CONSULTORIA LEGISLATIVA

PRIVACIDADE E INTERNET

Bernardo F. E. Lins
Consultor Legislativo da Área XIV
Comunicação Social, Telecomunicações,
Sistema Postal, Ciência e Tecnologia

ESTUDO

MARÇO/2000

Câmara dos Deputados
Praça dos 3 Poderes
Consultoria Legislativa
Anexo III - Térreo
Brasília - DF

ÍNDICE

PRIVACIDADE E INTERNET

Bernardo F. E. Lins

1. INTRODUÇÃO

O tema da privacidade é clássico na literatura da área jurídica, em virtude das inúmeras implicações que oferece para a doutrina. Aspectos análogos aos que interessam à relação entre privacidade e Internet têm sido tratados, em especial, diante da questão da relação entre a imprensa e indivíduo, uma vez que a primeira detem o direito e a obrigação de apurar e informar a sociedade acerca de acontecimentos de interesse público, invadindo, não raro, o direito à privacidade daqueles que são atingidos com a divulgação de notícias que os citem, ou até prejudiquem.

No entanto, nos últimos dez anos, o assunto da privacidade ganhou novas facetas, em virtude da disseminação das tecnologias de tratamento da informação. São essencialmente três os fenômenos que vêm contribuindo para uma maior preocupação com o tema: primeiramente, a estruturação de bases de dados, que abriu a possibilidade de se cruzar informações com grande facilidade, construindo perfis detalhados de praticamente qualquer pessoa, a um custo baixo, até mesmo sem a ciência do interessado; em segundo lugar, a disseminação da informática, que culminou com a ampla utilização da Internet, estimulando praticamente a todos a manterem em forma digital as suas informações, facilitando a sua coleta; e, finalmente, a padronização de equipamentos e sistemas, o que facilitou a aquisição de informações mantidas por usuários de informática, inclusive sem o seu conhecimento.

Na sociedade atual, que usa intensivamente a informação, o uso de dados pessoais para fins comerciais tornou-se prática corrente, que permite a fornecedores e produtores de todo tipo de mercadoria ou serviço alcançarem vantagens sobre seus concorrentes. Assim, perfis de consumidores bem elaborados, consolidando informações diversificadas, são de grande valia para todo tipo de empresa. Cate (1997, p. 2) cita alguns exemplos de dados pessoais que são coletados e cruzados a partir das nossas atividades usuais:

a) Cartórios, hospitais, seguradoras e bancos detêm informações sobre o nosso histórico familiar, financeiro e de saúde.

b) Empresas telefônicas mantêm cadastro dos números mais usados e da freqüência de ligações.

c) Editoras mantêm informações sobre hábitos de leitura e procuram elaborar perfis econômicos dos assinantes.

d) Operadoras de cartão de crédito elaboram perfis de consumo e histórico de compras.

e) Mercados e lojas mantêm histórico de consumo de alimentos, bebidas, vestuário, automóveis, aparelhos elétricos e outros bens e serviços.

f) Provedores na Internet mantêm registro de acesso a *sites*, envio e recebimento de e-mails e preferências de material acessado.

O cruzamento de informações permite a criação de retratos que mostram os nossos principais hábitos e práticas, revelando facetas das quais o próprio indivíduo muitas vezes não se apercebe. Podem ser elaborados por empresas privadas, para fins comerciais, ou por órgãos do governo, inclusive para fins de investigação criminal.

Tais práticas constituem um problema social e jurídico de grande interesse, uma vez que é preciso determinar até que ponto e de que forma poderão ser exercidas, se é que o podem, sem constituir uma violação da privacidade pessoal.

Este estudo aborda a questão analisando, primeiramente, os problemas de privacidade em face da Internet . A seguir, na seção 3, são examinados os aspectos relacionados com a estruturação e o cruzamento de bases de dados, no que diz respeito à sua implicação para a privacidade. Na seção 4 são discutidas as implicações para a privacidade das operações de intercâmbio de informações, o que enseja um breve comentário sobre as técnicas de criptografia. Na seção 5, enfim, apresentam-se as conclusões do trabalho.

