JURIDISKA FAKULTETEN
Vid Lunds Universitet

Isak Magnusson

Dataavläsning i ett utredningssammanhang

En komparativ studie mellan Sverige och Danmarks lagstiftning om tvångsingreppet dataavläsning.

LAGF03 Rättsvetenskaplig uppsats
Kandidatuppsats på juristprogrammet
15 högskolepoäng

Handledare: Richard Croneberg
Termin: VT2022

Innehåll

Summary

Secret data scanning is a criminal procedural coercive measure that was introduced in Sweden on 1 April 2020. The coercive measure has existed in Denmark since 2002, where it has since undergone changes on several occasions. The Swedish law is limited in time to five years and is thereafter to be evaluated. The purpose of this essay is to compare the regulation of secret data scanning in Sweden and Denmark in relation to personal integrity and to discuss possible improvements in this area. The subject has been limited to the data scanning that may occur during an investigation.

The material used is public print, rulings from the European Court of Justice, legal literature, and also some contributions from the media. In the purposes of this essay the comparative method has been applied, specifically the functionality method.

The thesis concludes that both countries meet the requirements of the European Convention, but that for the Swedish data scanning there are detailed regulations that would be useful for the Danish one as well. In addition, it is noted that Sweden to some extent is lacking in the application of these regulations.

Sammanfattning

Hemlig dataavläsning är ett straffprocessuellt tvångsmedel som infördes i Sverige 1 april 2020. Tvångsmedlet har förekommit i Danmark sedan 2002 där det sedan dess genomgått ändringar vid flera tillfällen. Den svenska lagen är tidsbegränsad till 5 år och kommer därefter utvärderas. Syftet med denna uppsats är att jämföra regleringen av hemlig dataavläsning i Sverige och Danmark i relation till personlig integritet och att diskutera möjliga förbättringar inom detta område. Ämnet har begränsats till den dataavläsning som kan förekomma under en utredning.

Materialet som använts är offentligt tryck, avgöranden från Europadomstolen, juridisk litteratur, och även en del bidrag från media. Komparativ metod har tillämpats, specifikt funktionalitetsmetoden.

Uppsatsens slutsats är att båda länder uppfyller Europakonventionens krav, men att det för den svenska dataavläsningen förekommer detaljregleringar som vore användbara även för den danska. Dessutom konstateras att sverige till viss del brister i tillämpningen av dessa regleringar.

1. Bakgrund

Den svenska lagen om hemlig dataavläsning infördes i Sverige 2020, den danska regleringen i Retsplejeloven § 791 b infördes för sin del 2002. Den tidsbegränsade och relativt nyinförda Svenska lagen om hemlig dataavläsning har gjort området ytterst aktuellt. Då lagstiftningen är djupt kopplad till den tekniska utvecklingen lär det bara vara en tidsfråga innan även den danska lagstiftningen på området måste uppdateras.

Europadomstolen har vid mål gällande hemlig övervakning angett att den vars rätt inskränks inte har rätt till insyn i den grad att de kan förutse när och hur övervakningen kommer utföras, utan inskränkningens speciella natur gör att Europadomstolen istället ställer högre krav på att lagstiftningen motverkar missbruk.[1] För att uppnå detta på bästa sätt verkar det naturligt att, så som ofta görs i förarbeten, studera vilka problem som identifierats i grannländerna och som följd vilka lösningar de därpå har ansett lämpliga.

1.1 Syfte och frågeställningar

Uppsatsens syfte är för det första att jämföra regleringen av hemlig dataavläsning under en utredning i Sverige och Danmark, samt respektive lands hantering av personlig integritet i relation till hemlig dataavläsning. För det andra att diskutera möjliga förbättringar inom detta område.

För att uppnå syftet kommer uppsatsen besvara följande frågeställningar:

1. I vilken utsträckning skyddar ländernas den personliga integriteten i relation till EKMR Artikel 8 och 13?
2. Vilka avgörande likheter och skillnader finns mellan den danska och svenska regleringen och motiveringen av hemlig dataavläsning?
3. Vilka åtgärder kan respektive land vidta för att bättre säkra den personliga integriteten?

1.2 Avgränsning

För att behandla hemlig dataavläsning kommer övergripande regler inom området för hemliga tvångsmedel att behandlas, dock inte individuella hemliga tvångsmedel utöver dataavläsning. Även om det möjligen hade gett en djupare förståelse för hemlig dataavläsning som en del av rättssystemet skulle uppsatsen bli för omfattande om dessa inkluderades för både svensk och

[1] Weber och Saravia mot Tyskland 29 juni 2006 p. 93.

dansk rätt. Inom regleringen för hemlig dataavläsning kommer bara dataavläsning som ett led i en utredning behandlas, då det är detta område som är fokus för uppsatsen.

Då uppsatsen fokuserar på den juridiska regleringen av hemlig dataavläsning kommer de tekniska aspekterna inte utforskas utöver vad som krävs för en grundläggande förståelse.

1.3 Teori och metod

För att uppnå uppsatsens syfte har den processrättsliga komparativa metoden tillämpats. Detta då komparativ metod fokuserar på just skillnader och likheter mellan jämförbara element av två eller flera rättssystem. För att jämförelsen ska bli betydelsefull krävs dock en djupare analys än en ren bokstavstolkning av paragrafer.[2]

En sådan analys kan uppnås genom tillämpning av funktionalitetsmetoden,[3] en närmare undersökning av de aktuella begreppen framställs senare i uppsatsen men utgångspunkten är att de regleringar som valts ut i följande kapitel uppfyller liknande resultat och bemöter liknande problem.

I jämförelsen av dessa behandlas både likheter och skillnader då dessa är oskiljaktiga delar av en helhet, vid regleringar med en inneboende likhet läggs dock av naturliga skäl mer fokus på skillnaderna.[4]

Valet av jämförelseländer motiveras delvis av praktiska skäl, då ländernas liknande rättssystem och språk sätter betydligt färre hinder för den som redan är bekant med det ena rättssystemet att även orientera sig i det andra, än en mer främmande rättsordning kunnat erbjuda.[5] Länderna är visserligen inte identiska men dock jämförbara i en rad andra faktorer vanligtvis ansedda relevanta för rättssystemets utformning såsom politiska och ekonomiska system, religion geografi och en mängd andra.[6] Då denna uppsats utgör en mikrokomparation, det vill säga har fokus på en detaljfråga,[7] möjliggör en interkulturell studie ett större fokus på den aktuella frågan och minimerar mängden övriga faktorer nödvändiga att redovisa för grundläggande jämförbarhet.

En viktig detalj vid utredning av utländsk rätt är behandlingen av juridiska begrepp. Många juridiska ord och fraser saknar en motsvarande översättning och även i de fall det existerar en språklig motsvarighet är det viktigt att inte anta att detta innebär att även begreppets faktiska

---

[2] Bogdan s. 45.
[3] Nääv och Zamboni s. 155, Bogdan s. 48.
[4] Bogdan s. 55.
[5] Bogdan s. 29.
[6] Bogdan s. 56-61.
[7] Bogdan s. 45-46.

betydelse är densamma.[8] För att detta inte ska bli ett problem i själva framställningen kommer dessa begrepp anges i originalspråk tillsammans med en förklaring av dess juridiska betydelse.

1.4 Forskningsläge

Ingen tidigare forskning jämför svenska och danska regleringen av hemlig dataavläsning genom privata integritetens lins.

1.5 Disposition

Uppsatsen är indelad i sex kapitel. Efter det inledande följer kapitel två vari redogörs för skyddet för den personliga integriteten i relevans till hemlig dataavläsning enligt Europakonventionen och Europadomstolens praxis. Kapitel tre redogör för svensk gällande rätt med fokus på HDAL och relevanta förarbeten. Kapitel fyra redogör för dansk gällande rätt med fokus på Retsplejeloven § 791 b och relevanta förarbeten. Kapitel fem jämför de två systemen och belyser skillnader gällande reglering och tillämpning. Kapitel sex presenterar sedan sammanfattande reflektioner och frågeställningarna besvaras.

