

# Motion till riksdagen 2019/20:3451

av **Linda Westerlund Snecker m.fl. (V)**

## med anledning av prop. 2019/20:64 Hemlig dataavläsning

---

### 1 Förslag till riksdagsbeslut

Riksdagen avslår proposition 2019/20:64.

### 2 Inledning

Vänsterpartiet värnar demokratiska grundvärden som rättssäkerhet och skyddet för den personliga integriteten. Vi vill samtidigt inte försvåra de brottsbekämpande myndigheternas arbete med att utreda och beivra brott. Därför är vi även angelägna om att det finns ett regelverk som ger ett gott skydd för Sveriges och landets invånares säkerhet. Det måste kunna ställas höga krav på att terrorism och grov brottslighet bekämpas på ett effektivt sätt med hjälp av lagstiftning som bygger på de grundläggande rättsliga principerna i en rättsstat. I stället för att ny straffrättslig lagstiftning hastas igenom som under tidigare mandatperioder bör det förebyggande arbetet förbättras. Förutsättningarna för att tillämpa befintlig lagstiftning ska vara goda, och lagstiftningen måste förstärkas där behov finns så att brottsbekämpningen blir effektiv. Samtidigt måste de som har till uppgift att motverka, förhindra och lagföra grov brottslighet få rätt resurser för att fullgöra sin uppgift.

Varje samhälle måste ha möjlighet att använda tvångsmedel för att kunna utreda och beivra brott. Sådana tvångsmedel innebär definitionsmässigt en inskränkning i grundläggande fri- och rättigheter, rättigheter som i sin tur är grundläggande för demokratin i vårt samhälle. Därför måste såväl lagstiftningen som de medel som lagstiftningen tillhandahåller omgärdas av de strängaste restriktioner. De viktigaste restriktionerna har vi i våra egna grundlagar och Europakonventionen till skydd för de mänskliga rättigheterna och grundläggande friheterna. När det gäller frågor om utvidgning av det straffbara området uppkommer frågor om behov, effektivitet och proportionalitet. Dessa överväganden gör sig särskilt gällande när det är fråga om centrala skyddsintressen som Sveriges säkerhet och grundlagsskyddade rättigheter

såsom yttrande- och tryckfrihet och skyddet för den personliga integriteten. Det handlar således om att skydda den demokratiska rättsstaten i flera bemärkelser.

Ett av fundamenten i en rättsstat är att medborgarna åtnjuter ett effektivt skydd mot statens maktutövning; den enskilda medborgaren ska vara tryggad mot statens missbruk av rättsordningen. Det primära värde som rättssäkerheten ska skydda är den enskildes intresse av självbestämmande och möjlighet till livsplanering. Rättssäkerheten bör i princip inte kunna åsidosättas. För att kravet på rättssäkerhet ska upprätthållas krävs bl.a. att lagstiftningen är av god kvalitet, vad gäller både straffprocessuella regler och det materiella innehållet, samt att rättstillämpningen är god.

Den andra bärande principen i vår rättsordning är proportionalitetsprincipen. Principen innebär att de åtgärder som det allmänna använder sig av för att uppnå ett visst syfte inte får vara mer betungande eller mer långtgående än vad som kan anses nödvändigt för att uppnå det eftersträlvade syftet. Det ska således råda en balans mellan mål och medel samt vara sannolikt att det syftet uppnås genom vidtagna medel. Finns det möjlighet att välja mellan flera verk samma åtgärder ska det minst tyngande alternativet väljas.

Vi ser med stor oro på den utveckling som skett sedan början av 2000-talet och som i dag lett till att vi börjar närma oss ett övervakningssamhälle. Frågor om personlig integritet och mänskliga rättigheter får gång på gång stå tillbaka. Varje inskränkning har motiverats utifrån skenbart goda syften som effektivare brottsbekämpning och ett generellt ökat skydd för invånarna. Sammantaget framstår dock helheten av snart två decenniers skärpta lagar när det gäller t.ex. kamerabevakning, hemliga tvångsmedel, signalspaning, utlänningskontroll och åtgärder i syfte att hindra terrorism som illavarslande. Varje inskränkning som godtas tenderar att bereda väg för ännu fler och mer ingripande skärpningar. Argument i stil med att den som har ett rent samvete inte har något att frukta riskerar att bli urvattnade floskler ju fler inskränkningar av den personliga integriteten som accepteras. Konsekvenserna för samhällsklimatet och demokratin på lång sikt är svåra att överblicka.

