Revista FACISA *ON-LINE.* Barra do Garças – MT, vol.6, n.3, p. 174 -188, jul. - dez. 2017.
(ISSN 2238-8524)

REPARAÇÃO CIVIL NO ÂMBITO DAS RELAÇÕES DIGITAIS

Rubens Rodrigues Diniz de Aguirre[1]
Josemar Lorenzoni[2]
Luzia Maria de Morais Nogueira y Rocha[3]
Ronny Cesar Camilo Mota[4]

RESUMO: As relações digitais, juntamente com os recursos dela advindos, proporcionaram à sociedade um avanço em todos os ramos de comunicação, sendo a *internet* a principal ferramenta utilizada para tal finalidade. Deixando de lado os benefícios acrescidos por aquelas advindas do meio humano e mesmo naturais, tem-se a facilitação expressa para a perpetração de crimes pelo meio informático, visando, neste artigo, explicitar a maneira pela qual o criminoso digital será responsabilizado cível e criminalmente, bem como as ferramentas e os institutos que o direito brasileiro utiliza, ou deveria utilizar para repreender e compor os danos decorrentes dos *cybercrimes*. Importante, também, a questão da responsabilidade objetiva dos provedores que mantêm as redes sociais, devendo elas serem solidariamente responsáveis pelos ilícitos ocorridos nos seus domínios. Metodologicamente, por meio de uma pesquisa aplicada, de cunho qualitativo, obteve-se a investigação e a resolução de um problema coletivo para, dedutivamente, tornar cristalinas questões, como a tangibilidade da legislação brasileira com o meio informático, a análise de legislações internacionais e, inclusive, a indagação quanto à criação de uma Lei/Estatuto independente, que abarque as relações cibernéticas. Destarte, evidentes os resultados almejados, avaliando se o ordenamento jurídico brasileiro tem a necessidade de uma reforma e integralização, tendendo a localizar, conter e sancionar o criminoso, e proporcionar ao lesado, uma justa reparação dos danos morais e/ou patrimoniais sofridos, isto é, verificando se a atual legislação torna viável a obtenção da eficiência e eficácia total para produzir resultados competentemente satisfatórios.

PALAVRAS-CHAVE: *Internet*. Crimes. Responsabilidade. Redes Sociais.

[1] Bacharel do Curso de Direito da Faculdade de Ciências Jurídicas e Sociais Aplicadas do Araguaia – FACISA. E-mail: diniz.rubens@gmail.com
[2] Especialista em Docência no Ensino Superior. Professor do Curso de Direito da Faculdade de Ciências Jurídicas e Sociais Aplicadas do Araguaia – FACISA. E-mail: j.lorenzoni@brturbo.com.br
[3] Doutorado em Ciências Pedagógicas pela Universidad Central de las Villas – Cuba. Mestrado em Educação pela Universidade de Cuiabá (2002). Graduada em Letras pela Universidade Federal de Mato Grosso (1993). Coordenadora Adjunta do Curso de Direito da Faculdade de Ciências Jurídicas e Sociais Aplicadas do Araguaia – FACISA. Email: luziayricha@hotmail.com
[4] Mestre em Direito, Relações Internacionais e Desenvolvimento, pela Pontifícia Universidade Católica de Goiás - PUC/GO, Coordenador do Curso de Direito da Faculdade de Ciências Jurídicas e Sociais Aplicadas do Araguaia - FACISA. E-mail: ronnycamilo@hotmail.com

1 INTRODUÇÃO

As relações digitais, compreendidas como todo e qualquer contato, entre duas ou mais pessoas, por meio de dispositivos eletrônicos e/ou cibernéticos, utilizando ou não a rede mundial de comunicação (*internet*), favorece aos seus adeptos um rol de novas possibilidades, isto é, ultrapassando as relações do mundo físico, tornou-se possível naquela, conversar, interagir, trocar fotos, vídeos e textos, bem como praticar diversos atos que, há alguns anos, muitos diriam impossíveis, como fazer compras e estudar, entre outras condutas.

E, por ser uma tecnologia recente, nem todas as ciências e ramos interativos do ser humano a acompanham. Igualmente, o Direito não possui a capacidade de escoltar, com equidade, a tecnologia que, em toda sua abrangência, traduz, com fidelidade, os crimes anteriormente praticados com condutas físicas e, agora, com condutas virtuais.

Fazendo uma meação entre as searas penal e civil, como um modo complementar para expor a Responsabilidade Civil advinda da prática de ilícitos, revela-se a problemática: a legislação civil e penal brasileira possui, ou não, ferramentas eficientes e eficazes, a ponto de possibilitar o ressarcimento dos danos causados a outrem por meios digitais?

Para tanto, necessário se faz a explanação de diversos pontos, como um paralelo entre as legislações brasileiras, verificando sua tangibilidade com as relações digitais; abordar legislações internacionais com escopo de utilizá-las no mundo jurídico brasileiro; corroborar a aplicação do direito material, no âmbito dos danos materiais e morais causados por meio das redes sociais; aferir a aplicação da responsabilidade civil objetiva nos provedores, domínios e proprietários das redes sociais envolvidas no dano e analisar a possível criação de uma Lei/Estatuto independente, abarcando as relações cibernéticas, com o escopo único de demonstrar, de modo contundente, como e quais as ferramentas o Direito pode, deve e utiliza, ou deveria utilizar, para repreender e/ou reparar, em âmbito cível, os danos causados a outrem, por meio das relações eletrônicas, visando responder à problemática proposta.

A partir do questionado, visando almejar o resultado previsto, tornou-se necessária a realização de uma pesquisa aplicada, ou seja, a reunião de informações, com o escopo de aplicação do ordenamento civil e/ou penal dentro do contexto de crime/dano, ocasionado, no âmbito cibernético, informações distribuídas em seções, com o intuito de uma melhor organização.

Quanto à abordagem das informações supracitadas, é trivial o método qualitativo, ou

seja, as pesquisas de fato, matéria e realidade serão empregadas de maneira a concatenar-se com o tema e o problema, para, juntos e harmonicamente, alcançar os objetivos propostos.

Feito o enunciado, a pesquisa por ação se mostra apropriada, pois trata-se de uma investigação para a resolução de um problema coletivo, selecionado, isto é, para os usuários de dispositivos informáticos, que são vítimas de crimes virtuais e/ou são legítimos no ressarcimento, reparação ou composição cível.

Considera-se o método dedutivo o mais adequado, pelo qual, por meio de análises gerais, chegar-se-á num entendimento particular a respeito do objetivo geral proposto, respondendo à problemática sugerida, apontando a eficácia e a efetividade da legislação brasileira, no tocante aos crimes digitais e sua composição, e a proposta de uma legislação específica para a matéria.

Como autores basilares para a construção deste artigo, tem-se Marcelo Xavier de Freitas Crespo, Luis Marcos Leite e Helita Barreira Custódio.

Sucessivamente, é evidente e crucial a solução do problema proposto, em virtude de a sociedade brasileira carecer de legislação própria voltada para as relações digitais, e, por tal, os ordenamentos jurídicos já positivados são aplicados analogicamente no que cabem, sendo, desta maneira, ineficazes na repressão/reparação dos acontecimentos, envolvendo aquela Relação.

Assim, justifica-se a necessidade de expor claramente se o direito material está acompanhando a evolução social e tecnológica do país, sendo errada tal assertiva, revelando as ferramentas necessárias que podem e devem ser utilizadas pelo legislador na profilaxia ou reparação do agravo ocorrido numa relação digital.

2 OS CRIMES VIRTUAIS E A LEGISLAÇÃO BRASILEIRA

Para trazer à tona o termo Responsabilidade Civil e suas modalidades de reparação aplicada à seara da informática, essencial torna-se a explanação de alguns termos, como, por exemplo, o Crime Virtual/Cibernético/Informático, pois, muitas vezes, é com sua prática que nasce o direito líquido e certo da composição cível. É praticando um crime – por meio da seara cibernética – que o criminoso dará à vítima a faculdade de pleitear na justiça a reparação do prejudicado e/ou perdido.

