåg grundläggande krav på rättssäkerhet. Hovrätten pekade bl.a. på att det vid bedömningen av om ett förfarande var straffbart var nödvändigt att göra en prövning i tre olika led, vilka alla delvis kräver skälighetsbedömningar. De olika momenten avsåg en bedömning av om

information avsåg ett allvarligt missförhållande och därför inte var skyddad som en företagshemlighet, om angreppet var behörigt på grund av att det syftat till att avslöja missförhållanden och om gärningen enligt den föreslagna straffbestämmelsen var mindre allvarlig eller försvarlig. Hovrätten framhöll också att den handlingsdirigerande verkan av straffbestämmelserna blev oklar eftersom ett visst handlande som var försvarligt enligt straffrätten samtidigt kunde medföra vitesförbud och skadestånd enligt andra bestämmelser i lagen.

Bland andra Sveriges akademikers centralorganisation (Saco), Landsorganisationen i Sverige (LO) och Tjänstemännens centralorganisation (TCO) avstyrkte också förslaget om utökat straffansvar. Arbetstagarorganisationerna ansåg att skadestånd var en tillräckligt verkningsfull sanktion och att förslaget ökade risken för inlåsningseffekter och kunde leda till minskad rörlighet på arbetsmarknaden.

Straffrättsliga överväganden i 2018 års proposition

I det fortsatta lagstiftningsarbetet med en ny lag om företagshemligheter begränsades i stort sett förslagen av straffrättslig karaktär till en skärpning av straffskalan för grova fall av företagsspionerі. Förslaget om ett utvidgat straffansvar för en anställd som olovligen utnyttjar eller röjer en företagshemlighet som han eller hon har fått del av inom ramen för sina arbetsuppgifter fördes alltså inte vidare.

Regeringen uttalade att möjligheterna till straffrättsliga ingripanden mot angrepp på företagshemligheter av personer inom företagets egen verksamhet var otillräckliga. Det betonades samtidigt att det var av stor betydelse att en utvidgad kriminalisering på området skedde återhållsamt. Detta gäller enligt regeringen särskilt som det straffbelagda området gränsade till centrala regler om tryck- och yttrandefrihet. Att det rörde sig om en strafflag som i praktiken var riktad mot i första hand arbetstagare ansågs även det tala för att nykriminaliseringen borde ske med små steg och att särskild hänsyn skulle tas till arbetstagares intressen och förhållandena på arbetsmarknaden. Regeringen framhöll den kritik som Lagrådet lämnat med anledning av 2013 års lagrådsremiss. Det lyftes fram att regeringens övriga förslag förbättrade möjligheterna att på civilrättslig väg

ingripa mot att företagshemligheter sprids och används illojalt. Detta medförde enligt regeringen att behovet av en nykriminalisering var mindre än tidigare. Regeringen pekade på fall då f.d. anställda olovligen använder sig av den tidigare arbetsgivarens kundregister för att starta en konkurrerande verksamhet och angav att det i lagstiftningsärendet inte hade framkommit något som talade mot att skadeståndssanktionen i dessa fall fyllde en effektiv preventiv funktion. Enligt regeringens mening borde även fortsättningsvis skadeståndsrättsliga och arbetsrättsliga sanktioner vara de sanktioner som erbjuds i sådana fall. Regeringen ansåg därför att utredningens förslag innebar att det straffbara området blev alltför omfattande. Till detta kom att det kunde riktas invändningar mot förslagets lagtekniska utformning.

Regeringen framhöll att en straffsanktion endast bör komma i fråga i de fall då det inte råder någon tvekan om att arbetsrättsliga åtgärder och skadeståndsskyldighet inte är tillräckligt avskräckande eller ingripande. Regeringen slog därför fast att straffansvaret bör omfatta endast mer kvalificerade fall av utnyttjande och röjande. Det saknades beredningsunderlag för en sådan mer begränsad utvidgning av straffansvaret. Regeringen uttalade därför att den avsåg att efter sedvanlig beredning återkomma till riksdagen i frågan om hur ett straffansvar för mer kvalificerade fall kan utformas (prop. 2017/18:200 s. 122 f.).

5 Utgångspunkter i fråga om ett utvidgat straffansvar

5.1 En nykriminalisering ska vara befogad

En kriminalisering av ett beteende som tidigare har varit straffritt förutsätter mycket starka skäl. En alltför omfattande kriminalisering riskerar t.ex. att undergräva förtroendet för straffsystemet och dess brottsavhållande verkan, särskilt om rättsväsendet inte kan ingripa mot brotten på ett effektivt sätt. För att en kriminalisering ska vara befogad förutsätts *att* beteendet i fråga kan leda till påtaglig skada eller fara, *att* en straffsanktion är nödvändig med hänsyn till gärningens allvar, *att* en straffsanktion utgör ett effektivt medel för att motverka det icke önskvärda beteendet, *att* alternativa sanktioner inte står till buds eller inte skulle vara rationella eller skulle kräva oproportionerligt höga kostnader eller inte i sig kan anses vara tillräckligt ingripande samt *att* rättsväsendet ska ha resurser att klara en eventuell ytterligare belastning som kriminaliseringen i fråga innebär (se t.ex. prop. 1994/95:23 s. 52 f. och SOU 2016:60 s. 257 f.).

Som tidigare har framhållits har regeringen även uttalat att det är av stor betydelse att en utvidgad kriminalisering på området sker återhållsamt och att straffansvaret bör omfatta endast mer kvalificerade fall av utnyttjande och röjande (prop. 2017/18:200 s. 122 f.).

5.2 Ett ökat hot mot företagshemligheter

En förändrad omvärld har medfört ett ökat hot mot svenska företag och innovationer

Frågan om hot mot svenska intressen har under senare tid kommit att stå i fokus på ett nytt sätt. Detta beror på ett förändrat säker-

hetsläge, och utvecklingen hänger bl.a. samman med att den säkerhetspolitiska situationen i Europa har försämrats. Det har medfört att Östersjöregionen och Sverige har fått en ökad militärstrategisk betydelse (prop. 2014/15:109 s. 42 f.). En konsekvens av detta är att totalförsvarsplaneringen har återupptagits.

I Säpo:s årsbok 2019 beskrivs att underrättelseverksamheten mot Sverige är påtaglig och att det är tydligt att Sveriges säkerhet måste prioriteras högre. Hotbilden är bredare och mer komplex. Den har fått genomslag på flera plan och har betydelse för både offentliga och privata aktörer. Detta har att göra med att främmande makter har kommit att rikta sin uppmärksamhet mot andra områden än de rent militära. De hot som detta medför har delvis ändrat karaktär och prioriteringen av säkerheten behöver ske på den politiska strategiska nivån samt hos myndigheter och i näringsliv. Information och kunskap som olovligen inhämtas kan enligt Säpo värderas till miljardbelopp och underrättelseverksamheten leder till ekonomiska förluster och till att jobb och tillväxt i Sverige påverkas negativt (Säpo:s årsbok 2019 s. 1, 2 och 19–24).

Industrispionage mot svenska företag och institutioner kan bedrivas av såväl en konkurrent som av främmande makt, så kallat statsstyrt industrispionage. Främmande staters underrättelseverksamhet har breddats speciellt mot forskning och utveckling inom civila områden och mot information som rör samhällsviktiga system (SOU 2015:25 s. 226). Det kan i sådana fall finnas olika motiv till angrepp, alltifrån illojal konkurrens till militärstrategiska hänsyn. Det kan vara mycket svårt att avgöra om ett angrepp på en företagshemlighet utförs av en stat, ett statsstyrt företag eller ett självständigt företag, särskilt när angreppet emanerar från en stat som inte är demokratisk (jfr t.ex. regeringens skrivelse 2019/20:18 s. 4). Främmande makt kan använda sig av cyberattacker eller av underrättelseofficerare som verkar i bulvanföretag eller i forskningsdelegationer (Säpo:s årsbok 2019 s. 1, 2 och 19–24).

Ett exempel på industrispionage riktat mot Sverige är att Kina bedriver avancerat cyperspionage för att främja sin egen ekonomiska utveckling och utveckla sin militära förmåga. Detta sker bl.a. genom stöld av teknologi, forskning och utveckling. I detta är underrättelsetjänster involverade, men det sker även genom civila kinesiskägda företag, som måste dela med sig av teknologi och kunskap till den kinesiska militären. Ett annat exempel är att Iran

bedriver industrispionage som riktar sig främst mot svensk högteknologisk industri och svenska produkter som kan användas i kärnvapenprogram. Hotet riktas även mot den civila industrin eftersom dess information kan vara användbar vid tillverkning av massförstörelsevapen (Säpo:s årsbok 2019 s. 1, 25, 29 och 38). Säpo grep under 2019 en person misstänkt för olovlig underrättelseverksamhet mot Sverige. Den misstänkte har arbetat inom svensk högteknologisk industri med uppgifter som är av intresse för främmande makts underrättelseverksamhet. Personen misstänks ha värvats som agent av en rysk underrättelseofficer som arbetat under diplomatisk täckmantel i Sverige. Det finns alltså konkreta misstankar om agenter som jobbar direkt mot svensk industri (Säpo:s årsbok 2019 s. 13).

Säpo har under en längre tid informerat om det hot som industrispionage utgör. Myndigheten har lyft fram att hotet mot svensk industris hemligheter finns här och nu och har betonat intresset av att sårbarheter skyddas (se t.ex. Ds 2007:2 s. 182 och Säpo:s årsbok 2018 s. 32). Säpo beskriver det också som ett särskilt problem att lagstiftningen inte har utvecklats i takt med hotbilden. Viktigt att uppmärksamma är att Säpo i princip endast kan agera mot brottslig verksamhet och att andra länder inhämtar uppgifter även i förberedande syfte. Sådana förberedande åtgärder genomförs långt innan Sverige når en höjd beredskap och uppgifterna kan sedan användas av främmande makt när eller om de behövs (Säpo:s årsbok 2019 s. 1, 2 och 19–24).

I sammanhanget kan även betänkandet av Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet uppmärksammas. Utredningen uttalade att det finns förfaranden som innefattar otillåten underrättelseverksamhet riktad mot forskning och utveckling inom civila områden som faller utanför spioneribestämmelsens tillämpningsområde, men som ändå kan vara straffvärda framför allt med hänsyn till svenska intressen och då i första hand intresset av en god ekonomisk tillväxt (SOU 2012:95 s. 192 f.). Den dåvarande regeringen bedömde att spioneribrottet även fortsättningsvis borde vara förbehållet sådana förfaranden som kan medföra men för Sveriges säkerhet. Det framhölls att spioneribestämmelsen är utformad så att även underrättelseverksamhet som riktar sig mot industrin kan omfattas. Vidare hänvisades till de förslag på ett utvidgat straffansvar som lämnats av 2007 års utred-

ning om skyddet för företagshemligheter (prop. 2013/14:51 s. 39 f.). Som framgår ovan har dock förslagen från 2007 års utredning inte lett till lagstiftning (se ovan avsnitt 4).

Digitaliseringen innebär nya och större risker

Informationstekniken har förändrat förutsättningarna för samhället. En rad verksamheter, både hos det allmänna och inom näringslivet, är helt beroende av digitala system för bl.a. styrning, reglering och övervakning. Digitaliseringen har medfört nya möjligheter som det är viktigt att ta vara på. Som exempel kan nämnas enkel och snabb kommunikation, och lagring av information och bearbetning av densamma. För anställda ger digitalisering möjligheter till ett flexibelt arbetssätt med mobila kontorslösningar i form av bärbara datorer, smarta mobiltelefoner och s.k. molntjänster.

Den nya tekniken har samtidigt medfört nya sårbarheter av strukturell karaktär. Det är på grund av digitaliseringen enkelt att kopiera eller sprida stora mängder information. Företagshemligheter som tidigare kunde skyddas fysiskt kan i dag kopieras på mycket kort tid av dem som har tillgång till informationen. För ett företag som drabbas av detta kan det leda till mycket stor skada. Dessa strukturella risker påverkar också företagandet i allmänhet negativt. Digitaliseringen har också underlättat angrepp och lett till fler angrepp mot skyddsvärda uppgifter (Säpo:s årsbok 2019 s. 39).

Avregleringar och konkurrensutsättningar av offentlig verksamhet, bl.a. på el- och telekommunikationsmarknaderna, har också inneburit att samhällsviktig verksamhet utsätts för nya hot genom att information tillgängliggörs för vidare kretsar.

Affärslivet och arbetsmarknaden har även internationaliserats. Det erbjuder svensk ekonomi stora möjligheter. Internationaliseringen har samtidigt påverkat förutsättningarna för informationssäkerheten. Det gäller t.ex. i samband med utflyttning av verksamhet eller informationslagring till utlandet, särskilt om det finns en koppling till Sveriges säkerhet eller annan samhällsviktig verksamhet, där informationen ska kunna vara tillgänglig även om t.ex. förbindelser till utlandet skärs av.

Kommande utmaningar är bl.a. utbyggnaden av den femte generationens mobilkommunikation (5G) och artificiell intelligens.

Även ”Internet of Things”, där elektronik och internetuppkoppling integreras i vardagsföremål utgör en kommande utmaning (Säpo:s årsbok 2019 s. 22).

5.3 Intressen som talar för en återhållsam kriminalisering

Det finns flera intressen att beakta vid en utvidgning av straffskyddet

En utvidgad kriminalisering av angrepp på företagshemligheter förutsätter att en rad olika hänsyn beaktas.

Frågor om informationsfrihet och yttrandefrihet aktualiseras i hög grad av lagen om företagshemligheter. Den fria opinionsbildningen får inte hindras. Ett annat särskilt intresse att beakta är arbetstagarnas rättigheter och ställning. Arbetstagarnas möjlighet att visselblåsa om missförhållanden i arbetsgivarens verksamhet ska kvarstå. Rörligheten på arbetsmarknaden måste vidare värnas. Risken för inlåsningseffekter måste därför beaktas. Straffrätten ska inte heller utan mycket starka skäl användas för att ingripa i förhållandet mellan arbetstagare och arbetsgivare. Det sistnämnda sammanhänger nära med den långa traditionen i svensk rätt att undvika straffpåföljder när andra effektiva sanktionsformer står till buds för att upprätthålla respekten för ingångna avtal (jfr prop. 1987/88:155 s. 18).

Flera av dessa intressen har beaktats dels genom definitionen av vad som utgör en företagshemlighet (2 §), dels genom att behöriga angrepp på företagshemligheter undantas (4 §). Dessa avvägningar kommer att kvarstå även vid en utvidgad kriminalisering eftersom en sådan måste utgå från lagens struktur. Det finns inte desto mindre skäl att noga överväga dessa frågor och bedöma hur en utvidgad kriminalisering skulle kunna påverka de intressen som gör sig gällande. Samtliga dessa intressen måste alltså beaktas och övervägas noga vid utformningen av den nya kriminaliseringen. I avsnitt 6.11 nedan redogörs för de närmare övervägandena i detta avseende.

Särskilt om yttrandefriheten och informationsfriheten

Tidigare förslag om utvidgad kriminalisering har ifrågasatts för att det har ansetts att förslagen inte har varit tillräckligt utredda i frågan om nykriminaliseringens relation till yttrandefriheten och informationsfriheten. Lagrådet lyfte vid sin granskning av 2013 års lagrådsremiss bl.a. frågan om hur ett straffansvar påverkar yttrandefriheten för anställda, t.ex. vid misstanke om missförhållanden inom företaget. Det finns därför skäl att närmare se över hur fri- och rättigheter påverkas av en utökad kriminalisering (se även följande rubrik samt avsnitt 6.11).

Var och en är tillförsäkrad yttrandefrihet och informationsfrihet i förhållande till det allmänna genom skyddet för grundläggande fri- och rättigheter som följer av 2 kap. regeringsformen. Yttrandefriheten för envar skyddas också genom Sveriges åtaganden om mänskliga rättigheter, såsom den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och EU:s stadga om de grundläggande rättigheterna (EU:s stadga).

Europakonventionen gäller som lag i Sverige (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna) och enligt 2 kap. 19 § regeringsformen får inte lag eller annan föreskrift meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Det är främst kriminaliseringen av röjande av företagshemligheter och den utökade kriminaliseringen av befattning med företagshemligheter som aktualiserar frågor om yttrandefriheten och informationsfriheten. Yttrandefriheten – friheten att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor – och informationsfriheten – friheten att inhämta och ta emot upplysningar samt att i övrigt ta del av andras yttranden – kan dock begränsas.

Yttrandefriheten och informationsfriheten får enligt regeringsformen begränsas genom lag (2 kap. 1 och 20–23 §§ regeringsformen). Sådana begränsningar får endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Begränsningen

får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 § regeringsformen). För yttrandefriheten och informationsfriheten gäller dessutom att dessa friheter endast får begränsas med hänsyn till särskilt angivna ändamål: rikets säkerhet, folkförsörjningen, allmän ordning och säkerhet, enskildas anseende, privatlivets helgd eller förebyggandet och beivrandet av brott. Därutöver får friheten att yttra sig i näringsverksamhet begränsas. I övrigt får begränsningar av yttrandefriheten och informationsfriheten göras endast om särskilt viktiga skäl föranleder det. Vid bedömningen av vilka begränsningar som får göras ska särskilt beaktas vikten av vidaste möjliga yttrandefrihet och informationsfrihet i politiska, religiösa, fackliga, vetenskapliga och kulturella angelägenheter.

Grundlagsskyddet för yttrande- och informationsfriheten i tryckta skrifter regleras i tryckfrihetsförordningen (TF) och för vissa andra medier, t.ex. radio, tv och vissa överföringar via internet, i yttrandefrihetsgrundlagen (YGL). En viktig del av det svenska skyddet för nämnda friheter är meddelarskyddet. Meddelarskyddet består bl.a. av meddelarfrihet och anskaffarfrihet. Meddelarfriheten innebär att var och en har rätt att lämna uppgifter i vilket ämne som helst för publicering i de medier som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen. Anskaffarfriheten innebär en rätt för var och en att straffritt anskaffa uppgifter för publicering i ett medium som omfattas av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen (1 kap. 7 § tryckfrihetsförordningen och 1 kap. 10 § yttrandefrihetsgrundlagen). Meddelar- och anskaffarfriheterna är i viss mån inskränkta om utlämnandet eller anskaffandet av en uppgift innefattar t.ex. grövre brott mot rikets säkerhet. Grundlagarna innehåller även ett skydd för meddelare och anskaffare när det rör sig om medier som inte ges ut eller på annat sätt offentliggörs i Sverige – det s.k. korrespondentskyddet (13 kap. 7 § tryckfrihetsförordningen och 11 kap. 3 § yttrandefrihetsgrundlagen, jfr prop. 2013/14:47 s. 18). Det kan avslutningsvis nämnas att meddelarfriheten och anskaffarfriheten kompletteras av anonymitetsskyddet (3 kap. 1–4 §§ tryckfrihetsförordningen och 2 kap. 1–4 §§ yttrandefrihetsgrundlagen), efterforskningsförbudet (3 kap. 5 § tryckfrihetsförordningen och 2 kap. 5 § yttrandefrihetsgrundlagen) samt repressalieförbudet (3 kap. 6 § tryckfrihetsförordningen och 2 kap. 6 § yttrandefrihetsgrundlagen).

En mycket viktig avgränsning av skyddet för de nu aktuella friheterna är att det endast gäller gentemot det allmänna. För att ett liknande skydd även ska gälla i privat verksamhet som är offentligt finansierad infördes lagen (2017:151) om meddelarskydd i vissa enskilda verksamheter (meddelarskyddslagen). Lagen gäller i yrkesmässigt bedriven enskild verksamhet som till någon del är offentligt finansierad och som tillhör bl.a. skolväsendet, hälso- och sjukvården, tandvården eller bedrivs enligt socialtjänstlagen. Arbetstagare i sådan verksamhet har i fråga om uppgifter om verksamheten samma rättigheter som de som föreskrivs i tryckfrihetsförordningen och yttrandefrihetsgrundlagen i fråga om rätt att lämna uppgifter för offentliggörande. Vidare gäller det som föreskrivs i tryckfrihetsförordningen och yttrandefrihetsgrundlagen angående förbud att ingripa mot bruk eller missbruk av tryckfriheten eller yttrandefriheten eller medverkan till sådant bruk eller missbruk samt förbud mot att efterforska bl.a. upphovsman och meddelare.

De privata arbetsgivare som inte omfattas av meddelarskyddslagen har rätt att efterforska vem som lämnat ett meddelande, dock inom ramen för god arbetsmarknadssed. Det bör dock särskilt noteras att Europakonventionens skydd går något längre än det svenska skyddet enligt grundlagen. Enligt Europadomstolens praxis finns det för staten i vissa fall även en positiv förpliktelse att skydda rätten till yttrandefrihet mot angrepp också från enskilda (dom av den 29 februari 2000 från Europadomstolen i målet Fuentes Bobo mot Spanien samt Ds 2001:9 s. 25). Samtliga arbetstagares rätt att slå larm om missförhållanden i arbetsgivarens verksamhet behandlas nedan.

Särskilt om arbetstagarnas rättigheter och visselblåsning

Det finns ett allmänt intresse av att missförhållanden inom företag, organisationer och myndigheter kommer till offentligheten och åtgärdas. Inom den offentliga sektorn kan det bidra till att allmänna medel används på ett mer effektivt sätt. Detsamma gäller för privata utförare inom offentligt finansierad verksamhet. Även andra privata företag har naturligtvis ett intresse av att verksamhetens resurser kan tas i anspråk på ett effektivt sätt. Om missförhållanden kommer fram bidrar det också till en sundare konkurrens mellan företag,

eftersom en ökad insyn innebär att det blir svårare för företag att skaffa sig konkurrensfördelar genom otillbörliga metoder (jfr prop. 2015/16:128 s. 10). Av dessa skäl finns ett skydd för arbetstagare i detta avseende som går längre än det skydd som grundlagarna ger. Detta skydd framgår delvis av lagen om företagshemligheter, men även av en särskild lag – lagen (2016:749) om särskilt skydd mot repressalier för arbetstagare som slår larm om allvarliga missförhållanden (visselblåsarlagen).

I fråga om lagen om företagshemligheter kan det inledningsvis noteras att uppgiftslämnande som omfattas av meddelar- eller anskaffarfriheterna inte överhuvudtaget omfattas av lagen om företagshemligheter. Därutöver ger lagen ett omfattande utrymme att anskaffa eller röja företagshemligheter i samband med s.k. visselblåsning, dvs. när någon inom ett företag eller en institution slår larm om ett missförhållande inom organisationen.

Information om något som utgör ett brott eller annat allvarligt missförhållande utgör inte en företagshemlighet (2 §) och faller av det skälet utanför lagens tillämpningsområde.

Lagen gäller vidare endast obehöriga angrepp på en företagshemlighet (4 §). I lagtexten anges exempel på angrepp på företagshemligheter som alltid är behöriga. Som ett obehörigt angrepp anses aldrig att någon angriper en företagshemlighet för att offentliggöra eller inför en myndighet eller ett annat behörigt organ avslöja något som skäligen kan misstänkas utgöra brott med fängelse i straffskalan, eller kan anses utgöra något annat missförhållande och offentliggörandet eller avslöjandet sker till skydd för allmänintresset.

Ett avslöjande av missförhållanden till en myndighet eller ett behörigt organ bör exempelvis kunna göras inför Polismyndigheten, länsstyrelserna, Arbetsmiljöverket eller en miljö- och hälsoskyddsnämnd. Med annat behörigt organ än myndighet avses bl.a. skyddskommittéer och skyddsombud samt andra fackliga förtroendemän liksom olika branschorganisationer inom näringslivet (prop. 2017/18:200 s. 150). Ett behörigt organ kan också finnas utomlands som exempelvis Europeiska byrån för bedrägeribekämpning (Olaf). För vissa situationer finns det lagstadgade skyldigheter för anställda och andra att rapportera om misstänkta överträdelser, t.ex. inom finansmarknadens område. Ett uppgiftslämnande om ett missförhållande kan dock också vara behörigt utan

att det finns någon uttrycklig rapporteringsskyldighet (prop. 2017/18:200 s. 148 med hänvisningar).

Lagens undantag för visselblåsning gäller också då angreppet på företagshemligheten sker i direkt syfte att offentliggöra brottsmisstankar eller det missförhållande som ska avslöjas till skydd för allmänintresset. Frågan om huruvida röjandet sker i direkt syfte att visselblåsa om ett missförhållande måste bl.a. bedömas med hänsyn till under vilka förhållanden och till vem ett röjande sker (se vidare bet. 1989/90:LU37 s. 29 f. och prop. 2017/18:200 s. 145 f.). Avgörande är om bedömningen leder till slutsatsen att angreppet har skett i direkt opinionsbildande syfte. Om syftet har varit att gagna någon ekonomiskt, sig själv eller någon annan, är angreppet obehörigt och kan därmed vara straffbart.

Om ett angrepp är obehörigt enligt 4 § bedöms från fall till fall. Det bör understrykas att lagen om företagshemligheter inte uttömmande anger under vilka förutsättningar det är tillåtet att röja företagshemligheter i syfte att slå larm. Det klargörs endast under vilka förhållanden det alltid är godtagbart för en enskild att lämna hemlig information till exempelvis en tillsynsmyndighet. Utgångspunkten är att det ska göras en avvägning mellan samhällsintresset av att viss information offentliggörs eller avslöjas för en behörig myndighet och innehavarens intresse av skydd för sina företagshemligheter. Det kan alltså vara godtagbart att även i andra situationer än de i lagtexten nämnda situationerna röja företagshemligheter i syfte att slå larm om missförhållanden.

Om angriparen av företagshemligheten har godtagbara skäl för sitt handlande – dvs. om angreppet är behörigt – gäller inte lagens bestämmelser. Den kriminalisering som föreslås i denna promemoria förändrar inte detta och påverkar alltså inte utrymmet för visselblåsning enligt 4 §.

Som tidigare nämnts bör även visselblåsarlagen beaktas i sammanhanget. Lagen fastställer en rätt till skadestånd för den arbetstagare som i strid med lagen drabbas av repressalier på grund av att han eller hon har slagit larm om allvarliga missförhållanden i arbetsgivarens verksamhet. Visselblåsarlagen reglerar inte arbetstagarnas rätt att avslöja företagshemligheter utan gäller parallellt med övriga regler som kan aktualiseras då arbetstagare slår larm om allvarliga missförhållanden (se 1 § första stycket visselblåsarlagen och prop. 2015/16:128 s. 94). Med allvarliga missförhållanden enligt

visselblåsarlagen avses brott med fängelse i straffskalan eller därmed jämförliga missförhållanden (1 § andra stycket visselblåsarlagen). Begreppet allvarliga missförhållanden anknyter alltså till motsvarande begrepp i 2 § lagen om företagshemligheter (jfr prop. 2015/16:128 s. 23). Innebörden är att information om sådana allvarliga missförhållanden inte heller anses vara företagshemligheter (jfr dock prop. 2017/18:200 s. 57 f.).