2. Europakonventionen

Europakonventionen (härefter benämnd EKMR) gäller som svensk lag.[9] Lag eller annan föreskrift får enligt 2 kap 19 § RF inte meddelas i strid med Sveriges åtaganden på grund av EKMR.

EKMR infördes som Dansk lag 1992.[10] EKMR har i Danmark företräde över vanlig lag,[11] men är underställd grundlagen,[12] och skulle lagstiftaren vilja så vore det möjligt att ge en dansk lag företräde i det fall den avviker från EKMR.[13]

2.1 Artikel 8

Artikel 8.1 EKMR anger att var och en har rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens.
Eventuella inskränkningar regleras i 8.2 EKMR enligt vilken dessa rättigheter inte får inskränkas annat än

1. Med stöd av lag
2. Om det i ett demokratiskt samhälle är nödvändigt

---

[8] Bogdan s. 36.
[9] Se Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[10] Se Lov nr. 285 af 29. april 1992 om Den Europæiske Menneskerettighedskonvention.
[11] Betænkning 1407 (2001), s. 308f.
[12] Jmf. UfR 1999.800 H, (förhållandet till EU-rätten).
[13] Betænkning 1220 (1991), s. 197.

3. Med hänsyn till statens säkerhet, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

2.1.1 Lagstöd

Kravet på lagstöd innebär i sig att tre krav är uppfyllda:

1. För det första att åtgärden inte får strida mot inhemsk lag. Med lag syftas då inte endast på lagar utan även rättspraxis, förordningar, och andra föreskrifter.[14] Också privat lag i form av kollektivavtal kan under vissa omständigheter anses som lag.[15]
2. För det andra måste normen vara tillräckligt tillgänglig och precist formulerad för att den som lagen riktar sig till ska veta vad som förväntas av densamma.[16]
3. För det tredje måste lagen innehålla vissa rättssäkerhetsgarantier och inte tillåta för "unrestrained discretion", det vill säga vara upp till det okontrollerade omdömet då detta skulle göra lagens konsekvenser oförutsägbara.[17]

Kravet på förutsebarhet har vid mål gällande hemlig övervakning tillämpats så att den vars rätt inskränks inte har rätt till insyn i den grad att de kan förutse när och hur övervakningen kommer utföras, utan inskränkningens speciella natur gör att Europadomstolen istället ställer högre krav på att lagstiftningen motverkar missbruk.[18] Till följd av detta har Europadomstolen genom praxis utvecklat en minimistandard för krav som bör ställas på lagstiftning om dolda spaningsåtgärder eller hemliga tvångsmedel.

2.1.2 Minimiregler

Lagstiftningen bör ange följande:[19]

- Arten av de brott som kan leda till beslut om åtgärden
- En definition av de personkategorier som kan riskera att få sådana åtgärder riktade mot sig
- En begränsning i tid för hur länge åtgärden får pågå
- Förfaranderegler för undersökning, användning och lagring av de uppgifter som inhämtas
- Vilka försiktighetsåtgärder som ska vidtas vid överföring av information till andra parter
- De omständigheter under vilka inspelningar kan eller måste raderas

[14] Sunday Times v. UK 26 April 1979, A/30 p. 47.
[15] Madsen v. Denmark, No. 58341/00, och Wretlund v. Sweden, No. 46210/99.
[16] Sunday Times, p. 49.
[17] Silver and others v. UK par. 88-9, och Maestri v. Italy.
[18] Weber och Saravia v. Germany 29 juni 2006 p. 93.
[19] Roman Zakharov v. Russia, p. 231.

Vid bedömningen följer av Europadomstolens praxis att åtgärder som utgör ett större intrång i privatlivet bör kopplas till tydligare bemyndiganden och fler restriktioner än mindre inträngande åtgärder.[20]

Gällande tillsyn fastställer Europadomstolens praxis att eftersom den enskilda individen hindras från att själv söka ett effektivt rättsmedel är det ytterst viktigt att de rutiner som fastställts borde innebära tillfredsställande och likvärdiga garantier som skydd för dennes rättigheter.[21] Den godkännande myndigheten måste kunna bekräfta att det föreligger en skälig misstanke mot den aktuella personen samt ta reda på huruvida den begärda avlyssningen uppfyller kravet på "nödvändighet i ett demokratiskt samhälle", bland annat genom att bekräfta om det är möjligt att uppnå ändamålet med mindre restriktiva medel.[22]

Kontroll i det utförande stadiet kan utföras av utomrättsliga organ under förutsättning att dessa är självständiga gentemot de organ som bedriver åtgärden och har tillräckliga befogenheter och tillräcklig behörighet att utöva verksam och fortlöpande kontroll.[23]

För att en inskränkning ska anses nödvändig i ett demokratiskt samhälle måste det föreligga ett angeläget samhälleligt behov (“pressing social need”)[24]. Inom avvägningen av vad som kan anses nödvändigt har staterna ett visst tolkningsutrymme,[25] där bland annat nationell säkerhet anses väga särskilt tungt.[26]

2.2 Artikel 13

Artikel 13 EKMR kräver att var och en som fått sina fri- och rättigheter enligt konventionen kränkta ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Då artikel 13 gäller tillgången till ett effektivt rättsmedel krävs det inte att en kränkning faktiskt förekommit, utan det räcker att en individ med ett icke-ogrundat hävdande om en kränkning inte haft möjlighet till prövning.[27] Denna prövning ska vara effektiv inte bara i allmänhet, utan också i det individuella fallet.[28]

Så snart meddelande kan lämnas utan att äventyra syftet med restriktionen efter att övervakningen upphört, bör information snarast ges till berörda personer, och frånvaron av ett sådant krav i nationell lagstiftning har konstaterats oförenligt med konventionen.[29] Ett alternativ

[20] Uzun mot Tysklad, 2 september 2010, punkt 34-48.
[21] Roman Zakharov v. Russia, p. 233.
[22] Roman Zakharov v. Russia, p. 260.
[23] Roman Zakharov v. Russia, p. 275.
[24] Handyside v. UK, 7 December 1976, p. 48.
[25] Cameron - An introduction to the European Convention on Human Rights, 7th edition, (2014), s.119.
[26] Leander v. Sweden, 8 Juli 1987, A/116, p. 67 och under sektioner 5.2 och 5.4.
[27] Cameron, s. 160.
[28] Al-Nashif v. Bulgaria Nr. 50963/9, 20 juni 2002.
[29] Roman Zakharov v. Russia p. 287-288.

till detta är att en person som misstänker sig ha blivit eller fortfarande tror sig vara avlyssnad kan vända sig till domstol för prövning så att domstolarnas domsrätt inte är beroende av att personen redan blivit meddelad om förekommen övervakning.[30]

3. Svensk reglering

3.1 Lagen om hemlig dataavläsning

Hemlig dataavläsning behandlas i svensk rätt i Lag (2020:62) om hemlig dataavläsning (härefter benämnd HDAL). Som hemlig dataavläsning definieras i 1 § HDAL
"att uppgifter avsedda för *automatiserad behandling*, i hemlighet och med ett *tekniskt hjälpmedel* läses av eller tas upp i ett *avläsningsbart informationssystem*"

Med uppgifter avsedda för automatiserad behandling avses alla sorters uppgifter som uttrycks i en för en dator anpassad och läsbar form.[31] Begreppet tekniskt hjälpmedel avser såväl hårdvara som programvara.[32] Uppgifterna ska även vara kopplade till ett visst avläsningsbart informationssystem. Detta begrepp innefattar för det första all slags utrustning som kan användas för att kommunicera elektroniskt,[33] för det andra användarkonton eller en på motsvarande sätt avgränsad del av en kommunikationstjänst, lagringstjänst eller liknande tjänst.[34]