2. A PRIVACIDADE E ALGUMAS DE SUAS IMPLICAÇÕES PARA A INTERNET

2.1 Direito à privacidade

O direito à privacidade nasceu da mudança de hábitos e costumes decorrente da ascensão da burguesia no século XVIII. Com a modernização do espaço urbano e a criação de várias facilidades domésticas, inúmeras atividades que eram exercidas comunitariamente, ou ao menos sem qualquer intimidade, passaram a fazer parte da vida particular das pessoas, dando a noção de um direito à privacidade. Este, embora seja um direito não escrito em muitos países, é hoje considerado parte essencial da liberdade. "O direito de ser deixado a sós é o começo de toda liberdade" (Meyer, 1987, p. 122, citando o juiz William O. Douglas).

A nossa Constituição Federal estabelece, como direito básico da pessoa o direito à privacidade:

> "*Art. 5º* .....
> .....
> *X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*
> .....=....".

2.2 Direito à privacidade, liberdade de imprensa e Internet

Com a expansão da imprensa, tornou-se claro o conflito entre o princípio da liberdade de imprensa e o direito à privacidade. Nas muitas situações em que estes entram em choque, configuram-se situações que o uso da Internet vem reproduzindo, com algumas especificidades. Segundo Meyer (1987, p. 124), duas são as razões que levam à violação da privacidade pela mídia: a revelação de fatos privados embaraçosos e o uso de métodos de reportagem questionáveis.

Se considerarmos a similaridade entre imprensa escrita e apresentação de informações no formato hipertexto usado na Web, estarão presentes as mesmas motivações que se encontram subjacentes às violações da privacidade cometidas pela imprensa. Servirão como referência, nesse caso, os princípios, práticas e disposições legais vigentes para a imprensa, que comentaremos brevemente a seguir.

A legislação de imprensa deveria tratar do conflito entre a liberdade de imprensa (ou seja, o direito de informar e expressar a opinião sobre um fato) e o direito à privacidade (ou seja, o direito do indivíduo em preservar a sua intimidade e vida privada, evitando que fatos a seu respeito sejam divulgados ou comentados). No entanto, a Lei de Imprensa vigente, Lei nº 5.250, de 9 de fevereiro de 1967, não caracteriza de maneira clara a violação à privacidade. Esta só fica evidenciada nos casos dos crimes contra a honra (calúnia, difamação, injúria e ofensa à memória dos mortos), abordagem evidentemente insuficiente.

Outro fator que restringe a eficácia da nossa Lei de Imprensa para tratar do conflito entre a liberdade de informar e o direito à privacidade são as limitações estabelecidas às indenizações por danos materiais e morais. Além disso, no caso específico da Internet, esta não se enquadra adequadamente em nenhuma das categorias de meios de imprensa conceituados na lei.

Já na legislação de outros países os conflitos entre privacidade e o direito de informar encontra um tratamento mais amadurecido. Nos EUA, por exemplo, liberdade de imprensa, direito à privacidade e censura são tratados à luz das interpretações dadas à Primeira Emenda à Constituição daquele país, que determina que "o Congresso não fará lei que limite a liberdade de expressão e de imprensa"[1].

À época de sua promulgação parecia ser simples aplicar a Primeira Emenda. Porém, com o crescimento, a abrangência e a diversificação dos meios de comunicação social foi tornando-se mais complexa a tarefa de interpretar adequadamente o espírito da disposição e a sua aplicação.

A Suprema Corte norte-americana desenvolveu, então, doutrinas de aplicação da primeira emenda. Talvez a mais clássica dessas teorias seja a do "livre intercâmbio de idéias"[2], segundo a qual a primeira emenda serve de proteção da verdade que emerge da discussão pública de idéias conflitantes. Interpretação similar é a de que a primeira emenda assegura um fluxo de debate que fundamentaria o autogoverno responsável do país. Essas teses redundam numa proteção quase que absoluta de qualquer pensamento, expressão ou comunicação, prejudicando outros direitos, inclusive o da privacidade. De fato, a limitação a qualquer forma de expressão, em qualquer nível, torna-se impossível e a liberdade é absoluta. Algumas ações recentes na Suprema Corte ainda foram decididas conforme essa visão[3].

