Utkast till lagrådsremiss

Ett mer heltäckande straffansvar vid angrepp på företagshemligheter

Stockholm xxx

xxx

xxx
(Justitiedepartementet)

Utkastets huvudsakliga innehåll

Skyddet för företagens och forskningsinstitutionernas företagshemligheter behöver stärkas. I utkastet föreslås ett mer heltäckande straffansvar vid angrepp på företagshemligheter. Förslaget bidrar till bättre förutsättningar för företagande, teknisk utveckling och ökad konkurrenskraft. Vidare syftar förslaget till att möta det hot som industrispionage utgör mot den svenska industrin och det svenska samhället.

Utkastets förslag är att det ska vara straffbart även för den som har lovlig tillgång till en företagshemlighet, t.ex. genom sin anställning, att olovligen utnyttja eller röja företagshemligheten. Kriminaliseringen gäller tekniska företagshemligheter, dvs. de företagshemligheter som är viktigast för den tekniska utvecklingen och industrin.

Lagändringarna föreslås träda i kraft den 1 januari 2026.

Innehållsförteckning

1 Lagtext

Utkastet har följande förslag till lagtext.

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 *på något annat sätt* 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 <u>*företagsspioneri*</u> 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 <u>*företagsspioneri*</u> till böter eller fängelse i högst två år.
För försök eller förberedelse till företagsspioneri ska det dömas till ansvar enligt 23 kap. brottsbalken.	*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.

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 eller röjer en företagshemlighet

1. som avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst (teknisk företagshemlighet), och

2. som han eller hon har fått del av genom att delta i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund, eller i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution,

ska dömas för olovligt utnyttjande av teknisk företagshemlighet eller olovligt röjande av teknisk företagshemlighet 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 ringa fall ska det inte dömas till ansvar. Vid bedömningen av om gärningen är ringa ska det särskilt beaktas om gärningen är mindre allvarlig på grund av att den har begåtts efter att ett sådant deltagande som avses i första stycket 2 har upphört.

26 b §

För försök eller förberedelse till företagsspioneri, olovligt utnyttj-

	ande av teknisk företagshemlighet eller olovligt röjande av teknisk 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 befattning med företagshemlighet* till böter eller fängelse i högst två år eller, om brottet är grovt, till fängelse i högst fyra år.	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 teknisk företagshemlighet med vetskap om att den som tillhandahåller hemligheten eller någon före honom eller henne i sin tur har röjt denna genom en gärning som avses i 26 a § första eller andra stycket.*
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 januari 2026.

1.2 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 27 kap. 18 a, 20 d, 33 och 34 §§ rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

27 kap.

18 a §[1]

Hemlig avlyssning av elektronisk kommunikation får användas om någon är skäligen misstänkt för brott som avses i andra stycket och åtgärden är av synnerlig vikt för utredningen.

Hemlig avlyssning av elektronisk kommunikation enligt denna paragraf får användas vid en förundersökning om

1. ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. grovt dataintrång enligt 4 kap. 9 c § andra stycket brottsbalken,
3. grovt sexuellt övergrepp, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, grovt sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, grovt utnyttjande av barn för sexuell posering, utnyttjande av barn genom köp av sexuell handling, sexuellt ofredande mot barn eller grovt sexuellt ofredande mot barn enligt 6 kap. 2 § tredje stycket, 5 §, 6 §, 8 §, 9 § eller 10 § första eller tredje stycket brottsbalken,
4. kontakt för att träffa ett barn i sexuellt syfte enligt 6 kap. 10 a § brottsbalken, om det kan antas att brottet inte leder till endast böter,
5. grovt bedrägeri enligt 9 kap. 3 § brottsbalken, om gärningen har begåtts med hjälp av elektronisk kommunikation,
6. utpressning enligt 9 kap. 4 § första stycket brottsbalken, om det kan antas att brottets straffvärde överstiger fängelse i tre månader,
7. sabotage enligt 13 kap. 4 § brottsbalken,
8. mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1 §, 3 § första eller andra stycket, 5 a § eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
9. mened enligt 15 kap. 1 § första stycket brottsbalken, om det kan antas att brottets straffvärde överstiger fängelse i tre månader,
10. grovt barnpornografibrott eller barnpornografibrott som inte är ringa enligt 16 kap. 10 a § brottsbalken,
11. övergrepp i rättssak eller skyddande av brottsling enligt 17 kap. 10 § första eller fjärde stycket eller 11 § första eller andra stycket brottsbalken, om det kan antas att brottets straffvärde överstiger fängelse i tre månader,
12. grovt skyddande av brottsling enligt 17 kap. 11 § tredje stycket brottsbalken,
13. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
14. spionerі, utlandsspionerі, 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. 5, 6 a, 7, 8, 10, 10 a eller 10 b § brottsbalken,

[1] Senaste lydelse 2023:534.

15. grovt penningtvättsbrott eller näringspenningtvätt, grovt brott, enligt 5 § eller 7 § andra stycket lagen (2014:307) om straff för penningtvättsbrott,

16. grovt insiderbrott enligt 2 kap. 1 § tredje stycket lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden,

17. företagsspionerи enligt 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,

17. företagsspionerи *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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,

18. deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),

19. försök, förberedelse eller stämpling till ett brott som avses i 1–5, 7, 8, 10 eller 12–18, om en sådan gärning är belagd med straff,

20. försök, förberedelse eller stämpling till ett brott som avses i 6, 9 eller 11, om en sådan gärning är belagd med straff och det kan antas att gärningens straffvärde överstiger fängelse i tre månader,

21. ett annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år, eller

22. flera brott, om

a) en och samma person är skäligen misstänkt för samtliga brott,

b) det kan antas att den samlade brottslighetens straffvärde överstiger fängelse i två år,

c) det kan antas att vart och ett av brotten har utgjort ett led i en brottslighet som har utövats i organiserad form eller systematiskt, och

d) det för vart och ett av brotten är föreskrivet fängelse i ett år eller mer.

Hemlig avlyssning av elektronisk kommunikation enligt denna paragraf får endast avse ett telefonnummer eller en annan adress eller en viss elektronisk kommunikationsutrustning som

1. under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte, eller

2. det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

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] Senaste lydelse 2023:534.

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

2. spionerі, utlandsspionerі eller grovt utlandsspionerі enligt 19 kap. 5, 6 a eller 6 b § brottsbalken,

3. företagsspionerі enligt 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 och det kan antas att brottet inte leder till endast böter,	3. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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. försök, förberedelse eller stämpling till ett brott som avses i 1–3, om en sådan gärning är belagd med straff,

5. ett annat brott, om det kan antas att brottets straffvärde överstiger fängelse i fyra år, eller

6. flera brott, om

a) en och samma person är skäligen misstänkt för samtliga brott,

b) det kan antas att den samlade brottslighetens straffvärde överstiger fängelse i fyra år,

c) det kan antas att vart och ett av brotten har utgjort ett led i en brottslighet som har utövats i organiserad form eller systematiskt, och

d) det för vart och ett av brotten inte är föreskrivet lindrigare straff än fängelse i sex månader eller det är fråga om försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff.

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 eller risk för men för utredningen inte har kunnat lämnas någon underrättelse inom ett år och sex månader från det att tvångsmedelsanvändningen avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller och om det kan ske utan men för utredningen.

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] Senaste lydelse 2024:327.

3. brott som avses i 18 kap. 1, 3, 5 eller 6 § eller 19 kap. 1, 2, 3, 4, 5, 6, 6 a, 6 b, 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. *företagsspionerи eller olovligt röjande av teknisk företagshemlighet enligt* 26 *eller 26 a* § 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 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666), 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.

En underrättelse enligt 31 § ska inte heller lämnas om den person som underrättelsen avser har avlidit eller om den juridiska person som underrättelsen avser har upphört.

34 §[4]

Frågor om tillstånd till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller kvarhållande av försändelse enligt 9 § eller 9 a § andra stycket får vid en förundersökning om följande brott, utöver av domstol som föreskrivs i 19 kap., prövas av Stockholms tingsrätt:

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

2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, grov 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, spionerи, grovt spionerи, utlandsspionerи, grovt utlandsspionerи, 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, 6 a, 6 b, 7, 8, 10, 10 a eller 10 b § brottsbalken,

5. företagsspionerи enligt 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. företagsspionerи *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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

[4] Senaste lydelse 2023:534.

som har agerat för en främmande makts räkning,

6. terroristbrott, deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666), eller

7. försök, förberedelse eller stämpling till ett brott som avses i 1–6, om en sådan gärning är belagd med straff.

Denna lag träder i kraft den 1 januari 2026.

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

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

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
Ett tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § rättegångsbalken, hemlig kameraövervakning enligt 27 kap. 20 a § rättegångsbalken, husrannsakan enligt 28 kap. 1 § rättegångsbalken, undersökning på annat ställe enligt 28 kap. 10 § rättegångsbalken, genomsökning på distans enligt 28 kap. 10 a § rättegångsbalken eller postkontroll enligt 2 § får beviljas 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, grov 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, utlandsspionerі, grovt utlandsspionerі, 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, 6 a, 6 b 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 eller av någon som kommer att agera för en främmande makts räkning,	5. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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, deltagande i en terroristorganisation, grovt brott, samröre med terroristorganisation, grovt brott, finansiering av terrorism eller särskilt allvarlig brottslighet, grovt brott, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, grovt brott, rekrytering till terrorism eller särskilt allvarlig brottslighet, grovt brott, eller utbildning	

[1] Senaste lydelse 2024:560.

för terrorism eller särskilt allvarlig brottslighet, grovt brott, enligt 4 §, 4 a § tredje stycket, 5 § tredje stycket, 6 § tredje stycket, 7 § tredje stycket, 8 § tredje stycket eller 9 § tredje stycket terroristbrottslagen (2022:666), eller

7. mord, grov misshandel, synnerligen grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1 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.

Ett tillstånd enligt första stycket får också beviljas 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.

1 b §[2]

Ett tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § första stycket rättegångsbalken får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar

1. grov mordbrand eller grov allmänfarlig ödeläggelse enligt 13 kap. 2 § eller 3 § tredje stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,

2. uppror eller väpnat hot mot laglig ordning enligt 18 kap. 1 eller 3 § brottsbalken,

3. högförräderi, spionering, grovt spionering, utlandsspionering eller grovt utlandsspionering enligt 19 kap. 1, 5, 6, 6 a eller 6 b § brottsbalken,

4. företagsspionering 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 eller av någon som kommer att agera för en främmande makts räkning och det kan antas att brottet inte leder till endast böter,

4. företagsspionering *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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 och det kan antas att brottet inte leder till endast böter,

5. terroristbrott enligt 4 § terroristbrottslagen (2022:666), eller

6. mord, synnerligen grov misshandel eller människorov enligt 3 kap. 1 § eller 6 § andra stycket eller 4 kap. 1 § 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.

Ett tillstånd enligt första stycket får också beviljas 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.

[2] Senaste lydelse 2024:560.

Denna lag träder i kraft den 1 januari 2026.

1.4 Förslag till lag om ändring i lagen (2024:562) 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, i stället för lydelse enligt lagen (2024:562) om ändring i den lagen, ska ha följande lydelse.

Lydelse enligt SFS 2024:562	*Föreslagen lydelse*
1 §	
Ett tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § rättegångsbalken, hemlig kameraövervakning enligt 27 kap. 20 a § rättegångsbalken eller postkontroll enligt 2 § får beviljas 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, grov 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, utlandsspionerі, grovt utlandsspionerі, 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, 6 a, 6 b 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 eller av någon som kommer att agera för en främmande makts räkning,	5. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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, deltagande i en terroristorganisation, grovt brott, samröre med en terroristorganisation, grovt brott, finansiering av terrorism eller särskilt allvarlig brottslighet, grovt brott, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, grovt brott, rekrytering till terrorism eller särskilt allvarlig brottslighet, grovt brott, eller utbildning för terrorism eller särskilt allvarlig brottslighet, grovt brott, enligt 4 §, 4 a § tredje stycket, 5 § tredje stycket, 6 § tredje stycket, 7 § tredje stycket, 8 § tredje stycket eller 9 § tredje stycket terroristbrottslagen (2022:666), eller	

7. mord, grov misshandel, synnerligen grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1 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.

Ett tillstånd enligt första stycket får också beviljas 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.

1.5 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. spionerі, utlandsspionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5, 6 a eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,

6. företagsspionerі 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. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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. samröre med en terroristorganisation, grovt brott, finansiering av terrorism eller särskilt allvarlig brottslighet, grovt brott, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, grovt brott, rekrytering till terrorism eller särskilt allvarlig brottslighet, grovt brott, eller utbildning för terrorism eller särskilt allvarlig brottslighet, grovt brott, enligt 5 § tredje stycket, 6 § tredje stycket, 7 § tredje stycket, 8 § tredje stycket eller 9 § tredje stycket terroristbrottslagen (2022:666),
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 jour-

[1] Senaste lydelse 2022:1522.

nalistik 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 januari 2026.

1.6 Förslag till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

Härigenom föreskrivs att 6 a kap. 2 § lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område ska ha följande lydelse.

Lydelse enligt prop. 2024/25:37	*Föreslagen lydelse*
6 a kap.	
2 §	
En jämförelse får göras vid en förundersökning om	
1. ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,	
2. sabotage enligt 13 kap. 4 § brottsbalken,	
3. mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1 §, 3 § första eller andra stycket, 5 a § eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,	
4. olovlig kårverksamhet eller brott mot medborgerlig frihet enligt 18 kap. 4 eller 5 § brottsbalken,	
5. spionerи, utlandsspionerи, 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. 5, 6 a, 7, 8, 10, 10 a eller 10 b § brottsbalken,	
6. företagsspionerи enligt 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,	6. företagsspionerи *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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. deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),	
8. försök, förberedelse eller stämpling till ett brott som avses 1–7, om en sådan gärning är belagd med straff, eller	
9. ett annat brott om det kan antas att brottets straffvärde överstiger fängelse i två år.	

Denna lag träder i kraft den 1 januari 2026.

1.7 Förslag till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

Härigenom föreskrivs att 14 § lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

14 §

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 13 §, ska en underrättelse enligt 12 § skjutas upp till dess att sekretess inte längre gäller.

Om det på grund av sekretess eller på grund av att ärendet inte avslutats, inte har kunnat lämnas någon underrättelse enligt 12 § inom ett år och sex månader från det att tvångsmedelsanvändningen avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller.

En underrättelse enligt 12 § ska inte lämnas, om uppgifterna med stöd av 10 § har tagits in i en förundersökning som angår

1. brott som avses i 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brotten 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, 6 a, 6 b, 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. *företagsspionerи eller olovligt röjande av teknisk företagshemlighet enligt* 26 *eller 26 a* § 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 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666), 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.

En underrättelse enligt 12 § ska inte heller lämnas om den person som underrättelsen avser har avlidit eller om den juridiska person som underrättelsen avser har upphört.

Denna lag träder i kraft den 1 januari 2026.

2 Ärendet och dess beredning

I departementspromemorian Bättre skydd för tekniska företagshemligheter (Ds 2020:26) lämnas bl.a. förslag på ett utvidgat straffansvar för angrepp på företagshemligheter. En sammanfattning av promemorian finns i *bilaga 1*. Promemorians lagförslag finns i *bilaga 2*.

Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga på regeringens webbplats (regeringen.se) och i lagstiftningsärendet (Ju2020/04525).

I detta utkast till lagrådsremiss behandlas förslagen i promemorian. I förhållande till promemorian har vissa ändringar gjorts, bl.a. föreslås en delvis annan utformning av straffbestämmelserna om olovligt utnyttjande och olovligt röjande och, till följd av senare ändringar i den hemliga och preventiva tvångsmedelslagstiftningen, att bl.a. fler tvångsmedel ska få användas i syfte att förhindra statsstyrt olovligt röjande av teknisk företagshemlighet.

3 Det straffrättsliga skyddet för företagshemligheter behöver stärkas

3.1 Ett mer heltäckande straffansvar

Utkastets förslag: Det ska bli straffbart att olovligen utnyttja eller röja en företagshemlighet även i de fall personen har lovlig tillgång till företagshemligheten, t.ex. inom ramen för en anställning. Straffansvaret ska omfatta tekniska företagshemligheter som avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst.

Straffansvaret ska gälla den som har tillgång till företagshemligheten genom sitt deltagande i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund. Straffansvar ska även gälla för den som har fått del av företagshemligheten i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution.

Innehavaren av en företagshemlighet ska kunna föra talan om vitesförbud och andra skyddsåtgärder i ett brottmål om ansvar för de nya brotten.

Förslagen i promemorian överensstämmer i huvudsak med utkastets förslag men innebär en annan lagteknisk lösning där de tekniska företagshemligheter som avses i straffbestämmelserna inte preciseras närmare i lagtexten.

Remissinstanserna: De flesta remissinstanser, bl.a. *Säkerhetspolisen, Stockholms tingsrätt (Patent- och marknadsdomstolen), Åklagarmyndigheten, Arbetsgivarverket, Ekobrottsmyndigheten*, *Kungl. Tekniska högskolan, Arbetsdomstolen* och *Konkurrensverket*, tillstyrker förslaget eller har inget att invända emot det.

Ett antal remissinstanser tillstyrker förslaget men anser att uttrycket teknisk natur inte är tydligt och bör preciseras. Bland dessa finns *Sveriges advokatsamfund, FICPI Sweden, Företagarna, Lunds universitet* och *Sveriges patentbyråers förening.*

Stockholms universitet, Patent- och registreringsverket, Läkemedelsindustriföreningen, Svenskt Näringsliv och *Svenska föreningen för immaterialrätt* tillstyrker förslaget men förordar att alla typer av företagshemligheter bör omfattas av kriminaliseringen.

Svea hovrätt avstyrker förslaget mot bakgrund av att avgränsningen till företagshemligheter av teknisk natur inte bedöms ändamålsenlig.

Akademikerförbundet SSR, *Tjänstemännens centralorganisation (TCO)* och *Sveriges ingenjörer* avstyrker förslaget. De anför att det riskerar att leda till inlåsningseffekter på arbetsmarknaden och anser att om kriminalisering ska ske bör den endast omfatta olovligt röjande av företagshemligheter. Även *Journalistförbundet* menar att förslaget får negativa effekter på anställdas vilja att lyfta fram problem på arbetsplatsen.

Några remissinstanser, bl.a. *Stockholms universitet*, *Svenskt Näringsliv*, *Svenska industrins IP förening* och *TCO*, anser att definitionen av den personkrets som kan träffas av straffansvar är oklar och behöver tydliggöras.

Svea hovrätt påtalar att det kan vara svårt att identifiera vilka personer som kan åläggas straffrättsligt ansvar i affärsförhållanden och att kriminaliseringen därför riskerar att leda till ett relativt långtgående straffrättsligt ansvar för en vid krets av personer. Svea hovrätt ifrågasätter också varför inte styrelseledamöter och revisorer omfattas av den personkrets som kan träffas av straffansvar utifrån att även sådana bolagsfunktionärer kan anses delta i en rörelse eller en verksamhet.

Företagarna anser att även oavlönade praktikanter bör omfattas av den personkrets som kan träffas av straffansvaret.

Sveriges advokatsamfund anser att det bör framgå av straffbestämmelsen att företagshemligheten ska ha fåtts i förtroende för att bättre överensstämma med vad som gäller för skadeståndsansvar i samband med affärsförbindelser när det gäller företagshemligheter.

Skälen för utkastets förslag

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. I dagens samhälle är det inte ovanligt att företagshemligheter används som ett strategiskt övervägt alternativ vid sidan av immaterialrättsliga skydd. Stora värden står på spel för enskilda företag och för samhället i stort. 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 medför. Det gäller både för produktionen inom den befintliga industrin och utvecklande, distribution och konsumtion av nya varor och tjänster.

En mer konfliktfylld omvärld leder till en ökad hotbild 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 repre-

senterar stora värden för företag och samhället i stort. Hotet mot företagshemligheter framstår som särskilt påtagligt för svensk industri eftersom den utmärks av en hög kunskapsnivå och innovationskraft. En ökad internationell konkurrens gör också 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 innebär även strukturella sårbarheter och ställer nya krav på skyddet mot 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. De har möjlighet att arbeta långsiktigt och metodiskt med inriktningen att komma över värdefull information som finns i svenska företag och forskningsinstitutioner.

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 underlättas i någon mån 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 stor skada. Även lärosäten och forskningsutförare 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 är på så sätt mer påtaglig i dag än när straffansvaret för angrepp på företagshemligheter utformades på 1980-talet. Behovet av ett mer heltäckande straffrättsligt skydd har därför ökat.

Straffbestämmelserna i lagen (2018:558) om företagshemligheter omfattar inte personer som har lovlig tillgång till den företagshemliga informationen, dvs. personer inom företags och forskningsinstitutioners egna verksamheter. Straffansvaret för företagsspionerі enligt lagen om företagshemligheter omfattar nämligen endast den som olovligen anskaffar företagshemligheten. Motsatsvis innebär det att den som lovligen har tillgång till företagshemligheten, t.ex. som en del av ett arbetsmaterial, inte kan drabbas av sådant straffansvar. Däremot kan andra straffbestämmelser komma i fråga, t.ex. trolöshet mot huvudman enligt 10 kap. 5 § brottsbalken, men de är inte utformade på ett sådant sätt att de ger ett ändamålsenligt skydd för just företagshemligheter. Skadliga angrepp från anställda eller liknande som kan innebära att den företagshemliga informationen hamnar i orätta händer kan alltså falla utanför det allmänt utformade straffansvaret i annan lag, företrädesvis i brottsbalken. Den här bristen bör åtgärdas.

Olovligt utnyttjande och olovligt röjande av en företagshemlighet är som utgångspunkt skadliga gärningar

För personer som inte har lovlig tillgång till en företagshemlighet kan det vara straffbart att bereda sig tillgång till eller anskaffa en företagshemlig-

het (26 och 27 §§ lagen om företagshemligheter). Utifrån lagens systematik är ett olovligt utnyttjande eller ett olovligt röjande av en företagshemlighet de möjliga obehöriga angrepp på en företagshemlighet som den som har lovlig tillgång till den kan göra sig skyldig till. Som utgångspunkt medför sådana angrepp ett skadeståndsansvar enligt lagen, 6 och 7 §§.

Med utnyttjande av en företagshemlighet 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 (proposition En ny lag om företagshemligheter, 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 av en företagshemlighet 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).

Den skada som kan uppkomma till följd av ett olovligt utnyttjande eller ett olovligt röjande av en företagshemlighet kan vara mycket kännbar. Det kan avse illojal konkurrens, att ett möjligt patent går om intet och ytterst uteblivna intäkter. 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 använder information som rätteligen är förbehållen någon annan. Det är fråga om ett illojalt beteende, ett brott mot ett förtroende eller tystnadslöfte.

Akademikerförbundet SSR, TCO och *Sveriges ingenjörer* anser att den kriminaliserade gärningen bör avgränsas till endast röjande. TCO förespråkar dessutom att den straffbara gärningen avgränsas ytterligare genom att det ska krävas att röjandet sker genom användande av något, t.ex. en handling eller en teknisk förebild. En sådan snäv avgränsning bedöms emellertid inte lämplig. Ett olovligt utnyttjande innebär att företagshemligheten hamnar utom innehavarens kontroll och medför vidare en påtaglig risk för skada, både vid hanteringen av företagshemligheten och vid spridning av produkter eller tjänster. Ett exempel på detta är att varor som innehåller företagshemligheten görs tillgängliga för s.k. reverse engineering, en 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 ekonomisk skada för innehavaren. Med en avgränsning till röjande med hjälp av hjälpmedel, såsom TCO förespråkar, skulle straffansvar dessutom kunna kringgås genom att frigöra sig från hjälpmedel genom att memorera den företagshemliga informationen. En sådan risk för kringgående är inte önskvärd. Att avgränsa det straffbara handlandet till endast röjande eller röjande med hjälp av hjälpmedel skulle följaktligen utesluta straffansvar för flera klart klandervärda missbruk som typiskt sett medför en påtaglig risk för skada för innehavaren.

Både utnyttjande och röjande av en företagshemlighet av den som har lovlig tillgång till hemligheten kan innefatta så pass skadliga gärningar att de som utgångspunkt bör kunna komma i fråga för straffansvar.

Straffansvaret ska ta sikte på tekniska företagshemligheter

Företagshemlig information kategoriseras vanligen som kommersiell eller teknisk. Med kommersiella företagshemligheter avses information som tar sikte på ett företags eller en forskningsinstitutions affärsmässiga förhållanden, t.ex. kundlistor och affärsplaner. Tekniska företagshemligheter avser i stället information om själva produktionen eller tillverkningen i ett företag eller vid en forskningsinstitution, t.ex. framställningsprocesser och ritningar. 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

Även om angrepp på alla typer av företagshemligheter typiskt sett är förenade med risk för skada för innehavaren, framstår bristen i det straffrättsliga skyddet som särskilt allvarlig för företag och forskningsinstitutioner som ägnar sig åt – i vid bemärkelse – teknisk produktion av varor eller tjänster. Flera remissinstanser, bl.a. *Kungl. Tekniska högskolan, Företagarna* och *Tillväxtverket*, påtalar att företag och forskningsinstitutioner som ägnar sig åt innovationer och forskning behöver bättre förutsättningar att kunna skydda sina företagshemligheter. Inriktningen på en kriminalisering bör därför vara att träffa sådana angrepp som typiskt sett medför stor skada – eller risk för sådan – för företag och forskningsinstitutioner, och som även påverkar svenskt företagande och svensk innovation negativt.

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. Angrepp på sådan verksamhet är därför vanligtvis 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 makt, kan vidare antas i princip uteslutande riktas mot verksamhet av den typen.

Behovet av skydd för företagshemligheter som avser tekniskt kunnande ska 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 viktigt att företagens konkurrenskraft säkerställs och att förutsättningarna för innovation och kunskapsöverföring förbättras. Skyddet för företagshemligheter är centralt i det sammanhanget.

TCO, Sveriges ingenjörer och *Akademikerförbundet SSR* anser att det nuvarande sanktionssystemet vid angrepp på denna typ av företagshemlig-

heter är tillräckligt och ser inte något behov av utökad kriminalisering. Mot bakgrund av den förändrade hotbilden mot svenska företag och forskningsinstitutioner bedöms det sanktionssystem som idag står till buds – skadestånd och arbetsrättsliga sanktioner – emellertid inte tillräckligt avskräckande. Den eventuella risk för inlåsningseffekter på arbetsmarknaden som en kriminalisering kan innebära överväger inte de starka skäl som föreligger för ett utökat straffrättsligt skydd.

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 regler bl.a. civilrättsliga och straffrättsliga sanktioner. *Sveriges patentbyråers förening* framhåller att det immaterialrättsliga systemet riskerar att urholkas och på sikt försvagas utan ett väl fungerande och väl avvägt straffrättsligt sanktionssystem.

Ett exempel på när skyddet för företagshemligheter kan utgöra ett viktigt komplement till det immaterialrättsliga skyddet 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 utnyttjas eller röjs innan en ansökan om patent tilldelats en ingivningsdag hos Patent- och registreringsverket kan nyhetsvärdet vara förstört och möjligheten att få ett patenträttsligt skydd 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.

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 gällande skydd än patentets tjugo år. För innovativa företag kan användandet av olika sorters skydd vara noga genomtänkt, med en förväntan på ett likartat och väl avvägt sanktionssystem i sin helhet.

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

Även de kommersiella företagshemligheterna kan i många fall motsvara stora värden. För ett litet företag kan exempelvis kundlistan vara den väsentliga tillgången. Ett antal remissinstanser anser att även kommersiella företagshemligheter ska omfattas av en kriminalisering eftersom dessas värde många gånger är jämförbara med de tekniska företagshemligheterna. Bland dessa finns *Svenskt Näringsliv, Stockholms universitet* och *Säkerhets- och försvarsföretagen (SOFF).* Även *Svea hovrätt* förordar en lagteknisk lösning som innefattar alla företagshemligheter och menar att det skulle vara mer ändamålsenligt att i stället dra gränsen för det kriminaliserade området vid grova brott.

De kommersiella företagshemligheterna är visserligen ofta en viktig och värdefull tillgång för företag. Men även om angrepp på kommersiella företagshemligheter kan orsaka skada för innehavaren, framstår hotbilden

mot den typen av företagshemligheter som inte lika allvarlig. Typiskt sett torde angreppen vara mindre kvalificerade. Detsamma gäller för administrativa företagshemligheter. Det kan vidare antas att angrepp som på ett eller annat sätt involverar främmande makt är begränsade till tekniska företagshemligheter. I fråga om kommersiella företagshemligheter handlar det dessutom sällan 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. Att dra gränsen för det kriminaliserade området vid grova brott kan inte heller anses tillfredsställande. Vid en sådan avgränsning av det straffbara området är risken påtaglig att klart straffvärda gärningar alltjämt skulle vara straffria. Det förstärkta skydd för svenskt företagande och svensk innovation som en kriminalisering avser att ge skulle då i flera avseenden utebli.

När det kommer till angrepp från personer inom den egna verksamheten är skälen för en kriminalisering av angrepp på kommersiella företagshemligheter alltså inte lika starka som i fråga om angrepp på tekniska företagshemligheter. Med hänsyn till de andra sanktioner som står till buds bedöms det inte finnas skäl att nu kriminalisera angrepp på kommersiella företagshemligheter från personer med lovlig tillgång till informationen.

Denna slutsats ligger även väl i linje med regeringens uttalande i lagstiftningsärendet om en ny lag om företagshemligheter. Regeringen framhöll då att en straffsanktion endast bör komma i fråga i de fall då det inte råder någon tvekan om att arbetsrättsrättliga åtgärder och skadeståndsskyldighet inte är tillräckligt avskräckande eller ingripande, varför ett straffansvar bör avgränsas till mer kvalificerade fall. Som exempel på ett mindre allvarligt fall nämndes en tidigare anställds utnyttjande av den tidigare arbetsgivarens kundlista för att försöka ta över kundbasen (prop. 2017/18:200 s. 125 och 126).

