

FUNÇÃO SOCIAL DA PRIVACIDADE

*Cláudio de Lucena Neto**

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and except in darkness, every moment scrutinized.

George Orwell, 1984.

Apresentação

O desenvolvimento da sociedade contemporânea - a sociedade da informação -, na qual destaca-se como principal capital o conhecimento humano, traz consigo, tanto a necessidade de reavaliação de determinados conceitos e procedimentos técnicos, quanto de elaboração e definição de novos métodos e princípios que haverão de nortear e de buscar conferir equilíbrio às relações entre os indivíduos desta própria sociedade.

A informação, produto direto deste capital do conhecimento humano, é um dos bens de maior valia neste novo panorama mundial. Por esta razão, a sua guarda e a sua manutenção para uso eficiente e seguro deve ser objeto de preocupação de todos os segmentos da sociedade.

Com efeito, o tema já preocupa e ocupa diversas áreas da atuação humana, desde a Tecnologia da Informação, que procura desenvolver ferramentas, aplicativos e técnicas que venham a possibilitar o controle prático e efetivo desta segurança, passando pela Administração, que procura soluções para o gerenciamento das questões e dos recursos humanos envolvidos na manutenção da integridade de dados, chegando até o Direito, que, enquanto sistema normativo, tem como função precípua o estabelecimento de critérios que tornem a convivência social pacífica e equilibrada.

O impacto do problema no Direito é claro, à medida em que o uso indevido, inadequado e desautorizado da informação tende a causar significativos prejuízos, danos de naturezas e volumes os mais diversos, que, já começando a ser quantificados pelas empresas, reclamam reparação.

Dentro, ainda, do próprio Direito, é fácil constatar que o problema alcança vários de seus ramos. A privacidade e a segurança da informação suscitam discussão em matéria de Direito Administrativo, vez que o Estado passa a valer-se de grandes bancos de dados públicos para tornar determinados serviços mais ágeis e acessíveis à população. O Direito Penal, por sua vez, não pode estar alheio à questão, dado que tem urgência em tipificar as condutas violadoras dos seus princípios, de forma a fazer com que aquelas que porventura mostrem-se mais danosas tenham punição mais gravosa. O escopo deste trabalho, porém, há de se restringir a uma análise do problema no plano cível, comercial, empresarial, sem descuidar de traçar, quando cabível, os devidos paralelos com os demais segmentos do direito.

Inobstante a escassa literatura técnico-científica acerca do tema, pesquisas e estatísticas têm sido feitas com surpreendente regularidade, o que demonstra a urgente necessidade da compreensão fática do fenômeno.

O sigilo e a privacidade não são os únicos problemas trazidos pela necessidade de segurança da informação.

Recente pesquisa realizada pelo instituto *Forrester Research* dá conta de que em 62% das empresas americanas os funcionários acessam sites de sexo e de bate-papo durante o expediente. Pelas contas do instituto, isso representa uma perda anual de 470 milhões de dólares em produtividade. Um outro estudo, desta vez do *SurfWatch*, revela que mais de 25% do tempo gasto pelos funcionários conectados à Internet não tem nenhuma relação com trabalho. Perdas acidentais de dados, por sua vez, representam semelhante potencial de prejuízo, pelo que requerem igual tratamento de cautela.

São estas circunstâncias, que atentam diretamente contra a segurança da informação, e que, portanto, representam séria ameaça de dano e de prejuízo para as empresas, que serão objeto do estudo que segue, observadas sob a ótica da legislação, da doutrina jurídica e da tecnologia disponível.

Classificação da Informação

O *state of art* da tecnologia permite que se estabeleçam estágios de proteção diferentes para categorias de informação que requeiram maior ou menor nível de segurança. Com efeito, nem toda a sorte de informação é crucial ou essencial a ponto de merecer cuidados manifestamente especiais. Por outro lado, determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente.

