RP 277/2010 rd

Regeringens proposition till riksdagen med förslag till lag om ändring av 28 kap. 7 § i strafflagen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att strafflagen ändras så att såsom olovligt brukande inte ska anses användning av via en internetanslutning ett oskyddat trådlöst datanät. Den föreslagna lagen innebär att olovlig användning av ett oskyddat WLAN (wireless local area network) och motsvarande typ av trådlöst datanät samt en internetanslutning via det uttryckligen avkriminaliseras.

Lagen avses träda i kraft så snart som möjligt.

295363

INNEHÅLLSFÖRTECKNING

ALLMÄN MOTIVERING

1 Inledning

Användning av ett trådlöst lokalnät (wireless local area network), nedan WLAN, och motsvarande trådlösa datanät skiljer sig från användning av normal lös egendom. Vid tillkomsten av strafflagens (39/1989) gällande 28 kap. 7—9 § om olovligt brukande fanns det inte sådana nätverk som det här är fråga om. I rättspraxis har det ansetts att användning av oskyddade WLAN och internetanslutningar utan ägarens tillstånd kan uppfylla rekvisitet för olovligt brukande.

I denna proposition bedöms om det är ändamålsenligt att anse att en sådan gärning är straffbar. Slutsatsen är att det inte finns tillräckliga motiveringar för en kriminalisering. Därför föreslås att bestämmelsen om olovligt brukande ändras så att brottet avkriminaliseras.

2 Nuläge

2.1 WLAN och andra trådlösa nätverk

WLAN är en allmänt använd metod för trådlös uppkoppling till internet. WLAN är ett trådlöst lokalt nät som möjliggör kabellös anslutning av olika typer av dataterminaler. WLAN-näten möjliggör inte nödvändigtvis internetanslutning, men för en begränsad grupp användare kan sådana nätverk också fungera internt, dvs. som intranet.

Ett WLAN har en basstation vars räckvidd i flervåningshus vanligen sträcker sig åtminstone till grannlokalerna. Mot ett sådant nät kan man koppla upp sig exempelvis med en bärbar dator, en mobiltelefon, en spelkonsol eller någon annan dataterminal med WLAN-adapter. En uppkoppling till internet via någon annans WLAN innebär i praktiken att man använder dennes basstation och modem samt internetlicens. Användningen av nätet innebär inte uppkoppling till WLAN-ägarens dator.

Ägaren kan skydda sitt WLAN mot utomstående användning med ett lösenord. Skyddet förutsätter i allmänhet att ägaren läser de instruktioner som följer med basstationen eller får handledning, men det är inte fråga om en åtgärd som kräver specialsakkunskap. En WLAN-basstation kan också vara skyddad med lösenord redan i samband med fabriksinstallationerna.

En trådlös nätanslutning kan också hållas oskyddad och öppen, vilket innebär att vem som helst kan använda den. En oskyddad nätanslutning gör det möjligt för andra nätanvändare att se vilka andra terminaler som använder basstationen. Den som har skaffat ett trådlöst nät kan avsiktligt eller oavsiktligt lämna det oskyddat. Företag kan gratis erbjuda sina kunder öppna WLAN (t.ex. kaféer och flygplatser) och på offentliga platser där folk vistas (t.ex. kommunala rekreationsområden). Privatpersoner kan lämna sitt WLAN oskyddat t.ex. för att dela sin nätanslutning med sina grannar. Med specialåtgärder kan en basstation ställas in så att utomstående inte får tillgång till nätet. Dataöverföringskapaciteten kan med specialåtgärder avgränsas så att den endast delvis kan användas av utomstående.

Användning av ett oskyddat WLAN utan uttryckligt tillstånd kan medföra olägenhet för nätägaren närmast genom att så stora mängder data överförs att nätets fria kapacitet allvarligt reduceras. Detta innebär att ägarens nätanslutning blir långsammare. Användning av mindre krävande internetfunktioner, t.ex. läsning av e-post, bläddring i nyhetsmaterial med bilder och text, videotittande, nätköp eller radiolyssning, belastar i allmänhet inte att ett hushålls nätanslutning så att den blir märkbart långsammare. Tyngre funktioner, såsom nedladdning av filmer eller samtidig användning av flera sådana funktioner som nämns ovan, kan redan om en person använder dem samtidigt göra ägarens nätanslutning märkbart långsammare. Om flera datorer är uppkopplade samtidigt är det också mera sannolikt att nätanslutningen blir långsammare.

