UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de Marília

OFICINA UNIVERSITÁRIA
CULTURA ACADÊMICA
Editora

Reputação corporativa no ciberespaço:

implicações no direito autoral, propriedade intelectual, gestão da privacidade e acesso a conteúdos

Miguel Maurício Isoni
Silvana Aparecida Borsetti Gregório Vidotti

Como citar: ISONI, Miguel Maurício; VIDOTTI, Silvana Aparecida Borsetti Gregório. Reputação corporativa no ciberespaço: implicações no direito autoral, propriedade intelectual, gestão da privacidade e acesso a conteúdos. *In*: GUIMARÃES, José Augusto Chaves; FERNÁNDEZ-MOLINA, Juan Carlos. (org.). **Aspectos jurídicos e éticos da informação digital**. Marília: Fundepe; São Paulo: Cultura Acadêmica, 2008. p.95-112. DOI: https://doi.org/10.36311/2008.978-85-98605-52-4.p95-112.

Reputação corporativa no ciberespaço: implicações no direito autoral, propriedade intelectual, gestão da privacidade e acesso a conteúdos

Miguel Maurício Isomi
Silvana A. B. G. Vidotti

1 Introdução

> A tecnologia anda mais rápido que a sociedade. Primeiro vem a ferramenta, depois vem a cultura e a ética de uso da mesma de modo a manter protegidos os direitos e garantias fundamentais. O Direito vem atrás de tudo, pois só quando são definidos os valores éticos a serem protegidos é que pode ser feita uma norma, que irá traduzir e impor isto dentro de uma linguagem legislativa para determinar o padrão de comportamento social e juridicamente adequado. (PECK, 2003).

A construção de uma reputação institucional, seja ela no ciberespaço ou não, é feita de ações concretas ativas e pró-ativas dos valores éticos explícitos e implícitos, acordados ou aceitos de maneira tácita ou não, na convivência social, política, administrativa e operacional, que ocorre em cenários de ligações e conexões, interesses e necessidades.

Reputação deve ser gerenciada com critérios aceitos de sobrevivência, estrategicamente competitiva e transparente, e que ofereça credibilidade, tranqüilidade e reciprocidade no meio em que atua permanentemente.

Não obstante a reputação corporativa analisaremos, neste texto, as implicações no direito autoral, na propriedade industrial, na privacidade e na transparência na obtenção de conteúdos e no acesso às informações – é o que procuraremos apresentar no âmbito deste capítulo.

https://doi.org/10.36311/2008.978-85-98605-52-4.p95-112

A análise consiste em considerar esta ocorrência ética como sendo a expressão de uma "territorialidade corporativa" cuja especificidade aqui será tratada como virtual, isto é, presente no ciberespaço. Camilo (2005), analisando a importância do "espaço-informação" na expressão de uma 'territorialidade corporativa', descreve que o espaço virtual ocorre numa realidade cuja ponderação é incontornável quando se analisam os *sites* corporativos[1] ou institucionais das organizações presentes na Internet.

2 A questão do direito autoral e da propriedade intelectual

Um dos debates que vem ocorrendo há algum tempo envolve grandes discussões. Trata-se da proteção à criação intelectual de recursos de informação. Existe um ponto de equilíbrio entre a privacidade digital e o combate à quebra de direito autoral, em relação à proteção do conteúdo proprietário ou do conteúdo livre. Na verdade, em meio à questão do livre acesso à informação está o direito autoral.

Alternativas institucionais, como a Creative Commons (2006) criada nos EUA em 2001, sendo um de seus mentores o Professor Ph.D. de Direito da Stanford University, Lawrence Lessig, que propõem estabelecer termos legais entre todos os direitos reservados, dos contratos de direitos autorais tradicionais e os de domínio público. O uso das licenças criadas pela Creative Commons pode se aplicar a qualquer produção: música, literatura, cinema, fotografia, obras multimídias etc.

Lawrence Lessig estuda, também, aspectos legais das tecnologias de informação e comunicação (TIC) particularmente aplicados à Internet, e nos últimos seis anos publicou livros importantes sobre o tema. No livro - *Code and Other Laws of Cyberspace* -, Lessig (2000) argumenta que a liberdade de expressão e a privacidade estão sendo seriamente ameaçadas por interesses comerciais e defende que são perigosas as idéias de que o ciberespaço é um lugar livre, e de que os governos não devem interferir nele.

O *software* (código), que estrutura o ciberespaço tal como ele é forma um tipo de regulamentação das formas de comunicação, por exemplo, entre o

1 Por sites corporativos ou institucionais concebemos um conjunto estruturado de informações de natureza corporativa (segundo uma determinada estrutura e organização) que têm por objeto uma organização e por objetivo a sua identificação (publicitação, divulgação) e, simultaneamente, a legitimação dos valores (reais ou imaginários) que determinam a sua singularidade, a sua identidade (CAMILO, 2005, p. 2).

emissor (origem) e o receptor (destino) de uma mensagem tipo *e-mail*. Esclareça-se que o código de um *e-mail* pode apontar a procedência e o fluxo da informação, mas o conteúdo pode expressar valores diversos, diferentes ou iguais aos existentes na realidade.

