IMPLICAÇÕES CONSTITUCIONAIS DAS REDES WI-FI

Annuska Macedo S. F. PAIVA(1)
(1) CEFET-PB/UFPB, Av. Umbuzeiro, 1287/201 - Manaira, 8332463123/8388089072, e-mail: annuskamacedo@gmail.com

RESUMO

A Informática é essencial na realidade hodierna, e a vida frenética da sociedade ".com" exige, cada vez mais, mobilidade. A comunicação wireless vem como solução, o que pode ser visto com a rápida difusão de redes Wi-Fi domésticas e de empresas. Essa evolução, no entanto, ainda não recebeu quaisquer análises jurídicas, o que vulnerabiliza direitos fundamentais, como a segurança e privacidade, defesa do consumidor, saúde e desenvolvimento regional. Este trabalho consiste em uma revisão bibliográfica, buscando as considerações de especialistas em informática e saúde sobre questões de natureza constitucional, envolvendo Wi-Fi. Notamos, pois, que a segurança das redes é de responsabilidade do administrador, que pode ser acionado juridicamente, mas, no caso de redes domésticas, cabe ao próprio usuário protegê-la, através de procedimentos como criptografia e cuidados básicos que descrevemos, além de ressaltar a necessidade de informar o consumidor sobre os riscos. A OMS recomenda o uso de redes Wi-fi consciente, já que a exposição prolongada pode ultrapassar os limites diários recomendados. Por fim, notamos que essas redes apresentam mais pontos positivos, já que resolve problemas práticos a baixo custo, além de fornecer base para WMANs, que permitiriam acesso a locais sem infra-estrutura de cabos, facilitando a inclusão digital.

Palavras-chave: redes wi-fi, regulamentação constitucional, cidadania, saúde

1. INTRODUÇÃO

A sociedade atual enfrenta uma profunda mudança de paradigmas: passamos à era da informação, quando o cibernético apresenta efeitos concretos na vida humana, e os que são impossibilitados de acessar tal mundo virtual, ou por falta de conhecimento, ou por indisponibilidade de recursos, sofrem. Nesta perspectiva de diminuir os excluídos digitalmente, redes wireless mostram-se mais que um mero modismo: o Wi-fi (IEEE 802.11) já é consagrado em redes domésticas, por permitir mobilidade com recursos plausíveis, mas a realidade não distante de WMANs, como o WiMAX (802.16) permitirá acesso de lugares cuja infra-estrutura era empecilho.

Entretanto, sabe-se que, enquanto a ciência caminha lentamente por trilhas seguras, há indivíduos que se utilizam desta para iludir pessoas próbias, que presumem ser a sociedade em que vivem lugar de plena aplicação do princípio da boa-fé. Assim, é necessário um cuidado redobrado com a segurança, função esta do administrador da rede, a fim de evitar fraudes aos usuários. Constitucionalmente temos preservada a nossa privacidade – artigo 5º, XII –, mas o novo *e-commerce*, muitas vezes, diminui este direito fundamental a fim de um maior lucro.

O Direito é o melhor instrumento, para garantir o cumprimento de direitos e pode, sim, acompanhar as mudanças da sociedade a partir de uma interpretação adequada dos fatos, respeitando, contudo, o limite que a lei apresenta. O Direito da Informática e de Telecomunicações, campo novo e não muito explorado, necessita de contribuições para desenvolver-se. Pesquisas científicas são imprescindíveis para entender os efeitos das novas tecnologias e, assim, regulá-las ou adaptá-las à legislação vigente, e há diversas lacunas nas áreas de tecnologia sem fio, como mostra a Organização Mundial da Saúde – OMS –, por exemplo, que ainda não conseguiu atingir resultados satisfatórios no estudo da radiação de Rádio Freqüência - RF. Este trabalho tem por objetivo analisar o novo avanço das Redes Wireless à luz da Constituição – CF/88 –, mostrando onde difere de outras tecnologias usadas para acesso multimídia, às possibilidades trazidas pelo Wi-Fi e que medidas sociais serão necessárias, para permitir uma evolução segura, utilizando, para tanto, pesquisa bibliográfica. Tomaremos de empréstimo métodos originários nas ciências naturais – o indutivo – e nas ciências exatas – o dedutivo –, para a análise sistemática de obras doutrinárias e de jurisprudência pertinentes ao tema. Por fim, vale ressaltar a importância do método histórico-evolutivo, para organizar fatos e, a partir da análise da sociedade, arriscar previsões, baseadas na analogia com eventos similares, ocorridos no pretérito.

2. DIREITOS FUNDAMENTAIS E A LGT: RELAÇÕES DIRETAS ENTRE PRINCÍPIOS

O Direito das Tecnologias de Informação é recente: sua importância cresce, vinculada à evolução do uso da Internet, que redefiniu a dinâmica do mundo contemporâneo. Um dos seus maiores questionamentos versa sobre a necessidade ou não de novas codificações que abarquem a pululação inovativa atual. A maior parte de seus militantes opta por uma solução fácil: sendo o Direito uma ciência humana, depende da interpretação da realidade por seus aplicadores, logo, a hermenêutica é a chave para a resolução de problemas. Exemplifica-se: o homicídio não precisou ser reinventado quando se criaram as armas de fogo, já que houve apenas uma modificação em seu instrumento. A tecnologia seria, pois, um instrumento recentemente descoberto. Tal solução, no entanto, não é total, já que o Direito Penal, por ser taxativo, não consegue se adaptar a certos casos possibilitados por esse aparato tecnológico antes desconhecido, que pode criar tipos.