Casos mais complexos não foram, porém, resolvidos segundo essa linha doutrinária. Há, na verdade, quatro linhas básicas de interpretação sendo adotadas: além da adesão absoluta à emenda, adota-se o teste do "perigo claro e presente", o balanceamento de interesses e o balanceamento de definições.

O teste de "perigo claro e iminente" foi proposto em 1919[4], e permitiria punir a expressão de pensamento cujas palavras, em virtude da sua natureza e das circunstâncias em que fossem usadas, constituíssem um perigo claro e iminente de provocar males que o Congresso tivesse o direito de evitar, tendo em vista tais circunstâncias e o grau da expressão.

Já a tese do balanceamento de interesses "ad hoc" reconhece que outros direitos fundamentais, tais como o de um processo judiciário equânime e justo, ou o de preservar a intimidade do cidadão, podem entrar em conflito com o direito à livre expressão. A liberdade de expressão, nesses casos, não pode ser admitida de forma tão irracional que chegue a paralisar todas as demais liberdades. A defesa da liberdade de expressão não poderia, então, sacrificar os anseios por outras formas de liberdade igualmente preciosas. Decidir com base no balanceamento entre os princípios conflitantes exige, porém, um exame de cada caso, ficando a decisão a critério do juiz, mas a praticidade da abordagem foi por diversas vezes reconhecida[5].

O balanceamento de definições é a tese que advoga a posição de que certas categorias de expressão, por serem profanas, obscenas, panfletárias, injuriosas ou desmedidamente agressivas, não deveriam ser objeto da proteção da primeira emenda[6]. Embora, à primeira vista, essa posição ofereça melhor definição de abordagem do que a anterior, há o problema da dificuldade de se definir o que seja, por exemplo, profano, agressivo ou pornográfico. Também há o risco de se violentar desmedidamente a liberdade de expressão, pois a tese implica em que o interesse da sociedade em restringir certas formas de expressão é sempre mais importante do que a liberdade de expressão em si.

O tratamento da privacidade na Internet herdou a doutrina consolidada pelas decisões acerca de conflitos entre privacidade e imprensa. No entanto, em vista das muitas transformações tecnológicas que a Internet sofreu nos últimos anos, é interessante examinarmos a organização da rede, as suas origens e os serviços disponíveis na mesma para discutir, em seguida, de que forma pode configurar-se a violação à privacidade na rede.

2.3 Internet: origens, formas de comunicação e modalidades de serviços prestados

A Internet surgiu nos anos 60, a partir de um projeto do ARPA, organismo de financiamento à pesquisa ligado ao Pentágono, que desejava construir uma rede de computadores capaz de servir como elo de informações entre pessoas geograficamente isoladas, no caso de uma catástrofe nuclear. A rede, denominada Arpanet, logo mostrou-se um meio de comunicação à distância viável e prático para a troca de mensagens (os chamados "e-mails") e começou a ser amplamente utilizada pelos pesquisadores ligados ao projeto e pelo meio acadêmico em geral.

Embora a rede, à época, não permitisse a visualização de imagens, criou-se um mecanismo para enviar arquivos de programas e imagens apensados ("attached") às mensagens. Outros serviços auxiliares foram criados para a transferência de arquivos (protocolo ftp), para "páginas amarelas" ("gopher"), etc. Com a sua disseminação às universidades de outros países nos anos seguintes, a rede passou a chamar-se Internet.

Posteriormente, com o desenvolvimento de recursos gráficos para os computadores pessoais, tornou-se atraente desenvolver uma solução gráfica para a Internet, o que foi viabilizado com o protocolo http, nos anos 80. Com esse recurso, os computadores puderam receber páginas completas, com textos, imagens, referências a outras páginas e outros recursos (filmes, áudio, etc.). A partir de então, a Internet passou a ser palatável ao grande público e tornou-se uma rede pública mundial, a World Wide Web, acessada com o uso de programas de navegação específicos (os "browsers"). Desde então a Internet disseminou-se rapidamente. Estima-se que, no início dos anos 90, a rede tenha dobrado o número de usuários a cada cem dias.