Olovlig användning av ett WLAN kan indirekt medföra olägenheter för basstationens

ägare om nätet används för att begå brott, t.ex. dataintrång, spridning av skadliga program eller nerladdning av olagligt material via internet. Nätägaren kan då själv bli brottsmisstänkt. Ägaren kan emellertid enligt lag inte bli straffrättsligt ansvarig för brott som begåtts av en annan person. Obefogade misstankar kan undanröjas t.ex. med loggdata som lagrats i WLAN-routern eller med data från den misstänktes hårddisk.

Också mobiltelefonnät används i stor utsträckning för trådlös internetförbindelse. En avgörande skillnad mellan ett mobiltelefonnät och ett WLAN är att användning av mobiltelefonnätet innebär uppkoppling till en viss anslutning och att det sålunda inte är oskyddat och direkt står till allmänt förfogande. Prissättningen för användningen av mobiltelefonnät grundar sig ofta på mängden överförd data. Det går dock att skapa kontakt till ett mobiltelefonnät via ett WLAN-nät t.ex. med användning av vissa mobiltelefonmodeller. Det är tekniskt möjligt att lämna en sådan WLAN-kontakt oskyddad, varvid det också finns öppen tillgång till mobiltelefonnätet via WLAN. Sådana innehavare av anslutningar som inte skyddar sin kontakt och vars fakturering grundar sig på mängden överförd data kan därför orsakas överraskande ekonomisk skada. Den effektivaste metoden att skydda sig mot en sådan risk är att hålla sitt nät skyddat.

WiMAX (Worldwide Interoperability for Microwave Access) bygger på en modernare teknik än WLAN och används för trådlös dataöverföring med internetaccess. WiMAX ger en geografisk täckning på flera kilometer och erbjuder högre hastigheter. Eftersom ett WiMAX-nät inte behöver skyddas och sålunda kan erbjudas en ospecificerad användargrupp, kan det med avseende på olovlig användning jämställas med ett WLAN. I Finland är WiMAX inte ännu allmänt förekommande men kommer sannolikt att bli vanligare under de närmaste åren.

2.2 Lagstiftning och praxis

Finlands lagstiftning innehåller inga särskilda straffbestämmelser om olovlig användning av oskyddade trådlösa datanät. Enligt strafflagens 28 kap. 7 § är det straffbart att olovligen bruka någon annans lösa egendom eller fasta maskin eller anordning. Försök är straffbart. Straffskalan är böter eller fängelse i högst ett år. I kapitlets 8 § föreskrivs om grovt olovligt brukande. Enligt 9 § är det fråga om lindrigt olovligt brukande om det olovliga brukandet bedömt som en helhet är ringa, med beaktande av att brottet inte är ägnat att orsaka skada eller men som är av betydelse, eller med hänsyn till andra omständigheter vid brottet.

Bestämmelserna om olovligt brukande tillkom ursprungligen med tanke på fall där gärningsmannen fortfarande hade den olovligt brukade egendomen i sin besittning. Enligt sin ordalydelse gällde bestämmelserna t.ex. inte situationer där den olovligt brukade egendomen inte i något skede fråntogs en annan. Bestämmelserna ändrades i början av 1990-talet så att det med tanke på tillämpningen saknar betydelse om den egendom som använts olovligen är i gärningsmannens eller någon annans besittning vid den tidpunkt då den tas i bruk. Ändringen ansågs utsträcka kriminaliseringen exempelvis till s.k. hackers som via telefonlinjer tränger in i datasystem och använder dem olovligen, dvs. ”stjäl datortid” (RP 66/1988 rd).

Åbo hovrätt fastställde 31.3.2009 Salo tingsrätts dom 31.3.2008 där A ansågs ha gjort sig skyldig till lindrigt olovligt brukande då han uppsåtligen använt B:s oskyddade WLAN-förbindelse utan dennes tillstånd. I det material som justitieministeriet haft till sitt förfogande är detta det enda fallet där en person med stöd av strafflagens 28 kap. 7-9 § har dömts för olovlig användning av ett WLAN. Frågan om gärningens straffbarhet prövades inte av högsta domstolen.