Ett nytt direktiv om visselblåsning

Under slutet av 2019 trädde Europaparlamentets och rådets direktiv (EU) 2019/1936 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten (visselblåsardirektivet) i kraft. Medlemsstaterna ska senast den 17 december 2021 sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att genomföra direktivet. Regeringen tillsatte en utredning för genomförandet av direktivet (dir. 2019:24). Betänkandet, Ökad trygghet för visselblåsare (SOU 2020:38) bereds för närvarande inom Regeringskansliet.

Genom visselblåsardirektivet fastställs miniminormer till skydd för personer som rapporterar överträdelser av unionsrätten. Direktivets materiella tillämpningsområde är alltså begränsat till angivna rättsakter och syftar till att stärka genomförandet av unionsrätten. Vissa områden såsom nationell säkerhet och sekretess inom hälso- och sjukvården omfattas inte av direktivet.

Enligt direktivet ska vissa personkategorier som rapporterar om överträdelser (rapporterande personer) under särskilda förutsättningar vara skyddade mot repressalier av olika slag. Direktivet kräver även att aktörer av viss storlek i privat och offentlig sektor inrättar särskilda interna funktioner för rapportering (interna rapporteringskanaler). Vidare ska det vid behöriga myndigheter i medlemsstaterna finnas funktioner för rapportering av överträdelser (externa rapporteringskanaler). Överträdelser ska antingen rapporteras internt eller externt och i sista hand offentliggöras. Skyddet för en rapporterande person vid offentliggörande av en överträdelse är därför begränsat.

I visselblåsardirektivet finns särskilda bestämmelser som tar sikte på företagshemligheter.

Enligt artikel 21 ska medlemsstaterna vidta nödvändiga åtgärder för att säkerställa att rapporterande personer är skyddade mot repressalier. Sådana rapporterande personer ska inte åläggas ansvar av något slag som en följd av rapporter eller offentliggöranden enligt direktivet som innebär att en företagshemlighet röjs. Dessa personer ska också ha rätt att åberopa rapporten eller offentliggörandet för att yrka på att ärendet avslås, under förutsättning att de hade rimliga skäl att tro att det var nödvändigt att rapportera eller offentliggöra sådan information för att avslöja en överträdelse som avses i visselblåsardirektivet. Av artikel 21 framgår vidare att om en person som uppfyllt villkoren i visselblåsardirektivet rapporterar eller offentliggör information om överträdelser som omfattas av direktivet ska sådan rapportering eller sådant offentliggörande anses som lagligt enligt villkoren i artikel 3.2 i direktivet om företagshemligheter (2016/943).

Även om ändringarna för att genomföra direktivet om visselblåsning för närvarande bereds inom Regeringskansliet finns det skäl att i detta sammanhang belysa förhållandet mellan direktivet och lagen om företagshemligheter.

Som har utvecklats ovan ger lagen om företagshemligheter ett omfattande utrymme för visselblåsning. Lagens sanktioner kan inte göras gällande när någon angriper en företagshemlighet för att offentliggöra eller inför en myndighet eller ett annat behörigt organ avslöja något som kan anses utgöra ett missförhållande och offentliggörandet eller avslöjandet sker till skydd för allmänintresset. Information om något som utgör ett brott eller annat allvarligt missförhållande utgör vidare överhuvudtaget inte en företagshemlighet (2 §). Såvitt nu kan bedömas är utrymmet för visselblåsning tillräckligt också i förhållande till visselblåsardirektivet.

Under alla omständigheter anges i visselblåsardirektivet att tillåten visselblåsning inte ska anses vara ett olagligt angrepp på en företagshemlighet enligt direktivet om företagshemligheter. Detta får anses innebära att den svenska lagen om företagshemligheter – som genomför direktivet om företagshemligheter – ska tolkas mot den bakgrunden. Någon konflikt mellan lagen om företagshemligheter och visselblåsardirektivet kan således inte förutses.

6 Ett förstärkt straffrättsligt skydd för företagshemligheter

6.1 Det ska införas ett straffansvar för angrepp på företagshemligheter av teknisk natur

Förslag: Det ska införas två nya straffbestämmelser i lagen om företagshemligheter. De ska ta sikte på den som olovligen angriper en företagshemlighet som han eller hon har lovlig tillgång till. Straffansvaret ska vara begränsat till företagshemligheter av teknisk natur.

Skälen för förslaget

Nya hot har ökat behovet av ett förstärkt straffrättsligt skydd

För en kunskapsintensiv nation som Sverige är det av stor vikt att skyddet för företagshemligheter är ändamålsenligt och anpassat efter rådande förutsättningar. Stora värden står på spel för enskilda företag, och för samhället i stort kan det vara fråga om miljardbelopp. Därutöver är skyddet för företagshemligheter av betydelse för svenskt företagande i allmänhet, inte minst för att möta de utmaningar som informationssamhället och den digitala tekniken medfört för både produktion inom den befintliga industrin och utvecklande, distribution och konsumtion av nya varor och tjänster.

Flera faktorer gör att det i dag framstår som mer angeläget än tidigare att förstärka det straffrättsliga skyddet för företagshemligheter (se avsnitt 5.2).

En mer konfliktfylld omvärld har lett till ett ökat hot mot svenska intressen. I dag utgör underrättelseoperationer som stöds av

främmande makt ett reellt hot för svenska företag. Hoten gäller inte enbart teknik med direkt koppling till rikets säkerhet, utan även annan information som representerar stora värden för teknikintensiva företag och samhället i stort. Det finns skäl att tro att hotet mot företagshemligheter är särskilt påtagligt för svensk industri eftersom den utmärks av en hög kunskapsnivå och innovationskraft. Det kan inte heller bortses från att en ökad internationell konkurrens gör att kommersiella konkurrenter och andra affärsintressenter kan använda sig av industrispionage för att tillskansa sig fördelar av olika slag.

Utvecklingen i det svenska samhället med en ökad digitalisering och utkontraktering har även medfört strukturella sårbarheter och har på så vis underlättat angrepp på företagshemligheter. Ett exempel på den utvecklingen är att cyberspionaget har ökat väsentligt under senare år och att många företag ökat sina kostnader för att skydda sig mot sådana angrepp. Aktörer som bedriver cyberspionage kan ofta ställa stora resurser till förfogande för detta ändamål och har möjlighet att arbeta långsiktigt och metodiskt med inriktningen att komma över värdefull information som finns i svenska företag och forskningsinstitutioner. Det finns också flera exempel på att främmande makt använder sig av agenter för att komma åt olika typer av teknisk information som finns i den svenska industrin (se avsnitt 5.2).

Ett sätt att komma åt information är genom anlitande av insiders på målföretagen, dvs. anställda med lovlig tillgång till känslig information. Det kan i ett sådant fall handla om informationskedjor där flera personer på olika positioner och med olika befogenheter inom ett och samma företag medverkar. Även den typen av angrepp har underlättats av teknikutvecklingen på så sätt att det är möjligt att på kort tid komma över och tillgodogöra sig stora mängder information. Ett angrepp av det slaget kan röja ett företags centrala företagshemligheter och leda till mycket stor skada. Även universitet och forskarvärlden i övrigt riskerar att utsättas för sådana angrepp.

I praktiken är det i många fall svårt eller omöjligt för företag, trots stora nedlagda resurser, att genom tekniska hinder och säkerhetsrutiner fullt ut skydda sig mot angrepp på känslig information som utförs av anställda eller andra som betrotts tillgång till informationen.

Hotbilden mot företagshemligheter framstår mot denna bakgrund som mer påträngande i dag än när straffansvaret utformades på 1980-talet. Hoten är i dag av ett annat slag och emanerar från aktörer med stora resurser, även med koppling till utländska intressen. Det är också tydligt att angrepp kan orsaka långt större skada än vad som var möjligt före digitaliseringen. Behovet av ett bredare straffrättsligt skydd har därför ökat.

Ett straffansvar bör ta sikte på företagshemligheter av teknisk natur…

Det finns i dag luckor i det straffrättsliga skyddet för företagshemligheter beträffande personer som har lovlig tillgång till den företagshemliga informationen, dvs. personer inom företags och forskningsinstitutioners egna verksamheter. Företagsspionerі omfattar nämligen endast den som olovligen anskaffat företagshemligheten. Motsatsvis innebär det att den som lovligen har anskaffat hemligheten, t.ex. som en del av ett arbetsmaterial, inte kan drabbas av sådant straffansvar enligt lagen.

Frågan är om det ökade behovet av att motverka obehöriga angrepp på företagshemligheter är sådant att det framstår som nödvändigt att införa ett straffansvar för personer med lovlig tillgång till den företagshemlighet som angrips. Med tanke på att en kriminalisering på området bör ske med stor återhållsamhet handlar det om att identifiera de fall där behovet av ett straffrättsligt skydd är som störst.

Inriktningen på en ny kriminalisering bör alltså vara att träffa sådana angrepp som typiskt sett medför stor skada – eller risk för sådan – för företag och forskningsinstitutioner, och som därför även kan sägas påverka svenskt företagande och svensk innovation negativt.

Det finns kvalificerade fall av utnyttjande och röjande av företagshemligheter som får anses i hög grad straffvärda, men som i dag är straffria. Det är sådana fall av utnyttjande och röjande av företagshemligheter där det finns en stor risk för ekonomisk eller annan allvarlig skada, typiskt sett för att det är fråga om en företagshemlighet som föregåtts av stora investeringar eller motsvarar ett betydande värde. Sådana angrepp torde många gånger förutsätta

stora resurser, både för åtkomsten av företagshemligheten och för det efterföljande utnyttjandet av densamma.

Den friande domen för en av de inblandande i Ericsson-målet får ofta tjäna som illustration på ett fall som borde aktualisera straffansvar. I det fallet var det fråga om information om viktig teknisk infrastruktur och röjandet var en del i ett förslaget och välplanerat angrepp. Till detta kom att en främmande makt låg bakom angreppet, även om det inte kunde läggas den friade personen till last. Det var även fråga om värdefulla tekniska företagshemligheter och angreppet får anses ha varit särskilt skadligt, inte bara för det drabbade företaget utan även för Sverige och svenskt företagande i allmänhet.

Även om alla angrepp på företagshemligheter typiskt sett är förenade med risk för skada för innehavaren, framstår bristen i det straffrättsliga skyddet som särskilt allvarlig för företag som ägnar sig åt – i vid bemärkelse – teknisk produktion av varor eller tjänster.

Teknikintensiv verksamhet är helt beroende av att företagshemligheter inte lämnar verksamheten och är även ofta förknippad med stora investeringar. Det rör sig typiskt sett om värdefull information för företagen och många gånger också för samhället, som i Ericsson-fallet. Angrepp på sådan verksamhet kan därför beskrivas som särskilt skadliga. Teknikintensiv verksamhet kan även antas vara särskilt utsatt för allvarliga angrepp. Det torde ofta förhålla sig så att olika aktörer arbetar parallellt för att lösa tekniska problem allt eftersom de uppkommer i samhället. Det gör att tekniska företagshemligheter är särskilt åtråvärda för konkurrenter. Det gör också att ett utnyttjande eller röjande av uppgifterna i ett tidigt skede kan få mycket stora konsekvenser för företagen. Hotet från resursstarka aktörer, däribland främmande makter, kan vidare antas i princip uteslutande riktas mot verksamhet av den typen. Det finns därför sammantaget skäl att tro att de sanktioner som står till buds – skadestånd och arbetsrättsliga sanktioner – inte är tillräckligt avskräckande i dessa kvalificerade fall.

Frågan om behovet av straffrättsligt skydd för företagshemligheter som avser tekniskt kunnande bör även ses mot bakgrund av att Sverige är ett litet land med kunskapsföretag i världsklass. Inom den svenska exportindustrin har flera stora företag vuxit fram. Även inom den digitaliserade ekonomin är svenska företag framgångsrika. För att Sverige i en ny verklighet präglad av hård internationell

konkurrens ska kunna fortsätta att vara en kunskapsekonomi i framkant är det av största betydelse att företagens konkurrenskraft säkerställs och att förutsättningarna för innovation och kunskapsöverföring förbättras. Skyddet för företagshemligheter är centralt i det sammanhanget.

Det finns alltså flera tungt vägande skäl för att ett trovärdigt straffrättsligt skydd är särskilt viktigt för tekniska företagshemligheter.

Skyddet för företagshemligheter bör vidare på ett effektivt sätt komplettera det immaterialrättsliga skyddet. Immaterialrätten syftar till att bl.a. främja skapande, innovation och tekniskspridning. Det immaterialrättsliga skyddet innebär att innehavaren som utgångspunkt får en tidsbegränsad ensamrätt att exploatera det som han eller hon har skapat. För att säkerställa att de immateriella rättigheterna inte blir innehållslösa finns det i alla immaterialrättsliga lagar regler om bl.a. civilrättsliga och straffrättsliga sanktioner. De olika immaterialrättslagarna uppvisar här stora likheter (jfr prop. 2015/16:57 s. 115). Nyligen har straffskalorna för de allvarligaste fallen av immaterialrättsintrång skärpts genom att särskilda straffskalor för uppsåtliga grova brott införts i samtliga immaterialrättsliga lagar (prop. 2019/20:149).

Skyddet för företagshemligheter kan i flera avseenden utgöra ett viktigt komplement till immaterialrätterna när det kommer till företagens möjligheter att skydda sina innovationer och sina produktionsprocesser.

Ett sådant exempel är möjligheten till skydd för en uppfinning som potentiellt skulle kunna skyddas genom ett patent. Om ett företag vill skydda sin uppfinning genom ett patent, krävs bland annat att den är ny. Om en uppfinning utnyttjats eller röjts innan en ansökan om patent tilldelats en ingivningsdag hos PRV kan nyhetsvärdet anses vara förstört och möjligheten att få ett patenträttsligt skydd kan ha gått om intet. Det kan få stora konsekvenser för den presumtiva patenthavaren. Det är därför viktigt att företagshemligheterna som kan ligga till grund för en uppfinning effektivt kan skyddas, bl.a. med straffrättsliga sanktioner, som kompletterar och kopplar ihop med det immaterialrättsliga skyddet. I samband med att en patentansökan beviljas skyddas uppfinningen genom ett patent och ett intrång i den rättigheten kan bl.a. medföra straffansvar. Mot den bakgrunden kan

det också ifrågasättas om det är rimligt att tidpunkten för ett utnyttjande får så stora konsekvenser i fråga om vilka sanktioner som kan bli aktuella, trots att utnyttjandet kan avse samma objekt och skyddsintressena kan anses vara jämförbara.

Ett ytterligare exempel på hur skyddet för företagshemligheter och immaterialrätten samverkar är att en del företag ser skyddet för företagshemligheter som ett alternativ till att söka patent, något som bl.a. kan motiveras med att skyddet potentiellt kan innebära ett längre skydd än patentets tjugo år (prop. 2017/18:200 s. 105). Företaget kan också bedöma att det tar för lång tid att ansöka om och få ett patent för innovationer, särskilt om de bedöms ha en kort livslängd.

Sammanfattningsvis görs bedömningen att en kriminalisering bör ta sikte på företagshemligheter som avser innovationer och produktionsmetoder för en vara eller en tjänst. Vidare bedöms kriminaliseringen i dessa fall vara nödvändig med hänsyn till gärningarnas allvar. Den bedöms även vara effektiv för att motverka de oönskade beteendena.

Avgränsningen i denna del bör uttryckas så att kriminaliseringen avser ”företagshemligheter av teknisk natur”. Uttrycket ”av teknisk natur” finns sedan tidigare i svensk rätt. I 5 kap. 12 § konkurrenslagen (2008:579) anges t.ex. att det inte finns någon skyldighet att röja företagshemligheter av teknisk natur vid Konkurrensverkets åtgärder, som t.ex. att ålägga ett företag att inkomma med uppgifter (se även lagen [1970:417] om marknadsdomstol m.m.). Uttrycket har även använts tidigare (se t.ex. SOU 1966:71 s. 138 f.).

I sammanhanget kan det nämnas att även våra nordiska grannländer sett behovet av ett straffrättsligt skydd för företagshemligheter av teknisk natur (se danska Lov nr 309 af 25/04/2018: Lov om forrettningshemmeligheder, norska Lov om vern av forretningshemmeligheter och finska Lag om företagshemligheter, 595/2018). Även Tyskland har bestämmelser med liknande innebörd (se Gesetz zum Schutz von Geschäftsgeheimnissen).

…men angrepp på kommersiella företagshemligheter bör inte omfattas av en kriminalisering

Även de kommersiella företagshemligheterna kan i många fall motsvara stora värden. För ett litet företag kan kundlistan vara den

väsentliga tillgången. Samtidigt handlar det nu om att sortera ut de fall av angrepp på företagshemligheter där behovet av kriminalisering är särskilt starkt. I fråga om kommersiella företagshemligheter framstår skälen för en kriminalisering inte som lika påtagliga som för de tekniska företagshemligheterna.

Även om angrepp på kommersiella företagshemligheter kan orsaka skada för innehavaren, framstår hotbilden mot den typen av företagshemligheter som mindre allvarlig. Typiskt sett torde angreppen vara mindre kvalificerade. Det kan vidare antas att angrepp som på ett eller annat sätt involverar främmande makt är begränsade till företagshemligheter av teknisk natur. Vidare handlar det mindre ofta om sådan information som är av särskild betydelse för företagens möjlighet till innovationer och teknikutveckling. Det är alltså fråga om en situation i vilken allmänintresset är mindre uttalat i jämförelse med angrepp på tekniska företagshemligheter. I fråga om de kommersiella företagshemligheterna är jämförelsen med det immaterialrättsliga skyddet inte heller lika närliggande, även om också en kommersiell företagshemlighet kan skyddas exempelvis enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk. Sammantaget framstår därför skadestånd och arbetsrättsliga sanktioner som tillräckliga sanktioner i sådana fall (jfr prop. 2017/18:200 s. 125).

Denna slutsats ligger även väl i linje med regeringens uttalande om att straffansvaret bör avgränsas till mer kvalificerade fall. Som exempel på ett mindre allvarligt fall nämndes det fallet att en tidigare anställd utnyttjar den tidigare arbetsgivarens kundlista för att försöka ta över kundbasen (jfr prop. 2017/18:200 s. 125).

Skälen för en kriminalisering av angrepp från personer inom den egna verksamheten på kommersiella företagshemligheter är alltså inte lika starka som i fråga om företagshemligheter av teknisk natur, trots att kommersiella företagshemligheter kan ha stort värde för ett företag. En kriminalisering av angrepp på sådana företagshemligheter från personer med lovlig tillgång till informationen kan därför inte anses nödvändig, givet de andra sanktioner som står till buds. Kriminaliseringen bör därför inte omfatta sådana angrepp.

Som en tredje kategori av företagshemligheter talas ibland om administrativa företagshemligheter. Det kan typiskt sett handla om löneuppgifter, verksamhetsrutiner eller mötesprotokoll, som någon gång kan uppfylla kraven på en företagshemlighet. Det finns inte

heller tillräckliga skäl för att angrepp på sådan information ska kunna bestraffas.

Vad som närmare avses med företagshemligheter av teknisk natur

Karakteristiskt för företagshemligheter av teknisk natur är att de typiskt sett utgör ett led i produktionen eller framställningen av en vara eller utförandet av en tjänst. Företagshemligheter av teknisk natur kan exempelvis vara ritningar, recept, källkoder, datorprogram, forskningsresultat eller forskningsunderlag, tekniska förebilder och andra modeller eller annan sådan teknisk information. Företagshemligheten kan, men behöver inte, innefattas i en framställd vara eller utförd tjänst, utan det är tillräckligt att informationen är sådan att den typiskt sett ingår i produktionen eller framställningen. Även förstadierna i utvecklingen av dessa, så som förstudier, prototyptillverkning, och förberedande tester omfattas. Detta syftar till att skydda företagshemligheter under hela produktionsprocessen. Även framställningsprocesser, maskinella anordningar eller andra hjälpmedel bör kunna omfattas (jfr prop. 1981/82:165 s. 300). Det bör inte krävas att företagshemligheten är dokumenterad i någon form, även om detta vanligtvis är fallet. I fråga om dokumenterade företagshemligheter saknar det givetvis betydelse om informationen har dokumenterats i fysisk eller digital form. Begreppet företagshemlighet är teknikneutralt (jfr 2 §).

Till företagshemligheter av teknisk natur bör däremot inte räknas information om innehavarens affärsmässiga förhållanden, exempelvis priskalkyler, marknadsundersökningar och kundlistor. Information av det slaget har närmast betydelse för hur företaget ska kommersialisera en vara eller en tjänst och kan inte anses hänförlig till produktionen eller framställningen av varan eller utförandet av tjänsten. Detsamma gäller information som enbart avser lagring eller transporter och annan information om distributionen av en vara. Inte heller affärsplaner eller samarbetsavtal bör anses utgöra företagshemligheter av teknisk natur. Handlingar av det slaget kan vara av stor betydelse som underlag för företagets beslut att t.ex. inleda viss produktion, men avser i första rummet rent kommersiella förhållanden, exempelvis om det finns förutsättningar att i framtiden kommersialisera en vara eller en tjänst eller om produktionen kan

antas bli lönsam. Inte heller information av enbart administrativt slag inordnas under begreppet företagshemligheter av teknisk natur, t.ex. ett system för att administrera företagets löneutbetalningar.

Företagshemligheter av teknisk natur bör inte förutsätta särskild verkshöjd eller särskilt värde

En fråga är om det för straffansvar bör krävas att företagshemligheten är av viss kvalitet eller är särskilt värdefull. Det kan variera stort både i fråga om innovationskraft och värde mellan olika företagshemligheter av teknisk natur. I vissa fall ligger miljardinvesteringar bakom utvecklingen av exempelvis en prototyp medan det i andra fall kan handla om en produktutveckling som i mångt och mycket bygger på tidigare kunskaper.

Till en början kan det konstateras att det förutsätts att informationen i fråga har ett i vart fall potentiellt kommersiellt värde för att den ska kunna skyddas som en företagshemlighet. Detta följer av kravet på att ett röjande av informationen ska vara ägnat att medföra skada i konkurrenshänseende för innehavaren. Det innebär i sig en avgränsning i förhållande till information som är av så begränsad ekonomisk betydelse för innehavaren att den inte förtjänar lagens skydd (2 § första stycket 4 lagen om företagshemligheter; jfr prop. 2017/18:200 s. 104).

Hur stort en företagshemlighets värde är, och i vissa fall även dess kommersiella användningsområden, kan i många fall vara svårt att bedöma, särskilt på ett tidigt stadium. Det talar mot att göra kriminaliseringen beroende av en sådan gräns, eftersom det är tveksamt om kriminaliseringen då skulle träffa alla gärningar som bör kunna omfattas. Det kan dessutom antas vara väldigt svårt att formulera en godtagbar avgränsning av ett sådant straffansvar som avser endast företagshemligheter av särskilt värde eller viss verkshöjd.

Det föreslås dock att det införs ett undantag från straffansvar för ringa fall. Vid bedömningen av om gärningen är ringa ska bl.a. den uppkomna skadan eller risken för skada beaktas (se avsnitt 6.8).

Utöver att en företagshemlighet är av teknisk natur bör det alltså inte förutsättas att informationen har särskild verkshöjd eller är särskilt värdefull.

6.2 De angrepp som ska kriminaliseras är olovligt utnyttjande och olovligt röjande

Förslag: De angrepp som ska omfattas av en kriminalisering är olovligt utnyttjande och olovligt röjande av en företagshemlighet av teknisk natur.

Skälen för förslaget

Utnyttjande och röjande av företagshemligheter är till sin typ skadliga handlingar

Det är mot bakgrund av att det saknas straffansvar för personer med lovlig tillgång till företagshemligheter som olovligt utnyttjande och olovligt röjande av företagshemlighet tidigare har diskuterats som möjliga alternativ för en utvidgad kriminalisering. Sådana gärningar är inte beroende av hur informationen har kommits över, utan det intressanta är i stället hur informationen hanteras.

Med utnyttjande avses att någon i egen verksamhet praktiskt tillämpar den information som utgör företagshemligheten. Det ska vara fråga om ett kommersiellt utnyttjande, men det krävs inte att verksamheten går med vinst (prop. 2017/18:200 s. 37). Utnyttjande av företagshemlighet är närmare definierat i 3 § tredje stycket på så sätt att det även avser att någon tillverkar varor vars formgivning, egenskaper, funktion, tillverkning eller marknadsföring gynnas avsevärt av en angripen företagshemlighet och att detsamma gäller då någon bjuder ut sådana varor till försäljning, för ut dem på marknaden eller importerar, exporterar eller lagrar sådana varor för dessa ändamål.

Med röjande avses att angriparen avslöjar hemligheten för någon annan. Det saknar i princip betydelse om röjandet sker mot ersättning eller inte (prop. 2017/18:200 s. 37).

I samband med att brottstypen företagsspionerи infördes uttalades att kriminaliseringen inriktades på att förhindra den primära skaderisken, dvs. den risk för skada för den rättmätige innehavaren som inträder redan genom det olovliga anskaffandet (prop. 1987/88:155 s. 14 f.). Det är därför följdriktigt att även i fråga om utnyttjande och röjande av företagshemligheter utgå från risken

för skada för att få en ändamålsenlig avgränsning av det straffbara handlandet.

Det kan då till en början konstateras att olovligt utnyttjande och röjande ofta ligger närmare den realiserade risken för skada än ett anskaffande. Ett röjande kan t.ex. medföra att konkurrensfördelar försvinner och att företagshemligheten inte längre anses skyddad, vare sig såsom företagshemlighet eller inför ett eventuellt patent. Ett utnyttjande är ett missbruk av den hemliga informationen för vinning och medför också en risk för att företagshemligheten sprids. Ett utnyttjande och ett röjande kan i någon mån sägas realisera den risk som ett anskaffande innebär.