A equação de Lessig é simples: "quem controlar o código terá maior poder sobre a Internet" (MAISONNAVE; LOUZANO, 2000). Assim, o código é um protocolo significante, e cabe aos advogados, cientistas da infomação, políticos e principalmente aos cidadãos decidir quais os valores que esse código deve incorporar.

Quanto às questões da propriedade intelectual, Richard Stallman (2000, p. 1), em seu artigo sobre o Projeto GNU – que retrata sua experiência no desenvolvimento de um sistema operacional baseado como *software* livre - descreve que

> Quando os que publicam software falam de "fazer valer" os seus "direitos" ou de "deter a pirataria", o que "dizem", de fato, é secundário. A verdadeira mensagem contida nessas declarações está nos pressupostos não declarados que eles consideram garantidos; o público deve aceitá-los acriticamente [...] Um pressuposto é que as companhias de software têm um direito natural inquestionável à propriedade dos programas e, assim, de dispor de poder sobre todos os seus usuários - (Nada poderíamos objetar, independentemente do dano que causasse ao público, se isso fosse um direito natural). O interessante é que a Constituição dos EUA e a tradição legal rejeitam este ponto de vista; o copyright não é um direito natural, mas um monopólio artificial imposto pelo governo que limita o direito natural de copiar do usuário.

Em seu mais recente livro - *Free culture: how big media uses technology and the law to lock down creativity* - Lessig (2004) descreve a forma de controle exercida, atualmente, pelas empresas de comunicação sobre a propriedade intelectual. O autor destaca que as forças que regulam a propriedade intelectual deveriam possibilitar um equilíbrio entre controle e liberdade, pois, as leis estabelecidas hoje em dia limitam o uso e elevam o custo da produção intelectual, numa época em que a tecnologia possibilitaria reduzi-lo. Assim, ele defende que as leis deveriam acompanhar os avanços da tecnologia.

Outra questão a ser tratada é o ato de *criação* na sociedade digital, pois a mesma requer maior proteção do que estamos acostumados. A criação intelectual merece várias formas de proteção através de uma série de ferramentas legais disponí-

veis, que vão desde o simples registro da marca ou domínio, até uma patente. As garantias dos direitos autorais ou intelectuais sobre uma determinada obra, competem ao autor buscar. Por exemplo, através do Registro de Desenho Industrial e Patentes e Certificado de Adição de Invenção, relativos a produtos e a invenções. Além disso, há ainda outras formas de proteção dos direitos autorais de conteúdos, como os textos de obras literárias, artísticas ou científicas, composições musicais, obras audiovisuais, fotográficas ou de desenho e *layouts*. O Instituto Nacional da Propriedade Industrial (2006), no caso brasileiro, apresenta uma série de normas legais que regulam e protegem marcas, patentes e propriedades intelectuais.

Diante desse cenário, a Internet exige o enfretamento aos novos modelos de negócio e de exploração e remuneração do direito autoral. É possível proteger digitalmente na Internet "a obra" com códigos de programação, rastreando, por exemplo, uma foto não autorizada e exigir a sua retirada do ambiente digital que a disponibilizou com devida indenização.

Alegando o direito de *fair use* - que garante o uso de uma obra desde que não seja para fins comerciais, ou seja, de caráter informativo, explicativo, comparativo etc. - podemos usá-la citando o autor e sua obra, que no caso da *Worl Wide Web*, podemos, de forma hipertextual, colocar um link para a obra em formato digital. Desse maneira, cria-se uma rede de divulgação e visibilidade amarrada na obra verdadeira, que deve ser autorizada e creditada para tanto. Ao invés de ir contra a disseminação da imagem, se poderia estabelecer uma parceira em uma rede de cooperação para uso legal dessa imagem.

Como hoje em dia, texto, música e vídeo são criados e usados em formato digital, o que permite cópias perfeitas com pouco custo, usando computadores pessoais, há necessidade de atualização da legislação pertinente (LESSIG, 2000).

3 Privacidade, acesso e proteção legal para conteúdos digitais

Um dos aspectos preocupantes no ciberespaço é o papel duplo do receptor e do emissor na troca de mensagens, onde toda pessoa com acesso à Internet não está apenas sujeita ao recebimento de informação, mas pode também gerá-la. E esse processo é uma construção possível no ciberespaço, pois encontra-

mos nele interatividade extensiva, conectividade e cenário propício para a efetiva construção de comunidades virtuais que opinam, sugerem e questionam.

Na verdade, pelo modo como o ciberespaço se apresenta atualmente, torna-se muito difícil para qualquer governo controlar o que quer que seja nesse ambiente virtual, devido a dificuldade de saber quem vem de onde, e o que se está fazendo. Mas as novas tecnologias de informação e comunicação estão sendo integradas com o ciberespaço, e poderão tornar mais fácil saber de onde alguém está acessando e em alguns casos, o que ele ou ela está fazendo. Talvez a maior preocupação dos usuários dos meios eletrônicos em relação à privacidade seja a sensação de estar sendo observado.

