Comércio de dados pessoais, privacidade e Internet

Autor: Tiago Farina Matos
(Advogado)
| Artigo publicado em 18.07.2005 |

Sumário

Introdução

O enfoque deste estudo está na interferência, muitas vezes negativas, que a Internet pode ter na privacidade das pessoas, principalmente no que concerne à coleta e comercialização de dados pessoais. Não será nosso objetivo traçar planos legislativos para o fim da violação à privacidade no meio virtual, muito menos com relação a normas penais que têm caráter repressivo. Advogamos a tese de que, no caso da Internet, a prevenção ainda é o melhor caminho.

Ademais, devido ao caráter dinâmico-progressivo da Internet, não há como apontar os limites que lhe são peculiares, o que dificulta na elaboração de leis próprias. Podemos, isso sim, partindo do conhecimento das causas violadoras da privacidade na Internet, traçar metas de prevenção, que, a priori, parecem ser mais eficientes do que o combate meramente repressivo.

É com esse espírito que nos aventuramos a abordar a problemática da privacidade na Internet.

A abordagem do tema está dividida em dois capítulos. No primeiro iniciamos com uma rápida pincelada sobre conceitos técnicos relativos à Internet, principal meio de comunicação eletrônica na atualidade, e seguimos o seu desenvolvimento investigando as

causas que vivificam a assertiva de que a Grande Rede está categoricamente revolucionando o processo de captação e comercialização de dados pessoais, dando destaque ao valor atribuído a tais informações por determinados setores da sociedade. Por fim, identificamos os principais meios de coleta de dados encontrados na Internet.

No segundo capítulo, procuramos introduzir um enfoque essencialmente jurídico à questão da coleta e comercialização de dados pessoais pela Internet. Assim, aprofundamos o estudo do direito à privacidade e estruturamos algumas questões diretamente relacionadas à coleta de dados pessoais, como o spam e a monitoração eletrônica do estilo de vida. Ao final do estudo, propomo-nos a diagnosticar medidas de proteção à privacidade no espaço virtual.

Utilizamos uma extensa bibliografia, dividida entre livros editados, artigos publicados na Internet e matérias em jornais e revistas. Nem todas essas fontes de pesquisa foram citadas no decorrer do trabalho, entrementes, prestaram, em sua totalidade, plurais contribuições, sem as quais não haveria como elaborar esse estudo.

1. Sociedade da informação

1.1 Comunicação eletrônica: do telégrafo sem fio à internet

Sucintamente, comunicação eletrônica é a troca de informações através de circuitos ou ondas elétricas.

Seria uma tarefa extremamente árdua, para não dizer impossível, descrever todos os meios capazes de proporcionar uma comunicação eletrônica. Entretanto, alguns merecem ser lembrados, à guisa de ilustração: o primeiro meio da espécie foi o telégrafo sem fio. A partir dele, surgiram outros como o rádio, o cinema falado e a televisão. Sem esquecer do telefone fixo e do radar, este último muito utilizado na comunicação entre aeronaves.

O desenvolvimento tecnológico ainda trouxe ao mercado meios de comunicação eletrônica, como aparelhos de escuta e de interceptação telefônica, microfones e gravadores audiovisuais minúsculos e de longo alcance – hoje muito usados nas investigações criminais, mas também lamentavelmente visados por indivíduos mal intencionados, para violar a intimidade de outras pessoas – além do telex, das antenas parabólicas, do telefone celular, das teleobjetivas e câmaras fotográficas digitais, bem como do aparelho de fax.

Mas o grande protagonista do mundo eletrônico é, sem dúvida alguma, o computador, definido de forma bastante simples, pelo

lexicólogo Antônio Houaiss, como uma “máquina eletrônica que guarda, analisa e processa dados.” Principalmente porque, através da comunicação entre computadores ou entre usuários desta máquina, surgem as redes, das quais uma em particular é o principal instrumento de comunicação do mundo moderno: a INTERNET.

Marco Aurélio de Mello, então Ministro-Presidente do Supremo Tribunal Federal, fez um interessante comentário, quando assumiu a Presidência da República por alguns dias, durante a ausência do Presidente Fernando Henrique Cardoso, bem como de seus demais substitutos, ao dizer que, num mundo em plena era da informação, não haveria necessidade de substituir um Presidente da República durante uma simples viagem, haja vista os diversos recursos de comunicação, capazes de proporcionar um controle direto sobre o seu governo, de qualquer parte do planeta. Complementou dizendo que a substituição da figura do presidente tinha sentido nos tempos em que as viagens eram feitas por mar, onde se levava dias para atingir seu destino e também porque não existiam meios de comunicação instantâneos, capazes de cobrir eventuais emergências em seu país.

Mas, enfim, o que é a INTERNET? Qual sua origem e suas características?

A Internet embrionou-se no auge da Guerra Fria, com o projeto militar norte-americano denominado ARPAnet (ARPA: Advanced Research Projects Agency), criado como resposta ao lançamento do 1º Satélite ao espaço pela URSS.

O objetivo do ARPAnet era criar uma rede que pudesse se manter sem a necessidade de estar conectada a uma fonte central, ou seja, uma rede capaz de tornar todos os pontos de conexão equivalentes. Assim, eventual bombardeio sobre um determinado ponto da rede não prejudicaria a conexão entre os demais.

Na primeira fase do projeto, quatro pontos seriam interligados: UCLA – University of Califórnia at Los Angeles; SRI – Stanford Research Institute; UC Santa Bárbara e a Universidade de Utah. E, em 21 de novembro de 1969, deu-se o primeiro registro de conexão entre os servidores deste projeto, quando do contato realizado entre os computadores localizados na UCLA e no SRI. Já no fim do mesmo ano, todos os quatro servidores estavam conectados à ARPAnet.

Mas o termo Internet propriamente dito surgiu mesmo em meados de 1981, quando a tecnologia passou a ser também utilizada por cientistas e acadêmicos. Apenas em 1987, nos EUA, o uso da grande rede passou a ser feito também no âmbito comercial. Daí em diante, no mundo todo, começaram a surgir inúmeros provedores de acesso, destinados ao público em geral.

Vejamos agora alguns conceitos e particularidades acerca da Grande Rede.

Para o ilustre estudioso na área, Gustavo Testa Corrêa:

(...) A Internet é "um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento".

Assim, criada inicialmente para fins militares, a rede mundial de computadores tomou vulto na vida cotidiana, e hoje estima-se que mais de 200 milhões de pessoas espalhadas pelo planeta usufruam de todo seu potencial.

O uso acadêmico e científico abriu espaço também ao uso comercial. A interface amigável, cada vez mais interativa, também contribuiu para seu crescimento. Atualmente, não apenas trocas simples de mensagens de texto são realizadas através da rede, mas também a utilização de imagens, sons, gráficos e vídeos, o que faz despertar a curiosidade da população, tornando seu uso cada vez mais indispensável.

Isso tudo porque o ciberespaço apresenta uma gama inimaginável de utilidades para seus usuários, desde simples consultas a textos dos mais variados tipos até compras de mercadorias, investimentos em bolsas de valores, movimentações financeiras etc.

Diante desse quadro altamente evolutivo, surgem, no entanto, alguns pontos negativos, os quais merecem uma maior atenção dos operadores do Direito. Apenas para melhor ilustrar, sem, contudo, pretender esgotar os tópicos que carecem de discussão, temos a privacidade do usuário, no momento em que, por diversos meios, tem suas informações colhidas anonimamente por outros computadores também ligados à rede; a violação de correspondência pelos meios eletrônicos, como a legalidade de o empregador supervisionar o conteúdo dos e-mails recebidos e enviados por seus empregados no ambiente de trabalho; a tributação nas negociações eletrônicas, mormente quando se trata de negociações realizadas entre diferentes Estados ou Países. Esses são apenas parte dos entraves que cercam o uso da Internet, visto aos olhares jurídicos, sem olvidar, é claro, dos crimes cometidos também via rede, notadamente a pedofilia, que é o mais preocupante para os defensores da questão dos crimes virtuais.

Neste breve estudo, procuraremos adentrar na questão da privacidade no ciberespaço, especialmente em relação à coleta e comercialização de dados do usuário, sem sua prévia autorização; fato extremamente preocupante para a comunidade jurídica, uma vez que a privacidade da pessoa humana constitui um bem jurídico carecedor de inabdicável proteção.

1.2 A revolução da internet em termos de coleta e comercialização de informações pessoais

Informação sempre foi objeto de grande cobiça pela sociedade em geral. Corporações, governos, pesquisadores, acadêmicos e todos os demais setores da sociedade, a fim de aprimorar seus conhecimentos e otimizar resultados, estão constantemente em busca deste produto.

Enganam-se aqueles que dizem ter a informação se transformado num valioso recurso em decorrência dos avanços tecnológicos. Na verdade, tal bem sempre teve seu "valor de mercado" nas alturas. O que há de novo e, portanto, a faz parecer algo como um recém-descoberto poço de petróleo, é o fato de que, graças ao exponencial crescimento tecnológico, abrindo espaço para a comunicação eletrônica, nunca foi tão fácil e rápido obter e gerenciar informações dos mais variados assuntos, não importando tempo nem lugar.

Anne Grascomb, autora do livro "Who Owns Information? From Privacy to Public Access", citada por Demócrito Reinaldo Filho, sustenta que a informação é a chave para as decisões políticas, sociais e negociais. E complementa: "Na atual sociedade da informação, o bem mais valioso, o mais procurado é justamente o que dá nome a essa nova sociedade: a própria informação".