Med synnerlig anledning att anta menas i HDAL att det på grund av tillförlitliga uppgifter ska vara så gott som säkert, detta är ett betydligt högre krav än särskild anledning att anta, vilket innebär att utredningsläget ska visa någon faktisk omständighet som med viss styrka talar för.[35]

3.1.1 Tillämpningsområde under en förundersökning

För tillstånd till hemlig dataavläsning vid en förundersökning finns ett antal krav angivna i 4 § HDAL. Till att börja med ska åtgärden vara av synnerlig vikt för utredningen, detta innebär att det ska finnas skäl att räkna med att åtgärden verkligen kan få effekt, andra åtgärder ska vara otillräckliga, väsentligt svårare att genomföra eller förväntas leda till större integritetsintrång.[36] Förundersökningen ska gälla antingen:

1. Ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år

[30] Roman Zakharov v. Russia, p. 234.
[31] Prop 2019/20:64 s. 209.
[32] Prop 1994/95:227 s. 29.
[33] Prop 2019/20:64 s. 210-211.
[34] Prop 2019/20:64 s. 209 s.211.
[35] Prop 2019/20:64 s. 217.
[36] Prop 2019/20:64 s. 216.

2. Brott i 27 kap 2 § andra stycket 2-7 rättegångsbalken, dessa är samhällsfarliga brott,[37] bland annat sabotage och terroristbrott.
3. Försök, förberedelse eller stämpling till brott nämnt i punkt 1-2, om sådan handling är straffbelagd
4. Annat brott vars straffvärde kan antas överstiga fängelse i två år med hänsyn till omständigheterna.

Som huvudregel ska tillståndet gälla en i förundersökningen skäligen misstänkt. Denna misstankegrad är lägre än sannolika skäl, vilket är huvudregeln för häktning, men högre än kan misstänkas, vilket krävs för att hålla kvar en misstänkt för förhör längre tid än annars. Misstanken ska gälla ett konkret brott och grunda sig på en objektiv och allsidig bedömning av utredningsmaterialet.[38]

Vidare ska tillståndet avse ett avläsningsbart informationssystem som används, det finns särskild anledning att anta har använts eller kommer användas av den misstänkte. Informationsystemet i fråga kan ägas av den misstänkte men också av någon annan, det är heller inget hinder att andra personer använder informationsystemet.[39]

Kommunikationsavlyssning, kommunikationsövervakning, och platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta under den tid tillståndet gäller, det ska vara så gott som säkert att detta kommer ske. Uttrycket tar sikte på en riktad kontakt mellan informationssystem. Ett tillstånd gällande kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig, dock inte någons stadigvarande bostad.[40]

3.1.2 Tillstånd och beslutsfattande

Beslut

Frågor om hemlig dataavläsning prövas enligt 14 § HDAL av rätten på ansökan av åklagare. Åklagaren kan enligt 17 § HDAL ge tillstånd i avvaktan på rättens beslut om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens tillstånd. Dock aldrig för hemlig dataavläsning som gäller rumsavlyssningsuppgifter. Detta endast i situationer när ändamålet med åtgärden riskerar att gå förlorat om rättens tillstånd skulle

[37] Prop 2019/20:64 s. 216.
[38] Prop 2019/20:64 s. 216.
[39] Prop 2019/20:64 s. 217.
[40] Prop 2019/20:64 s. 217-218.

inväntas.[41] Har åklagaren gett ett tillstånd ska detta utan dröjsmål anmälas till rätten.[42] I anmälan ska skälen för åtgärden anges och rätten ska skyndsamt pröva ärendet.

Om rätten finner att det saknats skäl för åtgärden ska den omedelbart avbrytas och de uppgifter som lästs av eller tagits upp får inte användas i en brottsutredning till nackdel för någon som uppgifterna avser. Uppgifterna får däremot användas om de kan fria den berörde från brottsmisstankar eller på annat sätt användas till dennes fördel.[43]

Handläggning

Ett tillstånd till hemlig dataavläsning ska enligt 18 § HDAL ange:

1. Vilken tid tillståndet avser.
2. Vilket avläsningsbart informationssystem tillståndet avser. Uppgifterna måste vara så specifierade att det går att verkställa åtgärden och att det är möjligt att bedöma kopplingen mellan informationssystemet och den som åtgärden avser.[44]
3. Vilken uppgiftstyp som ansökan avser.[45]
4. Villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Dessa kan vara av teknisk karaktär, såsom en föreskrift om att den brottsbekämpande myndigheten som ska verkställa en åtgärd på en viss utpekad plats måste göra det tekniskt omöjligt att genomföra hemlig dataavläsning på annan plats. De kan också vara av en annan karaktär, såsom att endast samtal med en viss person får vara föremål för hemlig dataavläsning eller begränsning av vilka uppgifter som får läsas av eller tas upp.[46]
5. Vid åtgärd som gäller rumsavlyssningsuppgifter, vem som är skäligen misstänkt för brottet.

Om tillståndet avser kameraövervakningsuppgifter, rumsavlyssningsuppgifter eller är förenat med ett tillträdestillstånd ska även platsen anges i tillståndet.

Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad. Vid bedömningen får hänsyn tas till den tid som kan behövas för att installation eller motsvarande ska kunna utföras.[47]

Det finns inte någon lagstadgad bortre tidsgräns för tiden innan tillståndet beviljades, vilket kan ha betydelse när lagrade uppgifter ska läsas av. Rätten bör dock av bland annat integritetsskäl

[41] Prop 2019/20:64 s. 231.
[42] Prop. 2013/14:237 s. 183.
[43] Prop 2019/20:64 s. 232.
[44] Prop 2019/20:64 s. 232.
[45] Prop 2019/20:64 s. 233.
[46] Prop 2019/20:64 s. 233.
[47] Prop 2019/20:64 s. 234.

begränsa de uppgifter som får tas upp även såvitt avser tiden före beslutet. Även om det finns en bortre tidsgräns på en månad kan den sökande förlänga ett tillstånd genom att före tillståndstidens utgång kommer in med en ny ansökan.[48]

Som anges i 19 § HDAL ska handläggningen ske skyndsamt. Även inskränkande villkor kan överklagas, alternativt kan det offentliga ombudet överklaga ett tillståndsbeslut på grunden att det inte är förenat med tillräckliga villkor.[49]

Beslut om hemlig dataavläsning får verkställas omedelbart, om det inte längre finns skäl för ett tillstånd ska beslutet omedelbart upphävas av den som ansökt om åtgärden eller rätten. Detta följer av 20 § HDAL.