Den skada som kan uppkomma till följd av ett olovligt utnyttjande eller röjande av en företagshemlighet kan vara mycket kännbar. Det kan avse uteblivna intäkter, illojal konkurrens och att ett möjligt patent kan gå om intet. Redan en ökad risk för angrepp av detta slag kan inverka menligt på företagsklimatet. I fråga om röjande finns det dessutom säkerhetsaspekter kopplade till främmande makt.

Utnyttjande och röjande är angrepp som kan sägas handla om situationer då någon olovligen brukar information som rätteligen tillkommer någon annan. Det handlar alltså om ageranden som i allra högsta grad framstår som klandervärda. Det klandervärda agerandet kan sägas bestå i ett illojalt beteende, ett brott mot ett förtroende eller ett tystnadslöfte. Olovligt röjande och utnyttjande av företagshemligheter avser således beteenden som får anses vara klandervärda.

Sammanfattningsvis finns alltså goda skäl att låta den nya kriminaliseringen omfatta utnyttjande och röjande av företagshemligheter av teknisk natur.

Den utökade omfattningen av det kriminaliserade området leder till att olika sanktioner kan bli tillämpliga samtidigt. Detta har sin förklaring i att vitesförbud i högre grad kan tänkas omfatta fall av utnyttjande och röjande än fall av anskaffande.

Detta kan emellertid inte anses utgöra något problem. Enligt nu gällande lag får den som har brutit mot ett vitesförbud inte dömas till straff för en gärning som omfattas av förbudet (28 § andra stycket). Denna bestämmelse syftar just till att förhindra att flera sanktioner döms ut för samma gärning och är tillämplig även om det förfarande som vitesförbudet omfattar är straffbart enligt annan lag (prop. 2017/18:200 s. 179). Enligt artikel 4 i det sjunde tilläggs-

protokollet till den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna finns dock även ett förbud mot dubbla förfaranden. Högsta domstolen har därtill funnit att det för svenskt vidkommande är så att rättegångshinder föreligger om det redan påbörjats en process om samma sak, oavsett om denna avslutats (se rättsfallen NJA 2013 s. 502 och NJA 2015 s. 663, jfr även prop. 2017/18:165 s. 113 f.). Mot denna bakgrund kan det konstateras att det redan finns ett fullgott skydd mot dubbla sanktioner och dubbla förfaranden i detta sammanhang.

Avslutningsvis kan tilläggas att det inte finns tillräckliga skäl att överväga en kriminalisering för andra typer av förfoganden av företagshemligheter. I de fall någon vill göra information som den innehar lovligen till sin, t.ex. genom att kopiera och ta hem den men utan att utnyttja den är det en handling som ligger mycket nära ett legitimt och normalt handhavande av arbetsmaterial. En sådan kriminalisering är alltså inte önskvärd p.g.a. svåra gränsdragningsfrågor och får också anses bli alltför omfattande

Några ytterligare avgränsningar av de straffbara handlingarna behövs inte

Med hänsyn till de särskilda frågor som lyfts vid tidigare försök att kriminalisera utnyttjande och röjande av företagshemlighet finns det skäl att särskilt diskutera om de kriminaliserade gärningarna bör avgränsas så att det utökade straffansvaret blir mindre omfattande.

Ett möjligt alternativ är att låta kriminalisering av utnyttjande utgå och låta kriminaliseringen endast avse olovligt röjande av företagshemlighet av teknisk natur.

En sådan avgränsning skulle innebära att de mycket straffvärda gärningarna, som t.ex. ett röjande till en främmande makt som inte omfattas av spioneribestämmelsen, alltjämt skulle omfattas av straffansvar.

En sådan avgränsning skulle kunna göras ännu smalare. Det skulle då handla om att endast kriminalisera vissa former av röjande, t.ex. genom användande av vissa typer av informationsbärare.

Ett möjligt alternativ är att bestraffa den som uppsåtligen och olovligen röjer en företagshemlighet av teknisk natur, som han eller hon har fått del av i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution eller genom att delta i en

näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning, uppdrag eller på annan liknande grundgenom användande av handling, elektronisk fil, teknisk förebild, föremål, material eller ämne.

Ett typexempel på ”användande” i nu tänkt bemärkelse skulle vara att någon kopierar filer eller ritningar och röjer företagshemligheten genom att ge någon handlingen eller filen. Det torde även vara det praktiskt sett vanligaste tillvägagångssättet. Ett annat exempel på ”användande” skulle vara att för någon läsa upp handlingens innehåll och därigenom röja företagshemligheten. Men även ett sådant fall där någon skriver av handlingen och röjer företagshemligheten genom avskriften skulle föranleda sådant straffansvar. Tanken skulle alltså vara att handlingen, ritningen eller den aktuella dokumentationsformen har varit en nödvändig förutsättning vid röjandet av företagshemligheten. En ytterligare förutsättning skulle vara att handlingen, föremålet, materialet, ämnet eller den elektroniska filen innehåller företagshemligheten eller att den kan härledas från handlingen, föremålet, materialet, ämnet eller den elektroniska filen som har använts vid röjandet.

En sådan avgränsning skulle utesluta fall där en person utnyttjar kunskap som han eller hon har förvärvat vid normal yrkesutövning (jfr 2 § andra stycket). Även sådana fall där en person muntligt berättar om hemligheter utan hjälp av lagrad information skulle undantas från det straffbara området. Om någon läst en handling och har lagt den företagshemliga informationen på minnet och sedan röjer informationen, skulle gärningen inte omfattas av straffansvar. Begränsningen skulle i praktiken få betydelse för sådana fall där en person kan memorera den företagshemliga informationen; i annat fall behövs ett hjälpmedel. Dessa fall torde dock inte vara särskilt vanligt förekommande, även om de visar på den begränsning som ett sådant förslag har – det går att komma runt straffansvar genom att frigöra sig från hjälpmedel och memorera den kunskap som ska röjas.

Ett sådant straffansvar skulle rikta in sig på de absolut mest kvalificerade gärningarna i så måtto att röjande med hjälp av lagrad information förutsätter viss planering och ett hjälpmedel i form av en bärare av den lagrade informationen, såsom en handling. Det kan också antas att ett sådant röjande typiskt sett är mer skadligt eftersom det torde avse större mängder information. I praktiken torde

angrepp på mer värdefulla tekniska företagshemligheter ofta förutsätta att någon form av dokumentation utnyttjas eftersom minneskunskaper normalt inte räcker till.

Båda dessa alternativ, att endast kriminalisera röjande eller att endast kriminalisera röjande med hjälpmedel, har det gemensamt att de utesluter straffansvar för olovligt utnyttjande. Ett skäl som talar för att utesluta utnyttjande från det kriminaliserade området är att ett utnyttjande ofta torde avse en anställd som vill öppna en egen konkurrerande verksamhet. Detta sker åtminstone i vissa fall i mindre skala och kan då inte sällan antas leda till en mindre skada än ett röjande till en konkurrent eller liknande.

Något som dock talar för att låta det kriminaliserade området omfatta utnyttjande är att ett utnyttjande många gånger är en mer kvalificerad gärning än ett röjande. Ett utnyttjande torde kräva ett antal åtgärder och viss överläggning medan ett röjande kan ske oöverlagt och spontant. Sett till förfaringssättet kan alltså utnyttjande ofta vara mer klandervärt än ett röjande. Ett obehörigt utnyttjande innebär – liksom röjande – vidare att företagshemligheten hamnar utom innehavarens kontroll och medför i det avseendet en risk för skada, både vid hanteringen av företagshemligheten och vid spridning av produkter eller tjänster. Ett exempel på detta är att t.ex. varor som innehåller företagshemligheten görs tillgängliga för s.k. reverse engineering eller baklängeskonstruktion, där man analyserar eller plockar isär en befintlig produkt för att komma underfund med hur den är konstruerad. Själva utnyttjandet är vidare en gärning som typiskt sett kan medföra en ekonomisk skada för innehavaren.

En sådan smal avgränsning som beskrivits ovan skulle således utesluta straffansvar för flera klart klandervärda missbruk som typiskt sett medför risk för skada. I fråga om röjande som sker med ett hjälpmedel skulle ett sådant brott träffa en kategori av de mest klandervärda handlingarna. Samtidigt utesluts vissa ageranden som i dag anses så klandervärda att de kan utgöra synnerliga skäl för skadeståndsansvar (7 §). De nu diskuterade mer avgränsade alternativen till kriminalisering kan alltså inte anses vara effektiva i förhållande till syftet med kriminaliseringen.

Av dessa skäl görs bedömningen att det utvidgade straffansvaret ska omfatta såväl olovligt röjande som olovligt utnyttjande och att

någon annan begränsning av de kriminaliserade handlingarna inte bör införas.

6.3 Straffansvar ska gälla personer som deltar i innehavarens rörelse eller verksamhet

Förslag: Straffansvaret ska gälla den som har tillgång till den olovligt utnyttjade eller röjda företagshemligheten genom sitt deltagande i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund.

Skälen för förslaget

Straffansvar bör gälla för anställda, vissa uppdragstagare och andra som på liknande grund deltar i en näringsidkares rörelse…

Det finns som framgår ovan ett straffansvar för företagsspioneri för personer som olovligen bereder sig tillgång till företagshemligheter. Det som nu kommer i fråga är att utvidga ansvaret till personer som har lovlig tillgång till en företagshemlighet av teknisk natur och som röjer eller utnyttjar densamma. En sådan utvidgning innebär att hur hemlig information hanteras ges straffrättslig betydelse och inte, som i dag, endast hur informationen har anskaffats.

Det kan noteras att det i brottsbalken finns straffbestämmelser som kan få betydelse vid olika typer av klandervärd hantering av information. Dessa aktualiserar dock straffansvar under mer allmänna förutsättningar och är inte utformade specifikt för att ge ett ändamålsenligt skydd för företagshemligheter till vilka någon har lovlig tillgång. Det medför att gärningar som är straffvärda kan vara straffria på grund av omständigheter som saknar egentlig betydelse i relation till skyddet för företagshemligheter.

Ett exempel är trolöshet mot huvudman. Straffbestämmelsen omfattar den som på grund av förtroendeställning har fått till uppgift att sköta en ekonomisk angelägenhet för annan och som missbrukar förtroendeställningen till skada för huvudmannen (10 kap. 5 § brottsbalken). Skyddet som den straffbestämmelsen ger är

begränsat, eftersom långt ifrån alla anställda intar en sådan förtroendeställning som förutsätts för ansvar för trolöshet mot huvudman. I vissa fall kan tillgreppsbrotten i 8 kap. brottsbalken aktualiseras när det är fråga om tillgrepp av lösa saker av värde; ett sådant exempel kan vara en prototyp. En prototyp kan, vid sidan av ett potentiellt försäljningsvärde, representera ett stort värde som bärare av värdefull information. Även bestämmelserna om utpressning (9 kap. 4 § brottsbalken) kan aktualiseras vid t.ex. kapning av information. Även brott mot tystnadsplikt (20 kap. 3 § brottsbalken) skulle kunna aktualiseras.

Anställda och andra medarbetare måste många gånger få del av arbetsgivarens företagshemligheter för att kunna utföra sina arbetsuppgifter. Detta är också en av förklaringarna till att anställda har en lojalitetsplikt mot sin arbetsgivare. För innehavaren kan det dock vara svårt att skydda företagshemlig information från att användas illojalt. Detta har särskild betydelse om det är information av ekonomiskt eller annat värde och som därför är åtråvärd för konkurrenter och andra antagonister. Ett sätt för utomstående att komma åt information kan då vara att värva en intern informatör på företaget.

Det finns skäl att införa en kriminalisering som kan träffa sådana personkategorier som har tillgång till företagshemligheter under sådana omständigheter att det kan uppställas krav på att de inte ska bryta det förtroende som innehavaren av företagshemligheten har visat dem.

Även i 2013 års lagrådsremiss övervägdes vilka personer som bör omfattas av en kriminalisering av olovligt utnyttjande och olovligt röjande av företagshemlighet (2013 års lagrådsremiss s. 21 f.). De förslag och överväganden som då fördes fram är fortfarande ändamålsenliga och relevanta. Det finns skäl att bestämma omfattningen av den utvidgade kriminaliseringen i fråga om anställda och personer med en liknande ställning hos innehavaren utifrån i huvudsak samma riktlinjer som i det tidigare lagstiftningsärendet.

Ett utvidgat straffansvar bör sålunda omfatta den som genom sin anknytning till näringsidkaren – dvs. innehavaren av företagshemligheten – får anses delta i dennes rörelse. Detta kan förklaras med att dessa personer typiskt sett har lovlig tillgång till företagshemligheter och att dessa personer även får anses ha en typ av

lojalitetsplikt mot innehavaren av företagshemligheten (jfr direktivet artikel 4 tredje punkten c).

I första hand gäller det näringsidkarens egna anställda. Ansvaret bör också omfatta andra som har en motsvarande eller nästintill motsvarande insyn i företaget. Det kan vara t.ex. vissa uppdragstagare och personer som genom uthyrning eller utlåning från bemanningsföretag utför arbete åt näringsidkaren. Det kan också vara personer som medverkar i arbetsmarknadspolitiska program och studerande som genomför en längre praktikperiod eller utbildning förlagd till en arbetsplats. Näringsidkaren är på samma sätt som i fråga om anställda beroende av att dessa personer inte angriper företagshemligheter som de anförtros. En förutsättning för att någon ska omfattas av straffansvar bör dock vara att personen deltar i näringsidkarens verksamhet under omständigheter som liknar dem som förekommer i ett anställningsförhållande. Sådana omständigheter kan vara att arbetsförhållandet har viss varaktighet, att den som utför arbetet är underkastad näringsidkarens arbetsledning och kontroll samt att han eller hon fortlöpande ska ställa sin arbetskraft till förfogande.

Personer som utför tjänster av skilda slag och som har en lös koppling till näringsidkaren omfattas inte av en sådan beskrivning. Exempelvis berörs inte hantverkare med egen firma som självständigt utför installationer eller reparationer åt andra. Än mindre berörs personer som står helt utanför näringsidkarens rörelse, men som av olika skäl kommer i kontakt med företagshemligheter.

Bedömningen görs således att den utökade kriminaliseringen bör avse personer som deltar i näringsidkarens rörelse till följd av anställning eller uppdrag eller på annan liknande grund.

Det kan i sammanhanget påminnas om att en av förutsättningarna för att information ska anses vara en företagshemlighet är att innehavaren har vidtagit rimliga åtgärder för att hålla informationen hemlig. Den enskilde måste vidare ha uppsåt i förhållande till att det är fråga om hemlig information för att straffansvar ska kunna komma i fråga (se vidare i författningskommentaren). Den utvidgning av straffansvaret som föreslås får därför betydelse när innehavaren av företagshemligheten har vidtagit åtgärder för att dels hålla informationen hemlig, dels sett till att de som deltar i verksamheten förstår att informationen är hemlig. Kravet på innehavaren att vidta informationsåtgärder torde vara högre ställt i

förhållande till personer som inte har arbetstagares lojalitetsplikt eller som inte har kännedom om innehavarens verksamhet, t.ex. inhyrd personal, praktikanter och deltagare i arbetsmarknadspolitiska program.

… och i en forskningsinstitutions verksamhet

Tidigare förslag till kriminalisering av utnyttjande och röjande av företagshemlighet har inte omfattat företagshemligheter som innehas av forskningsinstitutioner. Läget är nu ett annat. Forskningsinstitutioner omfattas nämligen i och med nya lagen om företagshemligheter av samma skydd för sina företagshemligheter som näringsidkare (2 § och prop. 2017/18:200 s. 28).

Även vid universitet, högskolor och andra liknande institutioner finns värdefulla företagshemligheter. Som framkommit i avsnitt 5.2 förekommer det även att främmande makter använder sig av forskningsdelegationer för att komma åt åtråvärd information. Det finns alltså ett behov av utvidgat skydd för företagshemligheter även i sådana sammanhang. Det föreslås därför att de nya bestämmelserna ska omfatta också olovligt utnyttjande och röjande av anställda och andra som deltar i verksamheten vid forskningsinstitutioner. Även dessa personer kan komma i kontakt med företagshemligheter av teknisk natur och göra det under sådana omständigheter att det kan uppställas krav på att de inte ska bryta det förtroende som innehavaren av företagshemligheten har visat dem. Straffansvar bör därför gälla även den som fått del av företagshemligheten genom att delta i en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund.

Särskilt om bemanningsanställda

Det utvidgade straffansvaret gäller för bemanningsanställda på samma sätt som övriga som omfattas av det – avgörande är att det är fråga om ett deltagande i verksamheten eller rörelsen.

Bemanningsanställda är anställda av ett företag och hyrs sedan ut till ett annat företag. Den bemanningsanställde anses inte ha någon lojalitetsplikt mot det inhyrande företaget och har inte heller – i vart fall inte typiskt sett – någon nu relevant avtalsrelation till det in-

hyrande företaget. Detta särskiljer dem från arbetstagare och de flesta andra kategorier som omfattas av utvidgningen av straffansvaret, som normalt binds till innehavaren av företagshemligheten antingen genom anställningsavtal eller genom t.ex. uppdragsavtal.

Skadeståndsansvaret för anställda anses inte omfatta bemanningsanställda då de inte är arbetstagare i lagens mening (jfr 7 §). Någon bestämmelse som tar sikte på just bemanningsanställda finns inte utan de allmänna bestämmelserna om skadestånd får tillämpas, t.ex. om skadestånd vid brott. För bemanningsanställda innebär den nu föreslagna kriminaliseringen därför att skadeståndsansvaret utvidgas genom 5 §. Detta får anses vara motiverat.

Utvidgningen av skadeståndsansvaret för de bemanningsanställda kommenteras ytterligare nedan (se avsnitt 7).

Det bör inte ställas krav på samband mellan företagshemligheten och arbetsuppgifterna

En fråga att ta ställning till är om det bör ställas ett krav på ett samband mellan den utnyttjade eller röjda företagshemligheten och arbetstagarens arbetsuppgifter.

Det är straffbart som företagsspioneri när en anställd bereder sig tillgång till information som ligger klart utanför ramen för hans eller hennes arbetsuppgifter. Däremot gäller inte det straffansvaret då en anställd får del av överskottsinformation som finns tillgänglig på den del av arbetsplatsen där han eller hon normalt har rätt att uppehålla sig eller som finns i material som han eller hon använder i tjänsten. Inte heller omfattar det straffansvaret den som av en slump kommer över en företagshemlighet (se ovan avsnitt 3.3).

Företagshemligheter kan finnas dokumenterade i handlingar som den anställde av en händelse ser på arbetsplatsen. Företagshemligheter kan också komma på tal i en diskussion mellan kollegor som han eller hon råkar höra. Det kan röra sig om skyddsvärd information vars utnyttjande eller röjande i princip är lika klandervärt som ett utnyttjande eller röjande av information som låg inom ramen för den anställdes arbetsuppgifter.

Behovet av att skydda alla de företagshemligheter som finns inom en verksamhet talar mot att något krav på samband bör finnas mellan företagshemligheten och den egna arbetsuppgiften. Även om ett

sådant samband saknas får ett angrepp på företagshemligheten anses utgöra ett brott mot det förtroende som innehavaren av företagshemligheten har visat den person som deltar i verksamheten.

Även parallellen till de skadeståndsrättsliga reglerna talar för att något samband inte bör krävas. En arbetstagares skadeståndsansvar vid utnyttjande eller röjande av en företagshemlighet som arbetstagaren har fått del av i sin anställning är inte begränsat till företagshemligheter som angår tjänsten och som arbetstagaren behöver ha vetskap om för att fullgöra sina arbetsuppgifter, utan inkluderar alla företagshemligheter som omfattas av lojalitetsplikten (prop. 1987/88:155 s. 60 f.). Det är svårt att motivera att gränsen mellan tillåtet och otillåtet handlande dras annorlunda i fråga om straffansvar än när det gäller skadeståndsansvaret.

Sammanfattningsvis bör det alltså inte finnas något krav på samband mellan företagshemligheten och arbetsuppgifterna, utan deltagande i verksamheten är tillräckligt för att straffansvar ska bli aktuellt.

6.4 Straffansvar för gärningar efter att deltagandet har upphört ska förutsätta synnerliga skäl

Förslag: Som huvudregel ska det inte dömas till straffansvar om ett utnyttjande eller röjande sker efter att deltagandet i en näringsidkares rörelse eller forskningsinstitutions verksamhet har upphört. Endast om det finns synnerliga skäl ska straffansvar kunna komma i fråga.

Skälen för förslaget

Det straffrättsliga ansvaret bör motsvara det skadeståndsrättsliga ansvaret för arbetstagare

En utgångspunkt i lagen om företagshemligheter är att arbetstagaren efter anställningens upphörande är fri att utnyttja inte bara sin personliga skicklighet och sina egna erfarenheter, utan också information som utgör företagshemligheter hos den tidigare arbetsgivaren. Endast om det finns synnerliga skäl är ett utnyttjande eller

röjande av den tidigare arbetsgivarens företagshemligheter obehörigt och lagen överhuvudtaget tillämplig. Denna princip är dock dispositiv och gäller inte om arbetsgivaren och arbetstagaren avtalar annat, i t.ex. en sekretess- eller konkurrensklausul (prop. 2017/18:200 s. 147).

Principen kommer till uttryck i lagen om företagshemligheter genom stadgandet om arbetstagares skadeståndsskyldighet (7 §). Av paragrafens andra stycke framgår att om ett utnyttjande eller röjande har ägt rum sedan anställningen upphört gäller skadeståndsansvaret endast om det finns synnerliga skäl.

Synnerliga skäl får i allmänhet anses finnas då arbetstagaren har tagit anställning hos arbetsgivaren i syfte att komma över hemlig information eller då han eller hon under sin anställning har förberett ett överförande av hemlig information till en konkurrerande verksamhet. En omständighet som, kanske inte ensam men i förening med andra omständigheter, kan tala för att det finns synnerliga skäl är att den tidigare anställde har intagit en särskild förtroendeställning hos arbetsgivaren, exempelvis som verkställande direktör, produktionschef eller forskningschef. Det förhållandet att företagshemligheten har missbrukats med hjälp av dokumentation i någon form, exempelvis en teknisk förebild, är något som ofta talar för att det finns synnerliga skäl. En tidigare arbetstagare som använder sig av tekniska förebilder, ritningar, tekniska beskrivningar eller annan dokumentation som härrör från den tidigare arbetsgivaren och avser dennes företagshemligheter, bör i princip bli skadeståndsskyldig. Vid bedömningen har även skadans storlek en viss betydelse. Det kan normalt sett inte anses finnas synnerliga skäl om utnyttjandet eller röjandet endast i liten utsträckning har påverkat den tidigare arbetsgivarens konkurrensförmåga. En annan omständighet som kan tala mot ansvar är att arbetstagaren själv har utvecklat hemligheten hos sin tidigare arbetsgivare. I ett sådant fall kan det ofta finnas skäl att inte frångå huvudregeln om arbetstagarens frihet att utnyttja sin kunskap och erfarenhet på den öppna arbetsmarknaden (jfr prop. 1987/88:155 s. 46 och 61 samt bet. 1989/90:LU37 s. 41 f.; se även prop. 2017/18:200 s. 62 f.).

Bestämmelsen om arbetstagares skadeståndsansvar fanns redan i 1990 års lag och var i princip identisk med den nuvarande paragrafen. Det innebär att denna reglering har funnits och tillämpats, både rättsligt och faktiskt, under lång tid. Detta bidrar till förutsebarhet.

Det har inte heller framkommit något annat än att regleringen upprätthåller en rimlig balans mellan arbetstagarnas behov av att fritt kunna byta arbetsgivare och behovet hos innehavarna av företagshemligheter av att skydda sina företagshemligheter.

En liknande reglering föreslås därför gälla även i förhållande till den utvidgade kriminaliseringen.

I fråga om arbetstagare är en sådan regel i allt väsentligt att se som ett förtydligande då angrepp efter anställningens upphörande är behöriga, såvida det inte finns synnerliga skäl. Skadeståndsansvaret i dessa fall är också uttryckligen begränsat genom regeln i 7 § andra stycket. Om en arbetsgivare och en arbetstagare inte avtalar om annat är arbetstagaren efter anställningens upphörande förhindrad att utnyttja eller röja företagshemligheter som han eller hon fått del av i sin anställning endast om det finns synnerliga skäl (7 § andra stycket). I annat fall är utnyttjandet eller röjandet ett behörigt angrepp på företagshemligheterna (prop. 2017/18:200 s. 62 f. och 147).

När det gäller andra som deltar i rörelsen eller verksamheten motiveras deras straffansvar till stor del med de likheter som deras relation till näringsidkaren uppvisar med arbetstagares. Det är då rimligt att de behandlas på samma sätt i fråga om straffansvar efter att deltagandet i rörelsen har upphört. Dessa personers rörlighet på arbetsmarknaden är också viktig att värna. Även systematiska skäl talar för att bedöma samtliga personer som omfattas av straffbestämmelserna på samma sätt. De föreslagna reglerna om begränsningar i ansvaret för tiden efter det att grunden för deltagandet i verksamheten upphört föreslås därför gälla alla de personer som omfattas av straffbestämmelserna (jfr SOU 2008:63 s. 178 f.).

En sådan lösning har vidare den fördelen att man för alla som deltagit i rörelsen i stor utsträckning undviker svåra gränsdragningsfrågor i förhållande till vad som kan anses vara en företagshemlighet och vad som i stället är att anse som personlig skicklighet och egna erfarenheter (jfr 2 §), jfr SOU 2008:63 s. 90. Att låta den gränsdragningen få avgörande betydelse för avgränsningen av straffansvaret framstår inte som lämpligt.

2007 års utredning föreslog att det ska gälla ett krav på att gärningsmannen har agerat ”särskilt illojalt” i motsvarande straffrättsliga fall. Skälet var att det uttrycket ansågs mer informativt än

begreppet synnerliga skäl. Bedömningen gjordes att skadeståndsbestämmelsen för anställda (7 §) huvudsakligen tar sikte på särskilt illojala förfaranden för det fall angreppet skett efter anställningens slut (SOU 2008:63 s. 178).

Begreppet synnerliga skäl är etablerat sedan lång tid i lagen och det finns rättspraxis om dess innebörd. Det får anses vara en fördel att använda samma begrepp när samma typ av beteenden åsyftas. Även om begreppet särskilt illojalt agerande kan anses något mer informativt är detta knappast avgörande. Det finns också en risk för att särskilt illojalt agerande ges en snävare innebörd i rättspraxis än vad synnerliga skäl har. Det skulle i så fall innebära att klart klandervärda fall inte omfattas av ett straffansvar. Det kan vidare konstateras att begreppet synnerligen är ett vanligt kvalificerande begrepp i brottsbalken och att även begreppet synnerliga skäl förekommer där, om än inte i straffbestämmelser.