E, de fato, empresas que dispõem do maior número de informações, seja um método eficaz de "como atrair clientes" ou mesmo um know-how inovador e revolucionário na produção de novos equipamentos, são as que detêm o grande poder na economia. No mesmo raciocínio, Danilo Duarte Queiroz salienta:

"Na 'nova economia', empresas ágeis são as que conseguem adquirir e administrar a maior quantidade possível de informação, no menor tempo e com a maior eficiência. Conseqüentemente, quem consegue prover e distribuir informação com maior competência, torna-se um 'fornecedor' concorrido e rico" .

O crescimento tecnológico, além de permitir o acesso a uma infinidade de informações pelos diversos setores da sociedade, também é o grande facilitador da manipulação das mesmas. Em vista disso, grandes corporações estão investindo pesadamente em tecnologia, aumentando seus poderes de captação e gerenciamento

de dados, com o objetivo de superar a concorrência e direcionar seus investimentos de maneira a diminuir ao máximo eventuais riscos.

1.2.1. Informações Pessoais Identificáveis

Nesse contexto, vemos crescer assustadoramente a coleta e a comercialização de um tipo em especial de informações: as que dizem respeito à vida das pessoas; conhecidas como informações pessoais identificáveis, ou PII (Personally Identifiable Information), que são todas as informações relativas a uma determinada pessoa, desde características físicas até hábitos dos mais variados, de modo que do cruzamento desses dados seja possível traçar um verdadeiro perfil da respectiva pessoa.

"As PIIs referem-se a qualquer coisa na rede eletrônica que possa ser vinculada, de alguma forma, a uma pessoa de carne e osso; a alguém que tem um nome, um endereço e uma vida".

Quem costuma navegar pelos mares da grande rede certamente já se defrontou com algum tipo de questionário solicitando determinadas informações de cunho pessoal, como nome, endereço, e-mail, estado civil, áreas de interesse etc. A maioria dessas pessoas, entretanto, mal sabe para que servem tantas dessas informações, algumas absolutamente impertinentes. A verdade é que muitas empresas, a fim de atrair clientes, oferecem prêmios, ofertas ou até mesmo serviços gratuitos aos internautas que se "cadastrarem" nos seus respectivos sites. Com isso, essas empresas passam a deter um material altamente valioso: as PIIs – e muitos clientes-consumidores ficam mais que satisfeitos em participarem desta espécie de permuta (troca de mercadorias ou serviços por informações pessoais), pouco se importando com as futuras conseqüências oriundas de tal ato.

Por isso, Reinaldo Demócrito Filho afirma com extrema cautela que:

"(...) se, por um lado, a coleta de informações pessoais pode favorecer negócios, facilitar decisões governamentais ou mesmo melhorar a qualidade de vida material da sociedade como um todo, outros valores necessitam ser considerados à luz da privacidade individual."

E para não parecer um exagero frisarmos o fato de as PIIs serem o bem mais valorizado do mercado, basta considerarmos que analistas de Wall Street estão valorando empresas de acordo com a quantidade e qualidade de Informações Pessoais Identificáveis coletadas de seus clientes. Hoje, o valor de uma empresa é calculado pela quantidade de clientes que ela possui; mais precisamente, US$ 2.000,00 por cliente.

Nesse sentido, muitíssimo curioso um caso protagonizado pela empresa 800.com, no início do comércio eletrônico, o qual tomamos a liberdade de comentar, uma vez que trará um colorido adicional ao tema em apreço.

Criado pelo produtor de televisão John Ripper, o website da 800.com foi lançado em setembro de 1998, e, um mês depois, o CEO da empresa, Greg Drew, fez a seguinte promoção: cada visitante poderia encomendar três CDs ou DVDs, dos mais recentes e procurados, por apenas um dólar. Pode parecer piada, mas seu raciocínio foi algo acima de brilhante: a idéia central era "comprar" clientes por cerca de US$ 50,00 cada um (valor médio de varejo dos produtos).

Num primeiro momento, porém, Drew pensou em colocar um anúncio dentro de um website com grande número de visitantes. Mas, após um minucioso estudo, concluiu que seria mais econômico e eficaz eliminar o intermediário e utilizar o capital diretamente com os clientes, considerando que a notícia correria de boca em boca.

E foi o que aconteceu: o tráfego no site da empresa 800.com, por diversas vezes, congestionou os servidores da conexão. Resultado: a empresa teve um lucro quatro vezes acima do esperado – pois muitos clientes empolgados com a promoção do "um dólar" acabavam comprando outros produtos a preços normais.

Drew sustentou sua idéia milionária em números informais, citados por investidores e analistas de mercado. Levando em conta que as empresas de comércio eletrônico estavam sendo avaliadas em dois mil dólares por cliente, Drew planejou pagar cinqüenta dólares pelo nome de um, mesmo que este fizesse apenas uma compra de um dólar. De fato, foi um excelente negócio.

A razão de as PIIs valerem tanto no mercado de informação se deve ao seu poder de direcionar investimentos. Assim, para as empresas é muito vantajoso possuir grande quantidade de PIIs, uma vez que, conhecendo os gostos e as necessidades de seus clientes ou clientes em potencial, da forma mais detalhada possível, podem investir diretamente neles.
Portanto, quanto maiores e mais exatas as PIIs coletadas, menos riscos correrá a empresa e mais sólida será sua base de sustentação.

Mas, não são só as empresas comerciais as grandes vilãs do ciberespaço, quando o assunto é informações pessoais identificáveis. Os governos sempre tiveram o hábito de vasculhar os mais íntimos segredos de seus adversários (que podem ser qualquer um), ainda mais na atual conjuntura internacional, pós "11 de setembro de 2001", em que a obsessão por reduzir crimes e descobrir terroristas assumiu picos recordes.

Com efeito, EUA, Inglaterra, Canadá, Austrália e Nova Zelândia, em nome da segurança nacional, controlam o polêmico Projeto Echelon, cujo objetivo principal é interceptar todas as comunicações mundiais em quaisquer locais do planeta – sejam telefonemas, faxes, e-mails, telex, mensagens de pagers ou qualquer outra modalidade de comunicação.
Teoricamente, após coletadas as informações (de empresas, governos e civis), filtram-se palavras ou grupos de palavras que podem representar algum tipo de perigo à segurança nacional dos controladores do projeto.

Isso significa na prática que todos podemos estar sendo vigiados pelos que se consideram donos do universo. E, na verdade, o objetivo não é apenas a defesa nacional, mas principalmente satisfazer interesses comerciais e industriais, base para uma economia auto-sustentável.

1.2.2 Meios de coleta de dados pessoais pela internet

Já vimos, no início de nosso estudo, que existem inúmeros meios de comunicação eletrônica capazes de coletar informações das mais variadas formas, como imagens (câmaras fotográficas, circuitos internos de televisão, scanners etc) e sons (microfones, escutas telefônicas, gravadores etc).

Vimos também que tais informações podem compor as chamadas Informações Pessoais Identificáveis, ou seja, aquelas informações que dizem respeito à determinada pessoa, podendo, da reunião desses dados, traçar-se o perfil do indivíduo.

A Internet surge, nesse momento, como o meio mais propício para a coleta e o gerenciamento de PIIs, uma vez que coloca o mundo todo no mesmo espaço: o espaço virtual. Não existem, portanto, distâncias a serem percorridas. Pode-se obter PIIs de cidadãos americanos através de um computador situado na China, por exemplo. A grande rede permite este tipo de intercâmbio, para a felicidade dos que a utilizam como fonte de poder – Governos, empresas etc.

Mas, para os usuários da Internet, que assumem essa condição – na maioria dos casos – devido aos atrativos oferecidos pela rede, talvez essa disposição dos seus dados aos olhos alheios não seja algo tão excitante assim.

Antes de analisarmos o tratamento dispensado para as PIIs coletadas, importante nos familiarizarmos com alguns dos principais meios de coleta de dados pela Internet.

1.2.2.1 Formulários

Se não o mais conhecido, sem dúvida alguma, o mais explícito de todos os meios de coleta de dados pessoais através da grande rede.

Como já salientamos linhas atrás, através dos formulários, os visitantes espontaneamente informam ao site informações solicitadas, que variam entre as mais básicas como nome, endereço e profissão, às mais íntimas, como quais as áreas de seu interesse. Mas, apesar de parecerem dados banais e inofensivos, se comercializados ou mesmo cruzados a outras PIIs, podem compor um verdadeiro dossiê físico-psíquico do cidadão.

Neste tipo de coleta de dados, o informante sabe que está cedendo as informações, ou seja, tem total consciência de que está fornecendo PIIs – embora não saiba para que se destinam. Mas, de qualquer forma, fica a seu alvedrio fornecê-las ou não. Isso acaba colocando o site destinatário numa posição bem confortável, pois as informações coletadas foram-lhe entregues espontaneamente pelo navegante.

1.2.2.2 Cookies

Ao contrário dos formulários, que são explícitos coletores de informações pessoais, os cookies (biscoitos, em inglês) operam usualmente sem o consentimento ou o conhecimento do usuário.

Cookies são pequenos arquivos de informações lançados pelos sites visitados, dentro do computador do visitante, e ficam armazenados no respectivo disco rígido, para, enquanto houver navegação na web, serem utilizados pela memória RAM. Existem dois tipos de cookies: os que são gravados diretamente no computador dos usuários e servem para facilitar o carregamento do site numa posterior navegação, e os que se servem apenas para coletar dados dos visitantes, cujo destino é, inevitavelmente, o banco de dados do site visitado. A coleta de PIIs, através dos cookies, tem como principal objetivo – pelo menos é o que alegam os donos dos 'biscoitos' – personalizar o acesso do internauta ao respectivo site.