Dmitri Abreu, e Sean Boran expõem, de forma bastante clara, a necessidade de classificação da informação em níveis de prioridade, obviamente, conforme a necessidade de cada empresa, bem como conforme a vitalidade daquela classe de informação para a manutenção das atividades da empresa:

Ø *pública* – informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;

Ø *interna* – o acesso a esse tipo de informação deve ser evitado, embora as conseqüências do uso desautorizado não sejam por demais sérias. Sua integridade é importante, porquanto não seja vital;

Ø *confidencial* – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;

Ø *secreta* – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

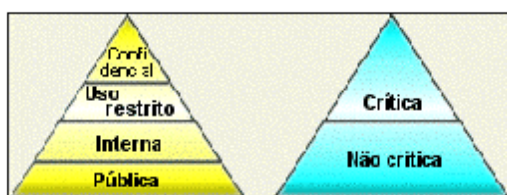


Fig 04. Esquema de classificação da informação segundo a importância de conteúdo e a necessidade de integridade

De forma que, tanto os cuidados, quanto a responsabilidade e o grau de envolvimento do pessoal eventualmente envolvido com a produção, guarda, manutenção e manipulação da informação devem obedecer a determinados critérios de classificação da importância e do

nível de dependência da empresa com relação à referida informação.

Privacidade - *The right to be left alone*

The right to be left alone – the most comprehensive of rights and the right most valued by a free people.

Juiz Louis Brandeis, Olmstead v. U.S. (1928)

Obviamente, sempre que se fala em acesso à informação, deve-se lembrar que, em um estado democrático de direito, a intimidade e a vida privada são garantias constitucionais, e a mera ameaça a qualquer desses direitos é causa de grande comoção e movimentação social. A Constituição Federal, em seu art. 5º, incisos X e XII, dispõe, *verbis*:

X - ... são invioláveis a intimidade, a vida privada, a honra e a intimidade das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua utilização.

XII - ... é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Assim sendo, é de se esperar que o respeito à privacidade seja uma das grandes preocupações no tratamento seguro da informação. Por outro lado, a discussão a esse respeito é delicadíssima, visto que a autenticação, a identificação, conforme já exposto, são requisitos essenciais para que o acesso adequado à informação armazenada em meios eletrônicos possa ser devidamente controlado.

A questão é complexa, e de sua discussão se ocupam renomados autores, evidentemente preocupados com o inegável direito do cidadão à preservação de seus direitos, mas igualmente cômicos de que a proteção à integridade dos dados constitui uma garantia para este mesmo cidadão. Neste sentido, o eminente constitucionalista José Afonso da Silva comenta, com propriedade:

O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.

Ora, é virtualmente impossível ao cidadão comum, ainda que lhe seja dado o direito de controlar a disponibilidade de suas informações pessoais nesses gigantescos e infundáveis bancos de dados, exercer, de fato, este direito. Se a parcela da vida humana que é monitorada, observada pelos outros no contexto dia-a-dia, ainda que volátil e temporária, já é suficientemente exposta a público, o que dizer da parcela de vida que é pesquisável, infinitamente menos transitória, que deixa rastros e registros escritos, visíveis e indelévels?

Cada dia mais os serviços de *e-government* ganham espaço, deixando as funções do estado mais acessíveis e as suas atitudes e políticas mais transparentes, o que parece ser muito positivo. Contudo, para que isso possa ser operacionalizado, enormes bases de dados públicas têm que ser criadas e disponibilizadas para

acesso remoto. Sem uma política consistente de segurança, será informação privada – toneladas dela – exposta a quem quer que tenha acesso a um computador e um canal de acesso à rede, o que, admita-se, pode vir a ter conseqüências desastrosas.

Caminhando na busca de uma solução compatível com os princípios de democracia e, ao mesmo tempo, que permita o necessário controle da informação, diversos estados e organismos internacionais já iniciaram o indispensável trabalho legislativo exigido.

França e Alemanha, esta última tendo sido uma das primeiras nações a regulamentar a matéria, têm codificações legais explícitas dispendo sobre a proteção da privacidade. A União Européia também dispõe de dispositivos normativos disciplinando o acesso, a coleta e o uso de informações privadas.

No Brasil, embora as implicações civis do uso indevido de dados privados já possam obedecer à legislação vigente, no que assim couber, com base no princípio da aplicação analógica da lei, o projeto de Lei n.º 234 tramita no Congresso Nacional, dispendo, especificamente, sobre os crimes contra a inviolabilidade de dados e de comunicações através de computadores, o que poderá contribuir para uma punição mais adequada pra aqueles que violam os princípios da privacidade em bases de dados.