Exempel från vår samtida omvärld visar dessutom tydligt att ökad övervakning av människor inte leder till minskad kriminalitet. Snarare riskerar vissa av de genomförda åtgärderna att invagga oss i en falsk trygghet. I stället är det andra åtgärder som krävs för att bekämpa kriminalitet och terrorism. Sverige har länge varit ett land med lägre kriminalitet än många andra länder. Det är inte för att vi har haft längre straff eller fler poliser på gatorna. Det har däremot en direkt koppling till att vi har haft ett starkt välfärdssamhälle med en välfungerande omsorg och skola samt tillgång till arbete och bostäder. Men det gäller inte längre överallt. En del förorter har drabbats av öppen narkotikahandel, våldsbrott och organiserad kriminalitet under många år utan att samhället har reagerat tillräckligt. Vänsterpartiet arbetar för ett samhälle där ingen har anledning att se kriminalitet som en lösning. Kriminaliteten utnyttjar och trycker ned människor, särskilt i arbetarområden. Vår lösning handlar om något större och mer effektivt än ökad övervakning. Vi vill ge alla barn en uppväxt som ger dem möjligheter i livet, från förskolan till skolan och det första jobbet. Det handlar om att ge alla människor i vårt samhälle verkliga möjligheter att välja andra livsvägar än en kriminell bana. För den som på allvar vill minska våldet och kriminaliteten är grunden att bygga ett rättvist samhälle. Men det krävs också en politik som är effektiv i att hjälpa dem som ligger i riskzonen för gängkriminalitet och återföra dem som begått brott till samhället. Polis, räddningstjänst, kollektivtrafik, vård och annan offentlig service ska finnas tillgänglig även på landsbygd och i förorter.

Vänsterpartiets inställning är och kommer att förbli att de mänskliga rättigheterna är odelbara. Dessvärre blir de mänskliga rättigheterna ofta ifrågasatta. Vi kommer inte att ge vika för dessa attacker, utan vårt mål är att ständigt försvara de friheter som är en förutsättning för att demokratin ska bestå och utvecklas. Vi är övertygade om att demokrati inte kan försvaras genom att begränsningar i de demokratiska rättigheterna införs. De rättigheter som generationer före oss slagits för att få till stånd måste i stället bevaras och utvecklas.

### 3 Regeringens antiterrorpaket

Regeringen har aviserat ett paket med antiterrorlagar som befinner sig i olika stadier i genomförandeprocessen. Terroristbrottsutredningen om skärpta straffskalor har nyligen presenterat ett betänkande, och nya regler om datalagring och om ökad tillgång till signalspaning har antagits av riksdagen. Vidare har riksdagen beslutat om borttagen tillståndsplikt för polisen för kameraövervakning, och ett betänkande om borttagen tillståndsplikt för kameraövervakning i kollektivtrafiken är under beredning i Regeringskansliet. Det pågår även ett arbete inom regeringen med att ta fram direktiv för att skärpa kraven för medborgarskap. Nyligen aviserade regeringen också en översyn av reglerna för husrannsakan i kriminella miljöer. Vid första anblicken kan dessa förslag, vart och ett för sig, verka helt rimliga och nödvändiga. Men enligt Vänsterpartiet måste samtliga redan genomförda, föreslagna och kommande åtgärder som syftar till att bekämpa terrorism, våldsbejakande extremism och annan grov kriminalitet bedömas som en helhet. Frågan vi ställer oss är om dessa åtgärder sammantaget är proportionella i förhållande till syftet och om de är effektiva för att uppnå målet.

### 4 Regeringens förslag

Regeringen föreslår i den aktuella propositionen att de brottsbekämpande myndigheterna får möjlighet att använda ett nytt hemligt tvångsmedel vid misstankar om allvarlig brottslighet. Det nya tvångsmedlet ska kallas hemlig dataavläsning. Regeringen bedömer att hemlig dataavläsning ska leda till bättre och effektivare möjligheter att ta del av information som i dagsläget inte är tillgänglig med de hemliga tvångsmedel som redan finns på grund av kryptering och anonymisering. I korthet syftar förslaget till att de brottsbekämpande myndigheterna ska kunna förhindra och utreda brott enligt de redan gällande lagarna om tvångsmedelsanvändning (regler i rättegångsbalken, inhämtningslagen, preventivlagen och lagen om särskild utlänningskontroll). Vidare kommer myndigheterna att via hemlig dataavläsning kunna samla in elektroniskt lagrade uppgifter som visar hur ett informationssystem används, något som inte är möjligt med dagens tvångsmedel. Hemlig dataavläsning ska kunna användas både under förundersökningar och utanför förundersökningar i underrättelseverksamhet och vid särskild utlänningskontroll. Möjligheten till hemlig dataavläsning ska enligt förslaget införas genom en särskild, tidsbegränsad lag.