Das informações coletadas, é possível identificar qual o navegador utilizado, o sistema operacional, os horários, a quantidade de acessos, as áreas de preferência, bem como o número do IP (Internet Protocol), que está para a Internet assim como a impressão digital está para a identificação de pessoas. Através desse número pode-se conhecer o provedor, o navegador, o sistema operacional e, inclusive, a localização de qualquer um que tenha acessado a Internet – o que, se de um lado pode ser muito útil para encontrar criminosos, por

outro lado, disseca a vida dos usuários comuns, que podem ter seu endereço e telefone divulgados para um incontável número de pessoas.

1.2.2.3 Hackers e crackers

É muito comum ouvir acusações direcionadas aos hackers, quando, na verdade, tecnicamente, o alvo seriam os crackers. Mas existe mesmo diferença entre esses dois personagens do mundo cibernético? Vejamos.

Os hackers (fuçadores, em inglês) podem ser definidos como indivíduos muito bem-informados, com conhecimentos informáticos acima da média e com imensa curiosidade em avaliar as falhas de um sistema de proteção computacional. Eles percorrem os sistemas em busca de falhas, utilizando técnicas das mais variadas em termos de computação, não para fins prejudiciais, mas para satisfação de seu próprio ego. Mais cedo ou mais tarde, esses indivíduos acabam sendo contratados por grandes empresas interessadas em profissionais capazes de coordenar seus sistemas de proteção e defesa.

Se tivermos como parâmetro o descobrimento de uma falha em determinado sistema informatizado, poderemos nos defrontar com o descobridor interessado em solucionar a questão da segurança, ou com aquele munido de objetivos escusos.

Esse é o liame que separa os hackers dos crackers. Enquanto o primeiro deles é atiçado unicamente pelo desafio de conhecer as falhas do sistema computacional, o segundo inicia sua jornada no momento em que descobre tais falhas, tendo em vista a obtenção de benefícios particulares ou a intenção de causar danos a terceiros.

Portanto, embora ambos tenham conhecimentos técnicos o suficiente para invadir sistemas de segurança, o hacker não deseja causar danos, nem tirar proveito da situação, ao contrário dos crackers. Estes, sim, representam iminente perigo à sociedade, pois, da invasão de sistemas informatizados protegidos, podem copiar todo um banco de dados contendo um incontável número de PIIs.

Ainda no que tange à coleta de PIIs, quanto valeriam para uma companhia de seguros de saúde as informações saqueadas por um cracker do banco de dados de um grande hospital? Veremos no momento oportuno. Por enquanto, vale a reflexão.

1.2.2.4 Bancos de dados

Além das PIIs coletadas diretamente da Internet, existem aquelas antes só encontradas em bases de dados proprietárias, ou seja, no

sistema interno de agências governamentais, empresas comerciais, consultórios médicos etc., que agora estão passando para o domínio público na Grande Rede.

Pelo elevado número de aplicações decorrentes dessa "onlinização" dos bancos de dados proprietários, colacionamos algumas delas para melhor compreensão do tema:
• os históricos dos alunos disponíveis nos sites das respectivas escolas e universidades;
• os dados relativos ao FGTS;
• agências governamentais detêm informações de todos os cidadãos que podem ser
acessadas por qualquer um, legal ou ilegalmente;
• a SERASA aponta o pretenso devedor em mora;
• os bancos de dados do judiciário trazem quem já tenha demandado em Juízo;
• os departamentos de trânsito dão informações sobre os veículos, multas e infrações;
• no site da Receita Federal, da posse do CPF de qualquer contribuinte, pode-se fazer uma devassa em sua vida fiscal.

Em síntese, a coleta de dados pode se dar através dos formulários, de forma explícita, ou, implicitamente, por intermédio dos cookies; licitamente consultando bancos de dados, antes fechados, agora abertos e disponíveis livremente na Grande Rede, ou utilizando-se de métodos ilícitos, como o caso dos crackers invasores de sistemas de bancos de dados fechados ou protegidos.

1.2.3 Cruzamento e comércio de dados pessoais

Conhecido o conceito de PIIs – Informações Pessoais Identificáveis – e os principais modos como essas informações são coletadas através da rede ou inseridas indiretamente nela, verificaremos agora o destino que levam os dados pessoais coletados na Internet, sempre tendo em vista eventuais violações ao direito de privacidade.

Para os usuários, as empresas justificam a coleta de dados pessoais baseados em argumentos que, em essência, se traduzem em um: a melhor satisfação do cliente.

A primeira justificativa – e também a mais simples – seria a de fazer da navegação no site a mais personalizada possível, de modo que o ambiente cibernético se moldasse aos gostos do cliente.

Outra justificativa é a de traçar perfis de consumo e preferências e, assim, oferecer ao cliente aquilo que ele realmente deseja. Fazer propaganda direcionada apenas ao público que efetivamente se interessa pelo produto sempre foi um sonho das grandes empresas,

pois evita gastos desnecessários com pessoas que jamais se tornariam clientes, devido a seus gostos e preferências não coincidirem com o produto o qual a empresa visa comercializar.

Mas o que o cliente ganharia com este marketing direto? O argumento das empresas se baseia no fato de o cliente não ter mais que perder seu precioso tempo indo atrás dos produtos de seu interesse. No caso, quem iria ao encontro dos clientes seriam os produtos em si.

Outra razão apresentada pelas empresas é a de identificar melhores locais para investimento, baseados em dados regionais e estatísticas.

Mas seriam apenas esses os objetivos da coleta de PIIs? Ou seriam tais informações vítimas indefesas de um mercado afoito por poder e riqueza?

A triste verdade é que as PIIs são, em larga escala, utilizadas ainda para outros fins, muitos dos quais vão além do conhecimento dos seus respectivos proprietários, mais relacionados com os interesses das empresas que as detêm. Aí entra o chamado comércio de informações.

Graças aos diversos meios de coleta de dados, alguns dos quais já analisamos como os formulários, os cookies e o papel dos hackers e dos crackers, uma gama imensurável de PIIs são coletadas para, posteriormente, serem utilizadas sem autorização do indivíduo ao qual essas informações pertencem, e quando pior, sem seu conhecimento.

Como conseqüência do comércio de informações, podemos citar a mala-direta de propagandas comerciais.

Através de dados como endereço, telefone ou e-mail, empresas encaminham mensagens de marketing direto para uma quantidade infinita de pessoas. Aí, entram também os chamados “corretores de informações” – aqueles que compram PIIs de diversas fontes, cruzam-nas e revendem-nas para quem se interessar – formando em seu banco de dados um verdadeiro perfil do indivíduo. Entrementes, esses corretores são procurados por empresas, que encomendam certo número de nomes (bem como dos demais dados referentes ao mesmo) entre os quais melhor se encaixam nas suas diretrizes de clientela.

A corretagem de PIIs, já no ano 2000, era uma indústria de mais de um bilhão de dólares nos Estados Unidos.

O que as pessoas mais temem, entretanto, não é a mera utilização de dados relativos a elas em listas de mala-direta para fins de marketing, mas a possibilidade de alguém descobrir mais do que elas desejam que seja revelado a seu respeito; informações que só dizem respeito à privacidade de cada um.

Charles Jennings e Lori Fena advertem:

"Embora não haja um sistema único de perfis PIIs, o advento das redes eletrônicas de computadores está atualmente criando algo bastante semelhante: acesso por intermédio de links aos muitos diretórios de computadores diferentes que atualmente armazenam PIIs. Cada vez mais informações com tag PII estão sendo inseridas, armazenadas e comercializadas por meio de uma matriz eletrônica comum" .

Em quase todos os segmentos da vida moderna, trocas de PIIs são efetivadas por intermédio de meio eletrônicos e não-eletrônicos. Para praticamente todos os atos da vida civil estamos fornecendo dados pessoais – quando queremos ir ao médico; retirar dinheiro de um caixa eletrônico; fazer compras através do cartão de crédito; contratarmos um provedor de acesso ou mesmo para poder navegar no interior de um website – sem nem sequer refletirmos para onde essas informações estão indo, quem as receberá, onde e por quanto tempo ficarão armazenadas, quais os fins a que elas se destinam e, de modo geral, quais serão as conseqüências.

Só para termos uma idéia da dimensão do problema, imaginemos o que aconteceria se uma empresa de cartão de crédito comercializasse clandestinamente informações a respeito do poder de compra de um indivíduo qualquer para uma seguradora de saúde, e, dentre os produtos adquiridos pelo indivíduo, constassem várias garrafas de bebidas alcoólicas. Poderíamos presumir que a seguradora no mínimo teria uma grande suspeita de que tal cidadão poderia vir a sofrer males decorrentes do excesso de álcool no sangue. Vamos além. Caso o mesmo indivíduo fosse na verdade um alcoólatra, ex-paciente de uma clínica de reabilitação, cujo tratamento restara infrutífero, e o administrador dessa clínica comercializasse os nomes de seus pacientes à mesma seguradora. Quais as conseqüências? Nesta hipótese, haveria subsídios suficientes para a seguradora considerar como duvidoso o estado de saúde do sujeito. Mas poderia piorar se o mesmo indivíduo houvesse, tempos atrás, sido internado por problemas de cirrose num hospital cujo banco de dados também entrasse na máfia do comércio com a mesma seguradora de saúde. Como conseqüência óbvia, o indivíduo teria sérios problemas se pretendesse contratar os serviços da seguradora, nomeadamente com relação à cobertura médica quando o problema fosse em razão do consumo de álcool. Além disso, se o cruzamento desses dados

viesse a ser publicamente divulgado, a vida privada dessa pessoa se tornaria um constante transtorno.

Como se vê, o cruzamento de dados é a grande preocupação dos defensores da privacidade da pessoa humana, principalmente numa era em que o comércio de informações pessoais identificáveis toma carona na calda do veloz cometa chamado Internet.