Função Social da Privacidade

Com o enorme potencial de exposição de informação privada que a sociedade da informação oferece, é claro que o direito à privacidade vem assumindo papel relevante como escudo do cidadão contra o poder onipresente do *Big Brother* de ORWELL (1949).

Há razões, contudo, de inegável interesse público, que parecem justificar a necessidade de um mínimo de controle legal sobre o tráfego de informação, muito embora esteja claro que o direito à privacidade não deve ser confundido com o direito ao sigilo profissional, bancário, postal dentre outros já extensivamente disciplinados em textos legais vigentes.

Da mesma forma que ocorreu ao longo dos séculos com o direito à propriedade, que, em seus primórdios, não conhecia limites, a privacidade absoluta pode desvirtuar-se, fazendo com que o indivíduo venha a tirar proveito de uma situação de anonimato – que também encontra vedação constitucional – passando a ser utilizada de forma nociva à sociedade que busca proteger.

Indicando que a esta é uma tendência bastante razoável, a Comissão de Educação do Senado aprovou, recentemente, projeto de lei que dispõe sobre as informações relativas ao acesso à Internet. Pela proposta, os provedores da Internet estarão obrigados a manter registros, por período não inferior a um ano, de todas as conexões realizadas por seus usuários. *Os registros das conexões entre provedores terão que indicar a data, o horário de conexão e desconexão, além do endereço eletrônico atribuído ao cliente.*

Por fim, vale a pena transcrever trecho no qual a Professora Lílian Minardi Paesani parece sintetizar de forma especialmente clara, *o que e como* devem ser consideradas as limitações ao indiscutível direito constitucional à privacidade, limitações essas que devem encontrar justificativas na prevalência do interesse coletivo, a partir da compreensão da *função social da privacidade*:

... podem ser impostos limites à normal esfera de privacidade até contra a vontade do indivíduo, mas em correspondência à sua posição na sociedade, se for de relevância pública. Nesses casos, será possível individualizar, se há interesse público em divulgar aspectos da vida privada do indivíduo. O interesse será relevante somente com relação à notícia cujo conhecimento demonstre utilidade para obter elementos de avaliação sobre a pessoa como personalidade pública, limitando, desta forma – e não eliminando – a esfera privada do próprio sujeito. (grifos da autora)

Controle de Conteúdo

Uma outra forma de estabelecer controle sobre o acesso a informação é por intermédio dos softwares supervisores de conteúdo, que, por intermédio de palavras-chave e de relatórios-padrão de acompanhamento, impedem ou restringem o acesso a determinado tipo de informação, condições previamente estipuladas pelos administradores de sistemas ou pelo *security officer*.

É fácil perceber que a navegação na Internet se transformou em uma gargalo à produtividade. Preocupadas com este panorama, as empresas, paulatinamente restringem sua política de acesso à Internet por meio de configurações especiais de *firewall*, *proxy* ou, ainda, pela monitoração dos *logs*. E começam a punir o que consideram excessos. Na Xerox, por exemplo, quarenta funcionários foram demitidos no ano passado, em várias unidades espalhadas pelo mundo, por uso impróprio da Internet, em *leading cases* mundiais de demissão por justa causa.

Monitoramento de e-mail

O e-mail, de há muito, já se transformou indispensável no mundo dos negócios. Por ser impossível e impensável às empresas visualizar o ambiente de trabalho sem esta ferramenta, elas buscam formas de se proteger do que consideram abusos. Uma delas é monitorar as mensagens eletrônicas, valendo-se de meios de controle de conteúdo. Mais uma vez, a dialética segurança *versus* privacidade vem à tona.

Pesquisa realizada pela revista Info Exame mostra que 34,5% das empresas já monitoram o tráfego das mensagens e 25% pretendem fazê-lo ainda este ano. Responderam à pesquisa, empresas como a Embraer, Pão de Açúcar, Basf, Antarctica, Banco do Brasil, BCP e Usiminas. Uma espiada nas estatísticas do instituto de pesquisas americano Worldtalk Corp. dá uma idéia do tamanho do problema. Baseado nos dados de 100 empresas, o levantamento mostra que 31% das mensagens corporativas têm conteúdo inadequado (de paquera e correntes a informações sigilosas); 10% são spam; 9% contêm arquivos pesados, que congestionam a rede; e 8% carregam vírus, pornografia ou piadas. "No Brasil, mais de 50% das mensagens que trafegam todos os dias nas redes corporativas são lixo", afirma Mauricio Strasburg, diretor da GS Sistemas, empresa especializada em segurança.