Det föreslås därför att undantaget från straffansvar när deltagandet i rörelsen eller verksamheten har upphört formuleras som ett krav på synnerliga skäl i överensstämmelse med motsvarande undantag från arbetstagares skadeståndsansvar.

I SOU 2008:63 föreslogs att straffansvar för gärningar begångna efter deltagandets upphörande ska inträda också för det fall det är fråga om ett grovt brott. Såsom lagen i dag kommit att tolkas är en sådan konstruktion inte möjlig. Det beror på att det är tveksamt om de grova brotten helt korresponderar med begreppet synnerliga skäl. Det kan vara fråga om ett handlande som i och för sig skulle kunna utgöra ett grovt brott på grund av omfattande skada, men som i det enskilda fallet inte skulle anses utgöra synnerliga skäl. I ett sådant fall är angreppet, om det begås av en arbetstagare, inte att se ens som ett obehörigt angrepp (prop. 2017/18:200 s. 62 och s. 147). Det skulle alltså inte omfattas av lagen överhuvudtaget och straffansvar enligt lagen vore därför uteslutet.

En situation som den ovanstående synes dock osannolik eftersom skadans storlek har en viss betydelse även vid bedömningen av om det finns synnerliga skäl. Det kan t.ex. också beaktas vem som tar emot den röjda eller utnyttjade företagshemligheten. Något som talar för att det finns synnerliga skäl kan då vara att mottagaren är den främsta konkurrenten i branschen eller främmande makt. Sådana mottagare kan antas kunna använda företagshemligheten på ett särskilt skadligt sätt. Det utrymme som synnerliga skäl ger för att

ingripa mot angrepp efter att ett deltagande i en rörelse eller verksamhet har upphört bedöms därför tillräckligt.

Det bör inte i lagen finnas någon fast tidsgräns för ansvaret

I 2013 års lagrådsremiss föreslogs att straffansvaret inte ska gälla om gärningen har begåtts senare än två år efter det att deltagandet i näringsidkarens rörelse har upphört. Detta motiverades bl.a. av att konkurrensklausuler i anställningsavtal inte är bindande i den mån de sträcker sig längre än vad som kan anses skäligt. I den då gällande 1969 års överenskommelse mellan vissa av arbetsmarknadens parter angående begränsning av användningsområdet för och innehållet i konkurrensklausuler i tjänsteavtal angavs att bindningstiden för en sådan klausul normalt inte bör överstiga just två år. Regeringen anförde också att företagshemligheter oftast har ett skyddsvärde som avtar med tiden. Ett straffrättsligt ansvar som är tidsmässigt obegränsat skulle därför inte bara kunna anses oskäligt ur arbetstagarens synpunkt, utan även onödigt från näringsidkarens och samhällets perspektiv (2013 års lagrådsremiss s. 25).

Att en företagshemlighets skyddsvärde som regel avtar med tiden innebär i förlängningen att ett röjande av informationen efter en viss tid inte längre är ägnat att orsaka innehavaren skada i konkurrenshänseende. Informationen är då inte längre skyddad som en företagshemlighet (2 §). Inte desto mindre kan vissa företagshemligheter, exempelvis tillverkningsprocesser och långsiktiga affärsstrategier, hållas hemliga och vara värdefulla under mycket lång tid (jfr rättsfallet NJA 1999 s. 469). En del företag ser skyddet för företagshemligheter som ett alternativ till att söka patent, något som bl.a. kan motiveras med att skyddet kan innebära ett potentiellt längre skydd än patentets tjugo år (prop. 2017/18:200 s. 105).

Till det sagda kommer att ett krav på synnerliga skäl för ansvar föreslås för gärningar som begås efter att ett deltagande i en rörelse eller verksamhet har upphört. Någon sådan begränsning föreslogs inte i 2013 års lagrådsremiss. Kravet på synnerliga skäl innebär att ansvaret i dessa situationer är reserverat för de mest skadliga handlingarna. Det saknas skäl att ytterligare begränsa ansvaret genom att införa en fast tidsgräns.

6.5 Straffansvar ska även gälla för den som ingår en affärsförbindelse med innehavaren av företagshemligheten

Förslag: Straffansvar ska gälla för den som haft lovlig tillgång till den olovligt utnyttjade eller röjda företagshemligheten genom att han eller hon har fått del av den i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution.

Skälen för förslaget: Det förekommer inte sällan att företagshemligheter utväxlas vid affärsförbindelser som innehavaren ingår med utomstående personer. En särskild fråga är därför om det är motiverat med ett straffansvar även för olovligt utnyttjande och röjande av företagshemligheter som någon har anförtrotts inom ramen för en sådan affärsförbindelse.

Ett straffansvar för affärsparters missbruk av företagshemligheter har behandlats i tidigare lagstiftningsärenden, bl.a. av 1979 års utredning om skydd för företagshemligheter, som lade fram förslaget till lagen om skydd för företagshemligheter. Den utredningen ansåg att straffansvar skulle drabba den som missbrukade en företagshemlighet som anförtrotts honom eller henne i samband med en affärsförbindelse (SOU 1983:52 s. 323 f.). Den dåvarande regeringen bedömde dock att en skadeståndssanktion var tillräcklig i dessa situationer. I propositionen framhölls att det inte är ovanligt i affärssammanhang att företagshemligheter delges motparten i större utsträckning än vad denne har behov av och är beredd att ta ansvar för. Det angavs vidare att det finns betydande skillnader mellan olika branscher när det gäller formerna för att anförtro företagshemligheter liksom i fråga om toleransen när det gäller utnyttjandet av dessa. Det angavs även att det kan vara svårt att placera det straffrättsliga ansvaret hos rätt person inom företaget. Avgörande för ställningstagandet var emellertid att respekten för avtal i största utsträckning borde vila på civilrättsliga regler (prop. 1987/88:155 s. 22 f.).

I SOU 2008:63 (s. 169 f.) framhölls att det såvitt framkommit inte var något stort problem att företagshemligheter som någon fått del av i samband med affärsförbindelser röjs eller utnyttjas obehörigt. Vidare framhöll utredningen att möjligheterna för ett

angripet företag att få ersättning för en skada i många fall var ganska goda eftersom företag vanligtvis har betalningsförmåga alternativt försäkringar som kan täcka ett skadeståndskrav och att skadeståndssanktionen fick anses fylla en effektiv preventiv funktion. Utredningen betonade också att en näringsidkare i ett affärssamarbete har möjlighet att i stor utsträckning välja vilka företagshemligheter som ska lämnas ut till en affärspart och att brister i riskbedömningen inför utlämnandet av en företagshemlig handling till en affärspart måste falla tillbaka på näringsidkaren själv. Utredningen ansåg att personer som har fått del av företagshemligheter i samband med en affärsförbindelse inte borde omfattas av ett utvidgat straffansvar (SOU 2008:63 s. 169 f.). Något förslag om straffansvar av det slaget lades inte fram i 2013 års lagrådsremiss eller av 2016 års utredning om skyddet för företagshemligheter.

Utgångspunkten är nu delvis en annan. Det straffansvar som nu föreslås är kvalificerat i det att det endast träffar utnyttjande och röjande av företagshemligheter av teknisk natur. Det finns i sådana fall – vid angrepp på kvalificerade företagshemligheter med anknytning till innovation och teknikutveckling – ett utökat skyddsbehov, och det handlande som nu föreslås kriminaliseras är skadligt inte bara för den enskilda innehavaren av en företagshemlighet utan för svenska innovationer och näringslivet i stort.

Att avgränsa det utvidgade straffansvaret så att det endast omfattar anställda och personer med en liknande ställning i företaget riskerar att leda till att straffvärda förfaranden då någon röjer eller utnyttjar en företagshemlighet som han eller hon har anförtrotts faller utanför det straffbara området. Ur innehavarens perspektiv kan det framstå som irrelevant huruvida hans eller hennes företagshemlighet olovligen angrips av en anställd eller om angreppet i stället utförs av en affärskontakt som har anförtrotts känslig information. Det kan i det sammanhanget konstateras att företag i olika branscher kan ha olika behov i fråga om personalförsörjning och därför kan organisera sig på olika sätt. Det kan påverka vilka typer av aktörer som behöver få del av företagshemligheter. Att möjligheten för innehavaren till ekonomisk ersättning typiskt sett är större i dessa fall talar inte emot att straffansvaret utvidgas, eftersom bestämmelserna även syftar till att skydda svenska innovationer och den sunda konkurrensen i allmänhet. Skyddsbehovet sträcker sig alltså längre än till att skydda enbart den enskilda innehavaren.

Detta gäller i synnerhet då affärsparten står i förbindelse med främmande makt eller någon som agerar för en sådan makts räkning. Det vore olyckligt om ett straffansvar inte omfattade även sådana fall då en affärspart röjer hemligheten till en främmande makt eftersom det då finns en risk att utländska underrättelseinsatser styrs om till affärsförbindelser med svenska företag. Som framgår ovan (avsnitt 5.2) har främmande makt under senare år visat större intresse för civila verksamheter och det förekommer även att underrättelsetjänster använder sig av bulvanföretag för att komma åt information. Det framstår därför som motiverat med ett förstärkt skydd mot statsstyrt industrispionage också då detta bedrivs i förhållande till information som företagen frivilligt delar i samband med affärsförbindelser.

Det bör även framhållas att regelverket blir mer lättillämpat när det utökade straffansvaret även omfattar fall då en affärspart olovligen utnyttjar eller röjer en företagshemlighet. Det kan nämligen i vissa fall vara tveksamt om en uppdragstagare kan sägas delta i näringsidkarens verksamhet under omständigheter som liknar dem som förekommer i ett anställningsförhållande och på den grunden omfattas av det utökade straffansvaret. Detta kommer dock normalt att sakna praktisk betydelse eftersom det i många fall bör stå helt klart att uppdragstagaren har ingått en affärsförbindelse med innehavaren och att straffansvar därför föreligger på den grunden. Av detta följer också att en sådan lösning ger bättre förutsättningar för att snarlika fall behandlas på samma sätt.

Personkretsen bör alltså motsvara den som omfattas av lagens skadeståndsansvar vid angrepp på företagshemligheter i samband med affärsförbindelser och således innefatta den som röjer en företagshemlighet hos en näringsidkare eller en forskningsinstitution som han eller hon i förtroende har fått del av i samband med en affärsförbindelse med näringsidkaren eller forskningsinstitutionen (jfr 6 §). Liksom vid bedömandet av skadeståndsansvaret bör det inte förutsättas att det finns ett bindande avtal mellan innehavaren av företagshemligheten och mottagaren, dvs. gärningsmannen. Redan under ett förhandlingsskede kan mottagaren ha fått del av företagshemligheten på ett sådant sätt att det får anses finnas ett förtroendeförhållande (prop. 1987/88:155 s. 42).

För arbetstagare och dem som liknar arbetstagare föreslås en begränsning av ansvaret för angrepp som sker efter att ett deltagande

i en rörelse eller verksamhet upphört. Det föreslås krävas synnerliga skäl för ansvar för denna personkategori, vilket knyter an till de överväganden som gjorts tidigare i fråga om intresset av att värna arbetstagares rörlighet. Något behov av ett liknande undantag vid affärsförbindelser finns typiskt sett inte och kan inte heller anses motiverat. Det föreslås därför inte något sådant undantag för angrepp som skett efter att en affärsförbindelse har upphört.

6.6 Straffansvaret bör inte utvidgas i fråga om styrelseledamöter eller revisorer i juridiska personer

Bedömning: Straffansvar bör inte gälla för styrelseledamöter eller revisorer i t.ex. aktiebolag som olovligen utnyttjar eller röjer uppdragsgivarens företagshemligheter.

Skälen för bedömningen: Styrelseledamöter och revisorer i t.ex. ett aktiebolag kan inom ramen för sina respektive uppdrag komma att ta del av företagshemligheter. Dessa har dock uttryckligen undantagits från skadeståndsansvar i lagen om företagshemligheter (10 § andra stycket, prop. 2017/18:200 s. 70 f., 153 och 159) och de omfattas inte heller av den skadeståndsparagraf som reglerar skadestånd i samband med affärsförbindelser (7 §).

Ovanstående har sin förklaring i att det i fråga om skadeståndsansvar för styrelseledamöter – från bolagsrättsliga utgångspunkter – ansetts som en enkel och ändamålsenlig ordning att skadeståndsansvaret regleras inom de associationsrättsliga regelverken. Det har även uttalats att det finns goda skäl för att i fråga om skadeståndsansvar inte göra skillnad på styrelseledamöterna och den valda revisorn i det aktuella bolaget (jfr bet. 1988/89:LU30 s. 30 f. och 39, bet. 1989/90:LU37 s. 33 och 43 samt prop. 2017/18:200 s. 70). Det samband som finns mellan skadeståndsansvaret för styrelseledamöter och revisorer kan också illustreras av att revisorers skadeståndsansvar enligt 29 kap. 2 § aktiebolagslagen knyter direkt an till skadeståndsansvaret för styrelseledamöter i 29 kap. 1 § aktiebolagslagen (2005:551).

En styrelseledamot eller revisor som angriper bolagets företagshemligheter kan dock bli föremål för andra skyddsåtgärder enligt lagen om företagshemligheter, t.ex. ett beslut om vitesförbud. I sammanhanget kan det också noteras att ett skadeståndsansvar kan uppkomma också för den som i ett senare led angriper den företagshemlighet som tidigare har angripits av en styrelseledamot eller revisor (prop. 2017/18:200 s. 71).

För revisorer finns vidare en tystnadsplikt enligt 26 § revisorslagen (2001:883). Om en revisor åsidosätter sina skyldigheter som revisor eller uppsåtligen gör orätt i sin revisionsverksamhet eller på annat sätt handlar oredligt, kan vidare disciplinära åtgärder vidtas av Revisorsinspektionen. Det kan då bli fråga om bl.a. varning, indragen auktorisation eller sanktionsavgift (32–35 §§ revisorslagen).

Det finns i dag ett antal straffbestämmelser som kan aktualiseras för styrelseledamöter och revisorer. Sådana finns bl.a. i aktiebolagslagen och lagen (2018:672) om ekonomiska föreningar. Dessa tar dock inte sikte på olovligt utnyttjande eller röjande av företagshemligheter, eller andra närliggande handlingar, utan på t.ex. uppsåtligt brott mot det s.k. spridningsförbudet (30 kap. 1 § aktiebolagslagen). Vid olovligt utnyttjande och röjande skulle dock ansvar för trolöshet mot huvudman enligt 10 kap. 5 § brottsbalken kunna aktualiseras. En sådan förtroendeställning som förutsätts för ansvar enligt paragrafen intar bl.a. styrelseledamöter och revisorer i aktiebolag. För dessa finns därmed redan ett straffansvar för det fall de missbrukar sin förtroendeställning och därigenom skadar huvudmannen.

Mot bakgrund av det breda skydd för företagshemligheter som finns i detta sammanhang samt de olika möjligheter till rättsliga sanktioner som redan i dag finns vad gäller styrelseledamöter och revisorer bedöms det inte finnas behov av ett utökat straffansvar för styrelseledamöter eller revisorer. Det finns också ett värde i att upprätthålla den valda modellen för att reglera dessa aktörers ansvar.

I förslaget undantas styrelseledamöter och revisorer genom kravet på deltagande i rörelsen eller verksamheten. En sådan funktionär kan nämligen inte genom att fullgöra sitt uppdrag anses uppfylla det kravet. Om en styrelseledamot däremot arbetar i bolaget kommer straffansvar kunna komma i fråga, men då på grund

av deltagandet i rörelsen och inte på grund av rollen som styrelseledamot.

6.7 Straffansvar ska förutsätta uppsåt

Förslag: Straffansvar vid olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet ska gälla enbart i uppsåtliga fall.

Skälen för förslaget: Utgångspunkten för nykriminaliseringen bör vara att endast uppsåtliga gärningar ska bestraffas. Olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet kan inte anses vara så allvarliga gärningar att även oaktsamhet ska bestraffas. I synnerhet i fråga om arbetstagare skulle en sådan reglering av straffansvaret vara för långtgående.

Denna slutsats ligger även i linje med det som gäller för företagsspionerі och olovlig befattning med företagshemlighet.

6.8 Ringa fall av gärningarna ska inte omfattas av straffansvar

Förslag: Ringa fall av olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet ska inte omfattas av straffansvar.

Skälen för förslaget: Till skillnad från de befintliga straffbestämmelserna omfattar nykriminaliseringen situationer där den enskilde har lovlig tillgång till företagshemligheten i fråga. Det finns i sådana situationer flera tänkbara omständigheter som kan göra att en gärning inte är så allvarlig att ett straffansvar framstår som motiverat. Det är även mycket angeläget att enskilda inte upplever sig förhindrade att använda och vidareutveckla de erfarenheter och kunskaper som de har förvärvat tidigare i yrkeslivet. En utvidgning av straffansvaret bör tillåtas att påverka detta i minsta möjliga mån och rörligheten på arbetsmarknaden bör skyddas.

Ringa fall av olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet bör därför inte vara straffbara.

Om en gärning är att anse som ringa eller inte bör avgöras efter en helhetsbedömning av samtliga omständigheter i det enskilda fallet. Om denna bedömning utmynnar i att gärningen som helhet framstår som bagatellartad, är den att bedöma som ringa. Vid bedömningen kan de omständigheter som utgör grunden för bedömningen av om ett brott är grovt tjäna till viss ledning. Således ska gärningens art beaktas, liksom det värde den avsett samt vilken skada gärningen inneburit.

Vad som bör anses vara ringa fall behandlas ytterligare i författningskommentaren (avsnitt 11.1).

6.9 Rubricering, straffskala och grova brott

Förslag: Brotten ska benämnas som olovligt utnyttjande av företagshemlighet respektive olovligt röjande av företagshemlighet. Straffskalan för respektive brott ska vara böter eller fängelse i högst två år. Om brottet är grovt, ska straffet vara fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.

Skälen för förslagen

Brotten ska benämnas olovligt utnyttjande av företagshemlighet respektive olovligt röjande av företagshemlighet

Det utvidgade straffansvaret omfattar vissa olovliga angrepp på företagshemligheter av teknisk natur. Närmast till hands ligger att benämna brotten olovligt utnyttjande av företagshemlighet respektive olovligt röjande av företagshemlighet. Även om kravet på att företagshemligheten är av teknisk natur inte framgår av dessa beteckningar, beskriver de på ett tydligt sätt det straffbara handlandet och beteckningarna bedöms därför som lämpliga.

Det föreslås att det ska vara fråga om två separata brottstyper som regleras i varsitt stycke, främst av det skälet att vissa andra

bestämmelser endast avser olovligt röjande av företagshemlighet (se t.ex. 27 § samt 27 kap. 2 § rättegångsbalken).

Straffskalan för olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet

De nya straffbestämmelserna har påtagliga likheter med varandra och med företagsspionerі. Samtliga avser ursprungliga angrepp på företagshemligheter och de kan även i fråga om gärningarnas allvar sägas vara likartade. Av dessa skäl bör straffskalan för de nya bestämmelserna vara densamma som för företagsspionerі och det bör även införas en särskild straffskala för de allvarligaste fallen.

Straffskalan för olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet bör alltså vara böter eller fängelse i högst två år. Om brottet är grovt, bör straffskalan vara densamma som vid företagsspionerі, grovt brott, dvs. fängelse i lägst sex månader och högst sex år.

Kvalifikationsgrunder för grovt brott

I fråga om företagsspionerі ska det vid bedömningen av om brottet är grovt särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada (26 §). Därvid ska hänsyn tas till omständigheterna i det enskilda fallet, bl.a. kan förfaringssättet och de värden som har utsatts för angreppet beaktas (prop. 1987/88:155 s. 39).

I de tidigare förslagen till straffansvar för gärningar bestående av olovligt utnyttjande eller röjande av företagshemlighet har det ansetts att de ovan omnämnda omständigheterna ska beaktas även vid bedömningen av om ett olovligt utnyttjande av företagshemlighet eller olovligt röjande är att anse som grovt brott.

Det är naturligt att samma omständigheter ska beaktas även vid bedömningar av om ett olovligt utnyttjande eller röjande utgör ett grovt brott. Detta har att göra med brottstypernas likartade natur. De angivna omständigheterna är vidare sådana som förekommer även i andra straffbestämmelser, t.ex. i bestämmelserna om grov stöld (8 kap. 4 § brottsbalken), grovt bedrägeri (9 kap. 3 § brottsbalken) och grov förskingring (10 kap. 3 § brottsbalken). Vid

bedömningen av om ett olovligt utnyttjande eller röjande utgör ett grovt brott bör det alltså särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.

Vad som bör anses vara ett grovt brott utvecklas närmare i författningskommentaren (avsnitt 11.1).

6.10 Försök och förberedelse till brott ska vara straffbart

Förslag: Försök och förberedelse till olovligt röjande av företagshemlighet respektive olovligt utnyttjande av företagshemlighet ska straffbeläggas.

Skälen för förslaget: Försök och förberedelse till brott regleras i 23 kap. 1 och 2 §§ brottsbalken. Ansvar förutsätter ett särskilt stadgande där det anges att den aktuella brottstypen är kriminaliserad på försöks- eller förberedelsenivå.

Försök till brott består i att någon har påbörjat utförandet av visst brott utan att detta kommit till fullbordan. Därutöver krävs att fara har förelegat för att handlingen ska leda till brottets fullbordan, eller att sådan fara varit utesluten av tillfälliga omständigheter. För straffansvar krävs även uppsåt till det fullbordade brottet.

Ansvar för förberedelse till brott kräver att en förberedelsegärning har företagits. En sådan gärning kan bestå antingen i att någon tar emot eller lämnar pengar eller annat som betalning för brottet eller för att täcka kostnader för utförande av brottet, eller att någon skaffar, tillverkar, lämnar, tar emot, förvarar, transporterar, sammanställer eller tar annan liknande befattning med något som är särskilt ägnat att användas som hjälpmedel vid brottet. Ytterligare förutsättningar är att gärningsmannen inte har fullbordat brottet eller gjort sig skyldig till ett straffbart försök till samma brott samt att det finns mer än ringa fara för att brottet ska fullbordas och att gärningen med hänsyn till andra omständigheter inte är mindre allvarlig. Vidare krävs att gärningsmannen har uppsåt att utföra eller främja brottet.

Redan ett försök eller en förberedelse till ett olovligt utnyttjande eller ett olovligt röjande av företagshemlighet är typiskt sett en så

allvarlig gärning att ett straffansvar bör kunna aktualiseras under de förutsättningar som stipuleras i 23 kap. brottsbalken. Brottsligheten föregås ofta av planering och förberedande åtgärder, något som gör att det är särskilt angeläget att möjliggöra ett tidigt ingripande. Det är också av att yttersta vikt att det finns möjlighet att avbryta ett pågående förlopp innan skada uppstått och att det även under sådana omständigheter finns möjlighet att lagföra den skyldige. De nya brotten bör alltså, i likhet med företagsspioneri, vara straffbara också på försöks- och förberedelsestadiet.

6.11 Den föreslagna kriminaliseringen är balanserad och rättssäker

Bedömning: Den föreslagna kriminaliseringen sker inom ramen för den avvägning av motstående intressen som gjorts i lagen. Den är vidare grundlagsenlig. De begränsningar som den medför i fråga om bl.a. yttrandefrihet och informationsfrihet för arbetstagare och andra personkategorier bedöms vara godtagbar. Straffbestämmelsernas utformning möjliggör en rättssäker tillämpning.

Skälen för bedömningen

Den föreslagna regleringen upprätthåller balansen mellan olika intressen

Frågan om hur långtgående ett nytt straffansvar bör vara har lyfts i olika sammanhang. Lagrådet ifrågasatte exempelvis om det i 2013 års lagrådsremiss redovisats tillräckliga skäl för en så omfattande nykriminalisering som där föreslogs.

Inledningsvis kan det klargöras att den nu föreslagna kriminaliseringen utgår från den existerande lagen och dess systematik. De begränsningar som gäller i dag kommer också att fortsätta gälla.

Straffansvar omfattar utnyttjande eller röjande av teknisk information som innehavaren vidtagit åtgärder för att hemlighålla. Det förutsätts att ett röjande eller utnyttjande är ägnat att leda till skada i konkurrenshänseende (jfr 2 och 3 §§).

Om angreppet inte är obehörigt kan inga sanktioner enligt lagen om företagshemligheter komma i fråga (4 §). En intresseavvägning ska göras för att bedöma om ett angrepp är obehörigt.

Straffansvar förutsätter att ovan nämnda omständigheter är uppfyllda och att de även omfattas av gärningsmannens uppsåt.

Straffansvaret föreslås vidare inte omfatta ringa gärningar. Från straffansvar undantas även som huvudregel utnyttjande och röjande efter att deltagandet i rörelsen eller verksamheten upphört; endast om det finns synnerliga skäl kan personen i fråga straffas.

Omfattningen av den föreslagna kriminaliseringen är avsevärt mindre i jämförelse med tidigare förslag om utvidgad kriminalisering på området. Detta beror på att kommersiella företagshemligheter inte omfattas av de föreslagna straffbestämmelserna. I praktiken är utnyttjande av en kundlista en av de vanligaste formerna av angrepp. Begränsningen av straffansvaret utesluter ansvar för sådana angrepp, vilket torde ha stor betydelse för hur många angrepp som i praktiken kommer att falla inom straffansvaret. Det innebär också att många angrepp som framstår som mindre allvarliga faller utanför straffbestämmelsernas tillämpningsområde.

Som utvecklats tidigare får ett sådant röjande eller utnyttjande av en företagshemlighet som uppfyller förutsättningarna för straffansvar anses utgöra klandervärda och farliga handlingar. De krav som brukar ställas upp för en kriminalisering är uppfyllda (se ovan avsnitt 5.1 och 6.1–6.5).

Sammanfattningsvis görs bedömningen att den balans mellan olika motstående intressen som upprätthålls av lagen inte rubbas av de lagförslag som nu läggs fram.