I strafflagens 38 kap. föreskrivs om informations- och kommunikationsbrott. Av kapitlets bestämmelser kan närmast 8 och 8 a § om dataintrång tillämpas på WLAN-nät. En förutsättning för tillämpning också av dessa bestämmelser är emellertid att gärningsmannen gör bruk av en användaridentifikation som han inte har rätt till eller annars bryter ett säkerhetsarrangemang. Bestämmelserna kan sålunda inte tillämpas på användning av oskyddade WLAN-nät.

2.3 Lagstiftningen i vissa EU-länder

Sverige

Sverige har inga särskilda bestämmelser och inte heller någon rättspraxis om olovlig användning av oskyddade WLAN-nät. Sådan olovlig användning anses inte vara straffbar, åtminstone inte om den inte innebär att ägarens möjligheter att själv använda nätet begränsas eller ändras. Olovlig användning av ett skyddat WLAN genom att bryta säkerhetsarrangemang anses som ett brott.

Estland, Ungern och Litauen

I dessa länder är det straffbart göra intrång i WLAN-nät och använda dem olovligen. Det finns ingen särskild lag eller rättspraxis om användning av oskyddade WLAN-nät, men sådan användning anses inte vara straffbar.

Tyskland

I Tyskland finns det inga särskilda bestämmelser om olovlig användning av oskyddade WLAN-nät. I lägre instans har det ansetts att användning av ett oskyddat WLAN kunde jämställas med olovligt uppsnappande av kommunikation, som är straffbart enligt tysk lag. Dessutom ansågs gärningen i det aktuella fallet uppfylla rekvisitet för olovligt inhämtande av personuppgifter. Avgörandet har emellertid kritiserats och betraktats som ett enskilt fall. Enligt kritiken kan användning av ett WLAN inte betraktas som telekommunikation och den information som den olovliga användaren fick om nätets ägare kunde inte betraktas som personuppgifter.

2.4 Bedömning av nuläget

Inledning

Straffbestämmelserna i strafflagens 28 kap. om olovligt brukande trädde i kraft 1990 och tillkom i ett skede då konsumenterna inte allmänt använde internet och då det inte fanns trådlösa nät av typen WLAN. Även om det i lagens förarbeten konstateras att kriminaliseringen omfattar också olovlig användning av datasystem (RP 66/1988 rd) var det då inte möjligt att beakta sådana situationer som uppkommer vid användning av trådlösa nät av typen WLAN, som avviker från användning av datasystem. Lagstiftaren hade sålunda inte tillfälle att bedöma frågan om tillämpning av straffbestämmelserna på sådana situationer. Det kan sålunda vara i någon mån tolkningsbart om straffbestämmelserna om olovligt brukande är tillämpliga på sådana situationer. Trots att en domstol och hovrätten som högsta instans endast i ett fall har ansett det vara straffbart att olovligen använda ett WLAN, inverkar detta fall sannolikt på rättspraxis och myndigheternas agerande. Den uppmärksamhet som fallet i fråga har rönt i massmedierna är också en bidragande orsak till att sådan olovlig användning generellt kan anses vara straffbar. Av de orsaker som nämns ovan är det skäl att göra en särskild bedömning av grunderna för straffbarheten i sådana fall.

Användning av ett WLAN utan ägarens tillstånd skiljer sig från sådant sedvanligt olovligt brukande som innebär att ägaren medan det olovliga brukandet pågår inte själv över huvud taget kan använda sin egendom (t.ex. olovligt brukande av en cykel). Olovligt brukande som sker via ett WLAN är inte riktat mot privatlivet eller hemfridssfären och kan sålunda inte heller jämställas t.ex. med en situation när någon olovligen går in i en privatbostad vars dörr är olåst. Användning av en annans WLAN kan å andra sidan i princip anses skilja sig också från en sådan icke-kriminaliserad gärning som innebär att användning av ett föremål som tillhör en annan inte medför olägenhet för ägaren. Till denna kategori av gärningar hör t.ex. läsning en annan persons tidning över dennes axel eller läsning av en bok i skenet av grannens belysning. Olovlig användning av ett WLAN är inte nödvändigtvis helt omärkbar för nätets laglige ägare eftersom användningen medan den pågår upptar en del av nätets dataöverföringskapacitet (”band”). Överföringshastigheten sjunker dock endast vid överföring av stora datamängder. Om nätet används på andra tider än när ägaren själv använder det

medför användningen inte över huvud taget någon olägenhet för ägaren.