Claro está que o funcionário não pode simplesmente ser devassado porque a empresa acredita que assim estará assegurando a integridade de suas informações confidenciais. No mesmo diapasão, o uso indevido de informação e de recursos computacionais da empresa deve ser, na medida do razoável, evitado, e, se preciso, coibido.

Uma solução coerente seria obter, já no momento da admissão do novo funcionário, a assinatura do mesmo no documento individual de adesão à política de uso de redes de dados, o que pode vir no bojo de outras regras, como diretrizes de ética corporativa e acordo sobre propriedade de obras e invenções. Os

funcionários que já estiverem no curso de seu contrato de trabalho também devem ser comunicados e conscientizados de tais políticas, e, ao final, devem aderir formalmente, por meio de assinatura de termo próprio.

Ainda segundo o autor acima citado, as razões da empresa para a adoção da política em questão, bem como as possíveis repercussões (sanções civis, trabalhistas e criminais) decorrentes de condutas e que forem identificadas através da monitoração também devem ser expressamente divulgadas.

Legislação e Normas

As iniciativas legais de disciplinar o tratamento e a segurança da informação já passam a fazer parte do ordenamento jurídico dos estados e das organizações internacionais.

O Parlamento Sueco, em 1973, foi o responsável pela elaboração do *Datalagen*, a primeira Lei orgânica da Europa visando à proteção da privacidade e dos bancos de dados, tanto públicos quanto privados.

Hoje, segundo boletim informativo do escritório de advocacia americano *McBride, Baker & Coles*, que acompanha a evolução da legislação relativa à Tecnologia da Informação, à privacidade e ao Comércio Eletrônico por todo o mundo, a Comunidade Européia (CE), estipulou cláusulas contratuais de proteção à informação e aos dados pessoais de forma a atender à Diretiva aprovada pela própria CE, que exige *proteção adequada* para qualquer transferência de informação privada para países não-membros. Seguindo tal determinação, os Estados integrantes da União são obrigados a reconhecer os países ou organizações internacionais que respeitem tais cláusulas como sendo instituições que oferecem a assim referida *proteção adequada*.

Ainda na Europa, a Alemanha destacou-se desde muito cedo, demonstrando grande agilidade na elaboração de diplomas legais que buscassem a defesa jurídica dos interesses envolvidos com a segurança da informação. Como exemplo, há legislação alemã, inclusive em matéria penal, responsabilizando provedores inclusive pelo conteúdo dos *links* incluídos nos limites de suas páginas. Em vigor desde 1997, o *Germany Information and Communication Services Act* é uma iniciativa legal de estabelecer padrões e políticas econômicas uniformes e seguras para a transmissão de informação e dados eletrônicos.

Na América Latina, a Colômbia, segundo o mesmo boletim, já elaborou texto legal definindo a assinatura digital, bem como regulamentando a atuação das autoridades certificadoras. A segurança jurídica do certificado digital, à luz da lei colombiana, dependerá da exclusividade pessoal do seu uso, da capacidade de verificação, do controle individual, da invariabilidade técnica, de modo que uma alteração impeça a verificação, e da obediência às formalidades normativas do governo colombiano, requisitos que, uma vez atendidos, conferem ao documento eficácia legal.

No Brasil, o projeto de lei PLS 672/99, cuja redação final segue à Câmara dos Deputados, pretende disciplinar o reconhecimento legal do documento eletrônico, bem como as relações jurídicas relativas ao *e-commerce* e ao intercâmbio eletrônico de dados (IED). Entrementes, as situações jurídicas de fato, que não esperam pela produção legislativa, vão sendo resolvidas e conciliadas com base na analogia, no que assim couber.

A respeito, especificamente, da infra-estrutura para chaves públicas – assinatura digital com base em criptografia assimétrica –, o decreto n.º 3.587, de 5 de setembro de 2000, já a define, com respeito ao Governo Federal, complementado pelo decreto n.º 3.865, que estabelece requisitos necessários para a contratação destes serviços pelos órgãos públicos federais.