Den föreslagna kriminaliseringen är väl avvägd i förhållande till yttrandefriheten och informationsfriheten

Den nu föreslagna kriminaliseringen är begränsad på flera sätt. Om meddelar- eller anskaffarfriheterna är tillämpliga på röjandet av en företagshemlighet gäller lagen om företagshemligheter överhuvudtaget inte för uppgiftslämnandet. Detta gäller givetvis också i förhållande till nykriminaliseringen. Vidare gäller meddelarskyddslagen framför lagen om företagshemligheter (prop. 2016/17:31 s. 38 f.).

I sammanhanget är det viktigt att ha i åtanke att uppgifter om förekommande brottsliga eller från samhällets synpunkt annars helt

oacceptabla förhållanden överhuvudtaget inte är att anse som företagshemligheter (2 §). Ibland hävdas det t.ex. att friheten att avslöja missvisande information från ett bolag om en produkt skulle kunna begränsas. Ett sådant röjande är dock inte straffbart då sådan information inte skyddas som en företagshemlighet eftersom lagen endast skyddar information som påverkar konkurrensförmågan negativt när innehavaren konkurrerar på marknaden med sådana konkurrensmedel som är förenliga med sund konkurrens (jfr Lagrådets yttrande över lagrådsremiss den 12 december 2013 med förslag till lag om ändring i lagen (1990:409) om skydd för företagshemligheter [protokoll vid sammanträde den 8 januari 2014]).

Av intresse är vidare den begränsning som innebär att behöriga angrepp är straffria (4 §). Som tidigare har berörts anses angrepp alltid som behöriga om de sker för att offentliggöra eller inför en myndighet eller ett annat behörigt organ avslöja något som antingen skäligen kan misstänkas utgöra brott med fängelse i straffskalan eller som kan anses utgöra något annat missförhållande. Det förutsätts att offentliggörandet eller avslöjandet sker till skydd för allmänintresset. Även andra angrepp kan anses som behöriga och därmed vara undantagna från lagens tillämpningsområde. Begränsningen till obehöriga angrepp syftar just till att möjliggöra en avvägning mellan intresset av att upprätthålla skyddet för företagshemligheter och intresset av att värna andra viktiga samhällsintressen (se vidare i avsnittet nedan).

Även med beaktande av ovanstående begränsningar utgör den kriminalisering som nu föreslås en begränsning av yttrandefriheten och informationsfriheten eftersom det handlar om en straffsanktion som träffar både visst anskaffande av information och visst meddelande av information.

Som framkommit tidigare har kriminaliseringen betydelse för att skydda svenska intressen, men den syftar i huvudsak till att skydda företag och forskningsinstitutioner inom ramen för deras näringsverksamhet. Detta får anses vara ett sådant särskilt viktigt skäl som kan föranleda begränsning av yttrandefriheten och informationsfriheten (jfr uttalandet om att undantaget för upphovsrätten är att hänföra till denna punkt, prop. 1975/76:209 s. 155). Som anges i avsnitt 6.1 och 6.2 bedöms den föreslagna kriminaliseringen vara nödvändig och avgränsad på ett sådant sätt att den endast träffar

avsedda och straffvärda fall. Bedömningen görs alltså att de nu föreslagna straffbestämmelserna är proportionerliga och förenliga med regeringsformen. Förslaget är också förenligt med Europakonventionen och EU:s stadga.

Det kan också påminnas om att det vid sidan av lagen om företagshemligheter finns arbetsrättsliga regler som i praktiken har större betydelse för arbetstagares rätt att offentligt framföra kritik mot arbetsgivaren eller mot förhållanden på arbetsplatsen. Med anställningsavtalet följer exempelvis en lojalitetsplikt för arbetstagaren. Denna innebär att arbetstagaren inte får vidta åtgärder som är ägnade att skada eller på annat sätt försvåra arbetsgivarens verksamhet. Med lojalitetsplikten följer bl.a. en tystnadsplikt. Om den anställde bryter mot lojalitetsplikten, kan det i vissa fall utgöra saklig grund för uppsägning. Detta förhållande kan förklaras av bl.a. repressalieförbudet enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen inte gäller i ett privaträttsligt förhållande utan endast i förhållande till en myndighet eller ett annat allmänt organ. Som tidigare har påpekats har dock staten enligt Europakonventionen en viss positiv förpliktelse att skydda privatanställda från angrepp på deras yttrandefrihet från privaträttsliga subjekt och vidare uppställs begränsningar av 4 §, visselblåsarlagen och god sed på arbetsmarknaden.

I förhållande till de arbetstagare som berörs av förslaget om utökad kriminalisering gör sig nu i princip inte några andra hänsyn gällande än de som beaktades av lagstiftaren när det gällande straffansvaret, för bl.a. företagsspionerі, utformades. Det kan dock hävdas att den nu föreslagna straffbestämmelsen om olovligt röjande av företagshemlighet kan medföra att det uppstår en osäkerhet om hur gränsdragningar ska ske i praktiken och att det i sin tur kan komma att leda till att arbetstagare självcensurerar.

Risken för att det föreslagna straffansvaret för röjande leder till sådana konsekvenser får emellertid bedömas som liten. Det beror dels på att straffansvaret knyter an till en befintlig struktur som skyddar yttrandefriheten och arbetstagares allmänna kritikrätt, dels på att det knyter an till befintliga sanktioner, som skadestånd, vite och arbetsrättsliga sanktioner. Exempel på det senare är att en arbetstagare som uppsåtligen eller av oaktsamhet angriper en företagshemlighet hos arbetsgivaren som han eller hon fått del av i sin anställning under sådana förhållanden att han eller hon insåg eller

borde ha insett att den inte fick avslöjas ska ersätta den skada som uppkommer genom förfarandet (7 §). Under de trettio år som denna ordning har gällt har det inte heller framkommit, t.ex. med anledning av rättsfall, att detta har orsakat problem eller verkat hämmande på arbetstagarnas yttrandefrihet (jfr Fahlbeck, R, Reinhold, Lagen om företagshemligheter – en kommentar, Norstedts Juridik 2019, s. 108 samt SOU 2017:45 s. 68).

För att straffansvar ska aktualiseras krävs vidare att det är fråga om ett uppsåtligt olovligt utnyttjande eller röjande och att det inte är fråga om ett ringa brott. Det finns alltså ingen risk för straffansvar då en arbetstagare av oaktsamhet röjer företagshemligheter och inte heller då angreppet får anses bagatellartat.

Sammantaget görs alltså bedömningen att den föreslagna kriminaliseringen är väl avvägd också i förhållande till yttrandefriheten, informationsfriheten och arbetstagarnas allmänna kritikrätt. Förslagen bedöms även vara i enlighet med unionsrätten i övrigt och då särskilt med artikel 1.1 i direktivet om företagshemligheter.

Den föreslagna regleringen möjliggör en rättssäker tillämpning

Centralt för att avgränsa ansvaret är begränsningen till företagshemligheter av teknisk natur. Till skillnad från tidigare förslag förutsätter det inte en skälighetsbedömning utan ger tvärtom relativt fasta hållpunkter för bedömningen. Det är särskilt viktigt med tanke på att lagen innehåller flera begrepp som förutsätter en bedömning. På så sätt undviker förslaget överlappande bedömningar där samma omständigheter värderas i olika led för att fastställa ett straffansvar.

Vidare föreslås att ringa gärningar ska vara undantagna från straffansvar (se avsnitt 6.8). Denna typ av bedömning är mycket vanlig inom straffrätten och får därför anses ge förutsättningar för en rättssäker tillämpning av straffbestämmelserna.

En fråga som har lyfts tidigare är de svårigheter som orsakas av lagens systematik. Som framgår ovan har detta beaktats vid utformningen av förslaget för att regleringen som helhet ska bli godtagbar. De nämnda svårigheterna med anledning lagens systematik ska heller inte överdrivas. Det kan påminnas om att det på flera håll inom straffrätten finns regleringar som förutsätter flera komplexa

bedömningar. Så måste det också vara. Ett exempel är brottstypen trolöshet mot huvudman, 10 kap. 5 § brottsbalken. För straffansvar ska det röra sig om en person som på grund av förtroendeställning, fått i uppgift att för annan sköta en ekonomisk angelägenhet eller självständigt hantera en kvalificerad teknisk uppgift alternativt övervakar en sådan angelägenhet eller uppgift. Därutöver förutsätts att personen i fråga missbrukar sin förtroendeställning och därigenom orsakar huvudmannen skada. De svårigheter som kan uppstå med anledning av detta är dock inte svårare än att de har kunnat hanteras inom den praktiska rättstillämpningen. Samma bedömning görs i fråga om nykriminaliseringen av utnyttjande och röjande av företagshemligheter av teknisk natur.

Den föreslagna kriminaliseringen bedöms därför ha en acceptabel utformning, även sett till lagen i övrigt.

6.12 Åtalsplikt ska gälla för olovligt utnyttjande av företagshemlighet samt olovligt röjande av företagshemlighet

Bedömning: Det bör inte införas någon särskild åtalsprövningsregel.

Skälen för bedömningen: Brotten företagsspionerи och olovlig befattning med företagshemlighet ligger under allmänt åtal. Några begränsningar av åklagarens rätt att väcka åtal för dessa brott finns inte. Detta innebär att åklagaren är skyldig att åtala när det framkommit tillräckliga skäl för åtal. 2016 års utredning om skyddet för företagshemligheter föreslog att samma ordning skulle gälla även för olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet (SOU 2017:45 s. 363 f.). Under remissbehandlingen riktades vissa invändningar mot förslaget. Bland annat Åklagarmyndigheten ansåg att förutsättningarna för åtal möjligen borde övervägas ytterligare. Myndigheten framhöll att det inte kunde uteslutas att det kan uppstå situationer där en näringsidkare inte vill medverka i en utredning om brott mot en anställd och att det då kan ifrågasättas om det är rimligt och försvarbart utifrån den allmänna åtalsplikten att driva en sådan förundersökning. En

bestämmelse om att åtal får ske endast efter angivelse av näringsidkaren eller motsvarande skulle därför enligt Åklagarmyndigheten kunna övervägas.

Frågan är då vilka principer som ska gälla för åtal av de nu föreslagna brottstyperna olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet.

Det kan på ett allmänt plan noteras att den förhärskande principen är att det ska finnas en absolut åtalsplikt. I och med att allt fler beteenden har kriminaliserats har dock även antalet åtalsprövningsregler ökat. Det har från lagstiftaren uttalats olika skäl för undantag från den absoluta åtalsplikten. Skäl som har anförts är brottets ringa betydelse, särskilda omständigheter när brottet begås och särskilda omständigheter hos den misstänkte, liksom processekonomiska skäl. Hänsyn till målsägandens situation har också anförts som skäl för särskilda åtalsprövningsregler, men även som argument mot sådana. Rättsväsendets bristande resurser samt behovet av att kunna göra prioriteringar har också kommit att anföras som ett skäl mot en absolut åtalsplikt (Landström, L, Åklagaren som grindvakt (diss), Iustus 2011, s. 138 f. och 206 f.).

Frågan kan även ses i ljuset av de immaterialrättsliga straffbestämmelsernas åtalsprövningsregler. Åtalsprövningsreglerna i de immaterialrättsliga lagarna har nyligen ändrats så att åklagare får väcka allmänt åtal för brott endast om åtalet är motiverat från allmän synpunkt. Det innebär att målsägandeangivelse i sig varken är en förutsättning för åtal eller ensamt kan leda till en skyldighet för åklagaren att väcka åtal. I flera av de immaterialrättsliga lagarna innebär förändringen vidare att kravet på att åtal av särskilda skäl ska vara motiverat från allmän synpunkt har sänkts (prop. 2019/20:149 s. 34 f). Lagändringarna trädde i kraft den 1 september 2020.

De immaterialrättsliga brottstyperna har vissa likheter med brottstyperna i lagen om företagshemligheter och de skäl som kan anföras för åtalsprövningsregler är till viss del desamma.

Om en åtalsprövningsregel övervägs för olovligt utnyttjande och olovligt röjande av företagshemlighet gör sig följande synpunkter gällande. Att de grova brotten har en straffskala som löper upp till sex års fängelse talar för att åtalsfrågan inte bör vara beroende av en målsägandeangivelse (jfr prop. 2019/20:149 s. 35). Att det både för grova brott och brott av normalgraden vidare får anses finnas systemhotande inslag talar också för att brotten är av sådant allvar

att åtalsfrågan inte bör vara beroende av målsägandens vilja att ange brottet till åtal. Den kvarvarande frågan blir då om ett krav på att åtal ska vara motiverat från allmän synpunkt skulle fylla en värdefull funktion vid olovligt utnyttjande och olovligt röjande av företagshemlighet. I sådant fall ska, liksom annars vid den bedömningen, hänsyn tas till vilken brottslighet det närmare rör sig om, vilket syfte lagföringen kan ha och vilka omständigheter som förelåg vid brottets förövande. Även målsägandens åsikt i frågan skulle kunna beaktas.

Det som talar för en sådan regel om åtalsprövning är främst att målsäganden kan ha ett intresse av att inte offentliggöra sina förehavanden och att skydda företagshemligheten i fråga. Det finns dock regler om sekretess som syftar till att skydda målsäganden från den typen av konsekvenser, se t.ex. 36 kap. 2 § offentlighets- och sekretesslagen (2009:400). Det finns även en reglering som innebär ett ytterligare skydd i form av skadeståndsansvar för den som röjer en företagshemlighet som denne har fått del av i samband med en rättegång (8 §). Det kan dock inte uteslutas att det kan komma att uppstå situationer där målsäganden inte vill medverka. Detta kan dock inte sägas vara något särskilt utmärkande för just dessa brottstyper. I praktiken torde vidare ett olovligt röjande eller utnyttjande av företagshemligheter inte komma till myndigheters kännedom utan insats från målsäganden.

Det finns samtidigt flera skäl som talar mot en regel om åtalsprövning för olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet. Det straffansvar som nu föreslås är mer begränsat än det som lades fram av 2016 års utredning i det att ansvaret endast gäller för angrepp på företagshemligheter av teknisk natur. Det utvidgade straffansvaret gäller för de gärningar där behovet av kriminalisering är som störst, i förhållande till de företag och forskningsinstitutioner som drabbas men även för förutsättningarna för innovation och företagande i stort. Själva brottstyperna är alltså sådana till sin konstruktion att de omfattar gärningar som typiskt sett är av allmänt intresse. I de fall det är fråga om brottslighet med koppling till statsstyrt spionage är detta förstås särskilt tydligt.

De nu förslagna straffbestämmelserna ska även ses i sitt sammanhang. För företagsspionerи och olovlig befattning med företagshemlighet finns som tidigare nämnts inga särskilda åtalsprövnings-

regler. Det finns stora likheter mellan företagsspionerі och olovligt utnyttjande eller röjande av företagshemlighet – dels är de straffbelagda gärningarna mycket likartade, dels torde de ofta förekomma i samma sammanhang. Gränsen är inte heller helt klar. Exempelvis kan en anställd begå företagsspionerі och olovligt röjande av företagshemlighet mot samma målsägande genom att först olovligen bereda sig tillgång till företagshemlig information från en annan avdelning än den där hon eller han själv jobbar och sedan röja den informationen tillsammans med företagshemlig information som han eller hon har lovlig tillgång till på den egna avdelningen. Skillnaden mellan dessa brott kan ofta vara liten.

Utifrån straffskalorna kan det även konstateras att olovlig befattning med företagshemlighet är ett mindre allvarligt brott än olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet. Det vore motsägelsefullt att införa en åtalsprövningsregel för ett mer allvarligt brott, när ett mindre allvarligt brott i samma lag inte är behäftad med en sådan regel. Även detta talar mot att införa särskilda åtalsprövningsregler endast för olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet.

Det kan i detta sammanhang särskilt nämnas att det inte heller har framkommit skäl för att införa åtalsprövningsregler för företagsspionerі eller olovlig befattning med företagshemlighet. Mot denna bakgrund kan det också sägas att en ytterligare fördel med en liktydig reglering är att lagen som helhet blir mer lättillgänglig.

Sett till hur få åtal gällande företagsspionerі som hanteras i rättsväsendet i dag, torde en åtalsplikt för olovligt utnyttjande eller röjande av företagshemlighet inte heller innebära någon märkbar skillnad i arbetsbörda hos polis, åklagare, domstolar eller inom kriminalvården.

Sammanfattningsvis bedöms de skäl mot en åtalsprövningsregel som redogjorts för ovan väga tyngre, främst då behovet av att i lagen om företagshemligheter ha en sammanhållen reglering av åtalsprövningsreglerna. Det ska därför inte införas en särskild åtalsprövningsregel för olovligt utnyttjande och röjande av företagshemlighet.

6.13 Straffskyddet för olovlig befattning med företagshemlighet ska stärkas

Förslag: Den som anskaffar en företagshemlighet av teknisk natur med vetskap om att den tillhandahålls, eller tidigare har tillhandahållits, genom ett sådant röjande som avses i straffbestämmelsen om olovligt röjande av företagshemlighet ska dömas för olovlig befattning med företagshemlighet, under förutsättning att röjandet inte är fritt från ansvar.

Skälen för förslaget: I dag kan den som anskaffar en företagshemlighet som har åtkommits genom en gärning bestående i företagsspionerі dömas för olovlig befattning med företagshemlighet (27 §).

Enligt 1931 års lag krävdes att den som tagit befattning med företagshemligheten hade tagit emot den direkt från den som hade begått förbrottet. I och med införandet av lagen om skydd för företagshemligheter togs det kravet bort och i stället infördes ett subjektivt krav på vetskap; gärningsmannen skulle ha vetskap om det föregående företagsspionerіet och om det fanns mellanhänder eller inte var inte längre av intresse för ansvarsfrågan (prop. 1987/88:155 s. 25). Även enligt nu gällande lag krävs att gärningsmannen har vetskap om att den som tillhandahåller hemligheten eller någon före den personen i sin tur har berett sig tillgång till denna genom en sådan gärning som avses i straffbestämmelsen om företagsspionerі. Kravet på vetskap innebär att straffansvar förutsätter insiktsuppsåt till denna omständighet (jfr prop. 2015/16:78 s. 69). Att observera är dock att ansvar för olovlig befattning med företagshemlighet kan komma i fråga även när den person som begått förbrottet inte döms för företagsspionerі utan enbart ett annat brott enligt brottsbalken på grund av att gärningen där är belagd med strängare straff. Det förutsätter att själva gärningen är att betrakta som ett företagsspionerі.

Frågan är om ett ansvar för olovlig befattning med företagshemlighet också bör gälla den som anskaffar en företagshemlighet som har varit föremål för olovligt röjande.

I situationer när ett anskaffande skett genom en annan person, t.ex. i form av att denne har röjt en företagshemlighet, kan det bli

aktuellt att överväga ett ansvar för ett osjälvständigt brott för den som tar emot företagshemligheten. Beroende på omständigheterna kan den som tar emot företagshemligheten tänkas göra sig skyldig till försök, förberedelse eller medverkan till ett visst brott. Exempelvis kan en mottagare av en röjd företagshemlighet tänkas ha utfört handlingar som kan innebära medverkan till företagsspionerі, t.ex. genom anvisningar eller transport. Det är också tänkbart att det skulle kunna bli fråga om förberedelse, försök eller medverkan till dataintrång, utpressning eller något annat förmögenhetsbrott enligt brottsbalken. Även straffansvar för häleri enligt 9 kap. 6 § 1 eller 2 eller häleriförseelse enligt 9 kap. 7 § brottsbalken kan komma i fråga. Detta förutsätter dock att de övriga kraven enligt paragraferna är uppfyllda, t.ex. i fråga om typ av förbrott eller kravet på näringsverksamhet enligt 9 kap. 6 § andra stycket brottsbalken (jfr prop. 1987/88:155 s. 24).

Det kan dock förekomma situationer där mottagaren inte omfattas av straffansvar enligt andra bestämmelser, trots att dennes gärning är sådan att den kan medföra påtaglig skada eller fara. Ett sådant exempel är att mottagaren inte har uppsåt i förhållande till det brott som han eller hon objektivt sett medverkar till. Som angavs i samband med införandet av lagen om skydd för företagshemligheter finns även andra skäl som talar för en särskild paragraf om olovlig befattning med företagshemlighet, bl.a. behovet av att anpassa rättsläget till de övriga nordiska länderna (jfr prop. 1987/88:155 s. 24 och 14).

Mot denna bakgrund finns det skäl för att straffansvaret för olovlig befattning med företagshemlighet ska gälla även i förhållande till den som tar emot en sådan hemlighet som tidigare har varit föremål för en gärning bestående i olovligt röjande av företagshemlighet. Också den som i ett senare led tar emot hemligheten med vetskap om förbrottet bör kunna bestraffas.

Straffansvaret bör dock inte omfatta den som anskaffar en företagshemlighet som varit föremål för ett olovligt röjande som ansetts som ringa och därför straffritt. Detsamma gäller om den föregående gärningen skulle vara straffri på grund av att röjandet skett efter att deltagande har upphört och det inte finns synnerliga skäl. Finns inget förbrott ska inte ansvar för olovlig befattning med företagshemlighet komma i fråga. I subjektivt hänseende bör det inte krävas att den som olovligen befattar sig med företags-

hemligheten har vetskap om att de ansvarsbefriande omständigheterna enligt 26 a § andra stycket inte föreligger. Det bör vara tillräckligt att denne har likgiltighetsuppsåt i förhållande till de omständigheter som innebär att det olovliga röjandet t.ex. inte är att anse som ringa.

Det får bedömas från fall till fall enligt allmänna principer om brottskonkurrens huruvida mottagaren bör bestraffas för olovlig befattning med företagshemlighet eller som medverkande till olovligt röjande av företagshemlighet eller något annat brott.

Straffskalan för olovlig befattning med företagshemlighet är böter eller fängelse i högst två år eller, om brottet är grovt, fängelse i högst fyra år. Den nuvarande straffskalan bör gälla även för de nu aktuella efterföljande angreppen. Straffmaximum för olovligt utnyttjande och olovligt röjande av företagshemlighet föreslås bli fängelse i högst sex år. I samband med att straffminimum för grova fall av företagsspionerи höjdes behandlades även straffskalan för olovlig befattning. Regeringen fann då att det saknades skäl för att lägga fram förslag om ytterligare förändringar av straffskalorna (se prop. 2017/18:200 s. 119–122). Det finns inte heller nu anledning att göra en annan bedömning och t.ex. föreslå att straffskalan för olovlig befattning med företagshemlighet görs till samma som för företagsspionerи.

Det kan avslutningsvis tilläggas att det inte kan bli aktuellt att överväga ett straffansvar för olovlig befattning med företagshemlighet vid ett föregående utnyttjande av en företagshemlighet. Detta har att göra med att en företagshemlighet inte kan anskaffas genom enbart ett föregående utnyttjande, utan det krävs en ytterligare gärning, såsom ett röjande, för att det ska röra sig om anskaffande enligt 27 §.

7 Ett utvidgat skadeståndsansvar för den som olovligen utnyttjar eller röjer en företagshemlighet

Förslag: Den som begår olovligt utnyttjande av företagshemlighet eller olovligt röjande av företagshemlighet ska ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten annars utnyttjas eller röjs.

Skälen för förslaget: I lagen om företagshemligheter finns flera bestämmelser om skadestånd, t.ex. för angrepp i samband med en affärsförbindelse (6 §) eller för angrepp mot en arbetsgivares företagshemlighet (7 §). Skadeståndsansvaret omfattar då endast den skada som uppkommit genom förfarandet (se dock 10 § som föreskriver ett mer omfattande ansvar vid anskaffande av företagshemlighet).

Skadeståndsansvaret på grund av brott är mer omfattande än vid andra skadliga handlingar. Det omfattar inte bara den skada som gärningsmannen orsakat genom det brottsliga förfarandet utan också den skada som uppstått till följd av hans eller hennes eller någon annans utnyttjande eller röjande av företagshemligheten (prop. 1987/88:155 s. 41 f. och 58).

Det finns skäl att likställa de nya brottstyperna med övriga brottstyper i fråga om skadestånd. Det förstärker det preventiva inslaget i regelverket och förbättrar möjligheten för innehavaren av företagshemligheten att få full kompensation för sin skada.

Det föreslås därför att skadeståndsskyldigheten på grund av brott enligt lagen ska gälla också för skadegörande handlingar som omfattas av de nya straffbestämmelserna (se 5 §). Den som gör sig skyldig till olovligt utnyttjande av företagshemlighet eller olovligt

röjande av företagshemlighet blir därmed skadeståndsansvarig inte bara för den skada som utnyttjandet eller röjandet orsakar utan även skada som uppkommer genom att företagshemligheten annars utnyttjas eller röjs. Beträffande de nya brottstyperna torde det då främst vara fråga om skada med anledning av utnyttjande eller röjande av en annan person.

En sådan lösning får större praktisk betydelse för bemanningsanställda än för arbetstagare. Det beror på att den förra kategorin inte i dag omfattas av skadeståndsansvaret enligt lagen om företagshemligheter. De kan dock, vid sidan av vanliga regler om skadestånd, omfattas av villkor om skadestånd i kollektivavtal eller anställningsavtal. Den avtalsgrundade skadeståndsskyldigheten gäller emellertid inte i förhållande till en skadelidande tredje man utan endast i förhållande till den egna arbetsgivaren (dvs. det uthyrande företaget). Förslaget utvidgar och tydliggör skadeståndsansvaret för denna grupp. En sådan förändring får anses motiverad.

Genom att det införs ett skadeståndsansvar för den som begår brottet olovligt utnyttjande av företagshemlighet eller olovligt röjande av företagshemlighet blir överlappningen mellan skadeståndsansvaret enligt 5 § och annat skadeståndsansvar enligt lagen något större. En anställd som olovligen utnyttjar eller röjer arbetsgivarens företagshemligheter kan alltså bli skadeståndsskyldig enligt både 5 och 7 §§. Motsvarande gäller enligt 6 § för en affärspart som olovligen utnyttjar eller röjer en företagshemlighet som han eller hon har tagit emot i förtroende. Som redan har påpekats är dock skadeståndsansvaret på grund av brott mer vidsträckt än annat skadeståndsansvar enligt lagen, eftersom det omfattar även skada som uppstår på grund av att företagshemligheten annars utnyttjas eller röjs. Den överlappning som i och för sig finns torde därför inte orsaka några tillämpningsproblem.

8 Beslag och hemliga tvångsmedel vid olovligt röjande av företagshemlighet

8.1 Företagsspioneri och hemliga tvångsmedel

Statsstyrt företagsspioneri

I lagen om företagshemligheter kriminaliseras företagsspioneri. I många fall är dock reglerna om tvångsmedel och andra utredningsåtgärder endast tillämpliga om det är fråga om en viss typ av kvalificerat företagsspioneri, så kallat statsstyrt företagsspioneri.

