OIKEUSMINISTERIÖ

Lainvalmisteluosasto
Lainsäädäntösihteeri Sami Kiriakos

MUISTIO

14.10.2009

SUOJAAMATTOMAN LANGATTOMAN INTERNET-LÄHIVERKON (WLAN) KÄYTÖN RIKOSOIKEUDELLISIA KYSYMYKSIÄ

1 Johdanto

Tässä muistiossa arvioidaan seikkoja, jotka liittyvät suojaamattoman langattoman internet-lähiverkon, jäljempänä WLAN, käyttöön ilman verkon tukiaseman omistajan nimenomaista lupaa. Muistiossa arvioidaan erityisesti sitä, onko tekoa tarkoituksenmukaista pitää rikoksena.

WLAN teknologiasta

WLAN (Wireless Local Area Network) on langaton lähiverkko, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita. Tukiaseman avulla luotu verkkoyhteys mahdollistaa yhteyden internetiin. WLAN-verkolla on tukiasema, jonka kantama kerrostaloissa ulottuu yleensä ainakin naapurihuoneistoihin. Tällaiseen verkkoon voi kytkeytyä esimerkiksi kannettavalla tietokoneella tai WLAN-ominaisuudella varustetulla matkapuhelimella tai muulla päätelaitteella. Toisen omistaman WLAN:in käyttäminen merkitsee käytännössä hänen tukiasemansa ja modeeminsa käyttöä. Verkon käyttäminen ei merkitse yhteyden muodostamista WLAN:in haltijan tietokoneeseen.

Verkkoyhteys ja tukiasema voidaan suojata ulkopuoliselta käytöltä laitteen ja lähiverkon asetuksilla. Verkkoyhteys voi myös olla avoin, jolloin kuka tahansa voi käyttää sitä. Suojaamaton verkkoyhteys mahdollistaa tukiasemaa käyttävien muiden laitteiden näkymisen toisille verkon käyttäjille. Langattoman verkon hankkinut voi jättää verkkonsa suojaamattomaksi tarkoituksella tai tahattomasti.

Suojaamattoman langattoman verkon käyttämisestä ilman nimenomaista lupaa voi aiheutua verkon tukiaseman omistajalle haittaa lähinnä siitä, että käyttäjä siirtää niin paljon tietoa, että verkon kaista kapenee, jolloin omistajan verkkoyhteys tuoksi ajaksi hidastuu. Kevyempien internet-toimintojen käyttäminen, esimerkiksi sähköpostin lukeminen, kuvia ja tekstiä sisältävän uutissivuston selaaminen, videon katsominen, verkko-ostosten tekeminen tai nettiradion kuuntelu eivät yleensä tuntuvasti hidasta normaalia kotitalouden verkkoyhteyttä. Raskaammat toiminnot, kuten elokuvan lataaminen tai useiden edellä mainittujen toimintojen samanaikainen käyttäminen, voivat jo yhden käyttäjän toimesta tuntuvasti hidastaa omistajan verkkoyhteyden nopeutta. Verkkoyhteys myös hidastuu sitä helpommin, mitä useampi henkilö verkkoa samanaikaisesti käyttää.

2 Nykytila

Suomen lainsäädännössä ei ole erityistä langattoman lähiverkon luvatonta käyttöä koskevaa rangaistussäännöstä. Rikoslain 38 luvussa on yleisemmät säännökset tieto- ja viestintärikoksista. Luvun säännöksistä tilanteeseen voisivat soveltua lähinnä 8-8a §:n tietomurtoa koskevat säännökset, jotka koskevat oikeudetonta tunkeutumista tietojärjestelmään. Näidenkin säännösten soveltamisen edellytyksenä on kuitenkin tekijälle kuulumattoman käyttäjätunnuksen käyttäminen tai turvajärjestelyn murtaminen, joten säännökset eivät sovellu suojaamattoman lähiverkon luvattomaan käyttämiseen.

Käytön rangaistavuus

Rikoslain 28 luvun 7 §:n nojalla rangaistaan *luvattomasta käytöstä* (24.8.1990/769) sitä, ”[j]oka luvattomasti käyttää toisen irtainta omaisuutta taikka kiinteää konetta tai laitetta. Yritys on rangaistava”. Luvun 9 §:n mukaan teko on rangaistava *lievänä luvattomana käyttönä* ”[j]os luvaton käyttö, huomioon ottaen se, että rikos ei ole omiaan aiheuttamaan merkittävää vahinkoa tai haittaa, tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen.”