Phil Agre (1997), em seu trabalho *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, ressalta que dados coletados podem ser usados de diversas formas. Baseados nas considerações do autor, os indivíduos deveriam se preocupar com o uso que pode ser feito de seus dados pessoais. Esse alerta de Agre é um dos principais motivadores para a criação de políticas de privacidade. Phil Agre tem publicado diversos artigos onde defende que privacidade e segurança não são antagônicos. Medidas como o *US Patriot Act*[2] *(United States, 2001)* são paliativos que servem não para melhorar a segurança, e sim para dar a falsa sensação desta. O ideal é termos uma sociedade estruturada, com princípios de privacidade sólidos, que seja capaz de se manter segura e com o controle sobre seus dados pessoais.

Na interatividade com algumas instituições na Internet, por exemplo, seremos francamente interceptados e até mesmo bloqueados e, assim, só teremos acesso a conteúdos, ou só concluiremos nossas consultas ou demandas, se tivermos um cadastro de identificação. Portanto, os propósitos para o armazenamento de dados pessoais devem ser indicados no momento da coleta de dados para aqueles que estarão prestando as informações, devendo ser exatos, completos e permanecer atualizados. Dados pessoais não podem ser divulgados, comunicados ou utilizados com finalidades outras das que foram especificadas, salvo com

---

2 Promulgada pelo Presidente Bush depois dos atentados terroristas de 11 de Setembro de 2001, a US Patriot Act deu ao governo federal americano mais poderes para efetuar registros de documentos privados e interferir nas comunicações, através de escutas, com intuito de levantar também questões sobre lavagem de dinheiro, patrulhas fronteiriças, imigração, e procedimentos de investigação, julgamento e condenação criminal relativos a indivíduos ou organizações suspeitas de terrorismo.

o consentimento do sujeito dos dados, ou por força de lei. Cópias de segurança regulares devem proteger os dados pessoais contra riscos tais como perda, ou acesso, destruição, uso, modificação ou divulgação desautorizada desses dados.

As Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, publicadas pela Organização para a Cooperação e Desenvolvimento Econômicos – OCDE (1980), representam uma orientação para coleta e gerenciamento de informação pessoal. Os princípios abrangem os meios utilizados para o processamento de dados referentes aos indivíduos (do computador local à rede), todos os tipos de dados pessoais e categorias consideradas como padrões mínimos para a proteção da privacidade e da liberdade individual.

A *Comissão Européia*, órgão da União Européia – UE – estabeleceu, através da Diretiva sobre Proteção de Dados - 95/46/EC - (COMUNIDADE EUROPÉIA, 1995), que dados pessoais, contidos em bases de dados de entidades privadas ou órgãos situados em países do bloco europeu, só podem ser processados e transferidos para um país não-integrante da comunidade européia se este oferecer um nível adequado de proteção. A Comissão, por força dessa exigência, indica quais países adotam o nível de proteção adequado. Para os que não possuem sistema de nível adequado na proteção de dados pessoais, a comissão elabora modelos de cláusulas contratuais a serem utilizadas por empresas e controladores de bancos de dados europeus que transfiram informações para outros países.

Reinaldo Filho (2003), presidente do Instituto Brasileiro da Política e do Direito da Informática (IBDI), relata que em 30 de junho de 2003 a *Comissão Européia* reconheceu que a Argentina estaria fornecendo um adequado nível de proteção aos dados pessoais de seus cidadãos. A decisão tem o efeito de permitir que dados pessoais contidos em bases de dados de empresas e órgãos públicos europeus sejam transferidos para entidades sediadas naquele país, sem necessidade de outras garantias, conforme previsto na Diretiva 95/46/EC - (COMUNIDADE EUROPÉIA, 1995) sobre proteção de dados. Decisões semelhantes têm sido adotadas em relação a outros países, reconhecendo a adequação de seus regimes jurídicos.

Conforme Peck (2004a), no Brasil as questões de proteção e regulamentação nas transações realizadas de modo não-presencial, via tecnologia de informação e comunicação, estão relativamente protegidas pela Constituição Federal de 1988 (artigo 5º), pelo Código de Defesa do Consumidor (artigo 43), pelo novo Código Civil (artigos 21, 89, 427, 428, 434, 966 e 1195), pelo Código Penal (artigos 171, 298, 299, 307) e pela Lei 9610/98.

Se tivéssemos adotado políticas de proteção a dados pessoais mais consistentes e abrangentes poderíamos já ter obtido parecer favorável da Comissão Européia, pois o nosso problema não é a ausência de leis. Temos uma lei padrão de proteção de dados, contendo princípios genéricos e normas programáticas dirigidas aos governos em suas diversas esferas, mas temos um nível de normatização ainda inconsistente.