Alegando as evidentes relevância e urgência da matéria, na Medida Provisória n.º 2.200, reeditada pela segunda vez em 24 de agosto de 2001, o Governo Federal responde à clara pressão do setor privado para a regulamentação de matéria cuja velocidade de desenvolvimento e intenso ritmo de transformação urgem medidas céleres.

A referida MP, portanto, define, em caráter provisório, a infra-estrutura genérica de chaves públicas brasileira, atribuindo competências para a regulamentação, expedição, distribuição e validação de certificados, bem como definindo os requisitos para que a assinatura digital produza efeitos em todas as esferas jurídicas.

Diversas discussões hão de surgir a respeito dos efeitos jurídicos e da adequação das normas propostas à realidade, sendo absolutamente natural o aprimoramento e a atualização periódica dos comandos legais promulgados, instrumentos sem os quais a proteção à esfera de privacidade e à segurança dos dados e da informação corporativa será tarefa inglória e improdutiva.

Considerações Finais

A discussão relativa ao confronto entre o direito à privacidade e o interesse público, entre a preservação da intimidade e o direito coletivo à segurança jurídica da informação, está longe de chegar a termo. Ao contrário, pelos indicadores disponíveis, este será um tema recorrente daqui por diante, à medida em que os sistemas de informação forem se tornando parte ainda mais presente, indissociável e indispensável na vida das pessoas.

Esta nova fronteira da era digital, já atingida pelo escopo de atuação do direito, viverá sempre a reclamar constante atenção e periódica reavaliação, de modo que a tecnologia e os métodos não venham a estabelecer um descompasso social, desarmonizando-se com relação aos princípios e aos valores que devem resguardar.

Há, com efeito, pairando no ar, um sem-número de ameaças à esfera de privacidade do indivíduo, ao intercâmbio eletrônico seguro e confiável de dados, e, por conseguinte, ao desenvolvimento eficiente das relações comerciais e empresariais.

As questões que tratam de segurança e da proteção jurídica da informação corporativa vêm introduzir alterações profundas, significativas, cruciais que, em sede jurídica, tendem a ocorrer inclusive na órbita processual. São procedimentos que irão impactar na maneira como o próprio processo é conduzido. Frise-se, portanto, que não é conveniente que o controle destes atos não esteja ao alcance da compreensão clara de quem, por lei, deve conduzi-los.

É necessário notar, que a esmagadora maioria dos especialistas em atividade no país é de brilhantes e geniais profissionais, que, a despeito da falta de bibliografia disponível, da carência de encontros que propiciem um maior intercâmbio profissional, da ausência de debates públicos e mais criteriosos a respeito dos

grandes temas da área, estudam, especializam-se, produzem, resolvem problemas e são muito, muito bons no que fazem.

Autodidatas, no entanto, apesar do inegável romantismo que suas histórias trazem, serão, dentro em pouco, exceções à regra. É preciso deixar de lado o corporativismo que, com freqüência, dispara ondas de protecionismo profissional para entender a dimensão que o movimento toma. De posse desse entendimento, será patente a necessidade de formar pessoal especializado, tanto para a solução prática e técnica dos problemas e limites que surjam, quanto para a teorização e a análise lógica e jurídica dos litígios que nascerem à sombra deste novo paradigma de mundo.

Quanto aos procedimentos e técnicas aqui expostos, apresentam, inegavelmente, limitações à solução satisfatória do problema da segurança apresentado. Limitações técnicas, contudo, são superáveis. As máquinas ficam mais rápidas, o tempo de processamento diminui, a capacidade de armazenamento aumenta. É por isso que, no momento, parece ser muito mais relevante discutir o *fundamento*, o *objeto* ou *interesse jurídico* que pretendemos proteger ao tratar da necessidade de segurança da informação corporativa, *de quem* queremos protegê-la, *para que*, *a que custo* social e econômico e *até que ponto*, decisões – essas sim – perenes, e que determinarão políticas e rumos.