Outra questão reside na organização dos serviços de telecomunicações e na regulamentação técnica de novos aparelhos, e com esse intuito, foi feita a Lei Geral de Telecomunicações – LGT –, lei nº 9.472, de 16 de julho de 1997, que, em seu artigo 60, §1º, dispõe: "Telecomunicação é a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza." As redes wireless se caracterizam pela integração de computadores sem a utilização de meios físicos na ponta dos usuários, possibilitando a transmissão de informações via ondas eletromagnéticas, sendo, portanto, regidas pela LGT.

"Há uma verticalidade fundamentadora entre os diplomas normativos, mediante a qual um diploma encontra respaldo e fundamento naquele que lhe é superior." Esta afirmação de Maurício Godinho Delgado (2007, p.139) é iluminadora, quanto à hierarquia que direciona todo o ordenamento jurídico. Pensando em uma pirâmide, a Constituição ocupa seu topo, e quaisquer instrumentos normativos devem apresentar direta

vinculação ao que lá está disposto, sob pena de sofrer controle de constitucionalidade e perder sua vigência e eficácia. A Constituição firmou princípios basilares para a ordem jurídica, o Estado e a sociedade. Atualmente, em grande medida, os princípios gerais do Direito, aplicáveis em todos os ramos, são princípios constitucionais. Assim, analisar certa área à luz da Constituição é, de maneira indireta, buscar seus princípios informativos.

O vínculo entre a CF/88 e a LGT está claro no art. 5º desta, que traz a obrigatoriedade da observância de certos princípios constitucionais:

> Art. 5º Na disciplina das relações econômicas no setor de telecomunicações observar-se-ão, em especial, os princípios constitucionais da soberania nacional, função social da propriedade, liberdade de iniciativa, livre concorrência, defesa do consumidor, redução das desigualdades regionais e sociais, repressão ao abuso do poder econômico e continuidade do serviço prestado no regime público.

Em uma feliz coincidência, este apresenta total conformidade com um outro artigo 5º de importância já consagrada: a CF/88, também chamada "Constituição Cidadã", devido à grande preocupação com os direitos humanos, traz neste uma relação de direitos fundamentais da pessoa humana, também conhecida como "direitos humanos de primeira geração", ligados, no lema da Revolução Francesa – Liberté, Égalité, Fraternité –, à igualdade. Relacionando estes artigos 5º e os artigos 3º e 4º da LGT, podemos detectar os seguintes pontos que devem ser respeitados pelos serviços de telecomunicações, logo, pontos críticos para as redes wireless:

- O sigilo de informações (art. 5º, XII CF/88, art. 3º, V, VI e IX, LGT) é um ponto de fortes questionamentos em redes wireless, pois sendo o meio de transmissão aberto – ar – toda a segurança da rede neste transporte depende de encriptações WEP ou WPA, que já foram quebradas. Tal falha de segurança do Wi-fi já é superada com o WiMAX, que utiliza encriptações mais fortes
- A defesa do consumidor (art. 5º, XXXII CF/88, art. 3º, VIII, X e XI) terá que lidar com uma questão delicada: já é ponto pacífico que a responsabilidade sobre a proteção da rede cabe a seu administrador, o que, em meios que utilizam conexões físicas, são, geralmente, empresas prestadoras de serviço. Uma das maiores aplicações do Wi-fi é a rede doméstica, fácil de ser implantada por qualquer usuário de computador, mesmo inexperiente, pois só depende de aparelhos que se configuram automaticamente. No entanto, para que estes ofereçam o mínimo de segurança, é necessário um prévio conhecimento para configurar a encriptação, por exemplo, o que passa despercebido, deixando tais redes vulneráveis. Como resolver a questão da responsabilidade? Outra questão é o direito à informação, intrínseco ao consumidor. Quem deverá informá-lo de que as redes Wireless exigem um especial cuidado com a segurança?
- O desenvolvimento regional (art. 3º, II, CF/88 e art. 5º, LGT) em questões tecnológicas pode ser barrado sob a alegação de falta de recursos para produzir a infra-estrutura necessária e os altos custos que decorreriam desta implementação. Redes metropolitanas resolveriam o problema a baixos custos, permitindo não apenas a integração regional, mas também a inclusão social através da alfabetização digital e um novo meio para a democracia participativa. É importante lembrar que o acesso a serviços de telecomunicações com tarifas razoáveis, boa qualidade e cobertura e o incentivo ao uso dessas redes são elencadas como deveres do poder público, no art. 2º da LGT. Estes podem ser usados inclusive na efetividade dos direitos ao Meio Ambiente – art. 225 – e nos direitos indígenas – arts. 231 e 232.
- O direito à saúde – arts. 196-200 – e a exposição à RF, decorrente inclusive de redes wireless e estações-base estão em lados opostos, sendo alvo de inúmeras pesquisas que, até agora, não alcançaram resultados conclusivos. Para garantir que os riscos sejam minorados, é essencial a observação à regulamentação de cada atividade, dada, no Brasil, pela Anatel, e das especificações técnicas recomendadas de cada produto, definidas por organismos internacionais, como o IEEE.