Rätten har en skyldighet angiven i 21 § HDAL att underrätta Säkerhets- och integritetsskyddsnämnden skyndsamt vid beslut om hemlig dataavläsning. Detta gäller alla rättens beslut, såväl bifall som avslag och kompletterande beslut, och bör lämpligen göras samma eller följande arbetsdag som beslutet fattas.[50]

3.1.3 Genomförande

Val av teknik

Det framkommer av 22 § HDAL att när ett tillstånd beviljats får de tekniska hjälpmedel som behövs användas. Den verkställande myndigheten får själv bestämma vilken teknik som ska användas i det enskilda fallet och tekniken omfattas inte av domstolens prövning. Rätten kan dock ställa villkor om verkställandet för att säkerställa intresset av att enskildas personliga integritet inte kränks i onödan.[51] Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas. Till exempel kan detta ske genom installation av programvara eller installation av ett fysiskt föremål på informationssystemet. Även tekniska hjälpmedel redan existerande i informationssystemet kan användas, såsom GPS eller kamera.[52]

Den valda tekniken ska enligt 23 § HDAL anpassas efter det tillstånd som beviljats, den får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet. Om sådana uppgifter ändå har lästs av ska de, och uppteckningar av dem, omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Det är då fråga om så kallad otillåten

[48] Prop 2019/20:64 s. 234.
[49] Prop 2019/20:64 s. 234.
[50] Prop 2019/20:64 s. 235.
[51] Prop 2019/20:64 s. 236.
[52] Prop 2019/20:64 s. 236.

tilläggsinformation.[53] Uppgifterna ska behandlas på samma sätt som uppgifter från ett felaktigt tillstånd från åklagare.[54]

Aktsamhetskrav

Vid verkställande får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt och även i detta fall får informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser inte åsidosättas, försämras eller skadas till följd av verkställigheten. Detta är aktsamhetsregler framställda i 25 § HDAL. När verkställigheten avslutas ska den de åtgärder som behövs vidtas för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla minst samma nivå som vid verkställighetens början. Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet har upphävts. Det är således inte möjligt för den verkställande myndigheten att efter det att tillståndstiden har löpt ut kunna utnyttja samma verktyg igen utan att installera utrustningen på nytt.[55]

3.1.4 Förbud mot hemlig dataavläsning

Förbud för vissa verksamheter

Det finns enligt 11 § HDAL ett absolut förbud mot hemlig dataavläsning för informationssystem som stadigvarande används eller är särskilt avsett att användas

1. I verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen. Här avses främst medieföretag.
2. I verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453).
3. Av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, dock endast i verksamhet för bikt eller enskild själavård.

Det är den brottsbekämpande myndigheten som ska presentera uppgifter som tydliggör att informationssystemet inte omfattas av förbudsregeln, om det finns en sådan risk. Visar det sig efter beviljat tillstånd att det gäller ett förbjudet informationssystem måste åtgärden omedelbart avbrytas.[56] Platser som används för någon av de fredade verksamheterna är fredade mot tillträdestillstånd för hemlig dataavläsning.[57]

[53] Prop 2019/20:64 s. 237.
[54] Prop 2019/20:64 s. 237.
[55] Prop 2019/20:64 s. 239.
[56] Prop 2019/20:64 s. 226.
[57] Se 13 § HDAL.

Förbud mot vissa uppgifter

Hemlig dataavläsning avseende lagrade uppgifter eller uppgifter som visar hur ett informationssystem används får enligt 27 § HDAL inte avse uppgifter som befattningshavare eller vissa angivna andra persongrupper, till exempel advokater och läkare, inte får höras som vittne om. Förutsatt att uppgifterna är i dessa personers innehav eller den av tystnadsplikt skyddade delen av deras verksamhete. Dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § 2-6 st rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Detta är samma persongrupp som avses gällande lagrade uppgifter. Kommer förbjudna uppgifter fram under verkställigheten ska åtgärden omedelbart avbrytas och förbjudna uppgifter förstöras.

3.1.5 Skyldighet att medverka

Vissa verksamheter är enligt 24 § HDAL skyldiga att på begäran medverka i samband med verkställighet av hemlig dataavläsning. Medverkan är inte närmare reglerat utan beror på hur den verkställande myndigheten formulerar sin begäran.[58] Detta handlar om aktörer som tillhandahåller allmänna kommunikationsnät, till exempel operatörer av mobiltelefoni och internet.[59] Tystnadsplikt föreligger enligt 32 § HDAL för den som i samband med sådan verksamhet har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning.[60]

3.1.6 Överskottsinformation och lagring av uppgifter

För hemlig dataavläsning under en förundersökning hanteras uppgifter enligt 27 kap 23 a, 24 §§ RB. Framkommer uppgifter om ett annat brott än det som legat till grund för beslutet får uppgifterna alltså användas för att utreda brottet. För att inleda en förundersökning måste dock vara föreskrivet fängelse i ett år eller mer för brottet alternativt finnas särskilda skäl. Undantaget är hemlig dataavläsning avseende rumsavlyssningsuppgifter, för vilka det för att inleda en förundersökning måste det vara föreskrivet tre år eller mer för brottet alternativt vara ett sådant brott som ger möjlighet till hemlig rumsavlyssning.[61]

Informationen ska granskas snarast möjligt och skall i de delar den är av betydelse från brottsutredningssynpunkt bevaras till dess förundersökningen har lagts ned eller avslutats eller,

[58] Prop 2019/20:64 s.237.
[59] Prop 2019/20:64 s.237.
[60] Prop 2019/20:64 s.244.
[61] 27 kap 23 a § RB.

om åtal väckts, målet har avgjorts slutligt. I de delar som informationen är av betydelse för att förhindra förestående brott skall den bevaras så länge det därför behövs och därefter förstöras.[62]

3.1.7 Offentligt ombud

Enligt 16 § HDAL ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde när ansökan har kommit in. Vid sammanträdet ska den som gjort ansökan och det offentliga ombudet närvara. Närvaroplikten gäller såväl vid grundbeslutet som vid eventuella kompletterande beslut.[63] Det offentliga ombudet ska i enlighet med 27 kap. 26 § RB bevaka enskildas integritetsintressen och har rätt att ta del av det som förekommer i ärendet, yttra sig och överklaga rättens beslut, uppdraget gäller enligt 27 kap. 28 § 2 st RB även i högre rätt.[64]

3.1.8 Underrättelse till en enskild

Underrättelse till en enskild behandlas enligt 27 kap 31-33 §§. Den som har varit misstänkt för brott och utsatts för åtgärden ska enligt 31 § som huvudregel underrättas om detta så snart det kan ske utan men för utredningen, dock senast en månad efter att förundersökningen avslutats. Underrättelse behöver inte lämnas om den enskilde redan fått ta del av uppgifterna eller om det är uppenbart utan betydelse. Har någon annan än den misstänkte utsatts för hemlig dataavläsning ska även denne underrättas. Om hemlig dataavläsning gällande kameraövervaknings- eller rumsavlyssningsuppgifter har utförts på en plats som är ägd av någon annan än den misstänkte och inte tillgänglig för allmänheten ska även innehavaren av platsen underrättas.

Underrättelsen ska enligt 33 § innehålla uppgifter om vilket tvångsmedel som har använts och när det har skett. Den som är eller har varit misstänkt för brott skall få uppgift om vilken brottsmisstanke som har legat till grund för åtgärden eller som åtgärden har lett till. Den som inte är eller har varit misstänkt för brott skall få uppgift om detta. Som huvudregel ska underrättelsen även innehålla en uppgift om vilket informationssystem som åtgärden avsett. För rumsavlyssnings- eller kameraövervakningsuppgifter ska även informeras om vilken plats dessa inhämtats.

För uppgifter som omfattas av vissa former av sekretess ska underrättelsen skjutas upp tills sekretess inte längre gäller. Har underrättelsen av denna anledning inte kunnat lämnas inom ett år behöver underrättelse inte lämnas. Underrättelse behöver inte heller lämnas om uppgifter som gäller ett antal brott specificerade i 33 § 3 st, till exempel sabotage eller terroristbrott.

---

[62] 27 kap 24 § RB.
[63] Prop 2019/20:64 s.230.
[64] Prop 2019/20:64 s.230.

3.1.9 Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden (SIN) utövar tillsyn över hemlig dataavläsning och är även tillsynsmyndighet för behandlingen av personuppgifter i de brottsbekämpande myndigheterna. Detta angivs i 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (tillsynslagen). Enligt 3 § 1 st tillsynslagen ska SIN på enskilds begäran kontrollera om den enskilde har utsatts för hemliga tvångsmedel och om användningen har varit i enlighet med lag. Enligt 2 § tillsynslagen ska SIN utöva sin tillsyn genom inspektioner och andra undersökningar.