Grundlagsutskottet och lagutskottet har ställt upp allmänna förutsättningar för begränsad tillämpning av straffrätten (GrUB 25/1994 rd, GrUU 23/1997 rd, GrUU 17/2006 rd, s. 2/II, GrUU 18/2007 rd, s. 5/I, LaUU 9/2004 rd, LaUB 8/2004 rd, LaUB 15/2005 rd och LaUB 2/2006 rd). För strafflagstiftning måste det finnas en godtagbar grund och ett vägande samhälleligt behov. Vidare måste strafflagstiftningen beakta redan existerande regleringar och alternativa metoder, kriminaliseringen måste vara förebyggande samt, med beaktande av legalitetsprincipen, tillräckligt exakt och noga avgränsad. Strafflagstiftning är det alternativ som kommer i sista hand (ultima ratio) efter andra samhälleliga metoder. De fördelar som kan uppnås genom en kriminalisering måste också alltid vara större än nackdelarna. Dessa s.k. kriminaliseringsgrunder ska tillämpas också när det är fråga om att överväga avkriminalisering av en straffbar gärning.

Godtagbar grund

Strafflagens bestämmelser om olovligt brukande tryggar egendomsskyddet som enligt grundlagens (731/1999) 15 § är en grundläggande rättighet. Skyddsobjektet är ägarens principiella rätt att fritt bestämma om användningen av sin egendom. En kriminalisering av användningen av WLAN-nät skulle framför allt skydda egendom i sådana fall då ägaren inte vill upplåta sitt nät för allmänt bruk. I detta avseende finns det en godtagbar grund för kriminalisering. Friheten att använda sin egendom kan å andra sida inbegripa möjligheten att upplåta ett WLAN för allmänt bruk. En kriminalisering av användning av oskyddade WLAN-nät skulle i många avseenden försvåra frivillig upplåtelse av WLAN-nät för andras användning. I denna bemärkelse innebär en kriminalisering också en begränsning av egendomsskyddet.

Alternativa metoder

Eftersom strafflagstiftning alltid ska vara den metod som kommer i sista hand är det skäl att bedöma effekten av alternativa sätt att förhindra olovlig användning av WLAN-nät. Det enklaste sättet att förhindra olovlig användning av ett WLAN är att skydda det med ett lösenord. Det är obetydligt besvärligare att använda ett skyddat nät än ett oskyddat. I de mest använda operativsystemen behöver man inte ens skriva lösenordet varje gång man loggar in.

De som använder WLAN har sannolikt lämnat dem oskyddade antingen som ett medvetet val, för att låta t.ex. sina grannar använda nätet, eller av oförstånd. Detta beror antagligen på att WLAN-teknologin är relativt ny och på att man inte insett riskerna med att lämna sitt nät oskyddat. Man kan sålunda utgå ifrån att medvetenheten ökar, i synnerhet med beaktande av att alternativet att skydda nätet med ett lösenord är en åtgärd som varken kräver särskild sakkunskap eller är svår att lära sig för en person som kan använda normala datatekniska applikationer.

Att skydda sitt nät med ett lösenord är ett säkert sätt att hindra att nätet olovligen används av utomstående som inte lyckas bryta skyddet. Den som bryter skyddet gör sig eventuellt skyldig till dataintrång enligt strafflagens 38 kap. 8—8 a §. Om basstationens ägare åsamkas skada genom olovlig användning av nätet kan han också i vissa fall få rätt till skadestånd. Eftersom det sålunda är effektivt och relativt enkelt att skydda WLAN-nät förefaller det inte behövas någon kriminalisering för att förhindra användning av oskyddade nät.