Embora sua nomenclatura não seja pacificada entre os doutrinadores – crimes virtuais, de computador, fraude informática, *cybercrimes* etc. – seu significado etimológico e conceitual é simples e objetivo: "Os crimes informáticos seriam de meio, isto é, delitos tradicionalmente já tipificados no ordenamento jurídico, mas que diante das facilidades trazidas pela tecnologia, passam a ser cometidos por meio desta." (CRESPO, 2011, p.50).

A Legislação brasileira, embora não possua um ordenamento fixo e exclusivo a respeito dos crimes virtuais, vem utilizando instrumentos jurídicos diversos e esparsos, como por exemplo, as Leis nº 11.829/2008 (crimes relacionados à pedofilia na *internet*), nº 9.983/2000 (acesso indevido a sistemas da administração pública), nº 9.609/1998 (proteção da propriedade intelectual de programa de computador), entre outras espalhadas na forma positivada, como legislação atinente ao meio digital, ou mesmo leis utilizadas de modo analógico das condutas físicas para as virtuais – como o Código Civil e Penal – sancionando, assim, os agentes ativos da lide, os criminosos cibernéticos.

A corrente majoritária brasileira defende a classificação dos crimes digitais em próprios e impróprios, sendo distribuídos nessas duas categorias, a depender do bem jurídico ofendido, se perpetrados contra um sistema digital, ou contra diversos bens jurídicos, respectivamente.

2.1 Crimes Digitais Próprios

Estes, de modo sucinto, podem ser entendidos como as condutas ilícitas voltadas à lesão do próprio sistema informático, ou seja, o bem jurídico atingido é a própria informação digital, não abarcando, nesta classificação, a ofensa ou o dano direto ao ser humano. No entanto, sabe-se poderem existir os danos indiretos, advindos do acesso não autorizado, obtenção, transferência e divulgação indevida de dados, que podem ser utilizados de inúmeras maneiras e com distintas finalidades, podendo, ainda, incluir-se, nesta seção, a disseminação proposital de vírus, com o intuito de deformar, modificar ou inutilizar o sistema operacional ou mesmo arquivos.

2.2 Crimes Digitais Impróprios

Intimamente ligados ao tema deste artigo, os crimes digitais impróprios são aqueles que, diferentemente dos próprios, atingem bens jurídicos diversos, ou seja, atingem de modo direto o ser humano, causando danos morais e/ou psíquicos.

Ante o dito, é notório que os crimes digitais impróprios predominam, ensejando direito à composição civil, certo de que, com bojo no Código Penal, vislumbra-se um quantitativo considerável de tais crimes, isto é, há uma gama de condutas, antes, praticadas pelos meios tangíveis e, agora, cometidos, também, pelo meio intangível/cibernético, a saber: a calúnia (art. 138), difamação (art. 139), injúria (art. 140), ameaça (art. 147), furto (art. 155), dano (art. 163), apropriação indébita (art. 168), estelionato (art. 171) entre outros, que, uma vez perpetrados, podem dar ocasião à reparação/composição civil.

Exposto o significado, bem como divisão e explanação a respeito dos crimes virtuais e a legislação brasileira voltada à área penal, mostra-se vital a exposição direcionada à seara civil, em concatenação com a responsabilidade devida à prática dos ilícitos mencionados.

3 DA RESPONSABILIDADE CIVIL

Versada no Livro I, Título IX da Lei 10.426/2002 – Código Civil –, a Responsabilidade Civil é o instituto que regula o dever/obrigação de determinado indivíduo de ressarcir outrem, em virtude de uma conduta nociva à sua imagem, saúde, pudor etc.

Helita Barreira Custódio denomina tal instituto como:

> Em princípio, a responsabilidade em geral manifesta a obrigação de determinada pessoa para responder por uma conduta (fato, ato ou ação, ou omissão) prejudicial à sociedade ou a outrem, sujeitando-se à penalidade definida de acordo com a natureza da norma jurídica violada (de direito público ou de direito privado). (CUSTÓDIO, 2006, p.39).

Consequentemente, uma vez dado causa à obrigação de compor o dano – repará-lo –, ela será regulada pelo Código Civil de 2002 que, em seu conteúdo, explana todos os meios, hipóteses e modalidades de uma justa reparação.

É certo que a divisão mais sucinta e aceita pela doutrina majoritária seja a

Responsabilidade Civil Subjetiva e Objetiva; igualmente, ambas darão, a uma ou a um conjunto de vítimas, o direito de ter seu direito reavido ou ressarcido, alterando, somente, o polo passivo da lide, ou seja, o devedor do quantitativo reparador.

3.1 Responsabilidade Civil Subjetiva

Talvez a primogênita das variáveis modalidades de responsabilidade, a subjetiva, remonte à necessidade de culpa para a imputação de um juízo de valoração negativo, a partir da conduta de determinado indivíduo, ou seja, para que ele seja enquadrado no perfil de um agressor de determinado bem jurídico, é basilar sua intenção, ou seja, o dolo e a intenção em prejudicar outrem, ou, mesmo, a falta de atenção em seus atos.

Como os objetivos estão enraizados nas relações cibernéticas, precisamente nas redes sociais – objeto de estudo nas próximas seções – tem importante participação o instituto da teoria da culpa/subjetiva, pois, praticado um crime impróprio, seu causador direto será o agente passivo da lide penal e também da lide cível, incidindo, esta última, na responsabilidade civil subjetiva, e obrigado a reparar o dano advindo de seu crime.

É necessária a compreensão de que a responsabilidade civil independe da criminal, assim, uma vez absolvido na esfera penal, a sentença não valerá como escusa para uma futura ou decorrente ação de reparação civil, salvo a que versar sobre inexistência de crime ou autoria (é a inteligência do código civil em seu art. 935), ou mesmo decorrente de atos advindos das excludentes de ilicitude, pois, tanto na cível como na criminal, tal situação exclui, também, a punibilidade do agente causador do dano.

3.2 Responsabilidade Civil Objetiva

Antagônica à retro modalidade de responsabilização do agente – teoria da culpa -, a responsabilidade civil objetiva vem atribuir às pessoas que não tenham causado, ainda que diretamente, o dano, ou praticado algum ilícito, a obrigação de reparar. Portanto, é a modalidade em que não existe a aferição da culpa/dolo do agente, mas, sim, a presunção de responsabilidade legal – devem estar elencadas na lei as situações aplicáveis ao caso concreto.

Como assunto da próxima seção, este tipo de responsabilidade será concatenada com

a característica consumerista das redes sociais, podendo o agente autor do crime/dano ser responsabilizado, juntamente com o meio utilizado para a prática da ação, ou seja, a própria rede social, também, será obrigada a compor, independentemente de culpa provada.

4 DAS REDES SOCIAIS E SUA RESPONSABILIDADE

Parcela importante a se estudar, as redes sociais podem ser caracterizadas como uma das modalidades de relacionamento público, utilizadas pelo internauta com a finalidade de contrair amizades, relacionamentos ou mesmo efetuar negócios de cunho empresarial. São exemplos: *facebook, orkut, myspace*[5]*, twitter e ask*[6].

Conceito semelhante e correto é o de Luís Marcos Leite:

> Redes Sociais são estruturas sociais virtuais compostas por pessoas e/ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns na internet [...] As redes sociais têm transformado a forma de comunicar das pessoas, tamanha a capacidade do seu alcance mundial, influenciando opiniões, mobilizando e criando grupos e trazendo informações em questão de segundos. (LEITE, 2013).

Devido às suas características - ser pública e de fácil acesso – muitas vezes podendo os usuários acessá-las sem nenhuma identificação, ou, quando identificados, não há nenhum mecanismo de autenticação dos dados fornecidos – é, no mundo virtual, a maior das portas de ocorrência dos crimes cibernéticos, isto é, por meio das redes sociais, meliantes dotados de má-fé, injuriam, caluniam, difamam, furtam, causam danos etc., aos usuários que, invariavelmente, caem nos golpes sem chance de defesa.

Como de praxe no mundo penal, uma vez identificados, os autores do delito são processados e julgados, conforme manda a legislação penal e processual penal, atentando-se para a seguinte situação: o Código Penal é datado do ano de 1940 e o Processual Penal de 1941, períodos em que jamais se cogitaria a existência da *internet*, computadores pessoais e crimes perpetrados atrás de um aparelho eletrônico. Por assim dito, nota-se que a aplicação

[5] Redes sociais voltadas para a comunicação interativa, entre usuários integrantes de uma rede, por meio do compartilhamento de perfis, fotos, vídeos e recados.
[6] Redes sociais voltadas para o envio e resposta de perguntas, bem como atualizações de *status* pessoais particulares ou em grupo.

dessas leis se dá por meio da analogia, ou seja, o magistrado busca encaixar as condutas tipificadas no Código Penal e em leis esparsas ao caso concreto, de modo a conseguir repelir a agressão vinda pelo meio intangível.

