Invasão de Privacidade

1. Uma Invasão da Intimidade

Rogério Tadeu Romano

Publicado em 07/2015. Elaborado em 07/2015.

O ARTIGO EXPÕE CASO CONCRETO EM QUE SE DISCUTE OS DIREITOS A INTIMIDADE E A PRIVACIDADE.

Uma invasão da intimidade

ROGÉRIO TADEU ROMANO

O Ministério Público Federal abriu inquérito para investigar o site "Tudo sobre Todos" por conta da divulgação e venda de dados pessoais na internet.

Além, do nome, o site disponibiliza o sexo, data de nascimento, a cidade, bairro em que a pessoa mora, e CEP onde a pessoa mora, e até um mapa mostrando o perímetro da sua casa. Em alguns casos, as informações estão desatualizadas, mas em outros, até os nomes dos vizinhos aparecem relacionados ao perfil que é buscado.

Em sendo assim ingressou o Parquet na Justiça Federal com uma ação cautelar com pedido de liminar para retirar do ar o site "tudosobretodos.se", que fornece ilegalmente informações particulares de cidadãos brasileiros, como endereço, CPF, nome de vizinhos, entre outros dados.

A ação tem como ré a empresa Top Documents LLC, sediada na República de Seicheles e que mantém o site. Entre os pedidos do MPF à Justiça, estão um requerimento para que empresas brasileiras de Internet não permitam o acesso ao endereço eletrônico, além de uma solicitação ao Reino da Suécia, via Ministério da Justiça, para que retire do ar o "tudosobretodos.se", tendo em vista que o site possui domínio naquele país europeu.

Tenha-se em mente o julgamento do CC 120.559, Relator Ministro Jorge Mussi, 3ª Seção do STJ, onde destacou-se que o fato de um delito ter sido cometido pela internet, ainda que em algumas páginas eletrônicas internacionais, não desloca a competência do caso para a Justiça Federal. Assim de acordo com esse entendimento, para ser fixada a competência da Justiça Federal é necessário que o crime ofenda bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional.

A inviolabilidade de dados, prevista no artigo 5º, XII, da Constituição, uma garantia constitucional, é correlata ao direito fundamental à privacidade, previsto no artigo 5º, X, da Constituição.

No modelo constitucional que temos, desde 1988, é razoável entender que há um direito do indivíduo de excluir do conhecimento de terceiros aquilo que a ele, só a ele, é pertinente e que diz respeito ao seu modo de ser exclusivo, seu *way of life*, no âmbito de sua vida privada.

Há um direito subjetivo fundamental visando a assegurar sua identidade, diante dos riscos proporcionados pela avassaladora pressão que contra ele é exercida pelo poder político e por terceiros de forma a resguardar sua intimidade.

Tutela o artigo 5º, inciso X, da Constituição o segredo e a liberdade da vida privada. Mas há separação entre a intimidade e outras manifestações da privacidade: vida privada, honra e imagem das pessoas.

Para René Ariel Dotti(Proteção da vida privada e liberdade de informação, São Paulo, 1980), a intimidade se caracteriza como "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais". Adriano de Cupis (Riservatezza e segretto, 1969, pág. 115) ensina que a intimidade é o modo de ser da pessoa que consiste na exclusão do conhecimento de outrem de quanto se refira à pessoa mesma.

Por sua vez, a garantia do sigilo de dados funciona como um complemento aos direitos à privacidade e à intimidade.

Bem disse o Professor Tércio Sampaio Ferraz que ninguém pode ser constrangido a informar sobre sua privacidade. Não estamos no âmbito puro e simples do público-político, onde o que se tem é a transparência; estamos no terreno da individualidade, onde há a privacidade que se rege pelo princípio da exclusividade.

Sabe-se que o direito à privacidade é o conjunto de informações acerca do individuo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem quando, onde e em que condições, sem isso poder ser legalmente sujeito, como disse Matos Pereira (Direito de informação, Lisboa, 1980, pág. 15).

Lembre-se que o nome é da pessoa, é patrimônio dela como pessoa natural. O nome integra os direitos da personalidade, direitos absolutos, especialmente protegidos por lei. Daí porque ninguém pode usurpar o nome da pessoa, que é privado e protegido como tal.

Não devemos esquecer que o artigo 5º, inciso XII, da Constituição, ao garantir a inviolabilidade do segredo, em suas diversas vertentes, consagrou o princípio da reserva de jurisdição em matéria de quebra de sigilo.

Essa a linha a adotar, na trilha da experiência constitucional italiana, para quem a quebra do sigilo pressupõe uma decisão Judicial motivada, caso a caso.

(Fonte: https://jus.com.br/artigos/41378/uma-invasao-da-intimidade, data de acesso 10/11/2018)

2. Há dano ao invadir a vida privada e a intimidade de uma pessoa ferindo a tutela constitucional?

DANIELA DE OLIVEIRA BRITO: Graduanda em direito pela Faculdade de Ciências Humanas e Sociais - AGES.

Quinta, 19 de Julho de 2012 05h15

» Daniela de Oliveira Brito

Encontra-se no art. 5º, inciso X da Constituição da Republica do Brasil de 1988 o direito à intimidade e a vida privada, direito esse que protege o bem viver em sociedade. Tal dispositivo constitucional, deve ser respeitado pelo Estado, como também pelos particulares sob pena de responsabilização por violação. Diante desses direitos, se faz necessário fazer menção à dignidade da pessoa humana como princípio fundamental do direito Constitucional que encontra-se inserido no art. 1º da Constituição da Republica.

Também no art. 5º., inciso XII da Constituição da República, encontra-se o complemento a essa garantia que torna inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo em caso de ordem judicial. Todo direto deve ser respeitado e a intimidade e vida privada é uma das garantias fundamentais mais importantes, pois refere-se à proteção da vida privada de cada ser humano, impedindo que sua intimidade seja invadida. Segundo George Sarmento, intimidade é:

> É o mais indevassável, o jardim secreto em que o indivíduo tem o poder de rechaçar as intromissões provenientes de terceiros. Nele estão guardados os segredos, as lembranças, os sonhos, os projetos de vida, os desejos, as fraquezas e todas as incursões introspectivas que a pessoa não deseja compartilhar com ninguém. Enfim, a intimidade é o espaço no qual a individualidade reina absoluta, resguardada da curiosidade alheia. É o que exige de mais profundo no interior de alguém. Sua verdadeira essência. É o direito público subjetivo de estar só com as emoções mais íntimas, longe dos olhares indiscretos, perscrutadores e curiosos. (SARMENTO, 2009, p. 2)

Diante do que foi dito, é percebido o quão é importante esse direito tutelado pela Constituição da Republica, e que é o modo de viver em sociedade que se exige que direitos como esse sejam protegidos, para assim poder manter seu lar longe da invasão alheia. Também George Sarmento descreve o conceito de vida privada:

> É, por sua vez, o espaço protegido pela confidencialidade. A vida privada está diretamente ligada ao círculo de relações intersubjetiva mantidas sob reserva ou em absoluto segredo. é o direito subjetivo público assegurado a cada ser humano de manter sob anonimato determinadas informações à sua vida particular. (SARMENTO, 2009, p. 3)

Portanto, é percebido que a violação a um dos direitos fundamentais, à privacidade estará sempre vinculada a uma ofensa à dignidade da pessoa humana, e assim, impondo limites ao poder estatal. Com isso, visa impedir que o poder público violasse a dignidade pessoal. Diante do exposto, afirmo que sim, que existe o dano ao invadir a privacidade e a intimidade de uma pessoa, pois causa constrangimento ao ver sua intimidade e vida privada invadida por outra pessoa que não faz parte de sua vida, pois terá sua intimidade exposta. Afirma a jurisprudência do STJ com relação à vida privada:

> Ingerência na vida privada, sem a devida autorização da pessoa, consiste em violar direito de privacidade. Cabe indenização por dano moral pelo uso indevido da imagem que, por se tratar de direito personalíssimo, garante ao indivíduo a prerrogativa de objetivar sua exposição, no que se refere à sua privacidade. (SARMENTO, 2009, p. 4)

Também defende Alexandre de Morais:

> Não existe qualquer dúvida de que a divulgação de fotos, imagens ou notícias apelativas, injuriosas, desnecessárias para a informação objetiva e de interesse público, que acarretem injustificado dano à dignidade humana autoriza a ocorrência de indenização por danos materiais e morais, além do respectivo direito à resposta. (MORAIS, 2008, p. 53)

Como foi demonstrado toda e qualquer invasão a intimidade e a vida privada causa danos, gerando assim o direito à indenização por ter violado um dos direitos fundamentais garantido na Constituição da Republica.

No âmbito familiar, os direitos à intimidade e a vida privada, devem ser interpretados de uma forma mais ampla, levando-se em conta as delicadas, sentimentais e importantes relações familiares, devendo também haver maior cuidado com qualquer intromissão externa.

Para que se caracterize um dano moral é necessário que a alma da pessoa seja atingida em sua dignidade, intimidade e vida privada e que não pode ser medido em valores, caso que a jurisprudência defende.

> TJDF - Apelação Cível APL 10792979200780700001 DF 0107929-79.2007...
>
> Data de Publicação: 11/05/2009
>
> Ementa: CIVIL E PROCESSUAL CIVIL. AÇÃO DE REPARAÇÃO POR DANOS MORAIS. INEXISTÊNCIA DE NEXO DE CAUSALIDADE E DE VIOLAÇÃO À HONRA, INTIMIDADE E VIDA PRIVADA DA AUTORA. 1 CONFIGURANDO O FATO LESIVO MERO ABORRECIMENTO, NÃO GERANDO VIOLAÇÃO À INTIMIDADE, À IMAGEM OU À VIDA PRIVADA DA AUTORA, NÃO HÁ FALAR EM INDENIZAÇÃO A TÍTULO DE DANOS MORAIS. 2 RECURSO NÃO PROVIDO. IMPROCEDÊNCIA, AÇÃO DE INDENIZAÇÃO, DANO MORAL, CARACTERIZAÇÃO, MERO ABORRECIMENTO, INOCORRÊNCIA, VIOLAÇÃO, HONRA. NEGAR PROVIMENTO AO RECUR... (JUSBRASIL)

> TJDF - Apelação Cível APL 32576820088070006 DF 0003257-68.2008.8...
>
> Data de Publicação: 18/11/2010
>
> Ementa: PROCESSO CIVIL. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO CUMULADA COM DANOS MORAIS. RELAÇÃO DE CONSUMO. COBRANÇA INDEVIDA. AUSÊNCIA DE VIOLAÇÃO À HONRA, INTIMIDADE E VIDA PRIVADA DO AUTOR. DANO MORAL. INEXISTÊNCIA. 1. CONFIGURANDO O FATO LESIVO (COBRANÇA INDEVIDA) MERO ABORRECIMENTO, E NÃO GERANDO VIOLAÇÃO À INTIMIDADE, À IMAGEM OU À VIDA PRIVADA DA AUTORA, NÃO HÁ FALAR EM INDENIZAÇÃO A TÍTULO DE DANOS MORAIS. 2. RECURSO NÃO PROVIDO.. Resultado sem Formatação NEGAR PROVIMENTO AO RECURSO, U..