Tentaremos, pois, esclarecer algumas discussões feitas sobre estes pontos, ao longo do artigo.

3. MOBILIDADE WIRELESS: UNIVERSALIZAÇÃO DE SERVIÇOS E CIDADANIA

Mike Walker *apud* Colin Roy (2005, p. 1), afirma que o mundo passa por uma "Mobile Revolution"- Revolução Móvel –, ao fornecer a interessante estatística de que mais de 1,4 bilhão de pessoas, ou 20% da população mundial possui um telefone celular, e dois bilhões de pessoas têm condições de fazer uma chamada telefônica. Quando esta acontece, é mais provável que ocorra via celular que utilizando linha fixa.[1]

No Brasil, os serviços de telecomunicações móveis viram-se difundidos após a privatização das empresas telefônicas, que gerou concorrência e conseqüente barateamento dos serviços, que atingiram camadas sociais antes excluídas de serviços de comunicação privados. O Estado, de acordo com o artigo 22 da CF/88, explora estes serviços mediante concessão dada a empresas, que devem responder à Agência Nacional de Telecomunicações – Anatel, sua agência reguladora.

Segundo Aires José Rover (2006, p.69), Mcluhan considera que a tecnologia cria um ambiente totalmente novo, modificando os indivíduos por suas técnicas de comunicação, e Negroponte ressalta que a informática não tem mais a ver com os computadores, mas com a vida das pessoas. Aí entra a função das tecnologias de informação, que podem permitir a participação de uma grande maioria permanentemente excluída das decisões políticas. A Internet pode ser vista como uma nova forma de controle e fiscalização da administração pública, bem como meio para desburocratizar as relações entre Estado e cidadãos/consumidores. Entramos, pois, na necessidade de um governo eletrônico:

> "Governo eletrônico é uma infra-estrutura única de comunicação compartilhada por diferentes órgãos públicos, utilizando a tecnologia da informação de forma intensiva, para melhorar a gestão pública e o atendimento ao cidadão, colocando o governo ao alcance de todos, ampliando a transparência de suas ações e incrementando a participação cidadã" [ROVER, 2006]

Do ponto de vista do Estado, é um instrumento de administração dos poderes do Estado e prestação de serviços públicos, mas a sociedade a vê como forma d realização de fins do Estado Democrático de Direito, tornando a tecnologia e a comunicação instrumentos da interação entre cidadãos.

Para que haja uma real democracia digital, é mister o desenvolvimento de políticas que reconheçam o direito de acesso à rede – integrante da quarta geração de Direitos Humanos –, tornando-o efetivo, o que implica o combate ao analfabetismo eletrônico. Em relação à informática, a população brasileira dispõe de salas de multimídia públicas em escolas e bibliotecas, mas estamos longe de atingir a tão sonhada inclusão digital. Segundo a pesquisa TIC Domicílios 2006 (CETIC.BR, 2006), realizada pelo Comitê Gestor da Internet no Brasil, os fatores socioeconômicos ainda são os principais determinantes do acesso às tecnologias da informação no Brasil - quanto maior a renda e a escolaridade, maior o acesso, além de as desigualdades regionais também se reproduzirem nos critérios de posse e uso de tecnologias da informação, pois os habitantes das regiões mais ricas têm mais acesso e utilizam mais essas tecnologias. O número de analfabetos em informática é insustentável em uma sociedade que caminha a passos largos para o ".com", o que acentua ainda mais a discrepância social típica do nosso país, o que fere profundamente os princípios fundamentais da cidadania e da dignidade da pessoa humana – artigo 1º, II e III, além do objetivo estatal de construir uma sociedade livre, justa e solidária, diminuindo as desigualdades sociais e regionais – artigo 3º, I e III.

Há também uma barreira sociológica, apresentada por pessoas de meia-idade cuja profissão não obriga o uso de computadores, e que se vêem desestimuladas a buscar instrução nesta área, porém são rodeadas por instrumentos eletrônicos que, muitas vezes, são a única opção de acesso, sem, no entanto, haver o assessoramento suficiente. O mercado de trabalho atual também exige conhecimentos de informática em quaisquer ofertas de emprego, fazendo o não acesso a esta ganhar conseqüências ainda mais graves.

---

[1] "This provided the interesting statistic that more than 1.4 billion people, or 20% of the global population, have a mobile phone, and 2 billion people in the world have yet to make a phone call. When that call takes place, it will most likely be on a mobile phone not a fixed line."

Esforços para diminuir esta disparidade são feitos, principalmente, em universidades públicas, através de programas de extensão que visam a ensinar à população carente como manejar o computador, porém, notamos também ser necessário campanhas de conscientização sobre a necessidade da informática, além de uma maior abrangência de cursos gratuitos – já que seu custo é alegado como maior empecilho pelas classes baixas – e de qualidade nesta área, nos locais mais variados possíveis, além de maior facilidade na aquisição do computador domiciliar – projeto lançado no início de 2007, através de incentivos fiscais –, apesar de termos consciência que seria ingenuidade priorizar esta em um país com tantos analfabetos – não apenas no sentido digital – e miseráveis.