Essa origem da Internet no meio acadêmico explica algumas de suas peculiaridades: é uma rede em que regras não escritas de educação e etiqueta são rigorosamente seguidas, em que o "livre pensar" é defendido com unhas e dentes e em que determinadas atitudes de cunho comercial, tais como o envio indiscriminado de mensagens, são consideradas deselegantes, sendo combatidas agressivamente.

Com a liberação da Internet ao grande público e a adoção dos “browsers”, a viabilidade de se oferecer serviços pela rede ficou evidente. Livrarias virtuais, como a hoje famosa Amazon Books, serviços de venda de todo tipo de produto pela rede, desde um CD até equipamentos de áudio e vídeo, flores ou comida, surgiram rapidamente. Também surgiram inúmeros serviços noticiosos e até páginas particulares com informações as mais diversas sobre pessoas de todo o mundo. Desses serviços, porém, poucos têm apresentado resultados comerciais satisfatórios, com a pouco honrosa exceção dos serviços de sexo.

Há, portanto, quatro serviços mais populares disponíveis ao usuário da Internet: a apresentação de informações em páginas de hipertexto, que é a Web propriamente dita, através da qual faz-se também comércio eletrônico, “home banking” e outros serviços ao usuário; o correio eletrônico, seja privado, seja em forma de listas de discussão; a transferência de arquivos e a identificação de endereços (“páginas amarelas”). A violação à privacidade pode ocorrer, portanto, no contexto de qualquer um desses serviços. Em alguns casos, decorre da própria natureza da rede que, por ser muito “aberta”, facilita a identificação de usuários e o acesso aos seus equipamentos. Em outros casos, trata-se de pura e simples invasão de privacidade.

2.4 Privacidade na Internet

A privacidade na Internet relaciona-se, de forma análoga à imprensa, à revelação de fatos privados embaraçosos e ao uso de métodos questionáveis para coleta de informações. No primeiro caso, a similaridade com o veículo de imprensa é clara: será violação à privacidade a divulgação, através da Internet, de dados ou fatos que atentem contra a intimidade, a vida privada, a honra e a imagem de uma pessoa. Tal divulgação poderá ser feita por um “site”, por correio eletrônico ou por arquivo disponível para cópia.

No entanto, a Internet traz um agravante: a rede é mundial e o fato poderá ser divulgado em escala nunca antes alcançada por outros meios de comunicação de massa. Tal circunstância levanta, inclusive, aspectos de natureza técnica: os fatos podem ser divulgados a partir de países que, por não dispor de legislação para tal, não punirão a ocorrência, dando um caráter de impunidade à atitude delituosa.

Já o uso de métodos questionáveis encontra amplas variações na Internet, em virtude da diversidade dos recursos de informática hoje existentes. Podem ser classificados nas seguintes categorias:

a) Coleta de informações no computador do usuário, sem o seu consentimento: trata-se de um procedimento mais comum e viável do que se imagina. Pode ocorrer através do uso de programas invasivos ou através da identificação dos acessos feitos pelo computador.

b) Monitoramento da linha de comunicação ou do teclado do computador do usuário através de programas invasivos: trata-se de uma variante mais grave do procedimento anterior.

c) Coleta ou compra de informações sobre o usuário em outros computadores, tais como o servidor que o atende ou os computadores de empresas cujos serviços a pessoa tenha utilizado: nesse caso, os dados podem estar sendo repassados sem o consentimento do interessado.

d) Cruzamento das informações sobre a pessoa, obtidas em sites diversos, sem o seu consentimento explícito: às vezes o usuário, por exemplo, consente que o seu e-mail ou seus dados sejam repassados a terceiros para recebimento de correspondência. No entanto, essa autorização não se estende à elaboração do seu perfil.

e) Violação da comunicação através de dispositivos externos de escuta: trata-se de procedimento incomum, em vista da complexidade dos protocolos de transmissão de dados adotado na Internet, mas viável.

f) Uso do codinome, da senha ou de outros dispositivos de segurança do usuário, para entrar na rede em seu lugar e obter, dessa forma, informações a seu respeito.