A Constituição brasileira consagra a proteção da intimidade e da vida privada e a inviolabilidade do domicílio entre os direitos e garantias individuais. Embora não dispondo de um arcabouço legal sistematizado e concatenado, algumas de nossas leis disciplinam certos aspectos da proteção das informações pessoais. O mais significativo, no entanto, é que não há uma cultura brasileira para proteção de dados pessoais, e os debates políticos não a tratam como questão relevante para o desenvolvimento da sociedade. Desde os anos 70, praticamente todos os países que hoje integram a União Européia editaram leis de princípios de proteção a dados pessoais, além de criarem comissões e autoridades supervisoras para garantir efetividade a essas leis.

Talvez a decisão em relação à Argentina sirva como incentivo para que autoridades brasileiras passem a tratar a questão da proteção da privacidade com mais seriedade. A própria Comissão Européia espera que sua decisão sirva de estímulo aos países da nossa região, para que dimensionemos os direitos individuais relacionados à proteção de dados pessoais.

4 Transparência das informações públicas e privadas

A garantia de que os cidadãos tenham acesso livre e transparente das informações coletadas, produzidas e armazenadas pelos diversos órgãos de governo, são os principais fundamentos da transparência dos atos governamentais, ficando assim evidente o papel do estado como gestor das informações públicas e a crescente importância da questão informacional na sociedade contemporânea para consolidação do processo de participação democrática.

É preciso frisar que, especialmente num país de desigualdades sociais graves, todas as informações que contribuem para tornar a administração mais transparente, ou que fornecem detalhes sobre direitos, deveres e benefícios, devem ser garantidas e gratuitas (FREY et al, 2002, p.380).

O grande problema neste cenário das novas tecnologias da informação e comunicação é a exclusão digital, que torna cada vez maior a distância entre os integrados ao mundo digital e os que estão dele excluídos. Cabe, portanto, ao estado estimular o uso das novas tecnologias da informação e comunicação para fins de emancipação social.

Mesmo nos países mais avançados, as classes mais pobres terão dificuldades de competir nos mercados da informação, pelo menos enquanto não houver incentivos e esforços específicos para garantir os recursos de acesso e para transmitir o conhecimento e a compreensão necessários (LOADER, 1998, p.9).

Além disso, tornou-se mais evidente que os órgãos públicos não podem mais restringir e reagir de forma passiva, e sim pró-ativa, às demandas de informação, pois precisam disponibilizá-la como uma função essencial de gestão e transparência do serviço público em relação, por exemplo, as receitas e despesas que validam suas políticas sociais. Trata-se de uma prática transparente e responsável de planejamento, que por sua vez é precondição para a sociedade civil e os cidadãos poderem exercer sua função de controle social, pois segundo Frey et al. (2002, p.381), "é preciso que os administradores reconheçam que as informações lhe são apenas confiadas pela sociedade e que eles não são os donos das informações públicas".

Uma nova compreensão de gestão pública dos fluxos de informações, que permita aos cidadãos chegar às informações requisitadas, se fez necessária tanto pela vertente gerencial da chamada nova administração pública, como pela vertente democratizante das chamadas administrações democráticas e populares. Contudo, é preciso salientar a necessidade de uma legislação clara referente ao acesso à informação e ao fluxo de serviços públicos, onde os instrumentos legais de garantia do direito à informação vão desde artigos constitucionais até leis ordinárias e decretos em diferentes esferas de poder. Assim, onde existe legislação – em conformidade, por exemplo, com os requisitos da *Freedom of Information Act* - (UNITED STATES, 1996) e da FOIA - Reference Guide (UNITED STATES, 2005), revisada em abril de 2005, vigentes nos EUA - podemos destacar um razoável direito do cidadão ao livre acesso às informações públicas, bem como à utilização de serviços públicos disponíveis na Internet.

O professor Marco Cepik (2000, p. 46) relata que a legislação canadense é uma das mais abrangentes nos aspectos de garantia de requisição e acesso de informações públicas, pois incluem quaisquer informações constantes em pastas de arquivos físicos, cartas, memorandos, relatórios, plantas arquitetônicas, fotografias, filmes, microfilmes, planos, desenhos, diagramas, mapas, sons

gravados, vídeos, arquivos de computador ou quaisquer outros dados digitais, com exceção aos segredos governamentais regulamentados pela lei.

A essência do direito de autodeterminação informativa consiste no direito de controle sobre os dados pessoais por parte de seu titular. Este controle se manifesta no poder de aceder, retificar e anular os dados pessoais armazenados em bancos de dados eletrônicos. Também exerce uma importante função preventiva o consentimento do titular dos dados pessoais para que estes sejam objetos de consulta, retificação, cessão, etc. O crescente uso das novas tecnologias exige que o Direito se adapte às mudanças produzidas nas relações sócio-jurídicas. O campo da proteção de dados pessoais não foge a esta regra, tendo em vista que a informática e a telemática apresentam instrumentos que possuem grande poder de armazenamento, administração, classificação e transmissão de dados. O reconhecimento, máxime a nível constitucional, do direito à intimidade frente ao uso da informática contribui para esta adaptação da Ciência Jurídica, sendo, em nosso entender, o caminho a ser seguido pelos países que pretendem manter um equilíbrio entre o surgimento de novas tecnologias e a ordem jurídica, respeitando, assim, os direitos fundamentais dos cidadãos (PEREIRA, 2001).