Como demonstrado, é notório que para que haja a violação da intimidade e a vida privada é necessário que haja ofensa em dimensões psíquica da vítima, afetando-lhe a auto estima, a respeitabilidade e a honra, pois ter sua intimidade divulgada gera total constrangimento tirando toda a tranquilidade antes existente.

Temos a intimidade e a honra como valor constitucional em que encontra-se inseridos no rol dos direitos e garantias fundamentais da pessoa humana, assim, a exclusão do conhecimento alheio com relação a que só se diz respeito à própria pessoa, configura-se no direito de resguardar-se da ingerência alheia.

Portanto, se houver negação ou violação ao direito ao respeito à vida privada e à intimidade, o ordenamento jurídico assegura o direito de toda e qualquer medida jurídica para coibir tal ato, seja penal, administrativo ou civil.

REFERÊNCIAS

JUSBRASIL. http://www.jusbrasil.com.br/jurisprudencia/busca?q=FATO+DA+VIDA+PRIVADA&s=jurisprudência. Acesso em 01 de novembro de 2011.

MORAES, Alexandre de. Direito constitucional. São Paulo: Atlas, 2008.

SARMENTO, George. Danos Morais. ed. São Paulo-SP: Saraiva, 2009.

SILVA. Felipe Ventin da. Fundamentos dos direitos de personalidade e o papel da tutela inibitória na sua proteção.

http://jus.com.br/revista/texto/18471/fundamentos-dos-direitos-de-personalidade-e-o-papel-da-tutela-inibitoria-na-sua-protecao. Acesso em 01 de novembro de 2011.

Conforme a NBR 6023:2000 da Associacao Brasileira de Normas Técnicas (ABNT), este texto cientifico publicado em periódico eletrônico deve ser citado da seguinte forma: BRITO, Daniela de Oliveira. Há dano ao invadir avida privada e a intimidade de uma pessoa ferindo a tutela constitucional?. Conteudo Juridico, Brasilia-DF: 19 jul. 2012. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.38015&seo=1>. Acesso em: 14 nov. 2018.

(Fonte: http://www.conteudojuridico.com.br/?artigos&ver=2.38015&seo=1, acesso em 10/11/2018)

3. Exemplos de invasão de privacidade no ambiente de trabalho

Por: José Roberto Marques | Blog | 17 de março de 2018

Duvido que exista alguém que gostem de ter sua intimidade profissional e ou pessoal exposta sem o seu consentimento. Quando falamos em invasão de privacidade no ambiente de trabalho, precisamos ser cautelosos para saber diferenciar o que é ser invasivo ou não.

Para isso, é preciso que o funcionário que julgou se sentir prejudicado de alguma forma, tenha conhecimento do código de ética da organização. Possuir essa informação é importante para distinguir o que é ou não é um comportamento incorreto ou mesmo ilegal.

Quer saber mais sobre o assunto? Acompanhe o texto para saber mais sobre o assunto e aprender proteger suas particularidades.

Como diferenciar o que é assunto público ou privado

Muitas vezes, no ambiente empresarial as pessoas não entendem a diferença entre o que é público e privado. Essa falta de conhecimento pode ser o fator primordial para que alguém quebre uma regra e invada a intimidade de outra pessoa no ambiente de trabalho.

Se, por exemplo, o líder tem acesso ao e-mail do colaborador e, este considera isso uma invasão, é importante reavaliar a situação. É o momento de analisar se a atitude é permitida pela política interna da empresa ou não. Caso não seja legal dentro da organização, é o momento de ter uma conversa franca com o líder. A discussão deve ser saudável: a pessoa que se sentiu mal deve explicar seus motivos, assim como aquele que cometeu a ação. Se não isso der certo, já é hora de entrar em contato com a área de Recursos Humanos (RH) e fazer uma denúncia.

Cada corporação tem o direito de desenvolver uma política interna que serve como um documento para que os colaboradores sigam os tópicos no dia a dia. O guia deve ser explicado a todos os funcionários, sejam novos ou não, e pode ser revisado regularmente, já que a sociedade e a comunidade da empresa estão em constante mudança.

Mesmo que cada organização tenha seu sistema de regras e normas internas em relação à privacidade dos colaboradores, vale lembrar que todas elas, independentemente de seu porte ou segmento, são passíveis de sofrerem sanções legais quando desrespeitam as leis constitucionais do País. Isso quer dizer que o código de ética da corporação não está acima da lei. Caso a organização, contrarie nossa legislação, pode ser processadas judicialmente tanto pelo funcionário que se sentiu lesado e exposto, quanto pela própria justiça, na defesa do bem coletivo e individual. Dica: antes de sair por aí processando a tudo e todos, procure reunir as políticas da empresa e as provas do acontecido. Depois, entre em contato com um advogado. Esse será o profissional ideal para lhe aconselhar corretamente sobre todos os passos que devem ser seguidos.

10 exemplos de condutas de invasão de privacidade

Agora vou destacar algumas condutas que podem ser consideradas como invasão de privacidade. Confira!

- Instalar câmeras de vigilância em locais privados como banheiros.
- Fazer com que o profissional passe pelo detector de mentiras. Isso talvez não seja válido para quem trabalha em organizações de inteligência.
- Instalar escutas eletrônicas sem o conhecimento de todos os profissionais envolvidos. Não importa o local: salas de reunião, mesa de trabalho ou até celular, é preciso pedir permissão primeiro.
- Monitorar de chamadas telefônicas, salvo aquelas que são feitas com clientes. No caso de quem trabalha com telemarketing, por exemplo, é comum que os líderes de célula escutem as ligações para avaliá-las.
- Fazer revistas de bolsas na entrada e na saída da empresa.
- Fazer revista íntima em qualquer momento.
- Cometer atos de assédio moral ou sexual são formas de invasão do espaço íntimo da pessoa.
- Usar informação pessoal como moeda de troca para conseguir promoção ou se manter no trabalho. Isso é chantagem!

- Pegar e ou mexer no celular, computador, documentos ou coisas da mesa do colega sem autorização prévia. Mesmo que os dispositivos sejam corporativos é essencial pedir aprovação antes independentemente do nível hierárquico.
- Revelar salário e bonificações dos colegas, caso o colaborador tenha acesso a essas informações. Geralmente, o profissional do departamento pessoal tem esses dados. Eles devem ser éticos e guardarem esse relatório apenas para as partes competentes.

Como você pode perceber, esses são comportamentos que extrapolam totalmente a linha do bom senso. Nunca viu nenhuma dessas atitudes acontecerem no local em que você trabalha? Que bom! Infelizmente, muitas pessoas já viram ou foram vítimas desse tipo de conduta.

Direitos e deveres corporativos

Você sabe quais são seus direitos e deveres enquanto empregado da empresa em que está agora? Além disso, você sabe quais são os direitos e deveres da organização para a qual trabalha? Ter conhecimento desses tópicos é essencial para entender se sua índole está de acordo com a cultura da empresa. E também para saber se algo fora do combinado está acontecendo.

As empresas têm o direito e dever de zelar por sua cultura e fiscalizar a execução de suas normas internas. Afinal, o guia de ética é uma forma de fazer com que todos os colaboradores sigam as regras básicas que irão ajudar a todos a cumprirem com os valores e a missão da corporação.

Por outro lado, isso não dá o direito da organização constranger ou mesmo de espionar seus funcionários. Além de contraditórias, algumas dessas atitudes são ilegais. Elas podem tanto gerar problemas emocionais nos colaboradores, como também sanções à empresa, que pode ser penalizada judicialmente pelo comportamento invasivo. Fique atento ao que está acontecendo em volta. Respeite a privacidade dos seus colegas e não deixe que invadam a sua!

O que fazer caso invadam minha intimidade na empresa

Conversar com o seu gestor é o primeiro passo para conseguir resolver a situação. Caso isso não funcione, é o momento de procurar pelo RH. E, se depois de tudo isso você ainda estiver com problemas, procure pela justiça. Minha recomendação é evitar ao máximo sair da esfera da sua empresa. Tente com todas suas forças resolver o problema com as pessoas da organização. Esse pode ser o caminho menos cansativo e mais rápido.

O melhor caminho é sempre aquele que envolve o respeito e a conciliação. Para conseguir esse ambiente saudável, basta que a organização crie regras claras, que atendam suas necessidades e anseios, mas que acima de tudo, respeitem os seus profissionais. Afinal, são eles que cooperam para que a empresa cresça no dia a dia. Lembre-se disso e tenha sempre bom senso!

Comente se ainda há mais alguma ação de invasão de privacidade que você conhece e não escrevi por aqui!

Copyright: 587575499 – https://www.shutterstock.com/pt/g/adiruch

(Fonte: https://www.jrmcoaching.com.br/blog/exemplos-invasao-privacidade-ambiente-de-trabalho/, acesso em 10/11/2018)

4. Saiba mais em corporativo

Neste treinamento, os profissionais passam por uma formação diferenciada, que tem como objetivo lhes proporcionar aprimoramento e aprendizado, técnico e comportamental, visando sempre à conquista efetiva de metas e objetivos estratégicos e planejados e a aceleração dos resultados das organizações.

(Fonte: https://www.jrmcoaching.com.br/especialidades/coaching-corporativo/, acesso em 10/11/2018)

5. Responsabilidade civil decorrente da violação do direito à privacidade na Internet

Fillipe Silva Sampaio

Publicado em 05/2015. Elaborado em 01/2015.

O artigo trata da aplicação do instituto da responsabilidade civil sobre algumas práticas violadoras do direito à privacidade na Internet. Tem por objetivo analisar a incidência da responsabilidade civil em relevantes e usuais condutas virtuais.

Resumo: O presente estudo trata da aplicação do instituto da responsabilidade civil sobre algumas práticas violadoras do direito à privacidade na Internet. Tem por objetivo analisar a incidência da responsabilidade civil em relevantes e usuais condutas que violam a privacidade na Internet. Parte-se do entendimento de que o direito à privacidade é uma garantia constitucional e precisa, por vezes, ser reinterpretado ante as mudanças comportamentais que ocorrem na sociedade, especialmente aquelas decorrentes dos avanços tecnológicos como o fenômeno da socialização digital. Debate-se sobre a prática de envio de spams e pragas digitais, a utilização de dados pessoais do consumidor sem consentimento assim como a exposição virtual de conteúdos ofensivos a privacidade alheia. Questiona-se ainda a responsabilidade de provedores de serviços de Internet quanto as violações mencionadas. Demonstra-se também a experiência jurisprudencial brasileira para orientar a prática forense nas lides atinentes ao tema.