As duas últimas modalidades ilustram casos extremos do uso de métodos questionáveis, que se configuram quando estes encontram-se associados à ocorrência criminal. Em tais casos, o infrator adota procedimentos considerados ilegais. Estes, por sua vez, dependem, para a sua caracterização, de uma tipificação criminal clara, o que a legislação brasileira ainda não oferece.

Na legislação norte-americana, por exemplo, o Computer Fraud and Abuse Act, de 1986, entre outros aspectos, pune o mero acesso indevido a uma rede ou serviço. A criminalização do acesso é uma concepção de prevenção de outros crimes e de proteção da privacidade e das informações contidas no sistema. A lei também tipifica outros crimes (uso de senhas de terceiros, fraude, furto de informações, sabotagem, danos a informações, aquisição ilícita de segredos). Tais dispositivos são invocados, entre outros casos, para incriminar os responsáveis pela invasão de equipamentos e recursos computacionais através da Internet, os "hackers".

Já a coleta indevida de dados e a sua disseminação indiscriminada têm sido tratadas na legislação de bases de dados de vários países, tema que será tratado a seguir.

3. TRATAMENTO DE BASES DE DADOS E PRIVACIDADE

3.1 O mercado de bases de dados

Bases de dados são coleções de dados, estruturadas e organizadas com o uso de recursos de informática, de modo a facilitar a seleção e recuperação das informações armazenadas. A tecnologia para o tratamento de bases de dados foi desenvolvida simultaneamente com o computador e bases mantidas para fins comerciais existem desde os anos sessenta.

O mercado de bases de dados sofreu, porém, uma radical transformação nos anos noventa, com a disseminação da Internet. Em 1989, por exemplo, estudo realizado pelo Departamento de Comércio do governo norte-americano sugeria a existência de cerca de 900 empresas provedoras de bases de dados e 300 empresas distribuidoras dessas bases. Esse mercado respondia, à época, por um faturamento global da ordem de US$ 7 bilhões. Hoje, são dezenas de milhares as empresas, entidades sem fins lucrativos e pessoas que mantêm bases de dados e a Internet tem sido o meio preferido para a disseminação das informações armazenadas.

O direito à privacidade do indivíduo em face ao uso de bases de dados pode ser definido como a expectativa de que este possa determinar por si próprio quando, como e em que medida informações sobre si sejam comunicadas a terceiros (Ianotta, 1987). Tal direito fundamenta-se nos seguintes parâmetros:

a) informações pessoais devem ser coletadas segundo procedimentos legítimos, com o prévio conhecimento e consentimento da pessoa a quem as informações se referem;

b) as informações armazenadas em bases de dados não devem ser utilizadas para quaisquer fins distintos daqueles para os quais a base de dados foi criada;

c) o indivíduo tem o direito de saber o que há sobre ele armazenado em uma base de dados;

d) o indivíduo tem o direito de corrigir ou de solicitar a correção ou retirada de dados pessoais incorretos armazenados em bases de dados.

Tais parâmetros tornam-se mais importantes na medida em que já existe, hoje, capacidade de armazenamento de dados suficiente para se elaborar, em nível governamental, um cadastro único contendo informações relevantes sobre boa parte dos habitantes de um país. Códigos como o número de CPF no Brasil ou o número de seguridade social nos EUA e na França poderiam, nesse contexto, ser usados como um número de identificação nacional, facilitando a tarefa. Nesse caso, a perda de privacidade torna-se uma possibilidade factível, com a qual deveremos conviver cada vez mais (Oliveira, 1977).

3.2 Bases de dados e privacidade na legislação comparada

Nos EUA, os aspectos de tratamento de dados pessoais são tratados no Privacy Act 1974, modificado pelo Computer Matching and Privacy Protection Act 1988 e pelo Computer Matching and Privacy Protection Ammendment 1990.

Entre as disposições mais relevantes instituídas por esses instrumentos cabe ressaltar diversas exigências impostas às agências governamentais para que possam fazer cruzamentos de informações entre diferentes bancos de dados, garantir aos indivíduos direitos de acesso a informações pessoais mantidas por órgãos governamentais, bem como a correção das informações armazenadas, e impor práticas éticas ("fair information practices") na coleta, manutenção e disseminação de dados.