Kriminaliseringen bör alltså ta sikte på tekniska företagshemligheter som avser innovationer och produktionsmetoder för en vara eller en tjänst.

Förslaget i promemorian är att avgränsningen i lagtext uttrycks så att kriminaliseringen avser angrepp på ”företagshemligheter av teknisk natur”. Flera remissinstanser, bl.a. *Sveriges advokatsamfund, Helsingborgs tingsrätt, FICPI Sweden, Lunds universitet, Företagarna* och Sveriges patentbyråers förening anser att uttrycket ”företagshemligheter av teknisk natur” är otydligt och att de företagshemligheter som avses behöver preciseras närmare. Med beaktande av den straffrättsliga legalitetsprincipen bör avgränsningen av de företagshemligheter som straffbestämmelserna ska omfatta uttryckas mer bestämt. De immaterialrättsliga intresseorganisationerna *AIPPI,* FICPI Sweden och Sveriges patentbyråers förening har förordat att avgränsningen borde utformas i närmare överensstämmelse med uttrycket ”teknisk karaktär” som används i det patenträttsliga systemet. Det uttrycket bedöms dock inte heller lämpligt för att avgränsa de företagshemligheter som avses innefattas av straffbestämmelserna. Detta eftersom uttrycket ”teknisk karaktär” bedöms vara behäftat med samma otydlighet som uttrycket ”teknisk natur” och därför ter sig problematiskt ur legalitetshänseende. Eftersom skydd av företagshemligheter kompletterar den immaterialrättsliga lagstiftningen skulle en sådan avgränsning dessutom kunna leda till att det straffrättsliga skyddet för företagshemligheter tolkas och utvecklas i ljuset av praxis på patenträttens område på ett sätt som inte

är önskvärt och som urholkar det komplement som skyddet av företagshemligheter utgör i det immaterialrättsliga systemet.

De företagshemligheter som i förslaget avses rymmas i ”företagshemligheter av teknisk natur” är sådana tekniska företagshemligheter som avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst. Avgränsningen bör uttryckas i enlighet med detta, vilket tydligare anger vilken typ av information som omfattas av det utökade straffrättsliga skyddet. En sådan ordning blir mer rättssäker. Något krav på att informationen i fråga bör vara av någon särskild kvalitet eller vara särskilt värdefull för att omfattas av avgränsningen bör inte uppställas.

Att det i vissa fall, som bl.a. *Svenskt Näringsliv* och *Stockholms universitet* påtalar, kan vara svårt att särskilja tekniska och kommersiella företagshemligheter innebär inte något starkt skäl emot en sådan avgränsning som nu föreslås. Avgörande för gränsdragningen av den nya kriminaliseringen blir om det är information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst.

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

Anställda och andra medarbetare behöver 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 för innehavaren om det är information av ekonomiskt eller annat värde och som därför är åtråvärd för konkurrenter och andra. Ett sätt för utomstående att komma åt information kan då vara att värva en intern informatör på företaget. I det avseendet saknar det för innehavaren av företagshemligheten betydelse om den person som fått del av företagshemligheten har ett anställningsavtal med innehavaren eller om personen ställt sin arbetskraft till förfogande på annan grund.

Det finns straffbestämmelser som kan vara aktuella vid olika typer av klandervärd hantering av information. Ett exempel är trolöshet mot huvudman (10 kap. 5 § brottsbalken). Straffbestämmelsen omfattar den som på grund av förtroendeställning har fått till uppgift att sköta en ekonomisk angelägenhet för annan eller självständigt hantera en kvalificerad teknisk uppgift eller övervaka skötseln av en sådan angelägenhet eller uppgift och som missbrukar förtroendeställningen till skada för huvudmannen. Det skydd 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 stöld och andra tillgreppsbrott (8 kap. brottsbalken) aktualiseras när det är fråga om tillgrepp av lösa saker av värde, t.ex. en prototyp. En prototyp kan, vid sidan av ett potentiellt försäljningsvärde, representera ett stort värde som bärare av värdefull information. Även brott mot tystnadsplikt (20 kap. 3 § brottsbalken) skulle kunna aktualiseras. Dessa bestämmelser aktualiserar emellertid 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 finns därför 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.

Ett utvidgat straffansvar bör omfatta den som genom sin anknytning till näringsidkaren – dvs. innehavaren av företagshemligheten – får anses delta i dennes rörelse. Dessa personer har typiskt sett lovlig tillgång till företagshemligheter och dessa personer får även anses ha en typ av lojalitetsplikt mot innehavaren av företagshemligheten. Att straffansvaret utformas på så sätt att det inte endast omfattar anställda välkomnas av bl.a. *Svenskt Näringsliv* och *Stockholms universitet*, som särskilt framhåller att den föreslagna omfattningen av personkretsen ligger i linje med arbetsmarknadens utveckling och företagens verklighet i fråga om anlitande av arbetskraft.

I första hand gäller det näringsidkarens egna anställda. Ansvaret bör också omfatta andra som har en liknande ställning 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.

Bemanningsanställda anses normalt sett inte ha någon lojalitetsplikt mot det inhyrande företaget och har som regel inte heller någon nu relevant avtalsrelation till det inhyrande företaget. Trots avsaknaden av en allmän lojalitetsplikt utgör bemanningsanställda typiskt sett en sådan kategori arbetstagare som deltar i innehavarens rörelse och som när det gäller handhavande av företagshemligheter bör likställas med andra arbetstagare.

Näringsidkaren är för samtliga av dessa typer av arbetstagare – anställda eller sådana som är knutna till företaget på annan grund – beroende av att de inte olovligen angriper företagshemligheter som de anförtros.

Ett antal remissinstanser, bl.a. *Företagarna, Svea hovrätt* och *TCO*, anser att definitionen av personkretsen är otydlig, särskilt vad avser den personkategori som omfattas av den föreslagna avgränsningen ”på annan liknande grund” och att detta kan leda till oförutsebarhet i tillämpningen.

Avgränsningen av personkretsen bedöms emellertid vara tillräckligt tydlig. Mot bakgrund av att de personer som idag kan komma i kontakt med företag för att utföra arbete i större utsträckning än förr inte endast är anställda, utan även bl.a. bemanningsanställda och konsulter, är det inte ändamålsenligt att i lagtext närmare än vad som nu föreslås definiera den berörda personkretsen. Om så skulle ske riskerar lagtexten att inte omfatta personer, som i takt med en föränderlig arbetsmarknad, med fog bör omfattas av kriminaliseringen. Den föreslagna avgränsningen av personkretsen bedöms därför vara väl anpassad till dagens förhållanden hos företag och därmed också ändamålsenlig.

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. 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.

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

Straffansvar bör gälla för anställda, vissa uppdragstagare och andra som på liknande grund deltar i en forskningsinstitutions verksamhet

Även vid universitet och högskolor samt hos andra forskningsutförare kan det finnas värdefulla företagshemligheter. Internationella forskningssamarbeten är i många fall avgörande för spetsforskning och innovation men kan också innebära vissa risker. I en alltmer osäker och polariserad värld finns geopolitiska utmaningar där öppenhet och samarbete riskerar att utnyttjas av främmande makt på ett otillbörligt sätt. *Kungl. Tekniska högskolan* framhåller att dagens sanktionssystem är otillräckligt i förhållande till forskningsmiljöer som präglas av stor personrörlighet och där tillhörigheten till forskningsinstitutionen inte alltid grundar sig på anställningsförhållanden.

Det finns därför ett behov av ett 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 som avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst 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.

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

Det förekommer inte sällan att företagshemligheter utväxlas vid affärsförbindelser. En särskild fråga är därför om det är motiverat med ett straffansvar även för olovligt utnyttjande och olovligt röjande av tekniska företagshemligheter som någon har anförtrotts inom ramen för en sådan förbindelse.

Det straffansvar som nu föreslås är kvalificerat i det att det endast träffar utnyttjande och röjande av tekniska företagshemligheter.

Att avgränsa 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 saknar det typiskt sett betydelse huruvida hans eller hennes företagshemlighet olovligen angrips av en anställd eller om angreppet

i stället utförs av en affärskontakt som har anförtrotts känslig information. Företag i olika branscher kan ha olika behov i fråga om personalförsörjning och kan organisera sig på olika sätt. Det kan påverka vilka typer av aktörer som behöver få del av företagshemligheter. Omständigheten att innehavaren typiskt sett har större möjligheter att få ekonomisk ersättning vid missbruk av en affärspart talar inte emot att straffansvaret utvidgas. Detta 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 sådan makts räkning. Främmande makt har under senare år visat större intresse för civila verksamheter, så väl företag som forskningsinstitutioner, och det förekommer även att underrättelsetjänster använder sig av bulvanföretag för att komma åt information. Det vore olyckligt om ett straffansvar inte omfattar även sådana fall då en affärspart röjer hemligheten till främmande makt eftersom det då finns en risk att utländska underrättelseinsatser styrs om till affärsförbindelser med svenska företag. 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 skulle 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 därför innefatta den som olovligen utnyttjar eller röjer en teknisk företagshemlighet hos en näringsidkare eller en forskningsinstitution som han eller hon har fått del av i samband med en affärsförbindelse med näringsidkaren eller forskningsinstitutionen. En sådan omfattning av personkretsen i straffrättsligt hänseende motsvarar i stort också vad som gäller i fråga om skadeståndsansvar (jfr 6 § lagen om företagshemligheter). Till skillnad från vid skadeståndsansvaret är det emellertid den person som olovligen utnyttjar eller röjer företagshemligheten som åläggs straffansvar och inte, som kan vara fallet vid skadeståndsansvar, företaget som ingått affärsförbindelsen med innehavaren. Den omständighet som *Svea hovrätt* lyfter fram, att det kan vara svårt att identifiera den person som kan åläggas straffansvar i dessa fall, utgör inte hinder mot att den berörda personkretsen bestäms i enlighet med vad som nu föreslås. Eventuella svårigheter att ringa in den person som rent faktiskt olovligt utnyttjat eller röjt företagshemligheten ska inte överdrivas. Typiskt sett bör det inte råda någon oklarhet i fråga om att en person som har tydlig koppling till en affärspart och som utnyttjar eller röjer en företagshemlighet omfattas av straffansvar.

Något uttryckligt krav på att mottagaren har fått del av företagshemligheten i förtroende, så som *Advokatsamfundet* förespråkar, bör inte uppställas. För att straffansvar ska komma i fråga förutsätts att utnyttjandet eller

röjande sker olovligen. I det ligger att den företagshemliga informationen mottagits under sådana former att det står klart att informationen inte får utnyttjas eller röjas. Ett uttryckligt krav på att den företagshemliga informationen har lämnats ut i förtroende till mottagaren bedöms därför som obehövligt.

Straffansvaret bör inte gälla för styrelseledamöter eller revisorer i juridiska personer om det har samband med fullgörandet av uppdraget

Styrelseledamöter och revisorer i t.ex. ett aktiebolag kan inom ramen för sina respektive uppdrag komma att ta del av företagshemligheter. Dessa funktionärers skadeståndsansvar regleras inte i lagen om företagshemligheter (10 § andra stycket, prop. 2017/18:200 s. 70–71 och 159). Att de undantagits 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 (bet. 1988/89:LU30 s. 30–31. 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 vid fullgörandet av uppdraget angriper bolagets företagshemligheter kan dock bli föremål för andra skyddsåtgärder enligt lagen om företagshemligheter, t.ex. ett beslut om vitesförbud. 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).

Revisorn har vidare 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 disciplinära åtgärder vidtas av Revisorsinspektionen. Det kan då bli fråga om bl.a. varning, indragen auktorisation eller sanktionsavgift (32–35 §§ revisorslagen).

Även i fråga om straffansvar finns ett antal bestämmelser 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 gärningar, utan på t.ex. uppsåtligt brott mot det s.k. spridningsförbudet (30 kap. 1 § aktiebolagslagen). Vid olovligt utnyttjande eller olovligt röjande av en teknisk företagshemlighet, som en styrelseledamot eller revisor har haft lovlig tillgång till, skulle dock ansvar för trolöshet mot huvudman enligt 10 kap. 5 § brottsbalken kunna aktualiseras. En sådan förtroendeställning som förutsätts för ansvar enligt paragrafen intar typiskt sett bl.a. styrelseledamöter och revisorer i aktiebolag. För dessa finns därmed redan ett straffansvar för det fall de missbrukar sin förtroendeställning genom att utnyttja eller röja företagshemligheter och därigenom skadar huvudmannen.

I promemorians förslag undantas styrelseledamöter och revisorer genom kravet på deltagande i rörelsen eller verksamheten. *Svea hovrätt* anser att i vart fall styrelseledamöter kan anses delta i en verksamhet eller rörelse när de är med och fattar beslut om åtgärder inom bolagets normala affärsverksamhet. Även om det kan anses finnas visst fog för den uppfattningen bedöms en styrelseledamots fullgörande av sitt uppdrag inte jämförbart med ett sådant deltagande i en verksamhet eller rörelse som följer av en anställning eller liknande förhållande. En sådan funktionär kan därför inte anses uppfylla kravet på deltagande genom att fullgöra sitt uppdrag. 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 uppdraget som styrelseledamot.

Mot bakgrund av de olika möjligheter till rättsliga sanktioner som redan i dag finns vad gäller styrelseledamöter och revisorer när dessa angriper företagshemligheter som de fått del av vid fullgörandet av sitt uppdrag bedöms det inte finnas behov av ett utökat straffansvar för styrelseledamöter eller revisorer. Av systematiska skäl finns det också ett värde i att inte frångå den valda ordningen för att reglera dessa aktörers ansvar. Sammantaget görs därför bedömningen att det i dagsläget inte har framkommit tillräckliga skäl för att låta styrelseledamöter och revisorer omfattas av straffansvaret.

Brottsbeteckning och uppsåtskrav

Det utvidgade straffansvaret omfattar olovliga angrepp på tekniska företagshemligheter. Närmast till hands ligger att benämna brotten olovligt utnyttjande av teknisk företagshemlighet respektive olovligt röjande av teknisk företagshemlighet. Sådana brottsbeteckningar beskriver på ett tydligt sätt, vilket *Lunds universitet* förordar, den straffbara gärningen och bör därför användas.

I fråga om subjektiv täckning kan olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet inte anses vara så allvarliga gärningar att även oaktsamhet ska bestraffas. Kriminaliseringen ska därför endast avse uppsåtliga gärningar.

Talan om vitesförbud i ett brottmål

Innehavaren av en företagshemlighet har enligt 22 § första stycket lagen om företagshemligheter möjlighet att föra talan om vitesförbud och andra skyddsåtgärder i syfte att hindra framtida angrepp på företagshemligheten. En talan om vitesförbud och andra skyddsåtgärder handläggs som tvistemål. Det är emellertid möjligt för innehavaren att föra talan om dessa frågor även i ett brottmål om ansvar för företagsspionerі och olovlig befattning med företagshemlighet (22 § andra stycket). Samma möjlighet för innehavaren att föra talan om vitesförbud och andra skyddsåtgärder bör finnas i ett brottmål om ansvar för de nya brotten.