## 5 Vänsterpartiets ställningstagande

Att det nya tvångsmedlet hemlig dataavläsning kommer att medföra ett stort ingrepp i rätten till privatliv och den personliga integriteten för enskilda är många av remissinstanserna till utredningen som ligger till grund för förslaget överens om (SOU 2017:89). Regeringen gör också bedömningen att hemlig dataavläsning ökar riskerna för kränkning av enskildas personliga integritet, jämfört med nuvarande användning av hemliga tvångsmedel (prop. 2019/20:64 s. 83). Vi gör dock, i motsats till regeringen, bedömningen att nyttan av hemlig dataavläsning inte är tillräckligt stor för att motivera dylika ingrepp i den personliga integriteten. Nedan redogör vi för några av de viktigaste skälen till detta.

### 5.1 Bristande effektivitet

Att komma åt krypterad kommunikation via olika former av appar är i dag tekniskt problematiskt för Polismyndigheten och Säkerhetspolisen. Dessvärre finns det mycket som tyder på att hemlig dataavläsning antagligen inte är den enkla lösning som många hoppas på. Enligt experter är det tveksamt om hemlig dataavläsning kommer att vara tillräckligt effektiv. Metoden är dyr och innebär i praktiken att staten kommer att installera ett virusliknande program, som placeras genom trojaner i människors telefoner och datorer. De brottsbekämpande myndigheterna kommer i korthet att identifiera och utnyttja det aktuella it-systemets sårbarheter, såsom tekniska brister och mänskliga svagheter (prop. 2019/20:64 s. 57). Trojanerna kan göra allt från att granska dokument, registrera position och se lösenord till att kolla av bilder och avlyssna chattar och samtal. Tanken är att hemlig dataavläsning ska ge en möjlighet att läsa av information innan den krypteras. Men vissa appar kommer sannolikt helt att omöjliggöra detta. Vidare är tillfället då det är möjligt att installera en trojan i ett kommunikationsmedel som en mobil eller dator nästintill obefintligt. Intrånget kan se ut på olika sätt, men en förutsättning är att det finns en sårbarhet i mobilen, vilket kan vara att luras att installera trojanen eller att få den misstänkt kriminella att installera en drivrutin. Polisen kan också använda sig av sårbarheter i själva it-systemet som inte är kända av tillverkaren, en teknik som tidigare såldes på svarta marknaden men som nu är öppet tillgänglig. Om myndigheterna kommer att använda sig av denna metod är oklart, och lika oklart är det om dessa sårbarheter sedan kommer att kommuniceras med tillverkarna av it-systemen så att företagen har möjlighet att åtgärda sårbarheten. En liknande händelse skedde i USA då NSA samlat på sig en verktygslåda med sårbarheter som de råkade läcka av misstag, vilket utnyttjades av kriminella och drabbade storföretag över hela världen. Då mobiltelefonen eller datorn är upplåst och informationen finns i klartext är hanteringen enkel när trojanen väl är placerad, men möjligheten att komma åt information i olika appar eller mejl som lagras på servrar eller i ett molnbaserat system är högst begränsad. När trojanen väl är installerad finns en möjlighet att avläsa information i realtid. Men att avläsa krypterad information kommer även fortsatt att vara en stor utmaning eftersom krypteringen sker via nycklar. Regeringen har dock inte aviserat att staten ska framställa en huvudnyckel för kryptering, en utveckling som skulle vara mycket oroande eftersom så pass mycket av privatpersoners kommunikation i dag sker krypterat. Vidare byter kriminella nätverk självfallet mobiltelefoner ofta, installerar mjukvara för kryptering eller använder olika former av mobiltelefoner med olika former av förinställda krypteringsverktyg, allt för att kunna kommunicera utan myndigheternas vetskap. Det

finns inget som tyder på att de kriminella nätverken kommer att sluta anpassa sina kommunikationsmetoder efter rådande lagstiftning. Även Sveriges Advokatsamfund lyfter i sitt remissvar risken för att det i kriminella miljöer snabbt skulle utvecklas tekniker som förhindrar informationshämtning genom hemlig dataavläsning. Enligt vår mening är det av den anledningen tveksamt hur länge hemlig dataavläsning kommer att vara en effektiv metod.