O *hábeas data*, no âmbito constitucional, é um dos princípios do direito à informação garantido em muitos países como principal instrumento jurídico para obrigar legalmente os responsáveis a cederem informações requisitadas. O exemplo estaria em países como Brasil, Argentina, Peru, Bulgária, Hungria e República Tcheca, onde as informações pessoais armazenadas nos arquivos dos serviços de segurança dos antigos regimes autoritários passaram a ser disponibilizadas por requisição de seus interessados. Destacando assim a necessidade de arbitragem legal por parte de governo, tribunais ou até mesmo outras autoridades constituídas (CEPIK, 2000, p. 47)

> Destacam-se como formatos institucionais positivos experiências tais como a do Office of Information Commissioner, da Irlanda, da Human Rights Commission, da África do Sul, da Commission d'Accèss aux Documents Administratifs, da França, além do aparentemente bem projetado National Council of freedon of Information, da Índia (FREY et al., 2002, p.385).

No Brasil, o sistema normativo que assegura e regula o direito à informação encontra-se em primeiro lugar consagrado na Constituição Federal (BRASIL, 1988), por meio dos incisos XIV e XXXIII do artigo 5º, a saber:

XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.

> XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Há, ainda, a Lei 8.159/91 (BRASIL, 1991) brasileira, que estabelece as diretrizes da política nacional de arquivos públicos e privados, assegurando o direito de acesso pleno a quaisquer documentos públicos, com exceção daqueles de caráter sigiloso "*cuja divulgação ponha em risco a segurança da sociedade e do Estado*" ou exponha indevidamente a intimidade, a vida privada ou a imagem das pessoas (art. 23, caput e § 1º).

Também se pode destacar o Código de Defesa do Consumidor - Lei n º 8.078/90 (BRASIL, 1990) - ao impor a política nacional das relações de consumo pautada pelos princípios de transparência e harmonia. Esta lei determina aos fabricantes e fornecedores o dever de informar o consumidor seja os aspectos de validade, seja a sua composição, restrições e até mesmo especificações técnicas, se for o caso.

O desconhecimento acerca do conteúdo dessas legislações, muito pouco divulgadas e menos ainda compreendidas, cuja aplicação encontra resistências e dificuldades, demonstra que nós, brasileiros, temos um longo caminho pela frente se quisermos garantir aos cidadãos o direito pleno a informações públicas. No Brasil, ainda é preciso enfrentar o enorme desafio político, legal e administrativo de democratizar o acesso às informações para que se alcance uma cidadania mais plena.

É preciso fixar prazos para o atendimento de demandas informacionais, definir prioridades para tornar os diferentes conjuntos de informação acessáveis alocando recursos tecnológicos, financeiros e humanos em quantidade e qualidade adequadas àquelas prioridades, responsabilizando algum órgão, agência, sistema ou pessoas pela supervisão da implementação dos instrumentos legais (FREY et al., 2002, p.389).

A construção de um modelo que privilegie uma relação com a sociedade baseada na circulação de informações, na co-responsabilização e no controle social das ações do governo exige uma série de mudanças nas práticas de gestão pública brasileira. É necessária uma maior participação popular em todo processo de gestão, com ações que ampliem o acesso aos processos de fluxo informacional, fornecendo à sociedade civil garantias de pleno atendimento às demandas públicas, abrindo assim as "caixas pretas" de informações, por exemplo, sobre políticas públicas oriundas do planejamento orçamentário através da tecnologia de informação como facilitadora do acesso às pressões na elaboração e no controle rotineiro de suas execuções financeiras. Um bom exemplo vem da Organização Não-Governamental - ONG *Contas-Abertas* (2006) que disponibiliza na Internet Relatórios de Dispêndios da União (incluindo os Três Poderes, exceto Empresas Estatais).

5 Reputação e a imagem corporativa no universo digital

A sociedade digital não é apenas uma evolução tecnológica da era pós-industrial. Representa a transformação da riqueza física, baseada na terra e nos bens de produção, em ativos intangíveis. Nesse sentido, ganharam significado patrimonial não só a "marca" individual, institucional, ou de produtos e serviços, mas também os domínios, os bancos de dados, os *softwares*, as tecnologias, as licenças, entre outros.

> A sociedade do conhecimento está baseada num modelo de riqueza gerado pelo capital humano, que se transforma em ativos intangíveis. Por isso, todo e-business deve prever a proteção e o adequado tratamento patrimonial destes ativos, até para fins de valuation da empresa e de tributação (PECK, 2004b).

Para haver uma base de relacionamento transparente entre a instituição e seus *stakeholders*[3] no mundo digital, torna-se necessário adotar um conceito de suporte à informação, como um canal de atendimento que disponibilize

3 Termo em Inglês muito utilizado na Administração para designar pessoas ou organizações que são afetadas pelos processos e ações de uma instituição privada ou pública que, de alguma maneira, mantém relações direta ou indireta entre si.

as "perguntas mais freqüentes" com suas devidas respostas. Ou mesmo, disponibilizar o acesso a informações de interesse específico, tais como: listas de estoques e preços, relatórios financeiros, comunicados institucionais etc.

