Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

# A Tecnologia de Identificação por Radiofreqüência e seus Riscos à Privacidade

Rodrigo Otávio Ribeiro Hagstrom

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação – Licenciatura

Orientadora
Prof.ª Cláudia Nalon

Brasília
2008

Universidade de Brasília – UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Curso de Computação – Licenciatura

Coordenador: Prof. Flávio Leonardo Cavalcanti de Moura

Banca examinadora composta por:

Profª. Cláudia Nalon (Orientadora) – CIC/UnB
Prof. Pedro Antonio Dourado de Rezende – CIC/UnB
Prof. Ly Freitas Filho – CIC/UnB

**CIP – Catalogação Internacional na Publicação**

Hagstrom, Rodrigo Otávio Ribeiro.

A Tecnologia de Identificação por Radiofreqüência e seus Riscos à Privacidade / Rodrigo Otávio Ribeiro Hagstrom. Brasília : UnB, 2008.
54 p. : il. ; 29,5 cm.

Monografia (Graduação) – Universidade de Brasília, Brasília, 2008.

1. privacidade, 2. identificação, 3. radiofreqüência, 4. direito civil e penal, 5. legislação.

CDU 004

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro – Asa Norte
CEP 70910–900
Brasília – DF – Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

# A Tecnologia de Identificação por Radiofreqüência e seus Riscos à Privacidade

Rodrigo Otávio Ribeiro Hagstrom

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação – Licenciatura

Profª. Cláudia Nalon (Orientadora)
CIC/UnB

Prof. Pedro Antonio Dourado de Rezende
CIC/UnB

Prof. Ly Freitas Filho
CIC/UnB

Prof. Flávio Leonardo Cavalcanti de Moura
Coordenador do Curso de Computação – Licenciatura

Brasília, 12 de junho de 2008

# *Agradecimentos*

À minha Orientadora e Professora Cláudia Nalon pela paciência e compreensão durante a execução deste trabalho. Muito Obrigado.

Aos demais professores que tive ao longo de minha graduação na UnB, de diversos departamentos, como Educação, Engenharia Mecânica, Física, Matemática, Estatística, Linguas Estrangeiras, Ciência da Computação, entre outros. Destaco alguns nomes: Célius Antônio Magalhães, Xia Chang Yu, Carla Denise Castanho, Priscila América Solís Barreto, Aline Gomes da Silva Pinto, Mansour Rastegar Fasaei, Pedro Antônio Dourado de Rezende. Há muitos outros nomes aqui não presentes que igualmente participaram minha formação; minha pequena homenagem aos meus professores.

Aos meus colegas da universidade, em especial ao meu colega Reinaldo Araújo Barreto Júnior; meu sincero abraço e desejo de sucesso.

Aos colegas da Anatel, especialmente da Assessoria de Relações com os Usuários.

À minha mãe, Júnia, e minhas irmãs, Cynthia Risia e Fabiana Cristina, por seu apoio no dia-a-dia durante toda a minha vida. Ao meu primo Daniel Filho.

Ao meu Deus, por tudo que citei aqui. Muito Obrigado.

> *"Enriquecidos da plenitude da inteligência, para conhecimento do mistério de Deus - Cristo, em quem estão escondidos todos os tesouros da sabedoria e da ciência."* (Epístola aos Colossenses 2:2 e 3).

*In Memorian, Josias Ribeiro* (avô materno).

# *Resumo*

A tecnologia de Identificação por Radiofreqüência, que utiliza sinais de rádio para a comunicação entre etiquetas eletrônicas com um leitor de identificação computadorizado, não possibilita apenas identificar qualquer objeto ou ser, mas também possibilita o rastreamento de diversas informações sobre a vida privada das pessoas, uma vez que os sinais de rádio transmitidos por etiquetas eletrônicas nem sempre são rastreados com o conhecimento do cidadão.

A falta de regulamentação legal do direito de privacidade, principalmente frente ao desenvolvimento das tecnologias, incluindo a Identificação por Radiofreqüência, oportuna o abuso contra os direitos de personalidade do cidadão. A legislação brasileira, que constitucionalmente protege esse direito de privacidade, não especifica, entretanto, os detalhes necessários ao correto julgamento das violações deste direito. O direito brasileiro acaba entregando os julgamentos de privacidade à subjetividade das autoridades judiciárias.

Urge então o estabelecimento de normas capazes de proteger a privacidade quanto ao uso da Identificação por Rádiofreqüência, por meio do envolvimento do Estado, dos operadores e representantes dos cidadãos, restabelecendo os limites entre o que é vida privada e o que é vida pública. Acabar-se-á protegendo os direitos básicos do cidadão conforme as noções de democracia e direitos individuais conquistados recentemente no Brasil, se ocorrer uma análise cuidadosa do alcance de tal tecnologia e o estabelecimento de uma legislação capaz de coibir os abusos contra os direitos individuais, principalmente o de privacidade.



**Palavras-chave:** privacidade, identificação, radiofreqüência, direito civil e penal, legislação.

# *Abstract*

The Radio Frequency Identification technology, which basically comprises the communication between eletronic tags and a computer-based scanner, allows not only for the identification of objects and individuals but also for tracking information related to the private life of those individuals who are either themselves tagged or carrying tagged objects. This may happen because the radio signals which are transmitted by electronic tags can be tracked without the knowledge of the individual.

In face of recent developments and uses of technologies, including the Radio Frequency Identification technology, the lack of a specific norm about privacy may cause abuse of civil rights. By one hand, the Brazilian laws have shown some concerns about the right of privacy. By the other hand, however, this legislation has not provided specific details on how the violation of such rights should be addressed. As such, the Brazilian legislation allows a subjective understanding and judgement of the matter.

The new developments in techonology urge the stablishment of norms and laws to protect the citizen's privacy. It is even more urgent in the case of technologies which are already widely spreaded, as the Radio Frequency Identification. In order to stablish those norms, the government, operators and controllers of systems based in such technology, as well as citizen's representatives should be involved in this process. The main goal is to defining the limits between private and public life. After careful analisis of how this technology can affect the citizens, it is possible to stablish norms that prevent the abuses of the civil rights, specially the right of pivacy. Such norms are desirable since they end up by protecting the basics rights of their citizens, according to the democratic rights and civil liberties which have been recently acquired in this country.



**Keywords:** privacy, identification, radiofrequency, civil rights, law.

# *Sumário*

# *Lista de Figuras*

# Capítulo 1

# Introdução

Diante do surgimento contínuo e cada vez mais rápido de novas aplicações das tecnologias computacionais, o atendimento das demandas humanas deve ter prioridade sobre as possíveis aplicações de qualquer ferramenta. Por isso, a manutenção do respeito aos direitos da pessoa humana deve ser defendida tanto por meios tecnológicos como por meio da ciência jurídica. O respeito aos direitos individuais passa pelo respeito ao direito de privacidade. A privacidade, entretanto, encontra-se cada vez mais ameaçada. Internet, telefones celulares, radiotransmissores, tudo isso que se encontra cada vez mais presente nas atividades humanas pode ser usado para quebrar o direito de privacidade.

Dentre as tecnologias capazes de facilitar a exposição da vida privada de um cidadão está a Identificação por Radiofreqüência, que, como veremos no Capítulo 2, é uma tecnologia resultante da junção da velha tecnologia do rádio com a tecnologia da computação moderna. Serão apresentadas a capacidade que esta tecnologia possui e as aplicações que pode encontrar em segurança, finanças, gestão de negócios, entre outros.

No Capítulo 3 será mostrado, porém, que, como toda tecnologia, a Identificação por Radiofreqüência tem seus reveses. Será exposto como esta tecnologia pode proporcionar a quebra de privacidade dos cidadãos e como isto poderia ocorrer em várias formas de aplicação desta tecnologia.

Mas saber como a Identificação por Radiofreqüência pode quebrar a privacidade é inútil se não se utilizar esta informação para defender os direitos do cidadão. Com este objetivo, os Capítulos 4 e 5 analisam o que já existe na legislação para proteger a privacidade e apresentam algumas sugestões para auxiliar a criação de uma possível lei específica sobre a Identificação por Radiofreqüência, informando quais destes pontos já estão elencados em legislações a serem votadas no Congresso Nacional.

O objetivo do presente trabalho é principalmente demonstrar que a disseminação de novas tecnologias deve ser antecipada pela compreensão dos impactos sociais que esta tecnologia causa, incluindo os impactos nos direitos do cidadão. Propõe-se que e legislação nacional proteja, frente ao desenvolvimento da tecnologia de informação, os direitos civis fundamentais e democráticos, principalmente os individuais. Deve-se direcionar os profissionais da computação a utilizar a tecnologia e o conhecimento de suas

capacidades como ferramentas de proteção do estado democrático e dos direitos individuais.

O que motivou a presente análise foi a observação de que a tecnologia de Identificação por Radiofreqüência já vem sendo aplicada no Brasil sem que a população esteja ciente das implicações de seu uso em termos de responsabilidade sobre cessão de direitos de privacidade. O método utilizado foi o de análise bibliográfica de artigos, teses e palestras, bem como da legislação existente no Brasil e no exterior sobre o tema.

Espera-se que o trabalho contribua a análises críticas quanto ao uso disseminado de novas tecnologias, bem como as formas de sua implementação no cotidiano social.

# Capítulo 2

# A Tecnologia de Identificação por Radiofreqüência

A melhor forma de começar este estudo é entender o que é a tecnologia de Identificação por Radiofreqüência, também conhecida pela sigla RFID (do inglês *Radio Frequency Identification*), que é tida como solução para diversos problemas de identificação de objetos e de identificação pessoal, especialmente no que concerne à autenticação e confiabilidade do ente identificado.

De acordo com (Lockton e Rosenberg 2005), a RFID, no modo como é conhecida hoje, é atribuída ao trabalho de Charles Walton, que em 1973 patenteou um sistema com etiquetas eletrônicas e leitores. A pesquisa sobre a RFID é baseada na necessidade de identificar um objeto remoto. Um objeto pode ser reconhecido e identificado à distância, utilizando-se ondas de rádio que transmitem dados de identificação. Antes, entretanto da concessão da patente a Walton, a RFID já havia sido abordada em pesquisas militares durante a Segunda Grande Guerra. Durante a Segunda Guerra Mundial, os radares, que já eram capazes de informar a presença de aeronaves, não podiam, porém, identificar se estas aeronaves eram Aliadas ou do Eixo. Para solucionar este problema, foram colocados *transponders* nos aviões aliados. *Transponder* é um dispositivo que transmite um sinal específico do equipamento a ser identificado. Este sinal é capaz de informar qual é o avião detectado e qual sua localização, também por meio de ondas analógicas de rádio. Atualmente, a RFID é utilizada em aplicações não concebidas inicialmente pela Real Força Aérea Britânica

A RFID é uma forma de etiquetar eletronicamente qualquer objeto ou mesmo ser vivo. No ente a ser identificado é colocada uma etiqueta eletrônica, da qual são transmitidos os códigos de identificação. Geralmente este sinal consiste em números de identificação do objeto previamente configurados no sistema de identificação (Lockton e Rosenberg 2005). De fato, a tecnologica para RFID é bastante simples, sendo constituída de dois componentes básicos: uma etiqueta e um leitor. A etiqueta, geralmente um microprocessador, consiste de um circuito integrado, que armazena dados, e de uma antena transmissora. O leitor, também conhecido como *scanner*, possui uma antena receptora e transmissora de dados; um demodulador,

que é responsável por transformar o sinal analógico de rádio em informações digitais; e o processador de informações, que irá lidar com os dados recebidos do objeto e verificar sua autenticidade (Lockton e Rosenberg 2005). A Figura 2.1 exibe um esquema gráfico com os componentes básicos. Alguns autores defendem que o leitor não deve ser assim chamado, uma vez que ele é a base do sistema. Do leitor são emitidos comandos para as etiquetas responderem; assim, para este segmento de autores, o leitor deveria ser chamado de estação base ou interrogador (Dominique 2005).

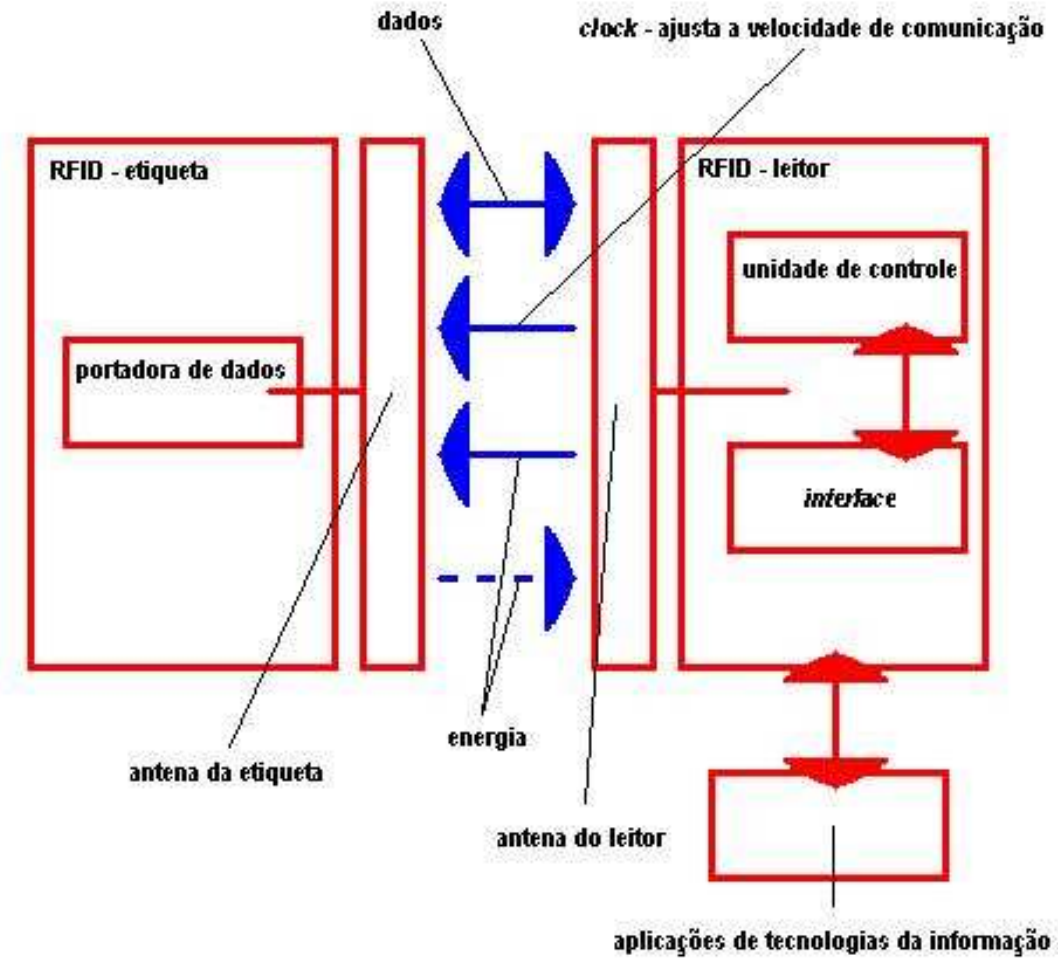


Figura 2.1: Componentes da Identificação por Radiofreqüência

O formato de etiquetas eletrônicas é bem variado. Podem ser colocadas em cartões, invólucros de plástico ou vidro e até mesmo cédulas de papel.