Na mesma pesquisa supracitada, nota-se um aumento na quantidade de usuários de computadores e de internet, porém esta é mais utilizada em escolas ou em centros de acesso público pagos, principalmente no caso das classes D e E. Estas classes, dentre os que possuem computadores em casa, destacam a não disponibilidade de internet banda larga na área. Com algum estudo de projetos de redes, percebemos que, muitas vezes, soluções sem fio são mais econômicas, dependendo do número de computadores que se deseja interligar e da topologia do terreno. Assim, é palpitante a possibilidade de aplicação de redes sem fio na construção de centros de acesso público gratuito, além de estas fornecerem a possibilidade de acesso à rede em áreas remotas, o que é, como já visto, direito do usuário de serviços de telecomunicações. O WiMAX (IEEE 802.16), probabilidade mais palpável de WMAN – rede metropolitana de acesso sem fio – pode, em um futuro breve, preencher esta lacuna, com um sinal de potência suficiente para cobrir uma cidade inteira através de uma única antena, carregando Internet de alta velocidade, ajudando, pois, o processo de inclusão digital tão ansiado. É importante lembrar que o Brasil é palco de experiências com o WiMAX em Brasília e em Ouro Preto, mas se considera que as especificações iniciais deste modelo não foram atingidas. Talvez isso seja decorrente de uma confusão feita quanto a velocidade e a área de cobertura máximas: elas não são complementares, mas inversamente proporcionais.

O acesso a Internet via redes sem fio também pode ser visto como meio de integração regional e de monitoramento do meio ambiente: neste sentido, foi posto em vigor, em maio de 2007, um acordo assinado pelo Ministério do Meio Ambiente, para oferecer Internet grátis via satélite a índios, pescadores e quilombolas, comunidades que são as verdadeiras protetoras de suas áreas, segundo reportagem de O maior objetivo deste programa é contribuir para a preservação do meio ambiente, e a Internet é um meio capaz de gerar grande repercussão, devido ao enorme número de usuários e ser um espaço democrático, onde todos podem publicar: a Internet já foi usada pelos índios ashaninka do Acre, para denunciar o desmatamento ilegal na reserva o Governo Federal proverá o acesso sem fio, já que estas áreas não apresentam infra-estrutura, mas prefeituras e governos estaduais deverão garantir os computadores. Este programa cobrirá 150 comunidades da Amazônia, do Pantanal e do sertão nordestino. Além da questão ambiental, podemos entender que tal medida possibilitará a maior inclusão social nestas áreas.

4. DIFUSÃO E SEGURANÇA DE REDES WIRELESS DOMÉSTICAS

A principal utilização das redes wireless é a referente ao modelo 802.11 – o Wi-fi. Este modelo define as camadas de controle de acesso ao meio – MAC – e a física – PHY – para uma rede local – LAN – com conectividade sem fio, na qual as estações conectados – notebooks, palms, impressoras ou outras máquinas habilitadas ao protocolo 802.11, abrangendo as características MAC, PHY e conexão com o meio sem fio – se comunicam pelo ar com outros componentes que estão na área de abrangência da rede. Há diversas arquiteturas de rede possíveis com este modelo, sendo as principais:

- *Independent Basic Service Set (IBSS)* abrangendo a conexão direta entre estações que estejam na área de cobertura, utilizando comunicação de modo ponto-a-ponto (P2P), também chamada *ad-hoc*

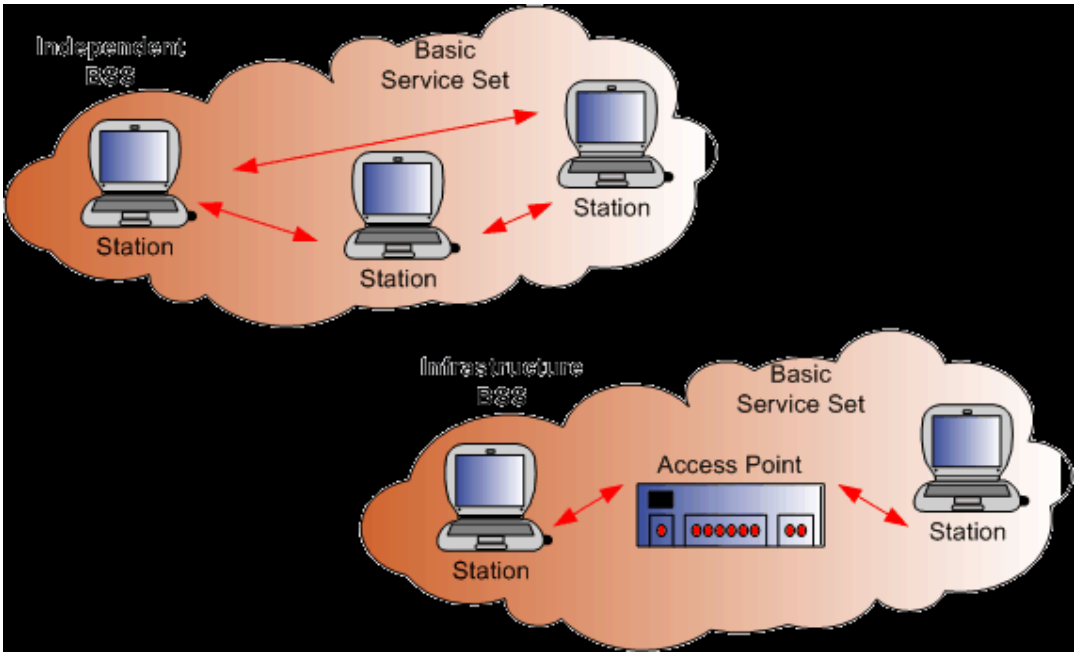

Figura 1 – Arquitetura IBSS

Fonte: http://www.mpirical.com/companion/mpirical_companion.html#http://www.mpirical.com/companion/Wi-Fi/BSS_-_Basic_Service_Set.htm