Curioso é notar, conforme lembra PAESANI (2001), que não há governos autoritários ou regimes totalitaristas fundamentando as ameaças a que o trabalho se refere. Ao contrário, elas decorrem do próprio progresso livre, que, por sua vez, somente foi permitido pela liberdade de criação e de pensamento e do incentivo à livre iniciativa, características típicas dos regimes democráticos, liberais.

Isto tomado no âmbito das relações internacionais, e posto que nem todas as nações terão a oportunidade de debate com a mesma profundidade, ou acesso, em igualdade de condições, aos mecanismos e às tecnologias de controle, é fácil constatar que este domínio da segurança da informação fatalmente há de se constituir em instrumento de imensa vantagem política e econômica, cabendo certamente ao direito, papel fundamental no sentido de disciplinar e estabelecer limites a esta desmedida vantagem, de impedir desequilíbrios flagrantes e injustos e de dar contornos menos sombrios ao lema que acompanha a sociedade da informação, desde o seu nascedouro.

Who controls the past,

controls the future.

Who controls the present,

controls the past.

George Orwell, 1984.

Bibliografia

ABREU, Dmitri. *Melhores Práticas para Classificar as Informações*. Módulo e-Security Magazine. São Paulo. ago. 2001.

ALMEIDA, Gilberto Martins de. *As Empresas podem "grampear" o e-mail de seus funcionários?* Módulo e-Security News. Rio de Janeiro. 1999.

- ALMEIDA, Gilberto Martins de. *Qual a responsabilidade jurídica dos websites*. Módulo e-Security News. mar. 2000.
- BAKER & MCKENZIE. Escritório de advocacia europeu especializado em Direito de Tecnologia da Informação Propriedade Intelectual e Comércio Eletrônico. <<http://www.bakermckenzie.com>>.
- BITTAR, Carlos Alberto, BITTAR, Carlos Alberto Filho. *Tutela dos Direitos da personalidade e dos Direito Autorais nas Atividades Empresariais*; São Paulo: Revista dos Tribunais; 1993.
- BRASIL EM TEMPO REAL. *Senado Aprova Normas de Acesso à Internet*. Brasília. ago. 2001. Disponível em: <<http://emtemporeal.com.br>>.
- BORAN, Sean. *The IT Security Cookbook Information classification*. EUA. dez. 1996.
- BORKING, John J. RABB; [Charles D.](#) *Laws PETs and Other Technologies for Privacy Protection*. Journal of Law Information Technology. London, v.8, n.1, fev. de 2001.
- BOTONI, Fernanda. *Sos Backup*. Infoexame, Rio de Janeiro. set. 2001.
- CAMPOS, Eduardo. *Investimentos em Segurança da Informação. Como Justificar?* Jornal da Segurança. São Paulo. mar. 1998.
- CÓDIGO CIVIL. 14ª edição. Saraiva. São Paulo. 1999.
- CÓDIGO DE DEFESA DO CONSUMIDOR COMENTADO PELOS AUTORES DO ANTEPROJETO. 4ª Edição. Forense Universitária. São Paulo. 1995.
- CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.. 20ª edição. Saraiva. São Paulo. 1998.
- COSTA, José Carlos Netto. *Direito Autoral no Brasil*. FTD. São Paulo. 1998.
- COVALLA, Tom. Safe and Sound. *Management Directions*. EUA, set. 2001. n.21. p. 5.
- GUEIROS, Nehemias Júnior. *Direito Autoral No Show Business. A Música*. 2ª edição. Gryphus. Rio de Janeiro. 2000.
- IDC – Empresa de análise mercadológica e estratégica em Tecnologia da Informação. Disponível em: <<http://www.idc.com>>.
- INFOEXAME. Portal da Revista Infoexame <www.infoexame.com.br>
- INFORMATION WEEK, *PriceWaterhouseCoopers & Global Information Security Survey*. Information Week. EUA, 2001.
- INTERNET SECURITY SYSTEMS. *Recognizing the Need for Enterprise Security Management – An Introduction to SAFEsuite® Decisions*. EUA. 2000.
- LESSIG, Lawrence. *The Architecture of Privacy. Conferência na Taiwan Net*. Taipei. mar. 1998.