Statsstyrt företagsspioneri innebär att främmande makt bedriver spionage mot svenska företag med avsikt att få tillgång till företagshemligheter. Till skillnad från traditionellt spionage, som syftar till att underminera ett lands säkerhet, är företagsspioneriets motiv främst att skaffa ekonomisk vinning och inhämta teknisk kunskap (se vidare i avsnitt 5.2).

De personer som deltar i spioneriverksamhet är ofta välutbildade underrättelseofficerare som tränats och understöds av främmande makt. Dessa personer är i allmänhet mycket säkerhetsmedvetna vilket gör brottsligheten svår att upptäcka och förhindra (se prop. 2018/19:86 s. 88 f.). Det förekommer även att sådana personer jobbar under täckmantel i t.ex. bulvanföretag eller forskningsdelegationer. Hotbilden är komplex och främmande makt använder stora resurser för att tillskansa sig information av olika slag. Det är därför av mycket stor vikt att myndigheter och rättsväsendet har goda och effektiva möjligheter att motarbeta sådant spioneri.

Om beslag och hemliga tvångsmedel

Beslag och hemliga tvångsmedel regleras i 27 kap. rättegångsbalken.

Huvudregeln enligt 27 kap. 1 § rättegångsbalken är att föremål som skäligen kan antas ha betydelse för utredning om brott, vara avhänt någon genom brott eller förverkat på grund av brott får tas i beslag. Detsamma gäller föremål som skäligen kan antas ha betydelse för utredning om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken. Med föremål avses som utgångspunkt även skriftliga handlingar.

Skriftliga meddelanden mellan en misstänkt och en närstående till honom eller henne eller mellan sådana närstående inbördes undantas från möjligheten till beslag. Detta utgör det s.k. beslagsförbudet (27 kap. 2 § första stycket rättegångsbalken) Med närstående avses den krets av personer som i sin egenskap av närstående till en part inte är skyldiga att avlägga vittnesmål enligt 36 kap. 3 § rättegångsbalken, t.ex. make, maka, sambo, föräldrar eller syskon.

Beslagsförbudet för närstående är inte absolut och gäller inte vid förundersökningar om allvarlig brottslighet eller viss brottslighet som anses samhällsfarlig. Detta framgår av 27 kap. 2 § andra stycket 1–7 rättegångsbalken, som föreskriver att sådant beslag det nu är fråga om får göras dels vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, dels vid förundersökning om vissa samhällsfarliga brott som specificeras i paragrafen eller försök, förberedelse eller stämpling till sådana brott. Exempel på sådan samhällsfarlig brottslighet är sabotage, uppror och terroristbrott. Även företagsspioneri återfinns bland dessa brott (punkt 6). För att bestämmelsen ska aktualiseras krävs att det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning (s.k. statsstyrt företagsspioneri).

Av de paragrafer som reglerar användningen av hemliga tvångsmedel (27 kap. 18–20 e §§ rättegångsbalken) framgår att hemliga tvångsmedel får användas bl.a. i de fall som anges i 27 kap. 2 § andra stycket 2–7 rättegångsbalken. Regleringen om de hemliga tvångsmedlen, som presenteras närmare nedan, hänvisar alltså till regleringen om undantaget från beslagsförbudet.

För samtliga hemliga tvångsmedel gäller att de får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som

åtgärden innebär för den misstänkte eller för något annat motstående intresse, den s.k. proportionalitetsprincipen. Samtliga hemliga tvångsmedel kan användas vid förundersökning om statsstyrt företagsspionerі. Det finns även möjlighet att använda hemlig övervakning av elektronisk kommunikation vid grovt företagsspionerі, utan att det är fråga om statsstyrt företagsspionerі (jfr 27 kap. 19 § rättegångsbalken och 26 § lagen om företagshemligheter).

Hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § rättegångsbalken innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet. Tvångsmedlet får som utgångspunkt användas vid en förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år samt vid förundersökning om vissa särskilt angivna samhällsfarliga brott.

Hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § rättegångsbalken innebär att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress eller elektroniska kommunikationsutrustningars geografiska placering. Hemlig övervakning av elektronisk kommunikation får som utgångspunkt användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, samt vid förundersökning om vissa särskilt angivna samhällsfarliga brott.

Hemlig kameraövervakning enligt 27 kap. 20 a § rättegångsbalken innebär att bl.a. fjärrstyrda TV-kameror kan användas för optisk personövervakning vid förundersökning i brottmål, utan att upplysning om övervakningen lämnas. Tvångsmedlet får som utgångspunkt användas vid en förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år samt vid förundersökning om vissa särskilt angivna samhällsfarliga brott.

Hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken innebär avlyssning eller upptagning som görs i hemlighet med ett tekniskt hjälpmedel och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till. Huvudregeln är att hemlig rums-

avlyssning, på grund av tvångsmedlets ingripande karaktär, får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år samt i vissa i paragrafen särskilt angivna fall. Vid förundersökning om företagsspionerі krävs för användning av hemlig rumsavlyssning att det kan antas att brottet inte leder till endast böter.

Användning av hemliga tvångsmedel enligt preventivlagen

Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) får tillstånd ges till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och kvarhållande av försändelse om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar viss i lagen angiven brottslighet. Sådant tillstånd får också meddelas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet. Lagen förutsätter inte att ett brott har begåtts eller att förundersökning inletts och reglerar således tvångsmedelsanvändning i underrättelseverksamhet.

Tvångsmedlet måste vara av synnerlig vikt för att förhindra sådan brottslighet som lagen omfattar och skälen för åtgärden måste uppväga det intrång eller men i övrigt som åtgärden innebär för den som tillståndet avser eller för något annat motstående intresse (5 §).

Lagen omfattar exempelvis brottslighet som innefattar sabotage, mordbrand, flygplatssabotage, uppror, spionerі och terroristbrott. Lagen omfattar även brottslighet som innefattar företagsspionerі, om det finns anledning att anta att den brottsliga verksamheten kommer att utövas på uppdrag av eller understödjas av en främmande makt eller av någon som kommer att agera för en främmande makts räkning.

Användning av hemliga tvångsmedel enligt inhämtningslagen

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) reglerar Polismyndighetens, Säkerhetspolisens och Tullverkets möjligheter att i underrättelseverksamhet hämta in uppgifter om elektronisk kommunikation. Lagen reglerar enbart inhämtning från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Den ger alltså inte stöd för de brottsbekämpande myndigheterna att hämta in uppgifter med hjälp av egna tekniska hjälpmedel.

De uppgifter som får hämtas in med stöd av lagen är historiska uppgifter om meddelanden och om elektroniska kommunikationsutrustningars geografiska placering.

Uppgifter får hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år samt om den brottsliga verksamheten särskilt räknas upp i lagen. Uppgifter får bara hämtas in om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse (2 §).

Lagen omfattar exempelvis brottslighet som innefattar sabotage, brott mot medborgerlig frihet och spionerі. Lagen omfattar även brottslighet som innefattar företagsspionerі, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understöds av en främmande makt eller av någon som agerar för en främmande makts räkning.

Hemlig dataavläsning

Lagen (2020:62) om hemlig dataavläsning trädde i kraft den 1 april 2020 och är tidsbegränsad till en tid av fem år. Hemlig dataavläsning är ett nytt hemligt tvångsmedel som kan användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll. Tvångsmedlet innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart

informationssystem. Ett sådant system innefattar all slags utrustning som kan användas för att kommunicera elektroniskt, t.ex. datorer, mobiltelefoner, läsplattor, interaktiva högtalare, servrar, smarta klockor och annan liknande utrustning. Det kan också vara fråga om t.ex. ett användarkonto till en kommunikationstjänst eller lagringstjänst (prop. 2019/20:64 s. 211 och 212).

Tillstånd till hemlig dataavläsning får beviljas för att läsa av olika slags uppgifter, vilka i stor utsträckning motsvarar sådana uppgifter som får hämtas in med övriga hemliga tvångsmedel. Det kan alltså bli fråga om att hämta in kommunikationsövervakningsuppgifter, platsuppgifter, kameraövervakningsuppgifter samt rumsavlyssningsuppgifter (1 och 2 §§ lagen om hemlig dataavläsning). Dessutom får tillstånd till hemlig dataavläsning beviljas för att läsa av eller ta upp uppgifter som finns lagrade i ett avläsningsbart informationssystem och uppgifter som visar hur ett avläsningsbart informationssystem används. Detta är uppgifter som tidigare inte kunnat hämtas in löpande eller i hemlighet utan att beslut om beslag fattats.

Regleringen om hemlig dataavläsning överensstämmer således till stor del med den som gäller befintliga tvångsmedel. Den stora skillnaden är att avläsningen eller upptagningen av uppgifterna inom ramen för hemlig dataavläsning får göras i det avläsningsbara informationssystemet, dvs. i exempelvis en dator, mobiltelefon eller en elektronisk kommunikationstjänst. Detta kan ge tillgång till uppgifter innan de blir föremål för kryptering, något som inte är tillåtet för övriga hemliga tvångsmedel (se prop. 2019/20:64 s. 69–71).

Tillstånd till hemlig dataavläsning får som huvudregel beviljas under en förundersökning om åtgärden är av synnerlig vikt och förundersökningen gäller brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller vid förundersökning om brott som avses i 27 kap. 2 § andra stycket 2–7 rättegångsbalken. Dessutom får tillstånd beviljas vid misstanke om försök, förberedelse eller stämpling till sådan brottslighet samt vid misstanke om annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år. För tillgång till rumsavlyssningsuppgifter uppställs dock samma krav som vid hemlig rumsavlyssning enligt rättegångsbalken, dvs. brott med ett minimistraff om fyra år samt viss annan särskilt angiven brottslighet.

Hemlig dataavläsning får också användas i underrättelseverksamhet, under samma förutsättningar och för att få tillgång till samma slags uppgifter som i preventivlagen respektive inhämtningslagen med de begränsningar som framgår av lagen om hemlig dataavläsning (7, 8 och 10 §§ lagen om hemlig dataavläsning). För tillstånd till hemlig dataavläsning krävs dock när det gäller inhämtning att åtgärden är av synnerlig vikt, till skillnad från inhämtningslagen där kravet är särskild vikt.

Hemliga tvångsmedel får i dag användas i fråga om statsstyrt företagsspionerі

I slutet av 00-talet utökades möjligheterna att använda hemliga tvångsmedel vid utredning av misstanke om företagsspionerі och det finns i dag möjlighet att använda samtliga hemliga tvångsmedel vid utredning av misstanke om företagsspionerі. En förutsättning är dock att det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som agerat för en främmande makts räkning (se 27 kap. 18–20 e §§ rättegångsbalken). I underrättelseverksamhet är kraven att det finns anledning att anta att så kommer ske (1 § första stycket 6 preventivlagen samt 2 § första stycket 6 inhämtningslagen). Detta krav på koppling till främmande makt gäller dock inte för användning av hemlig övervakning av elektronisk kommunikation under förundersökning om grovt företagsspionerі (27 kap. 19 § rättegångsbalken och 26 § lagen om företagshemligheter).

I fråga om utredning av statsstyrt företagsspionerі uttalade den dåvarande regeringen att det statsstyrda företagsspionerіet kan få allvarliga ekonomiska konsekvenser för svenska företag och i förlängningen för svenska samhällsintressen som är avgörande för välståndet. Man ansåg även att brottsligheten kan försämra förutsättningarna att utveckla och bibehålla skyddet för landets säkerhet och det ansågs också i praktiken vara svårt att dra någon klar gräns mellan sedvanligt spionerі och statsstyrt företagsspionerі. Som en följd av detta fick bekämpandet av det statsstyrda företagsspionerіet anses ingå i Säkerhetspolisens kärnverksamhet. Det fanns därför ett behov av en utvidgad möjlighet till tvångsmedelsanvändning vid utredningar om sådan brottslighet genom

införandet av lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott (prop. 2007/08:163 s. 55).

I ett senare lagstiftningsärende infördes en liknande reglering i preventivlagen. Som skäl för att utvidga den preventiva tvångsmedelsanvändningen till skydd mot statsstyrt företagsspionerі anfördes bl.a. att statsstyrt företagsspionerі ofta har ett väsentligt högre straffvärde än andra fall av företagsspionerі och, särskilt på ett tidigt stadium, ofta kan vara svårt att skilja från andra spioneribrott. Det anfördes även att sådana brott som är av systemhotande karaktär intar en särställning och att hemliga tvångsmedel i sådana fall kan vara ett särskilt värdefullt verktyg (prop. 2013/14:237 s. 88 f. och 114 f.).

Därefter har det blivit möjligt att få tillstånd att hämta in uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspionerі också enligt inhämtningslagen. Regeringen framhöll att inhämtningslagen inte innehåller något krav på att inhämtningen ska kunna kopplas till en viss person och att sådan informationsinhämtning är särskilt ägnad att identifiera det okända hotet genom att identifiera okända aktörer och bedöma vilket hot de utgör. Det ansågs stå klart att det fanns ett reellt behov, t.ex. för Säkerhetspolisen, av att kunna inhämta uppgifter enligt inhämtningslagen beträffande brottslig verksamhet som innefattar statsstyrt företagsspionerі (prop. 2018/19:86 s. 89 f.).

8.2 Hemliga tvångsmedel under en förundersökning om statsstyrt olovligt röjande av företagshemlighet

Förslag: Vid förundersökning om statsstyrt olovligt röjande av företagshemlighet ska förbudet mot att ta skriftliga meddelanden mellan den misstänkte och närstående i beslag inte gälla.

Det ska finnas möjlighet att använda hemliga tvångsmedel enligt bestämmelserna i rättegångsbalken och i lagen om hemlig dataavläsning vid en förundersökning om statsstyrt olovligt röjande av företagshemlighet. Den som har utsatts för hemliga tvångsmedel ska inte omfattas av rätten att underrättas om tvångsmedelsanvändningen.

Skälen för förslaget: De intressen som gör sig gällande vid olovligt röjande av företagshemlighet är i princip desamma som vid företagsspioneri (se ovan), när det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning. Ett statsstyrt olovligt röjande av företagshemlighet har sådana likheter med sedvanligt spioneri och statsstyrt företagsspioneri att det är motiverat att likställa brottstyperna när det gäller möjligheten till beslag och undantaget från det s.k. beslagsförbudet.

Såsom rättegångsbalken är uppbyggd innebär en sådan utformning av reglerna om beslag att reglerna om hemliga tvångsmedel i 27 kap. rättegångsbalken och i lagen om hemlig dataavläsning kommer att vara tillämpliga i förhållande till statsstyrt olovligt röjande av företagshemlighet. Så bör det också vara.

När det gäller frågan om proportionalitet kan det till en början noteras att straffskalan för olovligt röjande av företagshemlighet föreslås vara böter eller fängelse i högst två år. Vid grovt brott föreslås straffet vara fängelse i minst sex månader och högst sex år. Det är alltså samma straffskala som i fråga om företagsspioneri och således ett brott som bedöms lika allvarligt. Det är samtidigt fråga om en relativt vid straffskala som ska täcka in en mängd olika förfaranden. Det framstår dock som osannolikt att den undre delen av skalan skulle komma att användas i fråga om ett statsstyrt olovligt röjande av en företagshemlighet. Vidare ska en bedömning av åtgärdens proportionalitet i det konkreta fallet alltid göras i fråga om användning av tvångsmedel. Vid en sådan prövning får brottets allvar mycket stor betydelse. Om straffvärdet då kan antas vara så lågt att det framstår som oproportionerligt att använda tvångsmedlet, ska så inte ske.

Möjligheten att meddela tillstånd till hemlig rumsavlyssning vid en utredning om olovligt röjande av företagshemlighet bör – i likhet med vad som gäller i fråga om företagsspioneri – begränsas till fall där det kan antas att brottet leder till annan påföljd än böter. Det säkerställer att respekten för den enskildes integritet upprätthålls i mindre allvarliga fall.

I fråga om underrättelse till enskild som har varit föremål för ett hemligt tvångsmedel bör samma undantag från underrättelse-

skyldigheten gälla som vid statsstyrt företagsspioneri (27 kap. 33 § rättegångsbalken). Skälen för att undanta olovligt röjande av företagshemlighet får nämligen anses vara lika starka som i fråga om företagsspioneri. Som en följd av detta gäller inte heller underrättelseskyldigheten vid hemlig dataavläsning enligt 28 § lagen om hemlig dataavläsning.

8.3 Tvångsmedel enligt preventivlagen och lagen om hemlig dataavläsning vid statsstyrt olovligt röjande av företagshemlighet

Förslag: Användning av hemliga tvångsmedel enligt preventivlagen och lagen om hemlig dataavläsning ska kunna ske vid påtaglig risk för brottslig verksamhet som innefattar statsstyrt olovligt röjande av företagshemlighet.

Skälen för förslaget: Statsstyrt företagsspioneri finns i preventivlagens brottskatalog sedan 2015. Det förhållandet att det för användning av tvångsmedel enligt preventivlagen i sådana fall krävs att en främmande makt ska ligga bakom brottsligheten ansågs enligt regeringen innebära en betydande begränsning av de situationer där tvångsmedel kommer att kunna användas för att förhindra företagsspioneri. Behovet av utvidgad tvångsmedelsanvändning vid statsstyrt företagsspioneri ansågs i huvudsak detsamma som vid sedvanligt spioneri. Regeringen pekade också på att de omständigheter som gör statsstyrt företagsspioneri särskilt svårt att utreda innebär att brottsligheten också är särskilt svår att upptäcka och förhindra. Enligt regeringens mening vägde behovet och den förväntade nyttan av tvångsmedlen i detta fall tyngre än integritetsintresset hos dem som kunde komma att drabbas av tvångsmedlen. Regeringen föreslog därför att hemliga tvångsmedel ska kunna tillåtas för att förhindra brottslig verksamhet som innefattar statsstyrt företagsspioneri (prop. 2013/14:237 s. 88 och s. 114 f.).

Liksom när det gäller statsstyrt företagsspioneri finns det starka skäl att tillåta hemliga tvångsmedel om det behövs för att förhindra ett olovligt röjande av företagshemlighet. Alla de skäl som anfördes för att inkludera företagsspioneri i brottskatalogen i preventivlagen

gör sig gällande även vad gäller olovligt röjande av företagshemlighet. Ett krav för användning av tvångsmedel ska, såsom vid påtaglig risk för företagsspionerі, vara att det finns anledning att anta att den brottsliga verksamheten kommer att utövas på uppdrag av eller understödjas av en främmande makt eller av någon som kommer att agera för en främmande makts räkning. Genom ändringen i preventivlagen kommer det att vara möjligt att i motsvarande situationer ansöka om tillstånd till hemlig dataavläsning.

Det bör betonas att en bedömning av åtgärdens proportionalitet alltid ska göras i det konkreta fallet när frågan om tillstånd till hemliga tvångsmedel prövas (5 § 2 lagen om åtgärder för att förhindra vissa särskilt allvarliga brott). Att det blir möjligt att i preventivt syfte tillåta hemliga tvångsmedel i fråga om den nya brottstypen innebär alltså inte att tvångsmedelsanvändning tillåts helt oberoende av straffvärdet i det enskilda fallet (jfr prop. 2013/14:237 s. 90).

8.4 Inhämtning av uppgifter enligt inhämtningslagen vid statsstyrt olovligt röjande av företagshemlighet

Förslag: Inhämtning av uppgifter enligt inhämtningslagen och lagen om hemlig dataavläsning ska kunna ske om det är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar statsstyrt olovligt röjande av företagshemlighet. För hemlig dataavläsning ska det i dessa fall krävas att åtgärden är av synnerlig vikt.

Skälen för förslaget: Sedan den 1 oktober 2019 omfattas även statsstyrt företagsspionerі av inhämtningslagen. Detta motiverades bl.a. med att det redan i skedet innan en förundersökning om statsstyrt företagsspionerі har inletts är möjligt att använda de betydligt mer integritetskänsliga tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning och att det ur ett systematiskt perspektiv kan anses rimligt och logiskt att statsstyrt företagsspionerі även omfattas av den särskilda inhämtningsmöjligheten enligt inhämtningslagen. Säkerhetspolisens behov av uppgifter om elektronisk kommunikation i underrättelse-

verksamheten har inte ansetts i tillräcklig utsträckning tillgodoses genom möjligheten till hemlig övervakning av elektronisk kommunikation enligt preventivlagen, som kräver att det finns en koppling till en specifik person eller grupp. I inhämtningslagen finns det inte något sådant krav på att inhämtningen ska kunna kopplas till en viss person. Sådan informationsinhämtning har ansetts särskilt ägnad att tillgodose vissa behov hos Säkerhetspolisen, t.ex. att identifiera det okända hotet genom att identifiera okända aktörer och bedöma vilket hot de utgör (prop. 2018/19:86 s. 89).

Motsvarande argument gör sig gällande även i fråga om statsstyrda former av den nya brottstypen olovligt röjande av företagshemlighet. Behovet och den förväntade nyttan av att använda tvångsmedlet kan antas överväga de integritetsintrång som tvångsmedlet kan innebära. Det bör därför införas en möjlighet till inhämtning av de uppgifter som avses i inhämtningslagen också om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar statsstyrt olovligt röjande av företagshemlighet.

Genom ändringen i inhämtningslagen kommer det att vara möjligt att i motsvarande situationer ansöka om tillstånd till hemlig dataavläsning. För att den åtgärden ska beviljas krävs dock att den är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges ovan.

8.5 Det finns inte skäl att tillåta hemliga tvångsmedel vid olovligt utnyttjande av företagshemlighet

Bedömning: Det bör inte införas motsvarande möjligheter att använda hemliga tvångsmedel i fråga om brottet olovligt utnyttjande av företagshemlighet.

Skälen för bedömningen: Den utvidgade kriminaliseringen omfattar både olovligt utnyttjande och olovligt röjande av företagshemlighet. Genom den nu gällande regleringen i rättegångsbalken och den föreslagna straffskalan för olovligt utnyttjande av företagshemlighet, grovt brott, kommer det vara möjligt att använda tvångs-

medlet hemlig övervakning av elektronisk kommunikation (27 kap. 19 § första stycket 1 rättegångsbalken) under förundersökning om grovt olovligt utnyttjande av företagshemlighet.

Det praktiska behovet av att låta även olovligt utnyttjande av företagshemlighet av normalgraden omfattas av möjligheterna till hemliga tvångsmedel enligt rättegångsbalken och preventivlagen och möjligheten till inhämtning av uppgifter enligt inhämtningslagen får anses vara mycket litet. Detsamma gäller i fråga om hemlig dataavläsning.

En tänkbar situation skulle vara att en främmande makt understöder att en anställd bedriver en med arbetsgivaren konkurrerande rörelse genom att olovligen utnyttja dennes företagshemligheter. Det skulle i ett sådant fall kunna vara fråga om att den anställde tillverkar den substans eller skapar den kod som den främmande makten efterfrågar. För det fall den anställde avser att lämna ut den företagshemliga informationen till t.ex. främmande makt kan dock gärningen anses innefatta även förberedelse eller försök till annat brott, t.ex. olovligt röjande av företagshemlighet eller spionerі. På så sätt kan handlingen – i de verkligt skyddsvärda fallen – ändå komma att omfattas av den nu aktuella lagstiftningen. Något praktiskt behov av en mer omfattande reglering kan därför inte förutses.

En utvidgad tvångsmedelsanvändning innebär vidare en ingripande maktutövning från statens sida i förhållande till den enskilde. Möjligheter till sådan maktutövning ska inte införas om det inte finns mycket starka skäl. Några sådana skäl har inte framkommit i fråga om brottstypen olovligt utnyttjande av företagshemlighet. En möjlighet till hemlig tvångsmedelsanvändning bör därför inte gälla i dessa fall.

8.6 Den föreslagna användningen av beslag och hemliga tvångsmedel är förenlig med skyddet för den personliga integriteten

Bedömning: Den föreslagna utvidgningen av tillämpningsområdet för beslag och hemliga tvångsmedel är förenlig med regeringsformen och Europakonventionens bestämmelser om

skydd för privat- och familjelivet och tillgång till effektiva rättsmedel.

Skälen för bedömningen

Skyddet för den personliga integriteten enligt regeringsformen och Europakonventionen

Var och en är gentemot det allmänna skyddad bl.a. mot husrannsakan och liknande intrång, mot undersökning av brev eller annan förtrolig försändelse samt mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Därtill gäller ett skydd mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (se 2 kap. 6 § första och andra stycket regeringsformen). Det skyddet kan begränsas endast genom lag och för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. En begränsning får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 20 och 21 §§ regeringsformen).

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privatlivet är av mycket allmän art och omfattar skydd mot en mängd åtgärder.

För att en åtgärd som inskränker rättigheter enligt Europakonventionen ska vara godtagbar krävs att den har stöd i lag, vidtas för ett ändamål som är godtagbart i ett demokratiskt samhälle, att den objektivt sett är ägnad att uppnå syftet med åtgärden och att den är proportionerlig.

Den inskränkning som föreslås är godtagbar

Den utvidgning av tillämpningsområdet för bestämmelserna om beslag och hemliga tvångsmedel som nu föreslås medför inskränkningar i rättigheter som skyddas av regeringsformen och Europakonventionen. Reglerna motiveras av intresset av att förebygga,

förhindra, utreda och lagföra brott, vilket är godtagbara ändamål för sådana inskränkningar.

Den användning av tvångsmedel för statsstyrt röjande av företagshemlighet som nu föreslås har många likheter med den som får användas vid företagsspioneri och har samma skyddsintressen. I likhet med vad regeringen bedömt när bestämmelserna om företagsspioneri infördes får den föreslagna utvidgningen därför anses vara förenlig med skyddet för den personliga integriteten enligt bl.a. regeringsformen och Europakonventionen (se t.ex. prop. 2007/08:163 s. 64, prop. 2013/14:237 s 117, prop. 2018/19:86 s. 46–47 och prop. 2019/20:64 s 88.)

8.7 Internationella förhållanden

Genom de nya straffbestämmelser som föreslås och den lagändring som föreslås i rättegångsbalken öppnas en möjlighet för andra länder att begära rättslig hjälp av Sverige och för Sverige att begära motsvarande hjälp vid misstankar om olovligt utnyttjande eller röjande av företagshemlighet.