Turun hovioikeus 31.3.2009 on pysyttänyt Salon käräjäoikeuden 31.3.2008 antaman tuomion, jossa A:n katsottiin syyllistyneen lievään luvattomaan käyttöön, koska hän oli tahallaan käyttänyt B:n suojaamatonta langatonta verkkoyhteyttä ilman tämän lupaa.

Hovioikeuden tuomion perustelujen mukaan ”suojauksen toteuttamatta jättäminen tai suojaamattomien WLAN-verkkojen yleisyys eivät […] ole oikeudellisesti päteviä perusteita katsoa, että tällaisten verkkoyhteyksien käyttö ilman tukiaseman omistajan lupaa olisi kaikille sallittua. Toisen henkilön suojaamattoman verkkoyhteyden käyttö ei ole jokamiehenoikeus.” Hovioikeus katsoi sen vuoksi, että toisen suojaamattoman langattoman verkkoyhteyden käyttäminen tahallaan ilman tämän lupaa on rangaistava teko rikoslain 28 luvun 7 §:n 1 momentin luvatonta käyttöä koskevan tunnusmerkistön ja sitä täydentävän 9 §:n lievän luvattoman käytön tunnusmerkistön mukaisesti. Tapauksessa ei arviotu, voisivatko tapaukseen tältä osin soveltua rikoslain 38 luvun säännökset.

Tapauksessa ei ole haettu Korkeimmalta oikeudelta valituslupaa, joten hovioikeuden tuomio on lainvoimainen. Mainittu tapaus on tiettävästi ainoa, jossa tuomioistuin on ottanut kantaa toisen langattoman verkkoyhteyden luvattoman käytön rangaistavuuteen.

3 Kriminalisoinnin tarkoituksenmukaisuus

Vuonna 1990 voimaan tulleet rikoslain 28 luvun luvatonta käyttöä koskevat rangaistussäännökset on laadittu aikana, jolloin kuluttajat eivät yleisesti käyttäneet internetiä eikä WLAN-tyyppisiä langattomia verkkoyhteyksiä ollut olemassa. Säännöksiä laadittaessa ei näin ollen ole voitu ottaa huomioon tilanteita, joissa WLAN-verkkoa käytetään ilman laillisen haltijan lupaa.

WLAN-verkon käyttö ilman omistajan lupaa eroaa sellaisesta tavanomaisesta irtaimen esineen luvattomasta käytöstä, jossa omistaja ei luvattoman käytön aikana voi itse lainkaan käyttää esinettään (esim. polkupyörän luvaton käyttö). Toisaalta toisen omistaman WLAN:in käytön voidaan katsoa periaatteessa eroavan myös sellaisesta rangaistavuuden

ulkopuolelle jäävästä teosta, jossa toiselle kuuluvan esineen hyödyntäminen on omistajalle täysin huomaamatonta tai haitatonta. Tällaisia tekoja ovat esimerkiksi toisen henkilön sanomalehden lukeminen tämän selän takaa linja-autossa tai naapurissa soivan musiikin kuunteleminen. WLAN:in luvaton käyttäminen ei ole täysin huomaamatonta verkon lailliselle omistajalle, sillä käyttö varaa jonkin verran verkon tiedonsiirtokapasiteettia (”kaistaa”) käytön aikana. Tiedonsiirtonopeuden rajoittuminen kuitenkin hidastaa verkkoa vain, jos tietoa siirretään suuria määriä (ks. edellä). Jos verkkoa käytetään silloin kuin omistaja ei itse käytä verkkoa, käytöstä ei yleensä aiheudu hänelle minkäänlaista aineellista haittaa.[1]

Kriminalisoinnin perusteltavuutta arvioitaessa voidaan ottaa huomioon erityiset kriminalisointiperiaatteet, joita on muotoiltu Eduskunnan perustuslakivaliokunnan käytännössä (PeVL 23/1997). Periaatteiden mukaan muun muassa (1) rikosoikeutta tulee käyttää vain tärkeiksi katsottavien etujen suojaamiseksi, (2) rikosoikeuden tulee olla viimesijainen keino (ns. ultima ratio –periaate), (3) kriminalisoinnista tulee olla enemmän hyötyä kuin haittaa ja (4) kriminalisoinnin tulee olla toimiva ja täytäntöönpantavissa myös käytännössä.