Avvägning mellan fördelar och nackdelar

En av de största fördelarna med en kriminalisering kan i allmänhet anses vara dess allmänpreventiva verkan. Hot om påföljder avhåller människor från att begå brott. Den allmänpreventiva effekten korrelerar emellertid med risken för att bli avslöjad. Olovlig användning av ett WLAN kan normalt inte upptäckas av basstationens ägare utan att denne vidtar specialåtgärder, om inte data överförs i sådana mängder att nätet blir märkbart långsammare. På grund av gärningens natur kan risken för avslöjande knappast ökas genom effektivare övervakning från polisens sida. Av dessa orsaker är risken för avslöjande liten.

Dessutom är en kriminaliserings allmänpreventiva effekt mindre när det är fråga om personer som trots kriminaliseringen anser att gärningen är moraliskt godtagbar. En i USA gjord enkät visar att 40—50 % av medborgarna anser att det är moraliskt godtagbart att använda ett oskyddat WLAN utan ägarens tillstånd. Om en gärning allmänt anses vara moraliskt godtagbar och en kriminalisering av den anledningen uppfattas som orättvis, kan konsekvensen vara att respekten för det straffrättsliga systemet minskar bland allmänheten.

Ett brott medför också alltid sedvanliga verkställighetskostnader (övervakning, undersökning, rättskipning och straffverkställighet).

En kriminalisering av användning av oskyddade WLAN-nät kan dessutom medföra särskilda problem. På senare tid har det blivit vanligt att oskyddade WLAN-nät gratis tillhandahålls allmänheten på allmänna platser, t.ex. parker och flygplatser – s.k. ”access points” eller ”hot spots”. På sådana platser är man inte alltid klart medveten om att det finns ett gratis WLAN för allmänt bruk. Den som loggar in med en dator, mobiltelefon eller någon annan anordning får inte alltid annan information nätet än dess namn på det lokala språket och en uppgift om huruvida nätet är skyddat. En användare som inte är helt säker på om det är tillåtet att använda ett oskyddat nät tar risken att begå ett brott. Detta försvårar användningen av gratis WLAN-nät. En underlättande omständighet är att det kan ges information om huruvida det är tillåtet att använda nätet, men inte heller detta eliminerar alla från användarens synpunkt svåra tolkningssituationer.

Ett särskilt problem när det gäller straffbarheten är också att en dator enligt vissa operativsystems defaultinställningar automatiskt och utan användarens bekräftelse kan logga in på närmaste WLAN, vilken lätt kan undgå användaren.

Hur systemet fungerar i praktiken

Övervakningen av eventuell olovlig användning av ett oskyddat WLAN är i praktiken beroende av basstationens ägares aktivitet. Trots att det inte finns något tekniskt hinder för att operativsystemet alltid underrättar ägaren då dennes nät används, krävs det inom ramen för dagens teknologi särskild sakkunskap för att ta reda på om någon olovligen har använt ett nät. Trots att antalet WLAN-nät ökat kraftigt under de senaste åren, har veterligen endast en dom gällt olovligt brukande (det fall som nämns ovan). I praktiken skulle sålunda en kriminalisering av olovlig användning av oskyddade WLAN-nät få endast en marginell betydelse.

Slutsats

En kriminalisering av användning av oskyddade trådlösa nät av typen WLAN leder till många problem. Fördelarna med kriminaliseringen minskas av kostnaderna och i synnerhet nackdelarna, framför allt av den omständigheten att användaren inte alltid på förhand kan veta om ägaren avsett att nätet ska stå till fritt förfogande eller inte. Också den nästan obefintliga risken att bli avslöjad och den obetydliga allmänpreventiva effekten minskar åtminstone i nuläget nyttan av kriminaliseringen. En omständighet som talar emot ändamålsenligheten av straffbestämmelsen är framför allt möjligheten att enkelt skydda sin nätförbindelse mot olovlig användning. Av de skäl som nämns ovan är det inte motiverat att anse att det i enlighet med strafflagens 28 kap. 7—9 § ska vara straffbart att använda ett WLAN utan ägarens tillstånd, åtminstone inte i nuvarande utsträckning.

3 Målsättning och de viktigaste förslagen

3.1 Målsättning

Syftet med propositionen är att rätta till de ovan nämnda problem som beror på att användning av oskyddade trådlösa datanät är kriminaliserad som olovligt brukande.