Em relação à presença (ou não) de fonte de energia, as etiquetas são classificadas como *passivas* ou *ativas*. A etiqueta passiva não possui fonte própria de energia. Isso a torna mais barata e prolonga sua vida útil. O sinal de resposta produzido por este tipo de etiqueta consiste apenas do reenvio da onda recebida pelo leitor. Em conseqüência, sua distância em relação ao aparelho leitor não pode ser muito grande, fazendo com que este tipo de

etiqueta seja eficiente em distâncias reduzidas, geralmente menores que 10 metros. Já as etiquetas ativas possuem fonte própria de energia, o que faz com que transmita dados ininterruptamente, permitindo ainda identificação a distâncias maiores, inclusive acima de 100 metros de distância. Uma etiqueta destinada apenas a responder aos comandos enviados pelo leitor é chamada de *transponder*, (do inglês *transmitter - responder*). Se, por outro lado, a etiqueta também for capaz de emitir informações, ela é chamada *transceiver* (do inglês *transmitter - receiver*).

Outra forma de classificação das etiquetas é entre aquelas com ou sem processador. O processador permite a reescrita de dados, possibilitanto a alteração de informações mesmo após o etiquetamento. Esse recurso não é encontrado em etiquetas sem processador.

As etiquetas podem ainda ser classificadas quanto à freqüência de operação das ondas de rádio utilizadas no sistema. Etiquetas que utilizam ondas de baixa freqüência (entre 30 e 500 KHz) trabalham com alcance mais curto, ao passo que etiquetas eletrônicas de alta freqüência (entre 850 e 950 MHz e entre 2,4 e 2,5 GHz) possuem a capacidade operar a distâncias maiores (Bernardo 2004).

Diversos setores têm demonstrado interesse pela RFID. A pecuária, por exemplo, encontra na RFID uma maneira eficiente para rastrear o seu produto nas diversas fases de produção, monitorando desde as cabeças de gado no campo até peças de carne e produtos vendidos no mercado varejista (Lockton e Rosenberg 2005). Os grandes grupos do mercado varejista também encontram nesta tecnologia uma solução para melhorar os controles de estoques e do fluxo de mercadorias. O interesse destes grupos é devido ao fato de que a etiqueta permite o controle de um produto desde sua fabricação até o fim de sua vida útil (Bernardo 2004). Este controle permite que a loja seja capaz de observar, por exemplo, os prazos de validades dos produtos, momentos adequados de reposição, redução de estoques, alterações no fluxo de mercadorias e até mesmo como sistema anti-furto de pequenas mercadorias. Nestes casos de combate ao furto com uso de RFID, observa-se o interesse da Gillete, que chegou a solicitar o etiquetamento de seus produtos.

O caso mais conhecido de interesse do setor varejista foi o do Wal-Mart. Este grupo chegou a demandar, em junho de 2003, que seus produtos estivessem equipados com etiquetas eletrônicas até janeiro de 2005. O empecilho ao cumprimento desta demanda, entretanto, não se encontrava nos fabricantes de produtos comercializados no varejo, mas sim nos fabricantes de etiquetas eletrônicas que não se encontravam preparados para a produção de um bilhão de etiquetas. O Wal-Mart acabou não vendo a implementação de tais dispositivos na escala esperada, mas acabou por gerar estudos que podem reduzir o preço do etiquetamento eletrônico de 25 a 50 centavos de dólar por etiqueta para 5 a 10 centavos de dólar. Além disso, gerou-se uma expectativa acerca desta tecnologia, o que impulsionou os estudos acerca da RFID.

Os fabricantes de etiquetas possuem um mercado potencial bem vasto (Cavoukian 2006). Em verdade, não só a logística deste mercado é benefici-

ada, mas também o atendimento ao cliente. No caso dos códigos de barras utilizados hoje, só é permitido o cômputo de um produto por vez. Com a RFID, o leitor é capaz de computar e identificar vários produtos por vez, o que tenderia a diminuir ou até mesmo acabar com as filas em caixas de supermercados.

Em comparação com o código de barras hoje adotado, há ainda outras vantagens da RFID. O código de barras no modelo atual não permite que cada produto seja individualmente etiquetado devido à quantidade de informações que o código pode guardar. Na etiqueta eletrônica pode ser armazenada maior quantidade de informações, o que permite, por exemplo, que uma garrafa de Coca-Cola tenha um código diferente de outra garrafa do mesmo produto. Isto se deve ao fato que mesmo etiquetas mais simples podem guardar entre 96 e 128 bits de informações. Além disso, como as ondas de rádio não dependem de luz para trafegar, estoques empoeirados ou sem luz podem ser monitorados sem maiores dificuldades.

Analisando outras aplicações, as etiquetas podem ser ainda hoje encontradas na aviação, praticamente da mesma forma em que surgiram durante a Segunda Guerra. Hoje é obrigatório no mundo inteiro que os aviões sejam fabricados com *transponders* capazes de informar ao controle de vôo seu posicionamento e sua identificação. Entretanto, uma nova aplicação pode estar surgindo na aviação. A Boeing sugere que a RFID pode aumentar a eficiência na montagem de aviões se as peças estiverem equipadas com etiquetas RFID (Bernardo 2004). Ainda no campo da aviação, há a sugestão de etiquetamento eletrônico de bagagens e cargas despachadas para aumentar a eficiência no seu controle e identificação, evitando perdas e extravios.

Um uso já bastante disseminado da RFID é a identificação de animais. Além da já citada identificação de cabeças de gado, há também o caso português em que a legislação exigiu que cães de estimação fossem identificados e catalogados com a RFID para controle de informações sobre a raiva (Lockton e Rosenberg 2005). Não raro institutos de preservação e monitoramento da fauna etiquetam eletronicamente espécimes em extinção para controle populacional e estudo comportamental destas espécies. No Distrito Federal, desde setembro de 2007, etiquetas eletrônicas têm sido implantadas em cavalos, com um outro fim: localizar animais envolvidos em acidentes e, possivelmente, responsabilizar seus donos por danos materiais causados (Secom GDF 2007).

Na indústria automobilística, a RFID tem sido usada para o monitoramento de veículos em pedágios e também para a identificação mais precisa de chaves de partida (Lockton e Rosenberg 2005; Cavoukian 2006). São estas chaves com processadores que têm permitido uma redução em furtos de veículos. Empresas de segurança de veículos também utilizam identificação remota para encontrar veículos que eventualmente sejam furtados. Empresas que controlam pedágios já utilizam o sistema para o faturamento dos usuários (Cavoukian 2006). A Michelin, fabricante de pneus, pretende etiquetar seus produtos, o que faz com que não apenas o veículo, mas também seus componentes possam estar etiquetados eletronicamente em breve.

O uso da RFID para identificação pessoal também já é corrente. As etiquetas eletrônicas em cartões de identificação dentro de empresas e outras instituições não são novidade. A novidade na área de identificação pessoal é o uso de microprocessadores de identificação de humanos na forma como já vem sendo feita em animais, ou seja, a partir de implantes. Os processadores implantados podem ser usados para a própria identificação pessoal e para a segurança do implantado, por exemplo, como parte de sistemas anti-seqüestro (Reinaldo Filho 2006).

Para uso médico, conforme (Reinaldo Filho 2006), a etiqueta eletrônica auxilia na identificação instantânea do paciente e permite um acesso rápido ao seu histórico. Permite ainda que pacientes que necessitem de monitoramento constante sejam assim assistidos. Como exemplo, pacientes com doenças mentais ou que afetam a memória podem ser mantidos sob vigilância. Em outra aplicação médica, o sistema seria capaz de reduzir os erros de identificação de pacientes em hospitais (Crawford et al. 2003). Entretanto, nem todas estas aplicações necessitam que a etiqueta eletrônica esteja implantada no paciente. Há pulseiras e cartões de identificação que, em seu modo de funcionamento, não são diferentes das etiquetas implantadas (Smith et al. 2005).

Analisando agora algumas outras aplicações em ambientes abertos, a RFID permite ainda que o sistema seja utilizado para a detecção de atividades do indivíduo portador da etiqueta (Smith et al. 2005). É possível utilizar a RFID para o monitoramento de criminosos, dentro ou fora de penitenciárias. Outras pessoas a serem monitoradas seriam crianças, que se desaparecidas, seriam então mais rapidamente encontradas. Este serviço de monitoramento de crianças já existe em outras formas; entretanto, na forma de implante, teria a vantagem da etiqueta não poder ser removida facilmente.

Deve-se destacar porém que aplicações em ambientes fechados ou abertos dependem da instalação da infra-estrutura necessária à leitura. O monitoramento de ambientes abertos, como ruas ou campo, pode estar limitado pela eficiência do alcance de leitura. Dependendo da freqüência do sistema, esta infra-estrutura pode ter um custo limitador para a implementação do sistema de identicação.

O sistema de identificação por rádio já pode ser encontrado também em cartões inteligentes, conhecidos pelo nome em inglês *smart cards*. Neste caso, a RFID permite que o cartão possa ser operado sem contato físico com o terminal de cartões, realizando assim uma operação de compra e venda auxiliada pela identificação remota (Matos 2003). Estes mesmos cartões inteligentes também podem ser utilizados em uma série de sistemas de identificação. A junção dos conceitos de cartões inteligentes com a RFID possibilita um sistema onde não apenas os produtos comprados estejam eletronicamente etiquetados, mas o próprio consumidor também o esteja. Uma grande vantagem é que os cartões inteligentes podem guardar até 72 Kb de informações (Lockton e Rosenberg 2005). Assim, pode-se visualizar que a RFID permitiria que, num futuro próximo, os cartões inteligentes pudessem ser implantados em humanos, uma vez que isso poderia auxiliar na

solução para perdas, roubos e danos aos cartões. Em verdade, a tecnologia dos cartões inteligentes permite que um mesmo cartão seja utilizado para várias aplicações que exijam identificação e autenticação pessoal, inclusive via internet, como documento, ou ainda em sistemas de cobranças, como é feito hoje com cartões de crédito ou de débito em conta. Seria o início do fim dos documentos em papel e dos cartões, já que se teria disponível um cartão múltiplo inteligente implantável.

Um fato interessante na área financeira é que mesmo com a tendência de redução do número de cédulas de papel, devido ao crescimento do uso de cartões, o Banco Central Europeu chegou a sugerir o etiquetamento eletrônico de cédulas de Euro.

Alguns obstáculos têm sido encontrados na implementação da RFID. Primeiro, o preço da etiqueta ainda é proibitivo para algumas aplicações. O fato é que não basta avaliar o preço da etiqueta, mas também da infraestrutura computacional e eletrônica que o sistema demanda. Ainda há de se considerar o preço do custo operacional por produto ou ente etiquetado. Por exemplo, se o produto etiquetado for um *laptop*, o custo de 20 centavos de dólar por etiqueta é baixo, mas é extremamente alto se o produto etiquetado for uma caixa de leite ou um pacote de biscoitos (Bernardo 2004). As pesquisas em torno da RFID têm por objetivo a redução do preço por etiqueta e redução dos demais custos, mas é fato que estes ainda permanecem elevados.

Como outro obstáculo, a RFID utiliza ondas de rádio, um recurso escasso, já que as faixas do espectro ondulatório se encontram cada vez mais congestionadas e são limitadas. Assim, há a necessidade de regulamentação das faixas do espectro a serem utilizadas para a RFID. A utilização de ondas do espectro depende também de uniformização e normatização, já que boa parte dos produtos e entes a serem eventualmente etiquetados trafegam entre diferentes países e regiões. Como nem todos os países utilizam de forma semelhante as faixas de freqüências do espectro, isto poderia eventualmente gerar dificuldades técnicas para a implementação mais ampla da RFID (Bernardo 2004). Cabe ressaltar que o comércio internacional é uma das áreas a se beneficiar muito da RFID, reduzindo-se assim o contrabando e o tráfico de muitos produtos.

Uma área de estudos onde a RFID será indispensável é a computação pervasiva (Bolzani 2003). A computação pervasiva consiste na construção das chamadas *smart houses*, as casas inteligentes. Objetiva-se que eletrodomésticos, além da própria casa, sejam capazes de reconhecer e atender o usuário sem que este necessariamente tenha de acionar uma porta ou fogão por meio de fechaduras ou botões. Por exemplo, a aproximação do morador seria suficiente para abrir uma porta de casa ou da geladeira. Como o usuário estaria identificado por meio de RFID, o ambiente seria capaz de reconhecê-lo e por meio de seus padrões comportamentais até mesmo atendê-lo sem que ele acione, por exemplo, a lavadora de roupas. O sistema de casas inteligentes seria capaz também de atender a comandos do usuário, como comando de voz e botões.

Por fim, a RFID poderia trazer à realidade, em um futuro próximo, um

sistema de identificação capaz de integrar diversas áreas, como identificação e autenticação pessoal, sistemas de cobrança, comércio de produtos, sistemas de segurança, entre outros, tornando-se, desta forma, uma ferramenta que colaboraria para a obtenção maior eficiência nas atividades humanas que exijam algum tipo de identificação.

# Capítulo 3

# Como o uso da RFID Ameaça a Privacidade?

Após analisar as possibilidades de usos da RFID deve-se observar os possíveis inconvenientes que uma etiqueta eletrônica pode acarretar. Observando cada aplicação da RFID pode-se facilmente concluir que a privacidade do usuário é fortemente ameaçada.

Privacidade significa vida íntima, ou intimidade (Lima 2005). Mais precisamente, o conceito de privacidade pode ser entendido como aquilo que a pessoa vive individualmente, sem que isso seja dividido com a sociedade ou na vida pública. É na esfera privada que a pessoa exerce então os seus direitos de personalidade. Consiste assim a vida privada como o local onde a pessoa pode manter-se incógnita. Observa-se que o local onde o indivíduo exerce os direitos personalíssimos não se limita apenas à sua casa. O que o indivíduo compra, vende, os locais por onde circula, os indivíduos que o acompanham, o que faz daquilo que lhe pertence, tudo isso pode ser objeto do que uma pessoa considera parte de sua vida privada. Em outras palavras, parte de sua vida que a pessoa gostaria de manter oculta à coletividade.