Em um cenário conectado de relações interativas e *on-line*, os riscos e a imprevisibilidade são cada vez maiores, tornando necessária a adoção de metodologias preventivas e corretivas para a proteção da reputação e da imagem no universo digital. Muita coisa precisa ser revista e adequada às novas questões de proteção digital nos ambientes de interação e comunicação, cada vez mais hipermídia e interativos.

A empresa precisa transmitir confiança para que o cliente deposite seus dados junto a ela. Ter o dado não significa poder usá-lo ou compartilhá-lo. É preciso dar tratamento legal para poder usar dados de clientes, de fornecedores e de funcionários. Não adianta formar um valioso banco de dados se a empresa não definir o uso ético deles, baseado em políticas bem definidas. A instituição, seja ela privada ou pública, será legalmente responsável por suas ações ou omissões, por sua negligência no uso das novas tecnologias digitais.

No mundo dos negócios, as organizações precisam estar cada vez mais preparadas para fazer gestão e proteção dos seus ativos digitais intangíveis, pois dentro dos preceitos reputacionais é sabido que o melhor procedimento é investir na imagem e gerenciar a reputação, com vigilância contínua. Isso vai desde um *e-mail* até uma *home-page* com suas transações, trocas de arquivos, informações e consultas.

É importante reconhecer a importância da reputação em relações não presenciais, isto é, na interatividade existente no ciberespaço, onde privacidade e segurança da informação não são diferenciais, mas sim requisitos de confiabilidade.

A gestão estratégica de proteção à imagem e a gestão da reputação corporativa no ciberespaço necessitam de análise de como as tecnologias de informação e comunicação estão sendo utilizada com segurança e critérios éticos, evidenciando a necessidade de impor procedimentos, tais como:

I. Termos de privacidade, termos de adesão e regularização *online* e ações de cadastramento pela Internet dentro de padrões éticos e legais do Código de Defesa do Consumidor, com níveis de proteção oferecidas aos usuários ao preencher um cadastro na Internet;

II. Utilização de políticas eletrônicas corporativas no tocante à privacidade e à segurança de informação do tipo *trust marketing*[4], com garantias e controles éticos quanto ao uso e a privacidade dos dados armazenados, bem como a certeza de que as comunicações via *e-mail* não serão transformadas em *spam*[5];

III. Práticas e procedimentos claros e transparentes no uso de recursos eletrônicos entre empresa-cliente (nas compras *on-line*), empresa-fornecedor (na gestão da cadeia de suprimentos) ou empresa-governo (nos faturamentos, balanços contábeis e pagamentos de tributos); implementando controles de acesso com identificação, autenticação, privilégios e procedimentos de segurança;

IV. Planejamento de crise da imagem digital, a fim de preservar a reputação através de plano de contingência em caso de danos, invasões e uso incorreto das informações de bancos de dados, advindos dos relacionamentos externos e internos, com atitudes e defesa contra fraudadores e invasores;

V. Garantias de acordos, licenças, contratos, registros, patentes, direitos autorais, tecnologias proprietárias, métodos e processos próprios; em conformidade legal com os direitos de propriedade intelectual e autorais de *software* preservados;

VI. Obrigações e responsabilidades quanto a contratos eletrônicos, certificação digital, gestão de risco para fraudes eletrônicas, segurança de informação, contratos de prestação de serviços conhecidos como *Service Level Agreements*[6] - SLA - e contratos de terceirização de processos conhecidos como *Business Process Outsourcing*[7] - BPO.

---

4 Trust marketing, ou marketing de confiança, significa que a organização utiliza a comunicação eletrônica com uma estrutura adequada de segurança, privacidade, produtividade e legalidade, gerando credibilidade e confiança por parte do usuário-cliente em realizar negócios com a empresa.

5 Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês Unsolicited Commercial E-mail).

6 SLA é um documento formal, negociado entre as partes, na contratação de um serviço de TI ou Telecomunicações. O SLA é colocado geralmente como anexo do contrato e tem por objetivo especificar os requisitos mínimos aceitáveis para o serviço proposto.

7 Business Process Outsourcing, ou seja, delegação para terceiros da gestão de serviços cuja execução e operação técnica divergem da atividade principal da empresa, o que possibilita manter durante toda a execução do contrato o alto padrão de qualidade, know-how e constante atualização tecnológica ao projeto.

Avanços tecnológicos com a inversão da cadeia de produção, com um modelo de logística reversa, sem estoques, com terceirização de pessoas, processos e operações, criando interfaces de contatos multicanais e interativos, necessitam do mapeamento de responsabilidades nos espaços organizacionais.

Este novo cenário interativo e conectado em rede força as organizações a terem uma adequada Política Eletrônica Corporativa para evitar problemas dentro e fora da corporação, minimizando riscos de danos, interpretação errônea de suas políticas, e ações de captura, armazenamento, processamento e disseminação de informações, implementando controle e monitoramento de acesso a conteúdos de suas bases de dados.