De igual maneira ocorre na seara cível, que, embora juvenil em comparação à legislação penal (2002), não abarca em seu texto legal a reparação civil por danos advindos das relações digitais, utilizando-se o juiz da analogia para a fixação da obrigação e do *quantum* indenizatório que será devido à determinada ou determinadas vítimas das ações, envolvendo os dispositivos informáticos.

Visto nas seções anteriores, os crimes destinados aos usuários das redes sociais são denominados impróprios, e geram a responsabilidade civil subjetiva, pois demandam a comprovação da culpa do agente.

Entretanto, pouco conhecida é a modalidade de responsabilização objetiva por crimes impróprios ou até mesmo próprios, essa que imputa não só ao causador direto do crime/dano, como, também, dos servidores, provedores, ou responsáveis pela subsistência da rede social, ou qualquer outra plataforma de comunicação e transação de dados por meio informático.

4.1 Da Responsabilidade Objetiva dos Provedores das Redes Sociais

Embora gratuita a utilização da maioria esmagadora das redes sociais, elas visam uma modalidade de lucro diferenciada/indireta, por meio de propagandas e diversas espécies de *marketing*, tornando-a um verdadeiro balcão de negócios, colocando seus usuários na condição de consumidores, mesmo que não paguem pelos serviços prestados, pois, como dito, o lucro vem indiretamente.

Provada a relação de consumo, é nítida a aplicação do Código de Defesa do Consumidor (Lei nº 8.078/90), que, em sua base (art. 14), suscita a responsabilidade civil objetiva, responsabilização de prestadores de serviços por danos causados aos seus usuários, independentemente de culpa. Exemplificando, por mais que um crime de difamação seja praticado por um único agente, utilizando-se de uma determinada rede social, ele será responsabilizado (subjetivamente), juntamente com a rede social, que terá sua cota de responsabilização (objetivamente).

É como entende o Superior Tribunal de Justiça que, em decisão recente no Agravo em Recurso Especial 229712-RJ, deixou clara a responsabilidade objetiva aos provedores das

redes sociais:

> RESPONSABILIDADE CIVIL. AGRAVO REGIMENTAL. INTERNET. VIOLAÇÃO DO ART. 535 DO CPC. NÃO OCORRÊNCIA. RESPONSABILIDADE DO PROVEDOR DE HOSPEDAGEM. PRECEDENTES DO STJ. REEXAME FÁTICO-PROBATÓRIO. IMPOSSIBILIDADE. SÚMULA N. 7 DO STJ. 1. Afasta-se a alegada violação do art. 535 do CPC quando o acórdão recorrido, integrado pelo julgado proferido nos embargos de declaração, dirime, de forma expressa, congruente e motivada, as questões suscitadas nas razões recursais. 2. O provedor é responsável pelos danos morais, caso mantenha-se inerte quando solicitado a retirar conteúdo ofensivo veiculado em site sob seu domínio. 3. Aplica-se a Súmula n. 7/STJ na hipótese em que a apreciação da tese versada no recurso especial reclama a análise dos elementos probatórios produzidos ao longo da demanda. 4. Agravo regimental desprovido. (STJ - AgRg no AREsp: 229712 RJ 2012/0191852-6, Relator: Ministro JOÃO OTÁVIO DE NORONHA, Data de Julgamento: 04/02/2014, T3 - TERCEIRA TURMA, Data de Publicação: DJe 14/02/2014).

Portanto, uma vez notificado a retirar o conteúdo pejorativo do ar, aquele que se mantém inerte será responsabilizado, objetivamente, pelo dano causado a seus usuários.

Quanto à relação de consumo existente entre os provedores e os usuários, o Superior Tribunal de Justiça, também, se manifesta no REsp. 1193764/SP (em anexo), demonstrando, claramente, o suprassumo dos entendimentos, em que, o provedor da rede social, por exercer atividade presumida de risco, assume, objetivamente, qualquer dano advindo nos intermédios de suas subsidiárias. Assim, vicinal responsabilizá-lo com o mesmo grau de culpa que o utilizador de má-fé empregou em sua conduta criminosa.

Vê-se, a seguir, um pouco da legislação internacional atinente ao conteúdo em pauta, aplicando-a, ou não, à atual realidade jurídica brasileira.

5 O MUNDO JURÍDICO DIGITAL INTERNACIONAL

Aclarada a responsabilidade civil, juntamente com os crimes que a desencadeiam, observando que o exposto está intimamente ligado ao ordenamento jurídico brasileiro, passa-se a analisar um pouco do direito internacional que atina, também, às relações digitais, visto que o próximo tema é a proposta de uma legislação virtual brasileira própria, ou seja, aferir-se-á se existe, ou não, a necessidade da criação de uma lei específica totalmente voltada aos crimes cibernéticos – e sua decorrente responsabilidade cível -, eis que existe apenas uma

miscigenação de cartas jurídicas, independentes e cronologicamente incompatíveis.

A Convenção de Budapeste[7], em vigor desde 2004, vem tipificar diversas condutas relacionadas à informática e suas sanções, estabelecer conceitos e princípios, complementar todas as espécies de autoria, participação, e até envolvimento dos crimes com menores, além de uma série de peculiaridades que passam a reger com eficácia os crimes advindos das relações digitais.

Pela imensidão jurídica que paira sobre os cinco continentes, impossível seria citar legislação por legislação, lei por lei, crime virtual por crime virtual; por esta assertiva, mantém-se o foco principal na Convenção sobre o *cybercrime*, que abriu diversas vertentes para o desenvolvimento das legislações. Igualmente, é imperioso ressaltar que o Brasil não é signatário de tal convenção, sendo uma afronta total aos próprios direitos humanos, que devem ser resguardados de todas as maneiras e modalidades que necessitem ser protegidos.

Essa afronta é explicada da seguinte maneira: "De acordo com o Secretário-Geral do Ministério das Relações Exteriores, Samuel Pinheiro Guimarães, o país só pode se tornar signatário do tratado se for convidado pelo Comitê de Ministros do Conselho Europeu." (SAFERNET, 2007).

A verdade acompanha a citação, pois, realizado em Budapeste, em 2001, o acordo a respeito dos ilícitos informáticos tem como signatários apenas os Estados Membros do Conselho da Europa, aos não membros que participaram da sua elaboração e aos Estados convidados, ressaltando que o Brasil não atende a nenhuma dessas modalidades, restando, apenas, a elaboração de leis em observância à Convenção, para uma melhor padronização e mesmo homogeneização do assunto, que tanto é versado nos tribunais internacionais.

6 DA CRIAÇÃO DE UMA LEI/ESTATUTO VIRTUAL

Ante o visto, é transparente a necessidade que o Brasil possui de ter uma junção legislativa própria, assim, sendo a aglomeração de dispositivos materiais num só local.

[7]Criada em 2001, na Hungria, pelo Conselho da Europa, e em vigor desde 2004, a Convenção de Budapeste, ou Convenção sobre o *Cybercrime*, engloba mais de 20 países e tipifica os principais crimes cometidos na *Internet*. (LOPES et al, 2009).

Poderia ser chamado de Estatuto Virtual, Lei dos Crimes Virtuais/Cibernéticos ou mesmo Lei dos *cybercrimes*, contendo em um só Código Digital todas as tipificações, procedimentos e processo dos crimes e da própria responsabilidade civil advinda do dano em uma relação informática.

Nos moldes atuais, a defasagem é uma telespectadora assídua do ordenamento jurídico pátrio, pois ele vem tratar o assunto cibernético apoiado no Princípio da Especialidade, logo, se o crime versa sobre criança e adolescente, ele está tipificado no Estatuto da Criança e Adolescente; se aduz direito eleitoral, ele está no Código Eleitoral; e assim segue: Código Penal, Código Penal Militar, Lei dos Direitos Autorais e outras legislações específicas.