Palavras-chave: Privacidade. Internet. Spams. Pragas digitais. Responsabilidade civil.

Abstract: *The present study deals with the application of the institute of civil liability for certain practices that violate the right to privacy on the Internet. Aimed at analyzing the impact of tort law on relevant and usual conduct that would violate the privacy on the Internet. Started from the understanding that the right to privacy is a constitutional right and need sometimes to be reinterpreted because the behavioral changes that occur in society, especially those arising from technological advances such as the phenomenon of digital socialization. There is a debate about the practice of spamming and digital pests, the use of personal consumer data without consent and exposing content offensive to others privacy. It questions about the responsibility of Internet service providers on the*

violations previously mentioned. Also demonstrates the Brazilian judicial experience to guide forensic practice in litigations relating to this theme.

Keywords: *Privacy. Internet. Spams. Digital plague. Liability.*

Sumário: Introdução. 1. Spams. 2. Pragas digitais. 3. Cookies e tecnologia de controle. 4. Dados pessoais do consumidor. 5. Exposição da vida privada. Conclusão.

Introdução

A privacidade é um direito assegurado constitucionalmente e visa proteger aspectos da vida do indivíduo que não devem ser divulgados ou manuseados pela coletividade. No entanto, com a crescente socialização digital e a vulnerabilidade do usuário de Internet, esse direito tem sido constantemente desrespeitado, ensejando a aplicação de institutos jurídicos para a reparação dos danos causados às vítimas. Nesse contexto, como responsabilizar civilmente aqueles que violam o direito à privacidade na Internet?

Em resposta a esse cenário foi aprovada e publicada em 24 de abril de 2014 a Lei nº 12.965, também conhecida como "Marco Civil da Internet". Esse recente texto legal visa estabelecer princípios, garantias, direito e deveres para o uso da Internet no Brasil. Contudo, a Socialização Digital ainda não se encontra claramente regulamentada, principalmente no tocante à proteção de direitos da personalidade como o direito à privacidade, havendo assim possíveis lacunas jurídicas a serem preenchidas pelo legislador e pelo julgador, o que proporciona uma série de conflitos novos ao direito e um clima de insegurança jurídica relacionado as transformações sociais no âmbito virtual.

Existem no Brasil diversos dispositivos legais que tratam sobre a Internet e tecnologias afins em assuntos específicos como a Lei nº 9.295/1996 que organiza os serviços de telecomunicações, a Lei nº 9.609/1998 que protege a propriedade intelectual de programa de computador, a Lei nº 11.829/2008 que aprimora o combate a pedofilia na Internet, entre outras. Entretanto a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, é quem representa um divisor de águas no tocante a regulação da rede no Brasil, estabelecendo princípios, garantias, direito e deveres para o uso da Internet.

Questão ainda bastante controversa dentro do referido tema é a responsabilidade dos provedores de serviços de Internet sobre a divulgação de informações pessoais, de conteúdo íntimo ou ofensivas. Estas empresas atuam no mundo digital fornecendo acesso, hospedagem, conteúdo e outros recursos à terceiros que se manifestam em nome próprio ou até de forma anônima.

Percebe-se que as relações sociais não são as mesmas de cinquenta anos atrás. Muitas práticas novas surgiram com o desenvolvimento da tecnologia. Algumas positivas, que incentivam o progresso da humanidade como o compartilhamento e a acessibilidade de informações. E outras negativas, que violam direitos e ofendem a integridade moral de indivíduos como as violações de privacidade na Internet. É necessário que o operador do direito tenha uma compreensão de quais práticas violam a privacidade na Internet e como

elas ocorrem para a devida aplicação do instituto da responsabilidade civil. Além disso, é necessária a identificação dos agentes causadores do dano, a caracterização das condutas praticadas no meio digital e sua correspondência com as hipóteses presentes no ordenamento jurídico brasileiro para uma aplicação adequada do instituto da responsabilidade civil, o que se propõe a seguir.

1 Spams

Tem se tornado comum casos de pessoas que tiveram seus computadores ou outros dispositivos ligados a Internet invadidos por terceiros com o intuito de obter informações pessoais. À medida que a Internet cresce e se populariza, cresce também o número de invasões a esses aparelhos. Citando alguns meios dessa invasão, temos: spams, trojans, hackers, crackers, cookies, spywares, entre outros.

Em primeiro momento, trata-se do spam, considerando sua relevância jurídica e sua instrumentalidade para outras formas de invasão. Assim, a empresa Microsoft através de seu site, na Central de Proteção e Segurança, traz a definição de spam:

> "Spam é qualquer tipo de comunicação online não desejada. A forma mais comum de spam é o e-mail não desejado. Também é possível receber spam por SMS, em mensagens instantâneas (também conhecido como spim) e em redes sociais. Alguns tipos de spam incomodam, mas não causam danos. Entretanto, alguns tipos de spam fazem parte de golpes de roubo de identidade ou outros tipos de fraude. O spam de roubo de identidade é geralmente chamado de golpe de phishing. (MICROSOFT, 2014, online)"

Segundo Renata Cicilini Teixeia, apud Walter Aranha Capanema (2009, p. 19), spam é "toda mensagem eletrônica enviada a um ou mais usuários, sem que este(s) tenha(m) explicitamente solicitado o envio desta".

Walter Aranha Capanema (2009), autor do livro O Spam e as pragas digitais, comenta que o termo spam se deu em razão de uma marca de carne enlatada, da empresa Hormel Foods Corporation, que era enviada aos soldados durante a Segunda Guerra Mundial. A comparação feita com o referido produto significaria que os emails não solicitados eram repetitivos, cansativos e insuportáveis.

A literatura mencionada informa que o primeiro caso de spam ocorreu em 1994, quando um casal de advogados americanos teria postado uma série de mensagens anunciando seus serviços no sistema de mensagens Usenet. Assim, a prática ganhou repercussão e começou a ser bastante utilizada para fins comerciais.

Os spammers, como são denominados os emissores destas comunicações não desejadas, não se restringiram a contas de email e logo se utilizaram de serviços de mensagem instantânea, Blogs e redes sociais.

Os spams são geralmente enviados em massa para diversos destinatários. Algumas dessas mensagens costumam assemelhar-se a comunicados de sites confiáveis, levando o usuário ao engano. Assim, o internauta acaba muitas vezes por fornecer dados pessoais como CPF, senha e dados bancários acreditando se tratar de uma mensagem de seu banco

ou de alguma outra empresa confiável. Nesse caso, verifica-se roubo de informações pessoais através de meio fraudulento, ao qual é possível o enquadramento no crime de estelionato previsto no artigo 171 do Código Penal.

O autor Capanema (2009) aponta algumas formas de envio de spam, como através de emails, programas de mensagem instantânea, grupos de discussão online, blogs, sites de relacionamento e mensagens de telefones celulares.

Além do spam representar um meio rápido e barato de divulgação de produtos e serviços, uma de suas principais características é a ausência de autorização para o seu envio.

Há uma discussão quanto a forma de autorização para o envio de mensagens. Os Estados Unidos, em sua lei anti-spam, adotam o conceito opt out. Isso implica dizer que as mensagens podem ser livremente enviadas, desde que ofereçam a opção de cancelar o envio de futuras mensagens não desejadas. Trata-se da opção para sair da lista de envios de um determinado remetente. Deste modo, a mensagem só é considerada spam se encaminhada após a solicitação de cancelamento de envios.

Cristine Hoepers e Klaus Steding-Jessen (2005) fazem a seguinte crítica ao sistema opt out:

> "O opt-out coloca sobre o destinatário o ônus de ter que se desinscrever de um número enorme de fontes propaganda, quando provavelmente ele gostaria de receber mensagens apenas de um numero várias ordens de grandeza menor. Não é lógico pensar que deve ser responsabilidade do usuário dizer de quem ele não deseja receber mensagens, especialmente em função do número de mensagens envolvidas, quando é muito mais natural que parta do usuário a iniciativa de escolher as fontes de propaganda que deseja receber (opt-in). (HOEPERS; STEDING-JESSEN, 2005)"

A opinião dos autores está em consonância com nossa legislação consumerista atribuindo o ônus da publicidade ao fornecedor de produtos e/ou serviços, considerando a situação de vulnerabilidade do consumidor.

Na União Europeia a política adotada é o conceito opt in, ou seja, o destinatário precisa autorizar o envio dessas mensagens comerciais. Nesse caso, o problema dos spams é tratado de forma preventiva, evitando que o ônus recaia sobre o usuário em descadastrar-se de diversos sistemas.

Os prejuízos causados pelo spam são diversos, como o gasto desnecessário de tempo para apagar mensagens não solicitadas, o aumento de despesas com programas de computador para impedir a entrada de spams, o não recebimento de mensagens por esgotamento do espaço de caixa postal, entre outros.

No entanto, interessa a este trabalho os danos causados à privacidade do usuário. O spam, por si só, não representa grave prejuízo a privacidade do indivíduo, contudo, como mencionado anteriormente, ele consiste em um instrumento para diversas formas de pragas digitais. O spam é a comunicação não solicitada e abusiva, mas torna-se um veículo necessário para práticas que violam gravemente a privacidade como trojans, spywares, phishing scam, entre outros, dos quais trataremos a diante.

Deste modo, a prática do spam pode resultar na apropriação de informações pessoais por terceiros, na exposição do usuário a conteúdos indesejados, especialmente de cunho sexual, na perda de dados informáticos privados, entre outros. Como consequência dos prejuízos causados, analisa-se a possibilidade de aplicação do instituto da responsabilidade civil.

O envio de mensagens comerciais é direito de seu remetente, objetivando a divulgação de produtos, serviços e outras atividades de interesse. Entretanto, referida prática pode ser classificada como spam dependendo dos termos do envio da mensagem. Como já mencionado anteriormente, o spam é, em síntese, uma comunicação online não desejada, que normalmente ocorre por email, podendo ainda se dar de outras formas. Segundo ensinamento de Walter Aranha Capanema (2009), o envio de spams, mesmo que desacompanhado de outras pragas digitais pode ser configurado como abuso do direito, nos termos do artigo 187 do Código Civil.