2. Internet, privacidade e dados pessoais

2.1 O direito à privacidade

O direito à privacidade é uma das espécies dos direitos da personalidade, que regem (ou deveriam reger) os princípios mais básicos da relação do homem com a sociedade. Entretanto, o vocábulo "privacidade", por ser muito recente, não consta sequer na Carta Magna de 1988.

Como então podemos afirmar com tanta veemência ser a privacidade um princípio constitucional merecedor de irrefutável proteção? A resposta é simples: basta utilizarmos a velha técnica da dedução lógica.

Antônio Houaiss conceitua privacidade como vida privada, particular, íntima. E complementa: "trata-se de anglicismo de empréstimo recente na língua (talvez década de 1970), sugerindo-se em seu lugar o uso de intimidade, liberdade pessoal, vida íntima, sossego etc".

Por seu turno, o artigo 5º, inciso X, da atual Constituição Federal pátria dispõe que são direitos 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".

Contrapondo-se a definição de privacidade proposta acima ao precitado dispositivo constitucional, tem-se que o direito à privacidade trata de uma denominação genérica, que compreende a tutela da intimidade, da vida privada, da honra e da imagem das pessoas.

Intimidade e vida privada

O direito à vida privada revela a necessidade de a pessoa subtrair do conhecimento alheio fatos de sua vida particular, e também de impedir-lhes a divulgação. Porém, a natureza destes fatos não revela aspectos reservados.

Por outro lado, o direito à intimidade engloba a parcela dos fatos mais reservados de uma pessoa. Consiste na prerrogativa de excluir do conhecimento de terceiros fato que não se deseja ver exposto à publicidade alheia.

Vê-se, portanto, que, no âmbito da intimidade, os fatos estão revestidos de mais reserva e segredo que na esfera da vida privada.

Na proteção constitucional do direito à intimidade, podemos invocar a inviolabilidade do domicílio e o sigilo das correspondências.

Honra

Compreende a reputação e a auto-estima da pessoa, isto é, a consideração de que goza no meio social (honra objetiva), assim como a de que tem de si mesma (honra subjetiva).

Imagem

O direito à imagem tem duas acepções: a imagem-retrato – representação gráfica, fotográfica de uma pessoa; é o direito de não ter sua representação reproduzida por qualquer meio de comunicação sem a devida autorização. Vale lembrar, todavia, que as pessoas de vida pública, como os políticos, não podem invocar tal proteção, quando se tratar de imagens divulgadas quando no exercício de suas funções públicas. Já a imagem-atributo é a forma pela qual o indivíduo é visto no meio social onde vive.

Somando-se os subsídios até aqui apresentados, podemos concluir que os aspectos da privacidade são aqueles relacionados à individualidade do sujeito. E, como bem diz Victor Drummond, “um afastamento confortável do mundo exterior, por parte do titular do direito à privacidade, só pode dar-se, ou desejar-se, por ele próprio”.

É essa distância confortável que uma pessoa mantém espontaneamente, desde a sua mais profunda individualidade até o mundo exterior, que deverá ser tutelado pelo direito.

Trata-se, pois, de um critério estritamente subjetivo. Exatamente por isso, existe um distanciamento entre o conceito de privacidade (natureza subjetiva) e o que pode ser tutelado pelo direito (natureza objetiva). Daí a dificuldade em se buscar uma proteção jurídica proporcional às violações a que a privacidade está sujeita.

Neste diapasão, há que se transpor o universo filosófico para o universo jurídico. Mas, afinal, o que comportará a privacidade tutelada pelo direito?

Com a palavra o eminente jurista Victor Drummond:

“A vida em ambiente familiar, entre amigos, seja em momentos de descanso ou não. Quanto a estes casos, não há praticamente dúvidas ou divergências doutrinárias, visto que ocorrem em um domínio físico particular e controlado pela pessoa. E isto irá valer para qualquer local privado.

Para o caso de ambientes públicos pode-se dizer, com certeza, que não haverá dúvidas quanto à privacidade da pessoa se estiver ela em situações atinentes a si própria. Seja em um estádio de futebol, um restaurante, um cinema, em qualquer destes locais estará ainda a privacidade imperando sem detrimento de se estar circulando em vias ou locais públicos. Pois o grande diferencial e, agora cabe deixar claro, é que nem sempre a localização física é o fator que irá definir a existência ou não de privacidade.

Serão ainda tutelados pelo direito à privacidade: a intimidade dos objetos particulares, dos livros que se lê, da correspondência, todos estes fatores podem ser tutelados pelo direito à privacidade. De idêntico modo, a roupa que se veste, a conversa que se efetua com o jornaleiro ou o padeiro fazem parte da privacidade daqueles que dela participam.”

A despeito das casuísticas trazidas à baila pelo ilustre mestre Drummond, resta evidente a dificuldade de definir objetivamente aquilo que, por si, é essencialmente subjetivo.

É claro que nesse jogo de incertezas, a jurisprudência continuará sendo fundamental na manutenção do direito à privacidade, pois, diante de seu caráter subjetivo, a melhor solução é mesmo aquela evidenciada caso a caso.

2.2 Dados pessoais e privacidade na internet

Um aspecto curioso no comportamento das pessoas quando estão “em órbita” pelo universo da Internet pode ser observado quando esses indivíduos agem de determinado modo que, se não fosse pelo fato de estarem protegidos atrás de uma tela de computador, provavelmente não agiriam. É a sensação de invisibilidade, de achar que ninguém lhes observa. E como já vimos, essa sensação é pura fantasia.

Visto nessa óptica, fica clara a covardia empregada na coleta de dados pessoais através da rede e por isso mesmo é que a privacidade no ambiente cibernético deve ser seriamente tutelada.

E, embora encontremos pontos positivos na coleta de PIIs – como o atendimento personalizado oferecido por websites aos internautas nestes cadastrados – contratempos e até mesmo danos irreparáveis (senão por meio de indenizações) fazem parte do dia-a-dia das navegações virtuais.

Por oportuno, vamos analisar algumas questões diretamente relacionadas à coleta de dados pessoais através da Internet, na medida em que violam o direito à privacidade.

2.2.1 Spam

Dentre as diversas problemáticas acerca da questão da coleta de dados pessoais através da Internet, temos, como mais óbvia e crescente conseqüência da violação à privacidade do usuário da Internet, o denominado spam (mensagem eletrônica publicitária não solicitada).

A palavra "spam" surgiu em 1937, como marca registrada da empresa norte-americana Hormel Foods, ao criar a primeira carne suína enlatada. Diz o mito que, satirizando a novidade, o famoso grupo humorístico inglês Monty Python editou um episódio onde alguns vikings famintos entravam num bar e começavam a gritar "Spam, spam, spam, spam....." de maneira intermitente e irritante, impossibilitando qualquer comunicação entre as demais pessoas presentes no recinto.

Passados alguns anos – quando a utilização da Internet estava começando a se difundir – no meio de um grupo de discussão, algum cidadão teve a infeliz idéia de enviar mensagens comerciais aos participantes de determinados chats, atrapalhando a comunicação das pessoas. Assim, surge o termo spam no mundo digital, com a lembrança do episódio do Monty Python por um usuário de grupos de discussão, equiparando o desprazer causado pelo recebimento de mensagens não solicitadas nestes grupos com a gritaria ensurdecedora do programa cômico inglês. Como previsível já era, essas mensagens migraram para os endereços de correio eletrônico que começavam a se multiplicar. A partir de então, o spam pode ser definido como o envio de mensagem eletrônica não solicitada ou autorizada por quem a recebeu.

O spam, como o conhecemos na era virtual, tem cunho essencialmente comercial. Assim como os folders recebidos pelos correios convencionais, o spam é um tipo de publicidade invasiva, mas, ao contrário daqueles, estes podem causar sensíveis prejuízos materiais – quando não morais – aos receptores das mensagens.

Com efeito, para que uma pessoa receba um spam, é necessário que possua uma conta de correio eletrônico e, para tanto, são necessários alguns requisitos.

O primeiro requisito é o mais óbvio: ter um computador que, sabidamente, é um bem material dotado de valor econômico. O segundo requisito é estar o computador conectado à rede. Para que exista tal conexão é substancial a contratação de um provedor de acesso, além do serviço de telecomunicação – via telefônica ou mesmo por satélite ou cabo. Por último, mas sem menor importância, tem-se o consumo de energia elétrica, fonte de todo processo de envio e recebimento de mensagens eletrônicas. Portanto, como é passível de analisar, o ato de possuir uma conta de correio eletrônico é notavelmente oneroso. Daí dizer que o spam é algo similar à oferta de bens e serviços por uma ligação telefônica interurbana a cobrar.

Soma-se ainda aos prejuízos de ordem material o tempo despendido com o recebimento, leitura e exclusão do spam, o que acaba sendo em verdade um típico “furto” de horas.

Não podemos deixar de ressaltar o risco de danos morais, já que alguns spammers menos escrupulosos costumam enviar mensagens publicitárias com selos pornográficos. Um estudo realizado pela empresa norte-americana anti-spam Brightmail, divulgado pelo jornal Folha de São Paulo em 04.07.2002, constatou, na época, que o spam pornográfico crescera 450% na rede em menos de um ano.

Os prejuízos não atingem apenas os usuários, mas também os provedores de acesso, responsáveis pela intermediação das mensagens.

A Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Internet – ABRANET – elaborou um estudo para apurar os prejuízos causados pelo spam. Do resultado dessa pesquisa, restou consignado que os custos dos provedores são em muito majorados devido ao alto tráfego de spams, e o prejuízo financeiro mensal estimado é de noventa milhões de reais. Aproximadamente um terço de todos os e-mails enviados na Internet em território nacional corresponde a spams.