Em linhas gerais, a jurisprudência correlata admite as regras da não divulgação sem o consentimento da pessoa cujos dados serão divulgados ("no disclosure without consent"), do registro dos acessos autorizados e do direito de acesso do indivíduo a dados sobre sua pessoa. As agências são obrigadas a seguir, entre outros, os princípios de coletar apenas informações essenciais a suas atividades, coletá-las preferencialmente junto à própria pessoa, informar sobre os meios adotados para a coleta, publicar notícia acerca da natureza e da estrutura do banco de dados no Federal Register e não manter informações sobre como a pessoa exerce seus direitos individuais.

Já na legislação dos países europeus, a privacidade de dados pessoais encontra um tratamento mais orientado ao registro cartorial de provedores de dados e ao acompanhamento de suas atividades. A lei britânica, por exemplo, trata os aspectos relativos à violação de privacidade no Data Protection Act de 1984. O ato criou um "registrar", que é responsável pelo registro e acompanhamento das entidades que processem dados pessoais. A lei estabeleceu, ainda, critérios de proteção do direito autoral de bases de dados eletrônicas.

Disposição congênere é encontrada na legislação da França. Diversos aspectos da privacidade já eram tratados na Lei nº 78-17, de 6 de janeiro de 1978, que regulava aspectos relacionados com informática, bases de dados e privacidade. A lei criou uma comissão para assuntos ligados à informática e privacidade. O processamento de dados pessoais dependia de prévia aprovação da comissão, se efetuado por órgãos públicos ou empresas que estivessem prestando serviços ao Estado. (art. 16). O processamento de dados pessoais para fins privados depende de declaração da empresa à comissão (arts. 17 e 18), que poderá exigir medidas de segurança e proteção à privacidade.

Já a lei portuguesa que trata da proteção de dados pessoais face à informática, Lei nº 10/91, de 29 de abril de 1991, entre outros aspectos, determina que não é admitido o tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, origem étnica, condenações em processos criminais, suspeitas de atividades ilícitas, estado de saúde e situação patrimonial ou financeira. A violação a tais disposições implica em pena de multa ou detenção.

Os países escandinavos, pioneiros no tratamento da questão da privacidade em face do tratamento de bases de dados, além das restrições similares às da legislação francesa ou britânica, exigem anuência prévia de órgão governamental para que dados pessoais de seus cidadãos sejam armazenados ou processados no exterior.

3.3 O tratamento de bases de dados na lei brasileira

No Brasil, a realização de pesquisa para estruturação e comercialização de cadastros, bem como para outras finalidades comerciais não se encontra regulamentada. Algumas disposições foram consagradas na Lei nº 8.078, de 11 de setembro de 1990, que "dispõe sobre a proteção do consumidor e dá outras providências", no que diz respeito aos cadastros de compradores, estruturados para efeito de cobrança. Esse diploma dispõe, no art. 43:

> *"Art. 43 O consumidor, sem prejuízo do disposto no art. 86, terá acesso a informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.*
>
> *§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.*
>
> *§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*
>
> *§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.*
>
> *§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.*
>
> *§ 5º Consumada a prescrição relativa a cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos sistemas de proteção ao crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores."*

Entre os aspectos não regulamentados, cabe destacar a revenda de cadastros de pessoas físicas sem prévia autorização, hoje prática corrente. Também não há regulamentação quanto ao cruzamento de cadastros para fins de levantamento de perfis socio-econômicos e de consumo. É preciso estabelecer, ainda, a quem será atribuída a responsabilidade pela retificação da informação junto bases de dados.

Outro problema em aberto na legislação brasileira é o tratamento de dados pessoais pelos órgãos de governo, nos moldes tratados pela legislação comparada, apresentada na seção anterior. Um exemplo óbvio é o da elaboração de perfis socio-econômicos no contexto de uma investigação criminal. O perfil poderá caracterizar ou não o verdadeiro criminoso, mas certamente indiciará outras pessoas inocentes, que serão incomodadas, submetidas a procedimentos policiais ou expostas à opinião pública. Se considerarmos que, na elaboração desses cruzamentos de informações, diversos parâmetros ou dados são interpretados por terceiros, havendo um índice relativamente alto de incorreções, tal prática poderá levar a sucessivas violações da privacidade de cidadãos, sem oferecer, em contrapartida, resultados eficazes para a sociedade.