No entanto, a RFID é capaz de expor muitas das atividades comuns dos indivíduos. Começando pelo uso da RFID como meio de identificação e autenticação pessoal, se a etiqueta eletrônica transmite não apenas a identificação, mas também a localização de um indivíduo, torna-se possível rastrear os passos de um indivíduo utilizando RFID. O fator agravante, relativo à identificação pessoal, é que, no caso de implantes, o indivíduo pode ser rastreado 24 horas por dia. Quando isso é utilizado exclusivamente para a segurança contra a criminalidade e incolumidade do usuário, esta capacidade se torna benéfica. Entretanto, definir padrões segurança é uma atividade que deve ser realizada de maneira cuidadosa. Trata-se aqui do risco de que a definição de segurança ultrapasse o direito à privacidade. Quem definiria os limites do que é seguro em oposição aos limites de vida privada? E com que interesse? Este é um quesito que exige amplo debate. Há de se lembrar que, na maioria dos casos, o usuário que compra um sistema do comércio de segurança, não foi o definidor deste conceito de segurança.

É quase impossível afastar a idéia de que mal utilizada, a identificação pessoal por RFID pode colocar usuários em uma situação de prisão sem grades. Ao contrário do que buscam os defensores de sistemas de segurança baseados na RFID, a tecnologia pode servir como instrumento de ameaça ao usuário. Em um possível cenário, governos totalitários podem obrigar cidadãos a utilizarem o sistema para observar possíveis atividades de oposição a estes regimes, quebrando também a privacidade destes indivíduos. Se o sistema escolhido for o de implantes em humanos, cabe ressaltar que a etiqueta só poderia então ser retirada por cirurgia.

Não somente a governos totalitários serve a utilização de tecnologias de identificação remota para controle da segurança do estado. Há casos de implantes iniciados por entidades estatais do México que merece atenção. Autoridades e oficiais do governo daquele país, a título da segurança contra criminosos, estão sendo etiquetados. A proposta do programa mexicano afirma que o usuário adere voluntariamente, após a sugestão do Estado, ao sistema remoto de identificação. Neste caso o cargo governamental que o indivíduo ocupa tem sido a base da argumentação de possível insegurança.

Nos Estados Unidos, em alegada defesa da democracia, os cidadãos têm seus *e-mails* e outras formas de comunicação rastreados. Utilizar a RFID como aliada neste rastreamento não seria nenhuma surpresa. Fica caracterizada como urgente a atenção que deve ser dada a programas como o *TIA - Total Information Awareness*, que pode ser traduzido como Conhecimento (ou Monitoramento) Total de Informações. Este programa do governo dos Estados Unidos busca centralizar informações de milhares de fontes possíveis para órgãos de segurança daquele país, a título de se proteger de eventuais terroritas. Este tipo de programa é alvo de preocupações de entidades de proteção de direitos civis nos Estados Unidos. O sistema do programa e as precupações alegadas contra possíveis atos terroristas ocasionaram uma coleta de informações pessoais de cidadãos americanos em larga escala. Para concretizar uma vigilância total nos Estados Unidos, o crescimento do uso da RFID e o simples acréscimo de rotinas nos programas coletores de dados do *TIA* já seria suficiente. Não é à revelia que alguns representam o *TIA* graficamente por meio da Figura 3.1, obtida em (ACLU 2004). A preocupação se justifica, já que, embora banido pelo congresso americano em 2003, foi anunciado recentemente que a Agência Nacional de Segurança daquele país estaria de fato implementando tal programa (ACLU 2008).

O fato de obrigar cidadãos a utilizarem a tecnologia não se limita, entretanto, à ação de governos. Na verdade, os primeiros casos reportados de coerção à utilização de tecnologia implantável são atribuídos a empresas privadas, que têm aplicado a tecnologia à identificação funcional. Na certa, alguns indivíduos, mesmo que não queiram utilizar a tecnologia, acabam aceitando implantes para evitar um desgaste que poderia levar à perda de seus postos de trabalho. Em ambos os casos, ou seja, sugeridos/impostos por governos ou empresas, não estão claros os padrões de necessidade de identificação, segurança, enfim, os motivos reais do etiquetamento.

Aprofundando a análise da identificação pessoal e do uso de RFID com processadores implantáveis, se for esta a ferramenta que a computação

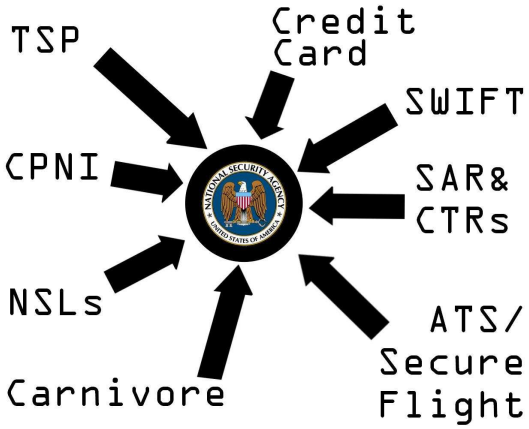


Figura 3.1: TIA - *Total Information Awareness*

pervasiva utilizar para a identificação de indivíduos dentro de uma casa inteligente, pode-se desenhar um cenário onde a vida doméstica poderá ser exposta de forma exagerada. Uma vez que a residência tenha a capacidade de acompanhar os passos do morador ininterruptamente, torna-se tecnologicamente possível a observação de pessoas até mesmo dentro de seus dormitórios, em um cenário semelhante ao livro de George Orwell, 1984.

Um outro detalhe muito simples nos processadores implantáveis que justifica a preocupação com seu uso: eles não podem ser desligados. Este modelo de etiqueta é que tem sido considerado e até mesmo utilizado para armazenamento de diversas informações sobre a pessoa que o utiliza, como informações de seu histórico médico e dados pessoais diversos. As empresas que vendem este produto baseado na RFID passam também a ser detentoras de informações diversas sobre seus clientes, que muitas vezes contratam os serviços como uma ferramenta de segurança pessoal.

Entretanto, não só na identificação pessoal se encontram ameaças à privacidade. O etiquetamento de produtos e objetos já pode acarretar problemas complicados. Primeiro, porque uma vez comprados, não necessariamente as etiquetas acopladas aos produtos deixariam de ser rastreadas. O fato é que as etiquetas continuam sendo capazes de responder aos sinais de leitores. Inclusive se torna possível rastrear os passos do comprador enquanto as etiquetas estiverem no raio de alcance de um leitor. Acrescente ainda a capacidade de estabelecer o padrão de consumo de um freguês de uma loja, já que se o mesmo tiver por hábito comprar produtos de uma mesma rede de lojas, isso se torna atividade simples. Desenha-se mais uma vez um cenário de observação da privacidade do usuário (Cavoukian 2006). Para um melhor entendimento, pode-se analisar casos de empresas que já solicitaram o etiquetamento de seus produtos e com isso geraram polêmica. Por exemplo, a empresa européia Benetton propôs o etiquetamento eletrônico de suas roupas, o que gerou protestos de usuários que enxergaram a perda de privacidade com o uso da marca.

O interesse maior de algumas empresas na RFID não é tanto nos aspectos de segurança, mas na valiosa coleção de informações sobre padrões

de consumo que a tecnologia viabilizaria (Cavoukian 2006). Ferramentas computacionais com poder para integrar os diversos bancos de dados poderiam caracterizar padrões de consumo não somente pessoais, mas também por cidades, regiões, etc. Destaca-se que não somente os produtos comprados seriam conhecidos, mas também em qual quantidade. Isso permite a quebra de privacidade, na medida em que o conhecimento dos padrões de consumo permite inferir renda, estilo de vida e atividades desenvolvidas por uma pessoa. Tais informações poderiam ser objetos de comércio por empresas processadoras de dados, bem como uma valiosa fonte de informações para agências governamentais para a criação de dossiês de cidadãos (Cavoukian 2006).

Em bibliotecas, a RFID também tem sido uma solução muito prática para as atividades de organização, empréstimos e outras aplicações necessárias ao seu funcionamento, permitindo, por exemplo, o auto-atendimento por parte dos seus usuários. No entanto, isto permite também saber o que o leitor anda lendo ou estudando. Mais uma vez a privacidade é colocada em xeque. Entretanto, neste caso, a ameaça se dá muito mais por conta dos bancos de dados que pelo alcance da etiqueta utilizada, que neste tipo de sistema, geralmente utiliza freqüências de cerca de 13 MHz.

Informação é poder. A RFID auxilia, se ligada a outras tecnologias já popularizadas e largamente adotadas, na retirada do poder de controlar as informações sobre si próprio que um indivíduo possui. Estas tecnologias, como celular ou cartões inteligentes, podem passar a utilizar a RFID sem o conhecimento de muitos usuários (Cavoukian 2006). Como qualquer tecnologia, o sistema baseado na RFID pode ser "grampeado" por criminosos. No caso de clonagem de etiquetas implantadas, acrescentar-se-ia o inconveniente já citado de uma cirurgia para a retirada ou substituição da etiqueta. O corpo do usuário passaria, então, por uma verdadeira invasão atribuída à manutenção de sistemas baseados na RFID. Isso pode agravar-se caso cidadão seja mais de uma vez vítima deste tipo de crime, o que não é impossível, ainda mais se for considerado que os padrões comportamentais deste cidadão já poderiam ter sido rastreados por grupos criminosos, que é claro, tão logo fosse possível, encontrariam meios de se beneficiar da RFID.

Todas estas ameaças à privacidade são, porém, passíveis de proteção, que pode utilizar ferramentas auxiliares como: a criptografia, que permitiria, por exemplo, que somente leitores específicos pudessem acessar as informações contidas em certas etiquetas; dispositivos metálicos, que pudessem envolver a etiqueta, evitando que ela transmita eficientemente os dados; e, é claro, senhas quando do uso de informações de etiquetas para sistemas de pagamentos.

Observando o fato de que a RFID permite que o objeto identificado possua um código de identificação exclusivo, pode-se então criar um sistema global de identificação. Isso permite uma capacidade de rastreamento incrível, onde um simples casaco pode permitir o rastreamento de alguns passos de seu comprador. Ou seja, conhecendo-se quem comprou determinado produto, não é necessário que este indivíduo esteja identificado diretamente com uma etiqueta implantada para que se possa rastrear parte de seus

passos. Basta que os produtos que compra estejam etiquetados sem seu conhecimento (Cavoukian 2006).

Embora ainda não tenha sido de fato definido um sistema global de identificação, projetos que buscam padronização internacional de identificação de produtos estão em andamento. Um exemplo é o ACTA (*Anti-Counterfeiting Trade Agreement*), um acordo comercial que visa a proteção da propriedade intelectual a partir de ações anti-fraudes. Este acordo está sendo negociado pelos países componentes do G8 (Canadá, França, Alemanha, Itália, Japão, Rússia, Reino Unido e Estados Unidos) com adesão declarada de alguns outras países, como, por exemplo, Suíça, Austália, Nova Zelândia, Coréia do Sul e México. Ressalta-se que as discussões acerca desse tratado ocorrem fora dos âmbitos tradicionais, ou seja, fora da Organização Internacional da Propriedade Intelectual e da Organização Mundial do Comércio. O acordo teria como objetivo rever normas e leis internacionais sobre patentes, bem como dificultar o comércio internacional de produtos falsificados ou pirateados, principalmente tecnológicos, como os iPods e computadores portáteis, protegendo a propriedade intelectual. As normas negociadas neste tratado não são claras, já que as discussões são realizadas em sessões privadas. Tentativas de se conhecer o conteúdo e abrangência do tratado têm sido frustradas. A Advocacia de Interesse Público do Canadá, por exemplo, requisitou acesso a informações sobre o tratado, mas obteve apenas um documento que declarava o título do acordo; o restante do documento estava censurado (Pilieci 2008). A preocupação acerca de tal tratado deve-se ao caráter secreto em que vem sendo discutido e do fato de que, em alguns dos países envolvidos, como nos Estados Unidos, tratados de comércio não precisam de aval dos representantes da sociedade civil, através de seus parlamentos. De informações vazadas acerca do conteúdo do tratado, conclui-se que este procura impor mais do que normas acerca da propriedade intelectual, dando poder de polícia a autoridades alfandegárias no que diz respeito a pirataria, determinando inclusive penalidades para infrações. Além disso, o tratado parece impor regulamentação estrita sobre provedores de serviços de Internet, forçando a entrega de informações de seus clientes sem necessidade de ordem judicial. Se tais informações forem confirmadas, caracterizam afrontamento claro aos direitos individuais dos cidadãos.

Além da identificação pessoal e de objetos, outros entes etiquetados podem contribuir para supressão de parte da privacidade do indivíduo. Curiosamente, a simples identificação de animais, como cães domésticos, pode levar ao rastreamento de uma pessoa. Em Portugal, os animais domésticos já têm que obrigatoriamente ser identificados com a tecnologia RFID. Em conseqüência, um cão pode involuntariamente denunciar alguns horários de saída de seu dono.

Mas e se as etiquetas dos produtos utilizados no dia-a-dia fossem retiradas ou desligadas, o usuário utilizasse apenas sua tradicional documentação em cartões e papel e resolvesse fazer uma viagem de automóvel? Ainda assim a RFID é capaz de ameaçar a privacidade do cidadão. Os automóveis também são objeto de identificação RFID. Como já destacado, qual-

quer objeto existente pode ser fabricado contendo este sistema. No capítulo anterior se destacou que automóveis também vêm sendo etiquetados e até mesmo peças e componentes diversos o são. Como na compra de um carro o usuário pode inadvertidamente não ter a oportunidade de desligar as etiquetas presentes no veículo, o automóvel pode no mínimo fornecer a leitores a informação da movimentação diária do usuário.

Estes padrões de movimentação diária de veículos, aliás, já começam a ser obtidos no Brasil. No ano de 2006, o CET - Conselho de Engenharia de Trânsito - de São Paulo desenvolveu um estudo com 550 veículos e algumas antenas receptoras espalhadas pela cidade, onde a RFID permitia a identificação de veículos e a identificação de sua movimentação. A cidade de São Paulo foi então palco do ensaio da implementação do SINIAV, o Sistema Nacional de Identificação Automática de Veículos. O SINIAV torna obrigatória a instalação de etiquetas RFID em veículos registrados no Brasil. A Resolução 212 de novembro de 2006, do CONTRAN, o Conselho Nacional de Trânsito, determina que em até 42 meses a partir de novembro de 2006, o processo de etiquetamento dos veículos no Brasil seja concluído. Este modelo permite a identificação de dados do veículo, como a situação de registro e de IPVA (Imposto sobre Veículos Automotores), antes mesmo de um automóvel parar em uma operação de fiscalização. A Wolkswagen já oferecia em 2006, em toda a sua linha, carros identificados com a RFID. Agora outros fabricantes terão de seguir a resolução do CONTRAN.