(1) *Tärkeäksi katsottava etu*. Tässä tapauksessa kriminalisoinnin suojeluobjektina on perusoikeutena turvattu omaisuudensuoja (perustuslaki 7 §), erityisesti omistajan yksinomainen oikeus määrätä omaisuutensa käytöstä. WLAN:in luvatonta käyttöä koskeva kriminalisointi suojaisi sellaisen henkilön omaisuutta, joka ei halua antaa verkkoaan vapaasti yleisesti käytettäväksi. Kriminalisointi suojaa näin ollen tärkeäksi katsottavaa etua.

(2) *Ultima-ratio*. Rikosoikeudellisen rangaistuksen erottaa muista (hallinto- ja siviilioikeudellisista) sanktioista se, että siihen koetaan sisältyvän erityinen moraalinen moite. Rikosoikeutta tulisikin käyttää vain vahingollisimpiin ja paheksuttavimpiin tekoihin. Perustuslakivaliokunnan mukaan ”perusoikeuksista voidaan johtaa rikoslain säätäjään kohdistuva velvoite säätää ja ylläpitää kriminalisointeja, jotka ovat *välttämättömiä* perusoikeuden turvaamiseksi ulkopuolisten loukkauksilta.” (PeVL 23/1997, kursivointi tässä). Sanottu ilmaisee paitsi julkisen vallan velvoitteen turvata (nykyisen perustuslain 22 §:n nojalla) perusoikeuden toteutuminen yksityisten välisissä suhteissa myös suhteellisuusperiaatteen, jonka mukaan kriminalisointiin on ryhdyttävä vain sen ollessa välttämätöntä. Suhteellisuus- ja ultima ratio –periaatteiden mukaisesti olisi arvioitava myös muiden keinojen kuin rikosoikeuden riittävyyttä WLAN-verkon luvattoman käytön torjumisessa.

Yksinkertaisin tapa estää WLAN:in luvaton käyttö on suojata verkko salasanalla. Toimenpidettä ei ole pidettävä vaikeana henkilölle, joka osaa käyttää normaaleja internetsovelluksia. Suojatun verkon käyttäminen ei aiheuta kuin vähäistä lisävaivaa avoimen verkon käyttämiseen nähden.[2] Jos WLAN:in haltija haluaa tarjota mahdollisuuden käyttää verkkoaan vain määrätylle henkilöryhmälle (esim. kerrostalonaapureilleen, muttei talon ulkopuolisille henkilöille), voi hän antaa heille verkkonsa salasanan.

---

[1] Jos toisen verkkoa kuitenkin käytetään rikosten tekemisessä, esimerkiksi tietomurrossa tai lapsipornografian lataamisessa, voi verkon omistaja joutua itse rikosepäilyn kohteeksi. Aiheeton rikosepäily voi olla kumottavissa verkon lokitietojen ja epäillyn tietokoneen kovalevyltä saatavien tietojen perusteella.

[2] Esimerkiksi yleisimmin käytetyissä käyttöjärjestelmissä (Microsoft Windows ja Apple Macintosh OS X) edes salasanan syöttämistä ei välttämättä edellytetä jokaisella kerralla muodostettaessa verkkoyhteys koneen sammuttamisen jälkeen, sillä salasana voidaan tallentaa tietokoneen muistiin.

Verkon suojaaminen salasanalla on varma keino estää verkon luvaton käyttö sellaisilta ulkopuolisilta, jotka eivät ryhdy murtamaan suojausta. Jos verkon suojaus murretaan, kysymys on rikoslain 38 luvun 8-8a §:ssa tarkoitetusta tietomurrosta, jota koskevilla rangaistussäännöksillä on eri suojeluobjektit (yksityisyyden suoja ja tietosuoja) kuin luvattomalla käytöllä (omaisuudensuoja).

On arvioitu, että suuri osa WLAN:in käyttäjistä eivät ole suojanneet verkkoaan. Tämän oletetaan johtuvan osittain tietoisesta valinnasta pitää verkko avoimena esimerkiksi naapureiden käytettäväksi ja osittain käyttäjien tietämättömyydestä tai osaamattomuudesta.[3] Tietämättömyyden ja osaamattomuuden voidaan kuitenkin olettaa johtuvan WLAN-teknologian tuoreudesta ja niiden voidaan otaksua lähitulevaisuudessa vähenevän etenkin, kun otetaan huomioon, että suojaaminen salasanalla on varsin yksinkertainen toimenpide.[4]

Jos verkon käytöstä ilman lupaa aiheutuu tukiaseman omistajalle vahinkoa, voi hän myös joissain tapauksissa turvautua oikeuteensa saada vahingonkorvausta.