- *Infrastructure Basic Service Set* (BSS), que utiliza a comunicação de modo infra-estrutura, que necessita de um concentrador de acesso – componente chamado *Access Point* (AP), que intermedeia a comunicação entre as estações em sua área de abrangência e entre estas e um sistema de distribuição de informações, geralmente uma rede externa com fio.

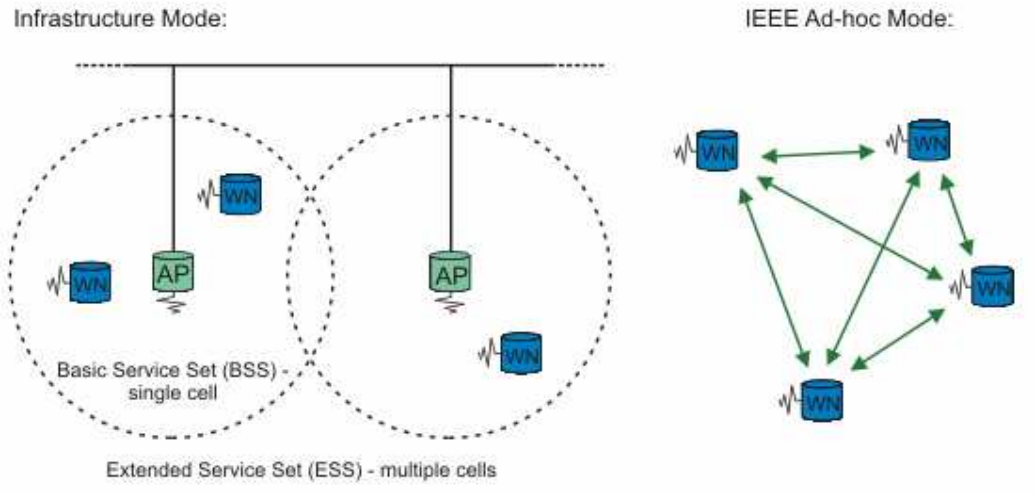

Figura 2 – Arquitetura BSS

Fonte: http://tldp.org/HOWTO/html_single/OLSR-IPv6-HOWTO/images/802-11.png

- . O conjunto de BSSs em uma mesma área forma o *Extended Service Set*, que permite a intercomunicação de APs, para trocar dados entre estações de suas respectivas BSSs, encaminhando as informações, para que sigam as estações móveis de uma BSS para a outra, além de permitir o acesso a um sistema de distribuição de informações, permitindo o contato com redes externas. O ESS esconde a rede sem fio de equipamentos conectados a redes externas, já que estas vêem suas

estações como um único bloco, munido de um único endereço MAC – o do ESS –, permitindo a comunicação de redes fixas com as redes wireless.

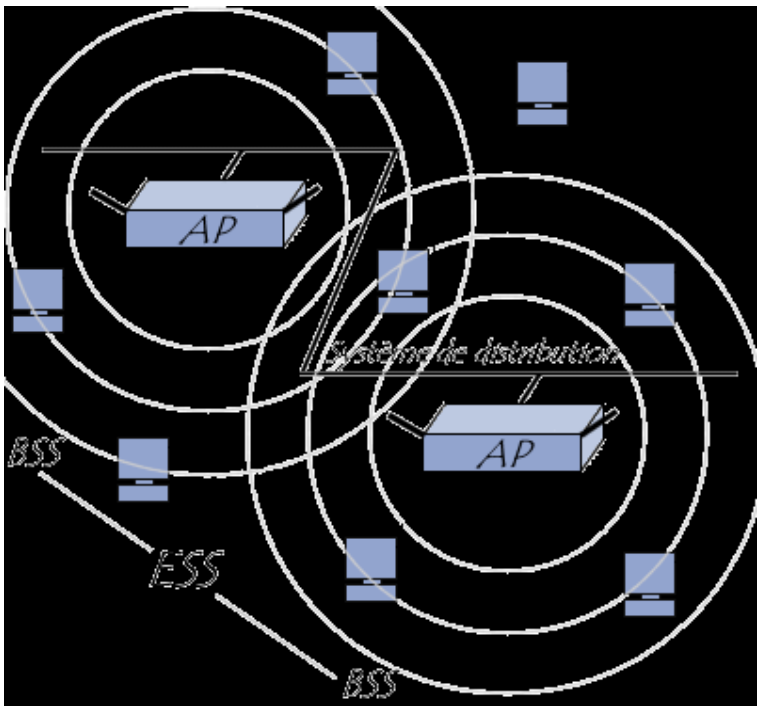

Figura 3 – Arquitetura ESS

Fonte: http://www.pckado-pro.com/e-marketing/wifi/images/essid.gif

A utilização de redes sem fio cresce rapidamente, devido a sua conveniência e facilidade para instalação. É possível encontrar áreas Wi-fi gratuitas. Há, todavia, questões de segurança importantes, já que estas redes utilizam sinais de rádio para a comunicação, e qualquer pessoa com um mínimo de equipamento poderá interceptar os dados transmitidos por um cliente da rede sem fio (como notebooks e PDAs). O problema aumenta, quando não há administradores de rede, como é o caso de redes domésticas: os usuários distribuem sua conexão de Internet para toda a casa sozinhos, simplesmente conectando o cabo de rede a um AP, sem maiores cuidados com segurança, criando uma rede wireless vulnerável, já que muitas vezes a deixam sem senha.