O uso da tecnologia exige estabelecimento de limites éticos, de privacidade e segurança. Toda forma de controle, para ser legítima, deve estar devidamente estruturada, acordada entre as partes de modo transparente e inequívoco.

6 Considerações Finais

Para a gestão corporativa o que se deve proteger é a obra intelectual, a propriedade, os dados, as patentes, os processos, as pesquisas e as informações individuais e institucionais de caráter estratégico.

Não há dúvida da necessidade de implementar uma tecnologia para gestão de direitos autorais digitais que garanta o acesso aos conteúdos e que possa ser controlado e monitorado.

Levando-se em consideração que privacidade circunda todas as informações pessoais dos indivíduos, a instituição precisa manter o máximo de informações em sigilo, mesmo aquelas que não aparentam a possibilidade de causar danos aos proprietários.

Existe na Internet uma grande interseção entre o problema da privacidade e o da segurança, em que muitos questionam: como teremos melhor controle do ciberespaço, se não existe nenhum governo exercendo um efetivo controle? Deve o ciberespaço ser regulamentado? Como isto pode ser feito? É na verdade falsa a crença de que o ciberespaço, por suas características e por sua natureza, seja impossível de ser regulamentado. Outra falsa crença é a de que o ciberespaço é diferente do espaço real: é na verdade uma construção inteiramente artificial, construída pelo homem. O mundo é o mesmo, seja real ou virtual. O que ocorre é que as TICs diminuíram as distâncias e otimizaram o tempo para

a conectividade, o acesso, a interatividade e a absorção de conteúdos pessoais e institucionais. As leis e as normas estão postas e necessitam de aperfeiçoamento – que ao longo do tempo pontualmente implicam adaptações contextuais.

As TICs, ampliaram o escopo de atuação das organizações, e é necessário definir os novos padrões éticos e legais que devem reger essas relações de interatividade inerente ao ciberespaço, e torná-las visíveis para todos os atores sociais envolvidos, tais como fornecedores, clientes e governo.

> Uma revolução tecnológica, concentrada nas tecnologias da informação está remodelando a base material da sociedade [...] As redes interativas de computadores estão crescendo exponencialmente, criando novas formas e canais de comunicação [...] Nossas sociedades estão cada vez mais estruturadas em oposição bipolar entre a Rede e o Ser. (CASTELLS, 1999, p.21-23).

Essa transformação do ambiente institucional na era digital permitiu através dos *sites* o atendimento *on-line* e o acesso a conteúdos, como também transferências de funcionalidades administrativas e operacionais para o próprio cliente ou usuário do sistema. Trouxe uma série de mudanças comportamentais e de linguagem entre os seus *stakeholders*.

Para evitar riscos, é fundamental as instituições terem uma adequada Política Eletrônica Corporativa que regule a interatividade e o uso dos recursos disponíveis, por exemplo, em suas bases de dados, e seus processos de negócios gerados no contexto de sua Intranet[8] ou da Internet.

Estamos assistindo a mudança do centro dos negócios em que toda a cadeia produtiva passa a ser "orientada pelo consumidor" pela ponta, e onde a tecnologia viabiliza este processo de modo mais eficiente, com menor custo e maior alcance. Mas a maior barreira de receita não é o uso, mas sim a ética e a legalidade (PECK, 2004b).

Clareza, transparência, preocupação constante e vigilância permanente, pois os limites éticos são muitas vezes confusos, e o que é legal nem sempre é

8 Intranet é uma rede de computadores privativa que utiliza as mesmas tecnologias utilizadas na Internet, onde podemos encontrar vários tipos de serviços de rede comuns na Internet, como por exemplo, o e-mail, chat, grupo de notícias, sites, transferência de arquivos entre outros.

ético. Assim, a reputação de uma organização pode ser afetada caso se comprove falha ética nessas interpretações e situações.

O impacto da Internet na formação da reputação corporativa vem se acelerando com aumento da interatividade dos negócios na rede, em que bens intangíveis como direitos autorais, patentes e relacionamentos com os diversos públicos são ativos intangíveis valiosos que agregam valor para a empresa. A reputação é um desses bens intangíveis que geram resultados de negócio sobre questões tais como de responsabilidade social e ética empresarial, podendo influenciar positivamente no comportamento de clientes, fornecedores, investidores e funcionários.

Referências

AGRE, P. E. Beyond the mirror world: privacy and the representational practices of computing. In: AGRE, P. E.; ROTENBERG, M. (Ed.) **Technology and privacy:** the new landscape. Massachusestt: MIT Press, 1997. cap. 1. Disponível em: <http://polaris.gseis.ucla.edu/pagre/mirror.html>. Acesso em: 15 nov. 2005.

BRASIL. Constituição (1988). Brasilia: Congresso Nacional, 1988. Disponível em: <http://www.senado.gov.br/sf/legislacao/const/>. Acesso em: 12 out. 2005.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: <http://www.presidenciadarepublica.gov.br/CCIVIL_03/LEIS/L8078.htm>. Acesso em: 12 out. 2005.