3.2 Ringa fall

Utkastets förslag: Ringa fall av olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet ska

inte utgöra brott. Vid bedömningen av om gärningen är ringa ska, när fråga är om anställningsförhållande eller liknande grund, särskilt beaktas om gärningen är mindre allvarlig på grund av att den har begåtts efter att deltagandet i en näringsidkares rörelse eller forskningsinstitutions verksamhet har upphört.

Förslaget i promemorian överensstämmer huvudsakligen med utkastets förslag. I promemorian föreslås att straffansvar då deltagandet i verksamheten eller rörelsen upphört ska regleras särskilt och att det för straffbarhet ska krävas att det föreligger synnerliga skäl.

Remissinstanserna: De flesta remissinstanser tillstyrker förslagen eller har inget att invända emot dem.

Åklagarmyndigheten invänder mot användningen av uttrycket synnerliga skäl i ett straffbud och påtalar att det kan leda till att straffbestämmelsens tillämpningsområde blir snävare än vad som avsetts. Liknande synpunkter framförs av *Säkerhets- och försvarsföretagen.*

Svenskt Näringsliv anser att skillnaden i fråga om ansvar mellan personer som deltar i en verksamhet eller rörelse jämfört med dem vars deltagande har upphört blir för stor.

Akademikerförbundet SSR framhåller att det föreligger en risk för inlåsningseffekter på arbetsmarknaden trots krav på synnerliga skäl efter anställningens upphörande.

Skälen för utkastets förslag: Till skillnad från de befintliga straffbestämmelserna omfattar kriminaliseringen 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.

Ringa fall av olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk 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, såsom gärningens farlighet, det värde den angripna företagshemligheten avsett och vilken skada gärningen medfört.

En särskild fråga är hur ansvaret efter att ett deltagande i en verksamhet eller en rörelse har upphört ska regleras.

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. Det är 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.

Förslaget i promemorian är att ansvar i sådana fall ska regleras särskilt och att det för straffbarhet ska krävas att det föreligger synnerliga skäl. *Åklagarmyndigheten* liksom *Säkerhets- och försvarsföretagen* påpekar att uttrycket synnerliga skäl inte används inom straffrätten för att bestämma det kriminaliserade området och att användningen av uttrycket riskerar att leda till att klart straffbara gärningar faller utanför det straffbara området. Liknande synpunkter framförs av *Svenskt Näringsliv* som även påtalar att förändringen i ansvar efter anställningens upphörande blir alltför stor.

Liksom promemorian funnit bör angrepp som sker efter att deltagandet i verksamheten eller rörelsen upphört endast undantagsvis ska kunna föranleda straffansvar. En annan ordning skulle innebära risk för inlåsningseffekter på arbetsmarknaden. Det skulle även innebära ett omotiverat avsteg från huvudregeln om arbetstagares frihet att utnyttja sin kunskap och erfarenhet på den öppna arbetsmarknaden. En sådan ordning innebär, vilket Svenskt Näringsliv påtalar, en skillnad i fråga om ansvar vid pågående deltagande i en verksamhet eller rörelse jämfört med när deltagandet upphört. Med beaktande av angivna arbetstagarhänsyn bedöms en sådan skillnad emellertid godtagbar. Dessa fall bör emellertid som regel bedömas som ringa. Att låta den omständigheten att gärningen har begåtts efter att deltagandet i verksamheten eller rörelsen upphört ingå som ett kriterium vid helhetsbedömningen av om gärningen är att anse som mindre allvarlig och därmed ringa innebär också att det, ur straffrättsligt hänseende, problematiska uttrycket synnerliga skäl undviks. Detta samtidigt som de klart straffvärda fallen av olovligt utnyttjande eller röjande efter att deltagandet i rörelsen eller verksamheten upphört alltjämt kan föranleda straffansvar.

Sammanfattningsvis bör ringa fall av olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet inte vara straffbara. Vid bedömningen om en gärning är ringa ska särskilt beaktas om gärningen har begåtts efter att deltagandet i rörelsen eller verksamheten har upphört. En sådan avgränsning av det kriminaliserade området bedöms upprätthålla en rimlig balans mellan arbetstagarnas behov av att fritt kunna byta arbetsgivare och behovet hos innehavarna av företagshemligheter av att skydda dessa.

Beträffande affärsförbindelser gör sig inte motsvarande intressen av rörligheten på arbetsmarknaden gällande. Det bedöms därför inte motiverat att låta avslutade affärsförbindelser utgöra en särskild omständighet att beakta vid bedömningen av om gärningen är att anse som ringa eller inte.

3.3 Straffskalor

Utkastets förslag: Straffet 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.

Förslagen i promemorian överensstämmer med utkastets förslag.

Remissinstanserna: Samtliga remissinstanser tillstyrker förslagen eller har inget att invända emot dem.

Skälen för utkastets förslag

Straffskalan för olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet

De två nya straffbestämmelserna har påtagliga likheter med varandra och med företagsspionieri. Samtliga avser ursprungliga angrepp på företagshemligheter och de kan även i fråga om gärningarnas allvar sägas vara likartade. Straffskalan för de nya brotten bör därför vara densamma som

för företagsspioneri och det bör även införas en särskild straffskala för de allvarligaste fallen.

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

Kvalifikationsgrunder för grovt brott

I fråga om företagsspioneri 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). Det är naturligt att samma omständigheter särskilt ska beaktas även vid bedömningar av om ett olovligt utnyttjande eller röjande av teknisk företagshemlighet utgör ett grovt brott.

3.4 Försök och förberedelse till brott ska vara straffbart

Utkastets förslag: Försök och förberedelse till olovligt utnyttjande av teknisk företagshemlighet respektive olovligt röjande av teknisk företagshemlighet ska straffbeläggas.

Förslaget i promemorian överensstämmer med utkastets förslag.

Remissinstanserna: Samtliga remissinstanser tillstyrker förslagen eller har inget att invända emot dem.

Skälen för utkastets förslag: 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 endast på grund av tillfälliga omständigheter. För straffansvar krävs även uppsåt till samtliga gärningsmoment, även de som inte fullbordats.

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 eller gjort sig skyldig till ett straffbart försök till brott samt att det finns mer än ringa fara för att brottet ska fullbordas eller 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 teknisk företagshemlighet är typiskt sett en så allvarlig gärning att ett straffansvar bör kunna aktualiseras under de förutsättningar som anges 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 yttersta vikt att det finns möjlighet att avbryta ett pågående förlopp innan skada uppstår och att det även under sådana omständigheter finns möjlighet att lagföra försök och förberedelse. De nya brotten bör alltså enligt regeringens bedömning, i likhet med företagsspionerі, vara straffbara också på försöks- och förberedelsestadiet.

3.5 Straffansvaret för olovlig befattning med företagshemlighet ska anpassas till olovligt röjande av teknisk företagshemlighet

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

Förslaget i promemorian överensstämmer med utkastets förslag.

Remissinstanserna: Samtliga remissinstanser tillstyrker förslaget eller har inget att invända emot det.

Skälen för utkastets förslag: Den som anskaffar en företagshemlighet som har åtkommits genom en gärning som utgör företagsspionerі döms för olovlig befattning med företagshemlighet (27 §). Även i situationer när ett anskaffande skett genom att en annan person, eller någon före honom eller henne, har röjt en företagshemlighet, är gärningen sådan att den kan medföra påtagliga skada eller fara. Det finns därför skäl att låta straffansvaret för olovlig befattning med företagshemlighet 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 teknisk företagshemlighet. Även 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. Finns inget förbrott ska således inte ansvar för olovlig befattning med företagshemlighet komma i fråga.

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 teknisk företagshemlighet eller något annat brott.

Motsvarande skäl gör sig inte gällande i förhållande till brottet olovligt utnyttjande av teknisk 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 §. Mot bakgrund av detta saknas det därför skäl att låta straffansvar för olovlig befattning med företagshemlighet vid ett föregående olovligt utnyttjande av teknisk företagshemlighet omfattas av kriminaliseringen.

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

Utkastets förslag: Den som gör sig skyldig till olovligt utnyttjande av teknisk företagshemlighet eller olovligt röjande av teknisk företagshemlighet ska ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten på något annat sätt utnyttjas eller röjs.

Förslaget i promemorian överensstämmer huvudsakligen med utkastets förslag. I promemorian föreslås en delvis annan lydelse av skadeståndsbestämmelsen.

Remissinstanserna: De flesta av remissinstanserna tillstyrker förslaget eller har inga synpunkter på det. Bland dessa finns *Ekobrottsmyndigheten*, *Åklagarmyndigheten*, *Säkerhetspolisen*, *Svenskt Näringsliv*, *Stockholms universitet* och *Sveriges advokatsamfund.*

Skälen för utkastets förslag: I lagen om företagshemligheter finns flera bestämmelser om skadestånd, t.ex. för angrepp i samband med en affärsförbindelse (6 §) och 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 (5 §) är mer omfattande än vid andra skadliga gärningar. 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 (proposition om skydd för företagshemligheter, prop. 1987/88:155 s. 41–42 och 58). Vid brott enligt lagen om företagshemligheter kan gärningsmannen alltså bli skadeståndsansvarig, inte bara för skada orsakad av sin egen brottsliga gärning, utan även för skada som uppkommer exempelvis till följd av att någon annan i ett senare led utnyttjar den företagshemlighet som tillgängliggjorts genom brott.

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

Skadeståndsskyldighet på grund av brott enligt lagen bör därför gälla också för skadegörande handlingar som omfattas av de nya straffbestämmelserna.

Genom att det införs ett skadeståndsansvar för den som begår brottet olovligt utnyttjande av teknisk företagshemlighet eller olovligt röjande av

teknisk 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. Skadeståndsansvaret på grund av brott är emellertid mer vidsträckt än annat skadeståndsansvar enligt lagen, eftersom det omfattar även skada som uppstår på grund av att företagshemligheten på något annat sätt utnyttjas eller röjs. Den överlappning som i och för sig finns bedöms med hänsyn till detta inte orsaka några tillämpningsproblem.

5 Särskilda frågor om brottsbekämpning vid statsstyrt olovligt röjande av företagshemlighet

Utkastets förslag: Hemliga tvångsmedel ska få användas vid en förundersökning om statsstyrt olovligt röjande av teknisk företagshemlighet. Det gäller hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning. Vid en förundersökning om statsstyrt olovligt röjande av teknisk företagshemlighet ska undantaget från skyldigheten att underrätta den som har varit föremål för ett hemligt tvångsmedel gälla.

Preventiva tvångsmedel ska få användas i syfte att förebygga, förhindra eller upptäcka statsstyrt olovligt röjande av teknisk företagshemlighet. Det gäller hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning, postkontroll, hemlig dataavläsning, husrannsakan, undersökning på annat ställe och genomsökning på distans som vidtas med stöd av lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen).

Biometrisk jämförelse ska få göras mot Migrationsverkets register över fingeravtryck och fotografier vid statsstyrt olovligt röjande av teknisk företagshemlighet.

Förslagen i promemorian överensstämmer i huvudsak med förslagen i utkastet. Både förslagen i promemorian och förslagen i utkastet innebär att möjligheterna till användning av hemliga och preventiva tvångsmedel vid statsstyrt olovligt röjande av teknisk företagshemlighet ska vara desamma som vid statsstyrt företagsspionerі. Förslagen i promemorian utgår från den tvångsmedelsreglering som gällde då, och innehåller därför inte förslag om att hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter även ska få användas för att utreda vem som skäligen kan misstänkas för statsstyrt

olovligt röjande av teknisk företagshemlighet. Promemorian innehåller inte heller förslag om att hemlig rumsavlyssning, hemlig dataavläsning som gäller rumsavlyssningsuppgifter, husrannsakan, undersökning på annat ställe eller genomsökning på distans ska få användas för att förhindra statsstyrt olovligt röjande av teknisk företagshemlighet. Det finns i promemorian inte något förslag om biometrisk jämförelse mot Migrationsverkets register över fingeravtryck och fotografier.

Remissinstanserna: Samtliga remissinstanser utom *Integritetsskyddsmyndigheten* tillstyrker förslagen om möjligheterna att använda hemliga och preventiva tvångsmedel eller har inga invändningar mot dem.

Integritetsskyddsmyndigheten anser dels att förslagen behöver kompletteras med en särskild integritetsanalys, dels att de avvägningar och bedömningar som gjorts vad gäller proportionaliteten, behovet och nyttan av förslagen behöver fördjupas och redovisas tydligare.

Skälen för utkastets förslag

Regleringen om hemliga och preventiva tvångsmedel

Kriminaliseringen av olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet innebär, liksom vid brott i allmänhet, att straffprocessuella tvångsmedel enligt 24–28 kap. rättegångsbalken kan komma att användas under förundersökningen. Vilka tvångsmedel som är tillgängliga styrs bl.a. av brottens straffskala. För vissa brott anges särskilt att tvångsmedlet i fråga ska vara tillämpligt.

Hemliga tvångsmedel får enligt nuvarande ordning användas vid en förundersökning om statsstyrt företagsspionerі, dvs. när det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av främmande makt eller av någon som agerat för främmande makts räkning, eftersom det brottet nämns särskilt i de brottskataloger som är kopplade till de olika hemliga tvångsmedlen. De hemliga tvångsmedel som kan användas för att utreda statsstyrt företagsspionerі är hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning (27 kap. 18–20 e §§ rättegångsbalken och 4–6 §§ lagen (2020:62) om hemlig dataavläsning). För att hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter ska få användas krävs dock att det kan förväntas att brottet inte endast leder till böter (se t.ex. 27 kap. 20 d § rättegångsbalken).

Preventiva tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) och lagen om hemlig dataavläsning kan användas för att förebygga, förhindra och upptäcka statsstyrt företagsspionerі, eftersom brottet anges i de särskilda brottskataloger som är kopplade till tvångsmedlen. När det gäller hemlig rumsavlyssning enligt preventivlagen och hemlig dataavläsning som gäller rumsavlyssningsuppgifter i preventivlagsfallen krävs det dock att det kan antas att brottet inte leder till endast böter för att tvångsmedlen ska få användas.

Senare års förstärkningar av de brottsbekämpande myndigheternas möjligheter att använda hemliga och preventiva tvångsmedel

Hemliga tvångsmedel kan användas i olika skeden av det brottsbekämpande arbetet, både för att förebygga, förhindra eller upptäcka allvarlig brottslig verksamhet i underrättelseverksamhet (s.k. preventiva tvångsmedel) och för att utreda brott i en förundersökning. Regleringen av de traditionellt sett hemliga tvångsmedlen, dvs. hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning återfinns huvudsakligen i 27 kap. rättegångsbalken. Tvångsmedelsanvändning enligt rättegångsbalken förutsätter att det finns en konkret misstanke om brott som är föremål för en förundersökning. Regleringen av de preventiva tvångsmedlen återfinns däremot i flera lagar, bl.a. i preventivlagen och inhämtningslagen. Hemlig dataavläsning, som får användas både i en förundersökning och i underrättelseverksamhet, regleras i lagen om hemlig dataavläsning.