O uso de *chips* de identificação pessoal sob a pele também já é corrente no Brasil. Famílias abastadas do país já utilizam o equipamento como parte de seu tratamento médico ou como mecanismo anti-seqüestro. As empresas que operam este tipo de equipamento garantem que não há riscos acerca do vazamento das informações coletadas ou mesmo risco de controle dos direitos do usuário, como o de livre circulação. Estes serviços começam a ser comercializados sem que haja uma clara legislação para a RFID. No caso de etiquetas de identificação de automóveis, exposto acima, o CET garante que os dados serão protegidos e que somente seriam cedidos a outrem mediante ordem judicial, como ocorre com dados bancários e telefônicos. Entretanto a proteção do usuário deve ir além de uma garantia dos criadores destes tipos de sistemas.

Um fato interessante é que um dos tópicos de maior debate acerca da RFID, antes mesmo de sua ampla disseminação, é justamente a manutenção do consumidor como um usuário cativo de produtos a serem etiquetados. Analisando do ponto de vista puramente econômico, a RFID é demasiado cara nos dias atuais, conforme observado no capítulo anterior. Além disso, para manter clientes avessos à tecnologia RFID, foram propostos modelos em que as etiquetas sejam bloqueáveis ou retiráveis. Tal tecnologia de etiquetas bloqueáveis consiste em modelos de etiquetas eletrônicas nas quais uma vez comprado o produto etiquetado, o sinal de identificação único da etiqueta deixa de ser reconhecido. Num modelo mais simples, permite-se a retirada da antena da etiqueta, tornando-a incomunicável. Em outro modelo, a etiqueta permite que se acione um sistema no qual é transmitido ao leitor um sinal múltiplo, no qual uma etiqueta passa a não ser reconhecida

por simular várias etiquetas com um mesmo sinal. Algo que pode ser traduzido com uma pessoa com dois rostos na mesma face. É claro que ambos os sistemas encarecem mais ainda a etiqueta e seus custos de operação.

Como o etiquetamento de produtos será com certeza mais rapidamente difundido que os usos de identificação pessoal, os grupos de defesas dos direitos civis têm se mobilizado em países como Canadá e Estados Unidos, onde a tecnologia se encontra mais difundida, para regulamentar melhor o uso destas etiquetas, em proteção aos direitos de privacidade.

Deveria então haver uma legislação que protegesse o interesse dos usuários da RFID também no Brasil. Ver-se-á então o que já existe na legislação brasileira para a proteção de privacidade no próximo capítulo. Aborda-se, também, o que já ocorre em outros países que passam semelhante urgência de proteção de privacidade. No Capítulo 5 sugerem-se alguns pontos para melhor a proteção de usuários desta tecnologia no Brasil.

# Capítulo 4

# A Legislação e o Direito à Privacidade

Após a apresentação sobre a RFID, vista nos capítulos anteriores, devemos questionar: como o direito brasileiro protege a privacidade? Ao contrário de outras nações, como a Grã-Bretanha, que não possui uma constituição escrita, o Brasil possui sim uma carta magna e a partir dela define-se a noção de direitos fundamentais do cidadão brasileiro. Desde a Revolução Francesa, a noção do respeito aos direitos individuais, entre eles o direito à privacidade, é bem difundido. Assim, no mundo ocidental, essa noção de respeito é característica intrínseca à maioria das legislações de suas nações. Se no Brasil, por um lado, a noção do indivíduo público é afetada pelo passado colonial, o mesmo não ocorre com a vida privada (Vieira 2003). Ou seja, o direito à privacidade no Brasil ainda é visto como um direito fundamental a ser respeitado.

A Constituição Federal de 1988 diz, em seu artigo 5º, inciso X, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". Este inciso constitucional demonstra como a privacidade faz parte dos direitos a serem protegidos, entre os demais direitos individuais. Segundo Victor Lima (Lima 2005), "o direito à privacidade pode encampar distintas ações objetivando cessar práticas lesivas e reparar danos patrimoniais e morais, visando sancionar todo tipo de divulgação indevida de informação sobra a privacidade alheia". Na Constituição Federal há outros incisos que buscam proteger a privacidade. Por exemplo, o inciso XI do mesmo artigo 5º defende que "a casa é o asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou durante o dia, por determinação judicial". No inciso XII, é assegurado o sigilo de comunicações e telecomunicações.

O direito brasileiro vai ainda mais longe. No Código Civil, também se encontra um artigo no qual se busca proteger a privacidade. No artigo 21, Capítulo dos Direitos de Privacidade, estabelece-se que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário

a esta norma" (Lima 2005). Assim, mais uma vez a legislação ressalta que a privacidade é direito fundamental. Portanto, verifica-se que o direito brasileiro buscou assegurar limites à invasão de privacidade.

Entretanto, alguns juristas entendem que essa proteção não é eficaz. Observam que se trata de norma genérica e que casos de violação de privacidade devem ser analisados um a um. "Adicionalmente a este fato, muitos juristas consideram que nem sempre é fácil definir a privacidade em situações concretas, e encaram a privacidade como um conceito eminentemente subjetivo, pois algumas pessoas não se sentem invadidas na sua intimidade ao serem observadas e até gostam disso" (Lima 2005). Além disso, "nem toda informação sobre a vida privada pode ser considerada ilícita (...) porque existe uma linha tênue entre o que pode ou não ser informado e inexiste legislação específica sobre o tema". (Savadintzky 2006). Assim, embora exista norma constitucional que visa proteger a privacidade, entende-se que o direito brasileiro ainda é ineficaz neste objetivo.

Mesmo, porém, que se leve em consideração que alguns indivíduos apreciem ver suas vidas expostas em virtude, por exemplo, de influências da mídia, não há que se questionar que parcela de privacidade as pessoas querem expor. Ao contrário, deve-se procurar compreender qual parcela de suas vidas as pessoas querem manter privada. Com este entendimento, muitos juristas defendem que a privacidade pode ser definida "como uma faculdade inerente a todo e qualquer indivíduo de manter fora do alcance de terceiros o conhecimento sobre fatos inerentes a sua própria pessoa ou atividades particulares. Ou ainda privacidade é o poder de controlar o que os outros podem saber sobre você" (Lima 2005). Deve ser lembrado que o direito coletivo não se deve sobrepor ao individual, no entendimento brasileiro, salvo em casos de finalidade científica ou de segurança.

Entretanto, deve-se tomar cuidado com a crença de que a definição de privacidade é de fato vaga. O argumento baseado no fato de que a privacidade é definida de forma subjetiva pode ser utilizado como ferramenta para a exposição do cidadão e, portanto, para a violação de seus direitos.

Ainda em relação à definição de direito à privacidade, há também o entendimento de que este pode ser visto como o direito de separar as diferentes identidades de uma pessoa. Identidade pode ser definida a partir do modo de reconhecer alguém (Clarke 1994). Assim, separa-se, por exemplo, a identidade doméstica da identidade pública de um indivíduo. Controla-se então o que pode ser conhecido de uma pessoa de acordo com os interesses do indivíduo frente ao papel social que exerce em determinado momento. Ao exercer um determinado papel social, o indivíduo controla a quantidade de informações que pode ser deduzida de outro papel social que desempenha. Pode-se portanto entender que há diferentes níveis de privacidade separados pelos diferentes contextos sociais freqüentados pelo indivíduo (Clarke 2006b).

Aprofundando, a identificação é um processo de reconhecimento. Para que haja identificação, ocorre antes a entificação (Clarke 2006a). Entificação é uma associação de uma marca a um ser (Rezende 2004). Por exemplo, associar uma assinatura a uma pessoa. Só depois pode ocorrer identifi-

cação, que seria o reconhecimento do ser. A entificação acarreta porém a existência de um conhecimento prévio de informações de identidade, que por conseqüência pode conduzir à idéia de que a privacidade seria também o poder de controlar a identificação.

No direito dos Estados Unidos, há normas mais específicas acerca da privacidade, como por exemplo, *Right of Privacy, Freedom of Information, Family Educational Rights and Privacy Act*, entre outros (Savadintzky 2006). Ou seja, o direito americano busca especificar melhor os limites entre a liberdade da informação e direitos de privacidade e vida íntima. Entretanto, este não é o padrão nas legislações de diferentes países. Conforme (Savadintzky 2006), o autor François Rigaux, em (Rigaux 2000), afirma que "a jurisprudência americana faz a balança pender para o lado da liberdade de expressão, ao passo que o Tribunal Constitucional Federal alemão parece mais atento ao direito de personalidade da vítima do caricaturista". No caso britânico, onde o direito é determinado pelos costumes, é provável que certas ações consideradas no Brasil ou em outros países como violações da privacidade não sejam assim vistas na Grã-Bretanha, já que naquele país a subjetividade também é imperante na questão da privacidade.

Cabe destacar que mesmo que hajam normas específicas sobre privacidade, as legislações de diversos países não se encontram prontas para lidar com privacidade e tecnologia da informação. Entretanto, é certo que a conceituação do que é lícito ou ilícito em direito de informação e privacidade é urgente frente ao advento da utilização de tecnologias avançadas como a Identificação por Radiofreqüência.

É claro que a RFID não é a única tecnologia capaz de permitir a quebra de privacidade de usuários de sistemas computacionais. Por isso, muitos países têm buscado aperfeiçoar a sua legislação acerca do tema de coleta e controle de informações eletrônicas referentes a seus cidadãos, antes mesmo da disseminação mais ampla da RFID. Aliás, em alguns países esta preocupação já é bem antiga e antecede inclusive o surgimento da RFID em seu formato atual. O motivo, ressalta-se, é que a RFID é apenas mais uma tecnologia eletrônica capaz de gerar informações pessoais sobre os indivíduos. Assim, muitos países, após o advento e disseminação da computação se preocuparam em legislar acerca da proteção de dados pessoais frente à tecnologia da informação. Na próxima seção, são apresentados exemplos das propostas implementadas em alguns países, conforme (Zorzo e Grande 2006). Na Seção 4.2 são apresentados alguns dos instrumentos legais do direito brasileiro, propostos e existentes, referentes à proteção do cidadão no que tange ao uso de tecnologias da informação.

## 4.1 Legislação em Outros Países

Nesta seção, apresenta-se brevemente tópicos referentes à abrangência das legislações de diversos países no que diz respeito à proteção do cidadão frente às tecnologias da informação. Dos países pesquisados, o México não possui nenhuma lei que trate diretamente da proteção de dados. Os demais

casos são apresentados a seguir.

### 4.1.1 Chile

Primeiro país latino-americano a criar uma lei de proteção de dados (Lei 19.628 - Proteção de Dados de Caráter Pessoal, 1999), assegurando o acesso e o controle de dados pessoais.

### 4.1.2 Peru

A constituição (1993) determina a existência do direito de privacidade e proteção de dados. Em 2002, foi criada comissão para detalhar melhor a proteção de dados.

### 4.1.3 Estados Unidos

No texto constitucional não há especificação do direito à privacidade. Entretanto há o Decreto de Privacidade, de 1974, que como já dito, trata especificamente do tema. Tal decreto restringe a coleta, o uso e a disseminação de informações por agências do governo. Porém, não há leis referentes ao setor privado, embora existam no congresso americano textos referentes ao tema.

### 4.1.4 Canadá

Dois decretos protegem a privacidade. O Decreto Federal de Privacidade (1982) e o Decreto de Informações Pessoais e Documentos Eletrônicos (2001). O decreto de 1982 é muito semelhante ao Decreto de Privacidade dos Estados Unidos. Já o de 2001 estabelece dez princípios que as organizações devem respeitar no que concerne à coleta, uso, divulgação e armazenamento de dados pessoais.

### 4.1.5 Portugal

A constituição cobre o direito à privacidade e à proteção de dados. O cidadão tem o direito de saber quais são os dados armazenados ao seu respeito e o objetivo da coleta. O Decreto de Proteção de Dados Pessoais (1998) limita a coleta, uso e disseminação das informações pessoais. A Comissão Nacional de Proteção de Dados fiscaliza o setor.

### 4.1.6 Espanha

Existe o Decreto Espanhol para Proteção de Dados (1992). O decreto regula tanto setor público quanto o privado. O cidadão tem o direito de conhecer, corrigir e apagar os dados armazenados.

### 4.1.7 França

Na França também existe um Decreto de Proteção de Dados (1978). Este decreto regula os setores público e privado, como na Espanha. As empresas privadas que pretendem manipular dados dependem de autorização da Comissão Nacional de Informática e Liberdades.

### 4.1.8 Alemanha

Regulando também os setores público e privado, a Lei Federal de Proteção de Dados (2002) é a mais rigorosa da Europa, abordando coleta, uso, armazenamento, processamento e disseminação da informação. O órgão responsável pela fiscalização é a Comissão Federal de Proteção de Dados.

### 4.1.9 Japão

Existe o Decreto para Proteção de Dados Pessoais Processados por Computador e Armazenados por Órgãos Administrativos (1998) com regras para a segurança, acesso e atualização de dados. No mesmo ano em que este decreto entrou em vigor, foi criada uma entidade para supervisionar as empresas no respeito e proteção de dados pessoais dos consumidores.

### 4.1.10 Rússia

Na Lei sobre Informação, Informatização e Proteção da Informação, todo dado pessoal é considerado confidencial. Por isso, coleta, uso, processamento e disseminação de qualquer informação pessoal sem consentimento do indivíduo é proibido. Entretanto, uma lei federal deverá regular melhor aquilo que é considerado informação pessoal, o que ainda não foi feito.

### 4.1.11 Austrália

No Decreto de Privacidade (1988) estão elencados onze princípios que se aplicam ao setor público e ao setor privado, existindo ainda a Comissão Federal de Privacidade para a fiscalização do setor.

## 4.2 Legislação no Brasil

O que se pode observar é que o Brasil, embora com algumas falhas na legislação acerca da privacidade, não está inativo frente ao choque que a computação pode gerar na vida privada, naquilo que concerne à proteção da informação. Se por um lado não está o país inativo, por outro está caminhando a passos lentos. Até o mês de abril de 2008, o Projeto de Lei Crimes Digitais não havia sido votada no Congresso Nacional. Um agravante maior, especialistas dizem que a referida lei possui tantas falhas, que na certa ocorreriam muitos casos de pessoas pagarem pelos crimes alheios, já

que o projeto de lei não levou em conta diversas tecnologias e procedimentos que os criminosos podem utilizar para cometer crimes, por exemplo, como a identificação de outros na rede.

Em 1999, foi proposto o Projeto de Lei da Câmara dos Deputados nº 84, que descreve os crimes de informação que envolvem coleta, processamento e divulgação da informação. O projeto acabou por condensar propostas do senado (Projeto de Lei do Senado nº 137 de 2000 e nº 76 de 2000). A forma final é apresentada no Projeto de Lei da Câmara nº 89 de 2003.