Os prejuízos causados aos provedores ocorrem pela ocupação de seus servidores de maneira não-otimizada, acarretando perda de tempo e conseqüente queda na qualidade dos serviços. Os investimentos em proteção de servidores, assim como os gastos com monitoração e segurança, poderiam ser drasticamente diminuídos caso houvesse um meio de conter o abuso cometido pelos spammers.

Do lado dos spammers, encontramos argumentos esdrúxulos do tipo: o spam é inofensivo, a grande maioria dos destinatários das mensagens não se importa com isso, basta apagar para se ver livre, e outros argumentos sem a menor sustentação para ouvidos mais atentos.
Mas, além das considerações levantadas acima contra a prática do spamming, está a questão do direito à privacidade.

A busca de endereços eletrônicos na Internet com o intuito de auferir vantagem comercial ou não agride o preceito constitucional exposto. É autêntica violação da vida privada o rastreamento promovido por spammers para formar bases de dados sobre participantes do mundo digital que não prestaram consentimento, bases estas oferecidas largamente na rede por preços acessíveis, servindo aos mais variados propósitos, com destaque para o oferecimento abusivo de bens e serviços.

Apavorados por tamanha intromissão na nossa privacidade, poderíamos questionar: como os remetentes das mensagens sabem tantas informações a nosso respeito, se nós, em diversos casos, nem sequer sabemos quem são eles?

Refletindo sobre tudo o que já foi observado até aqui, podemos concluir que um spam é produzido basicamente de duas maneiras: coleta e posterior comercialização dos dados pessoais dos visitantes de determinados sites, através da utilização de cookies, formulários e bancos de dados on-line.

Assim, ao navegarmos, consciente (formulários, p. ex.) ou inconscientemente (cookies, p. ex.), cedemos dados a nosso respeito; terceiros tomam conhecimento deles e podem utilizá-los diretamente para fins próprios ou, o que é mais freqüente, para vendê-los a outros interessados, dentre os quais os denominados corretores de informações, que, por sua vez, formam um complexo de dados relativos a determinadas pessoas – um verdadeiro código genético – e comercializam-no. Os principais compradores dessas PIIs – empresas comerciais – analisam os indivíduos que mais se adequam aos produtos comerciais colocados no mercado e fazem o chamado marketing direto, sendo o spam o meio mais difundido na atualidade para a realização de tal propaganda.

Devido ao caráter puramente anárquico assumido pela prática do spamming, conclusivamente, merecemos mais proteção à nossa privacidade do que os publicitários à sua liberdade de invadir caixas postais de correios eletrônicos.

Entrementes, o que mais preocupa os internautas não é o spam propriamente dito, mas o que está por trás dele. E, apesar de o

direito também proteger o receptor de correspondências não solicitadas e importunas, a maior problemática reside no fato de a coleta de dados decolar a altitudes inalcançáveis pelo poder de polícia estatal, correndo o risco de se abolir, por completo, o direito fundamental à privacidade que a todo ser humano é inerente.

2.2.2 A monitoração eletrônica do estilo de vida

Apenas observando a atividade dos spammers, fica evidente que, de fato, estamos sendo monitorados.
Já vimos que os cookies são capazes de monitorar tudo o que fazemos conectados à Internet: os sites que visitamos, quanto tempo permanecemos nele, qual a freqüência de visitação etc. Bem, por outro lado, verificamos também que outros meios eletrônicos, como o satélite, tem hoje capacidade de focalizar a fachada de nossa casa e espionar o fluxo de entrada e saída dela. O que é pior – no tocante à violação da privacidade – é que referido satélite também pode estar diretamente conectado à Grande Rede, podendo ser acessado e monitorado por quem tiver algum conhecimento básico de computação.

É, portanto, preocupante o destino que está reservado à privacidade da pessoa humana no andar do processo tecnológico. A vida está sendo monitorada escancaradamente nos seus mais íntimos aspectos. Somente para dar uma nova luz ao raciocínio, vejamos como um indivíduo comum poderia ter sua privacidade invadida através dos meios eletrônicos num dia de rotina. Daremos a esse sujeito o nome hipotético de Ruy:

7h. Acordar, tomar café e escovar os dentes.

Um dos poucos momentos em que Ruy ainda pode acreditar não estar sendo monitorado. Pelo menos o banho ele sabe que é particular.

7h45. Acessar a Internet para conferir as notícias, pagar contas “on-line” e verificar seu correio eletrônico pessoal.

Os cookies entram em ação finalmente. Cada página acessada por Ruy estará sendo registrada em algum lugar do planeta, e cada transação que Ruy fizer será armazenada e posteriormente analisada.

8h30. Apagar as luzes e sair de casa.

A empresa de serviços públicos local pode estar monitorando o consumo de luz de Ruy para poder operar seus sistemas com mais eficiência e para se antecipar aos períodos de carga elevada. Ao sair de casa, Ruy é vigiado pelo sistema de câmeras colocado em sua

cidade, com o fito de capturar bandidos ou mesmo um satélite a quilômetros de distância pode acompanhar seu trajeto ao ar livre.

9h. Atender o telefone celular e tratar de negócios com seu chefe.

Todas as chamadas discadas ou recebidas pelo telefone de Ruy estão sendo registradas na operadora telefônica respectiva. Além disso, embora seja algo não muito comum, existe a possibilidade de o telefone de Ruy estar interceptado. E se assim fosse, imaginemos a tragédia que seria para a empresa em que Ruy trabalha, se o autor da interceptação fosse seu concorrente mais férreo.

9h30. Entrar no prédio do escritório utilizando-se do crachá eletrônico.

Os crachás eletrônicos podem comprovar que Ruy esteve no escritório em um determinado horário, assim como as câmaras de vídeo no estacionamento, no elevador e no interior do edifício. Esses dados são utilizados, a priori, para fins de segurança, mas podem também ser usados para avaliações de desempenho e disputas entre funcionários.

10h. Verificar e enviar e-mail do local de trabalho.

Nesse caso, não apenas o provedor de acesso estará coletando toda a navegação de Ruy, mas também seu empregador – e legalmente, tem o direito de fazê-lo se o meio utilizado for o sistema do trabalho.

11h30. Comprar um livro no site da livraria Saraiva.

A Saraiva se estabeleceu como uma das maiores livrarias on-line do Brasil, em parte por oferecer serviço personalizado. Isso só pode ser feito por meio de coleta de informações sobre o que o cliente gosta ou não em relação a determinados títulos. E, apesar de a política de privacidade da empresa parecer séria, qualquer descuido pode ser fatal, tendo em vista a sensibilidade das PIIs coletadas.

12h30. Almoço com clientes em potencial; pagar a conta com cartão de crédito.

As administradoras de cartões de crédito estão entre as maiores coletoras de PIIs. Nada mais interessante para uma empresa do que saber exatamente quais as tendências de compra das pessoas. Ruy, neste caso, pode ser alvo de um direcionamento de marketing direto dos que detiverem tais informações.

15h. Participar de uma reunião virtual através de teleconferência.

Por motivos de segurança, muitas vezes é exigida uma identificação para se ter acesso à teleconferência. Essas informações são registradas nos sistemas de bancos de dados das empresas de telefonia e podem ser acessadas pelo comprador do serviço ou por autoridades policiais ou judiciais.

18h. Sair do escritório, passar no mercado para comprar mantimentos, utilizando cartão de desconto.

Ruy novamente vai precisar do crachá eletrônico para deixar o escritório. No mercado, o cartão de desconto, apesar de apresentar vantagens, é um eficiente captador de PIIs - todos os hábitos de consumo de alimentos, bebidas e demais mantimentos domésticos. Essas informações são valiosas não só para o mercado em si, mas também para seguradoras, empregadores e corretores de informações.

20h. Chegar a casa e pedir uma pizza por telefone.

Ao completar a ligação, o atendente saúda Ruy da seguinte maneira: “Boa noite, Sr. Ruy; deseja o de sempre?”. O atendimento personalizado se deve ao identificador de chamada – serviço oferecido pela telefonia local – que está diretamente ligado ao banco de dados do sistema da pizzaria, onde podem ser encontrado todos os pedidos feitos por Ruy, desde o primeiro feito anos atrás. Ao final da ligação, o atendente ainda flerta: “Gostaria de debitar o valor no seu cartão Visa?” (número também presente no sistema da pizzaria).

22h. Acessar um site que trata da doença contraída por sua mãe.

Embora Ruy saiba que as informações por ele procuradas dizem respeito à doença contraída por sua mãe, os donos do site não sabem. Para a empresa farmacêutica e a companhia de seguros patrocinadoras do site, Ruy será considerado uma pessoa que possivelmente tem uma doença séria. As conseqüências? ....

23h30. Ligar para o serviço de despertador telefônico para acordá-lo às 7h.

Esse será a primeira PII coletada de Ruy no dia.

2.3 Medidas de proteção à privacidade

Como já observado, a nossa Constituição Federal consagra o direito à privacidade como direito fundamental da personalidade e prevê ressarcimento indenizatório em caso de danos materiais e morais decorrentes de eventual violação a esse direito.

Também não pode fugir de nossa atenção o prescrito no artigo 12 do Novo Código Civil Brasileiro:
"Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei."
Vê-se, pois, que referida norma se coaduna perfeitamente com o texto do art. 5º, X, da Constituição Federal. Aliás, entendemos que ressaltou ainda mais a importância e a racional necessidade de se protegerem todos os direitos inerentes da personalidade, dos quais se destaca a privacidade.

Mas, não só no ordenamento jurídico brasileiro, o direito à privacidade é objeto de acalorada proteção. Tanto é fundamental a proteção a precitado direito, que a Declaração Universal dos Direitos Humanos prevê que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques às suas honra e reputação. Contra tais intromissões, ou ataques, toda pessoa tem direito à proteção da Lei."
Contudo, tanto os consagrados princípios da Declaração Universal dos Direitos do Homem quanto a pétrea cláusula constitucional e o Novo Código Civil parecem ser irrelevantes aos ombros da gigantesca rede mundial de computadores.