> "Numa abordagem civilista, o spammer poderia estar enquadrado no art. 187 do Código Civil, que trata do abuso de direito, pelo que o direito individual não pode ser exercido de forma absoluta, prejudicando terceiros. O limite é a liberdade do outro. Seria o caso do spammer. Este tem a liberdade em enviar mensagens e de divulgar seus produtos, serviços, ideias e pensamentos. Contudo, a partir do momento em que tal direito se mostra um estorvo a terceiros, seria possível enquadrar a conduta do spammer nesta hipótese, e pleitear indenização por danos materiais, mediante prova do prejuízo, admitindo-se, inclusive, sua cumulação com a compensação por danos morais, com fundamento no art. 927, CC. (CAPANEMA, 2009, p. 36)"

Segundo o mencionado autor, o spam é considerado uma prática abusiva, seja para fins comerciais, ou com intenções criminosas, que pode ser devidamente enquadrada pelos dispositivos legais existentes com vistas a proteção do direito à privacidade e da condição de vulnerabilidade do consumidor.

Nesse mesmo entendimento, Flavio Tartuce (2011, p. 355) comenta sobre o envio de spams como abuso de direito:

> "O ato de envio constitui abuso de direito – assemelhado ao ato ilícito pelas eventuais consequências –, eis que o usuário da Internet não a solicita, não fornece seu endereço virtual, e, mesmo assim, recebe em sua caixa de correio eletrônico convites a aderir aos mais variados planos, produtos, grupos, jogos, serviços, entre outros."

Para entender o que é o abuso do direito, segue as palavras de Flavio Tartuce (2011, p. 337): "o abuso de direito é um ato lícito pelo conteúdo, ilícito pelas consequências, tendo natureza jurídica mista - entre o ato jurídico e o ato ilícito - situando-se no mundo dos fatos jurídicos em sentido amplo".

O mencionado autor considera o abuso do direito primeiramente como ato lícito pelo conteúdo porque se trata de um exercício de um direito. O fato é que esse direito ao ser exercitado excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes, tornando-se um ato ilícito pelas consequências.

O artigo 187 do Código Civil, em que é possível se enquadrar a prática de envio de spams, consiste em uma cláusula geral de responsabilidade objetiva. Assim, considerar a

prática de spam um abuso de direito implica dizer que o remetente-spammer deve responder pelos prejuízos causados independentemente de culpa. Reforçando esse entendimento, segue a redação do Enunciado nº 37 do Conselho da Justiça Federal: "A responsabilidade civil decorrente do abuso do direito independe de culpa, e fundamenta-se somente no critério objetivo-finalístico".

Farias, Rosenvald e Netto (2014, p. 233) ensinam que:

> "Em tais situação, bastará à imputação do dano que o agente tenha exercitado um direito – subjetivo ou potestativo – de forma excessiva, frustrando a boa-fé objetiva, os bons costumes ou a função econômico-social para a qual aquela situação jurídica lhe fora concedida. Isto é, abstrai-se o elemento volitivo do causador do dano, sendo suficiente o exame de proporcionalidade entre o ato de autonomia e a finalidade perseguida pelo agente."

Ponto importante mencionado pelos autores é a configuração da forma excessiva, de modo que frustre a boa-fé objetiva, os bons costumes ou a função econômico-social do direito a que se faz uso. O spam, de fato, advém de um direito subjetivo ou da liberdade do remetente em enviar um determinado conteúdo a outros usuários. Na medida em que há esta liberdade, também há o direito do destinatário em não receber a mensagem indesejada, ou seja, o seu direito de ser deixado só, direito de não ser incomodado com aquilo que não solicitou, sendo estes aspectos de sua privacidade.

O direito à privacidade do outro naturalmente constitui um limite a liberdade individual. Assim, o spam configura-se como excesso a função econômico-social da liberdade individual justamente por confrontar com a privacidade alheia. Ademais, o remetente-spammer falta com a boa-fé ao desrespeitar o espaço de outros usuários enviando-lhe mensagens e conteúdos indesejados.

Flávio Tartuce (2011, p. 355) aponta que:

> "Pela falência que pode gerar a Internet deve-se entender que o spam contraria o fim social e econômico da grande rede, o que já serviria para enquadrar a prática como abuso de direito ou ato emulativo. Também é forçoso concluir que a conduta dos spammers é atentatória à boa-fé objetiva."

Sergio Cavalieri Filho (2014) define o abuso do direito como ato ilícito objetivo, desde que aquele que o pratica cause dano a outrem. O dano é um elemento necessário para tratar da incidência da responsabilidade civil, pois a natureza reparatória do instituto tem a sua justificativa no direito do indivíduo não ser prejudicado por outro.

Sergio Cavalieri Filho (2014, p. 92) trabalha com a seguinte ilustração para melhor explicar a relação entre o dano e o ato ilícito: "Se o motorista, apesar de avançar o sinal propositadamente, não atropela ninguém, nem bate em outro veículo, não haverá o que indenizar".

Desta forma, mesmo que seja constatada a prática do ato ilícito, se não houver dano, não há o que reparar e a responsabilidade civil perde seu objeto. Assim, como pressuposto da responsabilidade civil, é imprescindível que o destinatário do spam tenha

prejuízos com a prática, seja de ordem material ou moral, para a incidência o referido instituto.

Contudo, quanto a ilustração mencionada, mesmo que não haja o dever de indenizar em razão da ausência de dano, o ato ilícito deve ser reprimido de alguma forma, sob de pena de constituir um atentado ao estado de direito. Deste modo, verificando-se ou não a presença do dano decorrente da prática do envio de spams, fica claro que alguma providência deve ser tomada para a cessação do ato ilícito.

Apesar do raciocínio exposto até aqui, o entendimento jurisprudencial majoritário segue no sentido da não configuração do dano moral quanto à prática de envio de spams, conforme transcrição a seguir:

> "INTERNET - ENVIO DE MENSAGENS ELETRÔNICAS - SPAM - POSSIBILIDADE DE RECUSA POR SIMPLES DELETAÇAO - DANO MORAL NAO CONFIGURADO - Recurso Especial NAO CONHECIDO. 1 - segundo a doutrina pátria "só deve ser reputado como dano moral a dor, vexame, sofrimento ou humilhação que, fugindo à normalidade, interfira intensamente no comportamento psicológico do indivíduo, causando-lhe aflições, angústia e desequilíbrio em seu bem-estar. Mero dissabor, aborrecimento, mágoa, irritação ou sensibilidade exacerbada estão fora da órbita do dano moral, porquanto tais situações não são intensas e duradouras, a ponto de romper o equilíbrio psicológico do indivíduo". 2 - Não obstante o inegável incômodo, o envio de mensagens eletrônicas em massa - SPAM - por si só não consubstancia fundamento para justificar a ação de dano moral, notadamente em face da evolução tecnológica que permite o bloqueio, a deletação ou simplesmente a recusada de tais mensagens. 3 - Inexistindo ataques a honra ou a dignidade de quem o recebe as mensagens eletrônicas, não há que se falar em nexo de causalidade a justificar uma condenação por danos morais. 4 - Recurso Especial não conhecido. (REsp 844.736/DF, Rel. Ministro LUIS FELIPE SALOMAO, Rel. p/ Acórdão Ministro HONILDO AMARAL DE MELLO CASTRO (DESEMBARGADOR CONVOCADO DO TJ/AP), QUARTA TURMA, julgado em 27/10/2009, DJe 02/09/2010)"

De acordo com o referido julgado para a configuração do dano moral torna-se necessário que o envio de spams cause dor, vexame, sofrimento, humilhação, ou que interfira intensamente no comportamento psicológico do usuário, causando-lhe aflições, angústias e desequilíbrio em seu bem-estar. De fato, não se verifica dano desta ordem no recebimento de spams. Assim, a prática mencionada acaba por ser considerada como mero dissabor ou simples aborrecimento.

Diante da não configuração de dano algum ao usuário, pode ainda o magistrado reconhecer o spam como ato abusivo e sancionar o ofensor de acordo com as peculiaridades do caso. Neste sentido, Farias, Rosenvald e Netto (2014, p. 240):

> "Ao contrário, no artigo 187 do Código Civil, a reprovação do ordenamento jurídico se exprime por um juízo de retribuição à própria conduta do agente, independentemente dos efeitos de seu comportamento. Certamente, se o exercício de um ato abusivo repercutir lesões patrimoniais ou extrapatrimoniais, a sanção será transferida para a ***fattispecie*** do artigo 927 do Diploma Civil. Mas, é vital o correto enfrentamento do artigo 187 para a percepção quanto à possibilidade de se sancionar o abuso do direito com outras consequências diversas do plano reparatório, tais como a nulidade, a decadência ou a supressão de determinada situação jurídica do agente."

Destaca-se que a detecção do abuso do direito, caso a caso, cabe ao magistrado, uma vez que se trata de transgressão ao exercício de um direito. No caso de spams, reconhecido

o ato abusivo, o juiz de direito pode determinar em sede de tutela obrigacional que o remetente se abstenha de enviar novamente qualquer mensagem indesejada, independente da existência de danos ao destinatário, inclusive sob a força de preceito cominatório (astreintes). Na legislação consumerista, a medida encontra fundamento no artigo 84:

> "Art. 84. Na ação que tenha por objeto o cumprimento da obrigação de fazer ou não fazer, o juiz concederá a tutela específica da obrigação ou determinará providências que assegurem o resultado prático equivalente ao do adimplemento."

O que se pode perceber é uma autonomia do abuso do direito em relação a responsabilidade civil, tendo em vista que esta tem natureza reparatória e aquela, de preservação de direitos e ordem social.

Corroborando essa ideia, o Enunciado nº 539 do Conselho de Justiça Federal: "O abuso de direito é uma categoria jurídica autônoma em relação à responsabilidade civil. Por isso, o exercício abusivo de posições jurídicas desafia controle independentemente de dano".

Portanto, não resta dúvida que o remetente-spammer deve ser responsabilizado ou sancionado pela sua conduta com base no abuso do direito, no entanto, a aplicação do instituto da responsabilidade civil fica condicionada a existência de dano ao usuário.

Há casos em que os autores dessas práticas não são identificáveis em virtude das características da Internet e das tecnologias utilizadas pelos mesmos. Nesta situação surge a discussão quanto a responsabilização do provedor de email por essa prática.

No caso do recebimento de spams através de email, pode-se ter a figura do provedor de email como fornecedor em uma relação de consumo entre este e o usuário. Para a caracterização da relação de consumo é necessária a presença dos elementos subjetivos, o consumidor e o fornecedor, e dos elementos objetivos, o produto ou o serviço.

O conceito de fornecedor está elencado no artigo 3º do Código de Defesa do Consumidor, no qual se enquadra o provedor de serviços de email:

> "Art. 3º. Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços."

O usuário da conta de email, da mesma forma, encontra-se bem determinado como pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final, nos termos do artigo 2º do CDC.

Quanto ao elemento objetivo, a prestação do serviço de caixa postal eletrônica, a exigência do § 2º do artigo 3º do CDC é que se trate de uma atividade fornecida no mercado de consumo mediante remuneração. Apesar de boa parte dos serviços de email serem gratuitos, eles obtêm vantagens indiretas com a utilização do serviço pelo consumidor. No entendimento de Flavio Tartuce (2014, p. 98) "admite-se que o prestador tenha vantagens indiretas, sem que isso prejudique a qualificação da relação consumerista".