O projeto inicial e suas posteriores apresentações referem-se a crimes de informática. Entre os pontos polêmicos, que acabaram por gerar discussões que têm postergado a votação do projeto, encontram-se questões referentes à privacidade. O projeto prevê, por exemplo, que haveria a obrigação de o usuário da internet se cadastrar junto aos provedores de *e-mail* com validação de acesso dos internautas com base em dados pessoais a cada conexão à rede. Além disso, os provedores seriam obrigados a manter os registros de acesso por no mínimo três anos. Positivamente o projeto prevê uma pena de dois a quatro anos de detenção para a obtenção indevida de dados nas redes de computadores; e pena de um a dois anos de detenção para violação ou divulgação indevida de dados privados na internet. Críticos da proposta consideram a exigência de cadastro e identificação um risco às liberdades civis, sendo ainda essa medida uma forma de "burocratizar" a rede. Defensores da proposta por sua vez dizem que, por outro lado, esta identificação obrigatória permitiria uma melhor identificação de criminosos da rede.

A Resolução 212 de novembro de 2006 do CONTRAN, citada no Capítulo 3, também não é muito específica no que diz respeito à proteção da privacidade. Afirma, porém, em seu Anexo II, item 4, que " O SINIAV terá as seguintes características de segurança:

a. Segurança de integridade de dados da placa eletrônica: os dados de identificação da placa eletrônica nela gravados por seu fabricante, bem como os dados de identificação do veículo gravados pelo órgão executivo de trânsito do Estado ou do Distrito Federal, onde estiver registrado o veículo, conforme determina o Artigo 3º desta Resolução, devem possuir características de gravação tais que seja impossível alterá-los.

b. Segurança dos dados entre a placa eletrônica e antena leitora: devem ser utilizadas chaves de criptografia para autenticação da comunicação entre as placas eletrônicas e as antenas leitoras, ou outro meio que garanta a segurança necessária destes dados.

c. A arquitetura do SINIAV deve garantir a segurança das informações protegidas pelo sigilo de dados, nos termos da Constituição Federal e das leis que regulamentam a matéria".

É importante ressaltar que o texto insiste que os dados devem ser mantidos em sigilo. Tomando o sigilo como ferramenta auxiliar na manutenção da privacidade, há apenas uma proteção tênue na legislação sobre o SINIAV. A violação dos dados não pode ser considerada crime, pois não se

encontra indiscutivelmente definido o delito. O prejuízo resultante do vazamento de informações geralmente só é percebido a partir do uso indevido das informações ilegalmente obtidas, ou seja, após a ocorrência de tal prejuízo. Além disso, em caso de vazamento de informações, tanto do SINIAV como de qualquer outro banco de dados, pode ocorrer dificuldade em identificar o responsável. Não sendo identificado o responsável, há problema em tipificar crime. A dificuldade consiste em que acusação de delito qualquer precisa de autor. Na esfera privada, sem a identificação do autor não há possibilidade de aplicação de pena. No entanto, se o banco de dados estiver em poder órgão público, estaria caracterizada a falta de zelo com as informações. Há, neste caso, penalidades, ainda que pequenas, previstas na Lei 8.112 de 1990, que rege os direitos e obrigações do servidores públicos. Deve-se lembrar, contudo, que este regime não se aplica a qualquer órgão, pois alguns setores do governos não tem os servidores regidos por esta lei. Porém, a maioria dos regimes disciplinares prevê ferramentas semelhantes, inclusive em governos estaduais e municipais.

Se, na visão de juristas, a proteção à privacidade é falha, conclui-se que se faz necessária uma lei mais específica acerca de privacidade e vida íntima no Brasil. Observa-se que, na forma atual, a legislação confere muitos dos casos judiciais sobre privacidade ao julgamento subjetivo das autoridades judiciárias (Savadintzky 2006).

Semelhante às legislações de alguns países, apresentadas na seção anterior, a legislação brasileira protege o direito de conhecimento de informações sobre um indivíduo, por parte do próprio cidadão, no texto constitucional. Trata-se mais uma vez do artigo 5º, no inciso LXXII, onde encontra-se que "conceder-se-á *habeas data*:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

Alguns juristas defendem que a figura do *habeas data* é fundamental na proteção à privacidade do cidadão brasileiro. Isso ocorreria porque se o cidadão pode retificar os dados, ele teria, pelo menos em parte, conhecimento das informações coletadas e mantidas a seu respeito. Figurando então como ferramenta de proteção à privacidade, tal mecanismo está referenciado também no Projeto de Lei 3.494 de 2000, que dispõe sobre proteção de dados e ritos processuais do *habeas data*.

Outra importante ferramenta legal para a proteção à privacidade seria o *Mandado de Injunção*. O inciso LXXI do artigo 5º da Constituição brasileira determina que o Mandado de Injunção será concedido sempre que a falta de norma regulamentadora torne inviável o exercício dos direitos e liberdades constitucionais e das prerrogativas inerentes à nacionalidade, à soberania e à cidadania. Sendo a privacidade um direito fundamental, conforme determinado pela nossa Constituição, o Mandado de Injunção poderia ganhar

destaque entre os mecanismos já existentes para a proteção deste direito. Já que as normas protetoras de privacidade no direito brasileiro são normas gerais, o que poderia ocasionar interpretações desfavoráveis aos direitos de um indivíduo, mandados de injunção poderiam preencher parte desta lacuna.

### 4.2.1 Norma Técnica

No campo das normas e diretrizes da área de sistemas de informação está a Norma Técnica 27.002 da Associação Brasileira de Normas Técnicas. Essa diretriz estabelece alguns procedimentos para avaliação da segurança de dados, considerando que "a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida". A privacidade depende em certo nível do não vazamento de informações.

Já em sua introdução, a diretriz recomenda que "seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente". Estabelece, portanto, recomendação para quaisquer organizações detentoras de informação, incluindo aquelas que operam sistemas baseados na RFID, objeto deste trabalho.

Ressalvas são apresentadas na própria Norma, destacando-se que "esta Norma pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas para a organização. Nem todos os controles e diretrizes contidos nesta Norma podem ser aplicados. Além disto, controles adicionais e recomendações não incluídos nesta Norma podem ser necessários. Quando os documentos são desenvolvidos contendo controles ou recomendações adicionais, pode ser útil realizar uma referência cruzada para as seções desta Norma, onde aplicável, para facilitar a verificação da conformidade por auditores e parceiros do negócio". Em outras palavras, a Norma 27.002 pode em alguns pontos não ser suficiente à proteção adequada de privacidade.

Considerando-se o âmbito deste trabalho, cabe destacar, mais que os aspectos técnicos, os objetivos de proteção que a 27.002 estabelece. No campo da política de informação, o objetivo da Norma é "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização". Nestes termos e nos dos apresentados no parágrafo anterior, a Norma prevê a adaptação de políticas de segurança de acordo com os objetivos de cada organização gestora/detentora de informações, impondo que tal política esteja de acordo com a legislação e as regulamentações relevantes à atividade da organização.

A Norma destaca ainda que "convém que todas as responsabilidades pela segurança da informação, estejam claramente definidas". Aqui, a Nor-

ma estabelece o grau de responsabilidade em eventuais vazamentos. Definições de responsabilidade, o papel de cada setor da organização, bem como aspectos procedimentais para avalizações periódicas da segurança de dados são normatizados na 27.002. Todo este aparato pode servir como ferramental auxiliar na proteção à privacidade.

A proteção de informações é estabelecida pelo nível de confidencialidade do dado a ser protegido. Neste entendimento, a 27.002 orienta que "convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente, de forma regular". Em detalhe, estabelece que "convém que os acordos de confidencialidade e de não divulgação considerem os requisitos para proteger as informações confidenciais, usando termos que são obrigados do ponto de vista legal". A Norma recomenda a definição explícita, em termos de confidencialidade ou não, da informação a ser protegida. Uma vez que a organização define o nível de confidencialidade da informação e se compromete legalmente a mantê-lo, existe respaldo jurídico para imputabilidade da organização em caso de vazamento.

As diretrizes apresentadas na 27.002 recomendam que o profissional de sistemas de informação observe as normas legais na proteção de dados. A 27.002 é uma orientadora, portanto, a ser seguida pelos profissionais para que cumpram tecnicamente aquilo que a lei estabelece. Assim, a proteção de dados sigilosos, que resulta em derta proteção à privacidade, também é responsabilidade destes profissionais e das organizações para as quais trabalham.

Mais uma vez, porém, têm-se apenas diretrizes. O profissional de sistemas de informação não será responsável por uso de informações que a lei não proteja. A 27.002 então, como ferramenta auxiliar depende que a lei estabeleça os padrões de proteção de informações.

Logo, a lacuna existente na legislação de proteção de dados e de proteção à privacidade, pode ocasionar vários dos problemas possíveis apresentados no capítulo anterior. Diante do advento da RFID e da iminência de seus riscos de facilitar a violação de direitos fundamentais, urge a instalação de normas regulamentadoras do tema. A análise de algumas propostas relativas a esta necessidade será o tema do próximo capítulo.

# Capítulo 5

# Sugestão à Legislação Brasileira sobre RFID

Conforme visto nos capítulos anteriores, a RFID já é uma tecnologia de uso corrente, sem que, no entanto tenha ocorrido o devido debate acerca do tema de forma a gerar uma legislação abrangente, capaz de proteger a privacidade dos usuários. Mas como deveria ser esta legislação? O que ela deve conter? O que pode ajudar a criar uma legislação que diminua a subjetividade nos julgamentos de casos sobre privacidade e tecnologia? O uso amplo da RFID é inevitável devido às novas aplicações que foram encontradas para esta tecnologia.

A chave para entender como deve funcionar a legislação para o tema pode estar na combinação entre a legislação que já existe e o acréscimo de novos itens eventualmente faltantes e indispensáveis à não violação dos dados que o usuário quer preservar. No Capítulo 4, que se refere ao direito à privacidade na legislação, viu-se que no Brasil há o entendimento de que o direito coletivo não deve violar o direito individual, salvo em caso de segurança pública ou necessidade científica. De acordo com este entendimento, discute-se neste capítulo não somente o que a legislação deve conter, mas o próprio processo de construção e discussão de uma estrutura brasileira para a normatização da RFID.

## 5.1 Definição de Privacidade

Começando pela legislação já existente, mostrou-se que não é consenso no direito brasileiro o conceito de privacidade. Em outras palavras, a subjetividade ainda impera quando a privacidade vira objeto de confronto judicial. Isso é um obstáculo que aparenta ser pequeno, mas na realidade é gigantesco. Por exemplo, uma empresa que comercializa produtos etiquetados pode não receber as devidas sanções em casos de responsabilidade objetiva (dano com conhecimento ou intenção do prejuízo causado) ou subjetiva (dano não intencional) de violações de direitos de usuários. Algo semelhante já acontece mesmo sem a RFID. Não raro, empresas comercializam dados de clientes com outras empresas para fins de propaganda e até

mesmo venda de produtos que o cliente não solicitou. Isso acontece porque a informação de clientes tem sido tratada como algo pertencente à empresa que vendeu a informação e não aos clientes. Como exemplo recente, temos o caso de inúmeras pessoas que recebiam cartões de crédito não solicitados de várias administradoras, inclusive com limite de crédito estipulado pelo valor da renda dos clientes.

A definição de privacidade, que acaba sendo tratada quase que pelo costume no direito brasileiro, é vital à proteção do que o usuário entenderá por privacidade. Mas a proposta à criação de uma legislação abrangente sobre RFID acaba por demandar a definição mais uniforme de privacidade no direito brasileiro. Ou seja, os juristas teriam de realizar suas discussões e debates em torno do tema da privacidade para evitar que leis sobre tecnologia encalhem na inutilidade de não proteger o usuário porque o costume não previa que algo fosse tido como privado. Pode-se ver aqui um caso onde a ciência da computação pode impulsionar uma discussão na ciência jurídica, não apenas na criação de uma lei relacionada à informática, mas na própria discussão do conceito jurídico de limites de privacidade.

Uma análise fundamental: a RFID, como já exposto, ameaça acabar, além de limites antes considerados, com a possibilidade de o cidadão permanecer incógnito. Pode-se considerar que, assim como o direito fundamental e positivo à vida precisou ser protegido de violações por meio do direito penal, também o direito à privacidade está entrando em uma situação semelhante, onde a lei deverá determinar a criminalização de quebra de privacidade para coibir este ato. Assim pode-se considerar urgente a definição suscitada no parágrafo anterior, bem como a lei de criminalização citada neste. A própria Constituição, que define privacidade como direito básico, define também no artigo 5º, agora no inciso XLI, que a lei deve punir "qualquer discriminação atentatória dos direitos e liberdades fundamentais". Mas por outro lado, uma punição deve estar definida na lei, pois conforme expresso no mesmo artigo, inciso XXXIX, "não há crime sem lei anterior que o defina". Portanto, torna-se fundamental mais uma vez a existência da legislação sobre privacidade. Particularmente, é necessária a definição de uma legislação sobre RFID e privacidade.

Para a continuação da discussão a ser aqui apresentada, adota-se a que a preservação da privacidade impõe que apenas os dados essenciais sobre um cidadão possam ser utilizados em caso de necessidade e apenas em razão desta mesma necessidade. Adota-se também a noção proposta em (Lima 2005), citada no Capítulo 3, de que privacidade é o poder de controlar o que os outros podem saber sobre o indivíduo. Adota-se, portanto, uma noção mais precisa sobre o que é tratado como dado sigiloso e do que não o é, observando-se que apenas a necessidade urgente coletiva ou científica justifica a quebra do sigilo. A adoção de tais noções é justificada em virtude do costume, ou seja, porque tal costume tem definido a privacidade no direito brasileiro.

## 5.2 RFID e a ICP-Brasil

A tecnologia RFID, deve ser destacado, é o que o próprio nome afirma ser, uma tecnologia de identificação. Como tal, o sistema depende de proteção não apenas para garantir os direitos do usuário como para seu próprio funcionamento. Assim, conclui-se que alguma estrutura de chaves de proteção e de criptografia seja necessária.

No que concerne a chaves de proteção públicas e privadas, o Brasil já possui uma regulamentação, determinada pela *Infra-estrutura de Chaves Públicas Brasileiras*, a ICP-Brasil, a qual foi instituída pela Medida Provisória 2.200-2 de 24 de agosto de 2001 (Presidência da República 2001). Com a criação da ICP-Brasil, o governo buscava integrar o Estado e o povo à nova tecnologia de telecomunicações (internet), regulamentando a identificação de indivíduos (pessoas físicas ou jurídicas), de forma a evitar fraudes de identificação. Ao mesmo tempo, cultivou o direito do Estado brasileiro auditar sistemas e ter controle de informações nacionais, mesmo que utilizando tecnologia estrangeira (Barra 2006). Assim a gestão da ICP-Brasil certamente participará do processo de regulamentação da RFID, principalmente no que concerne à identificação de indivíduos, uma vez que uma das razões de sua criação foi justamente a identificação e autenticação eletrônica de indivíduos pela internet. A RFID é apenas um sistema eletrônico de identificação e, como tal, acaba por utilizar a internet ou outras redes de computadores menores.