Sedan den 1 december 2017 gäller lagen (2017:1000) om en europeisk utredningsorder i Sverige. Lagen genomför Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området. Lagen gäller gentemot alla medlemsstater i EU utom Danmark och Irland. Med en europeisk utredningsorder avses ett beslut i Sverige – eller i en annan medlemsstat – som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning i den andra medlemsstaten respektive i Sverige. Beslut om åtgärden ska som huvudregel ha meddelats av en åklagare eller domstol under en utredning eller rättegång i brottmål. De utredningsåtgärder som är möjliga att vidta enligt lagen är bl.a. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning (1 kap. 4 §). Direktivets tillämpningsområde sätter inga gränser för vilka utredningsåtgärder som kan ingå i lagstiftningen, så länge det rör sig om en åtgärd som innebär bevisinhämtning. Tvärtom förutsätter direktivet att medlemsstaterna, när det kommer en utredningsorder

från ett annat land, kan tillhandahålla samtliga åtgärder som de nationella myndigheterna kan använda sig av.

I förhållande till övriga stater tillämpas lagen (2000:562) om internationell rättslig hjälp i brottmål. Det är en uttalad målsättning med lagen att svenska åklagare och domstolar ska kunna lämna rättslig hjälp till utländska myndigheter med alla de åtgärder som kan vidtas vid en svensk förundersökning eller rättegång (prop. 1999/2000:61 s. 79 och 80).

De ändringar som nu föreslås kommer alltså, utan några ytterligare lagändringar, att kunna aktualisera tvångsmedelsanvändning enligt lagen om europeisk utredningsorder och lagen om internationell rättslig hjälp i brottmål vid misstanke om olovligt utnyttjande eller röjande av företagshemlighet. Det har inte framkommit något som talar mot en sådan ordning.

9 Ikraftträdande- och övergångsbestämmelser

Förslag: Lagändringarna ska träda i kraft den 1 juli 2022.
Bedömning: Det behövs inte några övergångsbestämmelser.

Skälen för förslaget och bedömningen: En lämplig tidpunkt för ikraftträdande bedöms vara den 1 juli 2022.

I fråga om straffbestämmelser följer av 2 kap. 10 § regeringsformen och 5 § lagen (1964:163) om införande av brottsbalken att ingen får dömas för en gärning för vilken det inte var stadgat straff när den begicks. Vidare följer att straff ska bestämmas efter den lag som gällde när gärningen företogs, om inte annan lag gäller när dom meddelas som leder till frihet från straff eller till lindrigare straff.

När det gäller skadestånd följer det av allmänna principer att nya bestämmelser om skadestånd inte är tillämpliga när den skadegörande handlingen har begåtts innan de nya bestämmelserna har trätt i kraft (jfr prop. 2017/18:200 s. 127 och prop. 1987/88:155 s. 33 samt prop. 1972:5 s. 593).

Mot denna bakgrund behövs inga övergångsbestämmelser.

10 Förslagens konsekvenser

Bedömning: De föreslagna lagändringarna ger bättre möjligheter att ingripa mot att företagshemligheter av teknisk natur sprids och används illojalt. Förslagen har ingen effekt på den administrativa bördan för företagen och förutses inte leda till ökade kostnader för företagen. Ändringarna inskränker inte arbetstagarnas möjligheter att påtala och slå larm om oegentligheter i arbetsgivarens verksamhet. Rörligheten på arbetsmarknaden bedöms inte påverkas märkbart. De ökade kostnader för rättsväsendets myndigheter som förslagen medför är inte större än att de kan finansieras inom ramen för befintliga anslag.

Skälen för bedömningen

Konsekvenser för företagen

De föreslagna lagändringarna innebär huvudsakligen att det kriminaliserade området för angrepp på företagshemligheter av teknisk natur utvidgas. Genom de föreslagna ändringarna förbättras möjligheterna att ingripa mot att företagshemligheter av teknisk natur sprids och används illojalt.

I Sverige finns det ca 1,2 miljoner företag. Förslaget har sannolikt störst betydelse för företag som bedriver innovationsverksamhet, vilket är 55 procent av alla företag med fler än tio anställda. För företag som saknar företagshemligheter av teknisk natur har förslaget ingen betydelse.

Det kan antas att de nya straffbestämmelserna bidrar till att olovligt utnyttjande och röjande av tekniska företagshemligheter minskar. Möjligheterna att ingripa mot gärningarna förbättras också genom bl.a. utökade möjligheter till användning av hemliga tvångs-

medel. Företag som innehar företagshemligheter av teknisk natur får därmed ett bättre skydd för sina investeringar. Detta torde leda till bättre förutsättningar för investeringar i teknisk utveckling, även om någon uppskattning av ett belopp knappast går att göra. Det stärker också innovationskraften och den internationella konkurrensförmågan, liksom marknadens sunda funktion. Detta gynnar i sin tur handeln av varor och tjänster. Sammantaget bidrar detta till ett gynnsamt ekonomiskt klimat och kan antas bidra till fler arbetstillfällen.

Skyddet för företagshemligheter avser endast sådan information som innehavaren har vidtagit rimliga åtgärder för att hemlighålla. Den föreslagna kriminaliseringen utgår från detta. Några nya administrativa kostnader eller liknande kan därför inte väntas uppkomma för företagen.

Konsekvenser för arbetstagarna och arbetsmarknaden

Förslaget om att utvidga kriminaliseringen till att också omfatta röjande av företagshemlighet innebär inte att arbetstagarnas möjligheter att påtala och slå larm om oegentligheter i arbetsgivarens verksamhet minskas. Detta har utvecklats i avsnitt 6.11.

Risken för att arbetstagares rörlighet på arbetsmarknaden påverkas negativt bedöms som låg.

Den utvidgade kriminaliseringen knyter an till vad som i dag gäller då arbetstagare byter arbete och det krav på synnerliga skäl som ställs för att skadeståndsansvar ska bli aktuellt efter anställningens slut. De nya straffbestämmelserna aktualiseras således endast i undantagsfall efter anställningens slut. I och med att arbetstagaren endast i de mest klandervärda fallen kan drabbas av straffansvar efter avslutad anställning bedöms risken vara liten för att arbetstagare hämmas på grund av att de t.ex. upplever risken för straffansvar som oklar. Till det sagda kommer att de nya straffbestämmelserna endast omfattar angrepp på företagshemligheter av teknisk natur. Den kanske mest typiska situationen – att en arbetstagare vill använda sig av t.ex. marknadskännedom eller tidigare kundkontakter och då behöver ta ställning till om informationen är skyddad som en företagshemlighet – påverkas inte alls av den föreslagna kriminaliseringen.

Nykriminaliseringen innebär ett utvidgat ansvar i fråga om bemanningsanställda, som utan att vara anställda hos innehavaren av en företagshemlighet arbetar där under anställningsliknande förhållanden. Deras angrepp på innehavarens företagshemligheter är i dag inte skadeståndssanktionerade enligt lagen om företagshemligheter. Även om det inte synes sannolikt att gruppen kommer i kontakt med företagshemligheter i någon större utsträckning, finns ett behov av att låta dem omfattas av nykriminaliseringen och på så sätt även utvidga skadeståndsansvaret enligt lagen. Även för denna grupp föreslås ett krav på synnerliga skäl för ansvar i fråga om angrepp efter att deltagandet i rörelsen eller verksamheten har upphört.

På det hela taget kan det därför antas att påverkan på rörligheten på arbetsmarknaden inte blir annat än låg.

Konsekvenser för staten och myndigheterna

Att det straffrättsliga skyddet för kvalificerade företagshemligheter blir mer heltäckande är ägnat att leda till ett ökat förtroende för Sverige som innovationsland och bör ge ökad investeringsvilja. Detta bidrar till bättre förutsättningar för att det skapas fler arbetstillfällen och därmed också ökat välstånd.

För de tekniska företagshemligheter som finns vid universitet, högskolor och andra liknande institutioner innebär lagändringarna ett starkare skydd mot att t.ex. främmande makt använder sig av forskningsdelegationer för att komma åt åtråvärd information. Som företagshemlighet skyddas, som tidigare nämnts, endast sådan information som innehavaren har vidtagit rimliga åtgärder för att hemlighålla. Några nya administrativa kostnader eller liknande kan därför inte väntas uppkomma för universitet, högskolor eller andra liknande institutioner.

Enligt uppgifter från 2016 års utredning aktualiseras i rättsväsendet årligen endast ett mindre antal fall av överträdelser av lagen om företagshemligheter. Detta överensstämmer också med den bild som regeringen gett av användningen av hemliga tvångsmedel (skr. 2019/20:56). De hemliga tvångsmedlen används främst för bl.a. narkotikabrottslighet och våldsbrottslighet. Företagsspioneri redovisas inte separat, utan ingår i kategorin ”övriga brott”. Det finns

skäl att tro att företagsspionerі står för en mycket liten andel av de övriga brotten. De övriga brotten stod för ca tio procent av användningen av hemliga tvångsmedel. I fråga om hemlig rumsavlyssning stod dock denna kategori endast för två procent.

Det är rimligt att anta att lagändringen kan komma att leda till en ökning av antalet anmälningar, förundersökningar och lagföringar. En sådan ökning som det kan bli fråga om kan antas medföra en mycket marginell ökning av arbetsbelastningen för polis, åklagare, domstolar och kriminalvård. Till saken hör att nästan samtliga av de förfaranden som omfattas av det utökade straffansvaret redan är obehöriga angrepp på innehavarens företagshemligheter och omfattas alltså av lagens sanktioner i övrigt. På det hela taget bör det alltså i stort sett handla om förfaranden som oavsett en nykriminalisering sannolikt skulle belasta rättssystemet. Någon egentlig ökning av antalet ärenden kan det därför inte tänkas bli fråga om. Det kan dock bli fråga om att förordna offentlig försvarare i något fler fall, vilket kan leda till marginellt ökade kostnader för rättsliga biträden.

Sammantaget bedöms genomförandet av den föreslagna kriminaliseringen inte medföra annat än marginellt ökade kostnader för rättsväsendets myndigheter. Dessa finansieras inom ramen för befintliga anslag.

Konsekvenser för kvinnor och män

Det övergripande målet för jämställdhetspolitiken är att kvinnor och män ska ha samma makt att forma samhället och sina egna liv (prop. 2008/09:1 utg.omr. 13 s. 42). Delmålet om ekonomisk jämställdhet handlar bl.a. om att kvinnor och män ska ha samma möjligheter och villkor i fråga om utbildning och betalt arbete som ger ekonomisk självständighet livet ut. Jämställdhet bidrar till ekonomisk tillväxt genom att både kvinnors och mäns fulla potential tillvaratas och främjas (skr. 2016/17:10 s. 16).

Innovation och entreprenörskap förknippas än i dag främst med mäns företagande. Studier har visat att kvinnor i allmänhet har svårt att identifiera sig som företagare, både eftersom företagande i allmänhetens ögon förknippas med manliga egenskaper och eftersom kvinnor som är företagare i hög grad är aktiva i sektorer där företagande generellt inte ses som entreprenörskap utan snarare som

en form av sysselsättning (Främja kvinnors företagande – gjorde programmet någon nytta? Tillväxtanalys rapport 2018:05, s. 12). Andelen av de svenska företagarna som är kvinnor var 2016 strax över 30 procent. Under 2018 var 6,8 procent av den svenska befolkningen aktiva i ett tidigt skede eller drev ett ungt företag. År 2017 var motsvarande siffra 7,3 procent. Minskningen beror i huvudsak på att kvinnors entreprenörskap visat en kraftig nedgång, från cirka 6 till 4 procent, medan motsvarande siffra bland män är 9 procent (Global Entrepreneurship Monitor (GEM) nationell rapport, 2019).

I forskningsintensiva miljöer, som t.ex. på högskolor och universitet, är andelen män fortfarande högre i seniora positioner. Av samtliga anställda på universitet och högskolor under 2018 var 47 procent kvinnor och 53 procent män, men endast 29 procent av professorerna var kvinnor. Detta är dock en ökning med 15 procentenheter sedan 2001 (SCB, statistiskt meddelande UF 23 SM 1901, 2018). Inom medicin och naturvetenskap utgör kvinnor närmare hälften av forskarna, men får endast 12,7 procent av excellensmedlen inom dessa områden (Delegationen för jämställdhet i högskolan, rapporten Hans Excellens, 2010, s. 99).

Regeringen har vidtagit ett flertal åtgärder för att komma till rätta med denna problematik. Det kan t.ex. nämnas att instruktionen för Verket för innovationssystem, Vinnova, har ändrats så att myndigheten ska integrera ett jämställdhetsperspektiv i verksamheten och främja jämställdhet vid fördelning av medel för forskning och innovation (4 b § förordningen [2009:1101] med instruktion för Verket för innovationssystem). Det kan också nämnas att myndigheten för tillväxtpolitiska utvärderingar och analyser, Tillväxtanalys, har i uppdrag att i utvärderingsarbetet särskilt belysa effekter för kvinnor respektive män och i övrigt utforma kunskapsunderlag med ett jämställdhetsperspektiv (6 § förordningen [2016:1048] med instruktion för Myndigheten för tillväxtpolitiska utvärderingar och analyser).

Det förslag till straffskydd för företagshemligheter av teknisk natur som läggs fram i denna promemoria har en könsneutral utformning. En företagshemlighet av teknisk natur utmärks av att den typiskt sett utgör ett led i produktionen eller framställningen av en vara eller utförandet av en tjänst. Det avgörande är alltså inte vilken vara eller tjänst som produceras, utan att det handlar om

information som ingår i en framställningsprocess. Förslaget ger bättre förutsättningar för innovation och företagande för både kvinnor och män. Bedömningen görs att det utökade straffskyddet gynnar kvinnor och män i lika hög grad.

11 Författningskommentar

11.1 Förslaget till lag om ändring i lagen (2018:558) om företagshemligheter

Skadeståndsansvar

5 § Den som gör sig skyldig till brott enligt 26, *26 a* eller 27 § ska ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten *annars* utnyttjas eller röjs.

I paragrafen regleras skadeståndsansvar för den som har begått brott enligt lagen. Övervägandena finns i avsnitt 7.

Paragrafen ändras på så sätt att det anges att även den som begår brott enligt straffbestämmelserna i 26 a § ska vara skadeståndsskyldig i enlighet med vad som gäller för övriga brott i lagen.

Skadeståndsansvaret enligt paragrafen omfattar inte endast skada som uppkommer genom brottet utan också skada som uppkommer genom att företagshemligheten utnyttjas eller röjs (se prop. 1987/88:155 s. 41 f. och 58). Genom tillägget av ”annars” anpassas paragrafen språkligt till att det kriminaliserade området efter införandet av de nya straffbestämmelserna även omfattar olovligt utnyttjande och röjande. I fråga om straffansvar enligt 26 a § torde sådan skada i huvudsak omfatta utnyttjande och röjande av annan person.

Frågor om talan i domstol

22 § En talan enligt 12–15, 17 och 18 §§ förs av innehavaren av företagshemligheten.

En talan enligt 12–15, 17 och 18 §§ får föras även i samband med åtal för brott som avses i 26, *26 a* och 27 §§.

Paragrafen innehåller bestämmelser om vem som får föra talan om vitesförbud och andra skyddsåtgärder samt om möjligheten att föra en sådan talan i samband med åtal för brott enligt lagen.

Ändringen i *andra stycket* gör det möjligt för innehavaren av företagshemligheten att föra talan om vitesförbud och andra skyddsåtgärder även i ett brottmål om ansvar enligt de nya straffbestämmelserna i 26 a §.

Straff

26 § Den som uppsåtligen och olovligen bereder sig tillgång till en företagshemlighet ska dömas för *företagsspionerи* till böter eller fängelse i högst två år.

Om brottet är grovt döms till fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.

I paragrafen finns bestämmelser om straff för företagsspionerи.

Paragrafen ändras på så sätt att bestämmelsen om grovt brott flyttas från *första stycket* till ett eget *andra stycke*. Ingen ändring i sak görs i den delen.

Bestämmelserna i hittillsvarande andra och tredje styckena flyttas till två nya paragrafer, 26 b respektive 27 a §.

26 a § *Den som uppsåtligen och olovligen utnyttjar en företagshemlighet av teknisk natur som han eller hon har fått del av i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution, eller genom att delta i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund ska dömas för olovligt utnyttjande av företagshemlighet till böter eller fängelse i högst två år.*

Den som uppsåtligen och olovligen röjer en företagshemlighet av teknisk natur som han eller hon har fått del av på ett sätt som anges i första stycket ska dömas för olovligt röjande av företagshemlighet till böter eller fängelse i högst två år.

Om ett brott enligt första eller andra stycket är grovt döms till fängelse i lägst sex månader och högst sex år. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada.

I ringa fall ska det inte dömas till ansvar enligt denna paragraf. Det ska inte heller dömas till ansvar om gärningen begås efter att deltagandet i rörelsen eller verksamheten har upphört och det inte finns synnerliga skäl för ansvar.

Paragrafen är ny. Den innehåller bestämmelser om straffansvar för olovligt utnyttjande av företagshemlighet i första stycket respektive olovligt röjande av företagshemlighet i andra stycket. Övervägandena finns i avsnitt 6.1–6.12.

Av principen om att grundlag har företräde framför vanlig lag följer att paragrafen inte ska tillämpas om den kommer i konflikt med reglerna om meddelar- eller anskaffarfrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen (jfr t.ex. prop. 2017/18:200 s. 177 samt bet. 1989/90:LU37 s. 38) eller annan bestämmelse av sådan dignitet.

Ett grundläggande krav för att straffansvar enligt paragrafen ska komma i fråga är angreppet på företagshemligheten är obehörigt enligt 4 §.

I paragrafen straffbeläggs två gärningar.

Enligt *första stycket* är det straffbart att olovligen utnyttja en företagshemlighet av teknisk natur. Innebörden av begreppet utnyttjande är detsamma som annars i lagen. Med utnyttjande avses att någon i egen verksamhet praktiskt tillämpar den information som utgör företagshemligheten. Det ska vara fråga om ett kommersiellt utnyttjande, men det krävs inte att verksamheten går med vinst (prop. 2017/18:200 s. 144).

Enligt *andra stycket* är det straffbart att olovligen röja en företagshemlighet av teknisk natur. Med röjande avses, liksom i övrigt i lagen, att angriparen avslöjar hemligheten för någon annan. Det saknar i princip betydelse om röjandet sker mot ersättning eller inte (prop. 2017/18:200 s. 144).

Det ligger redan i definitionen av ett angrepp att ett utnyttjande eller röjande sker utan innehavarens samtycke (3 §). Det kan i sammanhanget också noteras att det, för att information ska vara skyddad enligt lagen, finns ett krav på att innehavaren har vidtagit rimliga åtgärder för att hemlighålla informationen. I annat fall är informationen inte skyddad som en företagshemlighet (2 §). Kravet innebär att innehavaren kan behöva göra klart för mottagaren vad han eller hon får och inte får göra med informationen.

Båda gärningarna, olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet, avser angrepp på en företagshemlighet av teknisk natur.

Kännetecknande för företagshemligheter av teknisk natur är att det är information som är ägnad att utgöra ett led i produktionen

eller framställningen av en vara eller utförandet av en tjänst. Det som avses är exempelvis ritningar, recept, källkoder, datorprogram, forskningsresultat eller forskningsunderlag, tekniska förebilder eller andra modeller samt annan teknisk information om uppfinningar, produkter eller tjänster. Företagshemligheten kan, men behöver inte, innefattas i den framställda produkten eller den utförda tjänsten. Även framställningsprocesser, maskinella anordningar eller andra hjälpmedel omfattas av paragrafen (jfr prop. 1981/82:165 s. 300). Det kan också handla om sammanställningar av information, exempelvis data som används vid utveckling av smarta produkter såsom självkörande bilar. En förutsättning är dock att den sammanställda informationen uppfyller kraven för företagshemlighet i 2 § (jfr prop. 2017/18:200 s. 30 f.). Det förutsätts inte att företagshemligheten är dokumenterad i någon form, även om detta vanligtvis är fallet. Begreppet är teknikneutralt, i likhet med begreppet företagshemlighet i övrigt.

Informationen behöver inte vara särskilt avancerad eller värdefull för att anses vara av teknisk natur (se dock 2 § första stycket 4). Avgörande är i stället om informationen typiskt sett utgör ett led i produktion eller framställning av en vara eller utförandet av en tjänst eller försteg i utvecklingen av dessa. Huruvida någon vara framställs eller tjänst utförs i det enskilda fallet saknar betydelse för frågan om straffansvar.

Till företagshemligheter av teknisk natur hör inte information som endast ger upplysningar om innehavarens affärsmässiga förhållanden som exempelvis priskalkyler, marknadsundersökningar och kundlistor. Information av det slaget har närmast betydelse för hur företaget ska kommersialisera en vara eller en tjänst och kan inte anses hänförlig till produktion eller framställning. Detsamma gäller information som uteslutande avser lagring eller transporter och annan information om distributionen av en vara.

Affärsplaner eller samarbetsavtal är normalt inte företagshemligheter av teknisk natur. Handlingar av det slaget avser i första hand rent kommersiella förhållanden. Det kan exempelvis vara fråga om huruvida produktionen kan antas bli lönsam eller huruvida det finns förutsättningar att i framtiden kommersialisera en vara eller en tjänst. På motsvarande sätt omfattas typiskt sett inte heller information om en planerad prissänkning eller lansering av uttrycket företagshemlighet av teknisk natur.

Information av rent administrativ karaktär, t.ex. löneuppgifter, verksamhetsrutiner och mötesprotokoll, är normalt inte av teknisk natur (jfr även 2 § första stycket 4).

I andra stycket anges att gärningsmannen, för att ansvar för olovligt röjande av företagshemlighet ska kunna komma i fråga, ska ha fått del av företagshemligheten på ett sätt som anges i första stycket. Personkretsen är således densamma i första och andra styckena.

Personkretsen kan delas upp i två huvudsakliga grupper. Gemensamt för dessa är att gärningsmannen, till skillnad från företagsspioneri enligt 26 §, har lovlig tillgång till en företagshemlighet som innehas av en näringsidkare eller en forskningsinstitution.

Den första gruppen består av personer som har fått del av en företagshemlighet i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution.

Den andra gruppen består av personer som genom deltagande i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning, uppdrag eller på annan liknande grund har fått del av en företagshemlighet.

En första förutsättning är alltså att innehavaren av företagshemligheten är en näringsidkare eller en forskningsinstitution. Dessa två begrepp ska förstås på samma sätt som i lagen i övrigt (se bl.a. 2 §).

Begreppet näringsidkare ska förstås i vidsträckt bemärkelse. Det inbegriper varje fysisk eller juridisk person som yrkesmässigt bedriver verksamhet av ekonomisk art, oavsett om verksamheten är inriktad på vinst eller inte. Om en ideell organisation i någon del bedriver verksamhet som har kommersiell betydelse, bör organisationen anses som näringsidkare i fråga om den verksamheten. Vid bedömningen av om en person ska anses som näringsidkare eller inte i lagens mening finns det ofta anledning att fästa mindre vikt vid formella aspekter, exempelvis om personen är godkänd för F-skatt eller om näringsverksamheten är registrerad i vederbörlig ordning (prop. 2017/18:200 s. 137).

Begreppet forskningsinstitution avser varje icke-kommersiell verksamhet i vilken det bedrivs forskning under institutionaliserade former. Det kan röra sig om allt från statliga universitet och högskolor till små som stora privata forskningsinrättningar. Forskningsinstitutioner som hanterar det slags information som lagen skyddar

är dock ofta näringsidkare i lagens mening (jfr prop. 2017/18:200 s. 137 f.). I fråga om myndigheter som bedriver forskningsverksamhet avgränsas lagens tillämpningsområde framför allt av i vilken utsträckning som sekretess gäller för forskningsresultat och liknande hos myndigheten; offentlig information kan inte skyddas som en företagshemlighet (jfr 2 §).

I fråga om vad som avses med affärsförbindelse kan följande sägas.

Begreppet affärsförbindelse finns även i 6 § och har samma innebörd här (jfr prop. 1987/88:155 s. 42). Utgångspunkten är att någon i förtroende har fått del av en företagshemlighet, ofta till följd av en avtalsrelation. Det ligger emellertid i begreppet att det inte måste finnas något bindande avtal mellan parterna. Redan under ett förhandlingsskede kan mottagaren ha fått del av företagshemligheten på sådant sätt att det finns ett förtroendeförhållande (se prop. 2017/18:200 s. 152).

Det typiska är att det rör sig om kommersiella förhållanden med en näringsidkare som motpart. Med affärsförbindelse avses dock även då en forskningsinstitution har en förbindelse med någon utomstående som innebär att företagshemligheter utväxlas under krav på diskretion i fråga om hemligheterna. Företagshemligheter ingår typiskt sett i ett affärsmässigt utbyte, även om forskningsinstitutionen i och för sig skulle vara icke-kommersiell. Även i dessa fall är det därför naturligt att se förbindelsen som en affärsförbindelse (prop. 2017/18:200 s. 61 och 153).

Ansvaret enligt första eller andra styckena gäller för den person som är part i affärsförbindelsen med innehavaren av företagshemligheten (jfr prop. 2017/18:200 s. 152). Det förutsätts att personen i fråga själv har gjort sig skyldig till ett handlande som kan ligga till grund för ett straffrättsligt ansvar. I annat fall kan i stället reglerna om medverkan i 23 kap. brottsbalken vara tillämpliga.

Till skillnad från i 6 § anges inte att informationen ska ha mottagits i förtroende. Detta ligger i stället i att utnyttjandet eller röjandet ska ske olovligt, dvs. informationen ska ha mottagits under sådana omständigheter att det finns krav på att informationen inte får röjas eller utnyttjas.

När det gäller kravet på att gärningsmannen ska ha tagit del av företagshemligheten genom deltagande i en näringsidkares rörelse

eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund kan följande sägas.

Den arbetspresterande parten ska ha fått del av företagshemligheten på grund av sitt deltagande i rörelsen eller verksamheten. Det krävs inte att företagshemligheten har med de egna arbetsuppgifterna att göra. Inte heller krävs att den enskilde uttryckligen har anförtrotts företagshemligheten eller att han eller hon har utövat någon form av aktivitet för att få del av den; även den som av en tillfällighet får del av den hemliga informationen kan omfattas av straffansvar. Han eller hon måste dock ha uppsåt till att informationen utgör en företagshemlighet, se nedan.