Configurado o tipo de relação entre estes sujeitos deve-se apreciar a responsabilidade civil à luz do Código de Defesa do Consumidor, que em seu artigo 14 dispõe:

> "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos."

O provedor de email é um fornecedor de serviços, o qual presta ao usuário o serviço de correio eletrônico, fornecendo-lhe uma caixa postal virtual. Assim, aplica-se o dispositivo legal mencionado, incidindo sobre o provedor de email a responsabilidade objetiva pelos danos causados ao usuário por defeitos relativos à prestação de seu serviço.

É preciso a compreensão do que é um serviço defeituoso e a esse respeito, o §1º do referido artigo:

> "§ 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido."

A caracterização do serviço defeituoso é definida pela expectativa de segurança que o usuário pode ter em relação ao provedor de email. Como assevera Sergio Cavalieri Filho (2014, p. 556), "a responsabilidade do fornecedor de serviços tem também por fundamento o dever de segurança".

Ainda segundo lição de Sergio Cavalieri Filho (2014, p. 551):

> "[...] depreende-se que a noção de segurança depende do casamento de dois elementos: a desconformidade com um expectativa legítima do consumidor e a capacidade de causar acidente de consumo. Resulta daí que a noção de segurança tem uma certa relatividade, pois não há produto ou serviço totalmente seguro."

Assim, é preciso analisar a legítima expectativa do consumidor quanto a proteção de sua caixa de emails contra spams. De fato, é admissível que o cliente da conta de email espere uma caixa postal eletrônica segura, que não possa ser invadida por terceiros. Contudo, é notório e amplamente divulgado a existência da prática de spam e seus consequentes softwares mal-intencionados, bem como a dificuldade de se realizar o controle e a filtragem das mensagens. Vale ressaltar, como no já mencionado entendimento jurisprudencial, que existe a possibilidade de recusa destas mensagens eletrônicas por simples deletação. Assim, pode-se considerar como risco razoável o recebimento de spams, cabendo ao usuário a seleção do que abrir ou executar.

Sobre o assunto, Capanema (2009, p. 84) comenta que "se a tecnologia não garante a possibilidade de filtragem total dos spams, ainda assim os provedores deveriam ser responsabilizados? Assim, por questão de justiça, a resposta deve ser não." Considerando a impossibilidade técnica do provedor de email em realizar um filtro e identificação de todos os spams, imputar esse ônus a ele seria o mesmo que inviabilizar sua atividade comercial.

Outro ponto é a excludente de responsabilidade constante no artigo 14, § 3º, II, do CDC: a culpa exclusiva do consumidor ou de terceiro. O provedor de email, em regra, não tem vínculo com o remetente-spammer. Assim o defeito da prestação é causado por terceiro, estranho a relação de consumo do provedor com o usuário.

Portanto, o provedor de email não deve ser responsabilizado pela prática de spams em razão de sua incapacidade técnica e da culpa de terceiro, bem como da constatação que o risco do recebimento de spams é notório, razoável e de fácil superação pelo usuário.

2 Pragas digitais

Outra forma de violação da privacidade na Internet decorre de pragas digitais, como *trojans, screenloggers, keyloggers, vírus, worms, spywares, phishing scam*, entre outros. Elas consistem em softwares maliciosos com a finalidade de praticar um crime contra o patrimônio ou contra a privacidade do internauta. Geralmente a contaminação de dispositivos eletrônicos com as referidas pragas ocorre através da prática de spam, nesse caso, denominado por Walter Aranha Capanema como spam qualificado, ou através de um endereço eletrônico acessado pelo usuário.

Quanto ao spam qualificado, o criminoso vale-se de dois métodos, como mencionado a seguir:

> "a) automática: **a inserção de um programa de computador, através do envio de mensagem eletrônica, no computador da vítima, programa este que se executa automaticamente, sem qualquer intervenção.** b) engenharia social: **conhecido como *phishing scam*, é uma forma bastante elaborada de ataque, em que o agente incentiva ou induz em erro a vítima para que esta faça algo, como fornecer informações ou dinheiro, ou, ainda, execute determinado cavalo de troia, seria útil ou benéfico. (CAPANEMA, 2009, p. 25)"**

Seja através de spam ou não, a atuação criminosa se dá com a instalação de softwares no dispositivo eletrônico do internauta, dos quais trataremos a seguir.

O site da empresa Kaspersky (empresa que comercializa soluções contra invasões em computadores) menciona o conceito de trojans:

> **"Os Trojans são programas maliciosos que executam ações não autorizadas pelo utilizador. Estas ações podem incluir: eliminação, bloqueio, modificação e cópia de dados ou ainda perturbação do desempenho de computadores ou redes informáticas. (KASPERSKY LAB, 2014, online.)"**

Os trojans representam um gênero de uma grande quantidade de espécies de softwares maliciosos. O trojan-banker, por exemplo, consiste em um tipo especializado na captação de dados bancários, de informações de sistemas de pagamento armazenados no computador, bem como dados de cartões de débito ou crédito. O trojan-IM rastreia no computador nomes de usuários e senhas para que possa ter acesso a programas de mensagens instantâneas e chats, como MSN Messenger, Skype e outros. Há ainda o trojan-spy que monitora a utilização do computador infectado, criando um verdadeiro perfil do usuário com suas preferências de sites, assuntos de interesse, horário de navegação e etc. Os

tipos de trojans não encerram aqui, havendo ainda dezenas de técnicas empregadas para invadir a privacidade do indivíduo através desta modalidade de software.

Têm-se ainda os *screenloggers*, que de acordo com o glossário da página de segurança do banco HSBC, consistem em:

> "Tipo de trojan que grava as páginas que o usuário visita e a área em volta do clique do mouse e as envia pela Internet. Por isso são chamados de screenloggers (a palavra screen, em inglês, refere-se à tela do computador). Com isso, o screenlogger permite que um intruso roube senhas e outras informações privadas. Geralmente instala-se no sistema de modo furtivo e sua ação não é percebida pelo dono do computador atacado. (HSBC, 2014, online)"

Maurício Grego apud Capanema (2009, p. 26) define os *keyloggers* como "programa que registra o que é digitado no micro", com o objetivo de se apropriar das informações digitadas pela vítima.

Outro bastante conhecido, o *vírus*, segundo Capanema (2009, p. 26), "é o tipo de programa de computador cuja principal função seja a destruição dos dados informáticos com ou sem a alteração das funções computacionais". Diferentemente, o *worm* é uma espécie de vírus sem a finalidade de destruir dados, mas tão somente de autorreplicar-se para causar sobrecarga de servidor ou rede.

Outra modalidade de coleta de informações desautorizadas é o spyware, também conhecido como software espião. Renato Leite Monteiro (2009), em trabalho publicado nos Anais do XVIII Congresso Nacional do CONPEDI, conceitua:

> "Spyware, ou software espião consiste em um programa automático de computador, que recolhe informações sobre o usuário, sobre seus costumes na Internet e transmite estas informações a uma entidade externa na Internet, sem o seu conhecimento e o seu consentimento. (MONTEIRO, 2009)"

Quanto ao *phishing scam*, Juliana Carpanez, em matéria publicada na Folha de São Paulo, esclarece:

> "O que é: Esta técnica permite que piratas virtuais roubem informações da máquina da vítima. O principal objetivo é utilizar esses dados em transações financeiras, sem o consentimento do titular da conta corrente, por exemplo. Como acontece: Para instalar os programas espiões no computador das vítimas, os piratas oferecem links via e-mail ou sugerem visitas a sites maliciosos. O sucesso da estratégia está ligado ao poder de persuasão das mensagens --quanto melhor a história, maiores as chances de o usuário "obedecer" o pirata. (CARPANEZ, 2014)"

Todas as pragas digitais mencionadas trazem ao usuário prejuízo a sua privacidade, seja por captação de informações não autorizadas ou por invasão de um espaço privado, de acordo com as peculiaridades da atuação de cada uma.

Ademais, a prática em comento constitui crime, tipificado no artigo 154-A do Código Penal, a saber:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa."

A utilização das mencionadas pragas digitais não representa somente um ilícito na esfera penal. Essa prática, além de violar o direito à privacidade, também causa danos ao usuário, sendo, portanto, um ato ilícito também na esfera civil, nos termos do artigo 186 do Código Civil, transcrito abaixo:

> "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

Deste modo, o uso de pragas digitais enseja o dever de reparar o dano causado à vítima, nos termos do artigo 927 do Código Civil, o que significa a incidência do instituto da responsabilidade civil, em regra subjetiva, ao autor do delito.

Semelhantemente como ocorrem com os spammers não identificáveis, os autores dessas pragas digitais nem sempre são encontrados. Nesta circunstância analisa-se a possibilidade de responsabilização de provedores de hospedagem que armazenam em seus servidores arquivos e páginas contaminados contribuindo para a disseminação das pragas mencionadas.

Walter Aranha Capanema (2009, p. 85) comenta que:

> "Tendo em vista que esses programas podem ser detectados por antivírus e programas antiphishing, parece que o melhor entendimento é permitir a responsabilidade solidária do provedor com o remetente-criminoso, pois aquele só deveria disponibilizar um arquivo à comunidade se tiver certeza de que este é seguro. (CAPANEMA, 2009, p. 85)"

A relação jurídica entre o provedor de hospedagem, que disponibiliza um arquivo infectado, e o usuário, que faz o download do referido arquivo, não é diferente da relação estabelecida entre o provedor de email e o usuário da caixa postal eletrônica comentada anteriormente. Neste caso, também se verifica a relação de consumo e a caracterização de um serviço defeituoso pelos mesmos fundamentos, o dever de segurança.

Da mesma forma, também é perceptível a falta de capacidade técnica dos provedores de hospedagem em verificar o conteúdo de todos os arquivos e páginas nele armazenados. Isso se dá pela própria característica do serviço prestado, que oferece armazenamento e não edição de conteúdo. Esclarecendo, o provedor de hospedagem se assemelha a um guarda-volumes. Este tipo de serviço se presta a guardar o objeto indicado pelo contratante sem se importar com a natureza do objeto. Assim, em razão disto, é possível considerar como excludente de responsabilidade a culpa exclusiva de terceiro, prevista no artigo 14, § 3º, II, do Código de Defesa do Consumidor.

Por fim, vale ressaltar que cabe à hipótese mencionada a aplicação do artigo 18 da Lei 12.965/2014 que garante a não responsabilização do provedor por danos decorrentes de conteúdo gerado por terceiros.