Muito da discussão que criou a ICP-Brasil pode ser útil à elaboração da legislação sobre a RFID. Começando pela idéia do que pode ser trabalho da iniciativa privada e do que deve ser reservado ao Estado. O setor privado tem interesse em manter no mercado produtos que sejam de interesse dos consumidores, sejam eles pessoas físicas, jurídicas ou o próprio Estado. No caso da ICP-Brasil, o Estado buscou manter sua relação coercitiva diante dos administrados e do setor privado ao qual interessava vender ferramentas de autenticação e identificação remota, que poderiam de certa forma reduzir o poder do Estado no controle de informações vitais, uma vez que o maior interesse na constituição de ferramentas de identificação eletrônica provinha do setor bancário. Ciente da importância que a instituição de uma infra-estrutura adequada de chaves públicas teria para que não perdesse parte de seu controle sobre os administrados, o governo se valeu de sua força para implementar um sistema de chaves públicas ligado ao próprio Estado (Barra 2006).

Deve-se lembrar, então, que o governo chamou para si a responsabilidade de participar ativamente na manutenção futura da segurança de informações relativas à proteção dos códigos concernentes à ICP-Brasil. Neste caso, o Estado, por meio de seu poder, fez com que os controles de códigos da ICP-Brasil não ficassem de todo nas mãos das empresas que prestam os serviços computacionais do sistema de chaves públicas. O Estado Brasileiro, além de cliente destes serviços, tem então dois papéis fundamentais: normatiza e audita o sistema. O setor privado, entretanto, não deixou de "vender" seus serviços para a constituição da ICP-Brasil. Muito

pelo contrário, os serviços foram implementados e a ICP-Brasil foi então constituída.

Esta característica, de o sistema estar controlado e auditado pelo Estado, porém, não deveria ser contaminada pela política. Não é possível afirmar que a ICP-Brasil nunca seja influenciada pela política, mas o fato é que a presença de Estado traz este risco. Apesar disso, pode-se argumentar que a presença do Estado, para o controle das informações e para a auditória do sistema de chaves públicas, deva ser mantida a fim de evitar que a infra-estrutura esteja sujeita às vontades de pessoa privada. Como na constituição de uma infra-estrutura brasileira para a RFID estar-se-á falando, de certa forma, em uma expansão da ICP-Brasil, estas características da ICP-Brasil estarão presentes na infra-estrutura para a tecnologia baseada na RFID. Isso ocorrerá porque, assim como foi determinado no SINIAV, os sistemas de criptografia e identificação dependem desta infra-estrutura e herdam suas características.

No caso da ICP-Brasil, o maior consumidor do sistema era o próprio Estado, ao qual interessa a manutenção do controle sobre o sistema bancário, pois os bancos são os que mais utilizam a infra-estrutura. A auditoria estatal, neste caso, seria então justificada. De fato, em (Barra 2006) destaca-se que na constituição da ICP-Brasil, o Estado foi "Leviatã". O Estado, por meio coercitivo, manteve o controle sobre o sistema, retirando da iniciativa privada a possibilidade de controlar sozinha o mercado de autenticação. De fato isto foi benéfico no sentido em que o sistema ganha certa confiabilidade, uma vez que o Estado, como auditor, pode teoricamente evitar a submissão a interesses privados nos serviços de autenticação pessoal.

Por outro lado, influências políticas podem atingir as estruturas de poder. Por isso, deve-se evitar que o controle das informações e da própria infra-estrutura brasileira para a RFID seja exclusivo do Estado. O Estado hoje audita a ICP-Brasil e no futuro pode vir a auditar todos os sistemas de RFID. Ora, não é impossível que os auditores estejam influenciados em certo grau pelo grupo político que esteja no poder. Assim a legislação deve dispor que o controle é do Estado, que trabalharia para o bem comum, mas que as decisões sobre qualquer mudança de rumos na ICP-Brasil (e para a infra-estrutura a ser proposta para a RFID) deveria pertencer a um comitê com representação de toda a sociedade, fazendo prevalecer o entendimento de que o direito individual prevalece sobre o coletivo salvo nos casos já citados. Interessante é que, na formação da ICP-Brasil, esse fator não foi respeitado. Ao contrário, os representantes da sociedade foram indicados pelo próprio governo, de certa forma ferindo a lisura que um processo de tamanha magnitude exige. O Estado acabou se sobrepondo demais ao sistema. Conforme (Barra 2006), "Advogados da Subchefia para Assuntos Jurídicos da Casa Civil e técnicos da área de segurança da informação praticamente definiram toda a base jurídica da ICP-Brasil". Verifica-se ainda na ICP-Brasil o vício de que a auditoria é feita sem a devida publicidade que atividades públicas devem receber. A auditoria de sistemas RFID não deve seguir este padrão vigente na ICP-Brasil.

A autoridade certificadora, conforme determinado na Medida Provisória

2.200 de 24 de agosto de 2001, é também puramente Estatal. Trata-se do ITI - Instituto Nacional de Tecnologia da Informação, autarquia federal. O papel da representação da sociedade civil na ICP-Brasil ficou reduzido, então, tanto na certificação, quanto na composição da própria infra-estrutura. Este é um ponto delicado e que merece ampla discussão: até quando a participação da sociedade civil será tímida ou obscurecida pela abrangência das atuações do Estado ou de grupos política e/ou economicamente privilegiados? O questionamento é amplo e não somente dirigido à caracterização da ICP-Brasil e de uma possível infra-estrutura para sistemas baseados na RFID. Estende-se o questionamento a quaisquer setores econômicos regulados.

A Medida Provisória 2.200 de 2001 determina, em seu artigo 6º, parágrafo único, que "o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento". Este parágrafo pode gerar distorções indesejáveis. Como o usuário é responsável pelo controle das chaves, em caso de violações e vazamentos, o setor econômico, que exige a utilização de tais chaves para efetivação de transações, pode ser isentado. Se a chave for única para todas as aplicações, a situação se agrava, já que aparenta violação do princípio de proteção aos mais fracos nas relações entre o indivíduo e o setor econômico ou entre o indivíduo e o Estado. O Estado deve proteger o cidadão neste tipo de confronto e, portanto, deve ser o primeiro a evitar que o cidadão tenha uma responsabilidade que não lhe pode, de fato, ser imputada. Não se considera, portanto, razoável que a infra-estrutura para sistemas baseados na RFID herde todas as características da ICP-Brasil.

Embora a ICP-Brasil tenha sido construída visando a identificação de pessoas, seu papel na identificação de objetos e manufaturas continuará a ser essencial, pois a autoridade certificadora é quem terá a ferramenta capaz de autenticar corretamente os produtos etiquetados. Ou seja, o Estado é quem poderá dizer ao mercado quais serão as etiquetas que identificarão corretamente, de acordo com a legislação, os produtos. As etiquetas, conclui-se, teriam que conter a informação de já terem sido autorizadas a circular pela autoridade certificadora. A autoridade governamental teria interesse nisso, por exemplo, para evitar a sonegação de impostos.

## 5.3 Legislação Comparada

Um processo fundamental na formação das infra-estruturas para a tecnologia de identificação baseada em radiofreqüência no Brasil será, como também o foi na instituição da ICP-Brasil, a comparação com as leis que regem o setor em outros países. De certa forma, isso já vem sendo feito. Quando da criação da ICP-Brasil, a legislação comparada trouxe ferramentas de legislações de outras nações para a legislação da ICP-Brasil (Barra 2006). Mais além, os projetos de lei que visam a proteção de dados têm em seu processo de formação esta mesma característica. Em verdade, por ocasião de uma maior interdependência entre as nações, a implantação

de legislações semelhantes contribui para processo de integração, embora devam ainda prevalecer as características democráticas de respeito às identidades nacionais.

Há de se lembrar que quanto aos aspectos tecnológicos, as nações chamadas desenvolvidas também se encontram à frente dos demais países. Tal fato influi, inclusive, nas discussões decorrentes da implantação de certas tecnologias. No caso da RFID, Estados Unidos e Canadá, por exemplo, já se encontram em um nível de debate bem mais avançado acerca da RFID que o Brasil. No restante desta seção, serão apresentadas propostas surgidas do debate canadense acerca do uso da RFID, conforme (Cavoukian 2006).

A autora apresenta algumas proposições para o respeito à privacidade dos usuários. Sugere que sempre o usuário tenha o direito de ser informado e que a lei obrigue informar o consumidor quando uma etiqueta eletrônica está sendo usada. O usuário tem direito a esta informação. É a partir do direito de se conhecer como e onde a tecnologia está empregada que o usuário poderá ter a real consciência das implicações de seu funcionamento.

Indo mais além, a autora sugere que a lei sobre RFID deve estipular que o usuário tem o direito de saber qual o tipo de etiqueta usada e, em cada caso, quais informações a etiqueta pode fornecer sobre o usuário do produto etiquetado.

Outro direito fundamental que Cavoukian destaca é o direito ao consentimento, que pode ser implementado através da ativação ou desativação da etiqueta. Em caso de comprar produtos etiquetados, deve o consumidor sempre ter a oportunidade de optar pela desativação destas etiquetas, sem ônus para o usuário. Este direito seria a continuidade da liberdade e privacidade, caracterizando também a manutenção do direito de se manter incógnito.

Ainda segundo Cavoukian, o usuário deve ter o direito de manter as informações sobre produtos separadas das informações pessoais. Esclarecendo, produtos não devem ser usados como meio de coletar informações pessoais de um comprador, devendo-se evitar o cruzamento de informações de produtos comprados para se traçar o perfil de consumo do cidadão. Tais sugestões e análises estão em concordância com as noções adotadas em relação à privacidade, em conformidade com o direito brasileiro, devendo ser levadas em consideração quando da elaboração da infra-estrutura nacional para a RFID.

Segundo (Cavoukian 2006), a proposta de regulamentação para o uso da RFID deve limitar a quantidade e qualidade das informações que certos estabelecimentos podem coletar e manter. Com isto deseja-se evitar o comércio de informações ilegais sobre consumidores. Por exemplo, uma loja não poderia manter arquivos com informações sobre padrões de compra de consumidores se a lei obrigar que o estabelecimento não pode coletar esse tipo de informação. Se a coleta for permitida, a legislação deve determinar por quanto tempo pode-se manter certa informação. Além disso, o estabelecimento coletor deveria informar, compulsoriamente, a necessidade de se manter determinados tipos de informações. Os objetivos que levam à coleta de certas informações devem, portanto, ser claros e de acordo com objeti-

vos do estabelecimento, sem que estes objetivos e os meios para alcançá-los desrespeitem o direito à privacidade. Estas mesmas propostas devem estar presentes na legislação brasileira.

Analisando pelo lado do fabricante, a legislação pode, por exemplo, limitar a fabricação de alguns tipos de etiquetas, caso o modelo proposto para um produto seja incompatível com os restritos objetivos de uso propostos pelo estabelecimento solicitante ou fabricante. As informações coletadas para um certo objetivo não devem ser usadas para outro fim. Isso deve ser evitado inclusive dentro dos próprios bancos de dados das empresas que coletaram a informação. Havendo necessidade de se utilizar e acessar bancos de dados com informações dos cidadãos, tal acesso deve ser justificado e também limitado para o fim proposto.

Por último, é claro, a legislação deve estabelecer que o usuário tenha o direito de saber todas as informações coletadas a seu respeito, inclusive por estabelecimentos privados, aos quais o consentimento expresso do usuário não só na coleta, como também na manutenção de dados a seu respeito, deve ser manifestado. Mais uma vez é notório que estas propostas canadenses podem ser adaptadas ao direito brasileiro.

## 5.4 Sugestões

Além das sugestões apresentadas na seção anterior, no que se segue, são apresentadas algumas propostas para a legislação brasileira acerca da utilização de sistemas baseados na Identificação por Radiofreqüência.

### 5.4.1 Mecanismos Desligáveis

A legislação deve determinar que as etiquetas de certos produtos devem obrigatoriamente ser desligadas assim que tais produtos cheguem ao consumidor final, como roupas, por exemplo, a não ser que o usuário manifeste expressamente o desejo de mantê-las funcionando. Os estabelecimentos comerciais deveriam então manter funcionários disponíveis para orientar o desligamento de etiquetas ou sua retirada. Inclusive, poderiam ser criados instrumentos semelhantes aos sigilos, fiscal, telefônico e bancário. Mesmo que as informações sobre uma pessoa estejam nas mãos de empresas privadas, sua abertura até mesmo por órgão do governo deveria ser realizada apenas por meio de mandado judicial.

### 5.4.2 RFID e Meio Ambiente

O aspecto ambiental também deve ser contemplado pela legislação relativa à RFID. A legislação deveria estabelecer estímulo ao uso de etiquetas reaproveitáveis onde quer que fossem aplicáveis, orientando ainda os estabelecimentos e os cidadãos sobre como proceder para o reaproveitamento das mesmas.

Ainda na proteção ambiental, pode-se estimular o uso da tecnologia para a proteção de espécies ameaçadas, com o uso de monitoramento eletrônico, como foi apresentado nos primeiro capítulos. Observando-se o modelo mais adequado e este objetivo ecológico da RFID, poder-se-ia garantir estímulos como isenções de alguns impostos para empresas que participem deste tipo de empreendimento de proteções de fauna e flora.

### 5.4.3 Aspectos de Identificação Pessoal

Quanto à identificação pessoal e funcional, é importante ressaltar o que pode ou não ser utilizado em cada caso.

A identificação funcional com RFID de curto alcance é bem comum. O uso de crachás com etiquetas eletrônicas é amplo no Brasil. Este modelo tem sido capaz de identificar funcionários sem invadir sua vidas privadas, uma vez que as etiquetas são de curto alcance e não são implantáveis. Na verdade são etiquetas eletrônicas de alcance de leitura de apenas alguns centímetros.

Analisando, porém, o uso de etiquetas implantáveis em humanos, a legislação deve exigir que o usuário concorde com o implante. O cidadão que usa um cartão ou crachá de identificação não precisa estar acompanhado deste item 24 horas por dia. No caso de o Estado ou as organizações privadas começarem a instituir o uso de etiquetas eletrônicas em substituição a carteiras de identidade, ou quaisquer outros mecanismos de identificação, o cidadão deve ter o direito de não implantar as etiquetas, mas de utilizá-las em cartão, enquanto não se sentir seguro em utilizar a etiqueta implantável. A anuência do usuário respeitaria seu direito de dispor sobre o próprio corpo.

### 5.4.4 Fraudes

A legislação não pode se esquecer de que sistemas computacionais e eletrônicos são passíveis de fraudes. Conforme já citado, grupos criminosos rapidamente obtêm o conhecimento técnico necessário para burlar, fraudar ou fazer mal uso de novas tecnologias. Criptografar informações não torna os sistemas computacionais totalmente imunes às fraudes. Ninguém pode garantir que etiquetas RFID, quaisquer que sejam, estejam seguras contra cópias.