Den hemliga tvångsmedelsregleringen är uppbyggd på så sätt att ett visst hemligt tvångsmedel får användas för att utreda brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, två år eller fyra år beroende på vilket hemligt tvångsmedel det är fråga om. Därutöver får hemliga tvångsmedel användas om straffvärdet för ett brott eller det samlade straffvärdet för flera brott överstiger en viss nivå eller om brottet anges i den särskilda brottskatalog som är kopplad till tvångsmedlet i fråga.

Förutsättningarna för att använda preventiva tvångsmedel regleras i flera lagar. För tvångsmedelsanvändning enligt preventivlagen och lagen om hemlig dataavläsning i preventivlagsfallen krävs att den brottsliga verksamhet som avses innefattar ett brott som räknas upp i den särskilda brottskatalog som är kopplad till tvångsmedlet i fråga (1–1 c §§ preventivlagen och 7 § lagen om hemlig dataavläsning). Inhämtningslagen är dock uppbyggd på ett annat sätt. För tvångsmedelsanvändning enligt inhämtningslagen och lagen om hemlig dataavläsning i inhämtningslagsfallen krävs antingen att den brottsliga verksamheten innefattar ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller brott som räknas upp i de särskilda brottskataloger som finns i lagen (2 och 2 a §§ inhämtningslagen och 10 § lagen om hemlig dataavläsning).

I samtliga fall där användning av hemliga och preventiva tvångsmedel kommer i fråga ska en proportionalitetsbedömning göras. Skälen för att använda tvångsmedlet måste väga upp det intrång eller men i övrigt som åtgärden innebär för den person som åtgärden riktas mot eller för något annat motstående intresse för att tvångsmedlet ska få användas. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som kan vinnas med åtgärden (propositionen om vissa tvångsmedelsfrågor, prop. 1988/89:124 s. 26). Vid avvägningen är det viktigt att noggrant pröva samtliga omständigheter och väga dem som talar för mot dem som talar mot att en viss åtgärd används. En sådan prövning kan leda till att en åtgärd inte tillåts trots att de krav som lagen i övrigt ställer upp är uppfyllda (propositionen Modernare regler för användningen av tvångsmedel, prop. 2021/22:119 s. 85).

I takt med att samhället, brottsligheten och tekniken utvecklats har regleringen om hemliga och preventiva tvångsmedel också ändrats. På senare tid har möjligheterna att använda både hemliga och preventiva tvångsmedel

utökats på flera olika sätt. Genom lagändringar som trädde i kraft den 1 oktober 2023 utökades t.ex. möjligheterna att använda preventiva tvångsmedel med stöd av preventivlagen till att omfatta även vissa brott som begås inom kriminella nätverk, däribland mord, allmänfarlig ödeläggelse och allvarliga narkotika- och vapenbrott. Samtidigt utökades möjligheterna att använda hemliga tvångsmedel i en förundersökning, bl.a. på så sätt att hemlig avlyssning av elektronisk kommunikation och motsvarande hemlig dataavläsning får användas för att utreda vem som skäligen kan misstänkas för brott och att ett tillstånd till hemlig kameraövervakning, hemlig rumsavlyssning och motsvarande hemlig dataavläsning får riktas mot en skäligen misstänkt person i stället för en plats. Dessutom gjordes en viss omstrukturering av bestämmelserna i 27 kap. rättegångsbalken i syfte att förenkla regleringen (propositionen Hemliga tvångsmedel effektiva verktyg för att förhindra och utreda allvarliga brott, prop. 2022/23:126). Sedan den 1 juli 2024 är det även möjligt att, bl.a. med stöd av den nya lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, använda vissa hemliga tvångsmedel för att lokalisera personer som håller sig undan eller har avvikit från ett beslut om anhållande eller häktning eller från verkställighet av ett straff (se propositionen Bättre möjligheter att verkställa frihetsberövanden, prop. 2023/24:108). Genom lagändringar som trädde i kraft den 1 september 2024 utökades möjligheterna att använda preventiva tvångsmedel ytterligare, bl.a. på så sätt att fler tvångsmedel, t.ex. hemlig rumsavlyssning, husrannsakan och genomsökning på distans, får användas för att förhindra brottslig verksamhet med stöd av preventivlagen (se propositionen Preventiva tvångsmedel för att förebygga och förhindra allvarliga brott, prop. 2023/24:117). Dessutom har regeringen i propositionen Hemlig dataavläsning mot allvarliga brott (prop. 2024/25:51), som överlämnades till riksdagen i november 2024, föreslagit bl.a. att lagen om hemlig dataavläsning ska gälla utan tidsbegränsning. Det har alltså skett omfattande förändringar av regleringen om hemliga och preventiva tvångsmedel sedan promemorian togs fram.

Hemliga tvångsmedel ska få användas i en förundersökning om statsstyrt olovligt röjande av teknisk företagshemlighet

Straffskalan för olovligt röjande av teknisk företagshemlighet föreslås vara böter eller fängelse i högst två år. Vid grovt brott föreslås straffskalan vara fängelse i minst sex månader och högst sex år. Det är alltså samma straffskala som för företagsspionerі.

Vid bedömningen av om ett nytt brott bör läggas till i brottskatalogerna för de hemliga tvångsmedlen är regeringsformens, Europakonventionens och EU:s rättighetsstadgas reglering om grundläggande fri- och rättigheter en väsentlig utgångspunkt. Utvidgade brottskataloger medför begränsningar av rätten till förtroliga meddelanden, rätten till privatliv och rätten till skydd mot intrång i den personliga integriteten. En sådan begränsning får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Som *Integritetsskyddsmyndigheten* lyfter fram måste behovet och nyttan av åtgärderna redovisas och en särskild proportionalitetsbedömning göras.

Möjligheten att använda hemliga tvångsmedel vid en förundersökning om statsstyrt företagsspionerі motiveras av att sådant spionerі kan få allvarliga ekonomiska konsekvenser för svenska företag och i förlängningen för svenska samhällsintressen som är avgörande för välståndet. Brottslighet av sådant slag riskerar även att försämra förutsättningarna för att utveckla och bibehålla skyddet för landets säkerhet. Detta särskilt som det i praktiken ofta kan saknas någon klar gräns mellan sedvanligt spionerі och statsstyrt företagsspionerі (propositionen Åtgärder för att utreda vissa samhällsfarliga brott m.m., prop. 2007/08:163 s. 55). Det är fråga om allvarlig brottslighet av kvalificerat slag.

Ett statsstyrt olovligt röjande av teknisk företagshemlighet har, som konstaterats i promemorian, sådana likheter med sedvanligt spionerі och statsstyrt företagsspionerі att det är motiverat att likställa dem när det gäller användningen av hemliga tvångsmedel. Även statsstyrt olovligt röjande av teknisk företagshemlighet riskerar att allvarligt skada svenska företag och i förlängningen även samhället i stort. Många gånger kan det dessutom antas att statsstyrt företagsspionerі och statsstyrt olovligt röjande av teknisk företagshemlighet begås i samma brottsliga upplägg, med en gärningsman på insidan av företaget eller forskningsinstitutionen och en gärningsman på utsidan. I likhet med spionerі och statsstyrt företagsspionerі är statsstyrt olovligt röjande av teknisk företagshemlighet också svårt att utreda, eftersom de personer som begår brotten i regel är professionella och har ett väl utvecklat säkerhetstänkande samt stora resurser (prop. 2007/08:163 s. 54). Det är viktigt att de brottsutredande myndigheterna har effektiva verktyg vid utredning av denna typ av brottslighet. Det finns alltså ett påtagligt behov av att kunna använda hemliga tvångsmedel för att utreda statsstyrt olovligt röjande av teknisk företagshemlighet, på samma sätt som vid statsstyrt företagsspionerі, och sådana åtgärder kan också förväntas vara effektiva.

Genom att lägga till statsstyrt olovligt röjande av teknisk företagshemlighet i brottskatalogerna för de hemliga tvångsmedlen utökas tillämpningsområdet för tvångsmedlen. Fler personer än i dag kan förväntas bli föremål för hemliga tvångsmedel. En användning av tvångsmedel för att utreda vem som skäligen kan misstänkas för ett visst brott innebär också en ökad risk för att hemliga tvångsmedel används mot personer som visar sig inte vara delaktiga i brott. Därtill kommer risken för att tredje man kan drabbas av tvångsmedelsanvändningen. Förslagen innebär sammantaget en ökad risk för intrång i den personliga integriteten.

När det gäller statsstyrt olovligt röjande av teknisk företagshemlighet är det fråga om allvarlig brottslighet av kvalificerat slag som är särskilt svårutredd, vilket motiverar att hemliga tvångsmedel ska få användas för att utreda brottsligheten. Regleringen om hemliga tvångsmedel omges av ett väl utbyggt system med rättssäkerhetsgarantier som syftar till att begränsa integritetsintrånget för enskilda och att möjliggöra en effektiv tillsyn. Sammantaget bedöms förslagen innebära en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet i det här fallet.

Som huvudregel gäller att den som har utsatts för ett hemligt tvångsmedel, eller närmare berörs av att ett hemligt tvångsmedel har använts, också inom viss tid ska underrättas om tvångsmedelsanvändningen (27 kap. 31 § rättegångsbalken). Det finns dock undantag från under-

rättelseskyldigheten. Exempelvis undantas Säkerhetspolisens tvångsmedelsanvändning vid förundersökning av viss typ av brottslighet, såsom statsstyrt företagsspionerі (27 kap. 33 § tredje stycket rättegångsbalken). Samma undantag från underrättelseskyldigheten bör gälla vid statsstyrt olovligt röjande av teknisk företagshemlighet. Skälen för att undanta statsstyrt olovligt röjande av teknisk företagshemlighet får nämligen anses vara lika starka som i fråga om statsstyrt företagsspionerі. Som en följd av detta gäller inte heller underrättelseskyldigheten vid hemlig dataavläsning enligt 28 § lagen om hemlig dataavläsning. Därtill följer att Stockholms tingsrätt är alternativt forum vid prövning av tillstånd till användning av hemliga tvångsmedel (27 kap. 34 § rättegångsbalken).

De skäl som motiverar att hemliga tvångsmedel ska kunna användas i förhållande till statsstyrt olovligt röjande av teknisk företagshemlighet gör sig inte gällande i förhållande till olovligt utnyttjande av teknisk företagshemlighet. Detta särskilt som det kan antas att olovligt utnyttjande av teknisk företagshemlighet sällan begås på uppdrag av eller understöds av främmande makt eller av någon som agerar för främmande makts räkning. Något praktiskt behov av hemlig tvångsmedelsanvändning finns därför inte i förhållande till detta brott.

Preventiva tvångsmedel ska få användas vid statsstyrt olovligt röjande av teknisk företagshemlighet

Möjligheten att använda preventiva tvångsmedel när det gäller statsstyrt företagsspionerі har motiverats bl.a. av att det rör sig om allvarlig och svårutredd brottslighet, som därmed är svår att upptäcka och förhindra, och som kan orsaka samhällsskada (propositionen Hemliga tvångsmedel mot allvarliga brott, prop. 2013/14:237 s. 88–89 och 114–115, propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten, prop. 2018/19:86 s. 89 samt prop. 2023/24:117 s. 116–117 och 129–130). De skäl som gör sig gällande i fråga om möjligheten att använda hemliga tvångsmedel vid en förundersökning om statsstyrt olovligt röjande av teknisk företagshemlighet gör sig gällande även för användning av preventiva tvångsmedel (se vidare i avsnittet ovan). Det finns alltså ett påtagligt behov av att kunna använda preventiva tvångsmedel enligt preventivlagen, inhämtningslagen och lagen om hemlig dataavläsning för att förebygga, förhindra och upptäcka statsstyrt olovligt röjande av teknisk företagshemlighet. Sådana åtgärder kan också förväntas vara effektiva.

Genom att lägga till statsstyrt olovligt röjande av teknisk företagshemlighet i brottskatalogerna för de preventiva tvångsmedlen enligt preventivlagen, inhämtningslagen och lagen om hemlig dataavläsning utökas tillämpningsområdet för tvångsmedlen. Fler personer än i dag kan förväntas bli föremål för preventiva tvångsmedel, vilket också innebär en ökad risk för att sådana tvångsmedel används mot personer som visar sig inte vara delaktiga i brott. Därtill kommer risken för att tredje man kan drabbas av tvångsmedelsanvändningen. Förslagen innebär sammantaget en ökad risk för intrång i den personliga integriteten.

När det gäller statsstyrt olovligt röjande av teknisk företagshemlighet är det fråga om allvarlig brottslighet av kvalificerat slag som är särskilt svårutredd och mycket angelägen att förebygga, förhindra och upptäcka, vilket motiverar att preventiva tvångsmedel ska få användas på motsva-

rande sätt som för statsstyrt företagsspioneri. Regleringen om preventiva tvångsmedel omges av ett väl utbyggt system med rättssäkerhetsgarantier som syftar till att begränsa integritetsintrånget för enskilda och att möjliggöra en effektiv tillsyn. Sammantaget bedöms att förslagen innebär en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Av samma skäl som i förhållande till hemliga tvångsmedel (se avsnitt ovan) saknas det skäl för att det ska införas en möjlighet att använda preventiva tvångsmedel vid olovligt utnyttjande av teknisk företagshemlighet.

Biometrisk jämförelse ska få göras mot Migrationsverkets register över fingeravtryck och fotografier vid statsstyrt olovligt röjande av företagshemlighet

Som framgår ovan finns det alltså ett starkt intresse av att brottsbekämpande myndigheter har tillgång till effektiva och verkningsfulla verktyg för att utreda statsstyrt olovligt röjande av teknisk företagshemlighet. Utöver hemliga tvångsmedel kan det finnas andra verktyg som bör få användas i det syftet. Regeringen har nyligen föreslagit att biometriska jämförelser av ansiktsbilder och fingeravtryck av misstänkta gärningsmän ska få göras mot Migrationsverkets register över fingeravtryck och fotografier vid förundersökning om viss allvarlig brottslighet (propositionen Biometri i brottsbekämpningen, prop. 2024/25:37). Metoden innebär att en ansiktsbild eller ett fingeravtryck som kan antas härröra från en misstänkt men okänd gärningsman får jämföras med ansiktsbilder och fingeravtryck i Migrationsverkets register. Eftersom jämförelsen görs mot register som innehåller uppgifter även om personer som inte är misstänkta för brott får metoden endast användas vid allvarlig brottslighet och med särskild restriktivitet. Förutom brott med högt straffvärde är det framför allt samhällsfarliga brott som kan leda till att en jämförelse görs, alltså sådana brott som Säkerhetspolisen ansvarar för att utreda och som direkt eller indirekt hotar vitala samhällsintressen. Utmärkande för dessa brott är dessutom att de typiskt sett är mycket svårutredda (prop. 2024/25:37 s. 136). Ett av de brott som kan föranleda en jämförelse är statsstyrt företagsspioneri.

Som framgår ovan bedöms statsstyrt olovligt röjande av teknisk företagshemlighet vara jämförbart med statsstyrt spioneri i flera avseenden. Liksom ovan konstateras i förhållande till hemliga och preventiva tvångsmedel utgör även statsstyrt olovligt röjande av teknisk företagshemlighet allvarlig och potentiellt samhällsfarlig brottslighet. Det rör sig dessutom typiskt sett om svårutredd brottslighet. Behovet och den förväntade nyttan av att använda biometriska jämförelser mot Migrationsverkets register överväger det integritetsintrång som användandet kan innebära. Automatiserad ansikts- och fingeravtrycksjämförelse i Migrationsverkets register över fingeravtryck och fotografier bör därför kunna användas vid förundersökning om statsstyrt olovligt röjande av teknisk företagshemlighet.