3.1.10 Proportionalitetskrav

För att ett tillstånd till hemlig dataavläsning ska få beviljas måste proportionalitetsprincipen beaktas, enligt 3 § HDAL är det ett krav att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär, både för den åtgärden riktas mot och för annat motstående intresse.

För att proportionalitetskravet ska anses uppfyllt måste andra åtgärder för att komma åt de aktuella uppgifterna vara otillräckliga, väsentligt svårare att genomföra, eller förväntas leda till större integritetsintrång.[65]

3.2 Tillämpning

När SIN granskade en antal ärenden gällande hemlig dataavläsning visade det sig att flertalet tillstånd saknat sådana villkor som enligt 18 § HDAL är obligatoriska. Detta innebär att det i efterhand inte varit möjligt att kontrollera hur ärendet hanterats, till exempel i de fall då det vid ansökan redogjorts för hur åtgärden skulle verkställas och detta av rätten ansetts tillräckligt.[66] Detta blir av särskild vikt då majoriteten av granskade tillstånd omfattat alla uppgiftstyper med undantag för kameraövervaknings- och rumsavlyssningsuppgifter.[67]

4. Dansk reglering

4.1 Retsplejeloven § 791 b

Dataavläsning behandlas i Dansk rätt i § 791 b Retsplejeloven (härefter benämnd RpL) och definieras som avläsning av icke offentligt tillgängliga upplysningar i ett informationssystem med hjälp av program eller annan utrustning. Paragrafen infördes som en del av ett "anti-terrorpaket" i ett lagstiftningsintiativ intierat efter terrorangreppet mot USA 11 september 2001.[68]

[65] Prop 2019/20:64 s.214-215
[66] Dnr 92-2020 "Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts" st 5.3.4.
[67] Dnr 92-2020 "Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts" st 5.3.3.
[68] 2001/2 LSF 35 p. 1.1 (Forslag til Lov om aendring af straffeloven, retsplejeloven, lov om….).

Med informationssystem avses här en dator eller annat databehandlingssystem, även annan elektronisk utrustning kan dock omfattas av bestämmelsen om utrustningen har funktioner liknande dem som finns i persondatorer.[69] Danmarks högsta domstol har emellertid fastställt att begreppet inte innefattar en profil på en onlinetjänst som kan nås från var som helst.[70] Ingreppet kan ske med både hårdvara och mjukvara, dock omfattar inte dataavläsning ingrepp utan speciell utrustning, till exempel genom att utnyttja konkreta sårbarheter i systemet.[71]

4.1.1 Tillämpningsområdet för hemlig dataavläsning

Dataavläsning får i enlighet med 791 b § 1 st RpL användas om:

1. Det finns bestämda grunder att anta att informationssystemet används av en misstänkt i förbindelse med planerad eller begådd kriminalitet uppräknad i punkt nr 3,
2. ingreppet måste antas vara av avgörande betydelse för efterforskningen, och
3. efterforskningen gäller en överträdelse som enligt lag kan straffas med fängelse i 6 år eller mer eller en avsiktlig överträdelse av *Straffeloven* kapitel 12, om landsförräderi och andra förbrytelser mot mot statens självständighet och säkerhet eller 13, om brott mot statsförfattningen och de översta statsmyndigheterna.

Misstankegraden anges inte närmare i lagbestämmelserna, men misstanken ska i varje fall vara rimligt och konkret grundad i föreliggande information.[72] För att vara av avgörande betydelse ska ingreppet ha en mycket väsentlig betydelse för sakens efterforskning, men det är inte nödvändigt att ingreppet är den enda möjligheten.[73]

Då det viktiga är att informationssystemet används av en misstänkt spelar det ingen roll vem som äger informationssystemet, detta kan till exempel ägas av en annan privatperson eller den misstänktes arbetsplats.[74]

4.1.2 Beslut om dataavläsning

Beslut om dataavläsning behandlas i 791 b stycke 3 RpL och fattas av rätten genom *kendelse*, skillnaden mellan detta och "beslut" ligger i att *kendelse* ska styrkas.). I beslutet ska anges vilket informationssystem som ingreppet avser.

Om det inte är möjligt för polisen att lämna ytterligare uppgifter om informationssystemets fabrikat, nummer eller liknande som entydigt kan identifiera det, får i stället meddelas att

[69] 2001/2 LSF 35 Bemærkninger til lovforslagets enkelte bestemmelser.
[70] U 2012.2614 H - politiets adgang til Facebook og Messenger-profiler med rette kode.
[71] TfK2018.814 - Politiets hjemmel til »hacking« som led i en efterforskning s. 4.
[72] Bet 1984 nr. 1023 s. 97.
[73] 2001/2 LSF 35 Bemærkninger til lovforslagets enkelte bestemmelser.
[74] 2001/2 LSF 35 Bemærkninger til lovforslagets enkelte bestemmelser.

ingripandet ska avse den datorutrustning som används på en viss, avgränsad plats, till exempel en specifik hemadress eller ett kontor på en arbetsplats.[75] Ett annat alternativ är att informationssystemet identifieras genom ägaren, till exempel "den misstänktes bärbara dator".[76]

Kendelsen beskrivs närmare i 783 § RpL:

I 1 st, mening 3, fastställs att det i *kendelsen* ska anges de konkreta omständigheter vilka ligger till grund för att rekvisiten för ingreppet är uppfyllda, i mening 4 anges att *kendelsen* kan upphävas när som helst. Enligt 3 st ska det i *kendelsen* anges inom vilken tidsram ingripandet får genomföras. Denna tid bör vara så kort som möjligt och får inte överstiga 4 veckor. Perioden kan förlängas med högst 4 veckor i taget, även detta genom *kendelse*.

I 4 st anges att om det skulle innebära att syftet med insatsen vore bortkastat att avvakta rättens *kendelse* får polisen besluta om att ingripandet ska genomföras. Polisen ska i så fall lägga fram ärendet till rätten så snart som möjligt och senast inom 24 timmar efter ingripandet. Rätten avgör genom *kendelse* om ingripandet kan godkännas, samt om det kan upprätthållas och i så fall under vilken tid. Borde ingripandet enligt rättens bedömning inte genomförts ska domstolen underrätta Riksadvokaten.

4.1.3 Förbud mot vissa uppgifter

Enligt 782 § 2 st RpL får dataavläsning inte företas avseende den misstänktes anknytning till personer som enligt reglerna i 170 § RpL är uteslutna från att agera som vittne. Bland annat präster i folkkyrkan eller andra trossamfund, läkare, försvarare, domstolsmedlare, och jurister.

4.1.4 Överskottsinformation

Får polisen information om ett brott som inte har och inte kunnat ligga till grund för ingripandet får polisen i enlighet med 789 § RpL använda dessa uppgifter som ett led i efterforskningen av det nyupptäckta brottet. Uppgifter som inhämtats vid hemlig dataavläsning får inte användas som bevis i domstol om ett brott som inte har legat och inte heller kunnat ligga till grund för ingripandet. Ett undantag till detta är om andra åtgärder inte är lämpliga för att säkra bevis i målet, ärendet avser ett brott som enligt lag kan ge fängelse i 1 år och 6 månader eller mer, och domstolen finner det för övrigt ostridigt.

[75] 2001/2 LSF 35 Bemærkninger til lovforslagets enkelte bestemmelser.
[76] 2001/2 LSF 35 Bemærkninger til lovforslagets enkelte bestemmelser.

4.1.5 Förstörande av information

Återgivningar av vad som kommit till polisens kännedom vid ingripandet ska hanteras enligt 791 § RpL.