O fato de fazer uma junção jurídica com os crimes e o processo de responsabilização civil em um só documento não iria em nada atrapalhar quaisquer procedimentos investigatórios ou mesmo ação penal, mas, sim, agilizá-los-ia a ponto de se falar em um Código de Processo Digital, isto é, como a perpetração daqueles se dão de maneira diferenciada do crime comum, justo seria, também, tratar as investigações de maneira diferenciada, visando o escopo de localizar o infrator virtual e o responsabilizar criminal e civilmente por seus delitos.

Portanto, Rafael Fernandes responde à pergunta: – o Brasil precisa de uma lei para os crimes eletrônicos?

> Sendo o Brasil um país de tradições positivistas e sendo vedada a aplicação de analogia para criar tipos penais, não nos resta dúvida em responder afirmativamente a essa indagação. Especialmente para algumas condutas como a invasão de sistemas, tão específica e sem previsão semelhante no atual ordenamento [...] Talvez com a previsão dessas condutas específicas, passaremos a obter melhores resultados punitivos. Talvez (e somente talvez) em razão de que não é esse o único problema na persecução de crimes cibernéticos. (MACIEL, 2012).

Necessária a atenção, também, ao meio físico/estrutural, pois é dever e necessidade do Estado equipar as polícias judiciárias e o próprio Poder Judiciário com equipamentos e pessoas treinadas para sua utilização e com a meta de combater a criminalidade digital, não deixando tudo a cargo dos legisladores e da lei em si.

Não é de olvidar que a criação dessa Lei/Estatuto não ocorreu pelo fator tempo. Igualmente, não é omissão dos legisladores quanto ao tema, porque, a evolução tecnológica e social sempre está à frente da jurídica. Exemplo é o próprio Código Penal, que, desde 1940, vem sendo ajustado e atualizado para servir com eficiência e eficácia à nação, diferentemente da *internet*, que foi popularizada no Brasil a partir dos anos 1990, sendo, assim, uma criança perante o Direito.

7 CONSIDERAÇÕES FINAIS

Com a evolução tecnológica, é proporcionada ao meio social uma série de inovações, benefícios e facilidades, como a rápida comunicação, o livre acesso à informação com o auxílio da *internet* e mesmo a agilidade no cometimento de condutas ilícitas.

Como exposto, é contundente a perpetração de crimes pelos meios digitais, ocasião em que, utilizando um aparelho eletrônico/cibernético um agente tem a faculdade de ferir diversos bens jurídicos, como a própria informação (crime digital próprio), ou mesmo o ser humano (crime digital impróprio), erigindo, nesta e na maioria das vezes, o direito das vítimas em serem ressarcidas dos eventuais prejuízos e/ou danos advindos com a transgressão.

Visível se tornam as modalidades da responsabilidade civil, ocupando a subjetiva o espaço vislumbrado à culpa e à intenção do criminoso, e a objetiva, abrangendo os responsáveis pela mantença do meio pelo qual ocorreu a agressão – como, por exemplo, os provedores das redes sociais.

Diretamente ligadas ao seio desta pesquisa científica, as redes sociais têm papel basilar na construção de um antijurídico, pois, por elas é que, na maioria das vezes, os crimes ocorrem; assim, é a veiculação principal e de mais fácil acesso que *crackers*[8], ou mesmo, inexperientes e aventureiros no meio digital se aproveitam para lesar outrem, seja seu patrimônio ou imagem, como, por exemplo, a transferência bancária não autorizada e a exposição de fotos sensuais.

Como de praxe, uma vez localizados os malfeitores e atribuída a eles a

[8]Pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos. (MARTINS, 2012).

responsabilidade criminal e cível, devem responder nos termos e limites da lei.

Uniformemente, desconhecida pela maioria populacional, mas tratada com o devido amparo neste artigo, vem a responsabilidade civil objetiva dos provedores das redes sociais - instituto adotado pelo ordenamento civil brasileiro – atribuir, não somente ao causador do dano, ou seja, àquele que deu causa dolosa ou culposamente ao crime, mas, também, ao provedor/mantenedor dos domínios que, de certa maneira, foi utilizado para a prática antimoral, a obrigação de indenizar. São os casos em que a própria rede social, independente de culpa, tendo em vista seu mister, deve reparar objetivamente as vítimas.

Saindo da esfera nacional, buscando um espelho para futuras modificações na legislação brasileira, pois o Brasil não possui uma lei fixa que trate dos crimes virtuais e seu processamento, muitas vezes, aplicando, com analogia, o Código Penal e legislações esparsas que outrora foram criadas para punir atos físicos e não informáticos –, tem-se, como principal modelo, a Convenção de Budapeste, que traz todos os componentes necessários para criar uma lei eficaz e eficiente, não deixando de citar que os legisladores desta Convenção Informática não convidaram o Brasil para ser um de seus signatários (apenas países europeus), mas, tem-se o modelo para a criação de algo que dê resultados positivos, do ponto de vista a repreender/sancionar e responsabilizar os praticantes de crimes virtuais.

É o método a ser seguido pelos legisladores infraconstitucionais, pois, uma vez conhecido o conteúdo da Convenção de Budapeste, e, sabendo que ele foi objeto de amplo estudo, antes de ser colocado em pauta para votação, tem-se na Convenção uma fonte segura para analogias e, mesmo, espelho para futuras criações de leis no Brasil, algo que não vem ocorrendo com frequência, sabendo que a última razoável inovação em vigência no jurídico-virtual ocorreu em 30 de novembro de 2012 (Lei nº 12.737 – "Lei Carolina Dieckmann"**)**, acrescentando tão somente 2 (dois) artigos ao defasado Código Penal de 1940 (art. 154-A e 154-B) – que, por sinal, é o instrumento-mestre na aplicação de sanções para os *cybercrimes*, sendo que nos envoltos da sua criação não se cogitava sequer da existência do recurso chamado *internet*.

Respondendo à questão principal, se a legislação civil/penal brasileira possui ferramentas eficientes e eficazes, a ponto de ressarcir os danos causados a outrem por meios digitais, tem-se uma negativa, isto é, a legislação brasileira, independente se cível ou penal, não possui ferramentas eficientes e eficazes para ressarcir os danos causados a outrem por

meios digitais, e mesmo para sua eficaz repreensão dos crimes conexos ao meio informático.

Conclui-se, então, que é necessária, sim, sendo inclusive uma necessidade com característica de urgência, a criação de uma Lei/Estatuto Virtual de âmbito nacional, isto é, algo que abarque e tire a especialidade das legislações quanto aos crimes virtuais, pois há a indispensabilidade da punição diferenciada dos crimes, envolvendo a informática, não se olvidando da essencialidade de implemento estrutural aos órgãos persecutórios da lei.

Como visto, embora haja a responsabilização objetiva, nos casos em que há a efetiva lesão, em decorrência de um dano por meio de uma rede social, o caminho a se percorrer até a localização do criminoso e o método a ser utilizado pela justiça é ultrapassado, vez que a ciência da informática é juvenil perante o direito e a tecnologia existente no Brasil. Interpõe-se como única ideia de solução para tal deficiência a criação do já comentado Estatuto Virtual único, que abarque todas as espécies de tipificação, processos e modalidades em que as condutas virtuais possam se abarcar, para, assim, obter justiça propriamente dita, justa, consubstanciada em ferramenta eficiente e eficaz.

8 REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Decreto-Lei n. 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, de 31.12.1940.

_____. **Lei n. 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, de 12.9.1990.

_____. **Lei n. 9.609, de 19 de fevereiro de 1998.** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da União, de 20.02.1998.

_____. **Lei n. 9.983, de 14 de julho de 2000.** Altera o Decreto-Lei n. 2.848, de 07 de dezembro de 1940 – Código Penal. Diário Oficial da União, de 17.7.2000.

_____. **Lei n. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União, de 11.1.2002.

_____. **Lei n. 11.829, de 25 de novembro de 2008.** Altera a Lei n. 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente. Diário Oficial da União, de 26.11.2008.

_____. **Lei n. 12.737, de 30 de novembro de 2012.** Dispões sobre tipificação criminal de

delitos informáticos. Diário Oficial da União, de 03.12.2012.

_____. Superior Tribunal de Justiça. **Acordão no Recurso Especial n. 1.193.764-SP**. Rel. Ministra ANDRIGHI Nancy. Publicado no DJe de 08.08.2011.