Koska verkon suojaaminen on näin ollen tehokas ja vain hyvin vähäistä vaivaa aiheuttava keino, ei kriminalisointi vaikuta olevan välttämätön keino estää avoimen verkon käyttöä.

(3) *Hyöty-haitta punninta*. Kriminalisoinnin merkittävimpänä hyötynä voidaan pitää sen yleisestävää vaikutusta. Kriminalisointi välittää yleisölle viestin teon paheksuttavuudesta, minkä katsotaan vaikuttavan kansalaisten moraalikäsityksiin. Rikokseksi määriteltyyn tekoon liittyvä sanktion uhka ehkäisee ihmisten ryhtymistä tekoon.

Yleisestävyys on kuitenkin tehokkainta kiinnijäämisriskin ollessa korkea. WLAN:in luvaton käyttö ei normaalisti näy tukiaseman omistajalle ilman tämän erityistoimenpiteitä muulloin kuin silloin, kun dataa siirretään niin paljon, että verkko huomattavasti hidastuu. Teon luonteesta johtuen kiinnijäämisriskiä ei juurikaan voida nostaa poliisin valvontaa lisäämällä. Kiinnijäämisriski on näiden seikkojen vuoksi melko pieni. Lisäksi rangaistavuuden yleisiestävä vaikutus on alhaisempi sellaisiin ihmisiin, jotka pitävät tekoa kriminalisoinnista huolimatta moraalisesti hyväksyttävänä. Yhdysvalloissa tehtyjen kyselytutkimusten mukaan avoimen WLAN:in käyttöä ilman omistajan lupaa pitää kuitenkin moraalisesti hyväksyttävänä 40-50 % kansalaisista.

Kriminalisoinnista aiheutuu myös aina tavanomaiset toimeenpanoon (valvonta, tutkinta, lainkäyttö, rangaistuksen täytäntöönpano) liittyvät kustannukset. Lisäksi jos tekoa laajasti pidetään moraalisesti hyväksyttävänä ja kriminalisointi sen vuoksi koetaan epäoikeudenmukaiseksi, voi seurauksena olla rikosoikeusjärjestelmän legitimiteetin alentuminen.

Tämän lisäksi avoimen WLAN:in käytön kriminalisoinnista voi aiheutua erityisiä ongelmia. Yleisölle tarjottavien maksuttomien WLAN:inen tarjonta yleisissä tiloissa kuten puistoissa ja lentokentillä - ns. ”access pointit” tai ”hot spotit” - on viime aikoina yleistynyt. Näissä paikoissa ei aina ole selkeästi tiedotettu maksuttoman ja vapaasti käytettävän WLAN:in olemassaolosta. Tietokoneella, matkapuhelimella tai muulla laitteella verkkoyhteyttä muodostava ei aina saa tarjolla olevasta verkosta muuta tietoa kuin ver-

[3] *Tietokone* verkkolehti (Ari Karkimo), ”*Joka toinen wlan avoinna – ymmärtämättömyys syynä*”, 6.4.2009.
[4] Olisi myös teknisesti mahdollista määritellä tukiasemien asetukset jo tehtaalla sellaisiksi, että tukiasema edellyttää ensimmäisen käyttöönoton yhteydessä sen suojaamista salasanalla.

kon nimen ja sen, onko verkko suojattu. Jos käyttäjä ei ole aivan varma, onko suojaamatonta verkkoa luvallista käyttää, ottaa hän riskin syyllistyä rikokseen. Tämä vaikeuttaa yleisten maksuttomien WLAN:ien käyttöä. Ongelmaa vähentäisi mahdollisuus tiedottaa verkon käytön luvallisuudesta, mutta sekään ei välttämättä poistaisi kaikkia käyttäjän kannalta vaikeita tulkintatilanteita.

Toisena rangaistavuuteen liittyvänä ongelmana on pidetty sitä, että ainakin Windows–käyttöjärjestelmien oletusasetusten mukaisesti tietokone saattaa automaattisesti ja käyttäjältä varmistamatta muodostaa yhteyden lähimpään avoimeen WLAN:iin, mikä voi helposti jäädä käyttäjältä huomaamatta. Ongelma kuitenkin poistuisi, jos oletusasetukset muutetaan esimerkiksi sellaisiksi, että käyttöjärjestelmä pyytää aina ennen yhteyden muodostamista käyttäjältä varmistuksen. Siten ongelmaa voidaan pitää vain teknologisena.