6 Ikraftträdande- och övergångsbestämmelser

Utkastets förslag: Lagändringarna ska träda i kraft den 1 januari 2026.
Utkastets bedömning: Det behövs inte några övergångsbestämmelser.

Förslaget och bedömningen i promemorian överensstämmer med utkastets förutom att förslaget i promemorian innebar ett tidigare datum för ikraftträdande.

Remissinstanserna har inga synpunkter.

Skälen för utkastets förslag och bedömning: En lämplig tidpunkt för ikraftträdande bedöms vara den 1 januari 2026.

Vad gäller förslagen om kriminalisering av olovligt utnyttjande av teknisk företagshemlighet respektive olovligt röjande av teknisk företagshemlighet följer det av 5 § lagen (1964:163) om införande av brottsbalken, som anses generellt tillämplig inom straffrätten, att nya bestämmelser inte får tillämpas på ett sådant sätt att de ges retroaktiv verkan till den tilltalades nackdel.

När det gäller skadestånd följer det av allmänna skadeståndsrättsliga principer att nya bestämmelser om skadestånd endast tillämpas på skadefall som har inträffat efter ikraftträdandet (prop. 2017/18:200 s. 127, prop. 1987/88:155 s. 33 och proposition med förslag till skadeståndslag m.m., prop. 1972:5 s. 593).

Mot denna bakgrund behövs det inte några övergångsbestämmelser.

7 Förslagens konsekvenser

Utkastets bedömning: De föreslagna lagändringarna ger bättre möjligheter att ingripa mot att tekniska företagshemligheter 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 kostnadsökningar för berörda myndigheter inom rättsväsendet samt för Säkerhets- och integritetsskyddsnämnden som förslagen kan medföra bedöms inte vara större än att de kan hanteras inom berörda myndigheters befintliga ekonomiska ramar.

Bedömningen i promemorian överensstämmer med utkastets.

Remissinstanserna har inga synpunkter. Som framgår av avsnitt 4.1 framför emellertid bl.a. *Akademikerförbundet SSR* och *Tjänstemännens centralorganisation (TCO)* synpunkter som även har betydelse för förslagens konsekvenser.

Skälen för bedömningen

Konsekvenser för företagen

I Sverige finns det ca 1,2 miljoner företag. Förslagen har sannolikt störst betydelse för de företag som bedriver innovationsverksamhet, vilket är drygt hälften av dem. Förslagen innebär huvudsakligen att det kriminaliserade området för angrepp på tekniska företagshemligheter utvidgas. Genom de föreslagna ändringarna förbättras möjligheterna att ingripa mot att sådana företagshemligheter sprids och används illojalt.

Det kan antas att de nya straffbestämmelserna bidrar till att olovligt utnyttjande och röjande av tekniska företagshemligheter minskar. Möjligheterna att ingripa mot gärningarna kommer också vara goda genom bl.a. möjligheterna till användning av hemliga och preventiva tvångsmedel. Företag som innehar sådana företagshemligheter som avser information som är ägnad att utgöra led i produktionen eller framställningen av en vara eller utförandet av en tjänst får därmed ett bättre skydd för sina investeringar. Detta torde leda till bättre förutsättningar för investeringar i teknisk utveckling, även om några beloppsmässiga uppskattningar knappast går att göra. Det stärker också innovationskraften och den internationella konkurrensförmågan, liksom marknadens sunda funktion. Det gynnar i sin tur handeln av varor och tjänster. Sammantaget bidrar det till ett gynnsamt ekonomiskt klimat och kan antas bidra till fler arbetstillfällen.

Förslagen har ingen effekt på den administrativa bördan för företagen och förutses inte leda till ökade kostnader för företagen.

Konsekvenser för arbetstagarna och arbetsmarknaden

Förslagen bedöms inte innebära att arbetstagarnas möjligheter att påtala och slå larm om oegentligheter i arbetsgivarens verksamhet försämras.

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 för en arbetstagare som angripit en företagshemlighet efter anställningens slut. De nya straffbestämmelserna aktualiseras således endast i undantagsfall efter en anställnings slut, eftersom omständigheten att anställningen har upphört normalt sett innebär att gärningen ska anses vara ringa och fri från straff. 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 tekniska företagshemligheter. 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 av den föreslagna kriminaliseringen eftersom det då handlar om utnyttjande av kommersiella företagshemligheter.

Kriminaliseringen innebär ett tillkommande 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 skadestånds-

sanktionerade enligt lagen om företagshemligheter. Även om gruppen vanligtvis inte kommer i kontakt med företagshemligheter i någon större utsträckning, omfattas de av kriminaliseringen och därför även av skadeståndsansvar enligt lagen. Även för denna grupp föreslås att ansvar vid angrepp som sker efter att deltagandet i rörelsen eller i verksamheten har upphört begränsas genom att sådana fall vanligtvis bör bedömas som ringa och fria från ansvar.

På det hela taget kan det därför antas att rörligheten på arbetsmarknaden inte påverkas.

Konsekvenser för staten och myndigheterna

Att det straffrättsliga skyddet för 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 och högskolor samt andra forskningsutförare innebär lagändringarna ett starkare skydd mot att öppenhet och samarbete riskerar att utnyttjas av främmande makt för att komma åt information på ett otillbörligt sätt.

Förslagen innebär inte några administrativa kostnader för universitet, högskolor eller andra forskningsutförare.

Det är rimligt att anta att lagändringen kan komma att leda till en ökning av antalet anmälningar, förundersökningar och lagföringar. Även användningen av tvångsmedel kan antas öka i viss mån. Antalet ärenden bedöms emellertid bli få. En sådan ökning som det kan bli fråga om kan antas medföra en endast marginell ökning av arbetsbelastningen för polis, åklagare, de allmänna domstolarna och kriminalvård liksom för Säkerhets- och integritetsskyddsnämnden. Det kan bli fråga om att förordna offentlig försvarare och offentligt ombud i något fler fall.

Sammantaget bedöms genomförandet av den föreslagna kriminaliseringen inte medföra annat än marginellt ökade kostnader för berörda myndigheter. Dessa kostnader ryms inom ramen för befintliga anslag. Eventuella kostnadsökningar för rättsliga biträden bedöms vara marginella.

Övriga konsekvenser

Förslagen påverkar inte jämställdheten mellan kvinnor och män och har inte några andra nämnvärda konsekvenser. Förslagen är förenliga med EU-rätten.

8 Författningskommentar

8.1 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 *på något annat sätt* utnyttjas eller röjs.

I paragrafen regleras skadeståndsansvar för den som har begått brott enligt lagen. Övervägandena finns i avsnitt 4.

Paragrafen ändras på så sätt att den som begår brott enligt de nya straffbestämmelserna i 26 a § är skadeståndsskyldig på samma sätt som gäller vid annan brottslighet enligt lagen.

Skadeståndsansvaret enligt paragrafen omfattar inte endast skada som uppkommer genom brottet utan också skada som uppkommer på grund av efterföljande utnyttjande eller röjande som utförs av en annan person (se prop. 1987/88:155 s. 41, 42 och 58). Genom tillägget av ”på något annat sätt” anpassas paragrafen språkligt till att det kriminaliserade området efter införandet av de nya straffbestämmelserna också omfattar utnyttjande och röjande av en teknisk företagshemlighet.

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. Övervägandena finns i avsnitt 3.1.

Ändringen i *andra stycket* innebär att det är 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 *företagsspionerі* 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 företagsspioneri.

Paragrafen ändras på så sätt att bestämmelsen om grovt brott flyttas från *första stycket* till ett nytt *andra stycke*. Det innebär inte någon ändring i sak.

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 eller röjer en företagshemlighet*

1. som avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst (teknisk företagshemlighet), och

2. som han eller hon har fått del av genom att delta i en näringsidkares rörelse eller en forskningsinstitutions verksamhet till följd av anställning eller uppdrag eller på annan liknande grund, eller i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution,

ska dömas för olovligt utnyttjande av teknisk företagshemlighet eller olovligt röjande av teknisk företagshemlighet 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 ringa fall ska det inte dömas till ansvar. Vid bedömningen av om gärningen är ringa ska det särskilt beaktas om gärningen är mindre allvarlig på grund av att den har begåtts efter att ett sådant deltagande som avses i första stycket 2 har upphört.

Paragrafen, som är ny, reglerar straffansvar för olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet. Övervägandena finns i avsnitt 3.1–3.3.

Första stycket

Enligt första stycket är det straffbart att uppsåtligen och olovligen utnyttja eller röja en teknisk företagshemlighet. Ett grundläggande krav för att straffansvar enligt paragrafen ska komma i fråga är att angreppet på företagshemligheten är obehörigt enligt 4 §.

För straffansvar förutsätts att gärningsmannen har uppsåt som täcker de omständigheter som ligger till grund för ansvar. Det är tillräckligt med likgiltighetsuppsåt.

Att utnyttjandet eller röjande ska ha skett olovligen ska förstås på samma sätt som i 26 §. Det förutsätts att gärningsmannen tagit del av den företagshemliga informationen under sådana förhållanden att det finns krav på att informationen inte utnyttjas eller röjs. Frågan om gärningen varit olovlig tar alltså närmast sikte på i vilken mån gärningsmannen mot innehavarens vilja har brutit igenom den spärr som hemlighållandet är avsett att utgöra (prop. 2017/18:200 s. 121).

Innebörden av uttrycken utnyttjande samt röjande är desamma som annars i lagen. Med utnyttjande avses att angriparen utan innehavarens samtycke 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). Med röjande avses att angriparen utan innehavarens samtycke avslöjar hemligheten för någon annan. Det saknar i princip betydelse om röjandet sker mot ersättning eller inte (prop. 2017/18:200 s. 144).

Vad som avses med företagshemlighet regleras i 2 §. Det krävs t.ex. att innehavaren har vidtagit rimliga åtgärder för att hemlighålla informationen

för att den ska vara skyddad. I annat fall är informationen inte skyddad som en företagshemlighet. Det innebär att innehavaren kan behöva göra klart för mottagaren vad han eller hon får och inte får göra med informationen.

Enligt *punkt 1* är det endast angrepp på en teknisk företagshemlighet, alltså en sådan företagshemlighet som avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst, som omfattas av straffansvaret. Det kan exempelvis röra sig om ritningar, recept, källkoder, datorprogram, forskningsresultat eller forskningsunderlag, tekniska förebilder eller andra modeller samt annan teknisk information om uppfinningar, produkter eller tjänster.

För att det ska vara fråga om en sådan företagshemlighet ska det finnas en faktisk eller potentiell användning av företagshemligheten i produktionen av en vara eller tjänst som produceras eller utvecklas i företaget eller vid forskningsinstitutionen. Det kan också vara fråga om att den kan användas vid framtida produktion. Det är tillräckligt att informationen används eller kan användas i något led av produktionen eller framställningen av en vara eller utförandet av en tjänst. Det är den möjliga tillämpningen av företagshemligheten i produktionen som utgör avgränsningen mot sådana företagshemligheter som inte omfattas av det straffbara området. Företagshemligheten kan, men behöver inte, innefattas i den framställda produkten eller den utförda tjänsten. Även framställningsprocesser, maskinella anordningar eller andra hjälpmedel omfattas av paragrafen. 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 §. Det förutsätts inte att företagshemligheten är dokumenterad i någon form, även om detta vanligtvis är fallet.

Informationen behöver inte vara särskilt avancerad eller värdefull för att omfattas av bestämmelsen med undantag för att ett röjande av informationen ska vara ägnat att innebära skada i konkurrenshänseende för innehavaren (2 § första stycket 4). Det som är avgörande är i stället om informationen är ägnad att användas i hela eller delar av produktionen eller framställningen av en vara eller utförandet av en tjänst. Så kan också vara fallet i försteg i utvecklingen av dessa. Huruvida någon vara framställs eller tjänst utförs i det enskilda fallet saknar betydelse för frågan om straffansvar.

En företagshemlighet som avser information som endast ger upplysningar om innehavarens affärsmässiga förhållanden, som exempelvis priskalkyler, marknadsundersökningar och kundlistor, är inte sådan företagshemlig information som omfattas av bestämmelsen. 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 den. Detsamma gäller information som uteslutande avser lagring eller transporter och annan information om distributionen av en vara.

Affärsplaner eller samarbetsavtal är normalt inte heller företagshemligheter som avser sådan information som gör att de omfattas av bestämmelserna. 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 för att i framtiden kommersialisera en vara eller en tjänst. På motsvarande sätt omfattas typiskt sett inte heller en företagshemlighet som avser information om en planerad prissänkning eller lansering.

Information av rent administrativ karaktär, t.ex. löneuppgifter, verksamhetsrutiner och mötesprotokoll, är normalt inte av sådan beskaffenhet att de omfattas.

Frågan om en företagshemlighet avser information som är ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst får bedömas utifrån omständigheterna i det enskilda fallet. Att informationen ska vara ägnad att användas i produktionen eller framställningen av en vara eller utförandet av en tjänst innebär att informationen typiskt sett ska vara avsedd att tillämpas eller potentiellt tillämpas i produktionen eller framställningen. Exempelvis kan information om kunders preferens utgöra en teknisk företagshemlighet som omfattas av bestämmelsen i ett företag som sätter samman och förädlar sådan information i en tjänst om t.ex. reklamannonser på sociala medier, medan motsvarande information om kunders preferens i ett klädföretag typiskt sett får anses vara information som syftar till att kommersialisera varorna och som inte rör produktionen av kläderna. I det enskilda fallet får bedömas om informationen faktiskt är tillämpbar eller potentiellt tillämpbar i produktionen eller framställningen av en vara eller utförandet av en tjänst.

Den personkrets som enligt *punkt 2* kan träffas av straffansvaret kan delas upp i två huvudsakliga grupper. Gemensamt för dessa är att de har fått del av företagshemligheten. Till skillnad från när någon utan innehavarens samtycke anskaffar sig företagshemligheten, innebär det att den som kan träffas av straffansvaret i och för sig har lovlig tillgång till företagshemligheten.

I punkten 2 regleras även i vilka sammanhang en gärningsman kan ha fått del av en företagshemlighet för att straffansvar ska aktualiseras. Gemensamt för dessa är att det är en näringsidkare eller en forskningsinstitution som är innehavaren. Dessa två uttryck ska förstås på samma sätt som i lagen i övrigt (se bl.a. 2 §).

Med näringsidkare avses varje fysisk eller juridisk person som yrkesmässigt bedriver verksamhet av ekonomisk art. 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).

Med forskningsinstitution avses varje icke-kommersiell verksamhet i vilken det bedrivs forskning. Det kan röra sig om allt från statliga universitet och högskolor till små och stora forskningsutförare. Forskningsinstitutioner som hanterar den slags information som lagen skyddar är dock ofta näringsidkare i lagens mening (prop. 2017/18:200 s. 137 och 138.). 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.