Apesar disso, muitos países vêm adotando etiquetas eletrônicas em documentos tradicionais como passaportes. Estes passaportes porém já foram fraudados, inclusive por competentes profissionais da área de segurança computacional que demonstraram que o processo de fraudar esta tecnologia não é tão difícil. Demonstrações chegam a ser realizadas em congressos de segurança computacional, diante do público.

Em um cenário em que etiquetas implantáveis fossem clonadas ou fraudadas, seria necessária uma pequena cirurgia para adequação e/ou manutenção do sistema de identificação. O cidadão, portanto, tem que estar cons-

ciente disso. A criação, porém, de um modelo não implantável, poderia trazer a continuação da perturbação de possível perda ou roubo. Por outro lado, seria mais fácil que a etiqueta fosse trocada ou reposta. Fato é que a possibilidade de fraude deve também levar à proposição da seção anterior de que o usuário deva conhecer e concordar com os riscos do implante do sistema de identificação.

Pode-se ainda, em virtude das possíveis fraudes, propor que a legislação RFID deva expressar explicitamente que tal sistema sofre os riscos inerentes a qualquer tecnologia da computação, que os operadores do sistema tenham expressamente definidas suas responsabilidades de proteção ao usuário e também que determine qual seria a responsabilidades de tais operadores em ocasiões de vazamento de informações.

### 5.4.5 Rastreamento

O cidadão deve ter o direito de desligar sua etiqueta quando o desejar, assim como, por exemplo, faz com o celular. Desta forma, nos momentos em que julgar necessário, o cidadão teria o direito de não estar sendo observado. Deve ser lembrado que as etiquetas implantáveis já estão em uso como mecanismo de segurança. Como tais etiquetas não podem ser desligadas, os usuários podem ser observados vinte e quatro horas por dia. Começa a ser desenhado então um cenário em que se uma legislação eficaz não proteger o cidadão, este estará sem acesso à privacidade que ainda encontra hoje. A legislação deve também oferecer ao usuário opções por etiquetas de baixa e de alta freqüência, uma vez que estas diferenças implicam na capacidade de os sistemas coletarem dados do usuário. Um exemplo a ser seguido, é a *Senate Bill 362* do estado americano da Califórnia. Esta lei prevê uma multa de dez mil dólares por implantes considerados compulsórios, mais mil dólares por dia em que o *chip* esteja implantado no cidadão coagido.

Um outro ponto também muito importante deve ser considerado. Salvo em casos claros de desaparecimento e seqüestro, as informações da localização de um cidadão não podem ser fornecidas nem a parentes, uma vez que se o usuário desejar se manter incógnito, assim deve ser. No caso em que o usuário queira que a família saiba onde o mesmo se encontra, um simples telefonema pode satisfazer seu objetivo. Isso tem o único objetivo de manter livre o ir e vir do cidadão. Permitir que outros cidadãos tenham acesso a informações de uma pessoa, mesmo que parentes, pode gerar uma sociedade vigiada. Além disso, nenhuma empresa pode garantir que um cidadão permitiu que sua família tivesse acesso a quaisquer informações sobre seu respeito sem coação de alguma forma.

### 5.4.6 Alcance dos Leitores

A legislação deve ainda regulamentar o uso dos leitores RFID no que se refere aos locais onde podem ser instalados, determinando justificar diante da legislação qual o objetivo em se utilizar cada leitor. Este item seria a

continuidade da regulamentação da coleta de dados.

### 5.4.7 Prevalência dos Direitos Humanos

Deve-se impedir que mesmo no futuro a RFID possa estar aplicada ao controle de cidadãos por regimes políticos antidemocráticos. O Brasil respeita a soberania de outras nações. Entretanto, a legislação brasileira deve apresentar a condição de que o Brasil não apoiaria o uso de RFID para identificação de indivíduos em países onde os regimes de governo não são democráticos, uma vez que o Brasil tem por princípio não apoiar perseguições políticas, conforme pode ser verificado na Constituição Federal, em seu artigo 4º, inciso X. Não há garantias de que tais regimes respeitariam os direitos humanos de oposicionistas. A prevalência dos direitos humanos também está elencada no artigo 4º da Constituição Brasileira, inciso II. Apresentar tal mecanismo na legislação sobre a RFID seria a ratificação a tais incisos; mais importante, reforçaria a imagem de que o Brasil estimula o uso responsável e democrático da RFID.

### 5.4.8 Liberdade de Escolha

Seria ainda interessante que a regulamentação trouxesse consigo a capacidade de estimular outras ferramentas de proteção contra a violência visando substituir os implantes RFID por outras formas de identificação em humanos, uma vez que esta tecnologia gera debates inclusive sobre até que ponto uma pessoa pode ser etiquetada como é uma cabeça de gado ou um pacote de lâminas de barbear. O ideal é que seres humanos não fossem etiquetados.

A legislação deve manter a preocupação em ser pluralista, respeitando a cultura, a religião e as liberdades de pensamento dos cidadãos. Muitos cidadãos podem se sentir invadidos em sua privacidade pelo simples uso de etiquetas que não podem ser desligadas, estejam elas aplicadas a quaisquer objetivos. A legislação deve prever como respeitar tais casos.

Há ainda casos preocupantes em que a legislação deve determinar como contornar problemas e evitar a coação de cidadãos. Algumas correntes cristãs, por exemplo, consideram a RFID um empreendimento satânico. Tais correntes defendem que etiquetas implantáveis seriam o cumprimento de profecias do livro bíblico do Apocalipse, onde uma certa marca de identificação na mão direita ou na testa seria obrigatória a todos os cidadãos do mundo para poderem realizar operações financeiras de compra e venda, sendo então vigiados e controlados pelo governo de um anticristo, que obrigaria o cidadão a professar uma religião instituída, diferente de sua fé cristã. O fato de que as marcas no Apocalipse estariam na mão direita ou na testa, mas etiquetas RFID podem ser colocados em várias partes do corpo, pode afastar um pouco esta idéia. Entretanto, sendo adeptos de crenças religiosas, que são fruto de fé, estes cidadãos têm que ver preservados seus direitos fundamentais e não devem ser coagidos ao uso de tal sistema.

A coação não se dá apenas com ameaças explícitas e isso também deve ser objeto de atenção. Voltando ao caso mexicano, em que autoridades aderiram ao sistema de identificação pela RFID, pergunta-se: quantos dos membros deste governo realmente sabem do impacto desta tecnologia sobre suas vidas? Entre os que sabem no que implica usar sistemas como este, quantos realmente foram voluntariamente etiquetados? Deve-se verificar que a simples concordância não implica que não houve alguma forma de coação. No exemplo mexicano, bem como em casos de etiquetamento por empresas privadas, a possibilidade de se indispor com os que propõem o etiquetamento, tendo como conseqüente o risco de perda de prestígio público ou posto de trabalho, já pode ser uma forma de coação. A legislação deve prever qualquer forma de coação como crime e evitar sua prática a partir da imposição de penalidades bem definidas, tanto para o setor público quanto para o setor privado.

A coação pode ocorrer de uma forma tão sutil que é possível que o cidadão não perceba. Imagina-se um cenário onde a RFID seja utilizada amplamente no comércio, como são utilizados cartões, tendo em vista o interesse de grupos econômicos na redução de custos operacionais. Usuários relutantes em aderir à nova tecnologia poderiam ser sobretaxados. Assim, a adesão ao uso da RFID não pode ser considerada voluntária, mas forçada por aqueles que detêm o poder econômico. Vale aqui a analogia com o sistema monetário, onde não deve ser discriminado o indivíduo que opte, por exemplo, pela utilização do papel-moeda em detrimento de sistemas eletrônicos. A legislação deve prever, evitar e penalizar os responsáveis por tais casos de coação.

### 5.4.9 Identificação de Automóveis

Outro aspecto a ser levado em conta é a questão de identificação RFID em automóveis. Conforme já citado, o DENATRAN pretende que todos os automóveis do país estejam etiquetados em breve. Entretanto foi muito pouco discutido o tipo de impacto que isto pode ter na privacidade do cidadão. Embora os gestores deste tipo de sistema garantam não publicar os dados de usuários, a proposta de uma legislação para a utilização da RFID deve também ser rigorosa no sentido de evitar qualquer divulgação de informação dos automóveis etiquetados. Os objetivos em etiquetar carros – fiscalização e segurança – praticamente impedem o uso de etiquetas que possam ser desligadas. Deve ser estudado, porém, um meio termo no futuro, nos quais uma etiqueta poderia, por exemplo, ser desligadas por alguns períodos. Enquanto não se encontra esta solução, a legislação deve coibir a divulgação de informações sobre as movimentações do veículo que não ao dono do mesmo.

### 5.4.10 Órgão Regulador

Conforme visto na Seção 5.2, a ICP-Brasil teve um comitê gestor formado pelo governo. Mesmo os ditos representantes da sociedade civil foram indicados pelo Estado. Nas discussões da implementação da infraestrutura para a RFID a sociedade civil deve também participar da elaboração da legislação final, bem como da formação de seu comitê gestor. Espera-se, entretanto, que a indicação dos representantes da sociedade civil seja, de fato, feita por esta sociedade, contemplando todas as correntes sociais às quais interessa o debate sobre a RFID. Estes representantes devem entender não somente os aspectos técnicos e jurídicos da RFID, como também quais as demandas sociais que podem sofrer o impacto causado pelo uso desta tecnologia.

Em casos de violações de quaisquer aspectos expostos na legislação, ou violações do sistema, a empresa gestora das informações violadas deve responder pela quebra dos direitos do usuário, uma vez que, como dito anteriormente, a manutenção de informações deve ser fundamentada nos objetivos da empresa e que o fato de se manter informações implica na obrigação de protegê-las.

A ICP-Brasil gerencia chaves públicas. A RFID, entretanto, é um sistema um pouco mais complexo. Assim, um aspecto indispensável na legislação sobre a RFID é indicar claramente qual o papel de cada ente envolvido no sistema. O objetivo é evitar quaisquer conflitos de competência, para evitar que casos de violações acabem em um jogo de empurra-empurra, onde os responsáveis não são punidos pela quebra das normas. Seria inclusive interessante estudar a criação de um órgão regulador de informações, a exemplo do que ocorre no Japão. Este órgão teria o papel principal de proteger as informações colhidas por sistemas RFID, fiscalizando os coletores de informações, o que fazem delas, entre outras obrigações. O órgão regulador de informações determinaria também aspectos relativos ao uso de informações colhidas por outros meios, uma vez que não só por RFID se quebra a privacidade de usuários. Daí a necessidade de um novo órgão, uma vez que órgãos regulamentadores e fiscalizadores existentes no Brasil cumprem outros funções. Esta pode ser a justificativa para que, por exemplo, a ANATEL, a Agência Nacional de Telecomunicações, não realize este papel. Um outro órgão, porém, não substituiria o papel da ANATEL, na fiscalização do espectro, como também não substituiria a ICP-Brasil, que tem outros objetivos operacionais.

Pode-se também entender que a proteção à privacidade possa ser dividida entre os vários órgãos já existentes, sendo entretanto integrada por um possível Conselho Nacional de Proteção de Dados, composto por vários órgãos governamentais que regulamentam setores capazes de coletar dados diversos. Assim, cada órgão em seu setor de operação específico poderia conter algum seção direcionada à proteção de dados. O custo de criação desta segunda hipótese seria bem menor, uma vez que isentaria o Estado de criar um novo órgão.

Para o entendimento do que existe especificamente em telecomunica-

ções, que inclui radiofreqüência e privacidade, a Lei Geral de Telecomunicações (Lei Nº 9.472, de 16 de julho de 1997), em seu artigo 72, diz que "apenas na execução de sua atividade, a prestadora poderá valer-se de informações relativas à utilização individual do serviço pelo usuário". Está expresso, portanto, na Lei Geral de Telecomunicações, que o usuário tem o direito à preservação de sua privacidade. Mais restritamente expõe-se, no parágrafo primeiro, que "a divulgação das informações individuais dependerá da anuência expressa e específica do usuário". No segundo parágrafo fica estabelecido que "a prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade". Então, parte dos direitos à privacidade do cidadão que utiliza meios de telecomunicações já se encontra protegido, embora de maneira genérica.

A Lei Geral de Telecomunicações dispõe sobre a organização dos serviços de telecomunicações e a criação e funcionamento de um órgão regulador, a ANATEL. O papel da ANATEL inclui, além da organização e distribuição do espectro, a fiscalização dos serviços prestados como serviços de telecomunicações. A fiscalização deste órgão regulador incide sobre os operadores de quaisquer serviços de telecomunicações, incluindo as relações entre consumidores e operadores, além de seus respectivos direitos e deveres. A ANATEL também é responsável por fiscalizar interferências de operadores não outorgados de sinais de transmissão em ondas de operadores outorgados. Dessa forma, a ANATEL participa de parte do policiamento de crimes perpetrados em alguns meios de telecomunicações. A ANATEL, porém, não se responsabiliza pelo que ocorre com a informação indevidamente trafegada. Ela tem apenas o papel de identificar e coibir o tráfego ilegal de telecomunicações em casos de transmissões por meio do espectro ou outros meios classificados como meios de telecomunicações.

Logo, sobre sistemas baseados na RFID, há, além da distribuição das faixas de freqüência, alguns papéis possíveis para a atuação da ANATEL. O primeiro é a fiscalização das empresas legalmente operadoras de sistemas baseados nesta tecnologia com relação às coletas e manutenção de informações. Outro papel é o de auxílio no policiamento de tráfego de ondas indevidas de interferência no sistemas RFID, com ou sem capacidade de roubo de informações, com possibilidade de identificação de operadores indevidos por meio de ações de fiscalização.

Supondo, portanto, que a ANATEL assumisse novas atribuições, por já ser responsável pela fiscalização de parte específica dos sistemas baseados na RFID, ela deveria incorporar em sua estrutura de uma futura Superintendência de Proteção do Consumidor uma gerência de proteção de dados. O fato é que a proteção do consumidor pela ANATEL ainda é deficiente, por falta de pessoal e infra-estrutura adequadas à proteção de relações de consumo que a ANATEL já fiscaliza. A já existente Assessoria de Relações com os Usuários não tem o poder de punição que possuem outros departamentos da ANATEL, justamente por não ser uma Superintendência. Tal fato tem conduzido a situações onde os consumidores acabam vítimas de problemas que se repetem milhares de vezes sem que haja uma punição eficaz às ope-

radoras de telecomunicações. A fiscalização da proteção de dados exige um poder coercitivo que este departamento da ANATEL não está pronto para exercer, por falta de poder legal e por falta de infra-estrutura.