(4) *Käytännön toimivuus*. Avoimen WLAN:in luvattoman käytön valvonta jää käytännössä tukiaseman omistajan aktiivisuuden varaan. Nykyisen teknologian puitteissa sen selvittäminen, onko joku käyttänyt verkkoa luvatta, vaatii erityisasiantuntemusta edellyttäviä toimenpiteitä. Vaikka WLAN:it ovat viime vuosina yleistyneet huomattavasti, ei tuomioita luvattomasta käytöstä ole tiettävästi annettu kuin yhdessä (edellä mainitussa) tapauksessa. Näin ollen avoimen WLAN:in luvattoman käytön rangaistavuuden merkitys voi jäädä käytännössä melko vähäiseksi. Teknologista estettä ei kuitenkaan liene esimerkiksi sille, että käyttöjärjestelmä ilmoittaa käyttäjälle aina, kun hänen verkkoaan käytetään. Tämä voisi lisätä kriminalisoinnin käytännön merkitystä.

Johtopäätös

Edellä esitetyn perusteella nykyinen kriminalisointi voidaan nähdä monelta osin ongelmallisena. Kriminalisoinnin etuja vähentävät kriminalisoinnista aiheutuvat kustannukset ja erityiset haittavaikutukset, ennen kaikkea se, ettei käyttäjä voi aina ennalta tietää, onko omistaja tarkoittanut verkon avoimesti käytettäväksi vai ei. Myös yleisestävän vaikutuksen vähäisyys ainakin nykyisessä tilanteessa vähentää kriminalisoinnin hyötyjä. Rangaistussäännöksen tarkoituksenmukaisuutta vastaan puhuu ennen muuta helppous estää luvaton käyttö yksinkertaisesti verkkoyhteytensä suojaamalla. Näin ollen suojaamattoman WLAN:in käyttämistä ilman omistajan lupaa ei ole perusteltua pitää rikoslain 28 luvun 7-9 § nojalla rangaistavana ainakaan nykyisessä laajuudessa.

4 Vaihtoehtoja rajoittaa nykyistä luvattoman käytön rangaistavuutta

Vaihtoehto 1.

Suojaamattoman WLAN:in käyttö ilman omistajan antamaa lupaa olisi edelleen rangaistavaa luvattomana käyttönä, paitsi jos käyttäjällä on perusteltu syy olettaa, että verkko on luvan puuttumisesta huolimatta tarkoitettu yleisesti käytettäväksi. Tämän mukaan rangaistaisiin lähtökohtaisesti sellaisen suojaamattoman WLAN:ien luvattomasta käytöstä, joita ei markkinoida kaikille vapaasti käytettäviksi (esim. yksityisasunnoissa olevat tai kahviloissa kahvilan asiakkaille tarkoitetut WLAN:it). Sen sijaan sellaisten WLAN:ien käyttö ei olisi rangaistavaa, jotka ovat yleisissä tiloissa, kuten puistoissa, ja jotka esim. kyltin tai verkon nimen perusteella voidaan perustellusti olettaa vapaasti käytettäviksi.

Vaihtoehto tarkentaisi nykyistä 28 luvun 7-9 §:ää, joiden nojalla saattaa syntyä käsitys, että yleisölle tarkoitettujen suojaamattomienkin WLAN:ien käyttö on lain mukaan kiellettyä ilman nimenomaista lupaa. Laissa toisin sanoen tarkennettaisiin käsitettä ”luvattomasti”. Jos käyttäjällä on perusteltu syy olettaa, että verkko on erikseen annetun luvan puuttumisesta huolimatta tarkoitettu yleisesti käytettäväksi, käyttö ei olisi ”luvatonta”. Vaihtoehto suojaisi siten verkkonsa suojaamattomana pitävää omistajaa, joka ei halua antaa verkkoaan vapaasti yleisesti käytettäväksi, mutta turvaisi samalla mahdollisuutta tarjota yleisölle vapaasti käytettäviä WLAN:eja.