3 Cookies e tecnologia de controle

A estrutura aberta da Internet propicia não apenas o aperfeiçoamento da tecnologia, mas também o desenvolvimento de inúmeras tecnologias de controle, que interessam principalmente a governos e empresas.

Laura Schertel Mendes (2014, p. 101), citando Lawrence Lessig, afirma que "com o uso dessas tecnologias, é possível violar a privacidade". Essas tecnologias objetivam a coleta de dados pessoais e são realizadas de forma imperceptível ao usuário. Manuel Castells *apud* Mendes (2014, p. 102) classifica as tecnologias de controle disponíveis na Internet em três tipos, quais sejam, de identificação, de vigilância e de investigação.

As tecnologias de identificação, segundo Laura Schertel Mendes (2014, p.102), "constituem aquelas que permitem a localização do usuário, bem como a verificação de todos os seus movimentos online". Exemplo destas são os cookies.

Divulga-se que os cookies consistem em uma ferramenta de aprimoramento da navegação, como registros de determinados sites que ficam armazenados no computador contendo informações como idioma, cor e modo de exibição escolhidos pelo usuário na navegação anterior. Contudo, nem sempre as informações registradas são tão triviais como estas mencionadas.

Observa-se a explicação da Microsoft acerca do tema:

> "Cookies são pequenos arquivos que os sites colocam no disco rígido do seu computador quando você os visita pela primeira vez. Pense em um cookie como um cartão de identificação que é exclusivamente seu. A função do cookie é notificar o site quando você voltar. Embora seja possível sua utilização indevida quando armazenam dados pessoais, os cookies em si não são Mal-intencionados. Muitos sites, inclusive o da Microsoft, usam cookies. Os cookies nos dizem quantas vezes você visita páginas, o que nos ajuda a descobrir quais informações são de seu interesse. Desta forma, podemos oferecer mais do conteúdo que você gosta e menos do que não gosta. Os cookies podem ajudá-lo a ser mais eficiente. Alguma vez você já colocou algum item em um carrinho de compras virtual de uma loja online e, alguns dias mais tarde, quando voltou, descobriu que o item ainda estava lá? Esse é um exemplo de cookie em funcionamento. Os cookies permitem guardar preferências e nomes de usuário, registrar produtos e serviços e ainda personalizar páginas. Mas se você nunca registrar nem deixar informações pessoais no site, o servidor só saberá que alguém com o seu cookie retornou ao site. Ele não saberá nada além disso. (MICROSOFT, 2014, online)"

Para Laura Schertel Mendes (2014, p.102):

> "Os cookies são marcadores digitais que são automaticamente inseridos por websites visitados, nos discos rígidos do computador do consumidor, em sua casa ou no seu local de trabalho, para possibilitar a sua identificação e a memorização de todos os seus movimentos."

Se por um lado eles permitem o aprimoramento e personalização de serviços na Internet, por outro, eles possibilitam o rastreamento e monitoramento do comportamento do usuário, tornando-se uma ameaça a sua privacidade.

Outro problema dessa captação de dados é que a mesma é realizada sem o consentimento do indivíduo e não se conhece os reais termos de utilização desses dados.

Deste modo, mesmo empresas de boa reputação armazenam informações pessoais e podem se utilizar delas até mesmo em desfavor de seus clientes visando seus lucros.

A Lei 12.965/2014 em seu artigo 7º, IX, prevê que deve ser assegurado ao usuário o "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais".

Deste modo, a legitimidade da coleta de informações por meio de cookies instalados no navegador do usuário depende tanto do seu consentimento prévio como do fornecimento de informações completas a respeito da coleta.

Se a aplicação de Internet não seguir os termos legais mencionados, fica caracterizada uma nítida violação do direito à privacidade do indivíduo, podendo, sem prejuízo das demais sanções cíveis, criminais ou administrativas, culminar na aplicação das sanções constantes do artigo 12 da Lei 12.965/2014, conforme a seguir:

> "Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11."

Como dito, ainda cabe a devida responsabilização civil por violação da privacidade do indivíduo pela coleta de dados pessoais sem o consentimento prévio de seu titular. Vale ressaltar que a aplicação do instituto da responsabilidade civil tem como um de seus pressupostos a existência de dano à vítima. Assim, a incidência do dever de indenizar está condicionada a constatação de dano decorrente da prática em questão.

Apesar de não haver ainda uma experiência jurisprudencial notória quanto a responsabilidade civil pela simples coleta indevida de informações do usuário de Internet, a sua aplicação não é impossível. A esse respeito, o seguinte julgado, que trata também de violação da privacidade pela utilização de dados pessoais e configura indenização por dano moral:

"RESPONSABILIDADE CIVIL - Dano moral - Google Maps - Serviço da ré que disponibilizou na 'Internet' imagem da residência do autor vinculada a seus dados pessoais - Alegação de impossibilidade técnica para impedir a ocorrência de fatos como esse que não convence - Ademais, irrelevante prova dessa impossibilidade ante a teoria do risco da atividade - Ofensa aos direitos à privacidade e segurança do autor - Devida indenização por dano moral - Redução do valor arbitrado na origem em observância aos princípios da proporcionalidade, razoabilidade e modicidade - Desprovido apelo do autor e provido em parte apelo da ré, apenas para baixar valor da indenização. (TJ-SP - APL: 19507874201082601 00 SP 0195078-74.2010.8.26.0100, Relator: Roberto Solimene, Data de Julgamento: 20/10/2011, 6ª Câmara de Direito Privado, Data de Publicação: 26/10/2011)"

Por fim, a aplicação do instituto da responsabilidade civil torna-se mais viável na hipótese de utilização indevida de dados ao invés de sua simples coleta. Essa situação é observada especialmente nas relações de consumo, através do repasse de informações cadastrais a terceiros ou da comercialização de bancos de dados, que serão tratados adiante.

4 Dados pessoais do consumidor

Outra preocupação acerca da privacidade é a proteção dos dados do consumidor nas operações realizadas pela Internet. O comércio eletrônico tem crescido e se aprimorado supostamente para melhor atender as necessidades do consumidor. Na verdade, o que todo comerciante busca, dentro e fora da Internet, é lucro. O problema está nos meios usados para auferir vantagem em cima do consumidor.

É comum que empreendedores virtuais coletem informações acerca de seus clientes e estruturem um verdadeiro banco de dados com tais informações. Entende-se banco de dados como um conjunto de informações organizadas obedecendo a uma determinada lógica.

A manutenção de bancos de dados e cadastros de consumidores não é ilegal, porém precisa estar de acordo com as observâncias do Código de Defesa do Consumidor, que em seu artigo 43 prevê:

"Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1° 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.

§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3° 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.

§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5° Consumada a prescrição relativa à 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."

Um dos problemas é que nem sempre essas informações coletadas são usadas para atender melhor às necessidades do consumidor. Na realidade o mercado tem utilizado técnicas ilegítimas de marketing com as informações apuradas. Existe um verdadeiro assédio de consumo. Ao acessar um site de compras pela Internet, basta que o consumidor clique apenas uma vez em um determinado produto para que o site registre aquela ação. Com essa informação de suposto interesse por determinado produto dá-se início ao assédio. A loja se esmera para deixar a vista do consumidor o referido produto com estratégias de email, redes sociais, mensagens de celular, entre outros, cada vez com uma oferta mais tentadora até que o indivíduo concretize a compra.

Existe uma clara ofensa a privacidade do indivíduo que, primeiramente, não autoriza o registro de seu comportamento no site de compras. Em segundo lugar, o indivíduo não solicita receber informações e ofertas daquele determinado produto que por vezes lotam sua caixa de email ou mesmo atrapalham sua navegação pelas redes sociais.

Fernanda Nunes Barbosa (2014, p. 245) em participação na obra de título Direito privado e Internet, comenta sobre o direito do consumidor à não informação:

"Isso quer dizer que o consumidor tem o direito pleno de ser resguardado quanto ao recebimento de e-mails em sua caixa de mensagens eletrônicas com anúncio de produtos e serviços que não deseja e para cuja empresa não forneceu seus dados, bem como direito a não receber chamadas em seus telefones móvel e fixo, especialmente em horários inoportunos e de fornecedores que compraram seus dados cadastrais, situações comuns já vivenciadas pela grande maioria dos consumidores, se não a totalidade deles, o que, em nosso entender, constitui prática abusiva por parte dos fornecedores."

O que se observa é uma verdadeira política de marketing agressiva, que assedia o consumidor utilizando de todas as informações possíveis, mesmo que indevidas, para que o indivíduo seja compelido a realizar uma transação comercial. O direito a não informação

consiste na proteção do sossego do consumidor quando este não solicita uma demanda de ofertas. Deste modo, o direito à informação do consumidor em seu aspecto negativo relaciona-se ao direito à privacidade.

Outro problema relacionado ao mercado eletrônico e a privacidade é a comercialização de bancos de dados. Não bastando a coleta não autorizada de informações pessoais e a utilização destas em desfavor do consumidor, há ainda quem comercialize essas informações.

Barbosa (2014, p. 237) menciona o questionamento de Ronaldo Porto Macedo Júnior:

> "Acerca da abusividade existente na comercialização de banco de dados, Ronaldo Porto Macedo Júnior questiona se a venda de informações pessoais contidas num cadastro de consumidores – as ***mailing lists***, consideradas ativos patrimoniais das empresas – fornecido a uma empresa por outra configuraria uma violação do direito à privacidade e demandaria uma reparação com base nos princípios de privacidade constitucionalmente assegurados ou, antes, reclamaria participação e controle do consumidor na utilização de seus dados com finalidade não autorizada."

O questionamento mencionado trata, primeiramente, da configuração ou não de violação do direito à privacidade nos casos de venda de bancos de dados e cadastros de consumidores. É indiscutível que os tipos de dados comercializados são dados sensíveis do indivíduo como seu perfil econômico, suas preferências, hábitos de consumo e quase seus pensamentos. Estes dados representam a expressão da personalidade do consumidor. Assim, considerando o caráter pessoal das informações objeto dessa prática, não há como negar que a mesma ofenda a privacidade do indivíduo.

A doutrina também atribui ao caso em tela o direito à autodeterminação informacional, sendo este o direito do cidadão de tomar conhecimento sobre o arquivamento e uso de informações suas por terceiros, bem como de controlá-los e até mesmo impedi-los.

O direito à privacidade relaciona-se ao direito da autodeterminação informacional especialmente no tocante aos dados sensíveis, aqueles relativos à esfera íntima do sujeito, bem como sua situação econômica e suas pretensões.

Ressalta-se que não há como confundir com os bancos de dados de proteção ao crédito, tendo em vista que estes trabalham com informações de interesse público.

Portanto, verifica-se nestes relatos, de acordo com o conceito de Daniel J. Solove, a ofensa a privacidade no tocante a coleta e processamento de informações e ainda a disseminação destas.