LOBO, Paulo. *Direito e Globalização*. FACTUM, Informativo Jurídico. Campina Grande, set.1998. p.02

LONGDIN, Louise. *Liability for Defects in Bespoke Software: Are Lawyers and Information Scientists Speaking the same Language?*. Journal of Law Information Technology, London, v. 8. n.1. 2001.

MARTINS, Fran. *Curso de Direito Comercial*. Forense. Rio de Janeiro. 1999.

MCBRIDE, BAKER & COLES. Escritório de advocacia americano especializado em Direito de Tecnologia da Informação e Comércio Eletrônico. EUA.
<<http://www.mbc.com>>.

MILITELLO, Kátia. *Os perigos da Internet*. Infoexame, São Paulo, 2001. Disponível em: <<http://www.infoexame.com.br>>

MÓDULO SECURITY SYSTEMS. Empresa especializada em Segurança da Informação. Editora do Informativo *e-Security News* e da Revista Eletrônica *e-Security Magazine*. <www.modulo.com.br>.

NETWORK ASSOCIATES INC. *An Introduction to Cryptography*.EUA.1999.

PAESANI, Lilian Minardi. *Direito e Internet; Liberdade de Informação, Privacidade e Responsabilidade Civil*. Atlas. São Paulo. 2000.

PERDONCINI, Priscila. *Arquivos Públicos na Internet Ameaçam Privacidade*. InfoGuerra. ago. 2001. Disponível em: <<http://www.infoguerra.com.br>>.

PEREIRA, Cristiane Santos. *Implementação de Políticas e Procedimentos de Segurança em Ambientes Internet*. Universidade de Brasília. 2000.

PEREIRA, Raphael. *Como os registros de log podem ajudar nos processo de investigação?* Módulo e-Security Magazine. set. 2001.

REVISTA DA CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. *Com um pé no Futuro*. Brasília n.311. fev. 1999.

SCHLARMAN, Steven; *Enterprise Security Architecture System*. PriceWaterhousCoopers. jul. 2000.

SCHOUERI, Luís Eduardo. *Internet. O Direito na Era Virtual*. 2ª edição. Forense. Rio de Janeiro. 2001.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 15.edição. Malheiros Editora. São Paulo. 1998.

SOARES, José Carlos Tinoco. *Lei de Patentes, Marcas e Direitos Conexos*. Revista dos Tribunais. São Paulo. 1997.

STOCCO, Rui; FIGUEIRA, Joel Dias Júnior. *Responsabilidade Civil do Fabricante e Intermediários por Defeitos de Equipamentos e Programas de Informática*. Revista dos Tribunais. São Paulo. 2000.

STOCCO, Rui. *Responsabilidade Civil e sua Interpretação Jurisprudencial*. Revista dos Tribunais. São Paulo. 2000.

TERZIAN, Françoise. *EUA vão perder US\$ 10 bilhões Sistemas. B2B serão os mais afetados*, TCInet, 2001. Disponível em: <<http://www.tcinet.com.br>>

TCINET. Portal de serviços e notícias referentes à Tecnologia da Informação <<http://www.tcinet.com.br>>.

TEIXEIRA, Ivo Gico Júnior. *O Arquivo Eletrônico como Meio de Prova*. Revista IOB. Rio de Janeiro. 2000.

TIMMONS, Cindi, TIMMONS, Aaron. *The Right to Be Left Alone: An Examination of the Right of Privacy*. Greenhill School Dallas, Texas. 1998. Disponível em: <<http://www.nfhs.org/>>

TOLEDO, Antonio Luiz de, Siqueira, Luiz Eduardo Alves et al. *Consolidação das Leis do Trabalho*. 27 edição. Saraiva. São Paulo. 2000.

VENOSA, Sílvio de Salvo. *Direito Civil*. Direitos Reais. Editora Atlas S.A. São Paulo. 2001. v.04.

ZAKABI, Rosana. *HACKERS - Os nossos sãoos campeões*. Revista VEJA. São Paulo. set. de 2001.

*Cláudio de Lucena Neto - Consultor de Tecnologia da Informação, Estudante do 5º Ano de Direito, Monitor da Disciplina Informática Jurídica - Universidade Estadual da Paraíba, Campina Grande - Paraíba - Brasil - killa@zaz.com.br , fone: + 55 XX 83 9312 7454 - março de 2002.