3.2 Alternativ

Alternativ 1

Användning av oskyddade nät av typen WLAN ska fortsättningsvis vara straffbart

som olovligt brukande, utom i det fall att användaren har grundad anledning att anta att nätet står till fritt förfogande. Enligt detta alternativ kriminaliseras i första hand sådan olovlig användning av nät som inte uttryckligen står till fritt förfogande (exempelvis WLAN-nät i privatbostäder eller för kafékunder). Däremot ska det inte vara straffbart att använda nät som fungerar på allmänna platser, t.ex. i parker, och som t.ex. enligt en skylt eller med ledning av nätets namn med fog kan antas vara avsedda för allmänt bruk.

Detta alternativ skulle innebära en precisering av strafflagens nuvarande 28 kap. 7—9 § varav man kan få den uppfattningen att det enligt lag är förbjudet att utan uttryckligt tillstånd använda också oskyddade WLAN-nät som är avsedda för allmänt bruk. Om användaren har grundad anledning att anta att ett nät trots avsaknaden av ett uttryckligt tillstånd är avsett för allmänt bruk, är användningen inte ”olovlig”. Alternativet skyddar således en ägare som inte vill upplåta sitt nät för allmänt bruk men tryggar samtidigt möjligheten att ställa trådlösa nät till fritt förfogande.

Detta alternativ skulle dock innebära att flera av de ovan nämnda problemen kvarstår (kostnader, låg risk för avslöjande, tolkningsproblem i praktiska situationer och datorer som automatiskt loggar in på nätet). Det skulle alltid vara användaren som i praktiken ansvarar för en korrekt tolkning – dvs. om det är tillåtet att använda ett visst WLAN-nät eller inte.

Alternativ 2

Det skulle inte vara straffbart att använda oskyddade nät av typen WLAN, utom i sådana fall då användningen medför betydande olägenhet för den som äger basstationen. Som en sådan olägenhet skulle åtminstone betraktas att datakommunikationen blir klart långsammare. Bestämmelsen kunde utformas så att det räcker med en s.k. abstrakt risk för olägenhet (”är ägnad att”), vilket innebär att det inte krävs visshet om att basstationens ägare använder nätet samtidigt. En fördel med detta alternativ är att lagen skulle förbjuda endast sådan användning av nätet som stör ägaren. Ägaren kunde sålunda låta nätet vara öppet och ändå få rättsligt skydd mot störande användare.

Detta alternativ är emellertid förenat med problem. För det första är det omöjligt att ge en exakt definition på begreppet ”betydande olägenhet” eller motsvarande kriterium. Detta kunde leda till att eventuella användare för säkerhets skull låter bli att använda ett nät som avsiktligt lämnats öppet, vilket skulle strida mot syftet med bestämmelsen.

Dessutom skulle redan gärningsmannens uppsåt enligt definitionen i strafflagens 3 kap. 6 § förutsätta att denne med tillräcklig noggrannhet känner till nätförbindelsens kapacitet och den datamängd som överförs samt hur dessa faktorer inverkar på nätets snabbhet. I mera uppenbara fall, exempelvis vid överföring av stora mängder data, kan uppsåtskravet lättare bli uppfyllt. I en situation där överföringen avser en mindre mängd data kan det vara svårare att påvisa att gärningsmannen ansett det vara ytterst sannolikt att överföringen varit ägnad att göra basstationsägarens egen internetförbindelse långsammare.

Alternativ 3

Användning av oskyddade nät av typen WLAN avkriminaliseras helt. Det skulle sålunda inte heller vara straffbart att använda ett nät på ett sätt som gör basstationsägarens egen nätförbindelse långsammare. Ägaren kunde skydda sitt nät så att det kan användas endast av ägaren själv eller en viss persongrupp. Alternativet är klart och enkelt.

Också enligt detta alternativ skulle det fortfarande vara straffbart att via ett WLAN olovligen göra intrång i en basstationsägares dator eller att begå andra brott.

3.3 De viktigaste förslagen

I propositionen föreslås en sådan ändring i strafflagens 28 kap. 7 § om olovligt brukande att användning av internetförbindelser via oskyddade nät av typen WLAN uttryckligen avkriminaliseras. Det föreslås sålunda att det till paragrafen fogas ett nytt 3 mom. enligt vilket användning av en internetanslutning via ett oskyddat trådlöst datanät inte ska an-

ses som olovligt brukande. Ändringsförslaget ska gälla uttryckligen WLAN-nät men också nät av motsvarande typ (t.ex. WiMAX). Ändringsförslaget gäller inte nät som är skyddade eller avgränsade för vissa användare.