BRASIL. Lei nº 8.159 de janeiro de 1991. **Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.** Disponível em: <http://www.abin.gov.br/abin/pnpc_legis/07_LEI8159.pdf>. Acesso em: 12 out. 2005.

CAMILO, E. J. M. Da importância do espaço-informação na expressão de uma territorialidade corporativa. Biblioteca On-line de Ciência da Comunicação – bocc, 2005. Disponível em: <http://www.bocc.ubi.pt/_listas/tematica.php?codtema=5> . Acesso em: 03 jan. 2006.

CASTELLS, M. **A sociedade em rede**: a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra. 1999. v. 1.

CEPIK, M. Direito à informação: situação legal e desafios. **IP**: Informática Pública, Belo Horizonte, v. 02, n. 02, p. 43-56, 2000. Disponível em: <http://www.

article19.org/work/regions/latin-america/FOI/pdf/ip0202cepik.pdf>. Acesso em: 03 jan. 2006.

COMUNIDADE EUROPÉIA. Directiva 95/46. Proteção dos dados pessoais. Síntese de Legislação. 1995. Disponível em: <http://europa.eu.int/scadplus/leg/pt/lvb/l14012.htm>. Acesso em: 02 fev. 2006.

CONTAS-ABERTAS. **Relatórios de dispêndios da União** (Três Poderes, exceto Empresas Estatais). Disponível em: <http://contasabertas.uol.com.br/Siafi2006/basica.asp>. Acesso em: 01 maio 2006.

CREATIVE COMMONS WORLDWIDE. Disponível em: <http://creativecommons.org/>. Acesso em: 02 fev. 2006.

FREY, K. et al. O acesso à informação. In: SPECK, B. W. (Org.). **Caminhos da transparência**. Campinas: Ed. da Unicamp. 2002.

INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL (INPI). **Legislação sobre propriedade intelectual e patente**. Disponível em: <http://www.inpi.gov.br/legislacao/legislacao.htm>. Acesso em: 10 fev. 2006.

LESSIG, L. **Code and other laws of cyberspace.** Los Angeles: Basic Books, 2000.

_____. **Free culture: how big media uses technology and the law to lock down culture and control creativity.** Londres: Penguin; 2004.

LOADER, B. D. Cyberspace divide: equality, agency and policy in the information society. In: LOADER, B. D. (Ed.). **Cyberspace divide**. Londres: Routledge, 1988.

MAISONNAVE, F.; LOUZANO, P. O futuro sombrio da Internet. **Folha de São Paulo**, São Paulo, 5 mar. 2000. Disponível em: <http://www.race.nuca.ie.ufrj.br/journal/m/m.htm>. Acesso em: 29 dez. 2005.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICOS (OCDE). **Diretrizes para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais.** 1980. Disponível em <http://www.oecd.org/dataoecd/16/50/15590254.pdf>. Acesso em: 10 ago. 2005.

PECK, P. Cidadania, ética e internet. **Boletim AMI**, dez. 2003. Disponível em: <http://www.patriciapeck.com.br/cconhecimento_exibir.asp?inteMateriaID=12>. Acesso em: 10 ago. 2005.

_____. Responsabilidade digital da empresa. **Jornal Gazeta Mercantil**, São Paulo, 6 maio 2004a. Caderno Legal & Jurisprudência.

_____. E-business sem reputação não é negócio. **Web Insider**, 1 jun. 2004b. Disponível em: <http://webinsider.uol.com.br/vernoticia.php/id/2131>. Acesso em: 8 ago. 2005. Coluna Negócios.

PEREIRA, M. C. O sistema de proteção de dados pessoais frente ao uso da informática e o papel do direito de autodeterminação informativa: especial referência ao ordenamento jurídico espanhol. **Jus Navegandi**, n. 51, 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2266>. Acesso em: 12 out. 2005.

REINALDO FILHO, D. Argentina possui um sistema adequado de proteção. **Revista Consultor Jurídico**, 10 jul. 2003. Disponível em: <http://conjur.estadao.com.br/static/text/4578,1>. Acesso em: 15 nov. 2005.

STALLMAN, R. O projeto GNU. **DataGramaZero**, n. 1, fev. 2000. Disponível em: <http://www.dgz.org.br/fev00/F_I_glos.htm>. Acesso em: 24 nov. 2005.

UNITED STATES. US Patriot Act. **Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism**. HR 3162 RDS. 107th Congress. 1st Session, In The Senate of The United States, Oct. 24, 2001. Disponível em: <http://www.epic.org/privacy/terrorism/hr3162.html>. Acesso em: 10 jan. 2006.

UNITED STATES. FOIA. **The freedom of information Act. 5 U.S.C. § 552, As amended by public Law No. 104-231, 110 Stat. 3048.** Disponível em: <http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm>. Acesso em: 25 out. 2005.

UNITED STATES. United States Department of Justice (DOJ). FOIA. Reference guide. Revised April 2005. Disponível em: <http://www.usdoj.gov/04foia/04_3.htm l>. Acesso em: 25 out. 2005.