Vaihtoehto kuitenkin säilyttäisi useat edellä mainitut kriminalisointiin liittyvät ongelmat (kustannukset, alhainen kiinnijäämisriski, käytännön tilanteiden tulkintaongelmat, tietokoneen hakeutuminen verkkoon automaattisesti). Esimerkiksi yksityishenkilön, joka kerrostalossa haluaisi jättää WLAN:insa vapaasti naapuriensa käytettäväksi, olisi edelleen erikseen ilmoitettava heille, että verkkoa on luvallista käyttää.[5] Lisäksi huolimatta siitä, että WLAN:in käyttö eroaa edellä esitetyllä tavalla periaatteessa normaaliin irtaimen esineen käytöstä, kuvatun kaltainen tarkennussäännös yksinomaan WLAN:ien käytön osalta saattaisi olla liian kasuistinen.[6]

Vaihtoehto 2.

Suojaamattoman WLAN:in luvaton käyttö olisi rankaisematon teko paitsi silloin, kun se on omiaan aiheuttamaan omistajalle merkittävää haittaa. Tällaisena haittana pidettäisiin ainakin selvää tietoliikenteen hidastumista. Säännös voitaisiin muotoilla niin, että abstrakti vaara haitasta riittäisi (”on omiaan aiheuttamaan”), jolloin tietoa ei tarvitsisi olla siitä, että tukiaseman omistaja käyttää verkkoa samanaikaisesti. Vaihtoehdon etuna olisi, että sillä ehkäistäisiin omistajaa häiritsevää WLAN:in käyttöä. Tällöin omistaja voisi pitää verkkonsa avoimena ja saada silti suojaa häiritseviltä käyttäjiltä.

Vaihtoehtoon liittyy kuitenkin joitakin ongelmia. Ensinnäkin ”merkittävää haittaa” tai vastaavaa kriteeriä olisi mahdotonta määritellä täsmällisesti. Tästä voisi seurata se, että mahdolliset käyttäjät ”varmuuden vuoksi” jättävät käyttämättä avoimeksi tarkoitettua verkkoa, mikä olisi säännöksen tarkoituksen vastaista.

Lisäksi jo tekijän tahallisuuden täyttyminen edellyttäisi, että hänen olisi mahdollista tietää riittävällä tarkkuudella käyttämänsä verkkoyhteyden nopeus ja oman tiedonsiirtonsa määrä sekä näiden vaikutus verkon nopeuteen. Selvemmissä tapauksissa tahallisuus voisi olla helpommin täyttyvä. Esimerkiksi käyttäjän ladatessa samanaikaisesti useampaa elokuvaa tai pelatessa raskasta grafiikkaa käyttävää verkkopeliä voinee hän olettaa tämän hidastavan nykyään normaalia kotitalouden verkkoyhteyttä. Tilanteessa, jossa datan siirto on vähäisempää, voi olla vaikeampaa osoittaa, että tekijä on pitänyt varsin todennäköisenä, että tukiaseman omistajan oma internet-yhteys on ollut omiaan hidastumaan.

Vaihtoehto ei myöskään suojaisi käyttäjää sellaiselta tilanteelta, jossa useampi henkilö samanaikaisesti käyttää hänen verkkoaan sitä hidastaen, vaikka kukaan käyttäjistä ei yksin käytä verkkoa niin, että voisi olettaa siitä aiheutuvan hidastumista.

---

[5] Verkon tarjoaminen yleisesti käytettäväksi saattaa tosin erityisesti yksityishenkilöiden osalta olla internet-palveluntarjoajan kanssa tehdyn sopimuksen vastaista.

[6] Voitaisiin nimittäin kysyä, miksei yhtä hyvin kaikkien esineiden luvattoman käytön osalta säädetä vastaavaa tarkennusta. Vaikka myös jäljempänä esitettävää vaihtoehtoa 3 voidaan pitää kasuistisena, se ei aiheuta vastaavankaltaista ongelmaa.

Vaihtoehto 3.

Suojaamattoman WLAN:in luvattoman käytön rangaistavuus poistettaisiin kokonaan. Tällöin rankaisematon teko olisi siis sellainenkin käyttö, joka hidastaa tukiaseman omistajan omaa internet-yhteyttä. Omistaja voisi tarvittaessa helposti verkon suojaamalla rajoittaa verkon vain omaan tai määrätyn henkilöryhmän käyttöön. Vaihtoehto olisi selkeä ja yksinkertainen.

Vaihtoehto olisi lakiteknisesti toteutettavissa esimerkiksi niin, että luvatonta käyttöä koskevaan rikoslain 28 luvun 7 §:ään lisätään 3 momentti, jossa todetaan, ettei luvattomana käyttönä pidetä suojaamattoman internet-lähiverkkoyhteyden käyttämistä.