_____. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial**. Rel. Ministro NORONHA João Otávio de. Publicado no DJe de 14.02.2014.

BUDAPESTE. **Convenção sobre o Cybercrime.** Conselho da Europa, 23.11.2001.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CUSTÓDIO, Helita Barreira. **Responsabilidade civil por dano ao meio ambiente**. Campinas: Millenium, 2006.

LEITE, Luís Marcos. **O que são as Redes Sociais.** Disponível em: <http://ogestor.eti.br/o-que-sao-redes-sociais/>. Acesso em: 27 de janeiro de 2014.

LOPES, Gills et al. **A Convenção de Budapeste sobre Cibercrimes.** Disponível em: <http://www.mundialistas.com.br/blog/index. php/a-convencao-de-budapeste-por-gills-lopes/>. Acesso em 24 de março de 2014.

MACIEL, Rafael Fernandes. **O Brasil precisa de uma lei para os crimes eletrônicos?** Disponível em: <http://ultimainstancia.uol.com.br/conteudo/artigos/58571/o+brasil+precisa+de+uma+lei+para+os+crimes+eletronicos.shtml>. Acesso em 27 de janeiro de 2014.

MARTINS, Elaine. **O que é cracker?** Disponível em: <http://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm>. Acesso em 24 de março de 2014.

PAGANELLI, Celso Jefferson Messias. **Responsabilidade objetiva dos provedores de conteúdo na internet.** Disponível em: <http://www.crimespelainternet.com.br/tag/redes-sociais/>. Acesso em: 27 de janeiro de 2014.

SAFERNET, Jornalistas. **Brasil não pode aderir a Convenção de Budapeste sobre o Cibercrime**. Disponível em: <http://www.safernet.org.br/site/noticias/brasil-n%C3%A3-pode-aderir-conven%C3%A7-budapeste-sobre-cibercrime>. Acesso em: 27 de janeiro de 2014.

ANEXO

Revista FACISA *ON-LINE.* Barra do Garças – MT, vol.6, n.3, p. 174 -188, jul. - dez. 2017.
(ISSN 2238-8524)

ANEXO I

"DIREITO CIVIL E DO CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO SITE PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA. ***1.*** *A exploração comercial da internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90.****2.*** *O fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração" contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor.* ***3.*** *A fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos.* ***4.*** *O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02.****5.*** *Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada.****6.*** *Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de ropiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo.* ***7.*** *Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que*

corresponde à diligência média esperada dessa modalidade de provedor de serviço de internet. ***8.*** *Recurso especial a que se nega provimento.*" (REsp 1193764/SP, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 14/12/2010, DJe 08/08/2011).

RECURSO ESPECIAL Nº 1.193.764 - SP (2010/0084512-0)
RELATORA : MINISTRA NANCY ANDRIGHI

RECORRENTE : I P DA S B

ADVOGADO : SÉRGIO LUIZ AKAOUI MARCONDES E OUTRO(S)

RECORRIDO : GOOGLE BRASIL INTERNET LTDA

ADVOGADO : FERNANDA DE GOUVÊA LEÃO E OUTRO(S)

VOTO

A EXMA. SRA. MINISTRA NANCY ANDRIGHI (Relator):

Cinge-se a lide a determinar se provedor de rede social de relacionamento via *internet* é responsável pelo conteúdo das informações veiculadas no respectivo *site*.

I. Da negativa de prestação jurisdicional. Violação do art. 535, II, do CPC.

Da análise do acórdão recorrido, constata-se que a prestação jurisdicional dada corresponde àquela efetivamente objetivada pelas partes, sem vício que pudesse ter sido sanado pela via dos embargos de declaração. O TJ/SP se pronunciou de maneira a discutir todos os aspectos fundamentais do julgado, dentro dos limites que lhe são impostos por lei, tanto que integram o objeto do próprio recurso especial e serão enfrentados logo adiante. O não acolhimento das teses contidas no recurso não implica obscuridade, contradição ou omissão, pois ao julgador cabe apreciar a questão conforme o que ele entender relevante à lide. O tribunal não está obrigado a julgar a questão posta a seu exame nos termos pleiteados pelas partes, mas sim com o seu livre convencimento, consoante dispõe o art. 131 do CPC. Por outro lado,

encontra-se pacificado no STJ o entendimento de que os embargos declaratórios, mesmo quando manejados objetivando o prequestionamento, são inadmissíveis se a decisão embargada não ostentar qualquer dos vícios que autorizariam a sua interposição. Confiram-se os precedentes: AgRg no Ag 680.045⁄MG, 5ª Turma, Rel. Min. Félix Fischer, DJ de 03.10.2005; EDcl no AgRg no REsp 647.747⁄RS, 4ª Turma, Rel. Min. Aldir Passarinho Junior, DJ de 09.05.2005; EDcl no MS 11.038⁄DF, 1ª Seção, Rel. Min. João Otávio de Noronha, DJ de 12.02.2007. Constata-se, na realidade, o inconformismo da recorrente e a tentativa de imprimir aos embargos de declaração efeitos infringentes, o que não se mostra viável no contexto do mencionado recurso. Assim, não se vislumbra violação do art. 535 do CPC.

II. Do dano moral. Violação do art. 14 do CDC.

De acordo com a recorrente, "o *site* em questão configura uma prestação de serviços colocada à disposição dos usuários da rede" (fl. 336, e-STJ), concluindo, por conseguinte, pela "existência de responsabilidade objetiva" (fl. 342, e-STJ). Aduz que "o compromisso assumido de exigir que os usuários se identifiquem não foi honrado, fato que gera a falha do serviço" (fl. 337, e-STJ). Finalmente, afirma haver "fomentação do anonimato propiciado pela negligência na prestação do serviço pela recorrida" (fl. 343, e-STJ). O TJ⁄SP, por sua vez, consigna que a fiscalização pretendida pela recorrente, "na prática, implica exame de todo o material que transita pelo *site* (...), tarefa que não pode ser exigida de um provedor de serviço de hospedagem", bem como que "a verificação do conteúdo das veiculações implicaria, no fundo, restrição da livre manifestação do pensamento" (fls. 287⁄288, e-STJ).

(i) A natureza jurídica do serviço prestado pelo ORKUT.

Inicialmente, é preciso determinar a natureza jurídica dos provedores de serviços de *internet*, em especial do GOOGLE, pois somente assim será possível definir os limites de sua responsabilidade e a existência de relação de consumo. A *world wide web* (www) é uma rede mundial composta pelo somatório de todos os servidores a ela conectados. Esses servidores são bancos de dados que concentram toda a informação disponível na *internet*, divulgadas por intermédio das incontáveis páginas de acesso (*webpages*). Os provedores de serviços de

internet são aqueles que fornecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio dela. Trata-se de gênero do qual são espécies as demais categorias, tais como: (i) provedores de *backbone* (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade da *internet*, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores *backbone* e revendem aos usuários finais, possibilitando a esses conexão com a *internet*; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na *internet*; e (v) provedores de conteúdo, que disponibilizam na rede as informações criadas ou desenvolvidas pelos provedores de informação. É frequente que provedores ofereçam mais de uma modalidade de serviço de *internet*; daí a confusão entre essas diversas modalidades. Entretanto, a diferença conceitual subsiste e é indispensável à correta imputação da responsabilidade inerente a cada serviço prestado. Na hipótese específica do ORKUT, comunidade virtual na qual foram veiculadas as informações tidas por ofensivas, verifica-se que o GOOGLE atua como provedor de conteúdo, pois o *site* disponibiliza informações, opiniões e comentários de seus usuários. Estes usuários criam páginas pessoais (perfis), por meio das quais se relacionam com outros usuários e integram grupos (comunidades), igualmente criados por usuários, nos quais se realizam debates e troca de informações sobre interesses comuns.

(ii) A sujeição dos serviços de internet ao CDC.