4. TRANSMISSÃO DE INFORMAÇÕES E PRIVACIDADE

A transmissão de dados é outro mecanismo pelo qual é possível obter-se dados de forma questionável. O procedimento consiste em monitorar externamente uma conexão de computadores, interceptando as informações enviadas e recebidas, ou em usar uma rede pública, como a Internet, para colocar-se no lugar de um usuário e receber as informações a ele destinadas.

Há inúmeras alternativas técnicas para executar tais procedimentos e o seu detalhamento extrapola os objetivos deste texto. É preferível examinar, rapidamente, as implicações jurídicas de uma das alternativas de segurança adotadas para proteger dados na Internet: a criptografia.

Tradicionalmente, a criptografia dos dados transmitidos era feita através de um sistema de senhas, que eram usadas para codificar e decodificar a mensagem. Essas senhas eram armazenadas em ambos os computadores envolvidos na transmissão ou deveriam ser enviadas junto com a mensagem.

Se os computadores não estivessem ligados a uma rede, a segurança das senhas envolveria apenas aspectos de proteção física contra o acesso aos equipamentos e a segurança contra acessos ao sistema de senhas, em geral uma tabela ou um programa. Quem quisesse invadir o computador deveria primeiramente obter acesso a um terminal do mesmo e, então, violar a segurança do seu sistema (Nobre, 1999).

Hoje, no entanto, os computadores encontram-se conectados em rede, podendo ser acessados por todo tipo de "hacker" disposto a invadi-lo. Nesse contexto, a solução encontrada foi a de se usar um sistema de duas chaves. Uma chave é pública, sendo usada por qualquer um que queira enviar um arquivo para um certo destinatário. Este, por sua vez, dispõe de uma chave pessoal ou privada, a única forma de descriptografar a informação.

O processo pode ser usado em sentido inverso, para certificar um certo documento. Esse procedimento, comercialmente denominado de assinatura digital, consiste em enviar o documento ou arquivo em forma legível, acompanhado de uma "arrumação" dos dados feita por um processo de codificação pela chave privada. Qualquer um poderá ler o documento e, se estiver de posse da chave pública do remetente, autenticá-lo. Se o documento tiver sido modificado, não será autenticado.

O sistema de chave dupla já é usado, de forma simplificada, nas páginas seguras na Internet. Várias versões do mesmo, desenvolvidas a partir do sistema original – o PGP – estão incorporadas em programas comerciais, tais como os "browsers".

O processo descrito é um sistema de proteção de dados seguro. No entanto, coloca diversas questões de natureza jurídica ainda não tratadas na legislação brasileira. Primeiramente, a segurança depende de uma adequada proteção da chave privada e de sua configuração. Em segundo lugar, um mecanismo eficaz de disponibilização de chaves públicas deve ser organizado. Além disso, o alcance da responsabilidade das partes no caso de divulgação de dados pessoais deve ser formulado e deve ser qualificado em que grau a adoção de mecanismos de segurança servirá de atenuante nesses casos. Tais aspectos relacionam-se sobretudo com a legislação própria do comércio eletrônico, ainda que digam respeito à privacidade dos dados na Internet.

5. CONCLUSÕES

A privacidade, embora conceituada tendo-se em vista os problemas que o cidadão possa vir a enfrentar se aspectos da sua vida particular vierem a ser expostos, deve ser estendida ao direito de controlar de que forma as informações sobre a sua pessoa serão usadas por terceiros. De fato, dependendo do cruzamento de informações que outrem possa fazer, em especial quando se tratar de órgão governamental, a pessoa poderá ficar exposta a situações constrangedoras, ou que redundem em violação à sua honra, imagem ou intimidade.