O direito à privacidade de informações é um direito fundamental da pessoa humana, podendo ser encontrado na inviolabilidade da intimidade – art. 5º, X, CF – e do sigilo de correspondência – art. 5º, XII. Atualmente, uma das principais vias de trocas de informações é a rede mundial de computadores, que permite conversas com familiares e amigos, correspondências, compras e até acessos a contas bancárias. Já foi apresentado que as redes wireless apresentam grandes falhas de segurança. Como, então, podemos garantir este direito fundamental? Questões que envolvam a segurança da Internet em si não são objeto de estudo deste trabalho.

Precisamos analisar dois aspectos: a vulnerabilidade do usuário da rede, e a vulnerabilidade da rede propriamente dita. É essencial considerar que uma WLAN disponível através de *hotspots* em shoppings, por exemplo, é uma pública e, portanto, os computadores a ela conectados estarão expostos a ameaças. Para evitá-los, o cliente pode tomar medidas simples, como:

- instalar um *firewall* pessoal - programa que controla o tráfego na rede, impedindo o alastramento de dados nocivos;
- instalar e manter atualizado um bom programa antivírus;
- atualizar as assinaturas do antivírus diariamente;
- aplicar as últimas correções em seus softwares (sistema operacional, programas que utiliza, etc.);

- desligar compartilhamento de disco, impressora, etc.
- desabilitar o modo *ad-hoc* – comunicação direta entre computadores –, cuja utilização deve ocorrer apenas se for absolutamente necessária.
- sempre que possível usar WEP (*Wired Equivalent Privacy*), que permite criptografar o tráfego entre o cliente e o AP. Verificar junto ao administrador de rede se o WEP está habilitado e se a chave é diferente daquelas que acompanham a configuração padrão do equipamento. O protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;
- verificar com o provedor de rede sem fio sobre a possibilidade de usar WPA (*Wi-Fi Protected Access*) em substituição ao WEP, uma vez que este padrão pode aumentar significativamente a segurança da rede. Esta tecnologia inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário. Mesmo que o equipamento seja mais antigo, é possível que exista uma atualização para permitir o uso de WPA;
- considerar o uso de criptografia nas aplicações, por exemplo, o uso de PGP – *Pretty Good Privacy* – para o envio de e-mails, SSH – *Security Shell* – para conexões remotas ou ainda o uso de redes de comunicação privadas - VPNs;
- evitar o acesso a serviços que não utilizem conexão segura, ao usar uma rede sem fio em local público. dê preferência a serviços que usem criptografia;
- habilitar a rede sem fio somente quando for usá-la e desabilitá-la após o uso. Algumas estações de trabalho e *notebooks* permitem habilitar e desabilitar o uso de redes sem fio através de comandos ou botões específicos. No caso de *notebooks* com cartões PCMCIA – *Personal Computer Memory Card International Association* –, inserir o cartão apenas quando for usar a rede e retirá-lo ao terminar de usar.

Quando se instala uma rede sem fio doméstica, é preciso lembrar que a responsabilidade sobre a segurança é de quem instala. É preciso ter em mente que, dependendo da potência da antena de seu AP, sua rede doméstica pode abranger uma área muito maior que apenas a da sua casa. Com isto sua rede pode ser utilizada sem o seu conhecimento ou ter seu tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da sua casa, utilizando programas simples, como *sniffers*. Felizmente, os programas de instalação destes APs já apresentam uma interface de fácil manuseio pelo usuário, que poderá aumentar a segurança de sua rede através de alguns cliques. Enunciaremos, agora, algumas destas medidas, recomendadas pelo Comitê Gestor da Internet no Brasil, e disponibilizadas em forma de cartilha on-line para todos os cidadãos, no site http://cartilha.cert.br/ (CERT.BR):

- mudar configurações padrão que acompanham o seu AP. Alguns exemplos são:

  – alterar as senhas

  – alterar o SSID (*Server Set ID*);

  – desabilitar o *broadcast* – envio para toda a rede – de SSID;

- – permitir que um computador se conecte ao AP para alterar as configurações apenas através da rede cabeada, se esta opção estiver disponível. Desta maneira um possível atacante externo (via rede sem fio) não poderá acessar o AP diretamente para promover mudanças na configuração. Verificar a documentação do AP sobre como efetuar estas mudanças, caso estejam disponíveis;
- verificar se seus equipamentos já suportam WPA (*Wi-Fi Protected Acc*ess) ou WPA2, e utilizá-lo sempre que possível. Esta tecnologia é mais recente e inclui melhorias em relação ao protocolo WEP para prover uma segurança adicional contra acesso e escuta de tráfego não autorizada. Lembre-se que atualizações para WPA estão disponíveis para a maior parte dos equipamentos mais antigos.
- caso o WPA não esteja disponível, usar sempre que possível WEP, para criptografar o tráfego entre os clientes e o AP. Vale lembrar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;

- se for utilizar WEP, trocar as chaves que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- desligar seu AP quando não estiver usando sua rede.