"O direito de estar só, de ser deixado só, cada vez mais se distancia de uma esperada tutela jurisdicional. Cada vez mais nos distanciamos do direito que nos autoriza a vagar pelo planeta sem termos nossa imagem divulgada ou impressa, sem termos nossos passos marcados e rastreados, sem termos nossas despesas conferidas pelas fuxiqueiras do Fisco ou pelas administradoras de cartões de crédito. Erodiu-se o direito de não fazer parte daquilo a que não fomos, por lei, obrigados".

No entanto, não podemos nos curvar aos caprichos da toda poderosa Internet. Temos (digo a sociedade em geral) que nos conscientizar que estamos, sim, tendo nossa privacidade invadida por meios eletrônicos que coletam nossos dados mais pessoais e comercializam-nos, não necessariamente para o nosso bem, mas para a satisfação dos seus interesses, que invariavelmente vão exatamente de encontro aos nossos.

Na medida em que a população usuária da Grande Rede se conscientiza que o valor da sua privacidade vale mais do que meros atrativos virtuais, os grandes responsáveis pela devassa nas informações da vida particular de terceiros se retraem e procuram não mais invadir uma esfera que não lhes diz respeito (nossa privacidade).

Já podemos constatar, na prática, que empresas sérias, preocupadas com a repercussão oriunda de um ato atentatório à privacidade de clientes, estão investindo em meios tecnológicos destinados à proteção dos dados armazenados nos seus bancos de dados.

Outrossim, políticas de privacidade passam a ser essenciais na captação de clientes. Pois, se hipoteticamente existissem duas empresas de comércio eletrônico, sendo uma movida de acordo com as políticas de privacidade enquanto a outra não, qual delas teria o maior índice de confiança por parte do usuário-consumidor? Por óbvio que a primeira delas. Em vista disso, muitos dizem que a Internet tem o poder de se auto-regularizar, pois quem não se moldar, objetivando a confiança do cliente quanto a sua privacidade, não terá vez no universo cibernético.

De qualquer forma, medidas de proteção à privacidade devem ser tomadas por toda coletividade, incluindo-se no gênero usuários, empresas e principalmente o Poder Público, responsável supremo pela manutenção do estado de direito, a que todos nos curvamos.

Naturalmente, não temos a pretensão de dar a solução para todos os problemas da questão da privacidade na Internet em decorrência da coleta e comercialização de dados, mas julgamos oportuno delinear algumas considerações sobre importantes medidas destinadas à tutela da privacidade.

2.3.1. Políticas de privacidade

A simples coleta de Informações Pessoais Identificáveis por parte de determinados websites configura-se invasão de privacidade. Por isso, é fundamental para a manutenção da ordem pública no ambiente virtual uma política clara e explícita, declarando quais dados serão coletados e o fim destinado aos mesmos. Na atual conjuntura, ter uma política de privacidade séria significa mais do que simplesmente respeitar a vida íntima dos usuários. Acima de tudo, demonstra o interesse do site em alcançar a confiança dos clientes – principal peça do processo de fidelização.

As políticas de privacidade devem de forma bastante clara, informar o usuário sobre o tipo de informações que serão coletadas, o modo como será realizada a coleta dos dados, outrossim, como serão eles gerenciados, os motivos pelos quais os armazenam em seus bancos de dados, a possibilidade de cruzamento das informações coletadas junto a terceiros etc.

Mas na seara jurídica, qual a natureza dessas políticas de privacidade?

Analisando detidamente políticas de privacidade de diversos sites, depreendemos tratar-se de contratos de prestação de serviços, os quais classificam-se como contratos de adesão, e, como tal, estão subordinados aos preceitos estabelecidos no Código Civil, e notadamente no Código de Defesa do Consumidor.

Vejamos, com efeito, o que elenca o artigo 54 do Código de Defesa do Consumidor:

"Art. 54: Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo."

De fato, no caso das políticas de privacidade encontradas em diversos sites da Internet, ou o usuário aceita seus termos, ou deixa de acessá-lo.

Vejamos, nesse sentido, o exemplo do site do Unibanco.com:

"Ao utilizar o Unibanco.com o usuário estará aceitando expressamente todas as práticas descritas nesta Política de Privacidade. Dessa forma, aconselhamos àqueles usuários que não concordarem com a nossa Política de Privacidade então adotada, a não utilização deste site."

Um ponto muito controverso encontrado na política de privacidade desse mesmo site aparece no assunto intitulado "Informação de outras fontes". Vale a pena analisar:

"Visando melhorar a personalização de nossos serviços (por exemplo, fornecer melhores recomendações de produtos ou ofertas especiais que acreditamos interessar aos nossos usuários) ou para fins de operações de processo de crédito, podemos vir a receber suas informações de outras fontes, tais como empresas do grupo Unibanco, empresas parceiras, outros sites da web, adicionando-as às informações que já detemos."

Num primeiro momento podemos pasmar ao lermos os termos acima expostos, mas a argumentação lógica dos sites adotantes dessas políticas é demasiadamente simples e legalista, pois vai ao encontro do princípio estampado no art. 5º, inciso II, da Constituição Federal, no sentido de que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". Ora, e por mais que pareça uma confissão de autoria de ato ilícito – participar do processo de comercialização de dados pessoais –, pois como já vimos a comercialização de Informações Pessoais Identificáveis é um

autêntico atentado à privacidade da pessoa humana, não podemos olvidar que o usuário que aceitar a política de privacidade estabelecida pelo site estará concomitantemente concordando com referido ato comercial. Por isso anteriormente já afirmamos que, em troca dos produtos e/ou serviços, os sites querem as chamadas PIIs, uma genuína permuta entre sites e usuários.

Existem, por outro lado, políticas de privacidade mais amenas como a do Banco Real que, inclusive, é certificada pelo Selo de Privacidade OnLine da Fundação Vanzolini. Nela, não há menção sobre o recebimento de PIIs a partir de outras fontes, o que a nosso ver apresenta mais fidedignidade ao cliente que na política mostrada pelo Unibanco.com.

Por outro lado, apesar de as políticas de privacidade claras e sérias estarem se proliferando, atendendo aos interesses dos usuários, não há como não ter um controle eficiente acerca do seu fiel cumprimento. Fácil é estabelecer regras; difícil é cumpri-las. Apoiado nesta assertiva, Danilo Duarte de Queiroz pontifica com extrema propriedade que:

"Como em termos de Internet e resoluções relacionadas à mesma, o Direito no mundo (e em especial no Brasil) ainda está engatinhando, as medidas jurídicas a serem tomadas em caso de abuso no tratamento das informações e de descumprimento das normas de privacidade estabelecidas, seriam as mesmas utilizadas em casos de descumprimento de contratos 'comuns' e de violações a direitos morais de maneira geral, com as ações judiciais pertinentes".

Percebendo a deficiência das políticas em se demonstrarem confiáveis, não quanto às regras que postulam cumprir, mas na sua fiel execução, surgem programas de controle de qualidade independentes que, aprioristicamente, têm a função de exercer uma fiscalização sobre as políticas de privacidade dos sites a ele filiados. É, pois, de extrema importância a difusão desse tipo de controle, uma vez que trará maior segurança aos usuários e seriedade no trato de dados pessoais alheios por parte das empresas.

Na frente destes programas, a Fundação Carlos Alberto Vanzolini encabeçou o Programa Selo de Privacidade OnLine, consubstanciado na NRPOL – Norma de Referência da Privacidade Online, cujo principal objetivo é estabelecer determinados Princípios Éticos que devem ser seguidos por Organizações atuantes na Internet, visando proteger a privacidade das Informações Pessoais Identificáveis de seus usuários.

O Programa Selo de Privacidade OnLine utiliza-se de um selo com o logotipo da Fundação Vanzolini como certificado de qualidade na

política de privacidade do site. Ter o selo significa que respectivo site é certificado por uma organização independente através de seus auditores, o que assegura o tratamento adequado aos dados pessoais dos seus usuários.

2.3.2 Anonimato

Se partirmos do princípio de que nossa privacidade é devassada na Internet pelo simples fato de, consciente ou inconscientemente, estarmos cedendo nossas informações pessoais, talvez a solução para este problema seja o anonimato, ou seja, o direito de não se identificar, sem, contudo, ter que se esconder.

Entretanto, primeiramente devemos analisar a legalidade do anonimato. A Constituição Federal pauta dois tipos de anonimato: o de expressão do pensamento e o de trânsito.

O mesmo texto constitucional declara vedado, em tese, o anonimato de expressão do pensamento (art. 5º, IV) e, por outro lado, autoriza o anonimato de trânsito; não expressamente, mas pela simples dedução do prescrito no art. 5º, II, onde está consagrado que ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei.

Transpondo o conceito para a questão relacionada à Internet, pode-se concluir que “um simples navegar anônimo através da Internet é estritamente legal, pois que no correr da navegação não se faz essencial a manifestação de pensamento”.

Mas mesmo vedado o anonimato de expressão do pensamento pela Constituição Federal, em particulares ocasiões, esta vedação é amortizada, tendo em vista a proteção de bens jurídicos de maior relevância. E dentre esses bens jurídicos de relevo encontra-se a privacidade.

Na Internet, nomeadamente, o direito à privacidade sofre profunda e inegável ameaça, ainda mais em relação ao destino reservado aos dados pessoais. Portanto, não pode ser considerado ilegítimo ou mesmo ilícito o anonimato na expressão do pensamento, quando o objetivo imediato é a proteção da privacidade.