Regeringen skriver i sitt förslag att det kommer att krävas ett omfattande förberedelsearbete och en förmåga att möta tekniska svårigheter vid verkställighet av hemlig dataavläsning. Mot den bakgrunden gör regeringen bedömningen att hemlig dataavläsning endast kommer att kunna användas i ett begränsat antal fall och att detta kommer att påverka effektiviteten negativt (prop. 2019/20:64 s. 81).

## 5.2 Bristande rättssäkerhetsgarantier vid verkställighet

Hemlig dataavläsning är en tekniskt komplicerad metod som kommer att vara mycket resurskrävande för Polismyndigheten och Säkerhetspolisen. Redan i dag har myndigheterna en eftersatt it-verksamhet med oklar kapacitetsbrist för att hantera komplicerade hemliga tvångsmedel. På frågan hur de brottsförebyggande myndigheternas handlingsutrymme, förmåga och möjlighet ser ut för att komma åt kommunikation med hemlig dataavläsning innan den krypteras har ansvarig minister svarat att han har fullt förtroende för att de brottsbekämpande myndigheterna har förmågan att tillämpa lagstiftningen (skriftlig fråga 2019/20:470). Regeringen föreslår i propositionen att själva verkställighetstekniken *inte* ska ingå i domstolsprövningen vid tillståndsgivning för hemlig dataavläsning. Detta är en brist, vilket även påtalas av Säkerhets- och integritetsskyddsnämnden (SIN) i dess remissvar på utredningen. SIN menar att de verkställande myndigheterna genom förslaget får stor frihet att själva avgöra vilka tekniska hjälpmedel som ska användas vid verkställigheten. Detta gör att det är oklart hur rättssäkerheten för enskilda ska garanteras. SIN anser att domstolen måste ha möjlighet att ange villkor för att enskildas personliga integritet inte ska kränkas i onödan. Därför bör verkställighetstekniken ingå i domstolsprövningen. Även Datainspektionen lyfter i sitt remissvar att domstolen måste veta vilka tekniska åtgärder som ska genomföras för att kunna göra en fullständig nödvändighets- och proportionalitetsbedömning. Att SIN föreslås utöva tillsyn över de brottsbekämpande myndigheternas användning av hemlig dataavläsning enligt samma regler som gäller för användandet av hemliga tvångsmedel i dag räcker enligt vår mening inte för att garantera rättssäkerheten för enskilda vid verkställighet.

## 5.3 Bristande proportionalitet och rättssäkerhet

Ett stort problem med förslaget är att regeringen gör bedömningen att utgångspunkten för hemlig dataavläsning bör vara de krav som gäller för det "bakomliggande" hemliga tvångsmedlet enligt redan gällande lag. Det hänger ihop med att regeringen huvudsakligen ser hemlig dataavläsning som en ny metod för att inhämta information som redan får hämtas in med befintliga tvångsmedel, och inte som ett helt nytt tvångsmedel (se t.ex. prop. 2019/20:64 s. 130).

Vi menar att det antagande regeringen gör är en av de verkligt stora bristerna med förslaget. I stället för att prova förutsättningarna att använda hemlig dataavläsning för

varje enskilt brott för sig utifrån rättsliga principer om proportionalitet, ändamålsenlighet och effektivitet gör regeringen i stället bedömningen att hemlig dataavläsning i huvudsak bara är en ny metod för att komma åt information som det redan är tillåtet att samla in med gällande tvångsmedelslagstiftning.

Vi anser att hemlig dataavläsning är så pass integritetskränkande att detta synsätt inte låter sig förenas med gällande rättsliga principer. Regeringen konstaterar nu bara att vissa åtgärder är tillåtna när det gäller vissa brott och att hemlig dataavläsning därför också ska tillåtas avseende samma brott. Man baserar i korthet ett helt nytt tvångsmedel på redan befintliga tvångsmedel utan att bedöma vare sig proportionalitet eller behov. Datainspektionen anför liknande kritik i sitt remissvar och menar att förslaget omfattar möjlighet till tvångsmedel för brott som inte är tillräckligt allvarliga och anser att utredningen borde ha provat behovet och proportionaliteten för vart och ett av de brott som kan aktualisera hemlig dataavläsning. Enligt Datainspektionen bör enbart de allra allvarligaste brotten kunna leda till att hemlig dataavläsning får användas.