Parece inegável que a exploração comercial da *internet* sujeita as relações jurídicas de consumo daí advindas à Lei nº 8.078⁄90. Newton De Lucca aponta o surgimento de "uma nova espécie de consumidor (...) – a do consumidor internauta – e, com ela, a necessidade de proteção normativa, já tão evidente no plano da economia tradicional" (***Direito e internet***: aspectos jurídicos relevantes, vol. II. São Paulo: QuartierLatin, 2008, p. 27).Com efeito, as peculiaridades inerentes a essa relação virtual não afastam as bases caracterizadoras de um negócio jurídico clássico: (i) legítima manifestação de vontade das partes; (ii) objeto lícito, possível e determinado ou determinável; (iii) e forma prescrita ou não defesa em lei. Fernando

Antônio de Vasconcelos observa que "o serviço preconizado na Lei 8.078⁄90 é o mesmo prestado pelas várias empresas que operam no setor [rede virtual]. Fica, pois, difícil dissociar o prestador [provedor] de serviços da *internet* do fornecedor de serviços definido no Código de Defesa do Consumidor" (**Internet. Responsabilidade do provedor pelos danos praticados.** Curitiba: Juruá, 2004, p. 116). Vale notar, por oportuno, que o fato de o serviço prestado pelo provedor ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração" contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. Na lição de Cláudia Lima Marques, "a expressão 'remuneração' permite incluir todos aqueles contratos em que for possível identificar, no sinalagma escondido (contraprestação escondida), uma remuneração indireta do serviço" (**Comentários ao código de defesa do consumidor**: arts. 1º ao 74. São Paulo: RT, 2003, p. 94). No caso do GOOGLE, é clara a existência do chamado *cross marketing*, consistente numa ação promocional entre produtos ou serviços em que um deles, embora não rentável em si, proporciona ganhos decorrentes da venda de outro. Apesar de gratuito, o *ORKUT* exige que o usuário realize um cadastro e concorde com as condições de prestação do serviço, gerando um banco de dados com infinitas aplicações comerciais. Ademais, o ORKUT é importante ferramenta de divulgação e crescimento da marca "GOOGLE" – a mais valiosa do mundo, cujo valor, em 2009, foi estimado em mais de 100 bilhões de Dólares (http://techcrunch.com/2009/04/30/guess-which-brand- is-now-worth-100-billion) – diretamente atrelada à venda de produtos do GOOGLE, em especial espaços de publicidade em outros *site*s por ela mantidos. Retomando os ensinamentos de Cláudia Lima Marques, a autora anota que "estas atividades dos fornecedores visam lucro, são parte de seu *marketing* e de seu preço total, pois são remunerados na manutenção do negócio principal", concluindo que "no mercado de consumo, em quase todos os casos, há remuneração do fornecedor, direta ou indireta, como um exemplo do 'enriquecimento' dos fornecedores pelos serviços ditos 'gratuitos' pode comprovar" (*op. cit*., p. 95).Há, portanto, inegável relação de consumo nos serviços de *internet*, ainda que prestados gratuitamente.

(iii) Os limites da responsabilidade do GOOGLE.

Não obstante a indiscutível existência de relação de consumo no serviço prestado por intermédio do ORKUT, a responsabilidade do GOOGLE deve ficar restrita à natureza da atividade por ele desenvolvida naquele *site*, que, a partir do quanto visto linhas acima, corresponde à típica provedoria de conteúdo, disponibilizando na rede as informações encaminhadas por seus usuários. Nesse aspecto, o serviço do GOOGLE deve garantir o sigilo, a segurança e a inviolabilidade dos dados cadastrais de seus usuários, bem como o funcionamento e a manutenção das páginas na *internet* que contenham as contas individuais e as comunidades desses usuários. No que tange à fiscalização do conteúdo das informações postadas por cada usuário, não se trata de atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o *site* que não examina e filtra o material nele inserido. Conforme anota Rui Stocco, quando o provedor de *internet* age "como mero fornecedor de meios físicos, que serve apenas de intermediário, repassando mensagens e imagens transmitidas por outras pessoas e, portanto, não as produziu nem sobre elas exerceu fiscalização ou juízo de valor, não pode ser responsabilizado por eventuais excessos e ofensas à moral, à intimidade e à honra de outros" (**Tratado de responsabilidade civil.** 6ª ed. São Paulo: RT, 2004, p. 901). Tampouco se pode falar em risco da atividade como meio transverso para a responsabilização do provedor por danos decorrentes do conteúdo de mensagens inseridas em seu *site* por usuários. Há de se ter cautela na interpretação do art. 927, parágrafo único, do CC⁄02.No julgamento do REsp 1.067.738⁄GO, 3ª Turma, Rel. Min. Sidnei Beneti, minha relatoria para acórdão, DJe de 25.06.2009, tive a oportunidade de enfrentar o tema, tendo me manifestado no sentido de que "a natureza da atividade é que irá determinar sua maior propensão à ocorrência de acidentes. O risco que dá margem à responsabilidade objetiva não é aquele habitual, inerente a qualquer atividade. Exige-se a exposição a um risco excepcional, próprio de atividades com elevado potencial ofensivo". Roger Silva Aguiar bem observa que o princípio geral firmado no art. 927, parágrafo único, do CC⁄02, "inicia-se com a conjunção quando, denotando que o legislador acolheu o entendimento de que nem toda atividade humana importa em 'perigo' para terceiros com o caráter que lhe foi dado na terceira parte do parágrafo" (**Responsabilidade civil objetiva**: do risco à solidariedade. São Paulo: Atlas, 2007, p. 50).Com base nesse entendimento, a I Jornada de Direito Civil, promovida pelo Centro de Estudos Judiciários do CJF, aprovou o Enunciado 38, que aponta interessante critério para definição dos riscos que dariam margem à

responsabilidade objetiva, afirmando que esta fica configurada "quando a atividade normalmente desenvolvida pelo autor do dano causar a pessoa determinada um ônus maior do que aos demais membros da coletividade". Transpondo a regra para o universo virtual, não se pode considerar o dano moral um risco inerente à atividade dos provedores de conteúdo. A esse respeito, Erica Brandini Barbagalo anota que as atividades desenvolvidas pelos provedores de serviços na *internet* não são "de risco por sua própria natureza, não implicam riscos para direitos de terceiros maior que os riscos de qualquer atividade comercial" (Aspectos da responsabilidade civil dos provedores de serviços da *internet*. *In* Ronaldo Lemos e Ivo Waisberg. **Conflitos sobre nomes de domínio**. São Paulo: RT, 2003, p. 361).Ademais, o controle editorial prévio do conteúdo das informações se equipara à quebra do sigilo da correspondência e das comunicações, vedada pelo art. 5º, XII, da CF⁄88.Não bastasse isso, a verificação antecipada, pelo provedor, do conteúdo de todas as informações inseridas na *web* eliminaria – ou pelo menos alijaria – um dos maiores atrativos da *internet*, que é a transmissão de dados em tempo real. Carlos Affonso Pereira de Souza vê "meios tecnológicos para revisar todas as páginas de um provedor", mas ressalva que esse procedimento causaria "uma descomunal perda na eficiência do serviço prestado, quando não vier a impossibilitar a própria disponibilização do serviço" (A responsabilidade civil dos provedores pelos atos de seus usuários na *internet*. *In* **Manual de direito eletrônico e internet**. São Paulo: Aduaneiras, 2006, p. 651). No mesmo sentido opina Paulo Nader, que considera inviável impor essa conduta aos provedores, "pois tornaria extremamente complexa a organização de meios para a obtenção dos resultados exigidos, além de criar pequenos órgãos de censura" (**Curso de direito civil.** vol. VII, 3ª ed. Rio de Janeiro: Forense, 2010, p. 385). Em outras palavras, exigir dos provedores de conteúdo o monitoramento das informações que veiculam traria enorme retrocesso ao mundo virtual, a ponto de inviabilizar serviços que hoje estão amplamente difundidos no cotidiano de milhares de pessoas. A medida, portanto, teria impacto social e tecnológico extremamente negativo. Mas, mesmo que, *ad argumentandum*, fosse possível vigiar a conduta dos usuários sem descaracterizar o serviço prestado pelo provedor, haveria de se transpor outro problema, de repercussões ainda maiores, consistente na definição dos critérios que autorizariam o veto ou o descarte de determinada informação. Ante à subjetividade que cerca o dano moral, seria impossível delimitar parâmetros de que pudessem se valer os provedores para definir se uma mensagem ou imagem é potencialmente ofensiva.