Dessa förstöras om ingen åtalas för det brott som legat till grund för ingripandet eller om åtal senare överges. Polisen underrättar förordnad advokat när förstörelse har skett. Om materialet är av fortsatt efterforskningsmässig betydelse får förstöring underlåtas eller skjutas upp under en viss tid. Polisen för ärendet till domstolen, som innan beslut fattas ska ge den förordnade advokaten tillfälle att yttra sig. Detta gäller inte material som inhämtats som ett led i efterforskning av brott mot 12 kap, och 13 kap straffeloven, icke inkluderat 116-117 §§ om valfusk.

Om det i samband med telefonavlyssning, annan avlyssning eller brevöppning har gjorts ingripande i den misstänktes anknytning till personer som enligt reglerna i 170 § RpL är uteslutna från att avlägga vittnesmål, ska material om detta ingripande förstöras omedelbart. Detta gäller dock inte om materialet föranleder åtal för brottslig verksamhet mot vederbörande eller att tjänsten som försvarare fråntas vederbörande. Polisen ska dessutom förstöra material som erhållits genom hemlig dataavläsning och som visar sig sakna efterforskningsmässig betydelse.

4.1.6 Offentligt ombud

Innan rätten fattar beslut ska enligt 784 § RpL en advokat förordnas för den som ingripandet avser och advokaten ska ha möjlighet att yttra sig. En advokat som har förordnats ska enligt 785 § RpL underrättas om alla rättsförhandlingar i målet och har rätt att närvara vid dessa samt att ta del av det material som polisen tillhandahåller. Advokaten har även rätt att få en kopia av materialet. Om polisen finner att materialet är av särskilt sekretessbelagt karaktär och att en kopia av det därför inte bör överlämnas, ska frågan om detta på begäran av advokaten föras till rätten för avgörande. Advokaten får inte vidarebefordra de inkomna uppgifterna till andra eller utan polisens samtycke kontakta den som ingripandet har begärts mot. Rätten får besluta att den förordnade advokaten inte senare under målet får fungera som försvarare för någon tilltalad.

Rätten avgör enligt 746 § 1 st RpL tvister om lagligheten av polisens efterforskning samt om den tilltalades och försvararens befogenheter, inklusive framställningar från försvararen eller den tilltalade om att ytterligare efterforskningsåtgärder vidtas.

4.1.7 Underrättelse till enskild

Efterföljande underrättelse om ett genomfört ingrepp behandlas i 788 § stycke 1, 3, och 4 RpL. Underrättelsen lämnas till den som råder över det informationssystem som varit avläst, normalt är detta ägaren, men även en brukare som inte äger informationssystemet kan ha sådan rådighet att underrättelse ska ske till denne.[77]

Efter avslutad åtgärd ska underrättelse lämnas. Har den till vilken anmälan ska lämnas varit misstänkt i ärendet, ska underrättelse lämnas om detta och om vilket brott misstanken avser.

Underrättelsen ska lämnas så snart som möjligt om polisen inte inom 14 dagar efter utgången av den tid för vilken tillstånd för ingripandet gällde har framställt begäran om underlåtenhet eller anstånd med underrättelse. Finns det enligt 784 § RpL, förordnad advokat, skall kopia av underrättelsen tillställas denne.

Kommer anmälan vara till nackdel för efterforskningen eller till nackdel för efterforskningen i annat pågående mål om brott som enligt lagen kan ligga till grund för hemlig dataavläsning, eller talar hänsyn till uppgifter om polisens efterforskningsmetoder eller andra omständigheter emot underrättelse, får rätten, på begäran av polisen, besluta att underrättelse ska underlåtas eller skjutas upp under en viss tid, som får förlängas genom ett senare beslut. Finns det förordnad advokat, ska han ha tillfälle att yttra sig innan rätten beslutar om underlåtenhet eller anstånd med underrättelsen.

4.1.8 Datatilsynet

Det finns möjlighet för den enskilde att efterfråga information om huruvida uppgifter om denne behandlas och i så fall vilken information som behandlas och dess syfte. Dessa rättigheter regleras huvudsakligen i lov om retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven) kapitel 4-8. Invändningar mot polisens behandling av den enskildes personuppgifter kan i första hand riktas till *Rigspolitiet*. Det finns även möjlighet att klaga över polisens avgöranden till *Datatilsynet*, vilket är en oavhängig statlig myndighet reglerad i retshåndhævelseslovens avsnitt 8, som även vid begäran kan kontrollera att behandlingen av personuppgifterna är lagenlig.[78]

4.1.9 Proportionalitetskrav

I 791 b § St 2 RpL fastställs ett krav på proportionalitet i förhållande till ingreppets syfte, sakens betydelse, och den kränkning och olägenhet som ingreppet kan antas förorsaka den eller de som drabbas.

[77] 2001/2 LSF 35 Bemærkninger til lovforslagets enkelte bestemmelser.
[78] Danska polismyndigheten, “Politiets brug af personoplysninger”.

4.2 Tillämpning

Enligt tidningen Information skriver Rikspolisen till en tysk kontakt att de har mycket liten erfarenhet på området - "några fall om året" i ett brev från 2007 som tidningen har fått tillgång till.[79] Även i andra fall har information "under handen" getts om att narkotikaefterforskande polis har begränsad nytta av bestämmelsen, då de saknar säkerhetspolisens (PET)s tekniska utrustning.[80]

5. Jämförelse

5.1 Definitonsmässigt

Definitionsmässigt är ingreppen väldigt lika. Det svenska begreppet "automatiserad behandling" och det danska "ikke offentlig tilgængelige oplysninger", har dock delvis olika funktion. Båda ger en relativt öppen begränsning av vilken typ av uppgifter som får tas upp, men den svenska syftar att visa att det inte finns någon begränsning på de uppgifter i en för en dator läsbar form, som får tas upp, den danska avser förtydliga att upptagning av offentliga upplysningar, vilket inte kräver lagstöd, inte utgör dataavläsning.

Det svenska "avläsningsbart informationssystem" kan avse både fysisk utrustning och, till exempel ett användarkonto. Detta skiljer sig från det danska "informationssystem" vilket inte kan avse användarkonton på onlinetjänster, förutsatt att de kan nås från vilket typiskt system som helst och det alltså inte är en viss hårdvara som avses.

5.2 Minimireglerna

Arten av de brott som kan leda till beslut om åtgärden

Den svenska regleringen tillåter dataavläsning för brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,[81] i RpL anges istället ingreppet för en överträdelse som enligt lag kan straffas med fängelse i 6 år.[82] Det vill säga att HDAL använder minimistraffet och RpL använder maxstraffet.
I tydlighet är dom närliggande, då ingen av avgränsningarna kräver en bedömning av det aktuella brottet.

För vissa uppräknade samhällsfarliga brott i HDAL frångås begränsningen, RpL har ett liknande undantag gällande bland annat landsförräderi och förbrytelser mot statsförfattningen.[83] HDAL

[79] Stræde, Koch, Mathias, A/S Information, "Myndigheder mørklægger brug af terrorbeføjelse".
[80] Schartum, Wiese, Dag, (red), Overvåking i en rettsstat, s. 207.
[81] Se Kap 3.1.1.
[82] Se Kap 4.1.1.
[83] Se Kap 3.1.1, resp, 4.1.1.

har emellertid en straffvärdeventil för "Annat brott vars straffvärde kan antas överstiga fängelse i två år med hänsyn till omständigheterna.".[84] I denna fråga är alltså den danska lagstiftningen klart mer avgränsad.

Definition av personkategorier som kan riskera att utsättas för åtgärden

Det framgår av 791 b 1 st RpL och 1 § HDAL att hemlig dataavläsning avser ett visst informationssystem eller avläsningsbart informationssystem, av vilka det svenska begreppet är mer vidsträckt.