É importante lembrar que as chaves criptográficas apresentadas – WEP, WPA e WPA2 – devem ser vistas como mais uma precaução, já que *hackers* já conseguiram quebrá-las. Há outras medidas de segurança wireless, mas, por essas exigirem conhecimento de administração de redes, não serão discutidas neste trabalho, que se volta ao cidadão comum. É importante lembrar que, ao comprar qualquer aparelho que permita o acesso wireless, o consumidor deve ser informado tanto pela loja quanto pelo fabricante sobre os riscos a que se sujeitará.

5. DIREITO À SAÚDE E PESQUISAS CIENTÍFICAS: CONSIDERAÇÕES DA OMS SOBRE RÁDIO-FREQÜÊNCIA

No início dos anos 70, a Organização Mundial da Saúde – OMS – reconheceu a necessidade de esforços coordenados para desenvolver esforços quanto a medidas protetivas para radiação não-ionizante. Documentos foram criados, mas pode ser surpreendente que a maior parte dos problemas apontados nestes ainda não foram resolvidos e isto – apesar dos estudos dos fenômenos terem-se globalizado – mostra que ainda há pouco entendimento sobre os mecanismos básicos de interação entre os campos eletromagnéticos e o organismo. Em 1993, outro grupo de estudos da OMS preparou critérios de saúde ambiental para capôs eletromagnéticos de 300Hz a 300GHz. Apesar de manter algumas partes dos documentos antigos, este desenvolveu totalmente e utilizou o conceito de SAR – taxa específica de absorção de energia – para a demarcação de limites de exposição nas faixas de alta freqüência, seguindo inclusive os conceitos do Instituto de Engenheiros Elétricos e Eletrônicos – IEEE – publicados em 1992 e, apesar da recomendação da ONU de que a SAR sozinha não pode ser usada para a o entendimento de efeitos biológicos de uma freqüência para outra, as propostas de precaução feitas em documentos anteriores foram esquecidas. Foi criada a Comissão Internacional para proteção contra radiação não-ionizante – ICNIRP –, que publicou em 1998 um documento influente trazendo passos para limitar a exposição a campos elétricos, magnéticos e eletromagnéticos que foi, depois, tomada pela Comissão Européia como recomendação para os países membros, apesar de reserves do parlamento da UE. No entanto, há grande variação nos valores de limite aplicados em diferentes países, e se reconhece os esforços para unificação.

Em junho de 2005, a OMS promoveu um workshop sobre estações-base e redes wireless, buscando respostas para os efeitos que a exposição a essa radiação tem nos humanos, e, se existentes, provas dessa influência. As informações que seguem baseiam-se no relatório deste evento (ROY, 2005). Peter Valberg, da Gradient Corporation, esclareceu que a transmissão da informação móvel é feita através da onda central, chamada portadora. Com o avanço da tecnologia, foi necessário mudar a modulação e se especula que isso pode ter um efeito adverso em sistemas biológicos. Uma discussão sobre a energia dos fótons mostrou a improbabilidade de mudanças significativas, contudo aparecem relatórios de pesquisas apresentando efeitos biológicos em baixas proporções, geralmente ligados a efeitos da modulação. Um mecanismo repetitivo, explícito e previsível capaz de produzir respostas biológicas significantes dependentes ou não da modulação, em áreas de RF de baixa freqüência ainda não foi achado, o que encoraja os pesquisadores a continuar examinando protocolos experimentais e a biofísica, em busca de provas d replicação. Em pesquisa feita pelo Chez Federal Institute of. Technology, Niels Kuster chegou a resultados preocupantes: o Wi-fi e o Bluetooth class I se aproximaram aos limites de exposição públicos SAR. O procedimento recomendado para estudos foi a avaliação dosimétrica sob as condições dos piores casos.

É preciso aplicar o princípio da precaução, segundo Eva Marsálek, da Plattform Mobilfunk-Initiativen, Áustria. Ela ressalta uma necessidade de revisão dos limites, já que para todos os poluentes, os limites são distintos para os trabalhadores cujo trabalho implica exposição ao poluente e os outros trabalhadores, que coincidiriam com o público em geral. Apenas quanto a freqüência eletromagnética, os modelos de proteção sugerem os mesmos limites de exposição tanto para os trabalhos envolvidos com a exposição e os outros. Nenhum procedimento de precaução foi aplicado quanto a campos elétricos, magnéticos ou eletromagnéticos, exceto por algumas autoridades locais na Itália e Suíça, enquanto já foi implantados procedimentos de precaução para substâncias que poderia ser perigosas à saúde se incorporadas pela pele, inalação ou ingestão.