É inegável dizer que o direito à privacidade implica em proteção a dados pessoais do indivíduo. Assim, torna-se útil a investigação sobre os termos de utilização dessas informações por parte de banco de dados que estão sob o domínio do Estado e de empresas privadas. O Ministro Ruy Rosado de Aguiar ressalta a importância do tema em sede do Recurso Especial 22.337-9/RS, conforme trecho a seguir:

"A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com plenos conhecimentos de causa, também pode servir, ao Estado ou ao particular para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica. (REsp 22.337-9/RS)"

Como mencionado no voto acima, a utilização indevida de dados pessoais é preocupante, uma vez que os mesmos podem ser usados para fins ilícitos ou abusivos à privacidade do indivíduo.

Outro ponto importante comentado pelo Ministro Ruy Rosado de Aguiar é a vulnerabilidade do indivíduo em razão do desconhecimento do processamento de informações referentes a sua pessoa e da indisponibilidade de instrumentos ao seu alcance para o controle das referidas informações.

Um exemplo de utilização indevida de dados pessoais é o repasse dos mesmos a terceiros sem o consentimento de seu titular, como ocorrido em caso julgado pelo TJSP em que um consumidor, após ter aberto um cadastro em uma loja de departamentos, descobriu que as suas informações cadastrais, incluindo informações sobre seus rendimentos, foram repassadas indevidamente à mãe de sua filha, o que embasou uma ação de alimentos contra ele. A seguir a transcrição da referida ementa:

"RESPONSABILIDADE CIVIL - Ação de indenização por danos morais - Cerceamento de defesa - Inocorrência - Ré que repassou dados cadastrais acerca dos rendimentos do autor a terceira estranha e com fins sem qualquer ligação a outra relação de consumo - Abuso do objeto cadastral em detrimento da privacidade do autor -Dano moral in re ipsa - Quantum que não merece reparo - Correção monetária, por outro lado, que deve incidir a partir da data em que o valor foi arbitrado - Incidência de juros mantida a partir da citação - Encargos da sucumbência Reciprocidade - Inocorrência - Gratuidade processual que não pode ser revogada com base em futura indenização - Litigância de má-fé -Inocorrência - Recurso provido em parte. (TJSP - AC: 3.55.607400-0, Relator: De Santi Ribeiro, Órgão julgador: 1ª Câmara de Direito Privado Data de Julgamento: 02/07/2009, Data de Publicação: 18/08/2009)"

Como se observa do referido julgado, a conduta da empresa ré de repassar dados cadastrais a terceiro culminou no dever de indenizar o titular das informações por danos morais sob o fundamento de que a atitude da empresa foi abusiva e violou a privacidade do autor.

5 Exposição da vida privada

Outra preocupação relacionada à privacidade é a exposição de conteúdo íntimo no âmbito da Internet. Tem ganhado repercussão o caso dos Revenge porns (traduzindo:

pornografia da vingança) que consistem na publicação de fotos ou vídeos de conteúdo sexual de ex-parceiros(as).

Uma característica comum dos relacionamentos afetivos é a confidencialidade. Assim, os indivíduos acabam consentindo com o registro fotográfico e videográfico de momentos de sua privacidade, baseando-se numa relação de confiança com a pessoa que compartilha do evento em questão.

Ocorre que quando os relacionamentos se rompem se instaura um clima de animosidade entre os ex-parceiros. O resultado disso, frequentemente, é a divulgação do registro íntimo feito entre os ex-parceiros com o intuito de criar embaraços e constrangimentos ao outro, muitas vezes por mera vingança.

Observando novamente o conceito esculpido por Daniel J. Solove, o caso dos revenge porns enquadra-se como uma ofensa à proteção contra disseminação de informações, na espécie revelação, tendo em vista que a prática referida, apesar de real e verdadeira, causa um impacto negativo à reputação do indivíduo.

Vale ressaltar que essa prática não viola apenas a privacidade, mas a dignidade da pessoa humana, tendo em vista que a situação pode causar um sentimento de humilhação na vítima.

A exposição de fotos, vídeos e outras formas conteúdos indesejados na Internet não se restringem aos casos de pornografia da vingança. A verdade é que existem inúmeros fatos e peculiaridades que os indivíduos não pretendem expor aos olhares públicos, mas, por diversas vezes, são expostos contra a própria vontade, como ocorre frequentemente nas redes sociais.

As redes sociais representam um ponto forte à violação de privacidade. De fato, a Internet é um espelho das relações sociais e o ser humano sempre demonstrou interesse pela vida alheia, nunca faltando-lhe assunto para tratar da vida de outros. Ocorre que a Internet potencializa os prejuízos causados ao indivíduo. A exposição de um detalhe sobre a vida privada de alguém pode gerar um impacto irreversível, seja de ordem moral ou até material.

Como já mencionado anteriormente, não são raros os casos em que são divulgados nos domínios da Internet aspectos da vida privada de indivíduos, seja de cunho sexual ou não, sem o consentimento dos mesmos. Esta situação merece a devida atenção do operador do direito, especialmente na aplicação do instituto de responsabilidade civil.

Independente do tipo de conteúdo íntimo exposto e do meio empregado para tal ação, observa-se a presença de três elementos: o autor da divulgação; a vítima, que teve sua privacidade violada; e o veículo de publicação. Merece comentar que na exposição de conteúdo íntimo na Internet, o veículo de publicação se trata, geralmente, de sites, blogs e outras aplicações relacionadas a Internet, que são hospedadas por provedores de hospedagem e indexadas por provedores de pesquisa.

A exposição de conteúdo íntimo na Internet acarreta ao autor do fato, aquele que intencionalmente divulga o conteúdo indevido, a mesma responsabilidade de um caso

similar fora do âmbito virtual, diferenciando-se tão somente quanto a amplitude do dano causado à vítima.

Merece atenção a temática do dano moral quanto aos casos de violação da privacidade por meio da Internet decorrente da exposição de aspectos da vida privada de indivíduos. É entendimento pacificado que o magistrado deve arbitrar valores de indenização por dano moral de forma razoável, de modo que a quantia não seja pequena o suficiente para estimular a prática de atos ilícitos e também não seja demasiadamente alta a ponto de configurar o enriquecimento sem causa da vítima.

Sabe-se que a indenização por dano moral visa compensar a vítima pelo infortúnio sofrido, bem como aplicar uma sanção ao autor da ofensa pela prática do ato ilícito ou abusivo. Como é impossível a quantificação precisa do sofrimento, especialmente pelo seu caráter subjetivo, os juízes acabam por estipular critérios variados para a sua fixação.

Marcel Leonardi (2012, p. 225) comenta sobre:

> "Um relevante estudo sobre as razões de decidir adotadas no arbitramento do dano moral mostra que são vários os fatores considerados – culpa ou dolo, posição social do ofendido, risco criado, gravidade da ofensa, situação econômica do ofensor; mas parece ser levado em conta, principalmente como ponto de partida, a gravidade da ofensa ou potencialidade lesivo do fato, vez que impossível uma quantificação psicológica do abalo sofrido."

No tocante a Internet, deve-se ponderar que ela pode causar maior repercussão às exposições indevidas do que outros meios de divulgação. Entretanto, este fator não é absoluto, cabendo ao autor do ilícito a prova de que não houve grande repercussão, seja em razão do meio utilizado não favorecer grandes volumes de tráfego, seja da imediata retirada do conteúdo do ar ou outras causas.

Por outro lado, a discussão que tem tomado relevância quanto ao caso em tela diz respeito à responsabilidade dos provedores de Internet por hospedarem as referidas páginas ou facilitarem suas buscas no meio da rede mundial.

A seguir a transcrição da ementa de um julgado do Superior Tribunal de Justiça (STJ) que trata de um caso de publicação de conteúdo difamatório acerca de um professor através de um perfil falso em uma rede social:

"RECURSO ESPECIAL. AGRAVO REGIMENTAL. DIREITO ELETRÔNICO E RESPONSABILIDADE CIVIL. DANOS MORAIS. PROVEDOR DA INTERNET SEM CONTROLE PRÉVIO DE CONTEÚDO. ORKUT. MENSAGEM OFENSIVA. NOTIFICAÇÃO PRÉVIA. INÉRCIA DO PROVEDOR DE BUSCA. RESPONSABILIDADE SUBJETIVA CARACTERIZADA. AGRAVO DESPROVIDO. 1. Este Tribunal Superior, por seus precedentes, já se manifestou no sentido de que: I) o dano moral decorrente de mensagens com conteúdo ofensivo inseridas em site por usuário não constitui risco inerente à atividade desenvolvida pelo provedor da Internet, porquanto não se lhe é exigido que proceda a controle prévio de conteúdo inserido e disponibilizado por usuários, pelo que não se lhe aplica a responsabilidade objetiva, prevista no art. 927, parágrafo único, do CC/2002; II) a fiscalização prévia dos conteúdos postados não é atividade intrínseca ao serviço prestado pelo provedor no ORKUT. 2. A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato. 3. O fornecimento do registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na Internet constitui meio satisfatório de identificação de usuários. 4. Na hipótese, a decisão recorrida dispõe expressamente que o provedor foi notificado extrajudicialmente, por meio de ferramenta que ele próprio disponibiliza para denúncia de abusos - na espécie, criação de perfil falso difamatório do suposto titular e ofensivo a terceiros -, não tendo tomado as providências cabíveis, optando por manter-se inerte, motivo pelo qual responsabilizou-se solidariamente pelos danos morais infringidos ao promovente, configurando a responsabilidade subjetiva do réu. 5. Agravo regimental não provido. (STJ - AgRg no REsp: 1396963 RS 2012/0221494-1, Relator: Ministro RAUL ARAÚJO, Data de Julgamento: 08/05/2014, T4 - QUARTA TURMA, Data de Publicação: DJe 23/05/2014)"

Segundo a mencionada jurisprudência, é pacificado o entendimento no Tribunal Superior de que o provedor da aplicação de Internet não é responsável por conteúdos ofensivos quando não lhe cabe o controle prévio de conteúdos inseridos por usuários, por não constituir risco inerente a sua atividade.

Acerca da teoria do risco, Caio Mario, apud Sergio Cavalieri Filho (2014, p. 183), de forma didática sintetiza: "aquele que, em razão de sua atividade ou profissão, cria um perigo, está sujeito à reparação do dano que causar, salvo prova de haver adotado todas as medidas idôneas a evitá-lo".

De acordo com a referida teoria, a empresa criadora da rede social ou o provedor da aplicação de Internet em que se fez a publicação ofensiva deveria responder objetivamente pelo simples fato de criar uma atividade que possibilita a agressão à intimidade do indivíduo. Contudo, o entendimento do Superior Tribunal de Justiça, em razão da fiscalização prévia dos conteúdos postados não consistir em atividade intrínseca ao serviço prestado pelo provedor, é que o mesmo deve responder subjetivamente, quando por omissão não retira do ar o conteúdo ofensivo de forma eficiente após a devida notificação ou quando não adota as providências necessárias para a identificação do real agressor.