Por outro lado, seria temerário delegar o juízo de discricionariedade sobre o conteúdo dessas informações aos provedores. Por todos esses motivos, não vejo como obrigar do GOOGLE a realizar a prévia fiscalização do conteúdo das informações que circulam no *ORKUT*. Entretanto, também não é razoável deixar a sociedade desamparada frente à prática, cada vez mais corriqueira, de se utilizar comunidades virtuais como artifício para a consecução de atividades ilegais. Antônio Lindberg Montenegro bem observa que "a liberdade de comunicação que se defende em favor da *internet* não deve servir de passaporte para excluir a ilicitude penal ou civil que se pratique nas mensagens por ela transmitidas" (**A *internet* em suas relações contratuais e extracontratuais**. Rio de Janeiro: Lumen Juris, 2003, p. 174).Trata-se de questão global, de repercussão internacional, que tem ocupado legisladores de todo o mundo, sendo possível identificar, no direito comparado, a tendência de isentar os provedores de serviço da responsabilidade pelo monitoramento do conteúdo das informações veiculadas em seus *site*s. Os Estados Unidos, por exemplo, alteraram seu *Telecomunications Act*, por intermédio do *Communications Decency Act*, com uma disposição (47 U.S.C. § 230) que isenta provedores de serviços na *internet* pela inclusão, em seu *site*, de informações encaminhadas por terceiros. De forma semelhante, a Comunidade Europeia editou a Diretiva 2000/31, cujo art. 15, intitulado "ausência de obrigação geral de vigilância", exime os provedores da responsabilidade de monitorar e controlar o conteúdo das informações de terceiros que venham a transmitir ou armazenar. Contudo, essas normas não livram indiscriminadamente os provedores de responsabilidade pelo tráfego de informações em seus *site*s. Há, como contrapartida, o dever de, uma vez ciente da existência de mensagem de conteúdo ofensivo, retirá-la imediatamente do ar, sob pena, aí sim, de responsabilização. Existe no Brasil iniciativa semelhante, corporificada no Projeto de Lei nº 4.906/01, do Senado Federal, que, além de reconhecer expressamente a incidência do CDC ao comércio eletrônico (art. 30), isenta de responsabilidade os "provedores de transmissão de informações" da responsabilidade pelo conteúdo das informações transmitidas (art. 35) e desobriga-os de fiscalizar mensagens de terceiros (art. 37), mas fixa a responsabilidade civil e criminal do provedor de serviço que, tendo conhecimento inequívoco da prática de crime em arquivo eletrônico por ele armazenado, deixa de promover a imediata suspensão ou interrupção de seu acesso (art. 38). Realmente, essa parece ser o caminho mais coerente. Se, por um lado, há notória impossibilidade prática de controle, pelo provedor de conteúdo, de toda a informação

que transita em seu *site*; por outro, deve ele, ciente da existência de publicação de texto ilícito, removê-lo sem delongas. Patrícia Peck comunga dessa ideia e apresenta exemplo que se amolda perfeitamente à hipótese dos autos. A autora considera "tarefa hercúlea e humanamente impossível" que "a empresa GOOGLE monitore todos os vídeos postados em seu sítio eletrônico 'youtube', de maneira prévia", mas entende que, "ao ser comunicada, seja por uma autoridade, seja por um usuário, de que determinado vídeo/texto possui conteúdo eventualmente ofensivo e/ou ilícito, deve tal empresa agir de forma enérgica, retirando-o imediatamente do ar, sob pena de, daí sim, responder de forma solidária juntamente com o seu autor ante a omissão praticada (art. 186 do CC)" (**Direito digital**, 4ª ed. São Paulo: Saraiva, 2010, p. 401). Do quanto exposto até aqui, conclui-se que não se pode considerar de risco a atividade desenvolvida pelos provedores de conteúdo, tampouco se pode ter por defeituosa a ausência de fiscalização prévia das informações inseridas por terceiros no *site*, inexistindo justificativa para a sua responsabilização objetiva pela veiculação de mensagens de teor ofensivo. Por outro lado, ainda que, como visto, se possa exigir dos provedores um controle posterior, vinculado à sua efetiva ciência quanto à existência de mensagens de conteúdo ilícito, a medida se mostra insuficiente à garantia dos consumidores usuários da rede mundial de computadores, que continuam sem ter contra quem agir: não podem responsabilizar o provedor e não sabem quem foi o autor direto da ofensa. Cabe, nesse ponto, frisar que a liberdade de manifestação do pensamento, assegurada pelo art. 5º, IV, da CF/88, não é irrestrita, sendo "vedado o anonimato". Em outras palavras, qualquer um pode se expressar livremente, desde que se identifique. Dessa forma, ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. A esse respeito, Marcel Leonardi observa que o provedor deve exigir do usuário, conforme a natureza do serviço prestado, "os números de IP atribuídos e utilizados pelo usuário, os números de telefone utilizados para estabelecer conexão, o endereço físico de instalação dos equipamentos utilizados para conexões de alta velocidade e demais informações que se fizerem necessárias para prevenir o anonimato do usuário" (**Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Juarez de Oliveira, 2005, p. 82). Portanto, sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as

circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do *site*, sob pena de responsabilização subjetiva por culpa *in omittendo*.Com efeito, o provedor que, movido pela ânsia de facilitar o cadastro e aumentar exponencialmente o número de usuários, ou por qualquer outro motivo, opta por não exercer um mínimo de controle daqueles que se filiam ao seu *site*, assume o risco dessa desídia, respondendo subsidiariamente pelos danos causados a terceiros. Antônio Jeová Santos esclarece que a não identificação, pelo provedor, das pessoas que hospeda em seu *site*, "não o exime da responsabilidade direta, se o anônimo perpetrou algum ataque causador de dano moral. Não exigindo identificação dos seus usuários, assume o ônus e a culpa pelo atuar indiscreto, criminoso ou ofensivo à honra e intimidade acaso cometido" (**Dano moral na internet.** São Paulo: Método, 2001, p. 143). Note-se, por oportuno, que não se está, aqui, a propor uma burocratização desmedida da *internet*. O crescimento e popularidade da rede devem-se, em grande medida, justamente à sua informalidade e à possibilidade dos usuários a acessarem sem identificação. Essa liberdade tornou-se um grande atrativo, especialmente nos *sites* de relacionamento, em que pessoas desenvolvem "personalidades virtuais", absolutamente distintas de suas próprias, assumindo uma nova identidade, por meio da qual se apresentam e convivem com terceiros. Criou-se um "mundo paralelo", em que tudo é intangível e no qual há enorme dificuldade em se distinguir a realidade da fantasia. Outrossim, não se pode ignorar a importância e os reflexos econômicos da *internet*. O dinamismo e o alcance da rede a transformou num ambiente extremamente propício ao comércio. Porém, ainda que concretizados de forma virtual, esses negócios exigem segurança jurídica. E, nesse universo, a identificação das pessoas se torna fundamental. Dessarte, quanto mais a *web* se difunde, maior o desafio de se encontrar um limite para o anonimato dos seus usuários, um equilíbrio entre o virtual e o material, de modo a proporcionar segurança para as inúmeras relações que se estabelecem via *internet*, mas sem tolher a informalidade que lhe é peculiar. Nesse aspecto, por mais que se queira garantir a liberdade daqueles que navegam na *internet*, reconhecendo-se essa condição como indispensável à própria existência e desenvolvimento da rede, não podemos transformá-la numa "terra de ninguém", em que, sob o pretexto de não aniquilar as suas virtudes, se acabe por tolerar sua utilização para a prática dos mais variados abusos. A *internet* é sem dúvida uma ferramenta consolidada em âmbito mundial, que se incorporou no cotidiano de todos nós, mas cuja continuidade depende da criação de mecanismos capazes de