Detta eftersom offentlig information inte kan skyddas som en företagshemlighet.

I fråga om anställda och andra uppdragstagare ska gärningsmannen 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. Det innebär att den arbetspresterande parten ska ha fått del av företagshemligheten på grund av sitt deltagande i rörelsen eller verksamheten. Det är inte en förutsättning för straffansvar 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. Det är således tillräckligt för att gärningsmannen ska anses ha fått del av företagshemligheten att informationen finns tillgänglig på den del av arbetsplatsen där han eller hon normalt har rätt att uppehålla sig (prop. 1987/88:155 s. 19 och 38). En företagshemlighet kan exempelvis finnas dokumenterad i handlingar som en anställd av en händelse ser på arbetsplatsen eller som kommer på tal i en diskussion mellan kollegor som någon råkar överhöra.

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 sannolikt inte är uppfyllt är 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 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. En omständighet som talar för att kravet på deltagande är uppfyllt är att den som utför arbetet är underkastad näringsidkarens arbetsledning och kontroll. Ytterligare omständigheter som talar för att kravet 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 under förutsättning att de där sysselsätts på ett liknande sätt som 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. Likaså talar omständigheten att ersättning utgår för arbetet för att kravet är uppfyllt.

Exempel på personer som många gånger inte kan sägas delta i rörelsen eller verksamheten är hantverkare som anlitas tillfälligt för att utföra installationer eller reparationer samt självständiga formgivare eller arkitekter som konsulteras för ett enskilt bestämt projekt. Andra exempel är datakonsulter, organisationskonsulter och juridiska ombud som anlitas för enstaka kortvariga uppdrag som saknar samband med kärnverksamheten. Inte heller studenter som deltar i forskningsverksamhet mer kortvarigt under sina studier omfattas typiskt sett av straffansvaret.

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 rörelsen eller verksamheten under omständigheter som liknar dem som förekommer i ett anställningsförhållande. Inte heller kan de anses ha fått del av uppdragsgivarens företagshemligheter i samband med en affärsförbindelse med innehavaren (prop. 2017/18:200 s. 153). Deras angrepp på huvudmannens företagshemligheter omfattas därmed inte av straffansvar enligt paragrafen. För dessa grupper kan däremot andra sanktioner aktualiseras, t.ex. enligt 30 kap. 1 § aktiebolagslagen (2005:551).

Den personkrets som kan träffas av straffansvar enligt punkt 2 omfattar även personer som har fått del av en företagshemlighet i samband med en affärsförbindelse med en näringsidkare eller en forskningsinstitution. Uttrycket affärsförbindelse finns även i 6 § och har samma innebörd här. Det måste inte finnas något bindande avtal mellan parterna för att det ska vara fråga om en affärsförbindelse. Redan under ett förhandlingsskede kan mottagaren ha fått del av företagshemligheten på sådant sätt att det finns ett förtroendeförhållande parterna emellan (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).

Brottsrubriceringen är olovligt utnyttjande av teknisk företagshemlighet respektive olovligt röjande av teknisk företagshemlighet.

Straffet är böter eller fängelse i högst två år.

Av principen om att grundlag har företräde framför vanlig lag följer att paragrafen inte ska tillämpas om den kommer i konflikt med reglerna om meddelarfrihet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Andra stycket

I andra stycket framgår straffskalan för grovt brott. Straffskalan i sådant fall är fängelse i lägst sex månader och högst sex år.

Om brottet är grovt får bedömas med hänsyn till samtliga omständigheter i det enskilda fallet. 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.

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.

En annan omständighet som kan tala för att det är ett grovt brott är om företagshemligheten representerar ett betydande värde.

Vid bedömningen av om gärningen inneburit synnerligen kännbar skada ska beaktas inte endast vilket värde företagshemligheten kan sägas representera, utan också hur kännbar skadan är för innehavaren av företagshemligheten. Röjandet av en företagshemlighet kan t.ex. innebära synnerligen kännbar skada om den är en mycket viktig tillgång för företaget. Ett exempel är att ett företag 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 företagshemligheten.

Tredje stycket

I tredje stycket görs undantag från det straffbara området för gärningar som är ringa.

Om gärningen är ringa får bedömas med hänsyn till samtliga omständigheter i det enskilda fallet. Vid bedömningen av om en gärning är ringa ska det särskilt beaktas om gärningen är mindre allvarlig på grund av att den har begåtts efter att deltagandet i rörelsen eller verksamheten har upphört.

Efter att deltagandet i en rörelse eller verksamhet har upphört är en arbetstagare, som utgångpunkt, fri att utnyttja sådan kunskap och erfarenhet, innefattande företagshemligheter, som denne tillgodogjort sig hos en arbetsgivare (prop. 1987/88:155 s. 46 och prop. 2017/18:200 s. 62 och 63.). Utnyttjanden och röjanden som sker efter att deltagandet i rörelsen eller verksamheten upphört är därför normalt sett att bedöma som mindre allvarliga och därmed ringa. För att straffansvar ska komma i fråga i en sådan situation bör normalt sett krävas att gärningsmannens agerande framstår som särskilt illojalt.

Ett deltagande i en rörelse eller verksamhet 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.

Ett särskilt illojalt agerande kan föreligga om gärningsmannen på ett stötande sätt har missbrukat det förtroende som följer av anställningsförhållandet eller den grund för deltagandet som annars är aktuell. Bedömningen av om agerandet framstår som särskilt illojalt knyter an till det som gäller avseende krav på synnerliga skäl för arbetstagares skadestånds-

ansvar i motsvarande situation enligt 7 § andra stycket. Typiskt sett är gärningen inte ringa när det är ett sådant fall att skadeståndsansvar aktualiseras med tillämpning av den bestämmelsen.

Omständigheter som talar för att ett agerande är särskilt illojalt är exempelvis att en person har tagit anställning eller åtagit sig ett uppdrag 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. Om röjandet eller utnyttjandet utförs av någon som har haft en särskild förtroendeställning, t.ex. som verkställande direktör, produktionschef eller forskningschef, kan det tala för att agerandet är särskilt illojalt. Även förekomsten av så kallade sekretess- och konkurrensklausuler kan beaktas. Det förhållandet att företagshemligheten har missbrukats med hjälp av dokumentation i någon form, exempelvis en teknisk förebild, är något som ofta talar för att agerandet är särskilt illojalt. 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, kan agerandet anses särskilt illojalt.

I bedömningen av om agerandet varit särskilt illojalt kan även beaktas vem företagshemligheten ges till. Om mottagaren är den främst konkurrenten i branschen talar det för att agerandet är att betrakta som särskilt illojalt.

Normalt sett kan ett agerande inte bedömas som särskilt illojalt 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.

En gärning är vidare att bedöma som ringa om gärningen vid en samlad bedömning är att anse som bagatellartad. Omständigheter som kan beaktas är således gärningens farlighet, vilket ekonomiskt värde den utnyttjade eller röjda företagshemligheten representerat samt en eventuell skadas omfattning. Om en företagshemlighet röjs till en person som inte kan tänkas utnyttja den kommersiellt och inte heller i sin tur för 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 vilken utsträckning det har uppkommit någon skada. Informationens art och dess värde för verksamheten eller rörelsen kan vara sådan 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.

Det ska inte dömas till ansvar enligt denna paragraf om gärningen är belagd med strängare straff i brottsbalken (se 27 a §).

Enligt 28 § första stycket gäller vidare att den som har brutit mot en tystnadsplikt som följer av lagen inte får dömas för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken på grund av den överträdelsen. Den som har brutit mot ett vitesförbud enligt lagen får inte dömas till straff för en gärning som omfattas av förbudet (se 28 § andra stycket).

26 b § *För försök eller förberedelse till företagsspionerі, olovligt utnyttjande av teknisk företagshemlighet eller olovligt röjande av teknisk 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 teknisk företagshemlighet och olovligt röjande teknisk företagshemlighet. Övervägandena finns i avsnitt 3.3.

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 olovligt utnyttjande eller olovligt röjande av teknisk företagshemlighet 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 teknisk företagshemlighet med vetskap om att den som tillhandahåller hemligheten eller någon före honom eller henne i sin tur har röjt denna genom en gärning som avses i 26 a § första eller andra stycket.*

Paragrafen innehåller bestämmelser om straff för olovlig befattning med företagshemlighet. Övervägandena finns i avsnitt 3.4.

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

Innebörden av att någon anskaffar en företagshemlighet är densamma oavsett om förbrottet är ett företagsspionerі eller ett olovligt röjande av teknisk företagshemlighet (prop. 2017/18:200 s. 178). Även kravet i subjektivt hänseende är detsamma oavsett om förbrottet är företagsspionerі eller olovligt röjande av teknisk företagshemlighet. Kravet på vetskap innebär att straffansvar förutsätter insiktsuppsåt till omständligheten att hemligheten tillhandahålls, eller tidigare har tillhandahållits, genom ett sådant röjande som avses i bestämmelsen om olovligt röjande av teknisk företagshemlighet.

På samma sätt som då företagsspionerі utgör förbrott krävs det inte att förbrottet bedöms som olovligt röjande av teknisk företagshemlighet.

Förbrottet kan vara ett annat brott enligt brottsbalken så länge själva gärningen är sådan som avses i bestämmelsen om olovligt röjande av teknisk företagshemlighet (prop. 2017/18:200 s. 178 om motsvarande fråga när företagsspionerі är förbrott).

Exempelvis kan straffansvar för olovlig befattning med företagshemlighet aktualiseras när en person mottar företagshemligheten från någon som, genom att dela med sig av informationen, gör sig skyldig till en gärning som är att anse som olovligt röjande av teknisk 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 teknisk 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 en gärning som utgör ett straffbart olovligt röjande.

Ansvar förutsätter att det tidigare röjandet inte är fritt från ansvar. Om röjandet är att anse som en ringa gärning finns det inte något förbrott och straffansvar för olovlig befattning med företagshemlighet kommer inte i fråga.

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.

Det ska inte dömas till ansvar enligt lagen om gärningen är belagd med strängare straff i brottsbalken. Paragrafen motsvarar i förhållande till företagsspionerі hittillsvarande 26 § tredje stycket och i förhållande till olovlig befattning med företagshemlighet hittillsvarande 27 § andra stycket. Även i förhållande till de nya brotten olovligt utnyttjande av teknisk företagshemlighet och olovligt röjande av teknisk företagshemlighet samt försök och förberedelse till brotten gäller att det inte ska dömas till ansvar enligt lagen om gärningen är belagd med strängare straff i brottsbalken.

8.2 Förslaget till lag om ändring i rättegångsbalken

27 kap. Om beslag och hemliga tvångsmedel

Hemliga tvångsmedel

18 a § Hemlig avlyssning av elektronisk kommunikation får användas om någon är skäligen misstänkt för brott som avses i andra stycket och åtgärden är av synnerlig vikt för utredningen.

Hemlig avlyssning av elektronisk kommunikation enligt denna paragraf får användas vid en förundersökning om

1. ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. grovt dataintrång enligt 4 kap. 9 c § andra stycket brottsbalken,
3. grovt sexuellt övergrepp, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, grovt sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, grovt utnyttjande av barn för sexuell posering, utnyttjande av barn genom köp av

sexuell handling, sexuellt ofredande mot barn eller grovt sexuellt ofredande mot barn enligt 6 kap. 2 § tredje stycket, 5 §, 6 §, 8 §, 9 § eller 10 § första eller tredje stycket brottsbalken,

4. kontakt för att träffa ett barn i sexuellt syfte enligt 6 kap. 10 a § brottsbalken, om det kan antas att brottet inte leder till endast böter,

5. grovt bedrägeri enligt 9 kap. 3 § brottsbalken, om gärningen har begåtts med hjälp av elektronisk kommunikation,

6. utpressning enligt 9 kap. 4 § första stycket brottsbalken, om det kan antas att brottets straffvärde överstiger fängelse i tre månader,

7. sabotage enligt 13 kap. 4 § brottsbalken,

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

9. mened enligt 15 kap. 1 § första stycket brottsbalken, om det kan antas att brottets straffvärde överstiger fängelse i tre månader,

10. grovt barnpornografibrott eller barnpornografibrott som inte är ringa enligt 16 kap. 10 a § brottsbalken,

11. övergrepp i rättssak eller skyddande av brottsling enligt 17 kap. 10 § första eller fjärde stycket eller 11 § första eller andra stycket brottsbalken, om det kan antas att brottets straffvärde överstiger fängelse i tre månader,

12. grovt skyddande av brottsling enligt 17 kap. 11 § tredje stycket brottsbalken,

13. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,

14. spionerі, utlandsspionerі, 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. 5, 6 a, 7, 8, 10, 10 a eller 10 b § brottsbalken,

15. grovt penningtvättsbrott eller näringspenningtvätt, grovt brott, enligt 5 § eller 7 § andra stycket lagen (2014:307) om straff för penningtvättsbrott,

16. grovt insiderbrott enligt 2 kap. 1 § tredje stycket lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden,

17. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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,

18. deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),

19. försök, förberedelse eller stämpling till ett brott som avses i 1–5, 7, 8, 10 eller 12–18, om en sådan gärning är belagd med straff,

20. försök, förberedelse eller stämpling till ett brott som avses i 6, 9 eller 11, om en sådan gärning är belagd med straff och det kan antas att gärningens straffvärde överstiger fängelse i tre månader,

21. ett annat brott, om det kan antas att brottets straffvärde överstiger fängelse i två år, eller

22. flera brott, om

a) en och samma person är skäligen misstänkt för samtliga brott,

b) det kan antas att den samlade brottslighetens straffvärde överstiger fängelse i två år,

c) det kan antas att vart och ett av brotten har utgjort ett led i en brottslighet som har utövats i organiserad form eller systematiskt, och

d) det för vart och ett av brotten är föreskrivet fängelse i ett år eller mer.

Hemlig avlyssning av elektronisk kommunikation enligt denna paragraf får endast avse ett telefonnummer eller en annan adress eller en viss elektronisk kommunikationsutrustning som

1. under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte, eller

2. det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Paragrafen innehåller bestämmelser om användning av hemlig avlyssning av elektronisk kommunikation när någon är skäligen misstänkt för brott. Övervägandena finns i avsnitt 5.

Paragrafen ändras på så sätt att brottet olovligt röjande av teknisk företagshemlighet enligt 26 a § lagen om företagshemligheter läggs till i *andra stycket sjuttonde punkten*. En förutsättning för att hemlig avlyssning av elektronisk kommunikation ska få användas när misstanken gäller olovligt röjande av teknisk företagshemlighet är 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. Det överensstämmer med vad som enligt hittillsvarande ordning redan gäller vid förundersökning om företagsspionieri.

Ändringen innebär också – på grund av hänvisningar i 27 kap. 19 a § andra stycket, 19 b § andra stycket, 19 c § första stycket, 20 b § första stycket och 20 c § andra stycket till förevarande bestämmelser – att tvångsmedlen hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning får användas vid en förundersökning om olovligt röjande av teknisk företagshemlighet samt för att lokalisera någon som är anhållen eller häktad för sådant brott. Ändringen innebär också att hemlig övervakning av elektronisk kommunikation med stöd av lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder får användas för att lokalisera en person som är dömd till fängelse, rättspsykiatrisk vård eller sluten ungdomsvård, 3 § den lagen Vidare innebär ändringen, genom hänvisning i 27 kap. 18 b § rättegångsbalken, att hemliga avlyssning av elektronisk kommunikation får användas för att utreda vem som skäligen kan misstänkas för olovligt röjande av teknisk företagshemlighet. Ändringen innebär även att hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning kan aktualiseras, 4 § den lagen.