Sveriges Advokatsamfund avstyrker förslaget med hänvisning till att det bl.a. inte uppfyller kravet på proportionalitet. Enligt Sveriges Advokatsamfund måste hemlig dataavläsning exklusivt förbehållas Säkerhetspolisen vid misstanke om mycket allvarlig brottslighet som utgör hot mot rikets säkerhet och som har ett straffminimum eller förväntat straffvärde på fängelse i fyra år eller mer för att förslaget över huvud taget ska kunna uppfylla kraven på proportionalitet. Detta skulle dock kräva ytterligare analys och utredning.

Vänsterpartiet är även sedan tidigare kritiskt till utformningen av vissa av de nämnda tvångsmedelsbestämmelserna. Vi anser att flera av dessa är både otydliga och för långtgående. Lagen om särskild utlänningskontroll (LSU) är t.ex. extremt rättsosäker för den enskilda, och insyn i myndigheternas tillämpning av den saknas i praktiken. Regeringens förslag om att bestraffa samröre med en terroristorganisation (genom en ändring i rekryteringslagen som förväntas antas av riksdagen i närtid) brister enligt vår mening på en rad punkter (se mot. 2019/20:3427). Därför är det extra bekymmersamt att regeringen inte har gjort någon bedömning av proportionalitet och behov av hemlig dataavläsning för varje brott för sig utan har anpassat det nya tvångsmedlet till redan befintliga tvångsmedel. På så sätt byggs rådande otydlighet och rättsosäkerhet i befintlig lagstiftning in i den nya lagen om hemlig dataavläsning.

Ett ytterligare problem är att regeringens bedömning, att hemlig dataavläsning i princip bara är en ny metod för att komma åt information som Polismyndigheten och Säkerhetspolisen redan har rätt att ta del av med befintliga hemliga tvångsmedel, får till följd att metoden i korthet kommer att tillämpas vid brott med två års fängelse som minimum i straffskalan. Hemlig dataavläsning skulle, enligt regeringen, även kunna aktualiseras vid misstanke om ett brott som inte har två års fängelse som minimistraff men som i det enskilda fallet bedöms ha ett straffvärde på mer än fängelse i två år (på grund av den s.k. straffvärdesventilen vid hemlig avlyssning av elektronisk kommunikation, 27 kap. 18 § 2 RB, se prop. 2019/20:64 s. 116). Enligt vår mening är det totalt orimligt ur proportionalitetssynpunkt. Såväl Norge som Danmark och Finland har lagar om hemlig dataavläsning där tvångsmedlet i huvudsak endast får användas vid brott med hårdare straff än vad som föreslås bli fallet i Sverige. I korthet handlar det om grova brott som landsförräderi, terroristbrott och brott mot rikets säkerhet. I Danmark krävs att det handlar om ett brott som kan bestraffas med fängelse i sex år eller mer eller att det rör sig om ett särskilt utpekade brott, såsom landsförräderi eller terroristbrott. I Norge gäller som utgångspunkt att maxstraffet ska vara fängelse i tio år eller mer eller

att det handlar om vissa angivna brott som brott mot rikets säkerhet, narkotikabrottslighet och människohandel. I Finland ingår även bl.a. grov spridning av barnpornografisk bild i brottskatalogen som kan aktualisera det tvångsmedel som motsvarar hemlig dataavläsning. I Danmark kan dataavläsning inte användas i underrättelseverksamhet, vilket däremot är möjligt i Norge (prop. 2019/20:64 s. 59–60).

Enligt Vänsterpartiets mening skulle det möjligen vara rimligt att använda hemlig dataavläsning vid vissa av de allra grävsta brotten, så som i våra grannländer och som Sveriges Advokatsamfund och Datainspektionen lyfter i sina remissvar. Men eftersom varken utredningen eller regeringen har gjort någon prövning av behovet vid varje brott för sig kan vi inte avgöra om så är fallet. Att den föreslagna lagen är tidsbegränsad är förvisso positivt, och vi förväntar oss en noggrann utredning av nyttan, behovet och proportionaliteten i samband med den fortsatta hanteringen. Dock har de tidsbegränsade lagar om hemliga tvångsmedel som riksdagen tidigare har beslutat om förlängts i olika omgångar för att sedan permanentas utan någon större debatt. Det är anmärkningsvärt att regeringen presenterar en proposition i slutet av december 2019 som ska träda i kraft den 1 mars 2020.

Vänsterpartiet kan sammantaget inte stå bakom regeringens förslag.

Riksdagen bör avslå regeringens proposition 2019/20:64. Detta bör riksdagen besluta.

*Linda Westerlund Snecker (V)*

*Christina Höj Larsen (V)*

*Jon Thorbjörnson (V)*

*Mia Sydow Mölleby (V)*

*Jessica Wetterling (V)*