Somam-se a esta situação dúvidas que a eventual legislação sobre RFID deve responder: será que o papel da ANATEL deve limitar-se à atribuição de faixas do espectro na RFID? Se a obtenção indevida de dados utilizar meios de telecomunicações, não deveria a ANATEL participar da fiscalização? Afinal, muitos modos de uso da RFID são utilização de sistemas de telecomunicações, se observada a forma de funcionamento do sistema. A legislação sobre a RFID deve especificar até onde um sistema pode ser classificado como de telecomunicação.

Pode-se também estudar qual seria o papel do ITI nesse novo contexto. O fato é que o ITI não é uma agência reguladora e seu papel de autoridade certificadora da ICP-Brasil contribui muito pouco para a proteção do cidadão, uma vez que certificar a emissão de chaves públicas ou privadas não implica em punição a quem emite uma chave falsa. Com certeza, devido à enorme aplicabilidade da RFID, muitas empresas explorarão este negócio. Tanto a ANATEL, quanto o ITI e a ICP-Brasil estarão envolvidos na gestão do sistema.

Num possível cenário onde a RFID já esteja mais difundida, será certamente muito freqüente a entrada de novos processos judiciais envolvendo privacidade. De momento, a proteção à privacidade do usuário ainda se encontra quase que totalmente nas mãos do Poder Judiciário e, em alguns casos, da Polícia. A questão pode ainda se encontrar prejudicada pelo fato de nem sempre os processos judiciais tramitarem em tempo hábil a coibir a prática de delitos no campo de informações sobre cidadãos. Daí a necessidade de um órgão ou conjunto de órgãos participantes de um sistema, que possa gerir processos na esfera administrativa com capacidade para imposição de multas aos responsáveis por violações, sem prejuízo das ações do Judiciário. A questão é que violações de privacidade, pela consecução e fornecimento indevido de dados, devem ser inibidas de todas as formas.

## 5.5 Os Primeiro Passos

Alguns dos mecanismos de proteção de dados aqui expostos já estão previstos no Projeto de Lei sobre Crimes Digitais. Entretanto, tal projeto não foi votado e logo ainda não é lei. O Projeto limita, por exemplo, a coleta de dados, por meio da aquiescência do usuário; limita a manutenção de cadastros por um tempo determinado; proibe a coleta e manutenção de dados à revelia; e garante o acesso peloo usuário aos dados sobre si em bancos de dados. O Projeto por meio do artigo 7º expressa ainda que:

> "As entidades que coletam, armazenam, processam, distribuem ou comercializam informações privadas, ou utilizam tais informações para fins comerciais ou para prestação de serviço de qualquer natureza, ficam obrigadas a explicitar, desde o início de tais

atividades:

I - os fins para os quais se destinam tais informações; e

II - os limites de suas responsabilidades no caso de fraude ou utilização imprópria das informações sob sua custódia, bem como as medidas adotadas para garantir a integridade dos dados armazenados e a segurança dos sistemas de informação".

No artigo 8º, o Projeto estabelece que

> "(...) entidades mencionadas no artigo anterior não poderão divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica ou religiosa, crenças, ideologia, saúde física ou mental, vida sexual, registros policiais, assuntos familiares ou profissionais, e outras que a lei definir como sigilosas, salvo por ordem judicial ou com anuência expressa da pessoa a que se referem ou do seu representante legal".

Pode-se dizer então que os primeiros passos para esta legislação que regulamentaria a RFID já foram dados. Entretanto, a lei específica para RFID deverá também abordar outros pontos, como evitar coletas de dados por pessoas não autorizadas ou mesmo discriminar que as mesmas implicações dos artigos 7º e 8º do Projeto de Lei de Crimes Digitais estariam aplicadas a coletas com o uso da RFID. Indiretamente, o Projeto de Lei de Crimes Digitais informa que é crime a coleta indevida de dados caracterizando como pena possível seis meses a dois anos além de multa.

A lei sobre RFID pode ir mais além e limitar o próprio comércio de equipamentos deste tipo de sistema. O comércio não autorizado de equipamentos baseados em RFID deve ser criminalizado. Deve-se estabelecer também penas mais enérgicas, uma vez que a violação de direitos fundamentais atenta contra a própria democracia, que é a ordem de formação do Estado Brasileiro.

Concluindo, o grande objetivo em se estabelecer uma legislação sobre a RFID no Brasil é o respeito ao cidadão. Depois da promulgação da Constituição de 1988, o cidadão passou a ter direitos fundamentais que antes não possuía. Não se deve retroceder em direitos civis. O Regime Militar que vigorou neste país de 1964 a 1985 já maculou a história da nação com desrespeito aos direitos humanos, violações à liberdade de pensamento e de expressão e, em certo grau, até mesmo o direito de ir e vir. Este país precisa agora evitar que uma tecnologia que pode beneficiar o cidadão vire arma para violar seus direitos.

# Capítulo 6

# Conclusão

Neste trabalho foi exposto o que é a tecnologia de Identificação por Radiofreqüência (RFID), como pode ser aplicada e como ela ameaça a privacidade de seus usuários. Foi analisado como a legislação brasileira protege a privacidade do cidadão e como pretende proteger o cidadão diante do avanço das tecnologias computacionais.

No Capítulo 5, viu-se que o Projeto de Lei de Crimes Digitais, que até a conclusão deste trabalho não havia ainda sido votada no congresso brasileiro, contempla a proteção de dados pessoais coletados por meios eletrônicos. Pode-se interpretar que a RFID estaria contemplada na expressão "meios magnéticos ou afins". Pode-se notar, entretanto, que embora traga consigo o aspecto de defender o cidadão diante de bancos de dados eletrônicos, o Projeto de Lei de Crimes Digitais e as demais leis de proteção aos direitos do usuário não são eficientes diante das possibilidades que a RFID carrega consigo.

Foi verificado que a própria definição de privacidade se vê pressionada a um detalhamento maior por parte dos legisladores brasileiros, em virtude do que a tecnologia como um todo, e em particular a RFID, pode realizar em termos de quebra dos limites da vida privada. A tecnologia pode estar conduzindo à rediscussão de conceitos jurídicos. Esta mesma tecnologia conduz à urgência de lei complementar sobre privacidade, sobre normatização de uso de tecnologias como a RFID para preservação da privacidade, assim como outros direitos fundamentais necessitaram de um maior detalhamento por meio de lei para coibir suas violações.

O presente trabalho defende ainda que a disseminação da tecnologia deve ser acompanhada da disseminação de informações sobre a tecnologia, suas implicações sobre direitos em geral e os direitos do usuário nas normas de uso desta tecnologia, como ocorre em países onde esta discussão já se encontra mais avançada.

Além do detalhamento em casos gerais, a legislação de proteção à privacidade deve prever uma regulamentação específica sobre a coleta, o armazenamento e a utilização de dados, além da normatização do uso de equipamentos para estas atividades. O Projeto de Lei de Crimes Digitais determina que a coleta deve ser justificada e que os dados não podem ser mantidos para objetivos diversos dos objetivos da coleta. No entanto o pre-

sente trabalho defende que se deve avançar mais na defesa dos direitos de privacidade, sugerindo que os estabelecimentos comecem desde já a serem regulamentados no que têm o direito de coletar frente ao tipo de negócio desenvolvido. A lei já apresenta carências, como a da necessidade, tão logo a RFID comece a ser mais aplicada, de se detalhar os modelos de etiquetas a serem usados em cada aplicação, bem como os demais equipamentos envolvidos. A lei deve já impor aos estabelecimentos que estes disponibilizem diversos mecanismos para orientar o usuário no conhecimento da RFID e de seus direitos diante da aplicação desta tecnologia.

O presente trabalho sugere ainda que, para identificação de humanos, a RFID não seja aplicada sem que o usuário tenha opções por diferentes tipos de etiquetas eletrônicas. O cidadão deve ter o direito de desligar cada etiqueta aplicada no seu dia a dia; em caso de impossibilidade do desligamento, determinado pela atual tecnologia, a legislação deve apresentar mecanismos de incentivo à criação de etiquetas que possam ser desligadas.

Ainda se destaca que urge o estabelecimento de um órgão regulador ou conselho de proteção de dados capaz de coordenar os diversos órgãos do governo na proteção de dados, devendo existir poder de coerção contra as operações indevidas de sistemas baseados na RFID, no âmbito administrativo. Isto deve ocorrer porque a lei sobre RFID deve dispor quem terá o direito de explorar estes serviços, como e porquê. Assim, deve existir um órgão com o poder de tanto advertir os operadores, bem como de retirar suas licenças de operação em casos de violações de normas. Este órgão deverá ser diverso da Polícia e do Poder Judiciário, mas sem prejudicar as ações destes últimos.

Enfim, ante o crescimento da RFID, surge a necessidade de começar a detalhar, como já acontece na regulamentação de outros setores, os direitos do usuário, dos estabelecimentos, os modelos de etiquetas para cada aplicação. Esta legislação deve tanto quanto possível se antecipar à disseminação da Identificação por Radiofreqüência dando ao usuário mecanismos de optar quanto às formas de uso da tecnologia. A base do uso da RFID deve ser a de que toda tecnologia deve estar a serviço do bem-estar do cidadão e da defesa dos direitos democráticos.

# Referências Bibliográficas


[ACLU 2004] AMERICAN CIVIL LIBERTIES UNION. *Data Mining*. 2004. Disponível em http://www.aclu.org/privacy/spying/14956res20040116.html. Acesso em 12/06/08.

[ACLU 2008] AMERICAN CIVIL LIBERTIES UNION. *Stunning New Report on Domestic NSA Dragnet Spying Confirms ACLU Surveillance Warnings*. 2008. Disponível em http://www.aclu.org/privacy/gen/34441prs20080312.html. Acesso em 12/06/08.

[Barra 2006] BARRA, M. C. *Infra-estrutura de chaves públicas brasileira (ICP-Brasil) e a formação do Estado Eletrônico*. Dissertação (Dissertação de Mestrado) — Universidade de Brasília, Brasília - DF, 2006.

[Bernardo 2004] BERNARDO, C. G. A tecnologia rfid e os benefícios da etiqueta inteligente para os negócios. *Revista Eltrônica de Produção Científica - Unibero*, Unibero, 2004. ISSN 1806-6968. Disponível em http://www.unibero.edu.br/download/revistaeletronica/Set04_Artigos/A Tecnologia RFID-BSI.pdf. Acesso em 06/05/2008.

[Bolzani 2003] BOLZANI, C. A. M. *Computação Pervasiva e Sistemas de Identificação*. 2003. Disponível em http://www.bolzani.com.br/artigos/art01_04.pdf. Acesso em 06/05/2008.

[Cavoukian 2006] CAVOUKIAN, A. Tag, you're it: Privacy implications of radio frequency identification (rfid) technology. *The Office Ontario Government Documents Collection*, Information and Privacy Comissioner, 2006.

[Clarke 1994] CLARKE, R. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, Emerald, v. 7, n. 4, 1994.

[Clarke 2006a] CLARKE, R. Introduction to dataveillance and information privacy, and definitions of terms. *TVET Australia Product Services*, TVET Australia Limited, 2006. Original de 15 August 1997, últimas revisões. 16 September 1999, 8 December 2005, 7 August 2006. Disponível em http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

[Clarke 2006b] CLARKE, R. *What's 'Privacy'?* [S.l.]: TVET Australia Limited, 2006. Prepared for a Workshop at the Australian Law Reform Commission - Disponível em http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html.

[Crawford et al. 2003] CRAWFORD, S. Y.; COHEN, M. R.; TAFESE, E. System factors in the reporting of serious medication errors in hospitals. *Journal of Medical Systems*, Plenum Press - New York USA, v. 7, n. 6, 2003.

[Dominique 2005] DOMINIQUE, P. Technical state of art of "radio frequency identification - RFID" and implications regarding standarization, regulations, human exposure, privacy. In: *RFID and Contactless Smart Cards Applications*. [S.l.]: ACM Press, 2005.

[Lima 2005] LIMA, V. M. B. Vida de gado: O uso de implantes eletrônicos de identificação e o direito de privacidade. *Instituto Brasileiro de Política e Direito da Informática*, Instituto Brasileiro de Política e Direito da Informática, 2005. Disponível em http://www.ibdi.org.br/site/artigos.php?id=73.

[Lockton e Rosenberg 2005] LOCKTON, V.; ROSENBERG, R. S. RFID: The next serious threat to privacy. *Ethics and Information Technology*, Springer Netherlands, v. 7, n. 14, 2005.

[Matos 2003] MATOS, C. L. *Smart Card*. Rio de Janeiro - RJ: 2003. Disponível em http://www.gta.ufrj.br/grad/012/smart@card/smartcard.html.

[Pilieci 2008] PILIECI, V. *Copyright deal could toughen rules governing info on iPods, computers*. 2008. The Vancouver Sun. Disponível em http://www.canada.com/vancouversun/story.html?id=ae997868-220b-4dae-bf4f-47f6fc96ce5e&p=1. Acesso em 12/06/2008.

[Presidência da República 2001] PRESIDÊNCIA DA REPÚBLICA. *Medida Provisória 2.200-2*. 2001. Disponível em http://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm.

[Reinaldo Filho 2006] REINALDO FILHO, D. A implantação de chips em seres humanos para uso médico e os riscos é privacidade. *Jus Navigandi*, Jus Navigandi LTDA, Ano 10, n. 1191, 2006. Disponível em http://jus.uol.com.br.

[Rezende 2004] REZENDE, P. A. D. *Identificação Digital*. 2004. Disponível em http://www.cic.unb.br/docentes/pedro/trabs/idpf2004.pdf. Acesso em 24/06/2008.

[Rigaux 2000] RIGAUX, F. *A Lei dos Juízes*. Instituto Piaget, 2000.

[Savadintzky 2006] SAVADINTZKY, L. *Informação e privacidade: direito à informação e à intimidade não podem se agredir*. Revista Consultor Jurídico, 2006.

[Secom GDF 2007] SECRETARIA DE COMUNICAÇÃO DO GOVERNO DO DISTRITO FEDERAL. *TAGUATINGA – Cadastro de carroceiros termina nesta quinta-feira (13)*. 2007. Disponível em http://www.df.gov.br/003/00301009.asp?ttCD_CHAVE=53956. Acesso em 06/05/2008.

[Smith et al. 2005] SMITH, J. R. et al. RFID-based techniques for human-activity detection. *Comunications of the ACM*, ACM Press, v. 48, n. 9, 2005.

[Vieira 2003] VIEIRA, J. L. P. Direito e privacidade na contemporaneidade: desafios em face do advento do correio eletrônico. *Jus Navigandi*, Jus Navigandi LTDA, Ano 7, n. 66, 2003.

[Zorzo e Grande 2006] ZORZO, S. D.; GRANDE, R. E. *Privacidade na Web*. 2006. Disponível em http://www.dc.ufscar.br/ zorzo/download/MiniCurso-aula1.ppt.