4 Propositionens konsekvenser

Den lagändring som föreslås förtydligar den nuvarande lagstiftningen om användning av oskyddade nät av typen WLAN, som trots det ovan nämnda domstolsavgörandet kan anses lämna utrymme för tolkning. Eftersom användning av oskyddade nät inte längre skulle vara förenad med risk för att begå brott, skulle det bli enklare att tillhandahålla öppna nät. Detta skulle främja i synnerhet offentlig- och privaträttsliga sammanslutningars möjligheter att tillhandahålla avgiftsfria nät av typen WLAN och motsvarande nätverk. Den föreslagna lagen skulle inte ha samma konsekvenser i fråga om WLAN-nät som tillhandahålls av privatpersoner, eftersom delning av internetlicenser med tredje parter ofta strider mot tjänsteleverantörens avtalsvillkor.

Olovlig användning av ett nät medför olägenhet om nätet används för att begå brott via internet, exempelvis dataintrång, upphovsbrott eller spridning av olagligt material. Relativt få sådana fall har emellertid uppdagats och det är då fråga om brott som kriminaliserats separat. Frågan om själva användningen av ett oskyddat nät ska vara straffbar har emellertid sannolikt ingen avgörande betydelse för användarens beslut att eventuellt begå andra berott. En kriminalisering av WLAN-användning har inte heller någon betydelse när det gäller de metoder för brottsundersökning som står till buds och främjar inte heller utredningen av andra brott i motsvarande fall.

Redan för närvarande kan olovlig användning av ett oskyddat trådlöst nät orsaka innehavaren av internetanslutningen ekonomisk skada i sådana fall där faktureringen grundar sig på mängden överförd data. Sådana fall har i praktiken inte förekommit i vid omfattning. När olovlig användning avlägsnas, faller ansvaret för att skydda sig mot en sådan risk på innehavaren av internetanslutningen själv.

Kriminalisering av användningen av oskyddade nät minskar användarens eget ansvar för att skydda sitt nät. Detta kan i sin tur minska användarnas intresse för att skydda sitt nät med lösenord. Myndigheterna har emellertid små möjligheter att övervaka olovlig användning. Den föreslagna lagändringen innebär att ansvaret för att skydda nät överförs på användarna själva. På detta sätt förbättras datasäkerheten.

Olovlig användning av WLAN har i ytterst få fall lett till brottsundersökning. För de myndigheter som svarar för brottsundersökning, rättegång och verkställighet medför det en hel del arbete om olovlig WLAN-användning leder till brottsundersökning. Om lagförlaget godkänns leder det för respektive myndigheters vidkommande till vissa resursbesparingar.

5 Beredningen av propositionen

Vid justitieministeriet färdigställdes den 14 oktober 2009 en promemoria om straffrättsliga frågor gällande användning av oskyddade trådlösa lokala nät (WLAN) (Suojaamattoman langattoman internet-lähiverkon (WLAN) käytön rikosoikeudellisia kysymyksiä). Promemorian behandlar omständigheter kring användning av WLAN utan ägarens uttryckliga tillstånd i sådana fall då nätet inte är skyddat med lösenord eller på något annat sätt. Bedömningen gäller främst frågan om det är ändamålsenligt att betrakta sådan användning som ett brott. Promemorian finns i elektronisk form (på finska) på adressen www.om.fi.

Justitieministeriet har bett sammanlagt 23 myndigheter, organisationer och personer yttra sig om promemorian. Sammanlagt 15 yttranden inkom.

Merparten av yttrandena stöder en fullständig avkriminalisering. Endast riksåklagarämbetet och centralkriminalpolisen understödde inte till denna del ändringen av bestämmelserna om olovligt brukande. I flera yttranden framhålls också behovet att i missbruksfall värna om rättssäkerheten för personer som inte skyddat sitt nät. I vissa yttranden anses

det också att lagstiftning som innebär avkriminalisering inte i allför hög grad bör bindas till en viss teknologi.