I svensk lagstiftning ska det finnas faktiska omständigheter som talar för både skuld och att det föreligger en koppling till den misstänkte. Dock kan det gälla ett informationssystem som används även av icke-misstänkta.[85] I RpL ska informationssystemet på bestämda grunder kunna antas användas av en misstänkt, även här kan informationssystemet användas av flera.[86]

Gällande kommunikationsavlyssning-, kommunikationsövervakning-, och platsuppgifter får även informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta avläsas i svensk lagstiftning, här avses en riktad kontakt.[87]

En begränsning i tid för hur länge åtgärden får pågå

Tillstånd enligt svensk lagstiftning är begränsade till en månad, varefter tillståndet måste förnyas. Det finns varken någon begränsning för hur många gånger tillståndet kan förnyas eller någon bortre tidsgräns för information insamlad innan tiden för beslutet, men dessa ska inte vara längre än nödvändigt.[88] Dansk dataavläsning har en motsvarande reglering, tidsramen för en *kendelse* är dock 4 veckor.[89]

Förfaranderegler

För undersökning

Det definieras i svensk rätt inte närmare vilken teknik som får användas för åtgärden och detta prövas inte av rätten, men tekniken får inte kunna läsa av någon uppgiftstyp som ligger utanför det aktuella tillståndet. Vid verkställandets avslut får informationssäkerheten i påverkade informationssystem inte vara försämrad.[90]

---

[84] Se Kap 3.1.1.
[85] Se Kap 3.1.1.
[86] Se Kap 4.1.1.
[87] Se Kap 3.1.1.
[88] Se Kap 3.1.2.
[89] Se Kap 4.1.2.
[90] Se Kap 3.1.3.

Dansk lagstiftning har ingen motsvarande reglering av förfarandet, emellertid är ingrepp som inte utnyttjar teknisk utrustning, utan endast information, inte omfattade av det danska dataavläsningsbegreppet.[91] Detta skiljer sig från det svenska som möjliggör att tekniska sårbarheter utnyttjas.[92]

För användning och lagring av inhämtade uppgifter

I svensk lagstiftning får uppgifter som inkommit användas för att utreda både det brott som legat till grund för åtgärden och andra brott. För att inleda en förundersökning måste dock vara föreskrivet fängelse i ett år eller mer för brottet alternativt finnas särskilda skäl. Upptagningarna ska granskas snarast möjligt och om de varken tillhör en pågående undersökning eller är av betydelse för att förhindra förestående brott ska de förstöras.[93]

I dansk rätt får information om ett brott som inte har legat och inte kunnat ligga till grund för ingripandet använda dessa uppgifter som ett led i utredningen av det brottet. De får dock endast användas som bevis i domstol i detta fall om andra åtgärder inte är lämpliga för att säkra bevis i målet, ärendet avser ett brott som enligt lag kan ge fängelse i 1 år och 6 månader eller mer, och domstolen finner det för övrigt ostridigt.[94] Om information hör till en utredning som inte längre är pågående, och materialet inte är av fortsatt utredningsmässig betydelse ska detta förstöras.[95]

Försiktighetsåtgärder vid överföring av information till andra parter

Svensk lagstiftning föreskriver tystnadsplikt för den som i samband med skyldigheten att medverka har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning. Tystnadsplikten gäller vem som helst som fått del av eller tillgång till uppgifterna och både direkta och indirekta uppgifter.[96]

I dansk rätt hanteras informationssamling med hjälp av verksamheter som hanterar kommunikationstjänster istället med tvångsingreppet *indgreb i meddelelseshemmeligheden*. Det anses alltså inte som hemlig dataavläsning.[97] Det offentliga ombudet får emellertid inte vidarebefordra de inkomna uppgifterna till andra.[98]

De omständigheter under vilka inspelningar kan eller måste raderas

Utöver vad som angetts gällande lagring av uppgifter finns det förbud mot hemlig dataavläsning i vissa fall, inhämtas ändå sådana uppgifter ska de omedelbart förstöras.

---

[91] Se Kap 4.1.
[92] Se Kap 3.1.3.
[93] Se Kap 3.1.6.
[94] Se kap 4.1.4.
[95] Se Kap 4.1.5.
[96] Se Kap 3.1.5.
[97] TfK2018.814 - Politiets hjemmel til »hacking« som led i en efterforskning s.4.
[98] Se kap 4.1.6.

Kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig inte skulle ha kunnat höras som vittne.[99] Även den danska lagstiftningen förbjuder dataavläsning avseende den misstänktes anknytning till personer uteslutna från att agera som vittne.[100] Då dansk rätt inte tillåter avläsning av informationssystem den misstänkte inte använder finns heller ingen begränsning av uppgifter som kunnat insamlas på detta vis.

5.3 Tillsyn och nödvändigt i ett demokratiskt samhälle

I Svensk rätt prövas frågor om hemlig dataavläsning av rätten, åklagaren har dock möjlighet att ge ett tillfälligt tillstånd i avvaktan på rättens beslut. Beslutar rätten att det saknats skäl för godkännande får uppgifterna inte användas i en brottsutredning de omfattades nackdel. Rätten har även möjlighet att förelägga villkor av teknisk karaktär eller annan karaktär.[101]

En liknande möjlighet för åklagaren finns i dansk rätt, polismyndigheten kan besluta om att åtgärden ska genomföras och detta prövas sedan av rätten.[102]

Om det inte längre finns skäl för åtgärden ska i svensk rätt beslutet omedelbart upphävas av den som ansökt om åtgärden eller rätten, domstolen har emellertid endast uppsyn vid tillståndsprövningen vilket i praktiken innebär att det är upp till den ansökande att avbryta i förtid. När beslutet fattats har rätten en skyldighet att skyndsamt underrätta SIN.[103] Även i dansk rätt kan *kendelsen* när som helst upphävas när rätten anser att det inte finns skäl att fortsätta.[104]

Dansk rätt har varken den typ av villkor som uppställs vid den svenska prövningen, eller det krav som där finns på att typen av uppgift ska anges i tillståndet.[105] Åtgärden måste emellertid vara av avgörande betydelse för efterforskningen[106] och både svensk och dansk rätt kräver att åtgärdens syfte är proportionerlig mot den kränkning alternativt det intrång som ingreppet kan antas förorsaka.[107] I dansk rätt ska dessutom i *kendelsen* anges de konkreta omständigheter vilka ligger till grund för att rekvisiten för ingreppet är uppfyllda.[108]

Ett offentligt ombud närvarar i både dansk och svensk rätt vid beslut om hemlig dataavläsning. Det offentliga ombudet har rätt att ta del av allt som förekommer i ärendet, yttra sig, och överklaga rättens beslut. I svensk rätt är ombudet syfte att bevaka integritetsintressen för enskilda

[99] Se Kap 3.1.4.
[100] Se Kap 4.1.3.
[101] Se kap 3.1.2.
[102] Se Kap 4.1.2.
[103] Se kap 3.1.2.
[104] Se kap 4.1.2.
[105] Se kAp 3.1.2.
[106] Se Kap 4.1.1.
[107] Se kap 3.1.10, 4.2.9.
[108] Se kap 4.1.2.

i allmänhet, detta skiljer sig från dansk rätt på så sätt att det där det är upp till domstolen om ombudet senare under målet får agera som försvarare för någon tilltalad, detta är alltså inte otänkbart.[109]

5.4 Tillgång till effektiva rättsmedel

Då den enskilda hindras från att själv söka ett effektivt rättsmedel måste de rutiner som fastställts innebära tillfredsställande och likvärdiga garantier som skydd för dennes rättigheter. Utöver vad som redan diskuterats om tillsyn utgör underrättelse till den enskilda en möjlighet för denne att själv i efterhand ta vara på sina rättigheter.