Corroborando a tese levantada linhas atrás, Amaro Moraes e Silva Neto saúda-nos, valendo-se de sua maestria ímpar, com o seguinte ensinamento:

“Numa sociedade livre, a anonimía não é apenas necessária: é indispensável, haja vista que diversas são as situações onde não queremos – e não devemos – ser identificados.”

Fica ainda mais claro perceber a importância do anonimato na Internet, se considerarmos – como já o fizemos – o que poderia ocasionar a uma pessoa que pertença a um grupo de minorias (os alcoólatras anônimos, por exemplo), se tivessem seu nome divulgado na grande rede à mercê de toda população mundial. No mesmo sentido, podemos citar o sujeito que faz uma denúncia anônima do paradeiro de um traficante de drogas.

De toda colação feita até aqui, parece-nos evidente a absoluta licitude do anonimato na Internet, tanto o de trânsito quanto em diversos casos na expressão do pensamento.

A despeito de parecer uma medida extremamente eficaz na tutela da privacidade no ambiente cibernético, já vimos que a capacidade tecnológica em coletar informações pessoais identificáveis, sem nosso consentimento e/ou conhecimento, vai além da nossa intenção de não cedermos dados pessoais, razão pela qual é certo afirmar que, sem auxílio da mesma tecnologia, não dispomos de meios que nos protejam em absoluto da violação de nossa privacidade. Pensando nisso, nobres programadores vêm disponibilizando inúmeros programas de computador que ocultam nossa navegação, bem como nossas mensagens eletrônicas.

Mas, atento às conseqüências decorrentes do anonimato na Internet, o Estado – sem dúvida alguma também pressionado pelas grandes corporações comerciais – vê no anonimato um campo propício para salvaguardar crackers, pedófilos, terroristas etc. Daí a existência de sistemas como o já analisado Echelon.

Em que pesem as alegações dos “seguranças do mundo”, não deve o direito à privacidade de todas as pessoas do planeta ficar sobreposto a meras investigações; seria um total contra-senso.

Há de existirem medidas no combate a terroristas, pedófilos e crackers que não violem o princípio maior do direito à privacidade.

2.3.3 Criptografia

A criptografia pode ser definida como a arte de cifrar a escrita, de modo a torná-la ilegível para quem não possuir o respectivo código. Vejamos o exemplo de uma palavra encriptada:

BQHOSNFQZEHZ

Parecem letras mortas colocadas aleatoriamente no papel, sem qualquer significado. Mas trata-se, na verdade, de uma representação criptográfica da palavra “CRIPTOGRAFIA” (desculpem o trocadilho). Parece complexo? Na verdade é bem simples. Cada letra do alfabeto

é substituída pela letra que a antecede. Observemos atentamente as duas representações da palavra “criptografia”:

C
= >
B

R
= >
Q

I
= >
H

P
= >
O

T
= >
S

O
= >
N

G
= >
F

R
= >
Q

A
= >
Z

F
= >
E

I
= >
H

A

=>
Z

Esta é a chamada criptografia simétrica. Nela, a mesma senha utilizada para cifrar a mensagem é também a necessária para decifrá-la. Fácil observar, portanto, que o processo é deveras limitado e inseguro, uma vez que a senha, em algum momento e por algum meio, deverá ser passada do remetente ao destinatário.

Mas a revolução da criptografia se deu mesmo com o surgimento da chamada criptografia assimétrica, que se utiliza de duas chaves, uma privada (senha) e outra pública (nome de identificação). A chave pública, como o próprio nome diz, pode ser do conhecimento de todos; já a privada é sabida apenas pelo destinatário da mensagem. Exemplificando: "Y" mandou uma mensagem encriptada para o endereço eletrônico de "X" (daí podemos deduzir que "Y" conhecia a chave pública de "X"). Agora, para que "X" consiga visualizar a mensagem lhe enviada por "Y" deverá abri-la com sua chave privada (que só ele, "X", conhece). Importante observar que a chave privada só abre a mensagem que foi enviada para a chave pública própria. Portanto, a chave privada de um suposto "K" jamais abriria a mensagem enviada à chave pública de "X".

É nítida, portanto, a superioridade da criptografia assimétrica diante da simétrica, bastando lembrar que nesta ao menos duas pessoas têm de saber a "senha", enquanto naquela apenas a destinatária final.

Além disso, através de programas de computadores com criptografia assimétrica, como o mundialmente conhecido PGP – Pretty Good Privacy (privacidade muito boa), desenvolvido por Philip Zimmermann, é possível encriptar mensagens utilizando complexas operações matemáticas praticamente indecifráveis, senão pela utilização da chave privada.

Mas o que importa para este estudo é saber como a criptografia pode ajudar na tutela do direito à privacidade com relação à coleta e posterior comercialização das Informações Pessoais Identificáveis.

Até o presente momento, o correio eletrônico é o maior carecedor de proteção criptográfica, pois, conquanto poucas pessoas saibam, a mensagem eletrônica, antes de chegar à caixa postal do respectivo destinatário, percorre um tortuoso caminho dentre os servidores do remetente e do destinatário, podendo ser, neste ínterim, facilmente interceptada, tanto pelos servidores como por hackers ou crackers. Mas o que mais assusta é que a interceptação de mensagens eletrônicas pode ser feita em larga escala, com uso de palavras-

chave (como o faz o projeto Echelon). Daí, para cair em mãos de terceiros mal intencionados ...

Por outro lado, a despeito da mensagem eletrônica ser considerada um meio vulnerável de troca de informações, se fosse usada a criptografia chegaríamos ao paradoxo de verificar ser ela (a mensagem eletrônica) o meio mais seguro de comunicação. Aí reside o diferencial da criptografia.

Parece, então, estar descoberta a solução para a defesa da privacidade, pelo menos no que concerne ao envio/recebimento de e-mails. No entanto, como não podia deixar de ser, temos, em contrapartida, interesses de ordem política, máxime aos de defesa militar de países como EUA e Canadá, que chegaram a proibir a exportação de produtos militares e estratégicos, dentre esses os de criptografia forte.

Proibir o uso da criptografia, a fim de impedir comunicações de terroristas e contrabandistas entre si, seria o mesmo, em termos de desproporção, que proibir a todos o uso de celulares, só porque está constatado que criminosos se utilizam desses aparelhos para traficar drogas. Um total disparate.

Da mesma forma que é proibido adquirir armas sem o devido porte legal para conter a criminalidade – e o que vemos na prática são os criminosos potencialmente armados –, impedindo-se o uso da criptografia, quem vai de fato sair prejudicado são as pessoas honestas que terão sua privacidade devassada, enquanto os criminosos, terroristas etc, farão total uso da tecnologia, embora, ilegalmente.

Inteligente foi o trocadilho colocado por Phillip Zimmermann: “se a criptografia foi considerada fora da lei, apenas os fora-da-lei terão criptografia”.

Outra aplicação utilíssima para a criptografia seria nos bancos de dados de PIIs. Isso, ao menos, dificultaria a ação dos hackers e crackers, bem como na manipulação dessas informações por parte de funcionários não treinados nem habilitados para tanto.

Aliás, temos visto empresas sérias, como a Unibanco.com, declarando em sua política de privacidade utilizar da criptografia na proteção dos dados pessoais. Senão vejamos:

“As informações dos usuários são coletadas pelo Unibanco por meios éticos e legais e guardadas de acordo com padrões rígidos de segurança e confidencialidade. Nós trabalhamos para proteger a segurança de sua informação durante a transmissão usando Secure

Socket Layers (SSL) que criptografa as informações que os usuários digitam.” (grifo nosso)

Derivado do direito à privacidade, podemos extrair o direito ao sigilo de informações, e, deste, o direito à criptografia que, na verdade, mais se aproximaria de uma garantia instrumental à preservação da privacidade.

2.3.4 Controle Estatal

Embora sejamos adeptos da corrente que acredita não ser a legislação, principalmente a punitiva, a grande arma para enfrentar os violadores da privacidade humana no ambiente virtual, dada a natureza distribuída e global da Internet, num período em que a Rede está em plena fase de desenvolvimento, temos que admitir a necessidade de determinadas questões serem regulamentadas, máxime no tocante à fiscalização dos detentores de informações pessoais.

Um instrumento garantidor dos preceitos constitucionais, genuinamente brasileiro, deve, neste ensejo, ser enfatizado devido à grandeza de sua importância para a proteção dos dados pessoais. Referimo-nos ao Habeas Data, instituto jurídico que permite a qualquer pessoa ter ciência das informações a seu respeito, detidas pelo governo, para exame e eventual retificação.

Com efeito, segundo é textual no artigo 5º, inciso LXXII, da Constituição Federal de 1988:

“Art. 5º ...
LXXII – 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;”

Conforme deliberado pelo texto constitucional, há duas hipóteses em que poderá o cidadão valer-se do HD: para ter conhecimento dos dados pessoais, tidos pelo governo, a seu respeito e a eventual retificação dos mesmos.

O remédio constitucional em análise somente se justificará, ocorrendo recusa do governo em prestar tais informações ou em retificar o dado supostamente incorreto.

É de se acentuar a relevância do instituto que dota o cidadão da necessária proteção de seus dados pessoais e de sua privacidade.

Mas, e quanto às informações pessoais constantes permanentemente nos bancos de dados de empresas privadas?

Atento aos eventuais danos à privacidade, decorrentes do mau uso de Informações Pessoais Identificáveis, trouxe o Código de Defesa do Consumidor uma série de regras destinadas à sua proteção, não especificamente no meio virtual, incluindo dispositivo semelhante ao Habeas Data, mas no âmbito privado;

"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.
Parágrafo 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.
Parágrafo 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.
Parágrafo 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.