É preciso levar em consideração a real atribuição do provedor de serviços e aplicações de Internet. Como já mencionado anteriormente, eles possuem uma posição ambígua, conforme lição de Gilberto de Almeida Martins, citado por Liliana Paesani (2013, p. 66):

> "Os provedores assumem uma posição ambígua, de um lado, eles são conduzidos a desenvolver o papel de operadores de telecomunicações, transmitindo mensagens por meio da rede sem conhecer o conteúdo e, portanto, sem assumir a responsabilidade. Por outro lado, eles são levados a desenvolver o papel tradicional do editor, e, nesse caso, responsáveis pelo conteúdo."

Se a referida entidade realiza edição de conteúdo, cabe a responsabilidade objetiva, todavia, se tão somente disponibiliza o serviço sem estabelecer um prévio controle do que é inserido no meio digital, ela não pode ser responsabilizada, salvo nas hipóteses elencadas pelo julgado do STJ anteriormente transcrito, quando a responsabilidade será subjetiva.

Vale ressaltar que segundo a jurisprudência da Corte Superior a notificação necessária ao provedor não precisa ocorrer em sede de processo judicial, sendo suficiente qualquer comunicação que denuncie a ofensa ao direito da vítima, inclusive por intermédio de ferramentas disponíveis no próprio site, se houver.

O Marco Civil da Internet (Lei nº 12.965/2014) prevê de forma similar a responsabilização do provedor por danos decorrentes de conteúdos gerados por terceiros, exigindo, entretanto, que a notificação seja judicial. A seguir o referido dispositivo da Lei:

> "Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário."

Porém, se o conteúdo ofensivo tratar-se de cenas de nudez ou de atos sexuais de caráter privado, a notificação pode ser extrajudicial, encaminhada pelo ofendido ou seu representante legal, o qual deve evidenciar sua legitimidade para apresentação do pedido bem como identificar o material apontado, a fim de que o provedor torne o conteúdo indisponível. Segue transcrição do artigo 21 da referida lei:

> "Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo."

Portanto, os provedores são responsáveis de forma subjetiva em três hipóteses: a) pelos conteúdos dos quais não fiscalizam previamente; b) quando não adotam as medidas necessárias para o resguardo do direito à privacidade da vítima; e c) quando não cooperam para a identificação do real autor do dano.

Conclusão

As práticas violadoras do direito à privacidade na Internet não são passíveis de serem enumeradas em um rol taxativo, principalmente em razão das constantes mudanças sociais, porém algumas condutas merecem especial atenção em virtude de sua relevância e implicações jurídicas e socio-econômicas.

No tocante aos spams, verifica-se que estes constituem abuso de direito, enquadrado pelo artigo 187 do Código Civil, razão pela qual aplica-se a responsabilidade objetiva ao spammer. Entretanto, o entendimento jurisprudencial majoritário o considera mero dissabor ou aborrecimento, ensejando a não configuração do dano moral.

Independentemente da aplicação da responsabilidade civil, cabe, ainda, contra a referida prática a tutela obrigacional devida, com o objetivo da cessação da conduta abusiva, inclusive sob a força de preceito cominatório.

O provedor de email, apesar de caracterizado como fornecedor em uma relação de consumo com o usuário, não deve ser responsabilizado pela prática de spams em razão de sua incapacidade técnica na identificação de todos os remetentes-spammers e também pela configuração da culpa de terceiro.

No que diz respeito as pragas digitais, que invadem dispositivos eletrônicos e roubam informações pessoais, aplica-se aos seus autores a responsabilidade subjetiva, por tratar-se de um ato ilícito sem qualquer relação jurídica especial.

Com relação aos provedores que hospedam esses conteúdos nocivos, filia-se por sua não responsabilização pelos mesmos fundamentos atinentes ao provedor de email pela prática de spam.

Os cookies, além de ferramenta de aprimoramento à navegação na Internet, também podem servir como tecnologia de controle ofensiva a privacidade, situação em que é possível a incidência do instituto da responsabilidade civil aos autores das aplicações de Internet que fazem seu uso indevido.

Nas relações de consumo, o direito à privacidade revela-se na proteção dos dados pessoais do consumidor, que são coletados e utilizados inadequadamente, configurando uma prática abusiva e culminando na responsabilização civil objetiva dos fornecedores.

Observe-se, ainda, o desrespeito a privacidade por parte de usuários que extrapolam os limites da vida privada alheia, publicando conteúdos ofensivos à esfera íntima de terceiros. A estes cabe a responsabilidade civil subjetiva pelos eventuais danos causados, similarmente a casos fora do ambiente virtual, devendo-se, no entanto, levar em consideração a amplitude dos danos em virtude das peculiaridades da Internet.

Nestes casos, o provedor de Internet só responde quando não adota as medidas necessárias, após a devida notificação, e de forma subjetiva segundo entendimento jurisprudencial do Superior Tribunal de Justiça.

Deste modo, conclui-se que a privacidade é um direito de suma importância que assiste a todo indivíduo, o qual com o surgimento dos novos domínios da Internet e da evolução de comportamento sociais decorrentes do aparato tecnológico que segue em constante desenvolvimento necessita de especial atenção e tutela. Nesse contexto, o consagrado instituto da responsabilidade civil mostra-se suficiente para este fim - proteção da privacidade no meio digital - desde que modernamente interpretado.

Referências

ABREU, Frederico do Valle. *Conceito jurídico indeterminado, interpretação da lei, processo e suposto poder discricionário do magistrado*. ***Jus Navigandi***, Teresina, *ano 10*, *n. 674*, *10 maio 2005*. Disponível em: <http://jus.com.br/artigos/6674/conceito-juridico-indeterminado-interpretacao-da-lei-processo-e-suposto-poder-discricionario-do-magistrado>. Acesso em: 25 set. 2014.

BARBOSA, Fernanda Nunes. Informação e consumo: a proteção da privacidade do consumidor no mercado contemporâneo da oferta. *In*: MARTINS, Guilherme Magalhães (coordenador). ***Direito privado e Internet.*** São Paulo: Atlas, 2014.

BITTAR, Carlos Alberto. ***Os direitos da personalidade.*** São Paulo: Revista dos Tribunais, 1992.

BRASIL. Constituição (1998). ***Constituição da República Federativa do Brasil.*** Brasília: DF, Senado, 1988.

BRASIL. ***Novo Código Civil.*** Lei nº 10.403 de 10 de janeiro de 2002. Aprova o novo código civil brasileiro. Brasília, DF, 2002.

BRASIL. ***Código de Defesa do Consumidor.*** Lei nº 8.078, de 11 de setembro de 1990. Aprova o código de defesa do consumidor. Brasília, DF, 1990.

BRASIL. ***Lei nº 12.965,*** de 23 abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2014.

CENTRAL DE PROTEÇÃO E SEGURANÇA. ***Microsoft.*** Disponível em: <http://www.microsoft.com/pt-br/security/resources/spam-whatis.aspx>. Acesso em 24 ago. 2014.

CAPANEMA, Walter Aranha. ***O spam e as pragas digitais***: uma visão jurídico-tecnológica. São Paulo: LTr, 2009.

CAVALIERI FILHO, Sergio. ***Programa de responsabilidade civil.*** 11. ed. São Paulo: Atlas, 2014.

CARPANEZ, Juliana. Saiba como funcionam os golpes virtuais. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u19456.shtml>. Acesso em: 05 nov. 2014.

DICIONÁRIO AURÉLIO. Disponível em: <http://www.dicionariodoaurelio.com>. Acesso em: 26 set. 2014.

DICIONÁRIO MICHAELIS. Disponível em: <http://michaelis.uol.com.br>. Acesso em: 26 set. 2014.

FARIAS, Cristiano Chaves de, ROSENVALD, Nelson, NETTO, Felipe Peixoto Braga. ***Curso de Direito Civil:*** Responsabilidade Civil. ed. 2014. Salvador: Juspodivm, 2014

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado. ***Cadernos de Direito Tributário e Finanças Públicas,*** nº 1, RT, São Paulo: 1992, pp. 141-154. Disponível em: <http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28>. Acesso em: 26 set. 2014.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. Relatório para a Comissão de Trabalho sobre Spam do Comitê Gestor da Internet no Brasil: Análise técnica de algumas legislações sobre Spam. ***Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br.***

19 de agosto de 2005. Disponível em: <http://www.cert.br/docs/ct-spam/ct-spam-analise-legislacao.pdf>. Acesso em: 16 out. 2014

HSBC. ***Glossário***. Disponível em <http://www1.hsbc.com.br/common/seguranca/glossario-s.shtml>. Acesso em: 05 nov. 2014

KASPERSKY LAB. ***Internet security center.*** Disponível em <http://www.kaspersky.com/pt/Internet-security-center/threats/trojans>. Acesso em: 24 ago. 2014.

LEONARDI, Marcel. ***Tutela e privacidade na Internet.*** São Paulo: Saraiva, 2012.

MERRIAM-WEBSTER ONLINE DICTIONARY. Disponível em: <http://www.merriam-webster.com>. Acesso em: 26 set. 2014.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. ***Curso de direito constitucional***. 5. ed. rev. e atual. São Paulo: Saraiva, 2010.

MENDES, Laura Schertel. ***Privacidade, proteção de dados e defesa do consumidor:*** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MICROSOFT. ***Central de proteção e segurança.*** Disponível em: <http://www.microsoft.com/pt-br/security/resources/cookie-whatis.aspx>. Acesso em: 24 ago. 2014.

MICROSOFT. ***Central de proteção e segurança.*** Disponível em: <http://www.microsoft.com/pt-br/security/resources/spam-whatis.aspx>. Acesso em: 24 ago. 2014.

MONTEIRO, Renato Leite. Cibernética: a invasão da privacidade e da intimidade. In: ***Anais do XVIII Congresso Nacional do CONPEDI***, 2009, São Paulo. Disponível em <http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2513.pdf>. Acesso em: 24 ago. 2014.

PAESINI, Liliana Minardi. ***Direito e Internet:*** liberdade de informação, privacidade e responsabilidade civil. 6. ed. São Paulo: Atlas, 2013.

PINHEIRO, Patrícia Peck. ***Direito digital***. 5. ed. São Paulo: Saraiva, 2013.

TARTUCE, Flávio. ***Direito civil, v. 2***: direito das obrigações e responsabilidade civil. 6. ed. São Paulo: Método, 2011.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. ***Harvard Law Review***, v. IV, n. 5, dezembro de 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 26 set. 2014.