I svensk rätt ska den som har varit misstänkt för brott eller någon annan än denne, som utsatts för hemlig dataavläsning, underrättas om detta senast en månad efter att förundersökningen avslutats. Underrättelsen ska inkludera uppgifter om vilket tvångsmedel som har brukats, när det har skett, och vilken brottsmisstanke som legat till grund för åtgärden. Föreligger vissa former av sekretess kan underrättelsen skjutas upp och eventuellt inte lämnas.[110]

I dansk rätt lämnas underrättelse istället till den som råder över informationssystemet i fråga, är detta en misstänkt i ärendet ska underrättelsen inkludera uppgifter om vilket brott misstanken avser. Kommer anmälan vara till nackdel för efterforskningen i detta eller annat pågående mål om brott som kan ligga till grund för hemlig dataavläsning, får rätten besluta att underrättelse ska skjutas upp eller underlåtas. Detta kan även ske med hänsyn till uppgifter om polisens efterforskningsmetoder eller andra omständigheter som talar emot underrättelse. Innan sådant beslut ska förordnad advokat ha tillfälle att yttra sig.[111]

Det finns möjlighet för en enskild att begära prövning av ingreppets lagenlighet i båda rättsordningar, i svensk rätt utförs detta av SIN och i dansk rätt av *Datatilsynet*. SYN ska tills skillnad från *Datatilsynet* skyndsamt bli underrättad vid alla beslut om hemlig dataavläsning.[112]

6. Analys och slutsatser

Båda länder har välutvecklade system i relation till de krav som ställs i EKMR. Lagstiftningen är tillräckligt precis för att säkerställa lagstöd och möjliggör prövning av denna vid flera stadier. Nödvändigheten i ett demokratisk samhälle försäkras för sin del genom angiva avvägningar att ingreppet inte blir orimligt i relation till det behov som ska fyllas.

Av de två regleringarna är den danska klart mer begränsad, dataavläsning kan i dansk rätt inte avse onlinetjänster och är inte aktuell vid rent informationsbaserade förfaranden. Den avser inte

[109] Se kap 3.1.7, 4.1.6.
[110] Se kap 3.1.8.
[111] Se Kap 3.1.7.
[112] Se Kap 3.1.2, 4.1.6.

heller informationsinsamling med hjälp av verksamheter som hanterar informationstjänster. Allt detta anses istället utgöra andra tvångsmedel.

En annan viktig distinktion är att svensk dataavläsning kan tillämpas på informationssystem som förväntas kontaktas av den misstänkte, medan den danska endast rör informationssystem använda direkt av individen. För vissa uppgifter kan alltså i sverige en person som inte på något sätt är misstänkt drabbas av åtgärden. Även om kraven är höga innebär detta att de möjliga personkategorier som kan drabbas blir mer oklar, särskilt i kombination med straffvärdeventilen vilket försvårar översikten av relevanta brott. Den danska lagstiftningen har för sin del ett mer oklart krav på graden av misstanke.

Möjligheten för rätten att ålägga villkor för utövandet i svensk rätt innebär en betydligt striktare kontroll än möjligt för dansk dataavläsning. Man kan i svensk rätt på det hela se ett större fokus på typen av uppgift som får inhämtas enligt tillståndet. Den danska dataavläsningens begränsning gällande utövande innebär emellertid en hårdare reglering av själva utförandet, då tillståndet inte vore tillämpligt för en åtgärd som inte längre utgör dataavläsning.

Att det i den danska regleringen föreskrivs att det är den som råder över informationsystemet som har rätt att i efterhand informeras om åtgärden lär i dom flesta men inte alla fall innebära att den misstänkte informeras. Det kan dock innebära att varken den misstänkte eller andra drabbade av ingreppet över huvud taget informeras om att detta förekommit. Hade det inte varit för möjligheten att vända sig till en oavhängig myndighet hade detta varit klart oförenligt med EKMR.[113]

De mest centrala åtgärderna för att i danmark ytterligare säkra den personliga integriteten vore att tydligare koppla tillståndet till specifika uppgifter, och gärna även implementera en möjlighet för rätten att implementera sådana tillstånd som föreskrivs enligt svensk rätt. Utöver detta kan det konstateras att en enskilds möjlighet att få saken prövad i efterhand riskerar att bli begränsad om inte reglerna om underrättelse till enskild säkerställer att underrättelsen når de faktiskt drabbade.

För svensk del kan ifrågasättas om straffvärdeventilen är lämplig för en åtgärd som möjliggör sådan vidsträckt övervakning. Av rapporter från SIN framkommer dessutom att de uppställda kraven på villkor och angivelse av uppgiftstyp kan ha begränsad betydelse i praktiken, med hänsyn till att lagen är relativt nytillkommen är det svårt att säga om det finns behov att öka inblandningen av SIN i individuella ärenden, eller om detta är ett problem som härrör från att rätten ännu inte utvecklat lämpliga rutiner för att hantera denna typ av ärenden.

[113]Roman Zakharov v. Russia, 5 Okt 2006, p 288.

Käll- och litteraturförteckning

Svenskt offentligt tryck

Utredningsbetänkande och propositioner

Prop 2019/20:64 - Hemlig dataavläsning

Prop 1994/95:227 - Hemlig teleavlyssning och hemlig teleövervakning

Prop. 2013/14:237 - Hemliga tvångsmedel mot allvarliga brott

Bet 1984 nr. 1023 - Politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter

Övrigt offentligt tryck

Säkerhets- och integritetsskyddsnämnden. Dnr 92-2020 - "Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts"

Lagstiftning

Lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Danskt offentligt tryck

Utredningsbetänkande och propositioner

Betænkning 1407 (2001) om inkorporering af menneskerettighedskonventioner i dansk ret

Betænkning 1220 (1991) om Den europæiske Menneskerettighedskonvention og dansk ret

Lagförarbeten

2001/2 LSF 35 - Forslag til Lov om aendring af straffeloven, retsplejeloven, lov om…

Lagstiftning

Lov nr. 285 af 29. april 1992 om Den Europæiske Menneskerettighedskonvention

Litteratur

Bogdan, Michael, Concise introduction to comparative law, 1. uppl, Europa Law Publishing, Groningen, 2013.

Nääv, Maria & Zamboni, Mauro (red.), Juridisk metodlära, 2. uppl, Studentlitteratur, Lund, 2018.

Cameron, Iain, An introduction to the European Convention on Human Rights, 7. uppl, Iustus, Uppsala, (2014)

TfK2018.814 - Politiets hjemmel til »hacking« som led i en efterforskning

Schartum, Wiese, Dag, (red), Overvåking i en rettsstat, 1. Uppl, Fagbokforlaget Vigmostad & Bjorke AS, Bergen, 2010

Elektroniska källor

Danska polismyndigheten, "Politiets brug af personoplysninger" <https://politi.dk/hjemmesiden/politiets-brug-af-personoplysninger>, hämtad 2022-05-22

Stræde, Koch, Mathias, A/S Information, "Myndigheder mørklægger brug af terrorbeføjelse" publicerad 16. oktober 2015, <https://www.information.dk/indland/2015/10/myndigheder-moerklaegger-brug-terrorbefoejelse>, hämtad 2022-05-22

Rättsfallsförteckning

Danmark

UfR 1999.800 H

U 2012.2614 H - Politiets adgang til Facebook og Messenger-profiler med rette kode

Europadomstolen

Weber och Saravia v. Germany 29 juni 2006

Sunday Times v. UK 26 April 1979

Madsen v. Denmark, No. 58341/00

Wretlund v. Sweden, No. 46210/99

Silver and others v. UK 25 Mar 1983

Maestri v. Italy 8 Jul 2021

Roman Zakharov v. Russia 5 Okt 2006

Uzun v, Germany, 2 september 2010

Handyside v. UK, 7 December 1976

Leander v. Sweden, 8 Juli 1987

Al-Nashif v. Bulgaria Nr. 50963/9