A necessidade de aparelhos pessoais PEM capazes de medir a exposição à radiação é discutida em vários fóruns. Os requisitos para um bom PEM incluem ser pequeno, leve e usável como uma roupa, capaz de

medir a exposição em todo o espectro, tendo boa precisão, pois, provavelmente a exposição no ambiente deve ser bem próxima, se não mais baixa que o limite de detecção. Padrões devem ser desenvolvidos internacionalmente e adotados nacionalmente, governos locais não devem impor seus próprios padrões, requisitos impostos para medições são de valor limitado, mecanismos de consulta a nível local devem ser consistentes com outros tipos de infra-estrutura e os processos de marketing devem ser transparentes. É necessária uma autoridade nacional independente, uma separação entre os ministérios da saúde e planejamento, uma aproximação para lidar com a questão de incertezas científicas., para Jack Rowley, da GSM Association na Irlanda.

De acordo com a Constituição Federal do Brasil, o Direito à Saúde faz parte dos Direitos Sociais, e exige ações estatais para garanti-los. No entanto, a necessidade de ações globais para definir modelos e esforços conjuntos para pesquisas não deve ser vista como empecilho, mas incentivo para cientistas brasileiros, que, observando as melhores experiências ocorridas no exterior, poderão gerar um "modelo brasileiro" aproveitando as melhores partes de outros, como ocorreu com a TV Digital. Este aspecto ressalta também a exigência da inserção do Brasil de modo uniforme neste quadro de cooperação internacional, já que vários de nossos pesquisadores foram citados nos trabalhos apresentados neste fórum.

6. CONSIDERAÇÕES FINAIS

A relação entre o Direito e as Tecnologias de Informação não requer, obrigatoriamente, a normatização, mas a adaptação do profissional às novas demandas existentes na sociedade. Para fazer uma interpretação bem feita da lei, é necessário conhecer os fatos, e isto inclui atualizações sobre as tecnologias e os novos problemas que surgem. Aplicar os princípios jurídico-constitucionais na análise destas é uma forma de conhecer as características desses novos processos e observar, de maneira objetiva, seus pontos fortes e fracos.

As redes wireless, a nosso ver, conseguem superar as desvantagens, devido aos novos horizontes que traçam: a mobilidade e a difusão do acesso a Internet em áreas sem prévia infra-estrutura é essencial para a inclusão digital e para a manutenção da democracia, já que pode ser usada como um instrumento eficaz da democracia participativa, através do governo eletrônico e da democracia digital.

As redes Wi-Fi apresentam, como qualquer novo instrumento, problemas, mas que podem ser resolvidos através da informação do seu público usuário sobre como evitá-los. Pesquisas científicas existem, mas são pouco divulgadas, e esta tecnologia vira um modismo, que pode gerar danos, já que aspectos como saúde e segurança são negligenciados. Cabe, aqui, lembrar que a adequação da infra-estrutura à necessidade do cliente deve obedecer a critérios técnicos de projetos de rede, avaliando, assim, as situações em que a utilização do Wi-Fi é realmente vantajosa.

REFERÊNCIAS

ANATEL. **Detalhes da Lei Geral das Telecomunicações**: banco de dados. Disponível em <http://www.anatel.gov.br/biblioteca/Leis/LeiGeral/leigeral.asp> . Acessado em 01 abr 2007

_____. **Wireless**: banco de dados. Disponível em: <http://www.anatel.gov.br/pesquisa/resultadobuscanova.asp> . Acesso em 30 mar 2007

[CETIC.BR, 2006] CETIC.BR TIC Domicílios e Usuários 2006. Disponível em <http://www.cetic.br/usuarios/tic/2006/> Acesso em 15 dez 2006

CERT.BR CERT.BR. Redes de Banda Larga e Redes sem Fio. In: CERT.BR **Cartilha de Segurança para a Internet**.versão 3.1. Disponível em <http://cartilha.cert.br/> . Acessado em 15 dez. 2006

[DELGADO, 2007] DELGADO, Maurício Godinho. **Curso de Direito do Trabalho**. 6ª edição. São Paulo: LTr, 2007

INTELLIGRAPHICS. **Introduction to IEEE 802.11**. Disponível em: <http://www.intelligraphics.com/articles/80211_article.html>. Acesso em 01 abr. 2007

JACQUES, Robert: **Experts warn of WiMAX security holes**. Disponível em http://www.vnunet.com/vnunet/news/2172121/experts-warn-wimax-security. Acessado em 4/03/07

MARTIN, Henrique: **Intel testa WiMAX em Brasília**. Disponível em http://www.rnp.br/noticias/imprensa/2004/not-imp-040916.html. Acessado em 4/03/07

MORAES, Alexandre de. **Direito Constitucional**, 19ª edição. Ed. Atlas S.A., São Paulo, 2006

[ROVER, 2006] ROVER, Aires José. A Democracia Digital: Algumas Questões de Base, **Revista de Direito das Novas Tecnologias**, São Paulo, IOB e IBDI: 1, jan - jun 2006, p.69

[ROY, 2005] ROY, Collin. **Rapporteur's report of Workshop on Base Stations and Wireless Networks**. Suiça: WHO International EMF Project, 2005. Disponível em <http://www.who.int/peh-emf/meetings/base_stations_june05/en/index.html>. Acesso em 15 jan 2007

STF. **A Constituição e o Supremo**. Disponível em <http://www.stf.gov.br/legislacao/constituicao/pesquisa/constituicao.asp> Acessado em 01 abr 2007