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

2. spionerі, utlandsspionerі eller grovt utlandsspionerі enligt 19 kap. 5, 6 a eller 6 b § brottsbalken,

3. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet enligt* 26 *eller 26 a* § 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. försök, förberedelse eller stämpling till ett brott som avses i 1–3, om en sådan gärning är belagd med straff,

5. ett annat brott, om det kan antas att brottets straffvärde överstiger fängelse i fyra år, eller

6. flera brott, om

a) en och samma person är skäligen misstänkt för samtliga brott,

b) det kan antas att den samlade brottslighetens straffvärde överstiger fängelse i fyra år,

c) det kan antas att vart och ett av brotten har utgjort ett led i en brottslighet som har utövats i organiserad form eller systematiskt, och

d) det för vart och ett av brotten inte är föreskrivet lindrigare straff än fängelse i sex månader eller det är fråga om försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff.

Paragrafen innehåller en definition av tvångsmedlet hemlig rumsavlyssning och anger när tvångsmedlet får användas under en förundersökning. Övervägandena finns i avsnitt 5.

Paragrafen ändras på så sätt att brottet olovligt röjande av teknisk företagshemlighet enligt 26 a § lagen om företagshemligheter läggs till i *andra stycket tredje punkten*. En förutsättning för att användning av tvångsmedlet ska kunna komma i fråga är att det kan antas 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 att det kan antas att brottet inte leder till endast böter. Det överensstämmer med det som gällt enligt hittillsvarande ordning redan vid förundersökning om företagsspioneri.

Ändringen innebär även att hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning kan aktualiseras, 6 § den lagen.

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 eller risk för men för utredningen inte har kunnat lämnas någon underrättelse inom ett år och sex månader från det att tvångsmedelsanvändningen avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller och om det kan ske utan men för utredningen.

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, 6 a, 6 b, 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. *företagsspioneri eller olovligt röjande av teknisk företagshemlighet enligt* 26 *eller 26 a* § 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 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666), 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.

En underrättelse enligt 31 § ska inte heller lämnas om den person som underrättelsen avser har avlidit eller om den juridiska person som underrättelsen avser har upphört.

Paragrafen anger de situationer då en underrättelse till enskild enligt 31 § ska skjutas upp på grund av sekretess eller risk för men för utredningen. Den innehåller även bestämmelser om i vilka fall en underrättelse inte ska lämnas alls. Överväganden finns i avsnitt 5.

Tredje stycket femte punkten ändras på så sätt att en underrättelse enligt 27 kap. 31 § inte ska lämnas om förundersökningen angår brottet olovligt röjande av teknisk företagshemlighet enligt 26 a § 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. Det överensstämmer med det som enligt hittillsvarande ordning redan gäller när förundersökningen angår företagsspionerі.

Vidare ändras punkten på så sätt att hänvisningen till ”brott enligt 26 §” tas bort och ersätts med ”företagsspionerі”. Ändringen görs för att språkligt anpassa punkten till det tillkommande brottet olovligt röjande av teknisk företagshemlighet. Det innebär inte någon ändring i sak.

Behörig domstol för prövning av vissa frågor om hemliga tvångsmedel

34 § Frågor om tillstånd till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller kvarhållande av försändelse enligt 9 § eller 9 a § andra tycket får vid en förundersökning om följande brott, utöver av domstol som föreskrivs i 19 kap., prövas av Stockholms tingsrätt:

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,
2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, grov 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, utlandsspionerі, grovt utlandsspionerі, 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, 6 a, 6 b, 7, 8, 10, 10 a eller 10 b § brottsbalken,
5. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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. terroristbrott, deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666), eller
7. försök, förberedelse eller stämpling till ett brott som avses i 1–6, om en sådan gärning är belagd med straff.

Paragrafen innehåller en alternativ forumregel för prövning av vissa frågor om hemliga tvångsmedel. Överväganden finns i avsnitt 5.

Paragrafen ändras på så sätt att brottet olovligt röjande av teknisk företagshemlighet enligt 26 a § lagen om företagshemligheter läggs till i *första stycket femte punkten*. En förutsättning för forumregelns tillämplighet är 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. Det överensstämmer med det som enligt hittillsvarande ordning redan gäller vid förundersökning om företagsspioneri.

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

1 § Ett tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § rättegångsbalken, hemlig kameraövervakning enligt 27 kap. 20 a § rättegångsbalken, husrannsakan enligt 28 kap. 1 § rättegångsbalken, undersökning på annat ställe enligt 28 kap. 10 § rättegångsbalken, genomsökning på distans enligt 28 kap. 10 a § rättegångsbalken eller postkontroll enligt 2 § får beviljas 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, grov 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, utlandsspionerі, grovt utlandsspionerі, 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, 6 a, 6 b eller 8 § eller 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,

5. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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, deltagande i en terroristorganisation, grovt brott, samröre med en terroristorganisation, grovt brott, finansiering av terrorism eller särskilt allvarlig brottslighet, grovt brott, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, grovt brott, rekrytering till terrorism eller särskilt allvarlig brottslighet, grovt brott, eller utbildning för terrorism eller särskilt allvarlig brottslighet, grovt brott, enligt 4 §, 4 a § tredje stycket, 5 § tredje stycket, 6 § tredje stycket, 7 § tredje stycket, 8 § tredje stycket eller 9 § tredje stycket terroristbrottslagen (2022:666), eller

7. mord, grov misshandel, synnerligen grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1 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.

Ett tillstånd enligt första stycket får också beviljas 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 reglerar förutsättningarna för att ett tillstånd till vissa tvångsmedel enligt lagen får beviljas. Övervägandena finns i avsnitt 5.

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 teknisk företagshemlighet enligt 26 a § 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 det som enligt hittillsvarande ordning redan gäller vid påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar företagsspionerі.

Ändringen innebär även att hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning kan aktualiseras, 7 § första stycket den lagen.

1 b § Ett tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § första stycket rättegångsbalken får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar

1. grov mordbrand eller grov allmänfarlig ödeläggelse enligt 13 kap. 2 § eller 3 § tredje stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
2. uppror eller väpnat hot mot laglig ordning enligt 18 kap. 1 eller 3 § brottsbalken,
3. högförräderi, spionerі, grovt spionerі, utlandsspionerі eller grovt utlandsspionerі enligt 19 kap. 1, 5, 6, 6 a eller 6 b § brottsbalken,
4. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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 och det kan antas att brottet inte leder till endast böter,
5. terroristbrott enligt 4 § terroristbrottslagen (2022:666), eller
6. mord, synnerligen grov misshandel eller människokorov enligt 3 kap. 1 § eller 6 § andra stycket eller 4 kap. 1 § 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.

Ett tillstånd enligt första stycket får också beviljas 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, som är ny, reglerar förutsättningarna för hemlig rumsavlyssning, i andra fall än de som anges i 1 c §. Övervägandena finns i avsnitt 5.

Första stycket fjärde 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 teknisk företagshemlighet enligt 26 a § 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 det som enligt hittillsvarande ordning redan gäller vid påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar företagsspionerі.

Ändringen innebär även att hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning kan aktualiseras, 7 § andra stycket den lagen.

8.4 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, utlandsspionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5, 6 a eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,
6. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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. samröre med en terroristorganisation, grovt brott, finansiering av terrorism eller särskilt allvarlig brottslighet, grovt brott, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, grovt brott, rekrytering till terrorism eller särskilt allvarlig brottslighet, grovt brott, eller utbildning för terrorism eller särskilt allvarlig brottslighet, grovt brott, enligt 5 § tredje stycket, 6 § tredje stycket, 7 § tredje stycket, 8 § tredje stycket eller 9 § tredje stycket terroristbrottslagen (2022:666),
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.

I paragrafen anges vilka brott som ska innefattas av en brottslig verksamhet för att den ska aktualisera en tillämpning av lagen. Övervägandena finns i avsnitt 5.

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 teknisk företagshemlighet enligt 26 a § 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 det som enligt hittillsvarande ordning redan gäller för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar företagsspionerі.

Ändringen innebär även att hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning kan aktualiseras, 10 § den lagen.

8.5 Förslaget till lag om ändring i lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område

6 a kap. Behandling av uppgifter i vissa register som inte förs med stöd av denna lag

2 § En jämförelse får göras vid en förundersökning om

1. ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. sabotage enligt 13 kap. 4 § brottsbalken,
3. mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1 §, 3 § första eller andra stycket, 5 a § eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
4. olovlig kårverksamhet eller brott mot medborgerlig frihet enligt 18 kap. 4 eller 5 § brottsbalken,
5. spionerі, utlandsspionerі, 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. 5, 6 a, 7, 8, 10, 10 a eller 10 b § brottsbalken,
6. företagsspionerі *eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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. deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),
8. försök, förberedelse eller stämpling till ett brott som avses 1–7, om en sådan gärning är belagd med straff, eller
9. ett annat brott om det kan antas att brottets straffvärde överstiger fängelse i två år.

Paragrafen anger tillsammans med 3 § vilka brott som kan aktualisera en jämförelse enligt 1 §. Övervägandena finns i avsnitt 5.

Sjätte punkten ändras på så sätt att en automatiserad ansikts- och fingeravtrycksjämförelse ska få göras även vid förundersökning av olovligt röjande av teknisk 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 i prop. 2024/25:37 föreslås gälla vid förundersökning avseende statsstyrt företagsspionerі.

8.6 Förslaget till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

14 § 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 13 §, ska en underrättelse enligt 12 § skjutas upp till dess att sekretess inte längre gäller.

Om det på grund av sekretess eller på grund av att ärendet inte avslutats, inte har kunnat lämnas någon underrättelse enligt 12 § inom ett år och sex månader från det att tvångsmedelsanvändningen avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller.

En underrättelse enligt 12 § ska inte lämnas, om uppgifterna med stöd av 10 § har tagits in i en förundersökning som angår

1. brott som avses i 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brotten 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, 6 a, 6 b, 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. *företagsspionerі eller olovligt röjande av teknisk företagshemlighet* enligt 26 *eller 26 a* § 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 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666), 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.

En underrättelse enligt 12 § ska inte heller lämnas om den person som underrättelsen avser har avlidit eller om den juridiska person som underrättelsen avser har upphört.

Paragrafen anger de situationer då en underrättelse till enskild enligt 12 § kan skjutas upp på grund av sekretess. Den innehåller även bestämmelser om när en underrättelse enligt 12 § i vissa fall inte ska lämnas alls. Övervägandena finns i avsnitt 5.

Tredje stycket femte punkten ändras på så sätt att en underrättelse enligt 12 § inte ska lämnas förundersökningen angår brottet olovligt röjande av teknisk företagshemlighet enligt 26 a § 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. Det överensstämmer med det som enligt hittillsvarande ordning redan gäller när förundersökningen angår statsstyrt företagsspionerі.

Vidare ändras punkten på så sätt att hänvisningen till ”brott enligt 26 §” tas bort och ersätts med ”företagsspionerі”. Ändringen görs för att språkligt anpassa punkten till det tillkommande brottet olovligt röjande av företagshemlighet. Det innebär inte någon ändring i sak.

Sammanfattning av promemorian Bättre skydd för tekniska företagshemligheter (Ds 2020:26)

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 företagsspionerі. 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.

Promemorians lagförslag

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 *företagsspionerі* 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 *företagsspionerі* till böter eller fängelse i högst två år.
För försök eller förberedelse till företagsspionerі ska det dömas till ansvar enligt 23 kap. brottsbalken.	*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.*
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 företagsspioneri, 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 befattning med företagshemlighet* till böter eller fängelse i högst två år eller, om brottet är grovt, till fängelse i högst fyra år.	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.*
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.

Bilaga 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, 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 enligt 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,	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.	

[1] Senaste lydelse 2018:559.

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 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,

3. *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 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,

[2] Senaste lydelse 2020:174.

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.

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 eller av någon som kommer att agera för en främmande makts räkning,	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, 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

[1] Senaste lydelse 2018:560.

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.

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. 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 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. 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.	

[1] Senaste lydelse 2019:499.

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.

Förteckning över remissinstanserna (DS 2020:26)

Remissyttranden över betänkandet Bättre skydd för tekniska företagshemligheter (Ds 2020:26) har lämnats av Almi Företagspartner AB, Arbetsdomstolen, Arbetsgivarverket, Bolagsverket, Chalmers tekniska högskola, Datainspektionen, Domstolsverket, Ekobrottsmyndigheten, Exportkreditnämnden (EKN), Finansinspektionen, Företagarna, Försvarets materielverk, Försvarets radioanstalt, Helsingborgs tingsrätt, Justitiekanslern, Konkurrensverket, Kommerskollegium, Kungliga tekniska högskolan, Landsorganisationen i Sverige (LO), Lunds universitet (Juridiska fakulteten), Mälardalens högskola, Patent- och registreringsverket (PRV), Riksdagens ombudsmän (JO), Skatteverket, Stockholms tingsrätt (Patent- och marknadsdomstolen), Stockholms universitet (Juridiska fakulteten samt Institutionen för mediestudier), Svea hovrätt, Svenska Föreningen för Immaterialrätt (SFIR), Svenska Industrins IP Förening (SIPF), Svenska Uppfinnareföreningen, Svenskt Näringsliv, Sveriges advokatsamfund, Sveriges akademikers centralorganisation (Saco), Sveriges Ingenjörer, Sveriges Kommuner och Regioner (SKR), Sveriges Patentbyråers Förening (SEPAF), Sveriges universitets- och högskoleförbund (SUHF), Säkerhets- och försvarsföretagen (SOFF), Säkerhets- och integritetsskyddsnämnden (SIN), Säkerhetspolisen, Teknikföretagen, Tillväxtverket, Tjänstemännens Centralorganisation (TCO), Totalförsvarets forskningsinstitut, TU- Medier i Sverige, Umeå tingsrätt, Verket för innovationssystem (VINNOVA) och Åklagarmyndigheten.

Akavia; Företagarförbundet Fria Företagare, IT&Telekomföretagen Almega, Kommunala Företagens Samorganisation (KFS), Livsmedelsföretagen, Läkemedelsindustriföreningen (LIF), Medieföretagen Almega, Näringslivets Regelnämnd (NNR), Polismyndigheten, Publicistklubben, RISE - Research Institutes of Sweden, Stockholms Handelskammare, Svenska Bankföreningen, Svenska Journalistförbundet, Svenska Patentombudsföreningen (SPOF), Svensk Exportkredit (SEK), Sveriges Export- och investeringsråd (Business Sweden), Swedfund, Swedish Incubators & Science Parks (SISP), Utgivarna, Myndigheten för samhällsskydd och beredskap och Regelrådet har fått tillfälle att yttra sig men har avstått från att göra det.