Parágrafo 4º - Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
Parágrafo 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". (grifo nosso)

Ratificando os termos do art. 34 do CDC, porém com mais ênfase à coleta e ao gerenciamento de dados pessoais através da Internet, tramita no Congresso Nacional o Projeto de Lei nº 3.360/00, dispondo sobre a privacidade de dados e a relação entre usuários, provedores e portais em redes eletrônicas.

Dentre outros detalhes, o Projeto de Lei supracitado reza, ainda, que as Informações Pessoais Identificáveis só poderão ser coletadas após expressa autorização do usuário e também assegura que os dados coletados não serão usados para outro fim senão o expresso na ciência do usuário. Fixa, ainda, uma multa no valor de R$ 300.000,00 (trezentos mil reais) para quem descumprir o prescrito nos seus mandamentos.

Em que pese o zelo merecido à proteção da privacidade, uma sanção pecuniária nesse patamar pode acabar transformando um diploma legal de profunda relevância em letra morta no mundo jurídico.

Faltam, por outro lado, normas fiscalizadoras das políticas de privacidade oferecidas pelos websites, o que talvez resolveria a maioria dos problemas relativos à coleta de PIIs. Pois, sem fiscalização, mesmo que, em tese, a política do site seja um modelo de respeito à privacidade, como poderemos ter certeza que está sendo cumprida? Só mesmo através de uma efetiva fiscalização por parte de agentes estatais ou independentes prestadores de serviços públicos.

De qualquer forma, nos casos envolvendo a privacidade, sobretudo no quanto afeto aos dados pessoais, os Juízes e Tribunais é que terão um papel imprescindível na solução das lides, mormente pelo fato de misturarem-se questões meramente subjetivas (privacidade) com temas modernos e carentes de legislação específica.

2.3.5 Auto-regulação

À medida que a Internet cresce, cresce também a preocupação com a privacidade dos seus usuários. É certo afirmar, portanto, que, partindo do princípio de que não existe controle direto sobre a manipulação de dados pessoais, gradativamente as decisões dos usuários terão como base o critério da confiança.

Significa dizer que haverá uma verdadeira declaração de guerra dos usuários comuns aos manipuladores de PIIs que não convergirem às regras da proteção à privacidade.

Sabido que as principais adestradoras de Informações Pessoais Identificáveis são as empresas “ponto com”, a essas nada interessa terem a antipatia dos consumidores. Isso, naturalmente, fará com que elas se moldem aos interesses dos seus clientes, ganhando-lhes a confiança. Confiança essa só garantida se forem seguidas à risca as políticas de privacidade previamente combinadas.

Portanto, parece-nos que o futuro da Internet seguirá o caminho traçado pela confiança que os usuários depositarem nela. Se houver efetiva procura por privacidade, as detentoras de PIIs terão que ceder, ou, então, nadarão contra a maré.

“Aprender a utilizar políticas de privacidade como parte de sua rotina individual de troca de dados pode ajudar a Internet a passar da era da coleta oculta de dados para um tempo em que os termos e condições da maioria das trocas de dados sejam caras, transparentes, mutuamente acordados e rigorosamente cumpridos” .

Conclusão

No decorrer do presente estudo, foram abordadas questões acerca da violação ao direito à privacidade na Internet, de cuja análise pode-se depreender as seguintes conclusões:

1. A Internet é, sem dúvida, o meio eletrônico de maior capacidade de captação e gerenciamento de informações.

2. Informações Pessoais Identificáveis têm alto valor econômico para diversos setores da sociedade, como empresas e governos, uma vez que do cruzamento desses dados é possível chegar ao perfil da pessoa correspondente e, com isso, direcionar investimentos (no caso das empresas) e investigar criminosos (no caso dos governos).

3. A coleta de dados na Internet, sem o conhecimento ou a prévia autorização do usuário, afronta o direito à privacidade, podendo acarretar danos irreparáveis ao usuário, o qual dispõe de poucos meios para impedir tal prática.

4. A melhor maneira de impedir que a privacidade do usuário da Internet seja violada é a sua própria conscientização. Quando os sujeitos que agora se sentem violados não mais embarcarem nos websites desprovidos de políticas de privacidade convenientes, sérias e, preferencialmente, fiscalizadas por agentes competentes, haverá uma substancial possibilidade de sopesar a questão.

Apoiar empresas com políticas de privacidade sólidas e claras não apenas ajuda a proteger sua privacidade como também encoraja uma tendência geral e direção à plena divulgação de todas as práticas que têm a ver com a confiabilidade de uma empresa.

Na nova economia Internet, empresas, que tentam esconder o jogo, em especial as que se engajam em atividades pouco confiáveis, ver-se-ão nadando contra a maré.

Portanto, estamos convencidos de que a melhor estratégia para a manutenção da nossa privacidade no ambiente virtual é, de fato, a prevenção.

Bibliografia

Livros

BAPTISTA, Luiz Olavo (coord.). Novas fronteira do direito na informática e telemática. 1. ed. São Paulo : Saraiva, 2001. 251 p.

BITTAR, Carlos Alberto. Os direitos da personalidade. 5. ed. Rio de Janeiro : Forense Universitária, 2001. 159 p.

CORRÊA, Gustavo Testa. Aspectos jurídicos da Internet. 1. ed. São Paulo : Saraiva, 2000. 135 p.

DE LUCCA, Newton ; SIMÃO FILHO, Adalberto (coords.). Direito & Internet – aspectos jurídicos relevantes. 1. ed. Bauru : Edipro, 2001. 512 p.

DRUMMOND, Victor. Internet, privacidade e dados pessoais. 1. ed. Rio de Janeiro : Lumem Juris, 2003. 277 p.

ERENBERG, Jean Jacques. Publicidade patológica na Internet à luz da legislação brasileira. 1. ed. São Paulo : Juarez de Oliveira, 2003. 152 p.

FILOMENO, José Geraldo Brito. Manual de direitos do consumidor. 5. ed. São Paulo : Atlas, 2001. 580 p.

GARCIA JÚNIOR, Armando Álvares. Contratos via Internet. 1. ed. São Paulo : Aduaneiras, 2001. 280 p.

GONÇALVES, Carlos Roberto. Principais inovações no Código Civil de 2002. 1. ed. São Paulo : Saraiva, 2002. 101 p.

GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (coords.) Direito e Internet: relações jurídicas na sociedade informatizada. 1. ed. São Paulo : Revista dos Tribunais, 2001. 257 p.

GRECO, Marco Aurélio. Internet e direito. 2 ed. São Paulo : Dialética, 2000. 223 p. (Não há indicação da data da 1ª Ed.)

HOUAISS, Antônio; VILLAR, Mauro de Salles. Minidicionário Houaiss da língua portuguesa. 1. ed. Rio de Janeiro : Objetiva, 2001. 481 p.

JENNINGS , Charles; FENA, Lori. Privacidade.com. Trad. Bazán Tecnologia e Lingüística. 1. ed. São Paulo : Futura, 2000. 265 p. (título original: The hundredth window: protecting your privacy and security in the internet. 2000)

MARCACINI, Augusto Tavares Rosa. Direito e informática – uma abordagem jurídica sobre a criptografia. 1. ed. Rio de Janeiro : Forense, 2002. 200 p.

MEIRELLES, Hely Lopes. Mandado de segurança, ação popular, ação civil pública, mandado de injunção, “Habeas Data”... 25. ed. São Paulo : Malheiros, 2003. 566 p.

MORI, Michele Keiko. Direito à intimidade “versus” informática. 1. ed. Curitiba : Juruá, 2001. 121 p.

PINHO, Rodrigo César Rebello. Teoria geral da Constituição e direitos fundamentais. 1. ed. São Paulo : Saraiva, 2000. v. 17. 188p. (Coleção sinopses jurídicas)

QUEIROZ, Danilo Duarte de. Privacidade na Internet. In: REINALDO FILHO, Demócrito (coord.). Direito da Informática – temas polêmicos. 1. ed. Bauru : Edipro, 2002. p. 81 - 96.

REINALDO FILHO, Demócrito (coord.). Direito da Informática – temas polêmicos. 1. ed. Bauru : Edipro, 2002. 432 p.

_____. A privacidade na “sociedade da informação”. In: REINALDO FILHO, Demócrito (coord.). Direito da Informática – temas polêmicos. 1. ed. Bauru : Edipro, 2002. p. 25 – 40.

SILVA NETO, Amaro Moraes e. Privacidade na Internet – um enfoque jurídico. 1. ed. Bauru : Edipro, 2001. 208 p.

_____. “Emails” indesejados à luz do direito. 1. ed. São Paulo : Quartier Latin, 2002. 207 p.

ST. LAURENT, Simon. Cookies. Trad. Sérgio Facchim. 1. ed. São Paulo : Berkeley Brasil, 1999. 418 p. (título original: Cookies. McGraw – Hill Companies, 1998)

VENTURA , Luis Henrique. Comércios e contratos eletrônicos – aspectos jurídicos. 1. ed. Bauru : Edipro, 2001. 134 p.

VIEIRA, Sônia Aguiar do Amaral. Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos. 1. ed. São Paulo : Juarez de Oliveira, 2002. 200 p.

Sites

Legaltech.com.br. Disponível em http://www.legaltech.com.br/LegaltechSpam1.htm. Acesso em 20/02/2003.

“Spam pornográfico cresce 450% em um ano na Internet”. Folha Online, 04/07/2002. Disponível em http://www1.folha.uol.com.br/folha/informatica/ult124u10419.shl. Acesso em: 20/02/2003.

Fundação Carlos Alberto Vanzolini. Disponível em http://www.privacidade-vanzolini.org.br/. Acesso em 20/02/2003.

REVISTA DE DOUTRINA DA 4ª REGIÃO
PUBLICAÇÃO DA ESCOLA DA MAGISTRATURA DO TRF DA 4ª REGIÃO - EMAGIS