Personer som är anställda hos näringsidkaren eller forskningsinstitutionen kan under normala förhållanden antas uppfylla kravet på deltagande oavsett tjänstgöringstid och typ av arbetsuppgifter. Ett exempel på när kravet på deltagande dock inte är uppfyllt kan vara när en nyanställd ännu inte tillträtt tjänsten.

Vid en prövning av om uppdragstagare och andra funktionärer, som t.ex. bemanningsanställda, uppfyller kravet på deltagande i rörelsen eller verksamheten får det göras en samlad bedömning av omständigheterna i det enskilda fallet. Det avgörande är om personen i fråga utför arbete för näringsidkarens eller forskningsinstitutionens räkning under omständigheter som liknar dem som förekommer i ett anställningsförhållande. Särskilt tydligt är så fallet när den arbetspresterande parten har en sådan nära anknytning till företaget eller forskningsinstitutionen att han eller hon är inordnad i organisationen på samma sätt som om ett anställningsförhållande hade förelegat. Omständigheter som talar för att kravet på deltagande är uppfyllt är att det arbete som utförs hör till arbetsgivarens kärnverksamhet och att arbetsförhållandet har viss varaktighet. Kravet på deltagande är ofta uppfyllt för fristående konsulter som utför arbete inom det centrala verksamhetsområdet. Det kan också vara uppfyllt för arbetskraft som ställts till förfogande genom inhyrning eller inlåning från bemanningsföretag, liksom för anställda hos ett konsultföretag som näringsidkaren eller forskningsinstitutionen anlitar. Även delägare som arbetar i företaget får anses delta i rörelsen eller verksamheten på det sätt som avses här. Detsamma gäller för lärlingar, studerande m.fl. som inom ramen för sin utbildning praktiserar på en arbetsplats och där sysselsätts på ett sätt som liknar det en anställd gör. Andra exempel är personer som

medverkar i arbetsmarknadspolitiska program eller sysselsättningsprojekt.

Om ett uppdrag är av mer långvarig eller regelbunden karaktär så att personen i fråga lika gärna hade kunnat vara anställd, talar det för att kravet på deltagande i rörelsen eller verksamheten är uppfyllt.

Som exempel på personer som många gånger inte kan sägas delta i rörelsen eller verksamheten kan nämnas hantverkare som anlitas tillfälligt för att utföra installationer eller reparationer samt självständiga formgivare, arkitekter eller personer inom reklambranschen som konsulteras för bestämda projekt. Andra exempel är datakonsulter, organisationskonsulter och juridiska ombud som anlitas för enstaka kortvariga uppdrag som saknar samband med kärnverksamheten.

Företagshemligheter som styrelseledamöter och revisorer i t.ex. aktiebolag får kännedom om inom ramen för sina respektive uppdrag och som innehas av bolaget i fråga kan inte anses ha kommit dem till del genom deltagande i en rörelse eller verksamhet under omständigheter som liknar dem som förekommer i ett anställningsförhållande (jfr 10 § andra stycket samt SOU 2017:45 s. 353). Inte heller kan de anses ha fått del av uppdragsgivarens företagshemligheter i samband med en affärsförbindelse med innehavaren (jfr prop. 2017/18:200 s. 153). Deras angrepp på huvudmannens företagshemligheter omfattas därmed inte av straffansvar enligt paragrafen. För dessa grupper kan andra sanktioner aktualiseras (se avsnitt 6.6).

För straffansvar förutsätts att gärningsmannen har uppsåt som täcker de omständigheter som ligger till grund för ansvar. Om någon exempelvis röjer en företagshemlighet som han eller hon har fått del av under sådana omständigheter som anges i förevarande paragraf utan att misstänka att det på arbetsplatsen finns en regel om att informationen inte får röjas, blir straffansvar inte aktuellt. Gärningsmannen har då inte haft uppsåt i förhållande till att det varit fråga om en företagshemlighet.

Brottsrubriceringen enligt första stycket är olovligt utnyttjande av företagshemlighet och enligt andra stycket olovligt röjande av företagshemlighet.

Straffet för brott enligt första eller andra stycket är böter eller fängelse i högst två år.

I *tredje stycket* framgår straffskalan för grovt brott. Straffskalan i sådant fall är fängelse i lägst sex månader och högst sex år och är förbehållen den mest allvarliga brottsligheten. Vid bedömningen av om brottet är grovt ska det – liksom vid grovt företagsspionerі – särskilt beaktas om gärningen har varit av särskilt farlig art, avsett betydande värde eller inneburit synnerligen kännbar skada. Uppräkningen är inte uttömmande.

Huruvida brottet är grovt får bedömas med hänsyn till samtliga omständigheter i det enskilda fallet. Något som talar för att gärningen varit av särskilt farlig art är att gärningsmannen utnyttjat ett särskilt förtroende eller att brottet har koppling till främmande makt. Det kan också handla om att någon i stor omfattning eller under en längre period levererat hemlig information till en utomstående. Så kan även vara fallet när gärningen har ingått som ett led i en brottslighet i organiserad form eller annars präglats av särskild förslagenhet. Om företagshemligheten representerar ett betydande värde kan vidare grovt brott föreligga på den grunden. Med betydande värde avses, i likhet med vad som gäller för förmögenhetsbrotten, som huvudregel värden överstigande fem prisbasbelopp. Vid bedömningen av om gärningen inneburit synnerligen kännbar skada ska beaktas inte endast vilket belopp det är frågan om utan också vilken skada målsäganden, ur ett subjektivt perspektiv, drabbats av. Denna grund kan vara tillämplig om företagshemligheten visserligen ännu inte har ett högt realiserbart kommersiellt värde som låter sig bestämmas men hemligheten är en viktig tillgång för bolaget. Ett exempel är att ett bolag lagt ned stora resurser på en produktionsmetod eller en teknisk innovation. Även om värdet av företagshemligheten inte går att bestämma säkert kan det stå klart att spridningen drabbar företaget hårt och omintetgör många av de investeringar som gjorts för att ta fram densamma.

I *fjärde stycket* görs undantag från det straffbara området till att börja med för ringa gärningar. Straffansvar ska inte dömas ut om gärningen vid en samlad bedömning är att anse som bagatellartad. Vid denna bedömning kan kvalifikationsgrunderna för grovt brott tjäna till ledning. Omständigheter som kan beaktas är således gärningens art, vilket värde den avsett samt en eventuell skadas omfattning. Om en företagshemlighet röjs för en person som inte kan tänkas utnyttja den kommersiellt och inte heller i sin tur föra den vidare, kan gärningen vara att anse som ringa. Så är exempelvis i

allmänhet fallet om en anställd berättar om sitt arbete för en nära anhörig och samtidigt i allmänna ordalag röjer en företagshemlighet. Ett annat exempel på vad som kan vara ett ringa fall är att en företagshemlighet röjs i samband med ett allmänt informationsutbyte vid en konferens utan att det finns en risk för vidare spridning eller utnyttjande. Vid bedömningen av om en gärning är ringa kan det också vara av betydelse vilken ställning gärningsmannen har i rörelsen eller verksamheten. Om gärningsmannen har självständiga befogenheter, finns det ofta större anledning att se allvarligt på gärningen. En viktig faktor vid bedömningen är vidare i vad mån det uppkommit någon skada. Informationens art och dess värde för verksamheten eller rörelsen, liksom risken för spridning kan vara sådana att skadan är mycket begränsad. I fråga om ett röjande av en företagshemlighet till en främmande makt bör det vara uteslutet att bedöma gärningen som ringa.

För det andra undantas enligt fjärde stycket som huvudregel också situationen att den som röjer eller utnyttjar företagshemligheten gör det efter att deltagandet i rörelsen eller verksamheten har upphört. Endast om det finns synnerliga skäl för straffansvar kommer ansvar enligt första eller andra stycket i fråga.

För situationen att någon olovligen utnyttjar eller röjer en företagshemlighet av teknisk natur som han eller hon har fått del av i samband med en affärsförbindelse saknar undantaget betydelse.

Kravet på synnerliga skäl för straffansvar knyter an till det som redan gäller för arbetstagares skadeståndsrättsliga ansvar i motsvarande situation (jfr 7 § andra stycket). Enligt vad som får anses vara en allmän princip är en arbetstagare – om denne inte avtalar om annat med sin arbetsgivare genom sekretessavtal eller konkurrensavtal – efter anställningens upphörande som huvudregel löst från sin lojalitetsplikt. En arbetstagares utnyttjande eller röjande av en tidigare arbetsgivares företagshemligheter anses inte heller som ett obehörigt angrepp så länge det inte föreligger synnerliga skäl (se prop. 2017/18:200 s. 62 f. och 147). Något ansvar enligt lagen kan då inte komma i fråga.

För arbetstagare har begränsningen som följer av den förevarande paragrafen sålunda närmast karaktären av ett förtydligande. Det följer nämligen redan av ovan nämnda princip att ansvar inte kan komma i fråga efter att ett deltagande i rörelsen eller verksamheten har upphört, om det inte finns synnerliga skäl. Av 7 § andra stycket

framgår även uttryckligt att skadeståndsansvar inte föreligger i en sådan situation. För övriga kategorier som omfattas av straffansvar för den som deltar i en verksamhet eller en rörelse innebär bestämmelsen att de på motsvarande sätt kan undantas från straffansvar.

En konsekvens av att straffansvar inte kan komma i fråga är att skadeståndsansvar enligt 5 § inte heller kan komma i fråga.

Deltagandet får anses ha upphört när personen i praktiken inte längre utför arbete för näringsidkarens eller forskningsinstitutionens räkning i sådan utsträckning att han eller hon kan sägas delta i rörelsen eller verksamheten. Vanligen, men inte alltid, sammanfaller detta med att det anställningsavtal, uppdragsavtal eller motsvarande som ligger till grund för deltagandet upphör och det faktiska arbetet har avslutats.

I fråga om vad som utgör synnerliga skäl får ledning hämtas från begreppets innebörd i 7 § andra stycket.

Omständigheter som talar för att synnerliga skäl föreligger är exempelvis att en person har tagit anställningen eller uppdraget i syfte att komma över hemlig information eller att han eller hon under deltagandet i rörelsen eller verksamheten har förberett ett överförande av information till exempelvis en konkurrent. Även personens ställning i rörelsen eller verksamheten kan beaktas. En särskild förtroendeställning, t.ex. som verkställande direktör, produktionschef eller forskningschef kan tala för att synnerliga skäl föreligger. Även förekomst av så kallade sekretess- och konkurrensklausuler kan beaktas vid prövningen. Det förhållandet att företagshemligheten har missbrukats med hjälp av dokumentation i någon form, exempelvis en teknisk förebild, är något som ofta talar för att det finns synnerliga skäl. Om en tidigare arbetstagare eller annan deltagare använder sig av tekniska förebilder, ritningar, tekniska beskrivningar eller annan dokumentation som härrör från den tidigare arbetsgivaren och avser dennes företagshemligheter, bör det i princip anses finnas synnerliga skäl. Vid bedömningen har även skadans storlek en viss betydelse (jfr prop. 1987/88:155 s. 46 och 61).

I bedömningen av om det föreligger synnerliga skäl kan även beaktas vem som tar emot den röjda eller utnyttjade företagshemligheten. Något som talar för att det föreligger sådana skäl kan då vara att mottagaren är den främsta konkurrenten i branschen eller

främmande makt. Sådana mottagare kan antas använda företagshemligheten på ett särskilt skadligt sätt.

Synnerliga skäl kan normalt inte anses föreligga om utnyttjandet eller röjandet endast i liten utsträckning har påverkat den tidigare arbetsgivarens konkurrensförmåga. Ett exempel är då företagshemligheten lämnas ut till en person som inte kan tänkas åstadkomma någon mer påtaglig skada (jfr också 2 § samt undantaget för ringa brott). En annan omständighet som kan tala mot ansvar är att arbetstagaren själv har utvecklat hemligheten hos sin tidigare arbetsgivare. I ett sådant fall kan det ofta finnas skäl att inte frångå huvudregeln om arbetstagarens frihet att utnyttja sin kunskap och erfarenhet på den öppna arbetsmarknaden (prop. 1987/88:155 s. 46 och prop. 2017/18:200 s. 62 f.).

Det kan knappast inträffa att en gärning bedöms som ringa samtidigt som det finns synnerliga skäl. Vid grova brott får det emellertid vanligtvis anses föreligga synnerliga skäl.

I lagen finns viss reglering om konkurrens, se 27 a § och 28 § första stycket. Övriga eventuella konkurrenssituationer som kan tänkas uppkomma får lösas genom tillämpning av de allmänna principer som gäller.

I detta sammanhang finns även skäl att särskilt peka på bestämmelsen i 28 § andra stycket som syftar till att förhindra åläggande av dubbla sanktioner vid vite (se även rättsfallen NJA 2013 s. 502 och NJA 2015 s. 663 samt jfr prop. 2017/18:165 s. 113 f.).

26 b § *För försök eller förberedelse till företagsspionerі, olovligt utnyttjande av företagshemlighet eller olovligt röjande av företagshemlighet ska det dömas till ansvar enligt 23 kap. brottsbalken.*

I paragrafen, som är ny, föreskrivs straffansvar för försök och förberedelse till företagsspionerі, olovligt utnyttjande av företagshemlighet och olovligt röjande av företagshemlighet.

I fråga om företagsspionerі motsvarar paragrafen bestämmelsen om ansvar för försök och förberedelse till sådan gärning i hittillsvarande 26 § andra stycket.

Straffansvar inträder under de förutsättningar som anges i 23 kap. brottsbalken.

En försöksgärning till ett olovligt utnyttjande eller röjande av företagshemligheter kan ske t.ex. i form av kopiering eller insamling av dokument med företagshemlig information med avsikt att

omedelbart använda den i en egen näringsverksamhet eller lämna ut den till en konkurrent.

27 § Den som uppsåtligen anskaffar en företagshemlighet med vetskap om att den som tillhandahåller hemligheten eller någon före honom eller henne i sin tur har berett sig tillgång till denna genom en gärning som avses i 26 §, ska dömas för *olovlig befattning med företagshemlighet* till böter eller fängelse i högst två år eller, om brottet är grovt, till fängelse i högst fyra år. *Detsamma gäller den som uppsåtligen anskaffar en företagshemlighet av teknisk natur med vetskap om att hemligheten tillhandahålls, eller tidigare har tillhandahållits, genom ett sådant röjande som avses i 26 a § andra stycket, och röjandet inte är fritt från ansvar enligt fjärde stycket i samma paragraf.*

Paragrafen innehåller bestämmelser om straffansvar för den som anskaffar en företagshemlighet som har varit föremål för vissa enligt lagen straffbelagda gärningar. Övervägandena finns i avsnitt 6.13.

I paragrafen görs ett tillägg som innebär att straffansvaret för olovlig befattning med företagshemlighet utökas till att omfatta även den som anskaffar en företagshemlighet med vetskap om att hemligheten tillhandahålls, eller tidigare har tillhandahållits, genom ett sådant röjande som avses i 26 a § andra stycket.

Det krävs inte att förbrottet bedöms som olovligt röjande av företagshemlighet, utan det kan vara annat brott enligt brottsbalken med en strängare straffskala så länge själva gärningen är sådan som avses i bestämmelsen om olovligt röjande av företagshemlighet (jfr 27 a § och prop. 2017/18:200 s. 178 om motsvarande fråga när företagsspionerі är förbrott).

Innebörden av att någon anskaffar en företagshemlighet är densamma oavsett om förbrottet är ett företagsspionerі eller ett olovligt röjande av företagshemlighet (jfr prop. 2017/18:200 s. 178). Även kravet i subjektivt hänseende är detsamma oavsett om förbrottet är företagsspionerі eller olovligt röjande av företagshemlighet. Kravet på vetskap torde motsvara insiktsuppsåt enligt det uppsåtsbegrepp som används i dag innebär att straffansvar förutsätter insiktsuppsåt till omständigheten att hemligheten tillhandahålls, eller tidigare har tillhandahållits, genom ett sådant röjande som avses i bestämmelsen om olovligt röjande av företagshemlighet (jfr prop. 2015/16:78 s. 69).

I fråga om fall då olovligt röjande av företagshemlighet utgör förbrott kan följande sägas. Till en början kan olovlig befattning med företagshemlighet komma i fråga när en person mottar företags-

hemligheten från någon som genom att dela med sig av informationen gör sig skyldig till en gärning som är att anse som olovligt röjande av företagshemlighet. Ansvar kan också aktualiseras om någon i ett tidigare led har gjort sig skyldig till en gärning som är att anse som olovligt röjande av företagshemlighet. Det kan t.ex. handla om att en person har röjt företagshemligheten enligt 26 a § till en person som sedan – utan att göra sig skyldig till brott – röjer hemligheten till någon annan. Den sista personen i kedjan kan då dömas för olovlig befattning med företagshemlighet. Det förutsätter att personen har vetskap om att företagshemligheten tidigare har varit föremål för ett straffbart olovligt röjande av företagshemlighet.

Ansvar förutsätter att det tidigare röjandet inte är fritt från ansvar. Om röjandet är att anse som en ringa gärning, eller röjandet är straffritt för att det begås efter att deltagandet har upphört och det inte föreligger synnerliga skäl för ansvar, finns det inte något förbrott och straffansvar för olovlig befattning med företagshemlighet kan inte komma i fråga.

I subjektivt hänseende gäller inte kravet på vetskap i förhållande till att sådana ansvarsbefriande omständigheter inte föreligger. Det är alltså tillräckligt med likgiltighetsuppsåt i förhållande till de omständigheter som innebär att det t.ex. inte är fråga om en gärning som är att anse som ringa enligt 26 a § fjärde stycket.

27 a § *Det ska inte dömas till ansvar enligt 26, 26 a, 26 b eller 27 § om gärningen är belagd med strängare straff i brottsbalken.*

Paragrafen, som är ny, behandlar förhållandet mellan straffbestämmelser i lagen om företagshemligheter och brottsbalken.

I fråga om företagsspionerі motsvarar paragrafen hittillsvarande 26 § tredje stycket och i fråga om olovlig befattning med företagshemlighet 27 § andra stycket. Någon ändring i sak är inte avsedd utan ändringen görs för ökad överskådlighet.

Även förhållandet till brottsbalken när det är fråga om olovligt utnyttjande av företagshemlighet eller olovligt röjande av företagshemlighet regleras. Det är en följd av att sådana gärningar straffbeläggs genom den nya 26 a §.

Det ska inte dömas till ansvar enligt lagen om företagshemligheter om gärningen är belagd med strängare straff i brottsbalken. Samma ordning ska gälla för alla de uppräknade brotten.

11.2 Förslaget till lag om ändring i rättegångsbalken

27 kap. Om beslag och hemliga tvångsmedel

Beslag m.m.

2 § En skriftlig handling får inte tas i beslag om

1. den kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § inte får höras som vittne om, och
2. handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för.

Ett skriftligt meddelande mellan den misstänkte och en närstående som avses i 36 kap. 3 §, eller mellan sådana närstående inbördes, får tas i beslag hos den misstänkte eller en närstående endast vid en förundersökning om

1. ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,
3. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
4. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,
5. högförräderi, krigsanstiftan, spionerі, grovt spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 7, 8, 10, 10 a eller 10 b § brottsbalken,
6. företagsspionerі *eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,
7. terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, brott enligt 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller
8. försök, förberedelse eller stämpling till brott som avses i 2–7, om en sådan gärning är belagd med straff.

Ett beslut enligt andra stycket 2–8 får meddelas endast av rätten eller åklagaren.

Om åklagaren har beslutat om beslag enligt tredje stycket, ska han eller hon utan dröjsmål anmäla åtgärden hos rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Paragrafen innehåller bestämmelser om att en skriftlig handling under vissa förhållanden inte får tas i beslag (det s.k. beslagsförbudet). Övervägandena finns i avsnitt 8.

Andra stycket sjätte punkten ändras på så sätt att beslagsförbudet inskränks också vid en förundersökning om olovligt röjande av företagshemlighet enligt 26 a § andra stycket lagen om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning.

Ändringen medför – på grund av hänvisningar i 27 kap. 18 § andra stycket 2, 19 § tredje stycket 3 och 20 a § andra stycket 2 rättegångsbalken till förevarande lagrum – att tvångsmedlen hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning får användas vid en förundersökning om olovligt röjande av företagshemlighet. Det medför också att hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning kan aktualiseras.

Hemliga tvångsmedel

20 d § Med hemlig rumsavlyssning avses avlyssning eller upptagning som

1. görs i hemlighet och med ett tekniskt hjälpmedel som är avsett att återge ljud, och
2. avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Hemlig rumsavlyssning får användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år,
2. spionerі enligt 19 kap. 5 § brottsbalken,
3. *företagsspionerі eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning och det kan antas att brottet inte leder till endast böter,
4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i fyra år och det är fråga om

a) människohandel enligt 4 kap. 1 a § brottsbalken,
b) grov människoexploatering enligt 4 kap. 1 b § tredje stycket brottsbalken,
c) våldtäkt enligt 6 kap. 1 § första stycket brottsbalken,

d) grovt sexuellt övergrepp enligt 6 kap. 2 § andra stycket brottsbalken,
e) våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken,
f) grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken,
g) grovt utnyttjande av barn för sexuell posering enligt 6 kap. 8 § tredje stycket brottsbalken,
h) grovt koppleri enligt 6 kap. 12 § tredje stycket brottsbalken,
i) grov utpressning enligt 9 kap. 4 § andra stycket brottsbalken,
j) grovt barnpornografibrott enligt 16 kap. 10 a § sjätte stycket brottsbalken,
k) grovt övergrepp i rättssak enligt 17 kap. 10 § tredje stycket brottsbalken,
l) grovt narkotikabrott enligt 3 § narkotikastrafflagen (1968:64), eller
m) grov narkotikasmuggling enligt 6 § tredje stycket lagen (2000:1225) om straff för smuggling,
5. försök, förberedelse eller stämpling till brott som avses i 1–3, om en sådan gärning är belagd med straff,
6. försök, förberedelse eller stämpling till brott som avses i 4, om en sådan gärning är belagd med straff och det med hänsyn till omständigheterna kan antas att gärningens straffvärde överstiger fängelse i fyra år.

Paragrafen behandlar tvångsmedlet hemlig rumsavlyssning. Övervägandena finns i avsnitt 8.

Paragrafen ändras på så sätt att brottet olovligt röjande av företagshemlighet enligt 26 a § andra stycket lagen om företagshemligheter läggs till i *andra stycket tredje punkten*. Det förutsätts för användning av tvångsmedlet att det kan antas att brottet inte leder till endast böter. Det överensstämmer för vad som gäller för statsstyrt företagsspioneri.

Underrättelse till enskild

33 § Om det gäller sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) för uppgifter som avses i 32 §, ska en underrättelse enligt 31 § skjutas upp till dess att sekretess inte längre gäller.

Om det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades, behöver underrättelsen inte lämnas.

En underrättelse enligt 31 § ska inte lämnas, om förundersökningen angår
1. brott som avses i 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
2. brott som avses i 13 kap. 4 eller 5 § brottsbalken,

3. brott som avses i 18 kap. 1, 3, 5 eller 6 § eller 19 kap. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 10 a, 10 b, 12 eller 13 § brottsbalken,

4. brott som avses i 3 eller 4 kap. brottsbalken, om brottet är av det slag som anges i 18 kap. 2 § eller 19 kap. 11 § samma balk,

5. brott som avses i 26 § *eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,

6. brott som avses i 2 § lagen (2003:148) om straff för terroristbrott, 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

7. försök, förberedelse eller stämpling till brott som anges i 1–6 eller underlåtenhet att avslöja sådant brott, om gärningen är belagd med straff.

Paragrafen innehåller bestämmelser om att en underrättelse till en enskild om att han eller hon har utsatts för ett hemligt tvångsmedel under vissa förhållanden ska skjutas upp eller inte lämnas. Överväganden finns i avsnitt 8.

Tredje stycket femte punkten ändras på så sätt att en underrättelse enligt 27 kap. 31 § inte heller ska lämnas om förundersökningen angår brott som avses i 26 a § andra stycket lagen om företagshemligheter – dvs. olovligt röjande av företagshemlighet – om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning. Det överensstämmer med vad som gäller för statsstyrt företagsspioneri.

11.3 Förslaget till lag om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott

1 § Tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första och andra styckena rättegångsbalken eller hemlig kameraövervakning enligt 27 kap. 20 a § första stycket rättegångsbalken får meddelas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,

2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,

3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,

4. högförräderi, krigsanstiftan, spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6 eller 8 § eller 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,

5. företagsspionerі *eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten kommer att utövas på uppdrag av eller understödjas av en främmande makt eller av någon som kommer att agera för en främmande makts räkning,

6. terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

7. mord, dråp, grov misshandel, synnerligen grov misshandel, människokorov eller olaga frihetsberövande enligt 3 kap. 1, 2 eller 6 § eller 4 kap. 1 § eller 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Tillstånd enligt första stycket får också meddelas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas brottslig verksamhet som avses i första stycket och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Paragrafen anger de typer av brottslig verksamhet vid vilka det enligt lagen är tillåtet att i preventivt syfte använda vissa tvångsmedel enligt 27 kap. rättegångsbalken. Övervägandena finns i avsnitt 8.

Första stycket femte punkten ändras på så sätt att beslut om tvångsmedel enligt paragrafen kan fattas även då det finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar olovligt röjande av företagshemlighet enligt 26 a § andra stycket lagen om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten kommer att utövas på uppdrag av eller understödjas av en främmande makt eller av någon som kommer att agera för en främmande makts räkning. Det överensstämmer med vad som gäller för statsstyrt företagsspionerі.

11.4 Förslaget till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

2 § Uppgifter får hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. sabotage enligt 13 kap. 4 § brottsbalken,
3. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
4. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
5. spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,
6. företagsspionerі *eller olovligt röjande av företagshemlighet enligt 26 § eller 26 a § andra stycket* lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understöds av en främmande makt eller av någon som agerar för en främmande makts räkning,
7. grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet,
8. grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Uppgifter får bara hämtas in om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Paragrafen innehåller förutsättningarna för att de uppgifter som anges i 1 § ska få hämtas in. Övervägandena finns i avsnitt 8.

Första stycket sjätte punkten ändras på så sätt uppgifter enligt 1 § får hämtas in också då åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar olovligt röjande av företagshemlighet enligt 26 a § andra stycket lagen om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understöds av en främmande makt eller av någon som agerar för en främmande makts

räkning. Det överensstämmer med vad som gäller för statsstyrt företagsspionerи.