Den 15 juni 2010 publicerades yttrandena i sammandrag (Justitieministeriet: Betänkanden och utlåtanden 35/2010).

DETALJMOTIVERING

1 Lagförslag

28 kap. **Om stöld, förskingring och olovligt brukande**

7 §. *Olovligt brukande*. Det föreslås att till paragrafen fogas ett nytt 3 mom. enligt vilket användning en internetanslutning via ett oskyddat trådlöst datanät inte ska anses som olovligt brukande. Bestämmelsen gäller i praktiken framför allt nät av typen WLAN men täcker i praktiken också användning av WiMAX och eventuella andra framtida nätverk av motsvarande typ. Att ett nät är oskyddat innebär att det inte är skyddat med lösenord eller på något annat sätt. Nätet kan sålunda användas av ett på förhand ospecificerat antal användare. Den föreslagna bestämmelsen kan tillämpas oberoende av om nätägaren har avsett att nätet får användas fritt. Utanför tillämpningsområdet faller sådana mobiltelefonnät som är skyddade och tekniskt avgränsade till vissa anslutningar. I situationer där det trådlösa datanätet inte är skyddat men användning av internet via nätet kräver registrering med hjälp av ett lösenord (s.k. captive portal-skydd) är det inte straffbart att endast gå in på registreringssidan. Att bryta ett sådant skydd är dock även i fortsättningen straffbart som dataintrång.

Bestämmelsen täcker nätanvändning med alla typer av terminalutrustning som möjliggör trådlös anslutning. Till denna kategori av terminalutrustning hör bl.a. datorer, mobiltelefoner och spelkonsoler. Med användning av Internetanslutning avses all slags överföring av data. Bestämmelsen täcker förutom surfande på intenetsidor också t.ex. internetsamtal, nedladdning av program och spelande av nätspel. Bestämmelsen förutsätter inte att användaren på förhand vet om basstationen är uppkopplad till internet eller inte. Avkriminaliseringen föreslås emellertid avse endast användning av internet. Sålunda kommer det också i fortsättningen att vara straffbart som olovligt brukande att koppla upp sig via ett oskyddat nät till t.ex. en intranetserver, till en annans dator eller till datasystem eller terminalanslutningar som används inom specialbranscher. Den som genom att bryta säkerhetsarrangemang gör intrång i en annans dator eller i en intranetserver straffas sålunda liksom enligt gällande lag för dataintrång.

2 Ikraftträdande

Lagen föreslås träda i kraft så snart som möjligt.

Med stöd av vad som ovan anförts föreläggs Riksdagen följande lagförslag:

Lagförslag

Lag

om ändring av 28 kap. 7 § i strafflagen

I enlighet med riksdagens beslut

fogas till 28 kap. 7 § i strafflagen (39/1889), sådan paragrafen lyder i lag 769/1990, ett nytt 3 mom. som följer:

28 KAP

Om stöld, förskingring och olovligt brukande

7 §

Olovligt brukande

Som olovligt brukande anses inte användning av en internetanslutning via ett oskyddat trådlöst datanät.

_____

Denna lag träder i kraft den 20 .

— — — — — — — — — — — — — — —

_____

Helsingfors den 3 december 2010

Republikens President

TARJA HALONEN

Minister *Astrid Thors*

Bilaga
Parallelltexter

Lag

om ändring av 28 kap. 7 § i strafflagen

I enlighet med riksdagens beslut
fogas till 28 kap. 7 § i strafflagen (39/1889), sådan paragrafen lyder i lag 769/1990, ett nytt 3 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
28 KAP	
Om stöld, förskingring och olovligt brukande	
7 §	7 §
Olovligt brukande	*Olovligt brukande*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Den som olovligen brukar någon annans lösa egendom eller fasta maskin eller anordning, skall för olovligt brukande dömas till böter eller fängelse i högst ett år.	Den som olovligen brukar någon annans lösa egendom eller fasta maskin eller anordning, skall för olovligt brukande dömas till böter eller fängelse i högst ett år.
Försök är straffbart.	Försök är straffbart.
	Som olovligt brukande anses inte användning av en internetanslutning via ett oskyddat trådlöst datanät.
	_____
	Denna lag träder i kraft den 20 .
	_____