reprimir sua utilização para fins perniciosos, sob pena dos malefícios da rede suplantarem suas vantagens, colocando em xeque o seu futuro. Diante disso, ainda que muitos busquem na *web* o anonimato, este não pode ser pleno e irrestrito. A existência de meios que possibilitem a identificação de cada usuário se coloca como um ônus social, a ser suportado por todos nós objetivando preservar a integridade e o destino da própria rede. Isso não significa colocar em risco a privacidade dos usuários. Os dados pessoais fornecidos ao provedor devem ser mantidos em absoluto sigilo – tal como já ocorre nas hipóteses em que se estabelece uma relação sinalagmática via *internet*, na qual se fornece nome completo, números de documentos pessoais, endereço, número de cartão de crédito, entre outros – sendo divulgados apenas quando se constatar a prática de algum ilícito e mediante ordem judicial. Também não significa que se deva exigir um processo de cadastramento imune a falhas. A mente criminosa é sagaz e invariavelmente encontra meios de burlar até mesmo os mais modernos sistemas de segurança. O que se espera dos provedores é a implementação de cuidados mínimos, consentâneos com seu porte financeiro e seu *know-how* tecnológico – a ser avaliado casuisticamente, em cada processo – de sorte a proporcionar aos seus usuários um ambiente de navegação saudável e razoavelmente seguro. Em suma, pois, tem-se que os provedores de conteúdo: (i) não respondem objetivamente pela inserção no *site*, por terceiros, de informações ilegais; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no *site* por seus usuários; (iii) devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no *site*, removê-los imediatamente, sob pena de responderem pelos danos respectivos; (iv) devem manter um sistema minimamente eficaz de identificação de seus usuários, cuja efetividade será avaliada caso a caso. Ainda que não ideais, certamente incapazes de conter por completo a utilização da rede para fins nocivos, a solução ora proposta se afigura como a que melhor equaciona os direitos e deveres dos diversos *players* do mundo virtual. Na análise de Newton De Lucca, "a implementação de medidas drásticas de controle de conteúdos na *internet* deve ser reservada para casos extremos, quando estiver presente manifesto interesse público e desde que ponderado o potencial prejuízo causado a terceiros, não havendo de ser adotada nas demais hipóteses, principalmente quando se tratar de interesse individual, salvo em situações absolutamente excepcionais, que representarão exceções raríssimas" (op. cit., p. 400).As adversidades indissociáveis da tutela das inovações criadas pela era digital dão origem a

situações cuja solução pode causar certa perplexidade. Há de se ter em mente, no entanto, que a *internet* é reflexo da sociedade e de seus constantes avanços. Se, ainda hoje, não conseguimos tutelar com total equidade direitos seculares e consagrados, seria tolice contar com resultados mais eficientes nos conflitos relativos à rede mundial de computadores.

(iv) A hipótese dos autos.

A recorrente interpôs a presente ação objetivando compelir o GOOGLE a suprimir do ORKUT texto cujo conteúdo considerava ofensivo à sua pessoa, bem como para ser indenizada pelos respectivos danos morais. Houve a concessão de tutela antecipada, para o fim de determinar a "exclusão de todo o material ofensivo que relacione o nome da autora" (fl. 148, e-STJ), tendo o GOOGLE prontamente dado cumprimento à ordem judicial, esclarecendo que a comunidade onde estavam sendo veiculadas as informações "foi removida em 28 de abril do corrente ano" (fl. 195, e-STJ).Nesse ponto, portanto, não houve ilegalidade nos atos praticados pelo GOOGLE que, uma vez ciente da existência de material de conteúdo ofensivo, adotou todas as providências tendentes à sua imediata remoção do site. Além disso, em consulta ao *site* do ORKUT na *internet*, verifica-se que o GOOGLE disponibiliza um canal para que as pessoas – usuários ou não – que tiveram sua identidade "roubada" solicitem a exclusão da conta falsa, bem como para que seja feita a denúncia de abusos na utilização de perfis individuais ou comunidades(http://www.google.com/support/orkut/bin/answer.py?hl=br&query=estatuto&answer=16198). Outrossim, cumpre verificar se o GOOGLE também adotou as medidas que estavam ao seu alcance visando à identificação do responsável pela inclusão no *ORKUT* dos dados agressivos à moral da recorrente. O próprio GOOGLE admite que a recorrente "informou especificamente nos autos a URL correspondente à página com o conteúdo ofensivo" (fl. 195, e-STJ).URL é a sigla que corresponde à expressão *Universal Resource Locator*, que em português significa localizador universal de recursos. Trata-se de um endereço virtual, isto é, diretrizes que indicam o caminho até determinado *site* ou página. Dessa forma, com base na URL fornecida pela recorrente, foi possível ao GOOGLE localizar especificamente a página na qual havia sido inserido o material de conteúdo ofensivo. A partir daí, teve condições de identificar o usuário daquela página e os dados obtidos no ato de cadastramento da sua conta, inclusive o IP (*internet protocol*), que é um número único, exclusivo, que individualiza cada computador na rede e por meio do qual cada máquina se

identifica e se comunica. O próprio GOOGLE informa que "todo usuário quando se conecta à internet recebe um número de identificação (IP: 'Internet Protocol') que possibilita o seu rastreamento e a localização de seus dados pessoais, como nome, endereço, CPF, RG etc.", ressalvando não haver pedido de identificação dos usuários responsáveis pela criação do material reputado ofensivo (...), de modo que jamais poderia apresentar os dados dos mesmos nos autos, sob pena de ser acusada e responsabilizada pela violação da garantia do sigilo de tais informações" (fl. 272, e-STJ).Realmente, compulsando os autos não se verifica a existência de pedido para que fosse identificado o autor direto das supostas ofensas, tampouco qualquer ordem judicial nesse sentido. Seja como for, o GOOGLE esclareceu que registra o número de protocolo na *internet* (IP) dos computadores utilizados para o cadastramento de cada conta, por meio do qual, em princípio, é possível identificar o respectivo usuário. Ainda que não exija os dados pessoais dos usuários do ORKUT, o GOOGLE mantém um meio razoavelmente eficiente de rastreamento desses usuários, medida de segurança que corresponde à diligência média esperada de um provedor de conteúdo. Portanto, não se vislumbra responsabilidade do GOOGLE pela veiculação das mensagens cujo conteúdo a recorrente considerou ofensivo à sua moral.

Forte nessas razões, NEGO PROVIMENTO ao recurso especial.

VOTO-MÉRITO

EXMO. SR. MINISTRO MASSAMI UYEDA:

Srs. Ministros, eu havia recebido o voto da Sra. Ministra Relatora e acompanhei a leitura do excelente voto, cumprimentando o Advogado, também, pela sustentação oral. É um dos primeiros casos - senão o primeiro - que estamos apreciando, e V. Exa., Sra. Ministra Nancy Andrighi, presta um relevante serviço para orientar a todos nós o que é esse mundo virtual. Realmente, pela leitura, o voto de V. Exa. é realmente um guia muito seguro para que possamos, também, entender esse mecanismo. E esse direito que têm os provedores, de serem elementos de comunicação, também não pode responsabilizá-los pelo excesso e abuso de seus usuários. V. Exa. muito bem ressaltou, aqui, que os mecanismos de segurança devem ser

observados pelo provedor. E isso foi feito, aqui, neste caso. Acompanho integralmente o voto de V. Exa., negando provimento ao recurso especial, e faço uma recomendação para a jurisprudência.

VOTO

O EXMO. SR. MINISTRO PAULO DE TARSO SANSEVERINO (Relator):
Sr. Presidente, o voto da eminente Relatora é modelar. S. Exa. se apoia na melhor doutrina e resolve uma das questões mais intrincadas que existem hoje a respeito da responsabilidade civil dos provedores de *Internet*. O voto é excelente e resolve todas as questões. Resta-nos, apenas, acompanhá-lo, negando provimento ao recurso especial, sugerindo-o também à publicação.

VOTO

O SR. MINISTRO VASCO DELLA GIUSTINA (DESEMBARGADOR CONVOCADO DO TJ⁄RS):

Sr. Presidente, faço minhas as palavras dos Colegas que me antecederam. Louvo o esmerado voto, aliás como sói acontecer com os pronunciamentos de S. Exa., e lembro, justamente, que se trata da primeira decisão envolvendo essa matéria tão importante em nosso dia-a-dia. Recomendo-o também à publicação, evidentemente. Nego provimento ao recurso especial.

CERTIDÃO

Certifico que a egrégia TERCEIRA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:
A Turma, por unanimidade, negou provimento ao recurso especial, nos termos do voto do(a) Sr(a). Ministro(a) Relator(a). Os Srs. Ministros Massami Uyeda, Sidnei Beneti, Paulo de Tarso Sanseverino e Vasco Della Giustina (Desembargador convocado do TJ⁄RS) votaram com a Sra. Ministra Relatora.