A Internet criou um contexto em que as questões de privacidade deverão ser repensadas. De fato, por se tratar de um meio que é, simultaneamente, ambiente de interação entre pessoas, correio eletrônico e meio de comunicação de massa, integrou fortemente as duas situações que caracterizam a violação da privacidade: a revelação de fatos privados embaraçosos e ao uso de métodos questionáveis para coleta de informações.

Através de seus serviços noticiosos e de divulgação, a Internet serve de meio de comunicação de massa, possibilitando a revelação de fatos privados, inclusive em uma escala nunca antes atingida, por se tratar de uma rede mundial. Nesse caso, a jurisdição das leis nacionais poderá ser um empecilho à investigação do delito, à identificação dos responsáveis e ao seu julgamento. Abre-se, então, uma oportunidade para o tratamento da questão no nível dos fóruns internacionais adequados.

Mas a Internet, ao facilitar a adoção de métodos discutíveis para a coleta de informações, coloca outros problemas na esfera da privacidade. Por um lado, os computadores e sistemas ligados à rede são continuamente invadidos, ainda que sem a intenção de provocar danos, sendo fácil a coleta de dados armazenados à revelia de seus proprietários. Por outro lado, o cruzamento dessas informações, ou até mesmo de informações obtidas de forma legítima, pode propiciar a construção de perfis socio-econômicos das pessoas, cujo conteúdo e cuja utilização lhes escapa.

Nesse contexto, impõe-se a criação de uma legislação apropriada. Nos países europeus, as leis que tratam de privacidade de dados pessoais e de comércio eletrônico cederam à tradição cartorialista, criando novas modalidades de registro de bases de dados e de assinaturas eletrônicas que, se simples de se fazer, levam a um efetivo encarecimento das atividades comerciais de informática em geral. Mais eficaz parece ser determinar direitos e deveres das partes e um procedimento judicial eficaz para dar solução rápida e justa aos conflitos que venham a colocar-se.

No Brasil, tal legislação é quase que inexistente. Alguns dispositivos da Lei de Imprensa poderão ser aplicados por analogia, mas esbarram na forma restritiva com que a mídia foi conceituada naquele diploma legal. Além disso, redundam em penalidades insuficientes, em face do potencial dano que a divulgação de fato embaraçoso possa vir a criar. Em relação a bases de dados, algumas disposições esparsas existem, enfocando aspectos muito específicos do problema.

REFERÊNCIAS BIBLIOGRÁFICAS

AHRENS, Ney da Gama et al. (1985). "Proteção à privacidade do cidadão: realidade e perspectivas" in*: Seminário Internacional de Informática, Justiça e Direito – Anais*. São Paulo: Prodesp, pp. 129-146.

CATE, Fred H. (1997). *Privacy in the Information Age*. Washington: Brookings.

ESTADOS UNIDOS. Departamento de Comércio (1989). *U.S. Industrial Outlook: Prospects for over 350 Industries*.

IANOTTA, Mark W. (1987). "Protecting individual privacy in the shadow of a national data base: the need for data protection legislation". *Capital University Law Review*, 17:117-135.

MEYER, Philip. (1987). *A Ética no Jornalismo*. Rio: Ed. Forense Universitária.

MIRANDA, Darcy A. (1995) *Comentários à Lei de Imprensa*. São Paulo: Ed. Revista dos Tribunais. 3ª ed.

NOBRE, Alexandre B. (1999). "A segurança de arquivos na Internet". *Mimeo.*

OLIVEIRA, Maria T. (1977). "A privacidade ameaçada". Dados e Idéias, 5(2):69-81.

[1]"Congress shall make no law ... abridging the freedom of speech or of the press...".

[2]Exposta e discutida pelos juízes Holmes e Brandeis nos casos Abrahams v. US (1919) e Whitney v. California (1927).

[3]Por exemplo, New York Times Inc. v. Sullivan (1964).

[4]Schenck v. US (1919).

[5]Por exemplo, em American Communications Association v. Douds (1950) e Konigsberg v. State Bar of California (1961).

[6]Adotou-se a tese, por exemplo, em Chaplinsky v. New Hampshire (1942). Em Jacobellis v. Ohio (1964), o juiz Stewart formulou a famosa expressão "não consigo definir pornografia, mas a reconheço quando a vejo".